# ETSI TS 129 244 V14.1.0 (2017-10)


**LTE;**
**Interface between the Control plane Plane and the User Plane of EPC Nodes**
**(3GPP TS 29.244 version 14.1.0 Release 14)**


Reference
RTS/TSGC-0429244ve10

Keywords
LTE

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

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

# Foreword

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

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

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

# Modal verbs terminology

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

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

# Contents

# Foreword

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

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

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

# 1 Scope

The present document specifies the Packet Forwarding Control Protocol (PFCP) used on the interface between the control plane and the user plane function in a split SGW, PGW and TDF architecture in EPC.

The architecture reference model and stage 2 information are specified in 3GPP TS 23.214 [2].

PFCP shall be used over the Sxa, Sxb, Sxc and the combined Sxa/Sxb reference points.

PFCP shall also be used over the Sxa' and Sxb' reference points specified in 3GPP TS 33.107 [20]. In the rest of this specification, no difference is made between Sxa and Sxa', or between Sxb and Sxb'. The Sxa' and Sxb' reference points reuse the protocol specified for the Sxa and Sxb reference points, but comply in addition with the security requirements specified in clause 8 of 3GPP 33.107 [20].

# 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: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.214: "Architecture enhancements for control and user plane separation of EPC nodes; Stage 2".

[3] 3GPP TS 29.281: "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)".

[4] IETF RFC 768: "User Datagram Protocol".

[5] IETF RFC 791: "Internet Protocol".

[6] IETF RFC 2460: "Internet Protocol, Version 6 (IPv6) Specification".

[7] 3GPP TS 23.203: "Policy and charging control architecture; Stage 2".

[8] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[9] 3GPP TS 29.274: "3GPP Evolved Packet System. Evolved GPRS Tunnelling Protocol for EPS (GTPv2)".

[10] 3GPP TS 36.413: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

[11] 3GPP TS 29.213: "Policy and Charging Control signalling flows and Quality of Service (QoS) parameter mapping".

[12] IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification".

[13] IETF RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[14] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[15] 3GPP TS 22.153: "Multimedia Priority Service".

[16] IETF RFC 4006: "Diameter Credit Control Application".

[17] 3GPP TS 32.251: "Telecommunication management; Charging management; Packet Switched (PS) domain charging".

[18] 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging application".

[19] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[20] 3GPP TS 33.107: "3G security; Lawful interception architecture and functions".

[21] 3GPP TS 29.251: "Gw and Gwn reference points for sponsored data connectivity".

[22] IETF RFC 2474, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[23] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[24] 3GPP TS 23.007: "Restoration procedures".

[25] 3GPP TS 29.303: "Domain Name System Procedures; Stage 3"

[26] IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification".

[27] IETF RFC 1035: "Domain Names - Implementation and Specification".

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**Match Field:** a field of the Packet Detection Information of a Packet Detection Rule against which a packet is attempted to be matched.

**Matching:** comparing the set of header fields of a packet to the match fields of the Packet Detection Information of a Packet Detection Rule.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

| | |
|---|---|
| ADC | Application Detection and Control |
| BAR | Buffering Action Rule |
| CP | Control Plane |
| DDoS | Distributed Denial of Service |
| DSCP | Differentiated Services Code Point |
| eMPS | enhanced Multimedia Priority Service |
| FAR | Forwarding Action Rule |
| F-SEID | Fully Qualified SEID |
| F-TEID | Fully Qualified TEID |
| IP | Internet Protocol |

| | |
|---|---|
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| LMISF | LI Mirror IMS State Function |
| PCC | Policy and Charging Control |
| PCEF | Policy and Charging Enforcement Function |
| PCRF | Policy and Charging Rule Function |
| PDI | Packet Detection Information |
| PDR | Packet Detection Rule |
| PFCP | Packet Forwarding Control Protocol |
| PFD | Packet Flow Description |
| PGW | PDN Gateway |
| PGW-C | PDN Gateway Control plane function |
| PGW-U | PDN Gateway User plane function |
| QER | QoS Enforcement Rule |
| S8HR | S8 Home Routed |
| SDF | Service Data Flow |
| SEID | Session Endpoint Identifier |
| SGW | Serving Gateway |
| SGW-C | Serving Gateway Control plane function |
| SGW-U | Serving Gateway User plane function |
| SX3LIF | Split X3 LI Interworking Function |
| TDF | Traffic Detection Function |
| TDF-C | Traffic Detection Function Control plane function |
| TDF-U | Traffic Detection Function User plane function |
| ToS | Type of Service |
| TSSF | Traffic Steering Support Function |
| UDP | User Datagram Protocol |
| UP | User Plane |
| URR | Usage Reporting Rule |

# 4 Protocol Stack

## 4.1 Introduction

The protocol stack for the control plane over the Sxa, Sxb, Sxc and combined Sxa/Sxb reference points shall be as depicted in Figure 4.1-1. Subclauses 4.2 and 4.3 further specify the related UDP and IP requirements.

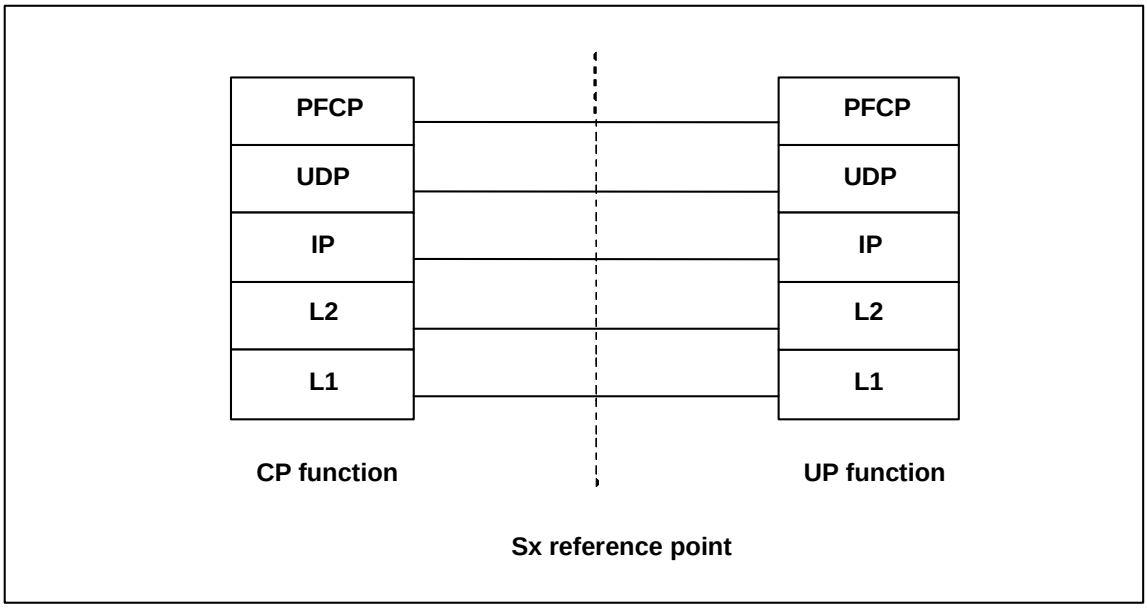


**Figure 4.1-1: Control Plane stack over Sxa, Sxb, Sxc and combined Sxa/Sxb**

The protocol stack for the user plane over the Sxa and Sxb reference points (see subclause 5.3) shall be as depicted in Figure 4.1-2. 3GPP TS 29.281 [3] further specifies the related GTP-U, UDP and IP requirements. Both IPv4 and IPv6 shall be supported.

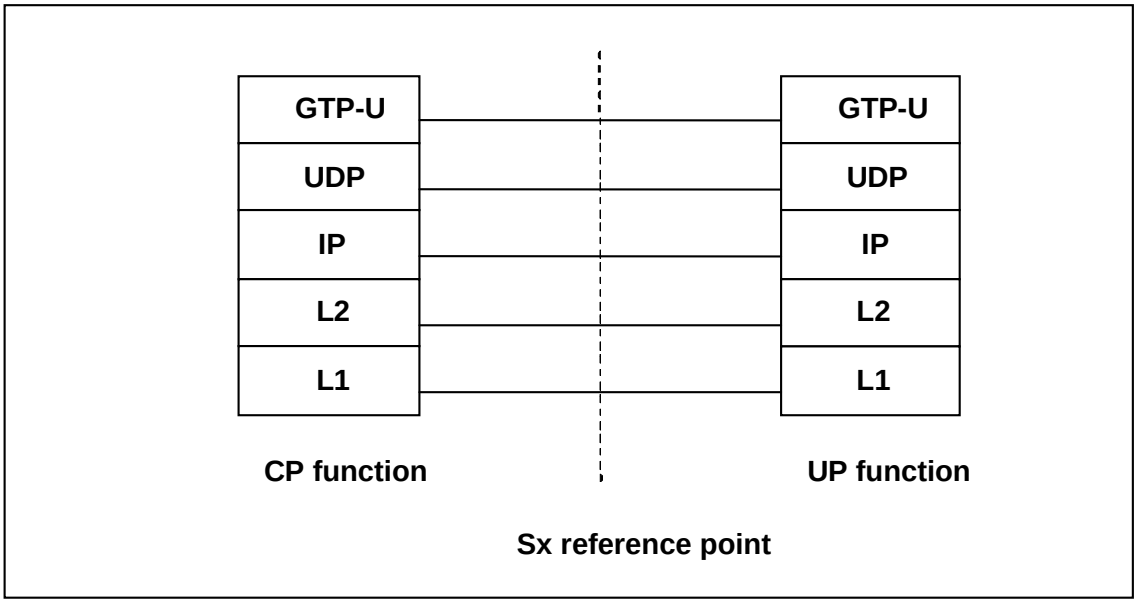


**Figure 4.1-2: User Plane stack over Sxa, Sxb and combined Sxa/Sxb**

# 4.2 UDP Header and Port Numbers

## 4.2.1 General

A User Datagram Protocol (UDP) compliant with IETF RFC 768 [4] shall be used.

### 4.2.2 Request Message

The UDP Destination Port number for a Request message shall be 8805. It is the registered port number for PFCP.

The UDP Source Port for a Request message is a locally allocated port number at the sending entity.

NOTE: The locally allocated source port number can be reused for multiple Request messages.

### 4.2.3 Response Message

The UDP Destination Port value of a Response message shall be the value of the UDP Source Port of the corresponding Request message.

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

## 4.3 IP Header and IP Addresses

### 4.3.1 General

In this subclause, "IP" refers either to IPv4 as defined by IETF RFC 791 [5] or IPv6 as defined by IETF RFC 2460 [6]. A PFCP entity shall support both IPv4 and IPv6.

### 4.3.2 Request Message

The IP Destination Address of a Request message shall be an IP address of the peer entity.

During the establishment of an Sx Session, the CP and the UP functions select and communicate to each other the IP Destination Address at which they expect to receive subsequent Request messages related to that Sx Session. The CP and the UP functions may change this IP address subsequently during an Sx Session Modification procedure.

The IP Source Address of a Request message shall be an IP address of the sending entity.

### 4.3.3 Response Message

The IP Destination Address of a Response message shall be copied from the IP Source Address of the corresponding Request message.

The IP Source Address of a Response message shall be copied from the IP destination address of the corresponding Request message.

## 4.4 Layer 2

Typically Ethernet should be used as a Layer 2 protocol, but operators may use any other technology.

## 4.5 Layer 1

Operators may use any appropriate Layer 1 technology.

# 5 General description

## 5.1 Introduction

The architecture reference model with Control and User Plane Separation of EPC nodes is described in subclause 4.2 of 3GPP TS 23.214 [2].

This clause specifies the high level principles of the PFCP protocol and describe how 3GPP functionalities are realised on the Sxa, Sxb and Sxc reference points, e.g. Packet Forwarding, Policy and Charging Control, Lawful Interception.

## 5.2 Packet Forwarding Model

### 5.2.1 General

The packet forwarding scenarios supported over the Sxa, Sxb and Sxc reference points are specified in 3GPP TS 23.214 [2].

The CP function controls the packet processing in the UP function by establishing, modifying or deleting Sx Session contexts and by provisioning (i.e. adding, modifying or deleting) PDRs, FARs, QERs, URRs and/or BAR per Sx session context, whereby an Sx session context may correspond to an individual PDN connection, a TDF session, or a standalone session not tied to any PDN connection or TDF session used e.g. for forwarding Radius, Diameter or DHCP signalling between the PGW-C and the PDN.

Each PDR shall contain a PDI, i.e. one or more match fields against which incoming packets are matched, and may be associated to the following rules providing the set of instructions to apply to packets matching the PDI:

- one FAR, which contains instructions related to the processing of the packets as follows:
  - an Apply Action parameter, which indicates whether the UP function shall forward, duplicate, drop or buffer the packet with or without notifying the CP function about the arrival of a DL packet;
  - forwarding, buffering and/or duplicating parameters, which the UP function shall use if the Apply Action parameter requests the packets to be forwarded, buffered or duplicated respectively. These parameters may remain configured in the FAR regardless of the Apply Action parameter value, to minimize the changes to the FAR during the transitions of the UE between the idle and connected modes. The buffering parameters, when present, shall be provisioned in a BAR created at the Sx session level and referenced by the FAR.

NOTE 1: Buffering refers here to the buffering of the packet in the UP function. The UP function is instructed to forward DL packets to the CP function when applying buffering in the CP function. See subclause 5.3.1.

- zero, one or more QERs, which contains instructions related to the QoS enforcement of the traffic;
- zero, one or more URRs, which contains instructions related to traffic measurement and reporting.

A FAR, a QER and a URR shall only be associated to one or multiple PDRs of the same Sx session context.

The QoS Enforcement Rule Correlation ID shall be assigned by the CP function to correlate QERs from multiple Sx session contexts. For instance, the enforcement of APN-AMBR in the PGW-U shall be achieved by setting the same QoS Enforcement Rule Correlation ID to the QERs from different Sx sessions associated with all the PDRs corresponding to the non-GBR bearers of all the UE's PDN connections to the same APN. The QERs that are associated to the same QoS Enforcement Rule Correlation ID in multiple Sx sessions shall be provisioned, with the same QER contents, in each of these Sx sessions.

The following principles shall apply for the provisioning of PDRs in the UP function:

- The CP function shall not provision more than one PDR with the same match fields in the PDI (i.e. with the same set of match fields and with the same value). The CP function may provision PDRs with the same value for a subset of the match fields of the PDI but not all;

- different PDRs of a same Sx session may overlap, e.g. the CP function may provision two PDRs which differ by having one match field set to a specific value in one PDR and the same match field not included in the other PDR (thus matching any possible value);

- different PDRs of different Sx sessions shall not overlap, i.e. there shall be at least one PDR in each Sx session which differs by at least one different (and not wildcarded) match field in their PDI, such that any incoming user plane packet may only match PDRs of a single Sx session;

NOTE 2: It is allowed for instance to provision in a PGW-U a same uplink PDR, matching any uplink traffic towards a particular application server's IP address, in two different Sx sessions of two different UEs, as long as each Sx session is also provisioned with another uplink PDR set with the respective UE IP address and/or uplink F-TEIDu, which allows the PGW-U to identify the Sx session to which the packet corresponds.

- As an exception to the previous principle, the CP function may provision a PDR with all match fields wildcarded (i.e. all match fields omitted in the PDI) in a separate Sx session, to control how the UP function shall process packets unmatched by any PDRs of any other Sx session. The CP function may provision the UP function to send these packets to the CP function or to drop them. The UP function shall grant the lowest precedence to this PDR.

On receipt of a user plane packet, the UP function shall perform a lookup of the provisioned PDRs and:

- identify first the Sx session to which the packet corresponds; and

- find the first PDR matching the incoming packet, among all the PDRs provisioned for this Sx session, starting with the PDRs with the highest precedence and continuing then with PDRs in decreasing order of precedence. Only the highest precedence PDR matching the packet shall be selected, i.e. the UP function shall stop the PDRs lookup once a matching PDR is found.

A packet matches a PDR if all the match fields of the PDI of the PDR are matching the corresponding packet header fields. If a match field is not included in the PDI, it shall be considered as matching all possible values in the header field of the packet. If the match field is present and does not include a mask, the match field shall be considered as matching the corresponding header field of the packet if it has the same value. If the match field is present and includes a mask (e.g. IP address with a prefix mask), the match field shall be considered as matching the corresponding header field of the packet if it has the same value for the bits which are set in the mask.
The match fields of the PDI shall correspond to outer and/or inner packet header fields, e.g. uplink bearer binding verification in the PGW-U may be achieved by configuring a PDR with the PDI containing the local GTP-U F-TEID (for outer IP packet matching) and the SDF filters of the data flows mapped to the bearer (for inner IP packet matching).

The UP function should drop packets unmatched by any PDRs.

The packet processing flow in the UP function is illustrated in Figure 5.2.1-1.

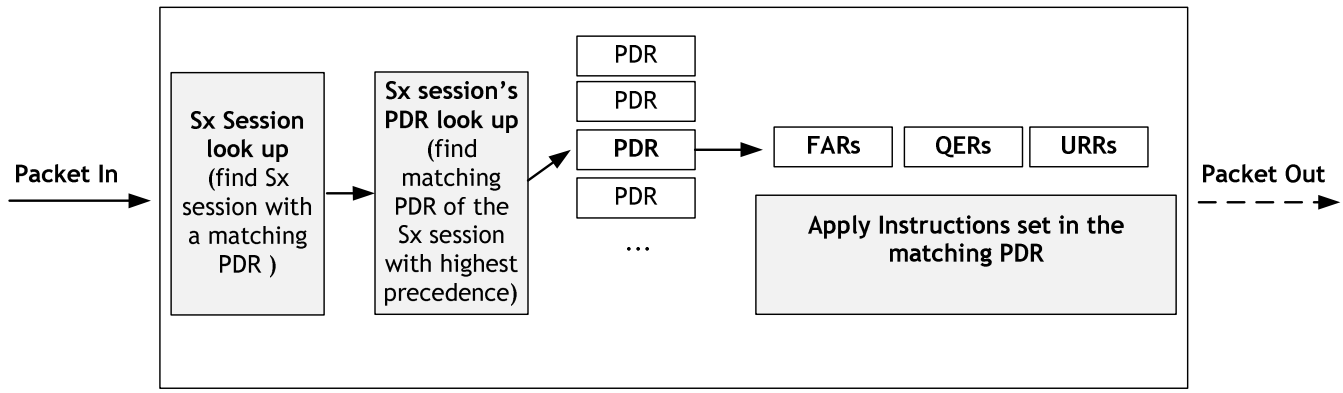


**Figure 5.2.1-1: Packet processing flow in the UP function**

At the deletion of an Sx session, the UP function shall delete the Sx session context and all the associated non-preconfigured rules.

NOTE 3: Deleting a QER in one Sx session does not result in deleting another QER in another Sx session even when these two QERs have the same QER ID and/or are associated with the same QER Correlation ID.

A UP Function controlled by multiple CP functions shall handle Rule IDs from the different CP functions independently from each other.

Rule ID used for PDR, FAR, BAR, QER or URR is uniquely identifying a rule of the corresponding rule type within a session.

## 5.2.2 Usage Reporting Rule Handling

### 5.2.2.1 General

The CP function shall provision URR(s) for an Sx session in an Sx Session Establishment Request or an Sx Session Modification Request to request the UP function to:

- measure the network resources usage in terms of traffic data volume, duration (i.e. time) and/or events, according to the provisioned Measurement Method; and
- send a usage report to the CP function, when the measurement reaches a certain threshold, periodically or when detecting a certain event, according to the provisioned Reporting Triggers.

NOTE: The UP function sends a usage report without performing network resources usage measurements when being requested to detect and report the the start of an SDF or application traffic.

### 5.2.2.2 Provisioning of Usage Reporting Rule in the UP function

When provisioning a URR, the CP function shall provide the reporting trigger(s) in the Reporting Triggers IE of the URR which shall cause the UP function to generate and send a Usage Report for this URR to the CP function. When adding or removing reporting trigger(s) to or from the URR, the CP function shall provide the new complete list of applicable reporting triggers in the Reporting Triggers IE in the Sx Session Modification Request message.

For the volume-based measurement method, the CP function may provision:

- the Volume Threshold IE, to request the UP function to generate a usage report when the measured traffic reaches the threshold;
- the Volume Quota IE, to request the UP function to stop forwarding packets and, if no Volume Threshold is provisioned, to also generate a usage report, when the measured traffic reaches the quota;
- the Dropped DL Traffic Threshold IE, to request the UP function to generate a usage report when the downlink traffic that is being dropped reaches the threshold; and/or

NOTE 1: The Dropped DL Traffic Threshold can be armed in a SGW-U for triggering the PGW Pause of Charging feature (see 3GPP TS 23.401 [14]).

- a Measurement Information with the 'Measurement Before QoS Enforcement' flag set to 1, to request the UP function to measure the traffic usage before any QoS enforcement.

For the time-based measurement method, the CP function may provision:

- a Time Threshold IE, to request the UP function to generate a usage report when the measured traffic reaches the threshold;
- a Time Quota, to request the UP function to stop forwarding packets and, if no Time Threshold is provisioned, to also generate a usage report, when the measured traffic reaches the quota; and/or
- an Inactivity Detection Time, to request the UP function to suspend the time measurement when no packets are received during the provisioned Inactivity Detection Time. The time measurement shall then be resumed by the UP function when subsequent traffic is received. If an Inactivity Detection Time value of zero is provided, or if no Inactivity Detection Time has been provided by the CP function, the time measurement shall be performed continuously from the point when the first packet is received until the time-based usage measurement is stopped. See Figure 5.2.2.2-1:

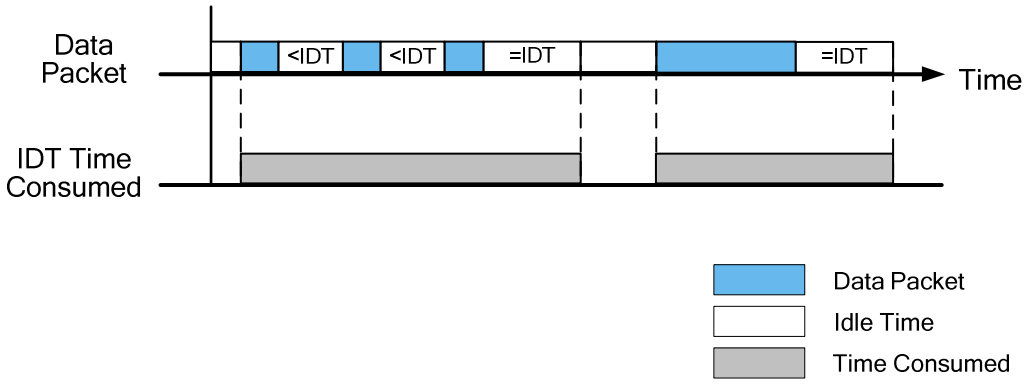


**Figure 5.2.2.2-1: IDT based charging**

NOTE 2: The Inactivity Detection Time can be set to the Quota Consumption Timer if received.

- a Time Quota Mechanism, including a Base Time Interval Type, which is either Continuous Time Period (CTP) or Discrete Time Period (DTP), and a Base Time Interval (BTI), to the UP function. See subclause 6.5.7 in 3GPP TS 32.299[18].

  - For CTP (Continuous Time Period), the time measurement starts from the time that traffic has occurred up to the first Base Time Interval (BTI) which contains no traffic. The time measurement shall include the last Base Time Interval, i.e. the one which contained no traffic. The time measurement resumes by the UP function when subsequent traffic is received. See Figure 5.2.2.2-2:

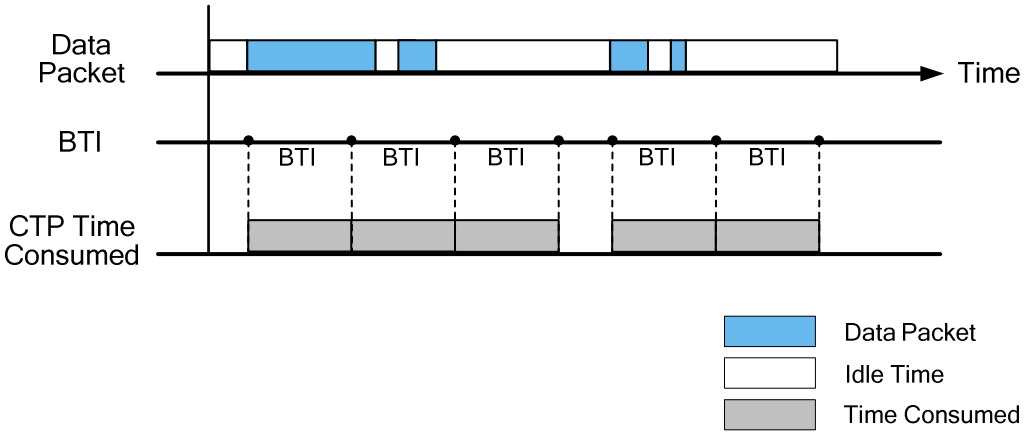


**Figure 5.2.2.2-2: CTP based charging**

  - For DTP (Descrete Time Period), the time measurement starts from the time that traffic has occurred up to the Base Time Interval end. The time measurement shall be resumed by the UP function when subsequent traffic is received. See Figure 5.2.2.2-3:

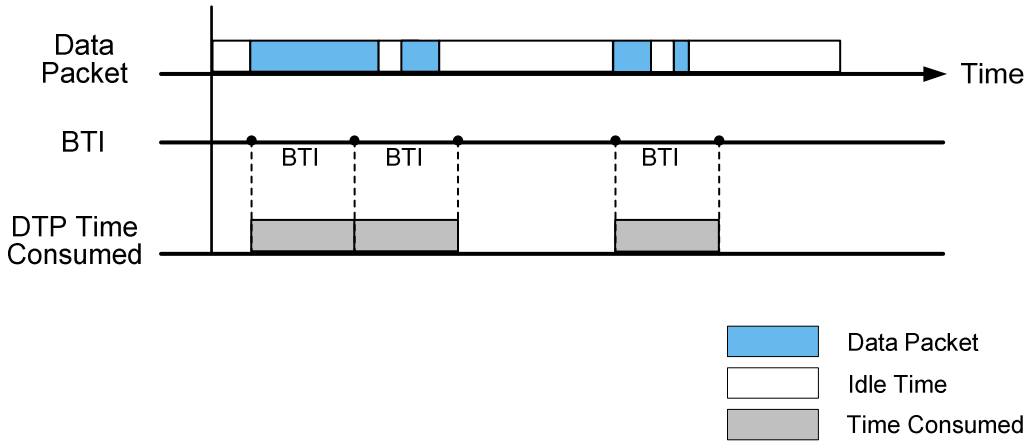


**Figure 5.2.2.2-3: DTP based charging**

When the time-based measurement method applies, and when the Envelope Reporting is required, the CP function shall request the UP function to report the usage by setting the reporting trigger to Envelope Closure in addition to other Reporting Trigger(s), in the Reporting Triggers IE. The CP function may indicate the UP function to report for just time, time and volume, time and events, or time and volume and number of events by setting Measurement Method accordingly.

The CP function may provision a Volume Threshold, a Volume Quota, or both (and/or respectively a Time Threshold, a Time Quota, or both).

When both a Volume (or Time) Threshold and a Volume (or Time) Quota are provisioned, the UP function shall send a usage report only when reaching the Volume (or Time) Threshold; when subsequently reaching the Volume (or Time) Quota, the UP function shall stop forwarding packets without sending a new usage report to the CP function.

NOTE 3: For online charging, the Volume Threshold (or Time Threshold) can be set in a PGW-U or TDF-U to the value of the granted volume (or time) quota minus the volume (or time) quota threshold, such as to get a usage report from the UP function when the volume (or time) based credit falls below the remaining quota thresholds provided by the OCS.

NOTE 4: The Volume Quota or Time Quota can be armed in a PGW-U or TDF-U for online charging to enable the traffic to be forwarded up to an intermediate or final quotas granted by the OCS. The CP function can provision both a Volume (or Time) Threshold and a Volume (or Time) Threshold to request the UP function to send a usage report when the consumed resources reach the volume (or time) usage threshold provided by the OCS, and to stop forwarding packets (without sending a second usage report) when the granted volume (or time) quota is exhausted.

For all the measurement methods (i.e. volume, time or event), the CP function may also provision:

- a Quota Holding Time, to request the UP function to send a usage report and to also stop forwarding packets when no packets have been received for the duration indicated in this parameter;

NOTE 5: A Quota Holding Time can be armed in a PGW-U or TDF-U for online charging to request the UP function to send a Usage Report when the Quota Holding Time provided by the OCS (see 3GPP TS 32.299 [18]) expires. The UP function can be instructed in the same Usage Reporting Rule with the Report Triggers – START to generate a new Usage Report upon receiving any subsequent packets associated with this URR.

- a Monitoring Time, to request the UP function to measure the network resources usage before and after the monitoring time in separate counts and to re-apply the volume and time thresholds at the monitoring time. The CP function may additionally provision a Subsequent Volume (or Time) Threshold IE, for a volume (or time) based measurement. When being provisioned with a Monitoring Time, the UP function shall:

  - reset its usage thresholds at the monitoring time to the value provided in the Subsequent Volume (or Time) Threshold IE, if provisioned in the URR, or to the remaining value of the Volume (or Time) threshold used before the monitoring time (i.e. excluding the already accumulated volume or time usage);

- shall indicate the usage up to the Monitoring time and usage after the Monitoring time in the first usage report after the Monitoring Time is reached;

- a Measurement Period, indicating the period to generate periodic usage reports to the CP function.

The CP function may request at any time the UP function to activate or deactivate a network resources usage measurement and the sending of corresponding Usage Reports, using the Inactive Measurement flag of the Measurement Information IE of the URR.

NOTE 6: This can be used in a PGW-U for the PGW Pause of Charging procedure (see 3GPP TS 23.401 [14]).

#### 5.2.2.3 Reporting of Usage Report to the CP function

When detecting that a provisioned reporting trigger occurs, the UP function shall generate a Usage Report for the related URR and send it to the CP function by initiating the Sx Session Report procedure.

When providing usage report information for a URR in a message, the UP function shall include the UR-SEQN (Usage Report Sequence Number) identifying the order in which a Usage Report is generated for the given URR. The UR-SEQN (Usage Report Sequence Number) shall be incremented for every Usage Report generated by the UP function for the URR. The UP function shall also indicate the trigger that causes the usage report to be generated in the Usage Report Trigger IE.

Upon generating a usage report for a URR towards the CP function, the UP function shall:

- reset its ongoing measurement counts for the related URR (i.e. the UP function shall report in a usage report the network resources usage measurement since the last usage report for that URR);

- re-apply the threshold provisioned for the related URR, if the usage report was triggered due to a threshold being reached; and

- continue to apply all the provisioned URR(s) and perform the related network resources usage measurement(s), until getting any further instruction from the CP function.

When receiving a new threshold or quota from the CP function for a measurement that is already ongoing in the UP function, the UP function shall consider its ongoing measurements counts for the related URR against the new threshold or quota to determine when to send its next usage report to the CP function.

NOTE 1: The UP function determines when to send its next usage report to the CP function by deducting from the newly provisioned threshold or quota the traffic it has forwarded since its last usage report. As an example, if the UP function has forwarded 10 Mbytes of traffic since it last usage report to the CP function and the CP function provisions a new volume threshold or quota of 100 Mbytes, the UP function sends its next usage report upon forwarding an additional 90 Mbytes traffic.

When reporting the network resources usage before and after a Monitoring Time, the UP function shall send two Usage Reports in the PFCP message (e.g. Sx Session Report Request) for the same URR ID. Each Usage Report shall then include the Usage Information IE indicating whether the reported network resource usage was consumed before or after the Monitoring Time. Omission of this IE in a Usage Report indicates that no monitoring time has occurred. The UP function shall send Usage Reports soon after the occurrence of the Monitoring Time.

NOTE 2: The UP function needs to take care to smooth the signalling load towards the CP function if Usage Reports need to be generated for a large number of Sx sessions after the occurrence of the Monitoring Time.

For the volume-based measurement method, the UP function shall report the traffic usage after any QoS enforcement. Additionally, if the CP function requested to measure the traffic usage before QoS enforcement, the UP function shall also report corresponding measurements, when measurements needs to be reported for the traffic usage after QoS enforcement, by sending two Usage Reports in the PFCP message (e.g. Sx Session Report Request) for the same URR ID. Each Usage Report shall then include the Usage Information IE indicating whether the reported network resource usage corresponds to the traffic before or after QoS enforcement. Thresholds provisioned in a URR shall apply to the traffic usage after any QoS enforcement.

A usage report triggered only due to the Dropped DL Traffic Threshold shall not contain any measurement information.

When being instructed to remove a URR, or deactivate a network resources usage measurement via the Inactive Measurement flag of the Measurement Information IE of the URR, the UP function shall include a Usage Report in the Sx Session Modification Response and reset its ongoing measurements for the URR that is removed or deactivated.

The CP function may request the UP function, in an Sx Session Modification Request, to report its ongoing network resources measurement for one or multiple URRs of the Sx session. In this case, the UP function shall generate usage report(s) for the URR(s) being queried, include them in the Sx Session Modification Response and proceed as specified above upon generating a usage report for a URR towards the CP function.

NOTE 3: It is up to the CP function to request the UP function to generate an immediate report (or not) as specified above when the CP function modifies a URR or any other rules of the Sx session. As an exception, the UP function always generates an immediate report when being instructed to remove a URR or deactivate a network resource measurement via the Inactive Measurement flag of the Measurement Information IE of the URR.

When the reporting trigger "Envelope Closure" is set in the corresponding Usage Reporting Rule, the UP function shall generate a usage report with the measurement of the time and/or volume as instructed in the Measurement Method:

- when the Inactivity Detection Time (if included) is expired; or
- when detecting no usage for the first Base Time Interval if the Base Time Interval Type in the Time Quota Mechanism is set to CTP; or
- at the end of each of base time interval if the Base Time Interval Type in the Time Quota Mechanism is set to DTP.

NOTE 4: Events (e.g. application detection information) are reported individually and independently from the usage report sent for envelope closure.

At the Sx session termination, the UP function shall indicate to the CP function, in the Sx Session Deletion Response, the resources that have been consumed for each URR that was provisioned in the Sx session since the last usage report (respective to each URR).

Upon receiving the Usage Report from the UP function, the CP function may initiate Sx Session Modification procedure as result of the communication with the PCRF or OCS, as described in subclause 5.3 of 3GPP TS 23.214 [2], e.g. by:

- modifying the URR (e.g. changing the Volume/Time threshold, Volume/Time quota, disabling the usage monitoring);
- creating a new FAR (e.g. for redirect) and/or modifying the existing FAR; or
- modifying the QER (s) in the Sx session.

#### 5.2.2.4 Reporting of Linked Usage Reports to the CP function

The CP function may instruct the UP function to generate a Usage Report for a URR "X" when a Usage Report is generated for another URR "Y", by:

- provisioning the URR "X" with the Reporting Triggers IE set to Linked Usage Reporting; and
- including in the URR "X" the Linked URR ID IE set to the URR ID of the URR "Y".

NOTE: This can be used by the CP function e.g. to request the UP function to report a Usage Report for an SDF (i.e. URR "X") when the UP function reports a Usage Report for a bearer (i.e. URR "Y").

When a usage report is to be generated for the URR "Y", the UP function shall also send a Usage Report for the URR "X" with the accumulated usage information, and the Usage Report Trigger IE set to Linked Usage Reporting.

The URR "Y" may be linked to more URRs than just URR "X".

## 5.2.3 Forwarding Action Rule Handling

### 5.2.3.1 General

The CP function shall provision one and only one FAR for each PDR provisioned in an Sx session. The FAR provides instructions to the UP function on how to process the packets matching the PDR.

By setting the appropriate flag(s) in the Apply Action IE in the FAR (see subclause 8.2.26), the CP function may request the UP function to:

- drop the packets, by setting the DROP flag;
- forward the packets, by setting the FORW flag and by provisioning the Forwarding Parameters providing instructions on how to forward the packets;
- buffer downlink packets by setting the BUFF flag and by optionally provisioning buffering parameters providing instructions on how to buffer the packets;
- notify the CP function about the arrival of a first DL packet being buffered, by setting the NOCP flag;
- duplicate the packets, by setting the DUPL flag and by provisioning the Duplicating Parameters providing instructions on how to forward the duplicated packets.

The CP function may request the UP function to duplicate packets that are to be dropped, forwarded or buffered.

The CP function may provision one or more FAR(s) per Sx session. Different FARs of a same Sx session may be provisioned with a different Apply Action flags, e.g. to enable the forwarding of downlink data packets for some PDRs while requesting to buffer downlink data packets for other PDRs.

NOTE 1: This is necessary to establish or release a partial set of radio access bearers in UTRAN.

When instructed to buffer and notify the CP function about the arrival of a DL packet, the UP function shall notify the CP function, when it receives a first downlink packet for a given FAR, by sending an Sx Session Report Request including a Downlink Data Report IE identifying the PDR(s) for which downlink packets have been received.

NOTE 2: Receipt of downlink packets on PDRs associated to different FARs can result in sending multiple Sx Session Report Request messages for the same Sx session.

If the UP function indicated support of Header Enrichment of UL traffic (see subclause 8.2.25), the CP function may provide the UP function with header enrichment information for uplink traffic, by including one or more Header Enrichment IE(s) in the FAR. In this case, the UP function should use this information to enrich the header of the uplink traffic (e.g. HTTP header enrichment).

NOTE 3: It is not defined how to support SGi PtP tunnelling mechanisms other than based on UDP/IP encapsulation (such as PMIPv6/GRE, L2TP, GTP-C/U, see subclause 4.3.17.8.3.3.3 of 3GPP TS 23.401 [14]) for Non-IP PDN connections.

## 5.2.4 Buffering Action Rule Handling

### 5.2.4.1 General

A BAR provides instructions to control the buffering behaviour of the UP function for all the FARs of the Sx session set with an Apply Action parameter requesting the packets to be buffered and associated to this BAR.

The CP function may create a BAR for an Sx session and associate it to the FAR(s) of the Sx session in an Sx Session Establishment Request or an Sx Session Modification Request to request the UP function to apply a specific buffering behaviour for packets requested to be buffered and associated to this BAR.

The CP function may modify the following buffering instructions provided in a BAR as follows:

- the Downlink Data Notification Delay in an Sx Session Modification Request; or
- the Downlink Data Notification Delay, DL Buffering Duration and/or DL Buffering Suggested Packet Count in an Sx Session Report Response message.

NOTE: The CP function needs to provision a (possibly empty) BAR and associate it to the FARs of the Sx session when establishing or modifying the Sx session to be able to modify the BAR in an Sx Session Report Response.

In this release of the specification, at most one BAR may be created per Sx session.

#### 5.2.4.2 Provisioning of Buffering Action Rule in the UP function

The CP function may provision the following buffering parameters in a BAR:

- the Downlink Data Notification Delay IE, to request the UP function to delay the sending of an Sx Session Report Request, between receiving a downlink data packet and notifying the CP function about it, if the UP function indicated support of the Downlink Data Notification Delay parameter (see subclause 8.2.28);

- the DL Buffering Duration IE, to request the UP function to buffer the downlink data packet for an extended duration without sending any further notification to the CP function about the arrival of DL data packets, if the UP function indicated support of the DL Buffering Duration parameter (see subclause 8.2.25);

- the DL Buffering Suggested Packet Count, to request the UP function to buffer the suggested number of downlink data packets, when extended buffering of downlink data packet is required in the UP function.

The UP function shall stop applying the DL Buffering Duration and DL Buffering Suggested Packet Count parameters and shall delete these parameters from the BAR (without explicit request from the CP function) when extended buffering of downlink data packets ends in the UP function.

NOTE: The CP function will provide the DL Buffering Duration and DL Buffering Suggested Packet Count parameters again when re-invoking extended buffering of downlink data packets.

### 5.2.5 QoS Enforcement Rule Handling

#### 5.2.5.1 General

The CP function shall provision QER(s) for an Sx session in an Sx Session Establishment Request or an Sx Session Modification Request to request the UP function to perform QoS enforcement of the user plane traffic.

#### 5.2.5.2 Provisioning of QoS Enforcement Rule in the UP function

The CP function may request the UP function to perform the following QoS enforcement actions in a QER:

- Gating Control, as specified in subclause 5.4.3;

- QoS Control, i.e. MBR, GBR or Packet Rate enforcement, as specified in subclause 5.4.4;

- DL flow level marking for application detection, as specified in subclause 5.4.5;

- SCI (Service Class Indicator) marking for service identification for improved radio utilisation for GERAN, as specified in subclause 5.4.12.

### 5.2.6 Combined SGW/PGW Architecture

The usage of a combined SGW/PGW remains possible in a deployment with separated control and user planes, see subclause 4.2.2 of 3GPP TS 23.214 [2]. This is enabled by supporting a combined Sxa/Sxb interface with a common packet forwarding model, message and parameter structure for non-combined and combined cases.

The following additional requirements shall apply to a combined Sxa/Sxb interface between a combined SGW/PGW-C and a combined SGW/PGW-U:

- all the functionalities specified for Sxa and Sxb shall be supported, possibly concurrently, over a combined Sxa/Sxb association;

- a single Sx session may be setup to support both the functionalities of an SGW-U and PGW-U;

- the CP function may provision PDRs, QERs, URRs, FARs (possibly with a buffering instruction) and BAR, possibly concurrently, for the same Sx session;
- the CP function may provision concurrently parameters in a message or for the Sx session that are applicable to Sxa and Sxb.

# 5.3 Data Forwarding between the CP and UP Functions

## 5.3.1 General

Forwarding of user plane data between the CP and UP functions may take place as part of the following scenarios (see 3GPP TS 23.214 [2]).

**Table 5.3.1-1: Data forwarding scenarios between the CP and UP functions**

| | Scenario description | Data forwarding direction | Applicable to |
|---|---|---|---|
| 1 | Forwarding of user-plane packets between the UE and the CP function. | UP to CP function<br>CP to UP function | PGW |
| 2 | Forwarding of packets between the CP function and the external PDN / Sgi. | UP to CP function<br>CP to UP function | PGW |
| 3 | Forwarding of packets subject to buffering in the CP function. | UP to CP function<br>CP to UP function | SGW |
| 4 | Forwarding of End Marker Packets constructed by the CP function to a downstream node. | CP to UP function | SGW, PGW |

User plane packets shall be forwarded between the CP and UP functions by encapsulating the user plane packets using GTP-U encapsulation (see 3GPP TS 29.281 [3]).

For forwarding data from the UP function to the CP function, the CP function shall provision PDR(s) per Sx session context, with the PDI identifying the user plane traffic to forward to the CP function and with a FAR set with the Destination Interface "CP function side" and set to perform GTP-U encapsulation and to forward the packets to a GTP-u F-TEID uniquely assigned in the CP function per Sx session and PDR. The CP function shall then identify the PDN connection and the bearer to which the forwarded data belongs by the F-TEID in the header of the encapsulating GTP-U packet.

For forwarding data from the CP function to the UP function, the CP function shall provision one or more PDR(s) per Sx session context, with the PDI set with the Source Interface "CP function side" and identifying the GTP-u F-TEID uniquely assigned in the UP function per PDR, and with a FAR set to perform GTP-U decapsulation and to forward the packets to the intended destination. URRs and QERs may also be configured.

Sx session contexts may correspond to individual PDN connections, TDF sessions, or standalone sessions not tied to any PDN connection or TDF session used e.g. for forwarding RADIUS, Diameter or DHCP signalling between the PGW-C and the PDN or for forwarding End Marker packets from the PGW-C or SGW-C to a downstream SGW-U or eNodeB.

The CP function may establish one Sx-u tunnel per:

- bearer of PDN connection e.g. for the data forwarding scenarios 1 and 3;
- UP function or PDN e.g. for the data forwarding scenario 1, 2 and 4.

Requirements for forwarding packets subject to buffering in the CP function between the UP and CP functions (scenario 3) are further specified in subclause 5.3.3.

Requirements for sending End Marker packets (scenario 4) are further specified in subclause 5.3.2.

## 5.3.2 Sending of End Marker Packets

The construction of End Marker packets may either be done in the CP function or UP function, based on network configuration, as specified in subclause 5.8 of 3GPP TS 23.214 [2]. The support of End Marker packets by the UP function is optional.

If the UP function indicated support of End Marker packets constructed in the UP function, the CP function shall request the UP function to construct and send End Marker packets by sending a Session Modification Request including FAR(s) with the new downstream F-TEID and with the SNDEM (Send End Marker Packets) flag set.

For End Marker packets constructed in the CP function, the CP function shall:

- establish (once) one standalone Sx session not tied to any PDN connection, per the UP function, for forwarding End Marker packets, and provision the UP function to perform one GTP-U decapsulation and to forward the resulting packets without any further change towards the destination IP address of these packets;

- construct the GTP-U End Marker packets, with the destination IP address and TEID set according to the old F-TEID value, and with a source IP address set according to the UP function's F-TEID value (e.g. S1 or Iu SGW F-TEID);

- encapsulate the constructed GTP-U End Marker packets in GTP-U packets according to the principles specified in subclause 5.3.1 for data forwarding between the CP function and the UP function, and send them towards the F-TEID assigned in the UP function for the above Sx session, after receipt of the Sx Session Modification Response indicating that the UP function has switched to a new F-TEID.

Upon receipt of an Sx Session Modification Request modifying the F-TEID in the Outer Header Creation of a FAR, the UP function shall send the Response message only after having switched to the new F-TEID.

## 5.3.3 Forwarding of Packets Subject to Buffering in the CP Function

### 5.3.3.1 General

The following requirements shall apply to the data forwarding scenario 3 of Table 5.3.1-1 in addition to the requirements specified in subclause 5.3.1.

The CP function shall establish one Sx-u tunnel per bearer of a PDN connection when applying the data forwarding scenario 3.

### 5.3.3.2 Forwarding of Packets from the UP Function to the CP Function

Regardless of whether the downlink traffic received by the UP function consists of T-PDUs (i.e. user data packet, see 3GPP TS 29.281 [3]) for a combined SGW/PGW-U, or G-PDUs (i.e. T-PDU plus a GTP-U header) for a SGW-U, the downlink traffic shall be forwarded from the UP function to the CP function as G-PDUs with the GTP-U header set to the IP address and TEID uniquely assigned in the CP function for the Sx-u tunnel corresponding to the bearer of the PDN connection.

NOTE 1: An SGW-U receiving G-PDUs from an S5/S8 bearer forwards the same G-PDUs towards the SGW-C but with the IP address and TEID in the GTP-U header changed to the SGW-C IP address and TEID of the corresponding Sx-u tunnel.

To forward the user plane data to be buffered in the CP function from the UP function, the CP function shall provision:

- a PDR per bearer of the PDN connection, matching the received downlink user plane packets and for a (non-combined) SGW-U, with the field Outer Header Removal Description in the Outer Header Removal IE set to "0" or "1" for IPv4 or IPv6 respectively;

- a FAR instructing the UP function to forward the received downlink data to the CP function, with the field Outer Header Creation Description in the Outer Header Creation set to "0" or "1".

NOTE 2: The PDR can be provisioned in the UP function before applying data forwarding to the CP function.

G-PDUs sent from the UP function to the CP function over the Sx-u tunnel shall include any GTP-U extension header(s):

- possibly received by the UP function over the S5/S8 bearers and stored during the Outer Header Removal;

- possibly created by the UP function as part of a QER rule.

#### 5.3.3.3 Forwarding of Packets from the CP Function to the UP Function

Likewise, when subsequently sending the downlink traffic buffered in the CP function back to the UP function, the downlink traffic shall be forwarded over Sx-u as G-PDUs with the GTP-U header set to the IP address and TEID uniquely assigned in the UP function for the Sx-u tunnel set up for the corresponding bearer of the PDN connection.

G-PDUs sent over Sx-u shall include GTP-U extension header(s) possibly received earlier from the UP function.

To forward the user plane data from the CP function to the UP function, the CP function shall provision:

a PDR per bearer of the PDN connection, with an IP address and TEID uniquely assigned in the UP function for the Sx-u tunnel, and with the field Outer Header Removal Description in the Outer Header Removal IE set to "0" or "1";

- a FAR enabling the UP function to forward the received downlink data from the CP function towards the RAN, with the field Outer Header Creation Description in the Outer Header Creation set to "0" or "1".

G-PDUs sent from the UP function towards the RAN shall include GTP-U extension header(s) possibly received from the CP function.

### 5.3.4 Data Forwarding between the CP and UP Functions with one Sx-u Tunnel per UP Function or PDN

#### 5.3.4.1 General

The following requirements shall apply to the data forwarding scenario 1 and 2 of Table 5.3.1-1, when establishing one Sx-u tunnel per UP function or PDN, in addition to the requirements specified in subclause 5.3.1.

#### 5.3.4.2 Forwarding of Packets from the UP Function to the CP Function

Regardless of whether the traffic received by the UP function consists of T-PDUs (i.e. user data packet, see 3GPP TS 29.281 [3]) from SGi or G-PDUs (i.e. T-PDU plus a GTP-U header) from the UE, the traffic shall be forwarded from the UP function to the CP function as G-PDUs with the GTP-U header set to the IP address and TEID uniquely assigned in the CP function for the Sx-u tunnel corresponding to the UP function or PDN.

To forward the user plane data to from the UP function, the CP function shall provision:

- a PDR per UP function or PDN, matching the received user plane packets and for uplink traffic, optionally with the field Outer Header Removal Description in the Outer Header Removal IE set to "0" or "1" for IPv4 or IPv6 respectively;

- a FAR instructing the UP function to forward the received data to the CP function, with the field Outer Header Creation Description in the Outer Header Creation set to "0" or "1".

NOTE 2: The PDR can be provisioned in the UP function before applying data forwarding to the CP function e.g. immediately after the Sx Association Setup procedure.

#### 5.3.4.3 Forwarding of Packets from the CP Function to the UP Function

When sending user plane data from the CP function, the traffic shall be forwarded over Sx-u as:

- T-PDUs encapsulated in GTP-U with the GTP-U header set to the IP address and TEID uniquely assigned in the UP function for the Sx-u tunnel set up for the UP function or PDN for traffic to be sent towards SGi, or

- G-PDUs encapsulated in GTP-U with the outer GTP-U header set to the IP address and TEID uniquely assigned in the UP function for the Sx-u tunnel set up for the UP function and with the inner GTP-U header set to the F-TEID assigned by the downstreams GTP-U peer (e.g. SGW) to the bearer over which the data shall be sent.

To forward the user plane data from the CP function to the UP function, the CP function shall provision:

a PDR per UP function, with an IP address and TEID uniquely assigned in the UP function for the Sx-u tunnel, and with the field Outer Header Removal Description in the Outer Header Removal IE set to "0" or "1";

- a FAR enabling the UP function to forward the received data from the CP function.

# 5.4 Policy and Charging Control

## 5.4.1 General

This subclause describe how Policy and Charging Control requirements are supported over the Sxa, Sxb and Sxc reference points.

## 5.4.2 Service Detection and Bearer Binding

Service detection refers to the process that identifies the packets belonging to a service data flow or application. See subclauses 6.2.2.2 and 6.8.1 of 3GPP TS 23.203 [7].

Bearer binding is the procedure that associates a service data flow to an IP-CAN bearer deemed to transport the service data flow. UL bearer binding verification refers to the process of discarding uplink packets due to no matching service data flow template for the uplink direction. See subclauses 6.1.1.4 and 6.2.2.2 of 3GPP TS 23.203 [7].

Service detection is controlled over the Sxa, Sxb and Sxc reference points by configuring Packet Detection Information in PDRs to match the intended service data flows or application.

The mapping of DL traffic to bearers is achieved by configuring and associating FARs to the downlink PDRs, with FARs set to forward the packets to the appropriate downstream bearers (S5/S8 or S1/S12/S4/Iu).

Uplink bearer binding verification is achieved by configuring Packet Detection Information in uplink PDRs containing the local F-TEID of the uplink bearer, the UE IP address (source IP address to match for the incoming packet), and the SDF filter or the Application ID. As a result, uplink packets received on the uplink bearer but that do not match the SDF filter or Application detection filter associated to the uplink PDRs are discarded.

NOTE 1: For PCC Rules that contain an application identifier (i.e. that refer to an application detection filter), uplink traffic can be received on other IP-CAN bearers than the one determined by the binding mechanism. The detection of the uplink part of the service data flow can be activated in parallel on other bearers with non-GBR QCI (e.g. the default bearer) in addition to the bearer where the PCC rule is bound to. See subclauses 6.1.1.1 and 6.2.2.2 of 3GPP TS 23.203 [7]. Therefore the uplink PDRs for these bearers can be provisioned with the PDI containing this service data flow and the local F-TEID of the uplink bearer.

NOTE 2: To avoid the PGW-U discarding packets due to no matching service data flow template, the operator can apply open PCC rules (with wildcarded SDF filters) to allow for the passage of packets that do not match any other candidate SDF template. Therefore an uplink PDR can be provisioned with the PDI containing only the local F-TEID of the uplink bearer.

NOTE 3: Uplink bearer binding does not apply to Non-IP PDN connections.

## 5.4.3 Gating Control

Gating control refers to the process within the PGW-U and TDF-U of enabling or disabling the forwarding of IP packets, belonging to a service data flow or detected application's traffic, to pass through to the desired endpoint (see subclause 4.3.2 of 3GPP TS 23.203 [7]).

The PGW-C and TDF-C controls the gating in the PGW-U and TDF-U by creating PDR(s) for the service data flow(s) or application's traffic to be detected, and by associating a QER, including the Gate Status IE, to the PDRs.

The Gate Status IE indicates whether the service data flow or detected application traffic is allowed to be forwarded (the gate is open) or shall be discarded (the gate is closed) in the uplink and/or in downlink directions.

The PGW-U and TDF-U shall identify UL and DL flows by the Source Interface IE in the PDI of the PDRs or the Destination Interface IE in the FARs. The PGW-U and TDF-U shall apply UL and DL gating accordingly.

### 5.4.4 QoS Control

QoS control refers to the authorization and enforcement of the maximum QoS that is authorized:

- at the session level (APN-AMBR, TDF session UL and DL bitrates, or UL and DL Packet Rate of a PDN connection);
- at the bearer level (GBR, MBR for GBR bearers);
- at the service data flow (SDF) or application level.

See subclause 4.3.3 of 3GPP TS 23.203 [7] subclause 4.5.5 of 3GPP TS 29.212 [8] and subclause 4.7.7 of 3GPP TS 23.401 [14].

The CP function shall control the QoS enforcement in the UP function by:

- creating the necessary PDR(s) to represent the service data flow, application, bearer or session, if not already existing;
- creating QERs for the QoS enforcement at session level, SDF/application level;
- creating QERs for the QoS enforcement of the aggregate of SDFs with the same GBR QCI;
- associating the session level QER to all the PDRs defined for the session;
- associating the SDF or application QER to the PDRs associated to the SDF or application;
- associating the QER of the aggregate of SDFs to the PDRs associated to SDFs or applications that share the QER.

The same QER may be associated to UL and DL PDRs. The UP function shall identify the UL and DL flows by the Source Interface IE in the PDRs or the Destination Interface IE in the FARs. The UP function shall enforce the QoS for the UL or DL flows accordingly.

The PGW-C shall map the precedence of a PCC rule to the precedence of the PDRs associated to the corresponding service data flows.

### 5.4.5 DL Flow Level Marking for Application Detection

DL flow level marking is performed using DL DSCP marking. DL DSCP marking for application indication refers to the process in the TDF of marking detected downlink application traffic with a DSCP value received within an installed ADC rule matching this traffic. See Annex U of 3GPP TS 23.203 [7] and subclauses 4.5.2.7 and 4b.5.14 of 3GPP TS 29.212 [8].

DL DSCP marking for application indication is controlled by the TDF-C by associating a QER, including the ToS or Traffic Class within the DL Flow Level Marking IE, to the PDR matching the DL traffic to be marked. The TDF-U performs the DL DSCP marking for the detected DL traffic and sends the marked packet to the PGW-U.

If a tunnelling protocol is used between the TDF-U and the PGW-U, the DSCP value for service data flow detection shall be carried in the inner IP header.

The TDF-C may stop the DL DSCP marking for the application during the Sx session by removing the related QER or removing the DL Flow Level Marking IE from the related QER, the TDF-U shall then stop such function consequently.

Policy and charging control in the downlink direction by the PCEF for an application detected by the TDF is performed by the PGW-C configuring a PDR with a PDI containing an SDF Filter with the corresponding DSCP value.

### 5.4.6 Usage Monitoring

Usage Monitoring Control refers to the process of monitoring the user plane traffic in the PGW-U or TDF-U for the accumulated usage of network resources per:

- individual or group of service data flows;
- individual or group of applications;

- IP-CAN session, possibly excluding an individual SDF or a group of service data flow(s), and/or
- TDF session, possibly excluding an individual application or a group of application(s).

See subclauses 4.4, 6.2.2.3 and 6.6 of 3GPP TS 23.203 [7] and subclauses 4.5.16, 4.5.17, 4b.5.6, 4b.5.7 of 3GPP TS 29.212 [8].

Usage Monitoring Control is supported over the Sxb and Sxc reference points by activating in the UP function the reporting of usage information towards the CP function, as specified in subclauses 5.3 and 7.8.4 of 3GPP TS 23.214 [2].

The CP function shall control the Usage Reporting in the UP function by:

- creating the necessary PDR(s) to represent the service data flow, application or session;
- creating a URR for each Monitoring key; and
- associating the URR to:
  - all the PDRs of the Sx session, for usage monitoring at IP-CAN or TDF session level, possibly excluding the PDRs matching the SDFs or Applications excluded from the usage monitoring at session level; or
  - the PDR(s) of the Sx session associated to the individual or group of SDF(s) or Application(s), for usage monitoring at SDF or application level.

### 5.4.7 Traffic Redirection

Traffic Redirection refers to the process of redirecting uplink application traffic, in a PGW or TDF, towards a redirect destination, e.g. redirect some HTTP flows to a service provisioning page. See subclause 6.1.13 of 3GPP TS 23.203 [7] and subclauses 4.5.2.6 and 4b.5.1.4 of 3GPP TS 29.212 [8].

The redirect destination may be provided by the PCRF or be preconfigured in the CP function or in the UP function.

The traffic redirection may be enforced in the CP function or in the UP function. If the traffic that the UP function can support may be subject to traffic redirection, traffic redirection enforcement in the UP function shall be supported by the UP function. The UP function reports to the CP function whether it supports traffic redirection enforcement in the UP function via the UP Function Features IE (see subclause 8.2.25).

NOTE: A UP function that supports traffic not requiring traffic redirection does not need to support traffic redirection enforcement in the UP function. The CP function can select a UP function supporting traffic redirection enforcement in the UP function for users or services which may require traffic redirection.

To enforce the traffic redirection in the CP function, the CP function shall instruct the UP function to forward the applicable user traffic to the CP function, as specified in subclause 5.3.1.

To enforce the traffic redirection in the UP function, the CP function shall:

- create the necessary PDR(s) to represent the traffic to be redirected, if not already existing;
- create a FAR with:
  - the Redirect Information IE including the redirect destination, if the traffic needs to be redirected towards a redirect destination provided by the CP function; a redirect destination provided by the CP function shall prevail over a redirect destination preconfigured in the UP function; or
  - the Forwarding Policy IE including the identifier of the forwarding policy to apply, if the traffic needs to be redirected towards a redirect destination preconfigured in the UP function;
- associate the FAR to the above PDRs of the Sx session.

### 5.4.8 Traffic Steering

Traffic Steering refers to the process of applying a specific (S)Gi-LAN traffic steering policy in the PCEF or TDF (or TSSF), for the purpose of steering the subscriber's traffic to appropriate operator or 3rd party service functions (e.g. NAT, antimalware, parental control, DDoS protection) in the (S)Gi-LAN, per service data flows level or applications level.

The UP function shall set the TRST feature flag in the UP Function Features IE if it supports Traffic Steering (see subclause 8.2.25).

Traffic Steering is supported over the Sxb and Sxc reference points by instructing the UP function to apply a specific Forwarding Policy, that is locally configured in the UP function and that can be used for the uplink, the downlink or for both directions. A Forwarding Policy is identified by a Forwarding Policy Identifier.

When so instructed, the UP function shall perform the necessary actions to enforce the forwarding policy referenced by the CP function, e.g. performing packet marking and routing the traffic towards the service functions within the (S)Gi-LAN.

See 3GPP TS 23.203 [7] and 3GPP TS 29.212 [8].

The CP function shall control Traffic Steering towards SGi-LAN in the UP function by:

- creating the necessary PDRs to represent the service data flows or applications to be steered towards SGi-LAN;
- creating a FAR with the Forwarding Policy IE including the Forwarding Policy Identifier set to the Traffic Steering Policy Identifier; and
- associating the FAR to the above PDRs of the Sx session.

The CP function shall control the processing of the traffic received from the (S)Gi-LAN in the UP function as specified in the rest of this specification for traffic received from any other interface, but with PDR(s) including a PDI with the Source Interface indicating "SGi-LAN". The UP function shall distinguish packets coming from (S)Gi-LAN based on local configuration.

### 5.4.9 Provisioning of Predefined PCC/ADC Rules

A Predefined PCC rule is preconfigured in the PCEF, e.g. a PGW. Predefined PCC rules can be activated or deactivated by the PCRF at any time. The Predefined PCC rules may be grouped allowing the PCRF to dynamically activate a set of PCC rules.

A predefined ADC rule is preconfigured in the TDF. In the case of solicited reporting, the Predefined ADC rules can be activated or deactivated by the PCRF at any time. Predefined ADC rules within the TDF may be grouped allowing the PCRF to dynamically activate a set of ADC rules.

See subclauses 4.3.1 and 4b.3.2 of 3GPP TS 29.212 [8].

The CP function may enforce an activated predefined PCC or ADC rule by the PCRF in the UP function by:

- determining the service data filters or application IDs referred by the activated predefined PCC or ADC rule(s) and the corresponding QoS and charging control information respectively;
- creating the necessary PDR(s) to identify the service data flow(s), application(s) that the predefined PCC or ADC rule refer to, if not already existing;
- creating the necessary QER for the QoS enforcement at service data flow or application level accordingly;
- creating the necessary FAR if a new FAR needs to be created as result of Bearer binding and QoS control for forwarding the detected service data flow or application traffic, or to redirect or to apply traffic steering control if included in the predefined PCC/ADC rule;
- creating the necessary URR(s) for each monitoring key, charging key, combination of Charging Key and Service ID, or combination of Charging Key, Sponsor ID and Application Service Provider Id if included in the predefined PCC or ADC rule;

And then:

- associating the created URR(s) to the newly created PDR(s);
- associating the existing FAR or the new FAR to the newly created PDR(s);

Optionally, the traffic handling policies (i.e. predefined QER(s)/FAR(s)/URR(s)) may be configured in the UP function. The CP function may activate these traffic handling policies by including the Activate Predefined Rules IE within:

- the Create PDR IE in an Sx session establishment request; or
- the Update PDR IE in an Sx Session Modification Request.

For traffic matching PDR(s) associated with the activated predefined rules, the UP function shall enforce the rules, e.g. for URR, the UP function shall generate Usage Report(s) and send it to the CP function and the CP function shall be able to handle the usage reports as described in subclause 5.2.2.

NOTE: The URR IDs used in reports triggered by a predefined rule in UP function are also pre-configured at the CP function.

For deactivating predefined rules which are activated in the UP function, the CP function shall include the Deactivate Predefined Rules IE in the Update PDR IE in an Sx Session Modification request to inform the UP function to deactivate the corresponding predefined rules for the related PDR.

## 5.4.10 Charging

The charging requirements for online and offline charging in the PS domain specified in 3GPP TS 32.251 [17] shall be preserved with a split SGW, PGW and TDF architecture.

Charging is supported by the CP function by activating in the UP function the measurement and reporting of the accumulated usage of network resources per:

- IP-CAN bearer, for an SGW;
- IP-CAN bearer, IP-CAN session and/or individual or group of service data flows, for a PGW;
- TDF session and/or individual or group of applications, for a TDF.

See subclauses 5.3 and 7.8.4 of 3GPP TS 23.214 [2].

The CP function shall control the usage measurement and reporting in the UP function by:

- creating the necessary PDR(s) to represent the service data flow, application, bearer or session, if not already existing;
- creating URR(s) for each Charging Key, combination of Charging Key and Service ID, or combination of Charging Key, Sponsor ID and Application Service Provider Id;
- associating the URR(s) to the relevant PDRs defined for the Sx session, for usage reporting at IP-CAN bearer, IP-CAN session, TDF session, SDF or application level.

For online charging, the CP function shall provision the URR with the Volume (or Time) Quota, and with the Volume (or Time) Quota if a quota threshold was received from the OCS, as specified in subclause 5.2.2.2. Besides, when the OCS provides a final quota and requests to redirect the traffic towards a redirect destination when exhausing this quota, the CP function shall redirect the traffic towards a redirect destination as specified in subclause 5.4.7 upon being notified that the final quota has been reached; to permit HTTP traffic redirection, the UP function should have at least one HTTP packet, e.g. the UP function may store one packet when reaching the Volume (or Time) Quota. An example call flow is depicted in Annex C.2.1.1.

To avoid the risk of signalling storms between the CP and UP functions at times of tariff change, the CP function may include the Monitoring Time IE in the URR and set it to the time of tariff change to request the UP function to report separately the resource usage before and after the time of tariff change (see e.g. subclause 6.3.7.1 of 3GPP TS 32.299 [18]).

## 5.4.11 (Un)solicited Application Reporting

(Un)solicited Application Reporting refers to the process of reporting the start or stop of applications by the TDF or PCEF. See 3GPP TS 23.203 [3] and 3GPP TS 29.212 [8].

The CP function shall instruct the UP function to detect and report applications by:

- creating the necessary PDR(s) to represent the applications to detect;
- creating a URR with the Reporting Trigger IE set to detect the start and/or stop of Traffic;

- associating the URR to the PDR.

For unsolicited application reporting, an Sx session which is not linked to any specific TDF session may be established and the PDI in the PDR(s) does not contain any UE IP address.

When detecting the start or stop of an application, the UP function shall then initiate the Sx Session Report procedure and send a Usage Report with the Usage Report Trigger set to 'Start of Traffic' or 'Stop of Traffic'. The UP function shall also include the following information in the Usage Report:

- when reporting the start of an application:
  - the Application ID;
  - the Flow Information including the Flow Description and the Flow Direction, if the traffic flow information is deducible;
  - the Application-Instance-Identifier, if the traffic flow information is deducible; and
  - if no UE IP address was provisioned in the PDI, the UE's IP address, and the Network instance when multiple PDNs with overlapping IP addresses are used in the UP function.

NOTE: When the CP function instructs the UP function to perform unsolicited application reporting, the PDI in the corresponding PDR has no UE IP address.

- when reporting the stop of an application:
  - the Application ID;
  - the Application-Instance-Identifier, if an Application Identifier was provided when reporting the start of the application;
  - if no UE IP address was provisioned in the PDI, the UE's IP address, and the Network instance when multiple PDNs with overlapping IP addresses are used in the UP function.

### 5.4.12 Service Identification for Improved Radio Utilisation for GERAN

Service Identification for improved radio utilization for GERAN refers to the process in the PGW of marking DL user plane traffic with a Service Class Indicator (SCI) value. See subclause 5.3.5.3 of 3GPP TS 23.060 [19].

This is controlled by the PGW-C by associating a QER, including the Service Class Indicator within the DL Flow Level Marking IE, to the PDR matching the DL traffic to be marked. The PGW-U performs the SCI marking for the detected DL traffic and sends the packet with the GTP-U Service Class Indicator Extension Header downstreams.

The PGW-C may stop the SCI marking during the Sx session by removing the related QER or removing the DL Flow Level Marking IE from the related QER, the PGW-U shall then stop such function consequently.

## 5.5 F-TEID Allocation and Release

### 5.5.1 General

F-TEID shall be allocated either by the CP function or the UP function. The support of F-TEID allocation by the CP function is mandatory. The support of F-TEID allocation by the UP function is optional. See subclause 5.4 of 3GPP TS 23.214 [2].

The UP function shall set the FTUP feature flag in the UP Function Features IE if it supports F-TEID allocation in the UP function (see subclause 8.2.25). If so, the CP function shall determine whether F-TEIDs are allocated by the CP function or the UP function based on network configuration. The same F-TEID allocation option shall be used by all the CP functions controlling a particular UP function. The UP function shall reject a request to establish a new PDR with a different F-TEID allocation option than the option used for already created PDRs (by the same or a different CP function), with the cause "Invalid F-TEID allocation option".

### 5.5.2 F-TEID allocation in the CP function

When performing F-TEID allocation in the CP function, the CP function shall assign the Local F-TEID IE of the PDR IE (see Table 7.5.2.2-1) and provide the assigned F-TEID value to the UP function.

### 5.5.3 F-TEID allocation in the UP function

When performing F-TEID allocation in the UP function, the CP function shall request the UP function to allocate the F-TEID by setting the CHOOSE flag in the Local F-TEID IE of the PDR IE (see Table 7.5.2.2-1). The Source Interface IE indicates for which interface the F-TEID is to be assigned.

The CP function may request the UP function to allocate the same F-TEID to several PDRs to be created within one single Sx Session Establishment Request or Sx Session Modification Request by:

- setting the CHOOSE flag in the Local F-TEID IE of each PDR to be created with a new F-TEID, and
- setting the CHOOSE ID field of the Local F-TEID IE, for each PDR to be created with the same F-TEID, with the same CHOOSE ID value.

If the PDR(s) is created successfully, the UP function shall return the F-TEID(s) it has assigned to the PDR(s) in the Sx Session Establishment Response or Sx Session Modification Response.

Upon receiving a request to remove a PDR or delete an Sx session, the UP function shall free the F-TEID(s) that was assigned to the PDR or to the Sx Session.

## 5.6 Sx Session Handling

### 5.6.1 General

The following subclauses provide details on Sx Sessions handling.

### 5.6.2 Session Endpoint Identifier Handling

The SEID uniquely identifies an Sx session at an IP address of a PFCP entity. The F-SEID is the Fully Qualified SEID and it contains the SEID and IP address. The PFCP endpoint locally assigns the SEID value the peer PFCP side has to use when transmitting message. The SEID values are exchanged between PFCP endpoints using PFCP messages. The PFCP entity communicates to the peer PFCP entity the SEID value at which it expects to receive all subsequent control plane messages related to that Sx session via the "F-SEID" IE.

The Sx session related messages shall share the same F-SEID for the Sx session. A F-SEID shall be released after the Sx session is released.

### 5.6.3 Modifying the Rules of an Existing Sx Session

The following principles shall apply, unless specified otherwise in the specification.

When modifying an existing Sx session, the CP function shall only provide in the PFCP Request message the requested changes compared to what was previously provisioned in the UP function for this Sx session, i.e. the CP function shall:

- include IEs which needs to be newly provisioned in the UP function;
- include IEs which need to be provisioned with a modified value;
- remove IEs which need to be removed from the set of parameters previously provisioned in the UP function, as further specified below.

The CP function shall remove IEs which needs to be removed by either:

- removing the entire Rule if no other parameter of that rule needs to remain provisioned in the UP function, e.g. by including the Remove URR IE in the Sx Session Modification Request; or

- updating the Rule including the IEs to be removed with a null length, e.g. by including the Update URR IE in the Sx Session Modification Request with the IE(s) to be removed with a null length.

The CP function shall set a URR ID and/or QER ID with a length "0" in the Update PDR IE within Sx Session Modification Request, to request the UP function to stop applying the URRs and/or QERs for this PDR.

Upon receipt of an PFCP Request which modifies an existing Sx session, the UP function shall add, update or remove the parameters as instructed by the CP function, as defined above, and shall keep unchanged the set of parameters previously provisioned in the UP function which are neither modified nor removed.

# 5.7 Support of Lawful Interception

Requirements for support of Lawful Interception with a split SGW or PGW are specified in subclauses 12.9 and 20.4 of 3GPP TS 33.107 [20].

User plane packets shall be forwarded from the UP function to the SX3LIF (or LMISF for S8HR) by encapsulating the user plane packets using GTP-U encapsulation (see 3GPP TS 29.281 [3]).

The CP function shall instruct the UP function to duplicate the packets to be intercepted and to forward them to the SX3LIF (or to the LMISF for S8HR) as specified in subclause 5.2.3.

For forwarding data from the UP function to the SX3LIF (or LMISF for S8HR), the CP function shall set the DUPL flag in the Apply Action and set the Duplicating Parameters in the FAR, associated to the PDRs of the traffic to be intercepted, with the Destination Interface "LI Function" and set to perform GTP-U encapsulation and to forward the packets to a GTP-u F-TEID uniquely assigned in the SX3LIF (or LMISF for S8HR) for the traffic to be intercepted. The SX3LIF (or LMISF for S8HR) shall then identify the intercepted traffic by the F-TEID in the header of the encapsulating GTP-U packet.

# 5.8 Sx Association

## 5.8.1 General

An Sx Association shall be set up between the CP function and the UP function prior to establishing Sx sessions on that UP function. Only one Sx association shall be setup between a given pair of CP and UP functions.

The CP function and the UP function shall support the Sx Association Setup procedure initiated by the CP function (see subclause 6.2.6.2). The CP function and the UP function may additionally support the Sx Association Setup procedure initiated by the UP function (see subclause 6.2.6.3).

A CP function may have Sx Associations set up with multiple UP functions. A UP function may have Sx Associations set up with multiple CP functions.

## 5.8.2 Behaviour with an Established Sx Association

When an Sx Association is established with a UP function, the CP function:

- shall provision node related parameters (i.e. parameters that apply to all Sx sessions) in the UP function, if any, e.g. PFDs;
- shall provision the UP function with the list of features (affecting the UP function behaviour) the CP function supports, if any, e.g. support of load and/or overload control;
- shall check the responsiveness of the UP function using the Heartbeat procedure as specified in subclause 6.2.2;
- may establish Sx sessions on that UP function;
- shall refrain from attempting to establish new Sx sessions on the UP function, if the UP function has indicated it will shut down gracefully.

When an Sx Association is established with a CP function, the UP function:

- shall update the CP function with the list of features it supports;

- shall update the CP function with its load and/or overload control information, if load and/or overload control is supported by the CP and UP functions;

- may update the CP function with the set of its IP resources available for use by the CP function, when F-TEID allocation is performed by the CP function;

NOTE: The CP function can be aware of the available IP resources in the UP function e.g. based on the UP function reporting this information over Sx using Sx node related messages, or by other implementation specific means.

- shall accept Sx Session related messages from that CP function (unless prevented by other reasons, e.g. overload);

- shall check the responsiveness of the CP function using the Heartbeat procedure as specified in subclause 6.2.2;

- shall indicate to the CP function if it will shut down within a graceful period and, when possible, if it fails and becomes out of service.

### 5.8.3 Behaviour without an Established Sx Association

When an Sx Association is not established with a UP function, the CP function:

- shall reject any incoming Sx Session related messages from that UP function, with a cause indicating that no Sx association exists with the peer entity.

When an Sx Association is not yet established with a CP function, the UP function:

- shall reject any incoming Sx Session related messages from that CP function, with a cause indicating that no Sx association exists with the peer entity.

## 5.9 Usage of Vendor-specific IE

Vendor-specific IEs are defined to cover requirements and features not specified by 3GPP.

NOTE 1: When a IE is intended to be used by more than one vendor, the definition of the IE is encouraged to be specified by 3GPP to ease implementation and interoperability.

NOTE 2: The PFCP entities can use Vendor-specific IE(s) in the Sx message relevant to the Sx Association Setup procedure to learn which vendor specific enhancements are supported by the peer.

In a network with Vendor specific enhancements, unrecognized vendor specific IEs shall be handled as unknown optional IEs.

## 5.10 Error Indication Handling

Upon receipt of a GTP-U Error Indication message, the UP function:

- shall identify the related Sx session for which the message is received; and

- shall initiate an Sx Session Report procedure, towards the CP function controlling this Sx session, to send an Error Indication Report including the remote F-TEID signalled in the GTP-U Peer Address IE and the Tunnel Endpoint Identifier Data I IE of the GTP-U Error Indication (see subclause 7.3.1 of 3GPP TS 29.281 [3]).

Upon receipt of an Error Indication Report, the CP function shall then identify the bearer for which the Error Indication Report is received using the remote F-TEID included in the report and proceed as specified in subclauses 21.7 and 21.8 of 3GPP TS 23.007 [24], i.e.:

- modify the Sx session to instruct the UP function to buffer DL packets;

- modify the Sx session to delete the PDR and FAR, when having to delete a bearer; or

- delete the Sx session, when having to delete the PDN connection.

# 6 Procedures

## 6.1 Introduction

The following subclauses specify the procedures supported over the Sxa, Sxb and Sxc reference points.

## 6.2 Sx Node Related Procedures

### 6.2.1 General

The following subclauses specify the node related procedures over the Sxa, Sxb and Sxc reference points. The behaviour of the CP function und UP function when sending and receiving a node related message is described.

### 6.2.2 Heartbeat Procedure

#### 6.2.2.1 General

Two messages are specified for PFCP heartbeat procedure: Heartbeat Request and Heartbeat Response. The use of these messages is further specified in clause 19A of 3GPP TS 23.007 [24].

#### 6.2.2.2 Heartbeat Request

The CP function or the UP function may send an Heartbeat Request on a path to the peer node to find out if it is alive. Heartbeat Request messages may be sent for each peer with which an Sx control association is established.

For each peer with which an Sx control association is established, a CP function or UP function shall be prepared to receive an Heartbeat Request at any time and it shall reply with an Heartbeat Response.

#### 6.2.2.3 Heartbeat Response

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

### 6.2.3 Load Control Procedure

#### 6.2.3.1 General

Load Control is an optional feature defined over the Sxa, Sxb and Sxc reference points.

Load control enables the UP function to send its load information to the CP function to adaptively balance the Sx session load across the UP functions according to their effective load. The load information reflects the operating status of the resources of the UP function.

Load control allows for better balancing of the Sx session load, so as to attempt to prevent overload in the first place (preventive action). Load control does not trigger overload mitigation actions even if the UP function reports a high load.

Load control and overload control may be supported and activated independently in the network, based on operator's policy.

#### 6.2.3.2 Principles

The UP function may signal its Load Control Information to reflect the operating status of its resources, at the node level, allowing the receiving CP function to use this information to augment the UP function selection procedures.

The Load Control Information is piggybacked in PFCP request or response messages such that the exchange of Load Control Information does not trigger extra signalling.

NOTE: The inclusion of Load Control Information in existing messages means that the frequency of transmission of load control information increases as the session load increases, allowing for faster feedback and thus better regulation of the load.

The calculation of the Load Control Information is implementation dependent and its calculation and transfer shall not add significant additional load to the node itself and to its corresponding peer nodes.

### 6.2.3.3 Load Control Information

#### 6.2.3.3.1 General Description

A PFCP message may contain one instance of the Load Control Information (LCI) IE.

When providing load control information in a message for the first time or subsequently, the UP function shall always include the full set of load control information, i.e. all the node level instance of the Load Control Information, even if only a subset of the load control information has changed. The Load Control Sequence Number shall be incremented whenever the load control information is changed (see subclause 6.2.3.3.2.1).

Load Control Information shall be linked to the Node ID (i.e. FQDN or the IP address used during the UP function selection) of the UP function providing the Information.

The receiver shall overwrite any stored load control information of a peer with the newly received load control information from the same peer node if the new load control information is more recent than the old information as indicated by the Load Control Sequence Number, e.g. if the receiver has stored an instance of the load control information for a peer node, it overwrites this instance with the new instance received in a message from the same peer node.

The receiver shall consider all the parameters received in the same instance of the LCI IE in conjunction while using this information for UP function selection.

The parameters are further defined in subclause 6.2.3.3.2.

Load control information may be extended with new parameters in future versions of the specification. Any new parameter will have to be categorized as:

- Non-critical optional parameters: the support of these parameters is *not critical* for the receiver. The receiver can successfully and correctly comprehend the load control information instance, containing one or more of these parameters, by using the other parameters and ignoring the non-critical optional parameter.

- Critical optional parameters: the support of these parameters is *critical* for the receiver to correctly comprehend the instance of the load control information containing one or more of these parameters.

The sender may include one or more non-critical optional parameters within any instance of the LCI IE without having the knowledge of the receiver's capability to support the same. However, the sender shall only include one or more critical optional parameter in an instance of the LCI IE towards a receiver if the corresponding receiver is known to support those parameters. The sender may be aware of this either via signalling methods or by configuration (this will have to be defined when introducing any such new parameter in future).

#### 6.2.3.3.2 Parameters

##### 6.2.3.3.2.1 Load Control Sequence Number

The Load Control Sequence number contains a value that indicates the sequence number associated with the LCI IE. This sequence number shall be used to differentiate any two LCI IEs generated at two different instances by the same UP function. The Load Control Sequence Number shall be supported (if load control is supported) and shall always be present in the LCI IE.

The UP function generating this information shall increment the Load Control Sequence Number whenever modifying some information in the Load Control Information IE. The Load Control Sequence Number shall not be incremented otherwise. The UP function may use the time, represented in an unsigned integer format, of the generation of the Load Control Information to populate the Load Control Sequence Number.

This parameter shall be used by the receiver of the Load Control Information IE to properly collate out-of-order load control information, e.g. due to PFCP retransmissions. This parameter shall also be used by the receiver of the LCI IE to determine whether the newly received load control information has changed compared to load control information previously received from the same node earlier.

NOTE: The PFCP sequence number cannot be used for collating out-of-order load control information as e.g. load control information may be sent in both PFCP requests and responses, using independent PFCP sequence numbering.

If the receiving entity has already received and stored load control information from the peer UP function, the receiving CP function shall update its load control information only if the Load Control Sequence Number received in the new load control information is higher than the stored value of the Load Control Sequence Number associated with the peer UP function. However due to roll-over of the Load Control Sequence Number or restart of the node, the Load Control Sequence Number may be reset to an appropriate base value by the peer UP function, hence the receiving entity shall be prepared to receive (and process) a Load Control Sequence Number parameter whose value is less than the previous value.

#### 6.2.3.3.2.2 Load Metric

The Load Metric parameter shall indicate the current load level of the originating node. The computation of the Load Metric is left to implementation. The node may consider various aspects, such as the used capacity of the UP function, the load in the node (e.g. memory/CPU usage in relationship to the total memory/CPU available, etc.).

The Load Metric represents the current load level of the sending node as a percentage within the range of 0 to100, where 0 means no or 0% load and 100 means maximum or 100% load reached (i.e. no further load is desirable).

The Load Metric shall be supported (if load control is supported). The Load Metric shall always be included in the Load Control Information.

Considering the processing requirement of the receiver of the Load Control Information (e.g. handling of the new information, tuning the node selection algorithm to take the new information into account), the sender should refrain from advertising every small variation (e.g. with the granularity of 1 or 2), in the Load Metric which does not result in useful improvement in node selection logic at the receiver. During the typical operating condition of the sender, a larger variation in the Load Metric, e.g. 5 or more units, should be considered as reasonable enough for advertising the new Load Control Information and thus justifying the processing requirement (to handle the new information) of the receiver.

NOTE: The range of the Load Metric, i.e. 0 to 100, does not mandate the sender to collect its own load information at every increment/decrement and hence to advertise the change of Load Metric with a granularity of 1%. Based on various implementation specific criteria, such as: the architecture, session and signalling capacity, the current load and so on, the sender is free to define its own logic and periodicity with which its own load information is collected.

### 6.2.3.3.3 Frequency of Inclusion

How often the sender includes the load control information is implementation specific. The sender shall ensure that new/updated load control information is propagated to the target CP functions within an acceptable delay, such that the purpose of the information (i.e. effective load balancing) is achieved. The sender may include the LCI IE e.g. as follows:

- the sender may include Load Control Information towards a peer only when the new/changed value has not already been provided to that peer;
- the sender may include the Load Control Information in each and every message (extended with LCI IE) towards the peer;
- the sender may include Load Control Information periodically, i.e. include the information during a first period then cease to do so during a second period.

The sender may also implement a combination of one or more of the above approaches. Besides, the sender may also decide to include the Load Control Information only in a subset of the applicable PFCP messages.

The receiver shall be prepared to receive the load control information in any of the PFCP messages extended with an LCI IE and upon such reception, shall be able act upon the received load control information.

## 6.2.4 Overload Control Procedure

### 6.2.4.1 General

Overload Control is an optional feature defined over the Sxa, Sxb and Sxc reference points.

Overload control enables a UP function becoming or being overloaded to gracefully reduce its incoming signalling load by instructing its peer CP functions to reduce sending traffic according to its available signalling capacity to successfully process the traffic. A UP function is in overload when it operates over its signalling capacity which results in diminished performance (including impacts to handling of incoming and outgoing traffic).

Overload control aims at shedding the incoming traffic as close to the traffic source as possible generally when an overload has occurred (reactive action), so to avoid spreading the problem inside the network and to avoid using resources of intermediate nodes in the network for signalling that would anyhow be discarded by the overloaded node.

Load control and overload control may be supported and activated independently in the network, based on operator's policy.

### 6.2.4.2 Principles

When a UP function determines that the offered incoming signalling traffic is growing (or is about to grow) beyond its nominal capacity, the UP function may signal its overload, at node level granularity, to its peer CP functions by including Overload Control Information in PFCP signalling which provides guidance to the receiving CP functions to decide actions which lead to signalling traffic mitigation towards the sender of the information. This helps in preventing severe overload and hence potential breakdown of the UP function.

The Overload Control Information is piggybacked in PFCP request or response messages such that the exchange of Overload Control Information does not trigger extra signalling.

NOTE: The inclusion of Overload Control Information in existing messages means that the frequency of transmission of overload control information increases as the signalling load increases, thus allowing for faster feedback and better regulation.

The calculation of the Overload Control Information is implementation dependent and its calculation and transfer shall not add significant additional load to the node itself and to its corresponding peer nodes. The calculation of Overload Control Information should not severely impact the resource utilization of the UP function, especially considering the overload situation.

The overload control feature should continue to allow for preferential treatment of priority users (eMPS) and emergency services.

The overload mitigation actions based on the reception of the overload related information received from the UP function will not be standardized.

### 6.2.4.3 Overload Control Information

#### 6.2.4.3.1 General Description

A PFCP message may contain one instance of the Overload Control Information (OCI) IE.

When providing overload control information in a message for the first time or subsequently, the UP function shall always include the full set of overload control information, i.e. all the node level instance of the Overload Control Information, even if only a subset of the overload control information has changed. The Overload Control Sequence Number shall be incremented whenever the Overload control information is changed (see subclause 6.2.4.3.2.1).

The receiver shall overwrite any stored overload control information of a peer with the newly received overload control information from the same peer node if the new overload control information is more recent than the old information as indicated by the Overload Control Sequence Number, e.g. if the receiver has stored an instance of the Overload control information for a peer node, it overwrites this instance with the new instance received in a message from the same peer node.

The receiver shall consider all the parameters received in the same instance of the OCI IE in conjunction while applying the overload mitigation action.

The parameters are further defined in subclause 6.2.4.3.2.

Overload control information may be extended with new parameters in future versions of the specification. Any new parameter will have to be categorized as:

- Non-critical optional parameters: the support of these parameters is *not critical* for the receiver. The receiver can successfully and correctly comprehend the Overload control information instance, containing one or more of these parameters, by using the other parameters and ignoring the non-critical optional parameter.

- Critical optional parameters: the support of these parameters is *critical* for the receiver to correctly comprehend the instance of the Overload control information containing one or more of these parameters.

The sender may include one or more non-critical optional parameters within any instance of the OCI IE without having the knowledge of the receiver's capability to support the same. However, the sender shall only include one or more critical optional parameter in an instance of the OCI IE towards a receiver if the corresponding receiver is known to support those parameters. The sender may be aware of this either via signalling methods or by configuration (this will have to be defined when introducing any such new parameter in future).

The Overload Control Information shall be associated by default to the PFCP entity corresponding to the peer node's IP address of the Sx session, over which the OCI IE is received, i.e. to the IP address received within the "UP F-SEID" IE.

Alternatively, the UP function may send Overload Control Information which is associated with the Node ID of the UP function (i.e. FQDN or the IP address used during the UP function selection). In that case, the UP function shall provide an explicit indication that the OCI IE included in the message belongs to the Node ID.

#### 6.2.4.3.2 Parameters

##### 6.2.4.3.2.1 Overload Control Sequence Number

The PFCP protocol requires retransmitted messages to have the same contents as the original message. Due to PFCP retransmissions, the overload control information received by a CP function at a given time may be less recent than the overload control information already received from the same UP function. The Overload Control Sequence Number aids in sequencing the overload control information received from an overloaded UP function. The Overload Control Sequence Number contains a value that indicates the sequence number associated with the Overload Control Information IE. This sequence number shall be used to differentiate between two OCI IEs generated at two different instants, by the same UP function.

The Overload Control Sequence Number parameter shall be supported (when supporting the overload control feature) and shall always be present in the Overload Control Information IE.

The UP function generating this information shall increment the Overload Control Sequence Number whenever modifying some information in the OCI IE. The Overload Control Sequence Number shall not be incremented otherwise. The UP function may use the time, represented in an unsigned integer format, of the generation of the overload control information, to populate the Overload Control Sequence Number.

This parameter shall be used by the receiver of the OCI IE to properly collate out-of-order OCI IEs, e.g. due to PFCP retransmissions. This parameter shall also be used by the receiver of the OCI IE to determine whether the newly received overload control information has changed compared to the overload control information previously received from the same UP function. If the newly received overload control information has the same Overload Control Sequence Number as the previously received overload control information from the same UP function, then the receiver may simply discard the newly received overload control information whilst continuing to apply the overload abatement procedures, as per the previous value.

NOTE 1: The timer corresponding to the Period of Validity (see subclause 6.2.4.3.2.2) is not restarted if the newly received overload control information has the same Overload Control Sequence Number as the previously received overload control information. If the overload condition persists and the overloaded UP function needs to extend the duration during which the overload information applies, the sender needs to provide a new overload control information with an incremented Overload Control Sequence Number (even if the parameters within the overload control information have not changed).

NOTE 2: The PFCP Sequence Number cannot be used for collating out-of-order overload information as e.g. overload control information may be sent in both PFCP requests and responses, using independent PFCP sequence numbering.

If the receiving CP function already received and stored overload control information, which is still valid, from the overloaded UP function, the receiving entity shall update its overload control information, only if the Overload-Sequence-Number received in the new overload control information is larger than the value of the Overload Control Sequence Number associated with the stored information. However due to roll-over of the Overload Control Sequence Number or restart of the UP function, the Overload Control Sequence Number may be reset to an appropriate base value by the peer UP function, hence the receiving entity shall be prepared to receive (and process) an Overload Control Sequence Number parameter whose value is less than the previous value.

#### 6.2.4.3.2.2 Period of Validity

The Period of Validity indicates the length of time during which the overload condition specified by the OCI IE is to be considered as valid (unless overridden by subsequent new overload control information).

An overload condition shall be considered as valid from the time the OCI IE is received until the period of validity expires or until another OCI IE with a new set of information (identified using the Overload Control Sequence Number) is received from the same UP function (at which point the newly received overload control information shall prevail). The timer corresponding to the period of validity shall be restarted each time an OCI IE with a new set of information (identified using the Overload Control Sequence Number) is received. When this timer expires, the last received overload control information shall be considered outdated and obsolete, i.e. any associated overload condition shall be considered to have ceased.

The Period of Validity parameter shall be supported (when supporting overload control).

The Period of Validity parameter achieves the following:

- it avoids the need for the overloaded UP function to include the Overload Control Information IE in every PFCP messages it signals to its peer CP functions when the overload state does not change; thus it minimizes the processing required at the overloaded UP function and its peer CP functions upon sending/receiving PFCP signalling;

- it allows to reset the overload condition after some time in the peer CP functions having received an overload indication from the overloaded UP function, e.g. if no signalling traffic takes place between these PFCP entities for some time due to overload mitigation actions. This also removes the need for the overloaded UP function to remember the list of CP functions to which it has sent a non-null overload reduction metric and to which it would subsequently need to signal when the overload condition ceases, if the Period of Validity parameter was not defined.

#### 6.2.4.3.2.3 Overload Reduction Metric

The Overload Reduction Metric shall have a value in the range of 0 to 100 (inclusive) which indicates the percentage of traffic reduction the sender of the overload control information requests the receiver to apply. An Overload Reduction Metric of "0" always indicates that the UP function is not in overload (that is, no overload abatement procedures need to be applied) for the indicated scope.

Considering the processing requirement of the receiver of the Overload Control Information, e.g. to perform overload control based on the updated Overload Reduction Metric, the sender should refrain from advertising every small variation, e.g. with the granularity of 1 or 2, in the Overload Reduction Metric which does not result in useful improvement for mitigating the overload situation. During the typical operating condition of the sender, a larger variation in the Overload Reduction Metric, e.g. 5 or more units, should be considered as reasonable enough for advertising a new Overload Reduction Metric Information and thus justifying the processing requirement (to handle the new information) of the receiver.

NOTE: The range of Overload Reduction Metric, i.e. 0 to 100, does not mandate the sender to collect its own overload information at every increment/decrement and hence to advertise the change of Overload Reduction Metric with a granularity of 1%. Based on various implementation specific criteria, such as the architecture, session and signalling capacity, the current load/overload situation and so on, the sender is free to define its own logic and periodicity with which its own overload control information is collected.

The computation of the exact value for this parameter is left as an implementation choice at the sending UP function.

The Overload Reduction Metric shall be supported (when supporting overload control) and shall always be present in the OCI IE.

The inclusion of the OCI IE signals an overload situation is occuring, unless the Overload Reduction Metric is set to 0, which signals that the overload condition has ceased. Conversely, the absence of the OCI IE in a message does not mean that the overload has abated.

#### 6.2.4.3.3 Frequency of Inclusion

How often or when the sender includes the overload control information is implementation specific. The sender shall ensure that new/updated overload control information is propagated to the target receivers with an acceptable delay, such that the purpose of the information, (i.e. the effective overload control protection) is achieved. The following are some of the potential approaches the sender may implement for including the OCI IE:

- the sender may include OCI IE towards a receiver only when the new/changed value has not already been provided to the given receiver;
- the sender may include the OCI IE in a subset of the messages towards the receiver;
- the sender may include the OCI IE periodically, i.e. include the information during a first period then cease to do so during a second period.

The sender may also implement a combination of one or more of the above approaches. Besides, the sender may also include the OCI IE only in a subset of the applicable PFCP messages.

The receiver shall be prepared to receive the overload control information received in any of the PFCP messages extended with an OCI IE and upon such reception, shall be able act upon the received information.

### 6.2.4.4 Message Throttling

#### 6.2.4.4.1 General

As part of the overload mitigation, a CP function shall reduce the total number of messages, which would have been sent otherwise, towards the overloaded peer based on the information received within the Overload Control Information. This shall be achieved by discarding a fraction of the messages in proportion to the overload level of the target peer. This is called "message throttling".

Message throttling shall only apply to Request messages. Response messages should not be throttled since that would result in the retransmission of the corresponding request message by the sender.

A CP function supporting PFCP overload control shall support and use the "Loss" algorithm as specified in this clause, for message throttling.

#### 6.2.4.4.2 Throttling algorithm – "Loss"

##### 6.2.4.4.2.1 Description

An overloaded UP function shall ask its peers to reduce the number of requests they would ordinarily send by signalling Overload Control Information including the requested traffic reduction, as a percentage, within the "Overload-Reduction-Metric", as specified in subclause 6.2.4.3.2.

The recipients of the "Overload-Reduction-Metric" shall reduce the number of requests sent by that percentage, either by redirecting them to an alternate destination if possible (e.g. the Sx Session Establishment Request message may be redirected to an alternate UP function), or by failing the request and treating it as if it was rejected by the destination UP function.

For example, if a sender requests another peer to reduce the traffic it is sending by 10%, then that peer shall throttle 10% of the traffic that would have otherwise been sent to this UP function.

The overloaded UP function should periodically adjust the requested traffic reduction based e.g. on the traffic reduction factor that is currently in use, the current system utilization (i.e. the overload level) and the desired system utilization (i.e. the target load level), and/or the rate of the current overall received traffic.

Annex A.1 provides an (informative) example of a possible implementation of the "Loss" algorithm, amongst other possible methods.

NOTE 1: This algorithm does not guarantee that the future traffic towards the overloaded UP function will be less than the past traffic but it ensures that the total traffic sent towards the overloaded UP function is less than what would have been sent without any throttling in place. If after requesting a certain reduction in traffic, the overloaded UP function receives more traffic than in the past, whilst still in overload, leading to the worsening rather than an improvement in the overload level, then the overloaded UP function can request for more reduction in traffic. Thus, by periodically adjusting the requested traffic reduction, the overloaded node can ensure that it receives, approximately, the amount of traffic which it can handle.

NOTE 2: Since the reduction is requested as a percentage, and not as an absolute amount, this algorithm achieves a good useful throughput towards the overloaded node when the traffic conditions vary at the source nodes (depending upon the events generated towards these source nodes by other entities in the network), as a potential increase of traffic from some source nodes can possibly be compensated by a potential decrease of traffic from other source nodes.

### 6.2.4.5 Message Prioritization

#### 6.2.4.5.1 Description

When performing message throttling:

- PFCP requests related to priority traffic (i.e. eMPS as described in 3GPP TS 22.153 [15]) and emergency have the highest priority. Depending on regional/national requirements and network operator policy, these PFCP requests shall be the last to be throttled, when applying traffic reduction, and the priority traffic shall be exempted from throttling due to PFCP overload control up to the point where the requested traffic reduction cannot be achieved without throttling the priority traffic;

- for other types of sessions, messages throttling should consider the relative priority of the messages so that the messages which are considered as low priority are considered for throttling before the other messages. The relative priority of the messages may be derived from the relative priority of the procedure for which the message is being sent or may be derived from the session parameters such as APN, QCI, ARP and/or Low Access Priority Indicator (LAPI).

NOTE: A random throttling mechanism, i.e. discarding the messages without any special consideration, could result in an overall poor congestion mitigation mechanism and bad user experience.

An overloaded node may also apply these message prioritization schemes when handling incoming initial messages during an overloaded condition, as part of a self-protection mechanism.

#### 6.2.4.5.2 Based on the Message Priority Signalled in the PFCP Message

Message prioritization may be performed by an overloaded node, when handling incoming messages during an overloaded condition, based on the relative PFCP message priority signalled in the PFCP header (see subclause 7.2.2.3).

A PFCP entity shall determine whether to set and use the message priority in PFCP signalling, based on operator policy. The requirements specified in this subclause shall apply if message priority in PFCP signalling is used.

A sending PFCP entity shall determine the relative message priority to signal in the message according to the principles specified in subclause 6.2.4.5.1. If the message affects multiple bearers, the relative message priority should be determined considering the highest priority ARP among all the bearers.

A PFCP entity should set the same message priority in a Response message as received in the corresponding Request message.

For incoming PFCP messages that do not have a message priority in the PFCP header, the receiving PFCP entity:

- shall apply a default priority, if the incoming message is a Request message;

- should apply the message priority sent in the Request message, if the incoming message is a Response message.

This feature should be supported homogenously across the CP functions and UP functions in the network, otherwise an overloaded node will process Request messages received from the non-supporting nodes according to the default

priority while Request messages received from supporting nodes will be processed according to the message priority signalled in the PFCP message.

## 6.2.5 Sx PFD Management Procedure

### 6.2.5.1 General

The Sx PFD Management procedure may be used by the CP function and UP function to provision PFDs to the UP function, for one or more Application Identifiers, as specified in subclauses 5.11.4 and 6.5.2 of 3GPP TS 23.214 [2].

Support of this procedure is optional for the CP function and the UP function. The UP function shall set the PFDM feature flag in the UP Function Features IE if it supports the PFD Management procedure (see subclause 8.2.25).

The UP function shall store the PFDs provisioned per Application Identifier. These PFDs shall apply to all the Sx session established in the UP function, for all the controlling CP functions, i.e. the scope of a PFD is not limited to the Sx sessions established by the CP function which provisioned the PFD.

### 6.2.5.2 CP Function Behaviour

The CP function initiates the Sx PFD Management procedure to provision PFDs in the UP function, for one or more Application Identifier(s).

The CP function:

- shall send the Sx PFD Management Request message, including the full set of PFD IDs and PFD contents to be provisioned in the UP function per Application Identifier.

When the CP function receives an Sx PFD Management Response with cause success, the CP function shall consider that the PFDs have been provisioned as requested.

### 6.2.5.3 UP Function Behaviour

When the UP function receives an Sx PFD Management Request message, it shall:

- if no Application ID's PFDs IE is present in the request (i.e. empty message),
  - delete all the PFDs received and stored earlier for all Application Identifier(s);
- if at least one Application ID's PFDs IE is present in the request,
  - delete all the PFDs received and stored earlier for the indicated Application Identifier(s);
  - store all the PFDs received in the request for the indicated Application Identifier(s);
- send an Sx PFD Management Response with the cause "success", if the above operations were performed successfully.

## 6.2.6 Sx Association Setup Procedure

### 6.2.6.1 General

The Sx Association Setup procedure shall be used to setup an Sx association between the CP function and the UP function, to enable the CP function to use the resources of the UP function subsequently, i.e. establish Sx Sessions.

The setup of an Sx association may be initiated by the CP function (see subclause 6.2.6.2) or the UP function (see subclause 6.2.6.3).

The CP function and the UP function shall support the Sx Association Setup initiated by the CP function. The CP function and the UP function may additionally support the Sx Association Setup initiated by the UP function.

### 6.2.6.2 Sx Association Setup Initiated by the CP Function

#### 6.2.6.2.1 CP Function Behaviour

The CP function initiates the Sx Association Setup procedure to request to setup an Sx association towards a UP function prior to establishing a first Sx session on this UP function.

The CP function:

- shall send the Sx Association Setup Request with the Node ID of the CP function;
- shall include the list of optional features the CP function supports which may affect the UP function behaviour, if any.

The CP function shall only initiate Sx Session related signalling procedures toward a UP function after it receives the Sx Association Setup Response with a successful cause from this UP function.

The CP function shall determine whether the UP function supports Sxa, Sxb, Sxc and/or combined Sxa/Sxb by local configuration or optionally via DNS if deployed.

#### 6.2.6.2.2 UP Function behaviour

When receiving an Sx Association Setup Request, the UP function:

- if the request is accepted:
  - shall store the Node ID of the CP function as the identifier of the Sx association;
  - shall send an Sx Association Setup Response with a successful cause, including, all supported optional features in the UP function and optionally including the available user plane resources, e.g. IP address(es) or F-TEID range;
- shall send an Sx Version Not Supported Response if the PFCP header of the request indicates a PFCP protocol version that is not supported by the UP function;
- otherwise, shall send an Sx Association Setup Response with an appropriate error cause if the request is rejected.

### 6.2.6.3 Sx Association Setup Initiated by the UP Function

#### 6.2.6.3.1 UP Function Behaviour

The UP function initiates the Sx Association Setup procedure to request to setup an Sx association towards a CP function. The UP function is configured with a set of CP functions to which it shall establish an Sx association.

The UP function shall send the Sx Association Setup Request including:

- the Node ID of the UP function;
- all supported optional features in the UP function and optionally including the available user plane resources, e.g. IP address(es) or F-TEID range.

#### 6.2.6.3.2 CP Function Behaviour

When receiving an Sx Association Setup Request, the CP function:

- if the request is accepted:
  - shall store the Node ID of the UP function as the identifier of the Sx association;
  - shall include the list of optional features the CP function supports which may affect the UP function behaviour, if any;
- shall send an Sx Version Not Supported Response if the PFCP header of the request indicates a PFCP protocol version that is not supported by the CP function;

- otherwise, shall send an Sx Association Setup Response with an appropriate error cause if the request is rejected.

The CP function shall only initiate Sx Session related signalling procedures toward a UP function after it has sent the Sx Association Setup Response with a successful cause to the UP function.

The CP function shall determine the UP function supports Sxa, Sxb, Sxc and/or combined Sxa/Sxb by local configuration or optionally via DNS if deployed.

## 6.2.7 Sx Association Update Procedure

### 6.2.7.1 General

The Sx Association Update procedure shall be used to modify an existing Sx association between the CP function and the UP function. It may be initiated by the UP function or by the CP function to update the supported features or available resources of the UP function.

### 6.2.7.2 Sx Association Update Procedure Initiated by the CP Function

#### 6.2.7.2.1 CP Function Behaviour

The CP function initiates the Sx Association Update procedure to report changes to the Sx association to the UP function, e.g. to update the supported features.

#### 6.2.7.2.2 UP Function Behaviour

When receiving an Sx Association Update Request, the UP function:

- shall update the list of optional features of the CP function, when received;
- shall send an Sx Association Setup Response with an appropriate error cause if the Node ID is not known by the UP Function;
- shall return an Sx Association Setup Response with a successful cause value, if the Sx Association Update Request is handled successfully.

### 6.2.7.3 Sx Association Update Procedure Initiated by UP Function

#### 6.2.7.3.1 UP Function Behaviour

The UP function initiates the Sx Association Modification procedure to report changes to the Sx association to the CP function, e.g. change of optional features, change of the available user plane resources, an indication to request to release the Sx association.

The UP function may send an Sx Association Update Request to request the CP function to perform the release of the Sx association, optionally providing a Graceful Release Period. After reception of the Sx Association Update Response, the UP function shall consider that the Sx association is still setup until receiving an Sx Association Release Request.

#### 6.2.7.3.2 CP Function Behaviour

When receiving an Sx Association Update Request, the CP function:

- shall update the list of optional features of the UP function, when received;
- shall send an Sx Association Setup Response with an appropriate error cause if the Node ID is not known by the CP Function;
- shall return an Sx Association Setup Response with a successful cause value if the Sx Association Update Request is handled successfully.

If the UP function has requested to release the Sx association in the Sx Association Update Request, the CP function should initiate an Sx Association Release Request to release the Sx association, as soon as possible if no Graceful Release Period was included in the request or before the expiry of the Graceful Release Period.

If the UP function has included User Plane IP Resource Information IE in the Sx Association Update Request message, the CP function shall use it to overwrite the User Plane IP Resource Information previously received from the UP function.

## 6.2.8 Sx Association Release Procedure

### 6.2.8.1 General

The Sx Association Release procedure shall be used to terminate the Sx association between the CP Function and the UP Function due to e.g. OAM reasons. The Sx Association Release Request may be initiated by the CP function.

### 6.2.8.2 CP Function Behaviour

If the CP function initiates the Sx Association Release procedure to release an existing Sx association, the CP function:

- shall delete locally all the Sx sessions related to that Sx association when receiving the Sx Association Release Response with the cause value success.

### 6.2.8.3 UP Function behaviour

When the UP function receives an Sx Association Release Request, the UP function:

- shall delete all the Sx sessions related to that Sx association locally;
- shall delete the Sx association and any related information (e.g. Node ID of the CP function);
- shall send an Sx Association Deletion Response with a successful cause.

NOTE: The UP function always accepts an Sx Association Release Request.

## 6.2.9 Sx Node Report Procedure

### 6.2.9.1 General

The Sx Node Report procedure shall be used by the UP function to report information to the CP function which is not related to a specific Sx session, e.g. to report a user plane path failure affecting all the Sx sessions towards a remote GTP-U peer.

### 6.2.9.2 UP Function Behaviour

The UP function shall initiate the Sx Node Report procedure to report information to the CP function. The UP function:

- shall send the Sx Node Report Request message, including the information to be reported.

When the UP function receives an Sx Node Report Response with the cause success, the UP function shall consider the information successfully delivered to the CP function.

### 6.2.9.3 CP Function behaviour

When the CP function receives an Sx Node Report Request message, it shall:

- process the information being reported as appropriate and send an Sx Node Report Response with the cause "success";
- otherwise return an appropriate error cause value.

# 6.3 Sx Session Related Procedures

## 6.3.1 General

The following subclauses describe the session related procedures over the Sxa, Sxb and Sxc reference points. The behaviour of the CP function and UP function when sending and receiving session related messages is described.

## 6.3.2 Sx Session Establishment Procedure

### 6.3.2.1 General

The Sx Session Establishment procedure shall be used to setup an Sx session between CP function and UP function and configure Rules in the UP function so that the UP function can handle incoming packets.

### 6.3.2.2 CP Function Behaviour

The CP function initiates the Sx Session Establishment procedure to create a Sx session for a PDN connection, or IP-CAN session or TDF session or for applying a certain IP packets treatment which is not associated with any PDN connection or TDF session.

The CP function:

- shall send the Sx Session Establishment Request message with a new Sx F-SEID together with Rules to be created;
- may assign a local F-TEID for the access side and/or core side and provide it in the PDI, if F-TEID allocation is performed in the CP function.

When the CP function receives an Sx Session Establishment Response with cause success, the CP function shall continue with the procedure which triggered the Sx Session Establishment procedure.

### 6.3.2.3 UP Function Behaviour

When the UP function receives an Sx Session Establishment Request message it shall:

- store and apply the rules received in the request and send an Sx Session Establishment Response with cause "success", if all rules in the Sx Session Establishment Request are stored and applied;
- Otherwise, if at least one rule failed to be stored or applied, return an appropriate error cause value with the Rule ID of the Rule causing the first error, discard all the received rules and not create any Sx session context.

## 6.3.3 Sx Session Modification Procedure

### 6.3.3.1 General

The Sx Session Modification procedure shall be used to modify an existing Sx session, e.g. to configure a new rule, to modify an existing rule, to delete an existing rule.

### 6.3.3.2 CP Function behaviour

The CP function initiates the Sx Session Modification procedure to modify an existing Sx session, e.g. triggered by an modification of PDN connection, IP CAN session or TDF session.

The CP function shall:

- include a complete PDI if the PDI in the existing PDR is to be updated;
- remove locally the reference to a rule in the PDRs when the related Rule is deleted;

- provide all the new, updated or deleted Rules. The Updated Rules shall contain only the information which are changed, added and/or deleted.

When the CP function receives an Sx Session Modification Response with the cause "success" it shall continue with the procedure which has initiated the Sx Session Modification procedure.

#### 6.3.3.3 UP Function Behaviour

When the UP function receives a Sx Session Modification Request it shall:

- send the Sx Session Modification Response message with a rejection cause value set to "Session context not found" if the F-SEID included in the Sx Session Modification Request message is unknown;

- discard any updates on the Sx session context included in the Sx Session Modification Request message if the request is rejected and send an Sx Session Modification Response with an appropriate error cause together with additional information e.g. indicating the first Rule ID of the Rule causing the error. In this case, the UP function shall continue with the existing Sx session context for the Sx session as if the Sx Session Modification Request had not been received;

- remove all rules identified by a Rule ID to be removed and remove the Rule ID from the PDR(s) from where they are referenced;

- send the Sx Session Modification Response with an acceptance cause value if all the requested modifications are accepted and performed successfully.

### 6.3.4 Sx Session Deletion Procedure

#### 6.3.4.1 General

The Sx Session Deletion procedure shall be used to delete an existing Sx session between the CP function and the UP function.

#### 6.3.4.2 CP Function Behaviour

The CP function initiates an Sx Session Deletion procedure towards the UP function to delete an existing Sx session e.g. when the corresponding PDN is deleted.

The CP shall:

- send an Sx Session Deletion Request with the F-SEID identifying the Sx session.

When the CP function receives Sx Session Deletion Response with cause success, the CP function shall continue with the procedure which triggers the Sx Session Deletion procedure.

#### 6.3.4.3 UP Function Behaviour

When the UP function receives a Sx Session Deletion Request it shall:

- send the Sx Session Deletion Response message with a rejection cause set to "Session context not found" if the F-SEID include in the Sx Session Deletion Request message is unknown;

- send the Sx Session Deletion Response message with an acceptance cause if the Sx session and associated rules are deleted successfully, and include any pending Usage Report(s) in the message.

### 6.3.5 Sx Session Report Procedure

#### 6.3.5.1 General

The Sx Session Report procedure shall be used by the UP function to report information related to the Sx session to the CP function.

#### 6.3.5.2 UP Function Behaviour

The UP function shall initiate the Sx Session Report procedure to report information related to an Sx session to the CP function. The UP function:

- shall send the Sx Session Report Request message, identifying the Sx session for which the report is sent and including the information to be reported.

When the UP function receives an Sx Session Report Response with the cause success, the UP function shall consider the information to be successfully delivered to the CP function.

#### 6.3.5.3 CP Function Behaviour

When the CP function receives an Sx Session Report Request message, it shall:

- send the Sx Session Report Response message with a rejection cause set to "Session context not found" if the F-SEID included in the Sx Session Report Request message is unknown;

- process the information being reported as appropriate and send an Sx Session Report Response with the cause "success";

- otherwise return an appropriate error cause value.

## 6.4 Reliable Delivery of PFCP Messages

Reliable delivery of PFCP messages is accomplished by retransmission of these messages as specified in this subclause.

A PFCP entity shall maintain, for each triplet of local IP address, local UDP port and remote peer's IP address, a sending queue with Request messages to be sent to that peer. Each message shall be sent with a Sequence Number and be held until a corresponding Response is received or until the PFCP entity ceases retransmission of that message. The Sequence Number shall be unique for each outstanding Request message sourced from the same IP/UDP endpoint. A PFCP entity may have several outstanding Requests waiting for replies.

When sending a Request message, the sending PFCP entity shall start a timer T1. The sending entity shall consider that the Request message has been lost if a corresponding Response message has not been received before the T1 timer expires. If so, the sending entity shall retransmit the Request message, if the total number of retry attempts is less than N1 times. The setting of the T1 timer and N1 counter is implementation specific.

A retransmitted PFCP message shall have the same message content, including the same PFCP header, UDP ports, source and destination IP addresses as the originally transmitted message.

A Request and its Response message shall have the same Sequence Number value, i.e. the Sequence Number in the PFCP header of the Response message shall be copied from the respective Request message. A Request and its Response messages are matched based on the Sequence Number and the IP address and UDP port.

Not counting retransmissions, a Request message shall be answered with a single Response message. Duplicated Response messages shall be discarded by the receiver. A received Response message not matching an outstanding Request message waiting for a reply should be discarded.

The PFCP entity should inform the upper layer when detecting an unsuccessful transfer of a Request message to enable the controlling upper entity to take any appropriate measure.

# 7 Messages and Message Formats

## 7.1 Transmission Order and Bit Definitions

PFCP messages shall be transmitted in network octet order starting with octet 1 with the most significant bit sent first.

The most significant bit of an octet in a PFCP message is bit 8. If a field in a PFCP message spans over several octets, the most significant bit is bit 8 of the octet with the lowest number, unless specified otherwise.

# 7.2 Message Format

## 7.2.1 General

The format of a PFCP message is depicted in Figure 7.2.1-1.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to m | PFCP message header | | | | | | | |
| m+1 to n | Zero or more Information Element(s) | | | | | | | |

**Figure 7.2.1-1: PFCP Message Format**

A PFCP message shall contain the PFCP message header and may contain subsequent information element(s) dependent on the type of message.

## 7.2.2 Message Header

### 7.2.2.1 General Format

PFCP messages use a variable length header. The message header length shall be a multiple of 4 octets. Figure 7.2.2.1-1 illustrates the format of the PFCP Header.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 1 | Version | | | Spare | Spare | Spare | MP | S |
| 2 | Message Type | | | | | | | |
| 3 | Message Length (1st Octet) | | | | | | | |
| 4 | Message Length (2nd Octet) | | | | | | | |
| m to k(m+7) | If S flag is set to 1, then SEID shall be placed into octets 5-12. Otherwise, SEID field is not present at all. | | | | | | | |
| n to (n+2) | Sequence Number | | | | | | | |
| (n+3) | Spare | | | | | | | |

**Figure 7.2.2.1-1: General format of PFCP Header**

Where:

- if S = 0, SEID field is not present, k = 0, m = 0 and n = 5;
- if S = 1, SEID field is present, k = 1, m = 5 and n = 13.

The usage of the PFCP header is defined in subclause 7.2.2.4.

Octet 1 bits shall be encoded as follows:

- Bit 1 represents the SEID flag (T).
- Bit 2 represents the "MP" flag (see subclause 7.2.2.4.1).
- Bit 3 to 5 are spare, the sender shall set them to "0" and the receiving entity shall ignore them.
- Bits 6-8 represent the Version field.

### 7.2.2.2 PFCP Header for Node Related Messages

The PFCP message header for the node related messages shall not contain the SEID field, but shall contain the Sequence Number field, followed by one spare octet as depicted in figure 7.2.2.2-1. The spare bits shall be set to zero

by the sender and ignored by the receiver. For the Version Not Supported Response message, the Sequence Number may be set to any number and shall be ignored by the receiver.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 | Version | | | Spare | Spare | Spare | MP=0 | S=0 |
| 2 | Message Type | | | | | | | |
| 3 | Message Length (1st Octet) | | | | | | | |
| 4 | Message Length (2nd Octet) | | | | | | | |
| 5 | Sequence Number (1st Octet) | | | | | | | |
| 6 | Sequence Number (2nd Octet) | | | | | | | |
| 7 | Sequence Number (3rd Octet) | | | | | | | |
| 8 | Spare | | | | | | | |

**Figure 7.2.2.2-1: PFCP Message Header for node related messages**

### 7.2.2.3 PFCP Header for Session Related Messages

For The PFCP message header, for session related messages, shall contain the SEID and Sequence Number fields followed by one spare octet. The PFCP header is depicted in figure 7.2.2.3-1. The spare bits shall be set to zero by the sender and ignored by the receiver.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 | Version | | | Spare | Spare | Spare | MP | S=1 |
| 2 | Message Type | | | | | | | |
| 3 | Message Length (1st Octet) | | | | | | | |
| 4 | Message Length (2nd Octet) | | | | | | | |
| 5 | Session Endpoint Identifier (1st Octet) | | | | | | | |
| 6 | Session Endpoint Identifier (2nd Octet) | | | | | | | |
| 7 | Session Endpoint Identifier (3rd Octet) | | | | | | | |
| 8 | Session Endpoint Identifier (4th Octet) | | | | | | | |
| 9 | Session Endpoint Identifier (5th Octet) | | | | | | | |
| 10 | Session Endpoint Identifier (6th Octet) | | | | | | | |
| 11 | Session Endpoint Identifier (7th Octet) | | | | | | | |
| 12 | Session Endpoint Identifier (8th Octet) | | | | | | | |
| 13 | Sequence Number (1st Octet) | | | | | | | |
| 14 | Sequence Number (2nd Octet) | | | | | | | |
| 15 | Sequence Number (3rd Octet) | | | | | | | |
| 16 | Message Priority | | | | Spare | | | |

**Figure 7.2.2.3-1: PFCP message Header for session related messages**

### 7.2.2.4 Usage of the PFCP Header

#### 7.2.2.4.1 General

The format of the PFCP header is specified in subclause 7.2.2.

The usage of the PFCP header shall be as defined below.

The first octet of the header shall be used is the following way:

- Bit 1 represents the "S" flag, which indicates if SEID field is present in the PFCP header or not. If the "S" flag is set to 0, then the SEID field shall not be present in the PFCP header. If the "S" flag is set to 1, then the SEID field shall immediately follow the Length field, in octets 5 to 12. Apart from the node related messages , in all Sx messages the value of the "S" flag shall be set to "1".

- Bit 2 represents the "MP" flag. If the "MP" flag is set to "1", then bits 8 to 5 of octet 16 shall indicate the message priority.
- Bit 3 is a spare bit. The sending entity shall set it to "0" and the receiving entity shall ignore it.
- Bit 4 is a spare bit. The sending entity shall set it to "0" and the receiving entity shall ignore it.
- Bit 5 is a spare bit. The sending entity shall set it to "0" and the receiving entity shall ignore it.
- Bits 6 to 8, which represent the PFCP version, shall be set to decimal 1 ("001").

The usage of the fields in octets 2 - n of the header shall be as specified below.

- Octet 2 represents the Message type field, which shall be set to the unique value for each type of control plane message. Message type values are specified in Table 7.3-1 "Message types".
- Octets 3 to 4 represent the Message Length field. This field shall indicate the length of the message in octets excluding the mandatory part of the PFCP header (the first 4 octets). The SEID (if present) and the Sequence Number shall be included in the length count. The format of the Length field of information elements is specified in subclause 8.2 "Information Element Format".
- When S=1, Octets 5 to 12 represent the Session Endpoint Identifier (SEID) field. This field shall unambiguously identify a session endpoint in the receiving Packet Forward Control entity. The Session Endpoint Identifier is set by the sending entity in the PFCP header of all control plane messages to the SEID value provided by the corresponding receiving entity (CP or UP function). If a peer's SEID is not available the SEID field shall be present in a PFCP header, but its value shall be set to "0", "Conditions for sending SEID=0 in PFCP header".

NOTE: The SEID in the PFCP header of a message is set to the SEID value provided by the corresponding receiving entity regardless of whether the source IP address of the request message and the IP Destination Address provided by the receiving entity for subsequent request messages are the same or not.

- Octets 13 to 15 represent PFCP Sequence Number field.

#### 7.2.2.4.2 Conditions for Sending SEID=0 in PFCP Header

If a peer's SEID is not available, the SEID field shall still be present in the header and its value shall be set to "0" in the following messages:

- Sx Session Establishment Request message on Sxa/Sxb/Sxc;
- If a node receives a message for which it has no session, i.e. if SEID in the PFCP header is not known, it shall respond with "Session context not found" cause in the corresponding response message to the sender, the SEID used in the PFCP header in the response message shall be then set to "0";
- If a node receives a request message containing protocol error, e.g. Mandatory IE missing, which requires the receiver to reject the message as specified in clause 7.6, it shall reject the request message. For the response message, the node should look up the remote peer’s SEID and accordingly set SEID in the PFCP header and the message cause code. As an implementation option, the node may not look up the remote peer’s SEID and set the PFCP header SEID to "0" in the response message. However in this case, the cause value shall not be set to "Session not found".

## 7.2.3 Information Elements

### 7.2.3.1 General

The format of PFCP Information Elements are defined in subclause 8.2.

### 7.2.3.2 Presence Requirements of Information Elements

IEs within PFCP messages shall be specified with one of the following presence requirement:

- Mandatory: this means that the IE shall be included by the sending entity, and that the receiver diagnoses a "Mandatory IE missing" error when detecting that the IE is not present. A response including a "Mandatory IE missing" cause, shall include the type of the missing IE.

- Conditional: this means that:

  - the IE shall be included by sending entity if the conditions specified are met;

  - the receiver shall check the conditions as specified in the corresponding message type description, based on the parameter combination in the message and/or on the state of the receiving node, to infer if a conditional IE shall be expected. Only if a receiver has sufficient information, if a conditional IE, which is necessary for the receiving entity to complete the procedure, is missing, then the receiver shall abort the procedure.

- Conditional-Optional: this means that:

  - the IE shall be included by a sending entity complying with the version of the specification, if the conditions specified in the relevant protocol specification are met. An entity, which is at an earlier version of the protocol and therefore is not up-to-date, cannot send this IE;

  - the receiver need not check the presence of the IE in the message. If the receiver checks the presence of the Conditional-Optional IE, then the IE's absence shall not trigger any of the error handling procedures. The handling of an absence or erroneous such IEs shall be treated as Optional IEs as specified in subclause 7.6.

- Optional: this means that:

  - the IE shall be included as a service option. Therefore, the IE may be included or not in a message. The handling of an absent optional IE, or an erroneous optional IE is specified in subclause 7.6.

For conditional IEs, the clause describing the PFCP message explicitly defines the conditions under which the inclusion of each IE becomes mandatory or optional for that particular message. These conditions shall be defined so that the presence of a conditional IE only becomes mandatory if it is critical for the receiving entity. The definition might reference other protocol specifications for final terms used as part of the condition.

For grouped IEs, the presence requirement of the embedded IE shall follow the rules:

- If the grouped IE is Mandatory within a given message: the presence requirements of individual embedded IEs are as stated within the Mandatory grouped IE for the given message;

- if the grouped IE is Conditional within a given message: if the embedded IE in the grouped IE is Mandatory or Conditional, this embedded IE is viewed as Conditional IE by the receiver. If the embedded IE in the grouped IE is Conditional-Optional, this embedded IE is viewed as Optional IE by the receiver. If the embedded IE in the grouped IE is Optional, this embedded IE is viewed as Optional IE by the receiver;

- if the grouped IE is Conditional-Optional within a given message: if the embedded IE in the grouped IE is Mandatory or Conditional, this embedded IE is viewed as Conditional-Optional IE by the receiver. If the embedded IE in the grouped IE is Conditional-Optional, this embedded IE is viewed as Optional IE by the receiver. If the embedded IE in the grouped IE is Optional, this embedded IE is viewed as Optional IE by the receiver;

- if the grouped IE is Optional within a given message: all embedded IEs in the grouped IE are viewed as Optional IEs by the receiver.

In all of the above cases, appropriate error handling as described in subclause 7.6 shall be applied for protocol errors of the embedded IEs.

Only the Cause IE at message level shall be included in the response if the Cause contains a value that indicates that the request is not accepted, regardless of whether there are other mandatory or conditional IEs defined for a given response message. The following are exceptions:

- the Node ID and Offending IE shall be included as per the requirements specified for the corresponding response message;

- the Load Control Information, Overload Control Information and the Failed Rule ID IEs may be included in an Sx session related message.

If the Cause IE at Grouped IE level contains a value that indicates that the Grouped IE is not handled correctly, the other IEs in this Grouped IE, other than the Cause IE, may not be included.

#### 7.2.3.3 Grouped Information Elements

A Grouped IE is an IE which may contain other IEs.

Grouped IEs have a length value in the TLV encoding, which includes the added length of all the embedded IEs. Overall coding of a grouped IE with 4 octets long IE header is defined in subclause 8.2. Each IE within a grouped IE also shall also contain 4 octets long IE header.

Grouped IEs are not marked by any flag or limited to a specific range of IE type values. The clause describing an IE in this specification shall explicitly state if it is a Grouped IE.

NOTE: Each entry into each Grouped IE creates a new scope level. Exit from the grouped IE closes the scope level. The PFCP message level is the top most scope.

If more than one grouped IEs of the same type, but for a different purpose are sent with a message, these IEs shall have different IE types.

If more than one grouped IEs of the same type and for the same purpose are sent with a message, these IEs shall have exactly the same IE type to represent a list.

#### 7.2.3.4 Information Element Type

An IE in a PFCP message or Grouped IE is identified by its IE Type and described by a specific row in the corresponding tables in clause 7.

If several IEs with the same Type are included in a PFCP message or Grouped IE, they represent a list for the corresponding IE name.

An IE Type value uniquely identifies a specific IE.

One IE type value is specified for Vendor Specific IEs.

## 7.3 Message Types

The PFCP message types to be used over the Sxa, Sxb and Sxc reference points are defined in Table 7.3-1.

**Table 7.3-1: Message Types**

| Message Type value (Decimal) | Message | Applicability | | |
|---|---|---|---|---|
| | | Sxa | Sxb | Sxc |
| 0 | Reserved | | | |
| | **Sx Node related messages** | | | |
| 1 | Sx Heartbeat Request | X | X | X |
| 2 | Sx Heartbeat Response | X | X | X |
| 3 | Sx PFD Management Request | - | X | X |
| 4 | Sx PFD Management Response | - | X | X |
| 5 | Sx Association Setup Request | X | X | X |
| 6 | Sx Association Setup Response | X | X | X |
| 7 | Sx Association Update Request | X | X | X |
| 8 | Sx Association Update Response | X | X | X |
| 9 | Sx Association Release Request | X | X | X |
| 10 | Sx Association Release Response | X | X | X |
| 11 | Sx Version Not Supported Response | X | X | X |
| 12 | Sx Node Report Request | X | X | X |
| 13 | Sx Node Report Response | X | X | X |
| 14 | Sx Session Set Deletion Request | X | X | - |
| 15 | Sx Session Set Deletion Response | X | X | - |
| 16 to 49 | For future use | | | |
| | **Sx Session related messages** | | | |
| 50 | Sx Session Establishment Request | X | X | X |
| 51 | Sx Session Establishment Response | X | X | X |
| 52 | Sx Session Modification Request | X | X | X |
| 53 | Sx Session Modification Response | X | X | X |
| 54 | Sx Session Deletion Request | X | X | X |
| 55 | Sx Session Deletion Response | X | X | X |
| 56 | Sx Session Report Request | X | X | X |
| 57 | Sx Session Report Response | X | X | X |
| 58 to 99 | For future use | | | |
| | **Other messages** | | | |
| 100 to 255 | For future use | | | |

# 7.4 Sx Node Related Messages

## 7.4.1 General

This subclause specifies the node related messages used over the Sxa, Sxb and Sxc reference points.

## 7.4.2 Heartbeat Messages

### 7.4.2.1 Heartbeat Request

**Table 7.4.2.1-1: Information Elements in Heartbeat Request**

| Information elements | P | Condition / Comment | IE Type |
|---|---|---|---|
| Recovery Time Stamp | M | This IE shall contain the time stamp when the node was started see clause 19A of 3GPP TS 23.007 [24]. | Recovery Time Stamp |

### 7.4.2.2 Heartbeat Response

**Table 7.4.2.2-1: Information Elements in Heartbeat Response**

| Information elements | P | Condition / Comment | IE Type |
|---|---|---|---|
| Recovery Time Stamp | M | This IE shall contain the time stamp when the node was started see clause 19A of 3GPP TS 23.007 [24]. | Recovery Time Stamp |

## 7.4.3 Sx PFD Management

### 7.4.3.1 Sx PFD Management Request

**Table 7.4.3.1-1: Information Elements in Sx PFD Management Request**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| Application ID's PFDs | C | This IE shall contain an Application Identifier and the associated PFDs to be provisioned in the UP function. Several IEs with the same IE type may be present to provision PFDs for multiple Application IDs. The UP function shall delete all the PFDs received and stored earlier for all the Application IDs if this IE is absent in the message. | - | X | X | Application ID's PFDs |

**Table 7.4.3.1-2: Application ID's PFDs**

| Octet 1 and 2 | Application ID's PFDs IE Type = 58 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| Application ID | M | This IE shall identify the Application ID for which PFDs shall be provisioned in the UP function. | - | X | X | Application ID |
| PFD | C | This IE shall be present if the PFD needs to be provisioned in the UP function. When present, it shall describe the PFD to be provisioned in the UP function. Several IEs with the same IE type may be present to provision multiple PFDs for this Application ID.<br><br>When this IE is absent, the UP function shall delete all the PFDs received and stored earlier in the UP function for this Application ID. | - | X | X | PFD |

**Table 7.4.3.1-3: PFD**

| Octet 1 and 2 | PFD IE Type = 59 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| PFD Contents | M | This IE shall describe the PFD to be provisioned in the UP function. Several IEs with the same IE type may be present to provision multiple contents for this PFD. | - | X | X | PFD Contents |

### 7.4.3.2 Sx PFD Management Response

**Table 7.4.3.2-1: Information Elements in Sx PFD Management Response**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | - | X | X | Cause |
| Offending IE | C | This IE shall be included if the rejection is due to an conditional or mandatory IE missing or faulty. | - | X | X | Offending IE |

## 7.4.4 Sx Association messages

### 7.4.4.1 Sx Association Setup Request

**Table 7.4.4.1-1: Information Elements in a Sx Association Setup Request**

| Information elements | P | Condition / Comment | IE Type |
|---|---|---|---|
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | Node ID |
| Recovery Time Stamp | M | This IE shall contain the time stamp when the node was started, see clause 19A of 3GPP TS 23.007 [24]. | Recovery Time Stamp |
| UP Function Features | C | This IE shall be present if the UP function sends this message and the UP function supports at least one UP feature defined in this IE.<br>When present, this IE shall indicate the features the UP function supports. | UP Function Features |
| CP Function Features | C | This IE shall be present if the CP function sends this message and the CP function supports at least one CP feature defined in this IE.<br>When present, this IE shall indicate the features the CP function supports. | CP Function Features |
| User Plane IP Resource Information | O | This IE may be present if the UP function sends this message.<br><br>When present, this IE shall contain an IPv4 and/or an IPv6 address, together with a TEID range that the CP function shall use to allocate GTP-U F-TEID in the UP function.<br>Several IEs with the same IE type may be present to represent multiple User Plane IP Resources. | User Plane IP Resource Information |

### 7.4.4.2 Sx Association Setup Response

**Table 7.4.4.2-1: Information Elements in a Sx Association Setup Response**

| Information elements | P | Condition / Comment | IE Type |
|---|---|---|---|
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | Node ID |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | Cause |
| Recovery Time Stamp | M | This IE shall contain the time stamp when the node was started, see clause 19A of 3GPP TS 23.007 [24]. | Recovery Time Stamp |
| UP Function Features | C | This IE shall be present if the UP function sends this message and the UP function supports at least one UP feature defined in this IE.<br>When present, this IE shall indicate the features the UP function supports. | UP Function Features |
| CP Function Features | C | This IE shall be present if the CP function sends this message and the CP function supports at least one CP feature defined in this IE.<br>When present, this IE indicates the features the CP function supports. | CP Function Features |
| User Plane IP Resource Information | O | This IE may be present if the UP function sends this message.<br><br>When present, this IE shall contain an IPv4 and/or an IPv6 address, together with a TEID range that the CP function shall use to allocate GTP-U F-TEID in the UP function.<br>Several IEs with the same IE type may be present to represent multiple User Plane IP Resources. | User Plane IP Resource Information |

### 7.4.4.3 Sx Association Update Request

**Table 7.4.4.3-1: Information Elements in a Sx Association Update Request**

| Information elements | P | Condition / Comment | IE Type |
|---|---|---|---|
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | Node ID |
| UP Function Features | O | If present, this IE shall indicate the supported Features when the sending node is the UP function. | UP Function Features |
| CP Function Features | O | If present, this IE shall indicate the supported Features when the sending node is the CP function. | CP Function Features |
| Sx Association Release Request | C | This IE shall be present if the UP function requests the CP function to release the Sx association. | Sx Association Release Request |
| Graceful Release Period | C | This IE shall be present if the UP function requests a graceful release of the Sx association. | Graceful Release Period |
| User Plane IP Resource Information | O | This IE may be present if the UP function sends this message.<br><br>When present, this IE shall contain an IPv4 and/or an IPv6 address, together with a TEID range that the CP function shall use to allocate GTP-U F-TEID in the UP function.<br><br>Several IEs with the same IE type may be present to represent multiple User Plane IP Resources. | User Plane IP Resource Information |

### 7.4.4.4 Sx Association Update Response

**Table 7.4.4.4-1: Information Elements in a Sx Association Update Response**

| Information elements | P | Condition / Comment | IE-Type |
|---|---|---|---|
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | Node ID |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | Cause |
| UP Function Features | O | If present, this IE shall indicate the supported Features when the sending node is the UP function. | UP Function Features |
| CP Function Features | O | If present, this IE shall indicate the supported Features when the sending node is the CP function. | CP Function Features |

### 7.4.4.5 Sx Association Release Request

**Table 7.4.4.5-1: Information Elements in a Sx Association Release Request**

| Information elements | P | Condition / Comment | IE Type |
|---|---|---|---|
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | Node ID |

#### 7.4.4.6 Sx Association Release Response

**Table 7.4.4.6-1: Information Elements in a Sx Association Release Response**

| Information elements | P | Condition / Comment | IE type |
|---|---|---|---|
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | Node ID |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | Cause |

#### 7.4.4.7 Sx Version Not Supported Response

This message shall only contain the PFCP header. The PFCP protocol version in the PFCP header shall indicate the highest PFCP Version that the sending entity supports.

NOTE: The Sx Version Not Supported Response message can be received by a PFCP entity when sending the very first message to a PFCP peer only supporting earlier version(s) of the protocol.

### 7.4.5 Sx Node Report Procedure

#### 7.4.5.1 Sx Node Report Request

##### 7.4.5.1.1 General

The Sx Node Report Request shall be sent over the Sxa, Sxb and Sxc interface by the UP function to report information to the CP function that is not specific to an Sx session.

**Table 7.4.5.1.1-1: Information Elements in Sx Node Report Request**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | Node ID |
| Node Report Type | M | This IE shall indicate the type of the report. | X | X | X | Node Report Type |
| User Plane Path Failure Report | C | This IE shall be present if the Node Report Type indicates a User Plane Path Failure Report. | X | X | - | User Plane Path Failure Report |

##### 7.4.5.1.2 User Plane Path Failure Report IE within Sx Node Report Request

**Table 7.4.5.1.2-1: User Plane Path Failure IE within Sx Node Report Request**

| Octet 1 and 2 | User Plane Path Failure IE Type = 102 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| Remote GTP-U Peer | M | This IE shall include the IP address of the remote GTP-U peer towards which a user plane path failure has been detected.<br>More than one IE with this type may be included to represent multiple remote GTP-U peers towards which a user plane path failure has been detected. | X | X | - | Remote GTP-U Peer |

### 7.4.5.2 Sx Node Report Response

#### 7.4.5.2.1 General

The Sx Node Report Response shall be sent over the Sxa, Sxb and Sxc interface by the CP function to the UP function as a reply to the Sx Node Report Request.

**Table 7.4.5.2.1-1: Information Elements in Sx Node Report Response**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | Node ID |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | X | Cause |
| Offending IE | C | This IE shall be included if the rejection cause is due to a conditional or mandatory IE missing or faulty. | X | X | X | Offending IE |

## 7.4.6 Sx Session Set Deletion

### 7.4.6.1 Sx Session Set Deletion Request

The Sx Session Set Deletion Request shall be sent over the Sxa and Sxb interface by the CP function to request the UP function to delete the Sx sessions affected by a partial failure.

The Sx Session Set Deletion Request shall be also sent over the Sxa and Sxb interface by the UP function to request the CP function to delete the Sx sessions affected by a partial failure.

**Table 7.4.6.1-1: Information Elements in a Sx Session Set Deletion Request**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| Node ID | M | This IE shall contain the node identity of the originating node of the message. | X | X | - | Node ID |
| SGW-C FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - | FQ-CSID |
| PGW-C FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - | FQ-CSID |
| SGW-U FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | - | - | FQ-CSID |
| PGW-U FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - | FQ-CSID |
| TWAN FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - | FQ-CSID |
| ePDG FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - | FQ-CSID |
| MME FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - | FQ-CSID |

### 7.4.6.2 Sx Session Set Deletion Response

The Sx Session Set Deletion Response shall be sent over the Sxa and Sxb interface by the UP function or the CP function as a reply to the Sx Session Set Deletion Request.

**Table 7.4.6.2-1: Information Elements in a Sx Session Set Deletion Response**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| Node ID | M | This IE shall contain the unique identifier of the sending node. | X | X | - | Node ID |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | - | Cause |
| Offending IE | C | This IE shall be included if the rejection is due to an conditional or mandatory IE missing or faulty. | X | X | - | Offending IE |

# 7.5 Sx Session Related Messages

## 7.5.1 General

This subclause specifies the session related messages used over the Sxa, Sxb and Sxc reference points.

## 7.5.2 Sx Session Establishment Request

### 7.5.2.1 General

The Sx Session Establishment Request shall be sent over the Sxa, Sxb and Sxc interface by the CP function to establish a new Sx session context in the UP function.

**Table 7.5.2.1-1: Information Elements in an Sx Session Establishment Request**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | Node ID |
| CP F-SEID | M | This IE shall contain the unique identifier allocated by the CP function identifying the session. | X | X | X | F-SEID |
| Create PDR | M | This IE shall include one or more PDRs to be associated to the Sx session.<br>See Table 7.5.2.2-1. | X | X | X | Create PDR |
| Create FAR | M | This IE shall include one or more FARs to be associated to the Sx session.<br>See Table 7.5.2.3-1. | X | X | X | Create FAR |
| Create URR | C | This IE shall be present if a measurement action shall be applied to packets matching one or more PDR(s) of this Sx session.<br>Several IEs within the same IE type may be present to represent multiple URRs.<br>See Table 7.5.2.4-1. | X | X | X | Create URR |
| Create QER | C | This IE shall be present if a QoS enforcement action shall be applied to packets matching one or more PDR(s) of this Sx session.<br>Several IEs within the same IE type may be present to represent multiple QERs.<br>See Table 7.5.2.5-1. | - | X | X | Create QER |
| Create BAR | O | When present, this IE shall contain the buffering instructions to be applied by the UP function to any FAR of this Sx session set with the Apply Action requesting the packets to be buffered and with a BAR ID IE referring to this BAR. See table 7.5.2.6-1. | X | - | - | Create BAR |
| PDN Type | C | This IE shall be present if the Sx session is setup for an individual PDN connection (see subclause 5.2.1).<br>When present, this IE shall indicate whether this is an IP or non-IP PDN connection. | X | X | - | PDN Type |
| SGW-C FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - | FQ-CSID |
| MME FQ-CSID | C | This IE shall be included when received on the S11 interface or on S5/S8 interface according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - | FQ-CSID |
| PGW-C FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - | FQ-CSID |
| ePDG FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - | FQ-CSID |
| TWAN FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - | FQ-CSID |

### 7.5.2.2 Create PDR IE within Sx Session Establishment Request

The Create PDR grouped IE shall be encoded as shown in Figure 7.5.2.2-1.

**Table 7.5.2.2-1: Create PDR IE within Sx Session Establishment Request**

| Octet 1 and 2 | Create PDR IE Type = 1(decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| PDR ID | M | This IE shall uniquely identify the PDR among all the PDRs configured for that Sx session. | X | X | X | PDR ID |
| Precedence | M | This IE shall indicate the PDR's precedence to be applied by the UP function among all PDRs of the Sx session, when looking for a PDR matching an incoming packet. | - | X | X | Precedence |
| PDI | M | This IE shall contain the PDI against which incoming packets will be matched.<br>See Table 7.5.2.2-2. | X | X | X | PDI |
| Outer Header Removal | C | This IE shall be present if the UP function is required to remove one or more outer header(s) from the packets matching this PDR. | X | X | - | Outer Header Removal |
| FAR ID | C | This IE shall be present if the Activate Predefined Rules IE is not included or if it is included but it does not result in activating a predefined FAR.<br>When present this IE shall contain the FAR ID to be associated to the PDR. | X | X | X | FAR ID |
| URR ID | C | This IE shall be present if a measurement action shall be applied to packets matching this PDR.<br>When present, this IE shall contain the URR IDs to be associated to the PDR.<br>Several IEs within the same IE type may be present to represent a list of URRs to be associated to the PDR. | X | X | X | URR ID |
| QER ID | C | This IE shall be present if a QoS enforcement action shall be applied to packets matching this PDR.<br>When present, this IE shall contain the QER IDs to be associated to the PDR. Several IEs within the same IE type may be present to represent a list of QERs to be associated to the PDR. | - | X | X | QER ID |
| Activate Predefined Rules | C | This IE shall be present if Predefined Rule(s) shall be activated for this PDR. | - | X | X | Activate Predefined Rules |

**Table 7.5.2.2-2: PDI IE within Sx Session Establishment Request**

| Octet 1 and 2 | PDI IE Type = 2 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| Source Interface | M | This IE shall identify the source interface of the incoming packet. | X | X | X | Source Interface |
| Local F-TEID | O | If present, this IE shall identify the local F-TEID to match for an incoming packet.<br>The CP function shall set the CHOOSE (CH) bit to 1 if the UP function supports the allocation of F-TEID and the CP function requests the UP function to assign a local F-TEID to the PDR. | X | X | - | F-TEID |
| Network Instance | O | If present, this IE shall identify the Network instance to match for the incoming packet. See NOTE 1. | X | X | X | Network Instance |
| UE IP address | O | If present, this IE shall identify the source or destination IP address to match for the incoming packet. | - | X | X | UE IP address |
| SDF Filter | O | If present, this IE shall identify the SDF filter to match for the incoming packet. | - | X | X | SDF Filter |
| Application ID | O | If present, this IE shall identify the Application ID to match for the incoming packet. | - | X | X | Application ID |
| NOTE 1: The Network Instance parameter is needed e.g. in the following cases:<br>- PGW/TDF UP function supports multiple PDNs with overlapping IP addresses;<br>- SGW UP function is connected to PGWs in different IP domains (S5/S8);<br>- SGW UP function is connected to eNodeBs in different IP domains. | | | | | | |

## 7.5.2.3 Create FAR IE within Sx Session Establishment Request

The Create FAR grouped IE shall be encoded as shown in Figure 7.5.2.3-1.

**Table 7.5.2.3-1: Create FAR IE within Sx Session Establishment Request**

| Octet 1 and 2 | Create FAR IE Type = 3 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| FAR ID | M | This IE shall uniquely identify the FAR among all the FARs configured for that Sx session. | X | X | X | FAR ID |
| Apply Action | M | This IE shall indicate the action to apply to the packets, See subclauses 5.2.1 and 5.2.3. | X | X | X | Apply Action |
| Forwarding Parameters | C | This IE shall be present when the Apply-Action requests the packets to be forwarded. It may be present otherwise.<br><br>When present, this IE shall contain the forwarding instructions to be applied by the UP function when the Apply-Action requests the packets to be forwarded.<br>See table 7.5.2.3-2. | X | X | X | Forwarding Parameters |
| Duplicating Parameters | C | This IE shall be present when the Apply-Action requests the packets to be duplicated. It may be present otherwise.<br><br>When present, this IE shall contain the forwarding instructions to be applied by the UP function for the traffic to be duplicated, when the Apply-Action requests the packets to be duplicated.<br>See table 7.5.2.3-3. | X | X | - | Duplicating Parameters |
| BAR ID | O | When present, this IE shall contain the BAR ID of the BAR defining the buffering instructions to be applied by the UP function when the Apply Action requests the packets to be buffered. See table 7.5.2.6-1. | X | - | - | BAR ID |

**Table 7.5.2.3-2: Forwarding Parameters IE in FAR**

| Octet 1 and 2 | Forwarding Parameters IE Type = 4 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| Destination Interface | M | This IE shall identify the destination interface of the outgoing packet. | X | X | X | Destination Interface |
| Network Instance | O | When present, this IE shall identify the Network instance towards which to send the outgoing packet. See NOTE 1. | X | X | X | Network Instance |
| Redirect Information | C | This IE shall be present if the UP function is required to enforce traffic redirection towards a redirect destination provided by the CP function. | - | X | X | Redirect Information |
| Outer Header Creation | C | This IE shall be present if the UP function is required to add one or more outer header(s) to the outgoing packet. If present, it shall contain the F-TEID of the remote GTP-U peer when adding a GTP-U/UDP/IP header, or the Destination IP address and Port Number when adding a UDP/IP header. | X | X | - | Outer Header Creation |
| Transport Level Marking | C | This IE shall be present if the UP function is required to mark the IP header with the DSCP marking as defined by IETF RFC 2474 [22]. When present, it shall contain the value of the DSCP in the TOS/Traffic Class field set based on the QCI, and optionally the ARP priority level, of the associated EPS bearer, as described in sub-clause 4.7.3 of 3GPP TS 23.214 [2]. | X | X | - | Transport Level Marking |
| Forwarding Policy | C | This IE shall be present if a specific forwarding policy is required to be applied to the packets. It shall be present if the Destination Interface IE is set to SGi-LAN. It may be present if the Destination Interface is set to Core. When present, it shall contain an Identifier of the Forwarding Policy locally configured in the UP function. | - | X | X | Forwarding Policy |
| Header Enrichment | O | This IE may be present if the UP function indicated support of Header Enrichment of UL traffic. When present, it shall contain information for header enrichment. | - | X | X | Header Enrichment |
| NOTE 1: The Network Instance parameter is needed e.g. in the following cases:<br>- PGW/TDF UP function supports multiple PDNs with overlapping IP addresses;<br>- SGW UP function is connected to PGWs in different IP domains (S5/S8);<br>- SGW UP function is connected to eNodeBs in different IP domains. | | | | | | |

**Table 7.5.2.3-3: Duplicating Parameters IE in FAR**

| Octet 1 and 2 | Duplicating Parameters IE Type = 5 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| Destination Interface | M | This IE shall identify the destination interface of the outgoing packet. | X | X | - | Destination Interface |
| Outer Header Creation | C | This IE shall be present if the UP function is required to add one or more outer header(s) to the outgoing packet. If present, it shall contain the F-TEID of the remote GTP-U peer. | X | X | - | Outer Header Creation |
| Transport Level marking | C | This IE shall be present if the UP function is required to mark the IP header with the DSCP marking as defined by IETF RFC 2474 [22]. When present, it shall contain the value of the DSCP in the TOS/Traffic Class field. | X | X | - | Transport Level Marking |
| Forwarding Policy | C | This IE shall be present if a specific forwarding policy is required to be applied to the packets. When present, it shall contain an Identifier of the Forwarding Policy locally configured in the UP function. | X | X | - | Forwarding Policy |

#### 7.5.2.4 Create URR IE within Sx Session Establishment Request

The Create URR grouped IE shall be encoded as shown in Figure 7.5.2.4-1.

**Table 7.5.2.4-1: Create URR IE within Sx Session Establishment Request**

| Octet 1 and 2 | Create URR IE Type = 6 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| URR ID | M | This IE shall uniquely identify the URR among all the URRs configured for this Sx session. | X | X | X | URR ID |
| Measurement Method | M | This IE shall indicate the method for measuring the network resources usage, i.e. whether the data volume, duration (i.e. time), combined volume/duration, or event shall be measured. | X | X | X | Measurement Method |
| Reporting Triggers | M | This IE shall indicate the trigger(s) for reporting network resources usage to the CP function, e.g. periodic reporting or reporting upon reaching a threshold, or envelope closure. | X | X | X | Reporting Triggers |
| Measurement Period | C | This IE shall be present if periodic reporting is required. When present, it shall indicate the period for generating and reporting usage reports. | X | X | X | Measurement Period |
| Volume Threshold | C | This IE shall be present if volume-based measurement is used and reporting is required upon reaching a volume threshold. When present, it shall indicate the traffic volume value after which the UP function shall report network resources usage to the CP function for this URR. | X | X | X | Volume Threshold |
| Volume Quota | C | This IE shall be present if volume-based measurement is used and the CP function needs to provision a Volume Quota in the UP function (see subclause 5.2.2.2) When present, it shall indicate the Volume Quota value. | - | X | X | Volume Quota |
| Time Threshold | C | This IE shall be present if time-based measurement is used and reporting is required upon reaching a time threshold. When present, it shall indicate the time usage after which the UP function shall report network resources usage to the CP function for this URR. | X | X | X | Time Threshold |
| Time Quota | C | This IE shall be present if time-based measurement is used and the CP function needs to provision a Time Quota in the UP function (see subclause 5.2.2.2) When present, it shall indicate the Time Quota value | - | X | X | Time Quota |
| Quota Holding Time | C | This IE shall be present, for a time, volume or event-based measurement, if reporting is required and packets are no longer permitted to pass on when no packets are received during a given inactivity period. When present, it shall contain the duration of the inactivity period. | - | X | X | Quota Holding Time |
| Dropped DL Traffic Threshold | C | This IE shall be present if reporting is required when the DL traffic being dropped exceeds a threshold. When present, it shall contain the threshold of the DL traffic being dropped. | X | - | - | Dropped DL Traffic Threshold |
| Monitoring Time | O | When present, this IE shall contain the time at which the UP function shall re-apply the volume or time threshold. | - | X | X | Monitoring Time |
| Subsequent Volume Threshold | O | This IE may be present if the Monitoring Time IE is present and volume-based measurement is used. When present, it shall indicate the traffic volume value after which the UP function shall report network resources usage to the CP function for this URR for the period after the Monitoring Time. | - | X | X | Subsequent Volume Threshold |
| Subsequent Time Threshold | O | This IE may be present if the Monitoring Time IE is present and time-based measurement is used. When present, it shall indicate the time usage after which the UP function shall report network resources usage to the CP function for this URR for the period after the Monitoring Time. | - | X | X | Subsequent Time Threshold |
| Inactivity Detection Time | C | This IE shall be present if time-based measurement is used and the time measurement need to be suspended when no packets are received during a given inactivity period. When present, it shall contain the duration of the inactivity period. | - | X | X | Inactivity Detection Time |

| | | | | | | |
|---|---|---|---|---|---|---|
| Linked URR ID | C | This IE shall be present if linked usage reporting is required. When present, this IE shall contain the linked URR ID which is related with this URR (see subclause 5.2.2.4). | - | X | X | Linked URR ID |
| Measurement Information | C | This IE shall be included if any of the following flag is set to 1.<br>Applicable flags are:<br>- Measurement Before QoS Enforcement Flag: this flag shall be set to 1 if the traffic usage before any QoS Enforcement is requested to be measured.<br>- Inactive Measurement Flag: this flag shall be set to 1 if the measurement shall be paused (inactive). The measurement shall be performed (active) if the bit is set to 0 or if the Measurement Information IE is not present in the Create URR IE | -<br><br>- | X<br><br>X | X<br><br>- | Measurement Information |
| Time Quota Mechanism | C | This IE shall be present if time-based measurement based on CTP or DTP is used. | - | X | - | Time Quota Mechanism |

### 7.5.2.5 Create QER IE within Sx Session Establishment Request

The Create QER grouped IE shall be encoded as shown in Figure 7.5.2.5-1.

**Table 7.5.2.5-1: Create QER IE within Sx Session Establishment Request**

| Octet 1 and 2 | Create QER IE Type = 7 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| QER ID | M | This IE shall uniquely identify the QER among all the QER configured for that Sx session | - | X | X | QER ID |
| QER Correlation ID | C | This IE shall be present if the UP function is required to correlate the QERs of several Sx sessions, for APN-AMBR enforcement of multiple UE's PDN connections to the same APN. | - | X | - | QER Correlation ID |
| Gate Status | M | This IE shall indicate whether the packets are allowed to be forwarded (the gate is open) or shall be discarded (the gate is closed) in the uplink and/or downlink directions. | - | X | X | Gate Status |
| Maximum Bitrate | C | This IE shall be present if an MBR enforcement action shall be applied to packets matching this PDR. When present, this IE shall indicate the uplink and/or downlink maximum bit rate to be enforced for packets matching the PDR.<br><br>This IE may be set to the value of:<br>- the APN-AMBR, for a QER that is referenced by all the PDRs of the non-GBR bearers of a PDN connection;<br>- the TDF session MBR, for a QER that is referenced by all the PDRs of a TDF session;<br>- the bearer MBR, for a QER that is referenced by all the PDRs of a bearer;<br>- the SDF MBR, for a QER that is referenced by all the PDRs of a SDF. | - | X | X | MBR |
| Guaranteed Bitrate | C | This IE shall be present if a GBR has been authorized to packets matching this PDR. When present, this IE shall indicate the authorized uplink and/or downlink guaranteed bit rate.<br><br>This IE may be set to the value of:<br>- the aggregate GBR, for a QER that is referenced by all the PDRs of a GBR bearer;<br>- the SDF GBR, for a QER that is referenced by all the PDRs of a SDF. | - | X | X | GBR |
| Packet Rate | C | This IE shall be present if a Packet Rate enforcement action (in terms of number of packets per time interval) shall be applied to packets matching this PDR.<br>When present, this IE shall indicate the uplink and/or downlink maximum packet rate to be enforced for packets matching the PDR.<br>This IE may be set to the value of:<br>- downlink packet rate for Serving PLMN Rate Control, for a QER that is referenced by all PDRs of the UE belonging to the PDN connection using CIoT EPS Optimizations as described in 3GPP TS 23.401 [2])<br>- uplink and/or downlink packet rate for APN Rate Control, for a QER that is referenced by all the PDRs of the UE belonging to PDN connections to the same APN using CIoT EPS Optimizations as described in 3GPP TS 23.401 [2]). | - | X | - | Packet Rate |
| DL Flow Level Marking | C | This IE shall be set if the UP function is required to mark the packets for QoS purposes:<br><br>- by the TDF-C, for DL flow level marking for application indication (see subclause 5.4.5);<br>- by the PGW-C, for setting the GTP-U Service Class Indicator extension header for service indication towards GERAN (see subclause 5.4.12). | - | X | X | DL Flow Level Marking |

#### 7.5.2.6 Create BAR IE within Sx Session Establishment Request

The Create BAR grouped IE shall be encoded as shown in Figure 7.5.2.6-1.

**Table 7.5.2.6-1: Create BAR IE within Sx Session Establishment Request**

| Octet 1 and 2 | Create BAR IE Type = 85 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| BAR ID | M | This IE shall uniquely identify the BAR provisioned for that Sx session. | X | - | - | BAR ID |
| Downlink Data Notification Delay | C | This IE shall be present if the UP function indicated support of the Downlink Data Notification Delay parameter (see subclause 8.2.28) and the UP function has to delay the notification to the CP function about the arrival of DL data packets.<br>When present, it shall contain the delay the UP function shall apply between receiving a downlink data packet and notifying the CP function about it, when the Apply Action parameter requests to buffer the packets and notify the CP function. | X | - | - | Downlink Data Notification Delay |

## 7.5.3 Sx Session Establishment Response

### 7.5.3.1 General

The Sx Session Establishment Response shall be sent over the Sxa, Sxb and Sxc interface by the UP function to the CP function as a reply to the Sx Session Establishment Request.

**Table 7.5.3.1-1: Information Elements in a Sx Session Establishment Response**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | Node ID |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | X | Cause |
| Offending IE | C | This IE shall be included if the rejection is due to a conditional or mandatory IE missing or faulty. | X | X | X | Offending IE |
| UP F-SEID | M | This IE shall contain the unique identifier allocated by the UP function identifing the session. | X | X | X | F-SEID |
| Created PDR | C | This IE shall be present if the cause is set to "success" and the UP function was requested to allocate the local F-TEID for the PDR.<br>When present, this IE shall contain the PDR information associated to the Sx session. There may be several instances of this IE.<br>See table 7.5.3.2-1. | X | X | - | Created PDR |
| Load Control Information | O | The UP function may include this IE if it supports the load control feature and the feature is activated in the network.<br>See Table 7.5.3.3-1. | X | X | X | Load Control Information |
| Overload Control Information | O | During an overload condition, the UP function may include this IE if it supports the overload control feature and the feature is activated in the network.<br>See Table 7.5.3.4-1. | X | X | X | Overload Control Information |
| SGW-U FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | - | - | FQ-CSID |
| PGW-U FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - | FQ-CSID |
| Failed Rule ID | C | This IE shall be included if the Cause IE indicates a rejection due to a rule creation or modification failure. | X | X | X | Failed Rule ID |

### 7.5.3.2 Created PDR IE within Sx Session Establishment Response

The Created PDR grouped IE shall be encoded as shown in Figure 7.5.3.2-1.

**Table 7.5.3.2-1: Created PDR IE within Sx Session Establishment Response**

| Octet 1 and 2 | Created PDR IE Type = 8 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| PDR ID | M | | X | X | - | PDR ID |
| Local F-TEID | C | If the UP function allocates the F-TEID, this IE shall be present and shall contain the local F-TEID to be used for this PDR. | X | X | - | F-TEID |

### 7.5.3.3 Load Control Information IE within Sx Session Establishment Response

The Load Control Information grouped IE shall be encoded as shown in Figure 7.5.3.3-1.

**Table 7.5.3.3-1: Load Control Information IE within Sx Session Establishment Response**

| Octet 1 and 2 | Load Control Information IE Type = 50 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| Load Control Sequence Number | M | See subclause 6.2.3.3.2 for the description and use of this parameter. | X | X | X | Sequence Number |
| Load Metric | M | See subclause 6.2.3.3.2 for the description and use of this parameter. | X | X | X | Metric |

### 7.5.3.4 Overload Control Information IE within Sx Session Establishment Response

The Overload Control grouped IE shall be encoded as shown in Figure 7.5.3.4-1.

**Table 7.5.3.4-1: Overload Control Information IE within Sx Session Establishment Response**

| Octet 1 and 2 | Overload Control Information IE Type = 54 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| Overload Control Sequence Number | M | See subclause 6.2.4.3.2 for the description and use of this parameter. | X | X | X | Sequence Number |
| Overload Reduction Metric | M | See subclause 6.2.4.3.2 for the description and use of this parameter. | X | X | X | Metric |
| Period of Validity | M | See subclause 6.2.4.3.2 for the description and use of this parameter. | X | X | X | Timer |
| Overload Control Information Flags | C | This IE shall be included if any of flag in this IE is set. | X | X | X | OCI Flags |

## 7.5.4 Sx Session Modification Request

### 7.5.4.1 General

The Sx Session Modification Request is used over the Sxa, Sxb and Sxc interface by the CP function to request the UP function to modify the Sx session.

**Table 7.5.4.1-1: Information Elements in a Sx Session Modification Request**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| CP F-SEID | C | This IE shall be present if the CP function decides to change its F-SEID for the Sx session. The UP function shall use the new CP F-SEID for subsequent Sx Session related messages for this Sx Session. See Note 2. | X | X | X | F-SEID |
| Remove PDR | C | When present, this IE shall contain the PDR Rule which is requested to be removed. See Table 7.5.4-8.<br>Several IEs within the same IE type may be present to represent a list of PDRs to remove. | X | X | X | Remove PDR |
| Remove FAR | C | When present, this IE shall contain the FAR Rule which is requested to be removed. See Table 7.5.4-9.<br>Several IEs within the same IE type may be present to represent a list of FARs to remove. | X | X | X | Remove FAR |
| Remove URR | C | When present, this shall contain the URR Rule which is requested to be removed. See Table 7.5.4-10.<br>Several IEs within the same IE type may be present to represent a list of URRs to remove. | X | X | X | Remove URR |
| Remove QER | C | When present, this IE shall contain the QER Rule which is requested to be removed. See Table 7.5.4-11.<br>Several IEs within the same IE type may be present to represent a list of QERs to remove. | - | X | X | Remove QER |
| Remove BAR | C | When present, this IE shall contain the BAR Rule which is requested to be removed. See Table 7.5.4.12-1. | X | - | - | Remove BAR |
| Create PDR | C | This IE shall be present if the CP function requests the UP function to create a new PDR.<br>See Table 7.5.2.2-1.<br>Several IEs within the same IE type may be present to represent a list of PDRs to create. | X | X | X | Create PDR |
| Create FAR | C | This IE shall be present if the CP function requests the UP function to create a new FAR.See Table 7.5.2.3-1.<br>Several IEs within the same IE type may be present to represent a list of FARs to create. | X | X | X | Create FAR |
| Create URR | C | This IE shall be present if the CP function requests the UP function to create a new URR. See Table 7.5.2.4-1.<br>Several IEs within the same IE type may be present to represent a list of URRs to create. | X | X | X | Create URR |
| Create QER | C | This IE shall be present if the CP function requests the UP function to create a new QER. See Table 7.5.2.5-1.<br>Several IEs within the same IE type may be present to represent a list of QERs to create. | - | X | X | Create QER |
| Create BAR | C | This IE shall be present if the CP function requests the UP function to create a new BAR.<br>See Table 7.5.2.2-1. | X | - | - | Create BAR |
| Update PDR | C | This IE shall be present if a PDR previously created for the Sx session need to be modified. See Table 7.5.4.6-1.<br>Several IEs within the same IE type may be present to represent a list of PDRs to update. | X | X | X | Update PDR |
| Update FAR | C | This IE shall be present if a FAR previously created for the Sx session need to be modified. See Table 7.5.4.7-1.<br>Several IEs within the same IE type may be present to represent a list of FARs to update. | X | X | X | Update FAR |
| Update URR | C | This IE shall be present if URR(s) previously created for the Sx session need to be modified.<br>Several IEs within the same IE type may be present to represent a list of modified URRs. Previously URRs that are not modified shall not be included. See Table 7.5.4.8-1. | X | X | X | Update URR |
| Update QER | C | This IE shall be present if QER(s) previously created for the Sx session need to be modified.<br>Several IEs within the same IE type may be present to represent a list of modified QERs.<br>Previously created QERs that are not modified shall not be included.<br>See Table 7.5.4.9-1. | - | X | X | Update QER |

| | | | | | | |
|---|---|---|---|---|---|---|
| Update BAR | C | This IE shall be present if a BAR previously created for the Sx session needs to be modified.<br>A previously created BAR that is not modified shall not be included.<br>See Table 7.5.4.3-3. | X | - | - | Update BAR |
| SxSMReq-Flags | C | This IE shall be included if at least one of the flags is set to 1.<br>- DROBU (Drop Buffered Packets): the CP function shall set this flag if the UP function is requested to drop the packets currently buffered for this Sx session (see NOTE 1).<br>- QAURR (Query All URRs): the CP function shall set this flag if the CP function requests immediate usage report(s) for all the URRs previously provisioned for this Sx session (see NOTE 3). | X<br><br>X | -<br><br>X | -<br><br>X | SxSMReq-Flags |
| Query URR | C | This IE shall be present if the CP function requests immediate usage report(s) to the UP function.<br>Several IEs within the same IE type may be present to represent a list of URRs for which an immediate report is requested.<br>See Table 7.5.4.10-1.<br>See NOTE 3. | X | X | X | Query URR |
| PGW-C FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - | FQ-CSID |
| SGW-C FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - | FQ-CSID |
| MME FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - | FQ-CSID |
| ePDG FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - | FQ-CSID |
| TWAN FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - | FQ-CSID |

NOTE 1: The CP function may request the UP function to drop the packets currently buffered for the Sx session when using extended buffering of downlink data packets, buffering is performed in the UP function and the DL Data Buffer Expiration Time is handled by the CP function. In this case, when the DL Data Buffer Expiration Time expires, the CP function shall send an Sx Session Modification Request including the DROBU flag (to drop the downlink data packets currently buffered in the UP function) and updating the Apply Action within the FARs of this Sx session to request the UP function to start buffering the downlink data packets with notifying the arrival of subsequent downlink data packets. See subclause 5.9.3 of 3GPP TS 23.214 [2].

NOTE 2: When changing the CP F-SEID of an established Sx Session, the CP function shall be able to handle any incoming Sx Session related messages sent by the UP function with the previous CP F-SEID for a duration at least longer than twice the PFCP retransmission timer (N1xT1).

NOTE 3: The QAURR (Query All URRs) flag in the SxSMReq-Flags IE and the Query URR IE are exclusive from each other in a Sx Session Modification Request.

### 7.5.4.2 Update PDR IE within Sx Session Modification Request

The Update PDR grouped IE shall be encoded as shown in Figure 7.5.4.2-1.

**Table 7.5.4.2-1: Update PDR IE within Sx Session Modification Request**

| Octet 1 and 2 | Update PDR IE Type = 9 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| PDR ID | M | This IE shall uniquely identify the PDR among all the PDRs configured for that Sx session. | X | X | X | PDR ID |
| Outer Header Removal | C | This IE shall be present if it needs to be changed. | X | X | - | Outer Header Removal |
| Precedence | C | This IE shall be present if there is a change in the PDR's precedence to be applied by the UP function among all PDRs of the Sx session, when looking for a PDR matching an incoming packet. | - | X | X | Precedence |
| PDI | C | This IE shall be present if there is a change within the PDI against which incoming packets will be matched. When present, this IE shall replace the PDI previously stored in the UP function for this PDR. See Table 7.5.2.2-2. | X | X | X | PDI |
| FAR ID | C | This IE shall be present if it needs to be changed | X | X | X | FAR ID |
| URR ID | C | This IE shall be present if a measurement action shall be applied or no longer applied to packets matching this PDR.<br>When present, this IE shall contain the list of all the URR IDs to be associated to the PDR. | X | X | X | URR ID |
| QER ID | C | This IE shall be present if a QoS enforcement action shall be applied or no longer applied to packets matching this PDR.<br>When present, this IE shall contain the list of all the QER IDs to be associated to the PDR. | - | X | X | QER ID |
| Activate Predefined Rules | C | This IE shall be present if new Predefined Rule(s) needs to be activated for the PDR. | - | X | X | Activate Predefined Rules |
| Deactivate Predefined Rules | C | This IE shall be present if Predefined Rule(s) needs to be deactivated for the PDR | - | X | X | Deactivate Predefined Rules |
| NOTE: The IEs which do not need to be modified shall not be included in the Update PDR IE. The UP function shall continue to behave according to the values previously received for IEs not present in the Update PDR IE. | | | | | | |

### 7.5.4.3 Update FAR IE within Sx Session Modification Request

The Update FAR grouped IE shall be encoded as shown in Figure 7.5.4.3-1.

**Table 7.5.4.3-1: Update FAR IE within Sx Session Modification Request**

| Octet 1 and 2 | Update FAR IE Type = 10 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| FAR ID | M | This IE shall identify the FAR to be updated. | X | X | X | FAR ID |
| Apply Action | C | This IE shall be present if it is changed. | X | X | X | Apply Action |
| Update Forwarding parameters | C | This IE shall be present if it is changed.See table 7.5.4.3-2. | X | X | X | Update Forwarding Parameters |
| Update Duplicating Parameters | C | This IE shall be present if it is changed. See table 7.5.4.3-3. | X | X | - | Update Duplicating Parameters |
| BAR ID | C | This IE shall be present if the BAR ID associated to the FAR needs to be modified. See Table 7.5.4.11-1. | X | - | - | BAR ID |
| NOTE: The IEs which do not need to be modified shall not be included in the Update FAR IE. The UP function shall continue to behave according to the values previously received for IEs not present in the Update FAR IE. | | | | | | |

**Table 7.5.4.3-2: Update Forwarding Parameters IE in FAR**

| Octet 1 and 2 | Update Forwarding Parameters IE Type = 11 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| Destination Interface | C | This IE shall only be provided if it is changed.<br>When present, it shall indicate the destination interface of the outgoing packet. | X | X | X | Destination Interface |
| Network instance | C | This IE shall only be provided if it is changed. | X | X | X | Network Instance |
| Redirect Information | C | This IE shall be present if the instructions regarding the redirection of traffic by the UP function need to be modified. | - | X | X | Redirect Information |
| Outer Header Creation | C | This IE shall only be provided if it is changed | X | X | - | Outer Header Creation |
| Transport Level Marking | C | This IE shall only be provided if it is changed | X | X | - | Transport Level Marking |
| Forwarding Policy | C | This IE shall only be provided if it is changed | - | X | X | Forwarding Policy |
| Header Enrichment | C | This IE shall only be provided if it is changed | - | X | X | Header Enrichment |
| SxSMReq-Flags | C | This IE shall be included if at least one of the flags is set to 1.<br>- SNDEM (Send End Marker Packets): this IE shall be present if the CP function modifies the F-TEID of the downstream node in the Outer Header Creation IE and the CP function requests the UP function to construct and send GTP-U End Marker messages towards the old F-TEID of the downstream node. | X | X | - | SxSMReq-Flags |

**Table 7.5.4.3-3: Update Duplicating Parameters IE in FAR**

| Octet 1 and 2 | Update Duplicating Parameters IE Type = 105 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| Destination Interface | C | This IE shall only be provided if it is changed. When present, it shall indicate the destination interface of the outgoing packet. | X | X | - | Destination Interface |
| Outer Header Creation | C | This IE shall only be provided if it is changed. | X | X | - | Outer Header Creation |
| Transport Level Marking | C | This IE shall only be provided if it is changed. | X | X | - | Transport Level Marking |
| Forwarding Policy | C | This IE shall only be provided if it is changed. | - | X | - | Forwarding Policy |

### 7.5.4.4 Update URR IE within Sx Session Modification Request

The Update URR grouped IE shall be encoded as shown in Figure 7.5.4.4-1.

**Table 7.5.4.4-1: Update URR IE within Sx Session Modification Request**

| Octet 1 and 2 | Update URR IE Type = 13 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| URR ID | M | This IE shall uniquely identify the URR among all the URRs configured for that Sx session | X | X | X | URR ID |
| Measurement Method | C | This IE shall be present if the measurement method needs to be modified.<br>When present, this IE shall indicate the method for measuring the network resources usage, i.e. whether the data volume, duration (i.e. time), combined volume/duration, or event shall be measured. | X | X | X | Measurement Method |
| Reporting Triggers | C | This IE shall be present if the reporting triggers needs to be modified.<br>When present, this IE shall indicate the trigger(s) for reporting network resources usage to the CP function, e.g. periodic reporting or reporting upon reaching a threshold, or envelope closure. | X | X | X | Reporting Triggers |
| Measurement Period | C | This IE shall be present if the Measurement Period needs to be modified.<br>When present, it shall indicate the period for generating and reporting usage reports. | X | X | X | Measurement Period |
| Volume Threshold | C | This IE shall be present if the Volume Threshold needs to be modified. When present, it shall indicate the traffic volume value after which the UP function shall report network resources usage to the CP function for this URR. | X | X | X | Volume Threshold |
| Volume Quota | C | This IE shall be present if the Volume Quota needs to be modified.<br>When present, it shall indicate the Volume Quota value. | - | X | X | Volume Quota |
| Time Threshold | C | This IE shall be present if the Time Threshold needs to be modified. When present, it shall indicate the time usage after which the UP function shall report network resources usage to the CP function for this URR. | X | X | X | Time Threshold |
| Time Quota | C | This IE shall be present if the Time Quota needs to be modified.<br>When present, it shall indicate the Time Quota value. | - | X | X | Time Quota |
| Quota Holding Time | C | This IE shall be present if the Quota Holding Time needs to be modified.<br>When present, it shall contain the duration of the Quota Holding Time. | - | X | X | Quota Holding Time |
| Dropped DL Traffic Threshold | C | This IE shall be present if the Dropped DL Threshold needs to be modified.<br>When present, it shall contain the threshold of the DL traffic being dropped. | X | - | - | Dropped DL Traffic Threshold |
| Monitoring Time | C | This IE shall be present if the Monitoring Time needs to be modified. When present, this IE shall contain the time at which the UP function shall re-apply the volume or time threshold. | - | X | X | Monitoring Time |
| Subsequent Volume Threshold | C | This IE shall be present if the Subsequent Volume Threshold needs to be modified and volume-based measurement is used.<br>When present, it shall indicate the traffic volume value after which the UP function shall report network resources usage to the CP function for this URR for the period after the Monitoring Time. | - | X | X | Subsequent Volume Threshold |
| Subsequent Time Threshold | C | This IE shall be present if the Subsequent Time Threshold needs to be modified. When present, it shall indicate the time usage value after which the UP function shall report network resources usage to the CP function for this URR for the period after the Monitoring Time. | - | X | X | Subsequent Time Threshold |
| Inactivity Detection Time | C | This IE shall be present if the Inactivity Detection Time needs to be modified.<br>When present, it shall indicate the duration of the inactivity period after which time measurement needs to be suspended when no packets are received during this inactivity period. | - | X | X | Inactivity Detection Time |

| | | | | | | |
|---|---|---|---|---|---|---|
| Linked URR ID | C | This IE shall be present if linked usage reporting is required. When present, this IE shall contain the linked URR ID which is related with this URR (see subclause 5.2.2.4). | - | X | X | Linked URR ID |
| Measurement Information | C | This IE shall be included if any of the following flag is set to 1.<br>Applicable flags are:<br>- Inactive Measurement Flag: this flag shall be set to 1 if the measurement shall be paused (inactive). The measurement shall be performed (active) if the bit is set to 0 or if the Measurement Information IE is not present in the Update URR IE. | - | X | - | Measurement Information |
| Time Quota Mechanism | C | This IE shall be present if time-based measurement based on CTP or DTP needs to be modified. | - | X | - | Time Quota Mechanism |

### 7.5.4.5 Update QER IE within Sx Session Modification Request

The Update QER grouped IE shall be encoded as shown in Figure 7.5.4.5-1.

**Table 7.5.4.5-1: Update QER IE within Sx Session Modification Request**

| Octet 1 and 2 | Update QER IE Type = 14 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| QER ID | M | This IE shall uniquely identify the QER among all the QRs configured for that Sx session | - | X | X | QER ID |
| QER Correlation ID | C | This IE shall be present if the QER correlation ID in this QER needs to be modified.<br>See NOTE 1. | - | X | - | QER Correlation ID |
| Gate Status | C | This IE shall be present if the Gate Status needs to be modified. When present, it shall indicate whether the packets are allowed to be forwarded (the gate is open) or shall be discarded (the gate is closed) in the uplink and/or downlink directions.<br>See NOTE 1. | - | X | X | Gate Status |
| Maximum Bitrate | C | This IE shall be present if an MBR enforcement action applied to packets matching this PDR need to be modified.<br>When present, this IE shall indicate the uplink and/or downlink maximum bit rate to be enforced for packets matching the PDR.<br><br>This IE may be set to the value of:<br>- the APN-AMBR, for a QER that is referenced by all the PDRs of the non-GBR bearers of a PDN connection;<br>- the TDF session MBR, for a QER that is referenced by all the PDRs of a TDF session;<br>- the bearer MBR, for a QER that is referenced by all the PDRs of a bearer;<br>- the SDF MBR, for a QER that is referenced by all the PDRs of a SDF.<br>See NOTE 1. | - | X | X | MBR |
| Guaranteed Bitrate | C | This IE shall be present if a GBR authorization to packets matching this PDR needs to be modified. When present, this IE shall indicate the authorized uplink and/or downlink guaranteed bit rate.<br><br>This IE may be set to the value of:<br>- the aggregate GBR, for a QER that is referenced by all the PDRs of a GBR bearer;<br>- the SDF GBR, for a QER that is referenced by all the PDRs of a SDF.<br>See NOTE 1. | - | X | X | GBR |
| Packet Rate | C | This IE shall be present if a Packet Rate enforcement action (in terms of number of packets per time interval) need to be modified for packets matching this PDR. | - | X | - | Packet Rate |
| DL Flow Level Marking | C | This IE shall be set if the DL Flow Level Marking IE needs to be modified.<br>See NOTE 1. | - | X | X | DL Flow Level Marking |
| NOTE 1: The IEs which do not need to be modified shall not be included in the Update QER IE. The UP function shall continue to behave according to the values previously received for IEs not present in the Update QER IE. | | | | | | |

## 7.5.4.6 Remove PDR IE within Sx Session Modification Request

The Remove PDR grouped IE shall be encoded as shown in Figure 7.5.4.6-1.

**Table 7.5.4.6-1: Remove PDR IE within Sx Session Modification Request**

| Octet 1 and 2 | Remove PDR IE Type = 15 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| PDR ID | M | This IE shall identify the PDR to be deleted. | X | X | X | PDR ID |

## 7.5.4.7 Remove FAR IE within Sx Session Modification Request

The Remove FAR grouped IE shall be encoded as shown in Figure 7.5.4.7-1.

**Table 7.5.4.7-1: Remove FAR IE within Sx Session Modification Request**

| Octet 1 and 2 | Remove FAR IE Type = 16 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| FAR ID | M | This IE shall identify the FAR to be deleted. | X | X | X | FAR ID |

## 7.5.4.8 Remove URR IE within Sx Session Modification Request

The Remove URR grouped IE shall be encoded as shown in Figure 7.5.4.7-1.

**Table 7.5.4.8-1: Remove URR IE within Sx Session Modification Request**

| Octet 1 and 2 | Remove URR IE Type = 17 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| URR ID | M | This IE shall identify the URR to be deleted. | X | X | X | URR ID |

## 7.5.4.9 Remove QER IE Sx Session Modification Request

The Remove QER grouped IE shall be encoded as shown in Figure 7.5.4.9-1.

**Table 7.5.4.9-1: Remove QER IE Sx Session Modification Request**

| Octet 1 and 2 | Remove QER IE Type = 18 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| QER ID | M | This IE shall identify the QER to be deleted. | - | X | X | QER ID |

## 7.5.4.10 Query URR IE within Sx Session Modification Request

The Query URR grouped IE shall be encoded as shown in Figure 7.5.4.10-1.

**Table 7.5.4.10-1: Query URR IE within Sx Session Modification Request**

| Octet 1 and 2 | Query URR IE Type = 77 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| URR ID | M | This IE shall identify the URR being queried. | X | X | X | URR ID |

## 7.5.4.11 Update BAR IE within Sx Session Modification Request

The Update BAR grouped IE shall be encoded as shown in Figure 7.5.4.11-1.

**Table 7.5.4.11-1: Update BAR IE within Sx Session Modification Request**

| Octet 1 and 2 | Update BAR IE Type = 86 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| BAR ID | M | This IE shall identify the BAR Rule to be modified. | X | - | - | BAR ID |
| Downlink Data Notification Delay | C | This IE shall be present if the UP function indicated support of the Downlink Data Notification Delay parameter (see subclause 8.2.28) and the Downlink Data Notification Delay needs to be modified.<br>When present, it shall contain the delay the UP function shall apply between receiving a downlink data packet and notifying the CP function about it, when the Apply Action parameter requests to buffer the packets and notify the CP function. | X | - | - | Downlink Data Notification Delay |

## 7.5.4.12 Remove BAR IE within Sx Session Modification Request

The Remove BAR grouped IE shall be encoded as shown in Figure 7.5.4.12-1.

**Table 7.5.4.12-1: Remove BAR IE within Sx Session Modification Request**

| Octet 1 and 2 | Remove BAR IE Type = 87 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| BAR ID | M | This IE shall identify the BAR to be deleted. | X | - | - | BAR ID |

# 7.5.5 Sx Session Modification Response

## 7.5.5.1 General

The Sx Session Modification Response shall be sent over the Sxa, Sxb and Sxc interface by the UP function to the CP function as a reply to the Sx Session Modification Request.

**Table 7.5.5.1-1: Information Elements in a Sx Session Modification Response**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | X | Cause |
| Offending IE | C | This IE shall be included if the rejection is due to an conditional or mandatory IE missing or faulty. | X | X | X | Offending IE |
| Created PDR | C | This IE shall be present if the cause is set to "success", new PDR(s) were requested to be created and the UP function was requested to allocate the local F-TEID for the PDR(s).<br>When present, this IE shall contain the PDR information associated to the Sx session.<br>See Table 7.5.3-2. | X | X | - | Created PDR |
| Load Control Information | O | The UP function may include this IE if it supports the load control feature and the feature is activated in the network.<br>See Table 7.5.3-3. | X | X | X | Load Control Information |
| Overload Control Information | O | During an overload condition, the UP function may include this IE if it supports the overload control feature and the feature is activated in the network. | X | X | X | Overload Control Information |
| Usage Report | C | This IE shall be present if the Query URR IE was present in the Sx Session Modification Request and traffic usage measurements for that URR are available at the UP function.<br>Several IEs within the same IE type may be present to represent a list of Usage Reports. | X | X | X | Usage Report |
| Failed Rule ID | C | This IE shall be included if the Cause IE indicates a rejection due to a rule creation or modification failure. | X | X | X | Failed Rule ID |

### 7.5.5.2 Usage Report IE within Sx Session Modification Response

The Usage Report grouped IE shall be encoded as shown in Figure 7.5.5.2-1.

**Table 7.5.5.2-1: Usage Report IE within Sx Session Modification Response**

| Octet 1 and 2 | Usage Report IE Type = 78 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| URR ID | M | This IE shall identify the URR for which usage is reported. | X | X | X | URR ID |
| UR-SEQN | M | This IE shall uniquely identify the Usage Report for the URR (see subclause 5.2.2.3). | X | X | X | UR-SEQN |
| Usage Report Trigger | M | This IE shall identify the trigger for this report. | X | X | X | Usage Report Trigger |
| Start Time | C | This IE shall be present, except if the Usage Report Trigger indicates 'Start of Traffic' or 'Stop of Traffic'. When present, this IE shall provide the timestamp when the collection of the information in this report was started. | X | X | X | Start Time |
| End Time | C | This IE shall be present, except if the Usage Report Trigger indicates 'Start of Traffic' or 'Stop of Traffic'. When present, this IE shall provide the timestamp when the collection of the information in this report was generated. | X | X | X | End Time |
| Volume Measurement | C | This IE shall be present if a volume measurement needs to be reported. | X | X | X | Volume Measurement |
| Duration Measurement | C | This IE shall be present if a duration measurement needs to be reported. | X | X | X | Duration Measurement |
| Time of First Packet | C | This IE shall be present if available for this URR. | X | X | X | Time of First Packet |
| Time of Last Packet | C | This IE shall be present if available for this URR. | X | X | X | Time of Last Packet |
| Usage Information | C | This IE shall be present if the UP function reports Usage Reports before and after a Monitoring Time or before and after QoS enforcement. When present, it shall indicate whether the usage is reported for the period before or after that time, or before or after QoS enforcement. | X | X | X | Usage Information |

## 7.5.6 Sx Session Deletion Request

The Sx Session Deletion Request shall be sent over the Sxa, Sxb and Sxc interface by the CP function to request the UP function to delete the Sx session.

**Table 7.5.6-1: Information Elements in a Sx Session Deletion Request**

| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
|---|---|---|---|---|---|---|
| | | | **Sx a** | **Sx b** | **Sx c** | |
| | | | | | | |

## 7.5.7 Sx Session Deletion Response

### 7.5.7.1 General

The Sx Session Deletion Response shall be sent over the Sxa, Sxb and Sxc interface by the UP function to the CP function as a reply to the Sx Session Deletion Request.

**Table 7.5.7.1-1: Information Elements in a Sx Session Deletion Response**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | X | Cause |
| Offending IE | C | This IE shall be included if the rejection is due to an conditional or mandatory IE missing or faulty. | X | X | X | Offending IE |
| Load Control Information | O | The UP function may include this IE if it supports the load control feature and the feature is activated in the network. See Table 7.5.3.3-1. | X | X | X | Load Control Information |
| Overload Control Information | O | During an overload condition, the UP function may include this IE if it supports the overload control feature and the feature is activated in the network. See Table 7.5.3.4-1. | X | X | X | Overload Control Information |
| Usage Report | C | This IE shall be present if a URR had been provisioned in the UP function for the Sx session being deleted and traffic usage measurements for that URR are available at the UP function. Several IEs within the same IE type may be present to represent a list of Usage Reports. | X | X | X | Usage Report |

## 7.5.7.2 Usage Report IE within Sx Session Deletion Response

The Usage Report grouped IE shall be encoded as shown in Figure 7.5.7.2-1.

**Table 7.5.7.2-1: Usage Report IE within Sx Session Deletion Response**

| Octet 1 and 2 | Usage Report IE Type = 79 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| URR ID | M | This IE shall identify the URR for which usage is reported. | X | X | X | URR ID |
| UR-SEQN | M | This IE shall uniquely identify the Usage Report for the URR (see subclause 5.2.2.3). | X | X | X | UR-SEQN |
| Usage Report Trigger | M | This IE shall identify the trigger for this report. | X | X | X | Usage Report Trigger |
| Start Time | C | This IE shall be present, except if the Usage Report Trigger indicates 'Start of Traffic' or 'Stop of Traffic'. When present, this IE shall provide the timestamp when the collection of the information in this report was started. | X | X | X | Start Time |
| End Time | C | This IE shall be present, except if the Usage Report Trigger indicates 'Start of Traffic' or 'Stop of Traffic'. When present, this IE shall provide the timestamp when the collection of the information in this report was generated. | X | X | X | End Time |
| Volume Measurement | C | This IE shall be present if a volume needs to be reported. | X | X | X | Volume Measurement |
| Duration Measurement | C | This IE shall be present if a duration measurement needs to be reported. | X | X | X | Duration Measurement |
| Time of First Packet | C | This IE shall be present if available for this URR. | X | X | X | Time of First Packet |
| Time of Last Packet | C | This IE shall be present if available for this URR. | X | X | X | Time of Last Packet |
| Usage Information | C | This IE shall be present if the UP function reports Usage Reports before and after a Monitoring Time, or before and after QoS enforcement. When present, it shall indicate whether the usage is reported for the period before or after that time, or before or after QoS enforcement. | X | X | X | Usage Information |

## 7.5.8 Sx Session Report Request

### 7.5.8.1 General

The Sx Session Report Request shall be sent over the Sxa, Sxb and Sxc interface by the UP function to report information related to an Sx session to the CP function.

**Table 7.5.8-1: Information Elements in a Sx Session Report Request**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| Report Type | M | This IE shall indicate the type of the report. | X | X | X | Report Type |
| Downlink Data Report | C | This IE shall be present if the Report Type indicates a Downlink Data Report. | X | - | - | Downlink Data Report |
| Usage Report | C | This IE shall be present if the Report Type indicates a Usage Report.<br>Several IEs within the same IE type may be present to represent a list of Usage Reports. | X | X | X | Usage Report |
| Error Indication Report | C | This IE shall be present if the Report Type indicates an Error Indication Report. | X | X | - | Error Indication Report |
| Load Control Information | O | The UP function may include this IE if it supports the load control feature and the feature is activated in the network.<br>See Table 7.5.3.3-1. | X | X | X | Load Control Information |
| Overload Control Information | O | During an overload condition, the UP function may include this IE if it supports the overload control feature and the feature is activated in the network.<br>See Table 7.5.3.4-1. | X | X | X | Overload Control Information |

### 7.5.8.2 Downlink Data Report IE within Sx Session Report Request

The Downlink Data Report grouped IE shall be encoded as shown in Figure 7.5.8.2-1.

**Table 7.5.8.2-1: Downlink Data Report IE within Sx Session Report Request**

| Octet 1 and 2 | Downlink Data Report IE Type = 83 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| PDR ID | M | This IE shall identify the PDR for which downlink data packets have been received at the UP function.<br><br>More than one IE with this type may be included to represent multiple PDRs having received downlink data packets. | X | - | - | PDR ID |
| Downlink Data Service Information | C | This IE shall be included for an Sx session with an IP PDN type, if the UP function supports the Paging Policy Differentiation feature (see subclause 4.9 of 3GPP TS 23.401 [14]).<br>When present, for each PDR and for each packet that triggers a Downlink Data Notification, the UP function shall copy, into the Paging Policy Indication value within this IE, the value of the DSCP in TOS (IPv4) or TC (IPv6) information received in the IP payload of the GTP-U packet from the PGW (see IETF RFC 2474 [13]).<br><br>One IE with this type shall be included per PDR ID reported in the message. When multiple PDR ID IEs are present in the message, the Downlink Data Service Information IEs shall be reported according to the order of the PDR ID IEs. | X | - | - | Downlink Data Service Information |

### 7.5.8.3 Usage Report IE within Sx Session Report Request

The Usage Report grouped IE shall be encoded as shown in Figure 7.5.8.3-1.

**Table 7.5.8.3-1: Usage Report IE within Sx Session Report Request**

| Octet 1 and 2 | Usage Report IE Type = 80 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| URR ID | M | This IE shall identify the URR for which usage is reported. | X | X | X | URR ID |
| UR-SEQN | M | This IE shall uniquely identify the Usage Report for the URR (see subclause 5.2.2.3). | X | X | X | UR-SEQN |
| Usage Report Trigger | M | This IE shall identify the trigger for this report. | X | X | X | Usage Report Trigger |
| Start Time | C | This IE shall be present, except if the Usage Report Trigger indicates 'Start of Traffic' or 'Stop of Traffic'. When present, this IE shall provide the timestamp when the collection of the information in this report was started. | X | X | X | Start Time |
| End Time | C | This IE shall be present, except if the Usage Report Trigger indicates 'Start of Traffic' or 'Stop of Traffic'. When present, this IE shall provide the timestamp when the collection of the information in this report was generated. | X | X | X | End Time |
| Volume Measurement | C | This IE shall be present if a volume measurement needs to be reported. | X | X | X | Volume Measurement |
| Duration Measurement | C | This IE shall be present if a duration measurement needs to be reported. | X | X | X | Duration Measurement |
| Application Detection Information | C | This IE shall be present if application detection information needs to be reported. | - | X | X | Application Detection Information |
| UE IP address | C | This IE shall be present if the start or stop of an application has been detected and no UE IP address was provisioned in the PDI. See NOTE 1. | - | - | X | UE IP address |
| Network Instance | C | This IE shall be present if the start or stop of an application has been detected, no UE IP address was provisioned in the PDI and multiple PDNs with overlapping IP addresses are used in the UP function. See NOTE 1. | - | - | X | Network Instance |
| Time of First Packet | C | This IE shall be present if available for this URR. | X | X | X | Time of First Packet |
| Time of Last Packet | C | This IE shall be present if available for this URR. | X | X | X | Time of Last Packet |
| Usage Information | C | This IE shall be present if the UP function reports Usage Reports before and after a Monitoring Time, or before and after QoS enforcement. When present, it shall indicate whether the usage is reported for the period before or after that time, or before or after QoS enforcement. | X | X | X | Usage Information |
| NOTE 1: This is the case for unsolicited application reporting by the TDF. The Network instance is required when the UE IP address cannot be used to determine the corresponding PDN connection. | | | | | | |

**Table 7.5.8.3-2: Application Detection Information IE within Usage Report IE**

| Octet 1 and 2 | Application Detection Information IE Type = 68 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application ID | M | This IE shall identify the Application ID for which a start or stop of traffic is reported. | - | X | X | Application ID |
| Application Instance ID | C | When present, this IE shall identify the Application Instance Identifier for which a start or stop of traffic is reported. It shall be present, when reporting the start of an application, if the flow information for the detected application is deducible. It shall be present, when reporting the stop of an application, if it was provided when reporting the start of the application. | - | X | X | Application Instance ID |
| Flow Information | C | When present, this IE shall contain the flow information for the detected application. It shall be present, when reporting the start of an application, if the flow information for the detected application is deducible. | - | X | X | Flow Information |

### 7.5.8.4 Error Indication Report IE within Sx Session Report Request

The Error Indication Report grouped IE shall be encoded as shown in Figure 7.5.8.4-1.

**Table 7.5.8.4-1: Error Indication Report IE within Sx Session Report Request**

| Octet 1 and 2 | Error Indication Report IE Type = 99 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| Remote F-TEID | M | This IE shall identify the remote F-TEID of the GTP-U bearer for which an Error Indication has been received at the UP function.<br><br>More than one IE with this type may be included to represent multiple remote F-TEID for which an Error Indication has been received. | X | X | - | F-TEID |

## 7.5.9 Sx Session Report Response

### 7.5.9.1 General

The Sx Session Report Response shall be sent over the Sxa, Sxb and Sxc interface by the CP function to the UP function as a reply to the Sx Session Report Request.

**Table 7.5.9.1-1: Information Elements in a Sx Session Report Response**

| Information elements | P | Condition / Comment | Appl. | | | IE Type |
|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | X | Cause |
| Offending IE | C | This IE shall be included if the rejection is due to an conditional or mandatory IE missing or faulty. | X | X | X | Offending IE |
| Update BAR | C | This IE shall be present if a BAR previously created for the Sx session needs to be modified.<br>A previously created BAR that is not modified shall not be included.<br>See Table 7.5.9.2-1. | X | - | - | Update BAR |
| SxSRRsp-Flags | C | This IE shall be included if at least one of the flags is set to 1.<br>- DROBU (Drop Buffered Packets): the CP function shall set this flag if the UP function needs to drop the packets currently buffered for this Sx session (see NOTE 1). | X | - | - | SxSRRsp-Flags |
| NOTE 1: The CP function may request the UP function to drop the packets currently buffered for the Sx session, when buffering is performed in the UP function, upon receipt of an Sx Session Report Request notifying the CP function about the arrival of downlink data packets for which the CP function decides to throttle the corresponding Downlink Data Notification message over S11/S4 and. See subclause 5.9.3 of 3GPP TS 23.214 [2]. | | | | | | |

## 7.5.9.2 Update BAR IE within Sx Session Report Response

The Update BAR grouped IE shall be encoded as shown in Figure 7.5.9.2-1.

**Table 7.5.9.2-1: Update BAR IE in Sx Session Report Response**

| Octet 1 and 2 | Update BAR IE Type = 12 (decimal) | | | | | |
|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | |
| BAR ID | M | This IE shall identify the BAR Rule to be modified. | X | - | - | BAR ID |
| Downlink Data Notification Delay | C | This IE shall be present if the UP function indicated support of the Downlink Data Notification Delay parameter (see subclause 8.2.25) and the Downlink Data Notification Delay needs to be modified.<br>When present, it shall contain the delay the UP function shall apply between receiving a downlink data packet and notifying the CP function about it, when the Apply Action parameter requests to buffer the packets and notify the CP function. | X | - | - | Downlink Data Notification Delay |
| DL Buffering Duration | C | This IE shall be present if the UP function indicated support of the DL Buffering Duration parameter (see subclause 8.2.25) and extended buffering of downlink data packet is required in the UP function.<br>When present, this IE shall indicate the duration during which the UP function shall buffer the downlink data packets without sending any further notification to the CP function about the arrival of DL data packets. | X | - | - | DL Buffering Duration |
| DL Buffering Suggested Packet Count | O | This IE may be present if extended buffering of downlink data packet is required in the UP function.<br>When present, this IE shall indicate the maximum number of downlink data packets suggested to be buffered in the UP function. | X | - | - | DL Buffering Suggested Packet Count |
| NOTE 1: If the Apply Action requests the UP function to buffer and notify the CP function and the DL Buffering Duration is set, the UP function shall not notify the CP function for the duration indicated by the DL Buffering Duration. | | | | | | |

# 7.6 Error Handling

## 7.6.1 Protocol Errors

A protocol error is defined as a message or an Information Element received from a peer entity with an unknown type, or if it is unexpected, or if it has an erroneous content.

The term silently discarded is used in the following subclauses to mean that the receiving PFCP entity's implementation shall discard such a message without further processing or that the receiving PFCP entity discards such an IE and continues processing the message. The conditions for the receiving PFCP entity to silently discard an IE are specified in the subsequent subclauses.

The handling of unknown, unexpected or erroneous PFCP messages and IEs shall provide for the forward compatibility of PFCP. Therefore, the sending PFCP entity shall be able to safely include in a message a new conditional-optional or an optional IE. Such an IE may also have a new type value. Any legacy receiving PFCP entity shall, however, silently discard such an IE and continue processing the message.

If a protocol error is detected by the receiving PFCP entity, it should log the event including the erroneous message and may include the error in a statistical counter.

For Response messages containing a rejection Cause value, see subclause 7.2.3.2.

The receiving PFCP entity shall apply the error handling specified in the subsequent subclauses.

If the received erroneous message is a reply to an outstanding PFCP message, the PFCP transaction layer shall stop retransmissions and notify the PFCP application layer of the error even if the reply is silently discarded.

## 7.6.2 Different PFCP Versions

If a PFCP entity receives a message of an unsupported PFCP version, it shall return an Sx Version Not Supported Response message and silently discard the received message.

## 7.6.3 PFCP Message of Invalid Length

If a PFCP entity receives a message, which is too short to contain the respective PFCP header, the PFCP-PDU shall be silently discarded.

If a PFCP entity receives a Request message within an IP/UDP packet of a length that is inconsistent with the value specified in the Length field of the PFCP header, then the receiving PFCP entity should log the error and shall send the Response message with Cause IE value set to "Invalid Length".

If a PFCP entity receives a Response message within an IP/UDP packet of a length that is inconsistent with the value specified in the Length field of the PFCP header, then the receiving PFCP entity should log the error and shall silently discard the message.

## 7.6.4 Unknown PFCP Message

If a PFCP entity receives a message with an unknown Message Type value, it shall silently discard the message.

## 7.6.5 Unexpected PFCP Message

If a PFCP entity receives an unexpected request message, for example a known message that is sent over an interface for which the message is not defined, or a message that is sent over an interface for which the message is defined, but the direction is incorrect, then the PFCP entity shall silently discard the message and shall log an error.

If a PFCP entity receives an unexpected response message which is not a request message, for example a message for which there is no corresponding outstanding request, it shall discard the message and may log an error.

### 7.6.6 Missing Information Elements

A PFCP entity shall check if all mandatory IEs are present in the received Request message. Apart from Echo Request message, if one or more mandatory information elements are missing in the received Request message, the PFCP entity should log the error and shall send a Response message with Cause IE value set to "Mandatory IE missing" with the type of the missing mandatory IE.

If a PFCP entity receives a Response message with Cause IE value set to "Mandatory IE missing", it shall notify its upper layer.

A PFCP entity shall check if all mandatory IEs are present in the received Response message without a rejection Cause value. If one or more mandatory information elements are missing, the PFCP entity shall notify the upper layer and should log the error.

A PFCP entity shall check if conditional information elements are present in the received Request message, if possible (i.e. if the receiving entity has sufficient information available to check if the respective conditions were met). If one or more conditional information elements are missing, a PFCP entity should log the error and shall send a Response message with Cause IE value set to "Conditional IE missing" together with the type of the missing conditional IE.

A PFCP entity shall check if conditional information elements are present in the received Response message without a rejection Cause value, if possible (i.e. if the receiving entity has sufficient information available to check if the respective conditions were met). If one or more conditional information elements are missing, a PFCP entity shall notify the upper layer and should log the error.

For Response messages containing a rejection Cause value, see subclause 7.2.3.2.

Absence of an optional information element shall not trigger any error handling.

### 7.6.7 Invalid Length Information Element

An information element has an invalid length when the actual length of the IE is different from the value of the Length field in the IE header. Here, the actual length of the IE means the length of the content field of the received IE.

If a PFCP message contains more than one information elements and one or more of them have invalid length, the receiving PFCP entity can detect which of the IEs have invalid length only in the following cases:

- If the Length value in the IE header is greater than the overall length of the message;
- If the invalid length IE is the last one in the message.

Apart from Echo Request message, if a receiving PFCP entity detects information element with invalid length in a Request message, it shall send an appropriate error response with Cause IE value set to "Invalid length" together with the type of the offending IE.

### 7.6.8 Semantically incorrect Information Element

Apart from Echo Request message, the receiver of a PFCP signalling message Request including a mandatory or a verifiable conditional information element with a semantically invalid Value shall discard the request, should log the error, and shall send a response with Cause IE value set to "Mandatory IE incorrect" together with a type and instance of the offending IE.

The receiver of a PFCP signalling message Response including a mandatory or a verifiable conditional information element with a semantically invalid Value shall notify the upper layer that a message with this sequence number has been received and should log the error.

If a PFCP entity receives an information element with a value which is shown as reserved, it shall treat that information element as invalid and should log the error. If the invalid IE is received in a Request, and it is a mandatory IE or a verifiable conditional IE, the PFCP entity shall send a response with Cause set to "Mandatory IE incorrect" together with a type and instance of the offending IE.

The principle is: the use of reserved values invokes error handling; the use of spare values can be silently discarded and for IEs with spare values used, processing shall be continued ignoring the spare values.

The receiver of a PFCP 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, but shall treat the rest of the message as if this IE was absent and continue processing. The receiver shall not check the content of an information element field that is defined as "spare".

All semantically incorrect optional information elements in a PFCP signalling message shall be treated as not present in the message.

### 7.6.9 Unknown or unexpected Information Element

The receiver of a PFCP message including an unexpected information element with a known Type value that is not defined for this message shall discard the IE and log an error. The receiver shall process the message.

NOTE: An Information Element in an encoded PFCP message or grouped IE is identified by the IE Type.

### 7.6.10 Repeated Information Elements

An Information Element is repeated if there is more than one IE with the same IE Type in the scope of the PFCP message (or in the scope of the grouped IE). Such an IE is a member in a list.

If an information element is repeated in a PFCP 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 the number of repetitions of information elements is specified, only the contents of specified repeated information elements shall be handled and all subsequent repetitions of the information element shall be ignored.

# 8 Information Elements

## 8.1 Information Elements Format

### 8.1.1 Information Element Format

Figure 8.1.1-1 depicts the format of an Information Element.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = xxx (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| p to (p+1) | Enterprise ID | | | | | | | |
| k to (n+4) | IE specific data or content of a grouped IE | | | | | | | |

**Figure 8.1.1-1: Information Element Format**

NOTE 1: If the Bit 8 of Octet 1 is not set, this indicates that the IE is defined by 3GPP and the Enterprise ID is absent. If Bit 8 of Octet 1 is set, this indicates that the IE is defined by a vendor and the Enterprise ID is present identified by the Enterprise ID.

An IE has the following mandatory fields:

- Type: this field indicates the type of the Information Element. IE type values within the range of 0 to 32767 are reserved for IE defined by 3GPP and are listed in subclause 8.1.2 IE type values within the range of 32768 to 65535 are used for vendor-specific IE and the value allocation is controlled by the vendor.

- Length: this field contains the length of the IE excluding the first four octets, which are common for all IEs (Type and Length) and is denoted "n" in Figure 8.1.1-1 and in Figure 8.1.1-2. 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.

An IE has the following optional fields:

- Enterprise ID: if the IE type value is within the range of 32768 to 65535, this field shall contain the IANA-assigned "SMI Network Management Private Enterprise Codes" value of the vendor defining the IE. The Enterprise ID set to "10415" (IANA-assigned "SMI Network Management Private Enterprise Codes") shall not be used for the vendor specific IEs.

For illustration, Figure 8.1.1-2 depicts the format of a Information Element (IE) defined by 3GPP and is specified in this specification. For IE's defined by 3GPP, the IE type shall be within the range of 0 to 32767.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = xxx (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | IE specific data or content of a grouped IE | | | | | | | |

**Figure 8.1.1-2: 3GPP defined Information Element Format**

NOTE 2: Bit 8 of Octet 1 is not set. This indicates that the Information Element type value has been allocated by 3GPP.

For illustration, Figure 8.1.1-3 depicts the format of a vendor-specific Information Element, which content is not specified and the IE type value shall be within the range of 32768 to 65535.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = xxx (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 6 | Enterprise ID | | | | | | | |
| 7 to (n+4) | IE specific data or content of a grouped IE | | | | | | | |

**Figure 8.1.1-3: Vendor-Specific Information Element Format**

NOTE 3: Bit 8 of Octet 1 is set. This indicates that the IE type value has been allocated by the vendor identified by the Enterprise ID. The content of this IE is vendor specific and therefore out of scope of this specification.

## 8.1.2 Information Element Types

A PFCP message may contain several IEs. In order to have forward compatible type definitions for the PFCP IEs, all of them shall be TLV (Type, Length, Value) coded. PFCP IE type values are specified in the Table 8.1.2-1. The last column of this table indicates whether the IE is:

- Fixed Length: the IE has a fixed set of fields, and a fixed number of octets;

- Variable Length: the IE has a fixed set of fields, and has a variable number of octets.
  For example, the last octets may be numbered similar to "5 to (n+4)". In this example, if the value of the length field, n, is 0, then the last field is not present;

- Extendable: the IE has a variable number of fields, and has a variable number of octets.
  The last fields are typically specified with the statement: "These octet(s) is/are present only if explicitly specified". The legacy receiving entity shall ignore the unknown octets.

An IE of any of the above types may have a null length as specified in subclause 5.6.3. This shall not be considered as an error by the receiving PFCP entity.

In order to improve the efficiency of troubleshooting, it is recommended that the IEs should be arranged in the signalling messages as well as in the grouped IEs, according to the order the IEs are listed in the message definition table or grouped IE definition table in section 7. However the receiving entity shall be prepared to handle the messages with IEs in any order.

Within IEs, certain fields may be described as spare. These bits shall be transmitted with the value set to 0. To allow for future features, the receiver shall not evaluate these bits.

**Table 8.1.2-1: Information Element Types**

| IE Type value (Decimal) | Information elements | Comment / Reference | Number of Fixed Octets |
|---|---|---|---|
| 0 | Reserved | | |
| 1 | Create PDR | Extendable / Table 7.5.2.2-1 | Not Applicable |
| 2 | PDI | Extendable / Table 7.5.2.2-2 | Not Applicable |
| 3 | Create FAR | Extendable / Table 7.5.2.3-1 | Not Applicable |
| 4 | Forwarding Parameters | Extendable / Table 7.5.2.3-2 | Not Applicable |
| 5 | Duplicating Parameters | Extendable / Table 7.5.2.3-3 | Not Applicable |
| 6 | Create URR | Extendable / Table 7.5.2.4-1 | Not Applicable |
| 7 | Create QER | Extendable / Table 7.5.2.5-1 | Not Applicable |
| 8 | Created PDR | Extendable / Table 7.5.3.2-1 | Not Applicable |
| 9 | Update PDR | Extendable / Table 7.5.4.2-1 | Not Applicable |
| 10 | Update FAR | Extendable / Table 7.5.4.3-1 | Not Applicable |
| 11 | Update Forwarding Parameters | Extendable / Table 7.5.4.3-2 | Not Applicable |
| 12 | Update BAR (Sx Session Report Response) | Extendable / Table 7.5.9.2-1 | Not Applicable |
| 13 | Update URR | Extendable / Table 7.5.4.4 | Not Applicable |
| 14 | Update QER | Extendable / Table 7.5.4.5 | Not Applicable |
| 15 | Remove PDR | Extendable / Table 7.5.4.6 | Not Applicable |
| 16 | Remove FAR | Extendable / Table 7.5.4.7 | Not Applicable |
| 17 | Remove URR | Extendable / Table 7.5.4.8 | Not Applicable |
| 18 | Remove QER | Extendable / Table 7.5.4.9 | Not Applicable |
| 19 | Cause | Fixed / Subclause 8.2.1 | 1 |
| 20 | Source Interface | Extendable / Subclause 8.2.2 | 1 |
| 21 | F-TEID | Extendable / Subclause 8.2.3 | q-4 |
| 22 | Network Instance | Variable Length / Subclause 8.2.4 | Not Applicable |
| 23 | SDF Filter | Extendable / Subclause 8.2.5 | v+2-4 |
| 24 | Application ID | Variable Length / Subclause 8.2.6 | Not Applicable |
| 25 | Gate Status | Extendable / Subclause 8.2.7 | 1 |
| 26 | MBR | Extendable / Subclause 8.2.8 | 10 |
| 27 | GBR | Extendable / Subclause 8.2.9 | 10 |
| 28 | QER Correlation ID | Extendable / Subclause 8.2.10 | 4 |
| 29 | Precedence | Extendable / Subclause 8.2.11 | 4 |
| 30 | Transport Level Marking | Extendable / Subclause 8.2.12 | 2 |
| 31 | Volume Threshold | Extendable /Subclause 8.2.13 | q+7-4 |
| 32 | Time Threshold | Extendable /Subclause 8.2.14 | 4 |
| 33 | Monitoring Time | Extendable /Subclause 8.2.15 | 4 |
| 34 | Subsequent Volume Threshold | Extendable /Subclause 8.2.16 | q+7-4 |
| 35 | Subsequent Time Threshold | Extendable /Subclause 8.2.17 | 4 |
| 36 | Inactivity Detection Time | Extendable /Subclause 8.2.18 | 4 |
| 37 | Reporting Triggers | Extendable /Subclause 8.2.19 | 2 |
| 38 | Redirect Information | Extendable /Subclause 8.2.20 | 8+a-4 |
| 39 | Report Type | Extendable / Subclause 8.2.21 | 1 |
| 40 | Offending IE | Fixed / Subclause 8.2.22 | 2 |
| 41 | Forwarding Policy | Extendable / Subclause 8.2.23 | k-4 |

| IE Type value (Decimal) | Information elements | Comment / Reference | Number of Fixed Octets |
|---|---|---|---|
| 42 | Destination Interface | Extendable / Subclause 8.2.24 | 1 |
| 43 | UP Function Features | Extendable / Subclause 8.2.25 | 1 |
| 44 | Apply Action | Extendable / Subclause 8.2.26 | 1 |
| 45 | Downlink Data Service Information | Extendable / Subclause 8.2.27 | 1 |
| 46 | Downlink Data Notification Delay | Extendable / Subclause 8.2.28 | 1 |
| 47 | DL Buffering Duration | Extendable / Subclause 8.2.29 | 1 |
| 48 | DL Buffering Suggested Packet Count | Variable / Subclause 8.2.30 | Not Applicable |
| 49 | SxSMReq-Flags | Extendable / Subclause 8.2.31 | 1 |
| 50 | SxSRRsp-Flags | Extendable / Subclause 8.2.32 | 1 |
| 51 | Load Control Information | Extendable / Table 7.5.3.3-1 | Not Applicable |
| 52 | Sequence Number | Fixed Length / Subclause 8.2.33 | 4 |
| 53 | Metric | Fixed Length / Subclause 8.2.34 | 1 |
| 54 | Overload Control Information | Extendable / Table 7.5.3.4-1 | Not Applicable |
| 55 | Timer | Extendable / Subclause 8.2 35 | 1 |
| 56 | Packet Detection Rule ID | Extendable / Subclause 8.2 36 | 2 |
| 57 | F-SEID | Extendable / Subclause 8.2 37 | p+15-4 |
| 58 | Application ID's PFDs | Extendable / Table 7.4.3.1-2 | Not Applicable |
| 59 | PFD context | Extendable / Table 7.4.3.1-3 | Not Applicable |
| 60 | Node ID | Extendable / Subclause 8.2.38 | o-4 |
| 61 | PFD contents | Extendable / Subclause 8.2.39 | v-4 |
| 62 | Measurement Method | Extendable / Subclause 8.2.40 | 1 |
| 63 | Usage Report Trigger | Extendable / Subclause 8.2.41 | 1 |
| 64 | Measurement Period | Extendable / Subclause 8.2.42 | 4 |
| 65 | FQ-CSID | Extendable / Subclause 8.2.43 | (q+1)-4 |
| 66 | Volume Measurement | Extendable / Subclause 8.2.44 | q+7-4 |
| 67 | Duration Measurement | Extendable / Subclause 8.2.45 | 4 |
| 68 | Application Detection Information | Extendable / Table 7.5.8.3-2 | Not Applicable |
| 69 | Time of First Packet | Extendable / Subclause 8.2.46 | 4 |
| 70 | Time of Last Packet | Extendable / Subclause 8.2.47 | 4 |
| 71 | Quota Holding Time | Extendable / Subclause 8.2.48 | 4 |
| 72 | Dropped DL Traffic Threshold | Extendable / Subclause 8.2.49 | m+7-4 |
| 73 | Volume Quota | Extendable / Subclause 8.2.50 | q+7-4 |
| 74 | Time Quota | Extendable / Subclause 8.2.51 | 4 |
| 75 | Start Time | Extendable / Subclause 8.2.52 | 4 |
| 76 | End Time | Extendable / Subclause 8.2.53 | 4 |

| IE Type value (Decimal) | Information elements | Comment / Reference | Number of Fixed Octets |
|---|---|---|---|
| 77 | Query URR | Extendable / Table 7.5.4.10-1 | Not Applicable |
| 78 | Usage Report (in Session Modification Response) | Extendable / Table 7.5.5.2-1 | Not Applicable |
| 79 | Usage Report (Session Deletion Response) | Extendable / Table 7.5.7.2-1 | Not Applicable |
| 80 | Usage Report (Session Report Request) | Extendable / Table 7.5.8.3-1 | Not Applicable |
| 81 | URR ID | Extendable / Subclause 8.2.54 | 4 |
| 82 | Linked URR ID | Extendable / Subclause 8.2.55 | 4 |
| 83 | Downlink Data Report | Extendable / Table 7.5.8.2-1 | Not Applicable |
| 84 | Outer Header Creation | Extendable / Subclause 8.2.56 | r+1-4 |
| 85 | Create BAR | Extendable / Table 7.5.2.6-1 | Not Applicable |
| 86 | Update BAR (Session Modification Request) | Extendable / Table 7.5.4.11-1 | Not Applicable |
| 87 | Remove BAR | Extendable / Table 7.5.4.12-1 | Not Applicable |
| 88 | BAR ID | Extendable / Subclause 8.2.57 | 1 |
| 89 | CP Function Features | Extendable / Subclause 8.2.58 | 1 |
| 90 | Usage Information | Extendable / Subclause 8.2.59 | 1 |
| 91 | Application Instance ID | Variable Length / Subclause 8.2.60 | Not Applicable |
| 92 | Flow Information | Extendable / Subclause 8.2.61 | m-4 |
| 93 | UE IP Address | Extendable / Subclause 8.2.62 | p+15-1 |
| 94 | Packet Rate | Extendable / Subclause 8.2.63 | p+2-4 |
| 95 | Outer Header Removal | Extendable / Subclause 8.2.64 | 1 |
| 96 | Recovery Time Stamp | Extendable / Subclause 8.2.65 | 4 |
| 97 | DL Flow Level Marking | Extendable / Subclause 8.2.66 | p+1-4 |
| 98 | Header Enrichment | Extendable / Subclause 8.2.67 | q-4 |
| 99 | Error Indication Report | Extendable / Table 7.5.8.4-1 | Not Applicable |
| 100 | Measurement Information | Extendable / Subclause 8.2.68 | 1 |
| 101 | Node Report Type | Extendable / Subclause 8.2.69 | 1 |
| 102 | User Plane Path Failure Report | Extendable / Table 7.4.5.1.2-1 | Not Applicable |
| 103 | Remote GTP-U Peer | Extendable / Subclause 8.2.70 | p+15-4 |
| 104 | UR-SEQN | Fixed Length / Subclause 8.2.71 | 4 |
| 105 | Update Duplicating Parameters | Extendable / Table 7.5.4.3-3 | Not Applicable |
| 106 | Activate Predefined Rules | Variable Length / Subclause 8.2.72 | Not Applicable |
| 107 | Deactivate Predefined Rules | Variable Length / Subclause 8.2.73 | Not Applicable |
| 108 | FAR ID | Extendable / Subclause 8.2.74 | 4 |
| 109 | QER ID | Extendable / Subclause 8.2.75 | 4 |
| 110 | OCI Flags | Extendable / Subclause 8.2.76 | 1 |
| 111 | Sx Association Release Request | Extendable / Subclause 8.2.77 | 1 |

| IE Type value (Decimal) | Information elements | Comment / Reference | Number of Fixed Octets |
|---|---|---|---|
| 112 | Graceful Release Period | Extendable / Subclause 8.2.78 | 1 |
| 113 | PDN Type | Extendable / Subclause 8.2.79 | 1 |
| 114 | Failed Rule ID | Extendable / Subclause 8.2.80 | p-4 |
| 115 | Time Quota Mechanism | Extendable / Subclause 8.2.81 | 5 |
| 116 | User Plane IP Resource Information | Extendable / Subclause 8.2.82 | l+1-4 |
| 117 to 65535 | Spare. For future use. | | |

# 8.2 Information Elements

## 8.2.1 Cause

Cause IE is coded as depicted in Figure 8.2.1-1.

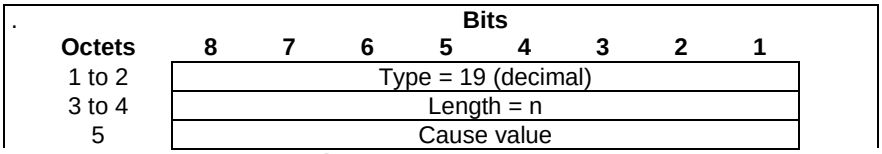


**Figure 8.2.1-1: Cause**

The Cause value shall be included in a response message. In a response message, the Cause value indicates the acceptance or the rejection of the corresponding request message. The Cause value indicates the explicit reason for the rejection.

**Table 8.2.1-1: Cause values**

| Message Type | Cause value (decimal) | Meaning | Description |
|---|---|---|---|
| | 0 | Reserved. | Shall not be sent and if received the Cause shall be treated as an invalid IE |
| Acceptance in a response | 1 | Request accepted (success) | "Request accepted (success)" is returned when the PFCP entity has accepted a request. |
| | 2-63 | Spare. | This value range shall be used by Cause values in an acceptance response message. See NOTE 1. |
| Rejection in a response | 64 | Request rejected (reason not specified) | This cause shall be returned to report an unspecified rejection cause |
| | 65 | Session context not found | This cause shall be returned, if the F-SEID included in a Sx Session Modification/Deletion Request message is unknown. |
| | 66 | Mandatory IE missing | This cause shall be returned when the PFCP entity detects that a mandatory IE is missing in a request message |
| | 67 | Conditional IE missing | This cause shall be returned when the PFCP entity detects that a Conditional IE is missing in a request message. |
| | 68 | Invalid length | This cause shall be returned when the PFCP entity detects that an IE with an invalid length in a request message |
| | 69 | Mandatory IE incorrect | This cause shall be returned when the PFCP entity detects that a Mandatory IE is missing in a request message. |
| | 70 | Invalid Forwarding Policy | This cause shall be used by the UP function in the Sx Session Establishment Response or Sx Session Modification Response message if the CP function attempted to provision a FAR with a Forwarding Policy Identifier for which no Forwarding Policy is locally configured in the UP function. |
| | 71 | Invalid F-TEID allocation option | This cause shall be used by the UP function in the Sx Session Establishment Response or Sx Session Modification Response message if the CP function attempted to provision a PDR with a F-TEID allocation option which is incompatible with the F-TEID allocation option used for already created PDRs (by the same or a different CP function). |
| | 72 | No established Sx Association | This cause shall be used by the CP function or the UP function if they receive an Sx Session related message from a peer with which there is no established Sx Association. |
| | 73 | Rule creation/modification Failure | This cause shall be used by the UP function if a received Rule failed to be stored and be applied in the UP function. |
| | 74 | PFCP entity in congestion | This cause shall be returned when a PFPC entity has detected node level congestion and performs overload control, which does not allow the request to be processed. |
| | 75 | No resources available | This cause shall be returned to indicate a temporary unavailability of resources to process the received request. |
| | 76 | Service not supported | This cause shall be returned when a PFCP entity receives a message requesting a feature or service that is not supported. |
| | 77 | System failure | This cause shall be returned to indicate a system error condition. |
| | 78 to 255 | Spare for future use in a response message. See NOTE 2. | This value range shall be used by Cause values in a rejection response message. See NOTE 2. |

NOTE 1: This value is or may be used in future version of the specification. If the receiver cannot comprehend the value, it shall be interpreted as an unspecified acceptance cause. Unspecified/unrecognized acceptance cause shall be treated in the same ways as the cause value 1 " Request accepted (success)".
NOTE 2: This value is or may be used in a future version of the specification. If the receiver cannot comprehend the value, it shall be interpreted as an unspecified rejection cause. Unspecified/unrecognized rejection cause shall be treated in the same ways as the cause value 32 "Request rejected (reason not specified)".

## 8.2.2 Source Interface

The Source Interface IE type shall be encoded as shown in Figure 8.2.2-1. It indicates the type of the interface from which an incoming packet is received.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 20 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | Interface value | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.2-1: Source Interface**

The Interface value shall be encoded as a 4 bits binary integer as specified in in Table 8.2.2-1.

**Table 8.2.2-1: Interface value**

| Interface value | Values (Decimal) |
|---|---|
| Access | 0 |
| Core | 1 |
| SGi-LAN | 2 |
| CP-function | 3 |
| Spare | 4 to 15 |
| NOTE: The "Access" and "Core" values denote an uplink and downlink traffic direction respectively. | |

## 8.2.3 F-TEID

The F-TEID IE type shall be encoded as shown in Figure 8.2.3-1. It indicates an F-TEID.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 21 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | CHID | CH | V6 | V4 |
| 6 to 9 | TEID | | | | | | | |
| m to (m+3) | IPv4 address | | | | | | | |
| p to (p+15) | IPv6 address | | | | | | | |
| q | CHOOSE ID | | | | | | | |
| k to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.3-1: F-TEID**

The following flags are coded within Octet 5:

- Bit 1 – V4: If this bit is set to "1" and the CH bit is not set, then the IPv4 address field shall be present, otherwise the IPv4 address field shall not be present.

- Bit 2 – V6: If this bit is set to "1" and the CH bit is not set, then the IPv6 address field shall be present, otherwise the IPv6 address field shall not be present.

- Bit 3 – CH (CHOOSE): If this bit is set to "1", then the TEID, IPv4 address and IPv6 address fields shall not be present and the UP function shall assign an F-TEID with an IP4 or an IPv6 address if the V4 or V6 bit is set respectively. This bit shall only be set by the CP function.

- Bit 4 – CHID (CHOOSE ID): If this bit is set to "1", then the UP function shall assign the same F-TEID to the PDRs requested to be created in a Sx Session Establishment Request or Sx Session Modification Request with the same CHOOSE ID value. This bit may only be set to "1" if the CH bit it set to "1". This bit shall only be set by the CP function.

- Bit 5 to 8: Spare, for future use and set to 0.

At least one of the V4 and V6 flags shall be set to "1", and both may be set to "1".

Octet 6 to 9 (TEID) shall be present and shall contain a GTP-U TEID, if the CH bit in octet 5 is not set. When the TEID is present, if both IPv4 and IPv6 addresses are present in the F-TEID IE, then the TEID value shall be shared by both addresses.

Octets "m to (m+3)" and/or "p to (p+15)" (IPv4 address / IPv6 address fields), if present, it shall contain the respective IP address values.

Octet q shall be present and shall contain a binary integer value if the CHID bit in octet 5 is set to "1".

## 8.2.4 Network Instance

The Network Instance IE type shall be encoded as shown in Figure 8.2.4-1. It indicates a Network instance.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 22 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Network Instance | | | | | | | |

**Figure 8.2.4-1: Network Instance**

The Network instance field shall be encoded as an OctetString and shall contain an identifier which uniquely identifies a particular Network instance (e.g. PDN instance) in the UP function. It may be encoded as a Domain Name or an Access Point Name (APN) as per subclause 9.1 of 3GPP TS 23.003 [2]. In the latter case, the PDN Instance field may contain the APN Network Identifier only or the full APN with both the APN Network Identifier and the APN Operator Identifier as specified in 3GPP TS 23.003 [2] subclauses 9.1.1 and 9.1.2.

NOTE: The APN field is not encoded as a dotted string as commonly used in documentation.

## 8.2.5 SDF Filter

The SDF Filter IE type shall be encoded as shown in Figure 8.2.5-1. It contains an SDF Filter.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 23 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | FL | SPI | TTC | FD |
| 6 | Spare | | | | | | | |
| m to (m+1) | Length of Flow Description | | | | | | | |
| (m+2) to p | Flow Description | | | | | | | |
| s to (s+1) | ToS Traffic Class | | | | | | | |
| t to (t+3) | Security Parameter Index | | | | | | | |
| v to (v+2) | Flow Label | | | | | | | |
| w to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.5-1: SDF Filter**

The following flags are coded within Octet 5:

- Bit 1 – FD (Flow Description): If this bit is set to "1", then the Length of Flow Description and the Flow Description fields shall be present, otherwise they shall not be present.

- Bit 2 – TTC (ToS Traffic Class): If this bit is set to "1", then the ToS Traffic Class field shall be present, otherwise the ToS Traffic Class field shall not be present.

- Bit 3 – SPI (Security Parameter Index): If this bit is set to "1", then the Security Parameter Index field shall be present, otherwise the Security Parameter Index field shall not be present.

- Bit 4 – FL (Flow Label): If this bit is set to "1", then the Flow Label field shall be present, otherwise the Flow Label field shall not be present.

- Bit 5 to 8: Spare, for future use and set to 0.

The Flow Description field, when present, shall be encoded as an OctetString as specified in subclause 5.4.2 of 3GPP TS 29.212 [8].

The ToS Traffic Class field, when present, shall be encoded as an OctetString on two octets as specified in subclause 5.3.15 of 3GPP TS 29.212 [8].

The Security Parameter Index field, when present, shall be encoded as an OctetString on four octets and shall contain the IPsec security parameter index (which is a 32-bit field), as specified in subclause 5.3.51 of 3GPP TS 29.212 [8].

The Flow Label field, when present, shall be encoded as an OctetString on 3 octets as specified in subclause 5.3.52 of 3GPP TS 29.212 [8] and shall contain an IPv6 flow label (which is a 20-bit field). The bits 8 to 5 of the octet "v" shall be spare and set to zero, and the remaining 20 bits shall contain the IPv6 flow label.

An SDF Filter may:

- be a pattern for matching the IP 5 tuple (source IP address or IPv6 network prefix, destination IP address or IPv6 network prefix, source port number, destination port number, protocol ID of the protocol above IP). In the pattern:

  - a value left unspecified in a filter matches any value of the corresponding information in a packet;

  - an IP address may be combined with a prefix mask;

  - port numbers may be specified as port ranges;

  - the pattern can be extended by the Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask;

- consist of the destination IP address and optional mask, protocol ID of the protocol above IP, the Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask and the IPsec Security Parameter Index (SPI);

- consist of the destination IP address and optional mask, the Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask and the Flow Label (IPv6).

NOTE 1: The details about the IPsec Security Parameter Index (SPI), the Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask and the Flow Label (IPv6) are defined in 3GPP TS 23.060 [19] clause 15.3.

- extend the packet inspection beyond the possibilities described above and look further into the packet. Such service data flow filters need to be predefined in the PGW-U, as specified in subclause 5.11 of 3GPP TS 23.214 [2].

NOTE 2: Such filters may be used to support filtering with respect to a service data flow based on the transport and application protocols used above IP, e.g. for HTTP and WAP. Filtering for further application protocols and services can also be supported.

## 8.2.6 Application ID

The Application ID IE type shall be encoded as shown in Figure 8.2.6-1. It contains an Application Identifier referencing an application detection filter in the UP function (e.g. its value may represent an application such as a list of URLs).

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 24 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Application Identifier | | | | | | | |

**Figure 8.2.6-1: Application ID**

The Application Identifier shall be encoded as an OctetString (see 3GPP TS 29.212 [8]).

## 8.2.7 Gate Status

The Gate Status IE shall be encoded as shown in Figure 8.2.7-1. It indicates whether the service data flow or application's traffic is allowed to be forwarded (gate is open) or shall be discarded (gate is closed) in uplink and/or in downlink direction.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 25 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | UL Gate | DL Gate |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.7-1: Gate Status**

**Table 8.2.7-1: UL Gate**

| UL Gate | Value (Decimal) |
|---|---|
| OPEN | 0 |
| CLOSED | 1 |
| For future use. Shall not be sent. If received, shall be interpreted as the value "1". | 2, 3 |

**Table 8.2.7-2: DL Gate**

| DL Gate | Value (Decimal) |
|---|---|
| OPEN | 0 |
| CLOSED | 1 |
| For future use. Shall not be sent. If received, shall be interpreted as the value "1". | 2, 3 |

## 8.2.8 MBR

The MBR IE type shall be encoded as shown in Figure 8.2.8-1. It indicates the maximum bit rate allowed for the uplink and/or downlink directions.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 26 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 9 | UL MBR | | | | | | | |
| 10 to 14 | DL MBR | | | | | | | |
| 15 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.8-1: MBR**

The UL/DL MBR fields shall be encoded as kilobits per second (1 kbps = 1000 bps) in binary value. The UL/DL MBR fields may require converting values in bits per second to kilobits per second when the UL/DL MBR values are received from an interface other than GTPv2 interface. If such conversions result in fractions, then the value of UL/DL MBR fields shall be rounded upwards. The range of UL/DL MBR is specified in 3GPP TS 36.413 [10].

NOTE: The encoding is aligned on the encoding specified in 3GPP TS 29.274 [9].

## 8.2.9 GBR

The GBR IE type shall be encoded as shown in Figure 8.2.9-1. It indicates the guaranteed bit rate authorized for the uplink and/or downlink directions.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 27 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 9 | UL GBR | | | | | | | |
| 10 to 14 | DL GBR | | | | | | | |
| 15 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.9-1: GBR**

The UL/DL GBR fields shall be encoded as kilobits per second (1 kbps = 1000 bps) in binary value. The UL/DL GBR fields may require converting values in bits per second to kilobits per second when the UL/DL GBR values are received from an interface other than GTPv2 interface. If such conversions result in fractions, then the value of UL/DL GBR fields shall be rounded upwards. The range of UL/DL GBR is specified in 3GPP TS 36.413 [10].

NOTE: The encoding is aligned on the encoding specified in 3GPP TS 29.274 [9].

## 8.2.10 QER Correlation ID

The QER Correlation ID IE type shall be encoded as shown in Figure 8.2.10-1. It contains a QoS Enforcement Rule Correlation ID to correlate QERs from different Sx sessions. The QER Correlation ID shall be dynamically assigned by the CP function and provisioned by the CP function in different Sx sessions to correlate QERs used in these Sx sessions.

NOTE: A QER Correlation ID is not a Rule ID. It is only a correlation number to correlate QERs from different Sx sessions.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 28 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | QER Correlation ID value | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.10-1: QER Correlation ID**

The QER Correlation ID value shall be encoded as an Unsigned32 binary integer value.

## 8.2.11 Precedence

The Precedence IE type shall be encoded as shown in Figure 8.2.11-1. It defines the relative precedence of a PDR among all the PDRs provisioned within an Sx session, when looking for a PDR matching an incoming packet.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 29 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Precedence value | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.11-1: Precedence**

The Precedence value shall be encoded as an Unsigned32 binary integer value.

## 8.2.12 Transport Level Marking

The Transport Level Marking IE type shall be encoded as shown in Figure 8.2.12-1. It indicates the DSCP to be used for UL/DL transport level marking.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 30 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 6 | ToS/Traffic Class | | | | | | | |
| 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.12-1: Transport Level Marking**

The ToS/Traffic Class shall be encoded on two octets as an OctetString. The first octet shall contain the IPv4 Type-of-Service or the IPv6 Traffic-Class field and the second octet shall contain the ToS/Traffic Class mask field. See subclause 5.3.15 of 3GPP TS 29.212 [8].

## 8.2.13 Volume Threshold

The Volume Threshold IE contains the traffic volume thresholds to be monitored by the UP function. It shall be encoded as shown in Figure 8.2.13-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 31 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | DLVOL | ULVOL | TOVOL |
| m to (m+7) | Total Volume | | | | | | | |
| p to (p+7) | Uplink Volume | | | | | | | |
| q to (q+7) | Downlink Volume | | | | | | | |
| s to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.13-1: Volume Threshold**

The following flags are coded within Octet 5:

- Bit 1 – TOVOL: If this bit is set to "1", then the Total Volume field shall be present, otherwise the Total Volume field shall not be present.
- Bit 2 – ULVOL: If this bit is set to "1", then the Uplink Volume field shall be present, otherwise the Uplink Volume field shall not be present.
- Bit 3 – DLVOL: If this bit is set to "1", then the Downlink Volume field shall be present, otherwise the Downlink Volume field shall not be present.
- Bit 4 to 8: Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

The Total Volume, Uplink Volume and Downlink Volume fields shall be encoded as an Unsigned64 binary integer value. They shall contain the total, uplink or downlink number of octets respectively.

## 8.2.14 Time Threshold

The Time Threshold IE contains the traffic duration threshold to be monitored by the UP function. It shall be encoded as shown in Figure 8.2.14-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 32 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Time Threshold | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.14-1: Time Threshold**

The Time Threshold field shall be encoded as an Unsigned32 binary integer value. It shall contain the duration in seconds.

## 8.2.15 Monitoring Time

The Monitoring Time IE indicates the time at which the UP function is expected to reapply the thresholds. It shall be encoded as shown in Figure 8.2.15-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 33 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Monitoring Time | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.15-1: Monitoring Time**

The Monitoring Time field shall indicate the monitoring time in UTC time. Octets 5 to 8 shall be encoded in the same format as the first four octets of the 64-bit timestamp format as defined in section 6 of IETF RFC 5905 [12].

NOTE: The encoding is defined as the time in seconds relative to 00:00:00 on 1 January 1900.

## 8.2.16 Subsequent Volume Threshold

The Subsequent Volume Threshold IE contains the subsequent traffic volume thresholds to be monitored by the UP function after the Monitoring Time. It shall be encoded as shown in Figure 8.2.16-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 34 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | DLVOL | ULVOL | TOVOL |
| m to (m+7) | Total Volume | | | | | | | |
| p to (p+7) | Uplink Volume | | | | | | | |
| q to (q+7) | Downlink Volume | | | | | | | |
| s to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.16-1: Subsequent Volume Threshold**

The following flags are coded within Octet 5:

- Bit 1 – TOVOL: If this bit is set to "1", then the Total Volume field shall be present, otherwise the Total Volume field shall not be present.
- Bit 2 – ULVOL: If this bit is set to "1", then the Uplink Volume field shall be present, otherwise the Uplink Volume field shall not be present.
- Bit 3 – DLVOL: If this bit is set to "1", then the Downlink Volume field shall be present, otherwise the Downlink Volume field shall not be present.
- Bit 4 to 8: Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

The Total Volume, Uplink Volume and Downlink Volume fields shall be encoded as an Unsigned64 binary integer value. They shall contain the total, uplink or downlink number of octets respectively.

## 8.2.17 Subsequent Time Threshold

The Subsequent Time Threshold IE contains the subsequent traffic duration threshold to be monitored by the UP function after the Monitoring Time. It shall be encoded as shown in Figure 8.2.17-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 35 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Subsequent Time Threshold | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.17-1: Subsequent Time Threshold**

The Subsequent Time Threshold field shall be encoded as an Unsigned32 binary integer value. It shall contain the duration in seconds.

## 8.2.18 Inactivity Detection Time

The Inactivity Detection Time IE contains the inactivity time period, in seconds, to be monitored by the UP function. It shall be encoded as shown in Figure 8.2.18-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 36 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Inactivity Detection Time | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.18-1: Inactivity Detection Time**

The Inactivity Detection Time field shall be encoded as an Unsigned32 binary integer value.

## 8.2.19 Reporting Triggers

The Reporting Triggers IE shall be encoded as shown in Figure 8.2.19-1. It indicates the reporting trigger(s) for the UP function to send a report to the CP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 37 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | LIUSA | DROTH | STOPT | START | QUHTI | TIMTH | VOLTH | PERIO |
| 6 | Spare | Spare | Spare | Spare | Spare | ENVCL | TIMQU | VOLQU |
| 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.19-1: Reporting Triggers**

Octet 5 shall be encoded as follows:

- Bit 1 – PERIO (Periodic Reporting): when set to 1, this indicates a request for periodic reporting.
- Bit 2 – VOLTH (Volume Threshold): when set to 1, this indicates a request for reporting when the data volume usage reaches a volume threshold
- Bit 3 – TIMTH (Time Threshold): when set to 1, this indicates a request for reporting when the time usage reaches a time threshold.
- Bit 4 – QUHTI (Quota Holding Time): when set to 1, this indicates a request for reporting when no packets have been received for a period exceeding the Quota Holding Time.
- Bit 5 – START (Start of Traffic): when set to 1, this indicates a request for reporting when detecting the start of an SDF or Application traffic.
- Bit 6 – STOPT (Stop of Traffic): when set to 1, this indicates a request for reporting when detecting the stop of an SDF or Application Traffic.
- Bit 7 - DROTH (Dropped DL Traffic Threshold): when set to 1, this indicates a request for reporting when the DL traffic being dropped reaches a threshold.
- Bit 8: - LIUSA (Linked Usage Reporting): when set to 1, this indicates a request for linked usage reporting, i.e. a request for reporting a usage report for a URR when a usage report is reported for a linked URR (see subclause 5.2.2.4).

Octet 6 shall be encoded as follows:

- Bit 1 –VOLQU (Volume Quota): when set to 1, this indicates a request for reporting when a Volume Quota is exhausted.
- Bit 2 – TIMQU (Time Quota): when set to 1, this indicates a request for reporting when a Time Quota is exhausted.
- Bit 3 – ENVCL (Envelope Closure): when set to 1, this indicates a request for reporting when conditions for closure of envelope is met (see subclause 5.2.2.3).
- Bits 4 to 8: Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

## 8.2.20 Redirect Information

Redirect Information is coded as depicted in Figure 8.2.20-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1-2 | Type = 38 (decimal) | | | | | | | |
| 3-4 | Length = n | | | | | | | |
| 5 | Spare | | | | | Redirect Address Type | | |
| 6-7 | Redirect Server Address Length=a | | | | | | | |
| 8-(8+a) | Redirect Server Address | | | | | | | |
| (8+a+1) to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.20-1: Redirect Information**

Redirect Address Type indicates the type of the Redirect Address. It shall be encoded as defined in Table 8.2.20-1.

**Table 8.2.20-1: Redirect Address Type**

| Redirect Address Type | Value (Decimal) |
|---|---|
| IPv4 address | 0 |
| IPv6 address | 1 |
| URL | 2 |
| SIP URI | 3 |
| Spare, for future use. | 4 to 15 |

The Redirect Server Address Length shall indicate the length of the Redirect Server Address.

The Redirect Server Address shall be encoded in UTF8String format and shall contain the address of the redirect server (e.g. HTTP redirect server, SIP server) with which the end user is to be connected, as specified in subclauses 8.38 and 8.39 of IETF RFC 4006 [16].

## 8.2.21 Report Type

The Report Type IE shall be encoded as shown in Figure 8.2.21-1. It indicates the type of the report the UP function sends to the CP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 39 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | ERIR | USAR | DLDR |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.21-1: Report Type**

Octet 5 shall be encoded as follows:

- Bit 1 – DLDR (Downlink Data Report): when set to 1, this indicates Downlink Data Report

- Bit 2 – USAR (Usage Report): when set to 1, this indicates a Usage Report
- Bit 3 – ERIR (Error Indication Report): when set to 1, this indicates an Error Indication Report.
- Bit 4 to 8 – Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

## 8.2.22 Offending IE

Offending IE IE is coded as depicted in Figure 8.2.22-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 40 (decimal) | | | | | | | |
| 3 to 4 | Length = 2 | | | | | | | |
| 5 to 6 | Type of the offending IE | | | | | | | |

**Figure 8.2.22-1: Offending IE**

The offending IE shall contain a mandatory IE type, if the rejection is due to a conditional or mandatory IE is faulty or missing.

## 8.2.23 Forwarding Policy

The Forwarding Policy IE type shall be encoded as shown in Figure 8.2.23-1. It indicates a specific forwarding policy to apply to packets.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 41 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Forwarding Policy Identifier Length | | | | | | | |
| j to k | Forwarding Policy Identifier | | | | | | | |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.23-1: Forwarding Policy**

The Forwarding Policy Identifier Length shall indicate the length of the Forwarding Policy Identifier.

The Forwarding Policy Identifier shall be encoded as an Octet String containing a reference to a pre-configured Forwarding Policy in the UP function, with a maximum length of 255 octets.

## 8.2.24 Destination Interface

The Destination Interface IE type shall be encoded as shown in Figure 8.2.24-1. It indicates the type of the interface towards which an outgoing packet is sent.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 42 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | Interface value | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.24-1: Destination Interface**

The Interface value shall be encoded as a 4 bits binary integer as specified in Table 8.2.24-1.

**Table 8.2.24-1: Interface value**

| Interface value | Values (Decimal) |
|---|---|
| Access (see NOTE 1) | 0 |
| Core (see NOTE 1) | 1 |
| SGi-LAN | 2 |
| CP- Function | 3 |
| LI Function (see NOTE 2) | 4 |
| Spare | 5 to 15 |
| NOTE 1: The "Access" and "Core" values denote a downlink and uplink traffic direction respectively.<br>NOTE 2: LI Function may denote an SX3LIF or an LMISF. See subclause 5.7. | |

## 8.2.25 UP Function Features

The UP Function Features IE indicates the features supported by the UP function. It is coded as depicted in Figure 8.2.25-1.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 43 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 6 | Supported-Features | | | | | | | |
| 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.25-1: UP Function Features**

The UP Function Features IE takes the form of a bitmask where each bit set indicates that the corresponding feature is supported. Spare bits shall be ignored by the receiver. The same bitmask is defined for all PFCP interfaces.

The following table specifies the features defined on PFCP interfaces and the interfaces on which they apply.

**Table 8.2.25-1: UP Function Features**

| Feature Octet / Bit | Feature | Interface | Description |
|---|---|---|---|
| 5/1 | BUCP | Sxa | Downlink Data Buffering in CP function is supported by the UP function. |
| 5/2 | DDND | Sxa | The buffering parameter 'Downlink Data Notification Delay' is supported by the UP function. |
| 5/3 | DLBD | Sxa | The buffering parameter 'DL Buffering Duration' is supported by the UP function. |
| 5/4 | TRST | Sxb, Sxc | Traffic Steering is supported by the UP function. |
| 5/5 | FTUP | Sxa, Sxb | F-TEID allocation / release in the UP function is supported by the UP function. |
| 5/6 | PFDM | Sxb, Sxc | The PFD Management procedure is supported by the UP function. |
| 5/7 | HEEU | Sxb, Sxc | Header Enrichment of Uplink traffic is supported by the UP function. |
| 5/8 | TREU | Sxb, Sxc | Traffic Redirection Enforcement in the UP function is supported by the UP function. |
| 6/1 | EMPU | Sxa, Sxb | Sending of End Marker packets supported by the UP function. |
| Feature Octet / Bit: The octet and bit number within the Supported-Features IE, e.g. "5 / 1".<br>Feature: A short name that can be used to refer to the octet / bit and to the feature.<br>Interface: A list of applicable interfaces to the feature.<br>Description: A clear textual description of the feature. | | | |

## 8.2.26 Apply Action

The Apply Action IE indicates the action(s) the UP function is required to apply to packets. It is coded as shown in Figure 8.2.26-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 44 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | DUPL | NOCP | BUFF | FORW | DROP |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.26-1: Apply-Action**

The octet 5 shall be encoded as follows:

- Bit 1 – DROP (Drop): when set to 1, this indicates a request to drop the packets.
- Bit 2 – FORW (Forward): when set to 1, this indicates a request to forward the packets.
- Bit 3 – BUFF (Buffer): when set to 1, this indicates a request to buffer the packets.
- Bit 4 – NOCP (Notify the CP function): when set to 1, this indicates a request to notify the CP function about the arrival of a first downlink packet being buffered.
- Bit 5 – DUPL (Duplicate): when set to 1, this indicates a request to duplicate the packets.
- Bit 6 to 8 – Spare, for future use and set to 0.

One and only one of the DROP, FORW and BUFF flags shall be set to 1.

The NOCP flag may only be set if the BUFF flag is set.

The DUPL flag may be set with any of the DROP, FORW, BUFF and NOCP flags.

## 8.2.27 Downlink Data Service Information

The Downlink Data Service Information IE is used to carry downlink data service information. It is coded as shown in Figure 8.2.27-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 45 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | PPI |
| m | Spare | | Paging Policy Indication value | | | | | |
| p to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.27-1: Downlink Data Service Information**

The PPI flag in octet 5 indicates whether the Paging Policy Indication value in octet 'm' shall be present. If PPI is set to '1', then the Paging Policy Indication value shall be present. If PPI is set to '0', then octet 'm' shall not be present.

The Paging Policy Indication value, in octet 'm', shall be encoded as the DSCP in TOS (IPv4) or TC (IPv6) information received in the IP payload of the GTP-U packet from the PGW (see IETF RFC 2474 [13]).

## 8.2.28 Downlink Data Notification Delay

The Downlink Data Notification Delay IE indicates the delay the UP function shall apply between receiving a downlink data packet and notifying the CP function about the arrival of the packet. It is coded as depicted in Figure 8.2.28-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 46 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Delay Value in integer multiples of 50 millisecs, or zero | | | | | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.28-1: Downlink Data Notification Delay**

Delay Value shall be set to zero in order to clear a previously set delay condition.

## 8.2.29 DL Buffering Duration

The DL Buffering Duration IE indicates the duration during which the UP function is requested to buffer the downlink data packets. It is coded as shown in figure 8.2.29-1 and table 8.2.29.1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 47 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Timer unit | | | Timer value | | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.29-1: DL Buffering Duration**

**Table 8.2.29.1: DL Buffering Duration**

| |
|---|
| Timer value<br>Bits 5 to 1 represent the binary coded timer value.<br><br>Timer unit<br>Bits 6 to 8 defines the timer value unit as follows:<br>Bits<br>**8 7 6**<br>0 0 0 value is incremented in multiples of 2 seconds<br>0 0 1 value is incremented in multiples of 1 minute<br>0 1 0 value is incremented in multiples of 10 minutes<br>0 1 1 value is incremented in multiples of 1 hour<br>1 0 0 value is incremented in multiples of 10 hours<br>1 1 1 value indicates that the timer is infinite<br><br>Other values shall be interpreted as multiples of 1 minute in this version of the protocol.<br><br>Timer unit and Timer value both set to all "zeros" shall be interpreted as an indication that the timer is stopped. |

## 8.2.30 DL Buffering Suggested Packet Count

The DL Buffering Suggested Packet Count IE indicates the maximum number of downlink data packets suggested to be buffered in the UP function for this Sx session. It is coded as depicted in Figure 8.2.30-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 48 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to n+4 | Packet Count Value | | | | | | | |

**Figure 8.2.30-1: DL Buffering Suggested Packet Count**

The Packet Count value is encoded with the number of octets defined in the Length field, e.g. when n=2, the range of the Packet Count value is from 0 to 65535.

The length shall be set to 1 or 2 octets.

## 8.2.31 SxSMReq-Flags

The SxSMReq-Flags IE indicates flags applicable to the Sx Session Modification Request message. It is coded as depicted in Figure 8.2.31-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 49 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | QAURR | SNDEM | DROBU |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.31-1: SxSMReq-Flags**

The following bits within Octet 5 shall indicate:

- Bit 1 – DROBU (Drop Buffered Packets): if this bit is set to 1, it indicates that the UP function shall drop all the packets currently buffered for the Sx session, if any, prior to further applying the action specified in the Apply Action value of the FARs.

- Bit 2 – SNDEM (Send End Marker Packets): if this bit is set to 1, it indicates that the UP function shall construct and send End Marker packets towards the old F-TEID of the downstream node when switching to the new F-TEID.

- Bit 3 – QAURR (Query All URRs): if this bit is set to 1, it indicates that the UP function shall return immediate usage report(s) for all the URRs previously provisioned for this Sx session.

- Bit 4 to 8 – Spare, for future use, shall be set to 0 by the sender and discarded by the receiver.

8.2.32 SxSRRsp-Flags

The SxSRRsp-Flags IE indicates flags applicable to the Sx Session Report Response message. It is coded as depicted in Figure 8.2.32-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 50 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | Spare | Spare | DROBU |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.32-1: SxSRRsp-Flags**

The following bits within Octet 5 shall indicate:

- Bit 1 – DROBU (Drop Buffered Packets): if this bit is set to 1, it indicates that the UP function shall drop all the packets currently buffered for the Sx session, if any, prior to further applying the action specified in the Apply Action value of the FARs.

- Bit 2 to 8 – Spare, for future use, shall be set to 0 by the sender and discarded by the receiver.

## 8.2.33 Sequence Number

The Sequence Number IE shall be encoded as shown in Figure 8.2.33-1. It contains an Unsigned32 binary integer value.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 52 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Sequence Number | | | | | | | |

**Figure 8.2.33-1: Sequence Number**

## 8.2.34 Metric

The Metric IE shall be encoded as shown in Figure 8.2.34-1. It indicates a percentage and may take binary coded integer values from and including 0 up to and including 100. Other values shall be considered as 0.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 53 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Metric | | | | | | | |

**Figure 8.2.34-1: Metric**

## 8.2.35 Timer

The purpose of the Timer IE is to specify specific timer values. The Timer IE shall be encoded as shown in Figure 8.2.35-1 and table 8.2.35.1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 55 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Timer unit | | | Timer value | | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.35-1: Timer**

**Table 8.2.35.1: Timer information element**

Timer value
Bits 5 to 1 represent the binary coded timer value.

Timer unit
Bits 6 to 8 defines the timer value unit for the timer as follows:
Bits
**8 7 6**
0 0 0 value is incremented in multiples of 2 seconds
0 0 1 value is incremented in multiples of 1 minute
0 1 0 value is incremented in multiples of 10 minutes
0 1 1 value is incremented in multiples of 1 hour
1 0 0 value is incremented in multiples of 10 hours
1 1 1 value indicates that the timer is infinite

Other values shall be interpreted as multiples of 1 minute in this version of the protocol.

Timer unit and Timer value both set to all "zeros" shall be interpreted as an indication that the timer is stopped.

## 8.2.36 Packet Detection Rule ID (PDR ID)

The PDR ID IE is coded as depicted in Figure 8.2.36-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 56 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 6 | Rule ID | | | | | | | |
| 7to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.36-1: PDR ID**

Octets 5 to 6 contain the Rule ID and shall be encoded as an integer.

## 8.2.37 F-SEID

F-SEID is coded as depicted in Figure 8.2.37-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 57 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | Spare | V4 | V6 |
| 6 to 13 | SEID | | | | | | | |
| m to (m+3) | IPv4 address | | | | | | | |
| p to (p+15) | IPv6 address | | | | | | | |
| k to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.37-1: F-SEID**

The following flags are coded within Octet 5:

- Bit 1 – V6: If this bit is set to "1", then IPv6 address field shall be present in the F-SEID, otherwise the IPv6 address field is not present at all.
- Bit 2 – V4: If this bit is set to "1", then IPv4 address field shall be present in the F-SEID, otherwise the IPv4 address field is not present at all.
- Bit 3 to 8 are spare and reserved for future use.

At least one of V4 and V6 shall be set to "1", and both may be set to "1".

Octets "m to (m+3)" and/or "p to (p+15)" (IPv4 address / IPv6 address fields), if present, contain respective address values.

## 8.2.38 Node ID

The Node ID IE shall contain an FQDN or an IPv4/IPv6 address. It shall be encoded as shown in Figure 8.2.38-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 60 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | Node ID Type | | | |
| 6 to o | Node ID value | | | | | | | |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.38-1: Node ID**

Node ID Type indicates the type of the Node ID value. It shall be encoded as a 4 bits binary integer as specified in Table 8.2.38-2.

**Table 8.2.38-2: Node ID Type**

| Node ID Type Value (Decimal) | Node ID Type |
|---|---|
| 0 | IPv4 address |
| 1 | IPv6 address |
| 2 | FQDN |
| 3 to 15 | Spare, for future use. |

If the Node ID is an IPv4 address, the Node ID value length shall be 4 Octet.

If the Node ID is an IPv6 address, the Node ID value length shall be 16 Octet.

If the Node ID is an FQDN, the Node ID value encoding shall be identical to the encoding of a FQDN within a DNS message of section 3.1 of IETF RFC 1035 [27] but excluding the trailing zero byte.

NOTE 1: The FQDN field in the IE is not encoded as a dotted string as commonly used in DNS master zone files.

## 8.2.39 PFD Contents

The PFD Contents IE type shall be encoded as shown in Figure 8.2.39-1. It contains the description of a PFD.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 61 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | CP | DN | URL | FD |
| 6 | Spare | | | | | | | |
| m to (m+1) | Length of Flow Description | | | | | | | |
| (m+2) to p | Flow Description | | | | | | | |
| q to (q+1) | Length of URL | | | | | | | |
| (q+2) to r | URL | | | | | | | |
| s to (s+1) | Length of Domain Name | | | | | | | |
| (s+2) to t | Domain Name | | | | | | | |
| u to (u+1) | Length of Custom PFD Content | | | | | | | |
| (u+2) to v | Custom PFD Content | | | | | | | |
| w to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.39-1: PFD Contents**

The following flags are coded within Octet 5:

- Bit 1 – FD (Flow Description): If this bit is set to "1", then the Length of Flow Description and the Flow Description fields shall be present, otherwise they shall not be present.

- Bit 2 – URL (URL): If this bit is set to "1", then the Length of URL and the URL fields shall be present, otherwise they shall not be present.

- Bit 3 – DN (Domain Name): If this bit is set to "1", then the Length of Domain Name and the Domain Name fields shall be present, otherwise they shall not be present.

- Bit 4 – CP (Custom PFD Content): If this bit is set to "1", then the Length of Custom PFD Content and the Custom PFD Content fields shall be present, otherwise they shall not be present.

- Bit 5 to 8: Spare, for future use and set to 0.

The Flow Description field, when present, shall be encoded as an OctetString as specified in subclause 6.4.3.7 of 3GPP TS 29.251 [21].

The Domain Name field, when present, shall be encoded as an OctetString as specified in subclause 6.4.3.9 of 3GPP TS 29.251 [21].

The URL field, when present, shall be encoded as an OctetString as specified in subclause 6.4.3.8 of 3GPP TS 29.251 [21].

## 8.2.40 Measurement Method

The Measurement Method IE shall be encoded as shown in Figure 8.2.40-1. It indicates the method for measuring the usage of network resources.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 62 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | EVENT | VOLUM | DURAT |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.40-1: Measurement Method**

Octet 5 shall be encoded as follows:

- Bit 1 – DURAT (Duration): when set to 1, this indicates a request for measuring the duration of the traffic.
- Bit 2 – VOLUM (Volume): when set to 1, this indicates a request for measuring the volume of the traffic.
- Bit 3 – EVENT (Event): when set to 1, this indicates a request for measuring the events.
- Bit 4 to 8: Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

## 8.2.41 Usage Report Trigger

The Usage Report Trigger IE shall be encoded as shown in Figure 8.2.41-1. It indicates the trigger of the usage report.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 63 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | IMMER | DROTH | STOPT | START | QUHTI | TIMTH | VOLTH | PERIO |
| 6 | Spare | Spare | ENVCL | MONIT | TERMR | LIUSA | TIMQU | VOLQU |
| 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.41-1: Usage Report Trigger**

Octet 5 shall be encoded as follows:

- Bit 1 – PERIO (Periodic Reporting): when set to 1, this indicates a periodic report.
- Bit 2 – VOLTH (Volume Threshold): when set to 1, this indicates that the data volume usage reaches a volume threshold.
- Bit 3 – TIMTH (Time Threshold): when set to 1, this indicates that the time usage reaches a volume threshold.
- Bit 4 – QUHTI (Quota Holding Time): when set to 1, this indicates that no packets have been received for a period exceeding the Quota Holding Time.
- Bit 5 – START (Start of Traffic): when set to 1, this indicates that the start of traffic is detected.

- Bit 6 – STOPT (Stop of Traffic): when set to 1, this indicates that the stop of traffic is detected.
- Bit 7 - DROTH (Dropped DL Traffic Threshold): when set to 1, this indicates that the DL traffic being dropped reaches a threshold.
- Bit 8 – IMMER (Immediate Report): when set to 1, this indicates an immediate report reported on CP function demand.

Octet 6 shall be encoded as follows:

- Bit 1 – VOLQU (Volume Quota): when set to 1, this indicates that the Volume Quota has been exhausted.
- Bit 2 – TIMQU (Time Quota): when set to 1, this indicates that the Time Quota has been exhausted.
- Bit 3 - LIUSA (Linked Usage Reporting): when set to 1, this indicates a linked usage report, i.e. a usage report being reported for a URR due to a usage report being also reported for a linked URR (see subclause 5.2.2.4).
- Bit 4 – TERMR (Termination Report): when set to 1, this indicates a usage report being reported (in a Sx Session Deletion Response) for a URR due to the termination of the Sx session, or a usage report being reported (in a Sx Session Modification Response) for a URR due to the removal of the URR.
- Bit 5 – MONIT (Monitoring Time): when set to 1, this indicates a usage report being reported for a URR due to the Monitoring Time being reached.
- Bit 6 – ENVCL (Envelope Closure): when set to 1, this indicates the usage report is generated for closure of an envelope (see subclause 5.2.2.3).
- Bits 7 to 8: Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

## 8.2.42 Measurement Period

The Measurement Period IE contains the period, in seconds, for generating periodic usage reports. It shall be encoded as shown in Figure 8.2.42-1.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 64 (decimal) |
| 3 to 4 | Length = n |
| 5 to 8 | Measurement Period |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.42-1: Measurement Period**

The Measurement Period field shall be encoded as an Unsigned32 binary integer value.

## 8.2.43 Fully qualified PDN Connection Set Identifier (FQ-CSID)

A fully qualified PDN Connection Set Identifier (FQ-CSID) identifies a set of PDN connections belonging to an arbitrary number of UEs on a SGW-C, PGW-C, SGW-U and PGW-U. The FQ-CSID is used on Sxa and Sxb interfaces.

The size of CSID is two octets. The FQ-CSID is coded as follows:

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 65 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | FQ-CSID Node-ID Type | | | | Number of CSIDs= m | | | |
| 6 to p | Node-Address | | | | | | | |
| (p+1) to (p+2) | First PDN Connection Set Identifier (CSID) | | | | | | | |
| (p+3) to (p+4) | Second PDN Connection Set Identifier (CSID) | | | | | | | |
| ... | ... | | | | | | | |
| q to q+1 | m-th PDN Connection Set Identifier (CSID) | | | | | | | |
| (q+2) to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.43-1: FQ-CSID**

Where FQ-CSID Node-ID Type values are:

0 indicates that Node-Address is a global unicast IPv4 address and p = 9.

1 indicates that Node-Address is a global unicast IPv6 address and p = 21.

2 indicates that Node-Address is a 4 octets long field with a 32 bit value stored in network order, and p= 9. The coding of the field is specified below:

- Most significant 20 bits are the binary encoded value of (MCC * 1000 + MNC).
- Least significant 12 bits is a 12 bit integer assigned by an operator to an MME, SGW-C, SGW-U, PGW-C or PGW-U. Other values of Node-Address Type are reserved.

Values of Number of CSID other than 1 are only employed in the Sx Session Delete Request.

The node that creates the FQ-CSID (i.e. SGW-C for SGW-C FQ-CSID, SGW-U for SGW-U FQ-CSID, PGW-C for PGW-C FQ-CSID and PGW-U for PGW-U FQ-CSID) needs to ensure that the Node-ID is globally unique and the CSID value is unique within that node.

## 8.2.44 Volume Measurement

The Volume Measurement IE contains the measured traffic volumes. It shall be encoded as shown in Figure 8.2.44-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 66 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | DLVOL | ULVOL | TOVOL |
| m to (m+7) | Total Volume | | | | | | | |
| p to (p+7) | Uplink Volume | | | | | | | |
| q to (q+7) | Downlink Volume | | | | | | | |
| s to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.44-1: Volume Measurement**

The following flags are coded within Octet 5:

- Bit 1 – TOVOL: If this bit is set to "1", then the Total Volume field shall be present, otherwise the Total Volume field shall not be present.
- Bit 2 – ULVOL: If this bit is set to "1", then the Uplink Volume field shall be present, otherwise the Uplink Volume field shall not be present.

- Bit 3 – DLVOL: If this bit is set to "1", then the Downlink Volume field shall be present, otherwise the Downlink Volume field shall not be present.

- Bit 4 to bit 8: Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

The Total Volume, Uplink Volume and Downlink Volume fields shall be encoded as an Unsigned64 binary integer value. They shall contain the total, uplink or downlink number of octets respectively.

## 8.2.45 Duration Measurement

The Duration Measurement IE type shall be encoded as shown in Figure 8.2.45-1. It contains the used time in seconds.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 67 (decimal) |
| 3 to 4 | Length = n |
| 5 to 8 | Duration value |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.45-1: Duration Measurement**

The Duration value shall be encoded as an Unsigned32 binary integer value.

## 8.2.46 Time of First Packet

The Time of First Packet IE indicates the time stamp for the first IP packet transmitted for a given usage report. It shall be encoded as shown in Figure 8.2.46-1.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 69 (decimal) |
| 3 to 4 | Length = n |
| 5 to 8 | Time of First Packet |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.46-1: Time of First Packet**

The Time of First Packet field shall contain a UTC time. Octets 5 to 8 shall be encoded in the same format as the first four octets of the 64-bit timestamp format as defined in section 6 of IETF RFC 5905 [12].

NOTE: The encoding is defined as the time in seconds relative to 00:00:00 on 1 January 1900.

## 8.2.47 Time of Last Packet

The Time of Last Packet IE indicates the time stamp for the last IP packet transmitted for a given usage report. It shall be encoded as shown in Figure 8.2.47-1.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 70 (decimal) |
| 3 to 4 | Length = n |
| 5 to 8 | Time of Last Packet |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.47-1: Time of Last Packet**

The Time of Last Packet field shall contain a UTC time. Octets 5 to 8 shall be encoded in the same format as the first four octets of the 64-bit timestamp format as defined in section 6 of IETF RFC 5905 [12].

NOTE: The encoding is defined as the time in seconds relative to 00:00:00 on 1 January 1900.

## 8.2.48 Quota Holding Time

The Quota Holding Time IE type shall be encoded as shown in Figure 8.2.48-1. It contains the quota holding time in seconds.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 71 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Quota Holding Time value | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.48-1: Quota Holding Time**

The Quota Holding Time value shall be encoded as an Unsigned32 binary integer value.

## 8.2.49 Dropped DL Traffic Threshold

The Dropped DL Traffic Threshold IE type shall be encoded as shown in Figure 8.2.49-1. It contains the dropped DL traffic volume thresholds to be monitored by the UP function.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 72 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | DLPA |
| m to (m+7) | Downlink Packets | | | | | | | |
| s to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.49-1: Dropped DL Traffic Threshold**

The following flags are coded within Octet 5:

- Bit 1 – DLPA: If this bit is set to "1", then the Downlink Packets field shall be present, otherwise the Downlink Packets field shall not be present.

- Bit 2 to 8: Spare, for future use and set to 0.

The Downlink Packets fields shall be encoded as an Unsigned64 binary integer value. It shall contain a number of downlink packets.

## 8.2.50 Volume Quota

The Volume Quota IE type shall be encoded as shown in Figure 8.2.50-1. It contains the volume quota to be monitored by the UP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 73 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | DLVOL | ULVOL | TOVOL |
| m to (m+7) | Total Volume | | | | | | | |
| p to (p+7) | Uplink Volume | | | | | | | |
| q to (q+7) | Downlink Volume | | | | | | | |
| S to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.50-1: Volume Quota**

The following flags are coded within Octet 5:

- Bit 1 – TOVOL: If this bit is set to "1", then the Total Volume field shall be present, otherwise the Total Volume field shall not be present.
- Bit 2 – ULVOL: If this bit is set to "1", then the Uplink Volume field shall be present, otherwise the Uplink Volume field shall not be present.
- Bit 3 – DLVOL: If this bit is set to "1", then the Downlink Volume field shall be present, otherwise the Downlink Volume field shall not be present.
- Bit 4 to bit 8: Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

The Total Volume, Uplink Volume and Downlink Volume fields shall be encoded as an Unsigned64 binary integer value. They shall contain the total, uplink or downlink number of octets respectively.

## 8.2.51 Time Quota

The Time Quota IE type shall be encoded as shown in Figure 8.2.51-1. It contains the time quota to be monitored by the UP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 74 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Time Quota value | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.51-1: Time Quota**

The Time Quota value shall be encoded as an Unsigned32 binary integer value. It contains a duration in seconds.

## 8.2.52 Start Time

The Start Time IE indicates the time at which the UP function started to collect the charging information. It shall be encoded as shown in Figure 8.2.52-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 75 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Start Time | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.52-1: Start Time**

The Start Time field shall contain a UTC time. Octets 5 to 8 shall be encoded in the same format as the first four octets of the 64-bit timestamp format as defined in section 6 of IETF RFC 5905 [12].

NOTE: The encoding is defined as the time in seconds relative to 00:00:00 on 1 January 1900.

## 8.2.53 End Time

The End Time IE indicates the time at which the UP function ended to collect the charging information. It shall be encoded as shown in Figure 8.2.53-1.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 76 (decimal) |
| 3 to 4 | Length = n |
| 5 to 8 | End Time |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.53-1: End Time**

The End Time field shall contain a UTC time. Octets 5 to 8 shall be encoded in the same format as the first four octets of the 64-bit timestamp format as defined in section 6 of IETF RFC 5905 [12].

NOTE: The encoding is defined as the time in seconds relative to 00:00:00 on 1 January 1900.

## 8.2.54 URR ID

The URR ID IE type shall be encoded as shown in Figure 8.2.54-1. It contains a Usage Reporting Rule ID.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 81 (decimal) |
| 3 to 4 | Length = n |
| 5 to 8 | URR ID value |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.54-1: URR ID**

The URR ID value shall be encoded as an Unsigned32 binary integer value.

The bit 8 of octet 5 is used to indicate if the Rule ID is dynamically allocated by the CP function or predefined in the UP function. If set to 0, it indicates that the Rule is dynamically provisioned by the CP Function. If set to 1, it indicates that the Rule is predefined in the UP Function.

## 8.2.55 Linked URR ID IE

The Linked URR ID IE type shall be encoded as shown in Figure 8.2.55-1. It contains the URR ID of a linked URR.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 82 (decimal) |
| 3 to 4 | Length = n |
| 5 to 8 | Linked URR ID value |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.55-1: Linked URR ID**

The Linked URR ID value shall be encoded as an Unsigned32 binary integer value.

## 8.2.56 Outer Header Creation

The Outer Header Creation IE type shall be encoded as shown in Figure 8.2.56-1. It contains the instructions to create an Outer Header.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 84 (decimal) |
| 3 to 4 | Length = n |
| 5 | Outer Header Creation Description |
| m to (m+3) | TEID |
| p to (p+3) | IPv4 Address |
| q to (q+15) | IPv6 Address |
| r to (r+1) | Port Number |
| s to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.56-1: Outer Header Creation**

The Outer Header Creation Description field, when present, shall be encoded as specified in Table 8.2.56-1.

**Table 8.2.56-1: Outer Header Creation Description**

| Outer Header to be created in the outgoing packet | Value (Decimal) |
|---|---|
| GTP-U/UDP/IPv4 (see NOTE 1) | 0 |
| GTP-U/UDP/IPv6 (see NOTE 1) | 1 |
| UDP/IPv4 (see NOTE 3) | 2 |
| UDP/IPv6 (see NOTE 3) | 3 |
| For future use. Shall not be sent. If received, shall be interpreted as the value "1". | 4 to 255 |
| NOTE 1: The SGW-U shall also create GTP-U extension header(s) if any has been stored for this packet, during a previous outer header removal (see subclause 8.2.64).<br>NOTE 2: This value may apply to UL packets sent by a PGW-U for non-IP PDN connections with SGi tunnelling based on UDP/IP encapsulation (see subclause 4.3.17.8.3.3.2 of 3GPP TS 23.401 [14]). | |

The TEID field shall be present if the Outer Header Creation Description requests the creation of a GTP-U header. Otherwise it shall not be present. When present, it shall contain the destination GTP-U TEID to set in the GTP-U header of the outgoing packet.

The IPv4 Address field shall be present if the Outer Header Creation Description requests the creation of a IPv4 header. Otherwise it shall not be present. When present, it shall contain the destination IPv4 address to set in the IPv4 header of the outgoing packet.

The IPv6 Address field shall be present if the Outer Header Creation Description requests the creation of a IPv6 header. Otherwise it shall not be present. When present, it shall contain the destination IPv6 address to set in the IPv6 header of the outgoing packet.

The Port Number field shall be present if the Outer Header Creation Description requests the creation of a UDP/IP header (i.e. it is set to the value 4). Otherwise it shall not be present. When present, it shall contain the destination Port Number to set in the UDP header of the outgoing packet.

## 8.2.57 BAR ID

The BAR ID IE type shall be encoded as shown in Figure 8.2.57-1. It contains a Buffering Action Rule ID.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 88 (decimal) |
| 3 to 4 | Length = n |
| 5 | BAR ID value |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.57-1: BAR ID**

The BAR ID value shall be encoded as a binary integer value.

## 8.2.58 CP Function Features

The CP Function Features IE indicates the features supported by the CP function. Only features having an impact on the (system-wide) UP function behaviour are signalled in this IE. It is coded as depicted in Figure 8.2.58-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 89 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Supported-Features | | | | | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.58-1: CP Function Features**

The CP Function Features IE takes the form of a bitmask where each bit set indicates that the corresponding feature is supported. Spare bits shall be ignored by the receiver. The same bitmask is defined for all PFCP interfaces.

The following table specifies the features defined on PFCP interfaces and the interfaces on which they apply.

**Table 8.2.58-1: CP Function Features**

| Feature Octet / Bit | Feature | Interface | Description |
|---|---|---|---|
| 5/1 | LOAD | Sxa, Sxb, Sxc | Load Control is supported by the CP function. |
| 5/2 | OVRL | Sxa, Sxb, Sxc | Overload Control is supported by the CP function. |
| Feature Octet / Bit: The octet and bit number within the Supported-Features IE, e.g. "5 / 1".<br>Feature: A short name that can be used to refer to the octet / bit and to the feature.<br>Interface: A list of applicable interfaces to the feature.<br>Description: A clear textual description of the feature. | | | |

## 8.2.59 Usage Information

The Usage Information IE shall be encoded as shown in Figure 8.2.59-1. It provides additional information on the Usage Report.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 90 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | UBE | UAE | AFT | BEF |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.59-1: Usage Information**

Octet 5 shall be encoded as follows:

- Bit 1 – BEF (Before): when set to 1, this indicates usage before a monitoring time.
- Bit 2 – AFT (After): when set to 1, this indicates a usage after a monitoring time.
- Bit 3 – UAE (Usage After Enforcement): when set to 1, this indicates a usage after QoS enforcement.
- Bit 4 – UBE (Usage Before Enforcement): when set to 1, this indicates a usage before QoS enforcement.
- Bits 5 to 8: Spare, for future use and set to 0.

## 8.2.60 Application Instance ID

The Application Instance ID IE type shall be encoded as shown in Figure 8.2.60-1. It contains an Application Instance Identifier referencing an application instance for which the start or stop of traffic is reported to the CP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 91 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Application Instance Identifier | | | | | | | |

**Figure 8.2.60-1: Application Instance ID**

The Application Instance Identifier shall be encoded as an OctetString (see 3GPP TS 29.212 [8]).

## 8.2.61 Flow Information

The Flow Information IE type shall be encoded as shown in Figure 8.2.61-1. It contains the description of a flow information.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 92 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | Flow Direction | | |
| 6 to 7 | Length of Flow Description | | | | | | | |
| 8 to m | Flow Description | | | | | | | |
| p to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.61-1: Flow Information**

The Flow Direction field, when present, shall be encoded as defined in Table 8.2.61-1.

**Table 8.2.61-1: Flow Direction**

| Flow Direction | Value (Decimal) |
|---|---|
| Unspecified | 0 |
| Downlink (traffic to the UE) | 1 |
| Uplink (traffic from the UE) | 2 |
| Bidirectional | 3 |
| For future use. Shall not be sent. If received, shall be interpreted as the value "0". | 4 to 7 |

The Flow Description field, when present, shall be encoded as an OctetString as specified in subclause 5.4.2 of 3GPP TS 29.212 [8].

## 8.2.62 UE IP Address

The UE IP Address IE type shall be encoded as shown in Figure 8.2.62-1. It contains a source or destination IP address.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 93 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | S/D | V4 | V6 |
| m to (m+3) | IPv4 address | | | | | | | |
| p to (p+15) | IPv6 address | | | | | | | |
| k to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.62-1: UE IP Address**

The following flags are coded within Octet 5:

- Bit 1 – V6: If this bit is set to "1", then the IPv6 address field shall be present in the UE IP Address, otherwise the IPv6 address field shall not be present.
- Bit 2 – V4: If this bit is set to "1", then the IPv4 address field shall be present in the UE IP Address, otherwise the IPv4 address field shall not be present.
- Bit 3 – S/D: This bit is only applicable to the UE IP Address IE in the PDI IE. It shall be set to "0" and ignored by the receiver in IEs other than PDI IE. In the PDI IE, if this bit is set to "0", this indicates a Source IP address; if this bit is set to "1", this indicates a Destination IP address.
- Bit 4 to 8 Spare, for future use and set to 0.

Octets "m to (m+3)" or "p to (p+15)" (IPv4 address / IPv6 address fields), if present, shall contain the address value.

## 8.2.63 Packet Rate

The Packet Rate IE contains the packet rate thresholds to be enforced by the UP function. It shall be encoded as shown in Figure 8.2.63-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 94 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | DLPR | ULPR |
| m | Spare | | | | | Uplink Time Unit | | |
| (m+1) to (m+2) | Maximum Uplink Packet Rate | | | | | | | |
| p | Spare | | | | | Downlink Time Unit | | |
| (p+1) to (p+2) | Maximum Downlink Packet Rate | | | | | | | |
| q to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.63-1: Packet Rate**

The following flags are coded within Octet 5:

- Bit 1 – ULPR (Uplink Packet Rate): If this bit is set to "1", then octets m to (m+2) shall be present, otherwise these octets shall not be present.
- Bit 2 – DLPR (Downlink Packet Rate): If this bit is set to "1", then octets p to (p+2) shall be present, otherwise these octets shall not be present.
- Bit 3 to 8: Spare, for future use and set to 0.

At least one bit in Octet 5 shall be set to 1. Several bits may be set to 1.

When present, octets m to (m+2) indicate the maximum number of uplink packets allowed to be sent within the uplink time unit.

When present, octets p to (p+2) indicate the maximum number of downlink packets allowed to be sent within the downlink time unit.

**Table 8.2.63.1: Uplink/Downlink Time Unit**

| Uplink/Downlink Time unit<br>Bits 1 to 3 define the time unit as follows:<br>Bits<br>**3 2 1**<br>0 0 0 minute<br>0 0 1 6 minutes<br>0 1 0 hour<br>0 1 1 day<br>1 0 0 week<br><br>Other values shall be interpreted as 000 in this version of the protocol. |
|---|

The Maximum Uplink/Downlink Packet Rate shall be encoded as an Unsigned16 binary integer value. They shall indicate the maximum number of uplink/downlink packets allowed to be sent in the indicated uplink/downlink time unit respectively.

## 8.2.64 Outer Header Removal

The Outer Header Removal IE type shall be encoded as shown in Figure 8.2.64-1. It contains the instructions to remove an Outer Header.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 95 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Outer Header Removal Description | | | | | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.64-1: Outer Header Removal**

The Outer Header Removal Description field, when present, shall be encoded as specified in Table 8.2.64-1.

**Table 8.2.64-1: Outer Header Removal Description**

| Outer Header to be removed from the incoming packet | Value (Decimal) |
|---|---|
| GTP-U/UDP/IPv4 (see NOTE 1) | 0 |
| GTP-U/UDP/IPv6 (see NOTE 1) | 1 |
| UDP/IPv4 (See NOTE 3) | 2 |
| UDP/IPv6 (See NOTE 3) | 3 |
| For future use. Shall not be sent. If received, shall be interpreted as the value "1". | 4 to 255 |
| NOTE 1: The SGW-U shall store GTP-U extension header(s) required to be forwarded for this packet (as required by the comprehension rules of Figure 5.2.1-2 of 3GPP TS 29.281 [3]).<br>NOTE 3: This value may apply to DL packets received by a PGW-U for non-IP PDN connections with SGi tunnelling based on UDP/IP encapsulation (see subclause 4.3.17.8.3.3.2 of 3GPP TS 23.401 [14]). | |

## 8.2.65 Recovery Time Stamp

The Recovery Time Stamp IE is coded as shown in Figure 8.2.65-1. It indicates the UTC time when the node started. Octets 5 to 8 are encoded in the same format as the first four octets of the 64-bit timestamp format as defined in section 6 of IETF RFC 5905 [26].

NOTE: The encoding is defined as the time in seconds relative to 00:00:00 on 1 January 1900.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 96 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Recovery Time Stamp value | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.65-1: Recovery Time Stamp**

## 8.2.66 DL Flow Level Marking

The DL Flow Level Marking IE type shall be encoded as shown in Figure 8.2.66-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 97 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | SCI | TTC |
| m to (m+1) | ToS/Traffic Class | | | | | | | |
| p to (p+1) | Service Class Indicator | | | | | | | |
| q to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.66-1: DL Flow Level Marking**

The following flags are coded within Octet 5:

- Bit 1 – TTC (ToS/Traffic Class): If this bit is set to "1", then the ToS/Traffic Class field shall be present, otherwise the ToS/Traffic Class field shall not be present.
- Bit 2 – SCI (Service Class Indicator): If this bit is set to "1", then the Service Class Indicator field shall be present, otherwise the Service Class Indicator field shall not be present.
- Bit 3 to 8: Spare, for future use and set to 0.

The ToS/Traffic Class field, when present, shall be encoded on two octets as an OctetString. The first octet shall contain the IPv4 Type-of-Service or the IPv6 Traffic-Class field and the second octet shall contain the ToS/Traffic Class mask field. See subclause 5.3.15 of 3GPP TS 29.212 [8].

Octets p and (p+1) of the Service Class Indicator field, when present, shall be encoded respectively as octets 2 and 3 of the Service Class Indicator Extension Header specified in Figure 5.2.2.3-1 of 3GPP TS 29.281 [3].

## 8.2.67 Header Enrichment

The Header Enrichment IE type shall be encoded as shown in Figure 8.2.67-1. It contains information for header enrichment.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 98 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | Header Type | | | | |
| 6 | Length of Header Field Name | | | | | | | |
| 7 to m | Header Field Name | | | | | | | |
| p | Length of Header Field Value | | | | | | | |
| (p+1) to q | Header Field Value | | | | | | | |
| s to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.67-1: Header Enrichment**

Header Type indicates the type of the Header. It shall be encoded as defined in Table 8.2.67-1.

**Table 8.2.67-1: Header Type**

| Header Type | Value (Decimal) |
|---|---|
| HTTP | 0 |
| Spare, for future use. | 1 to 31 |

Length of Header Field Name indicates the length of the Header Field Name.

Header Field Name shall be encoded as an OctetString.

Length of Header Field Value indicates the length of the Header Field Value.

Header Field Value shall be encoded as an OctetString.

For a HTTP Header Type, the contents of the Header Field Name and Header Field Value shall comply with the HTTP header field format (see subclause 3.2 of IETF RFC 7230 [23]).

## 8.2.68 Measurement Information

The Measurement Information IE shall be encoded as shown in Figure 8.2.68-1. It provides information on the requested measurement information.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 100 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | INAM | MBQE |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.68-1: Measurement Information**

Octet 5 shall be encoded as follows:

- Bit 1 – MBQE (Measurement Before QoS Enforcement): when set to 1, this indicates a request to measure the traffic usage before QoS enforcement.
- Bit 2 – INAM (Inactive Measurement): when set to 1, this indicates that the measurement shall be paused (inactive).
- Bits 2 to 8: Spare, for future use and set to 0.

## 8.2.69 Node Report Type

The Node Report Type IE shall be encoded as shown in Figure 8.2.69-1. It indicates the type of the node report the UP function sends to the CP function.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 101 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | UPFR |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.69-1: Node Report Type**

Octet 5 shall be encoded as follows:

- Bit 1 – UPFR (User Plane Path Failure Report): when set to 1, this indicates a User Plane Path Failure Report.
- Bit 2 to 8 – Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

## 8.2.70 Remote GTP-U Peer

The Remote GTP-U Peer IE shall be encoded as depicted in Figure 8.2.70-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 103 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | V4 | V6 |
| m to (m+3) | IPv4 address | | | | | | | |
| p to (p+15) | IPv6 address | | | | | | | |
| k to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.70-1: Remote GTP-U Peer**

The following flags are coded within Octet 5:

- Bit 1 – V6: If this bit is set to "1", then the IPv6 address field shall be present, otherwise the IPv6 address field shall not be present.
- Bit 2 – V4: If this bit is set to "1", then the IPv4 address field shall be present, otherwise the IPv4 address field shall not be present.
- Bit 3 to 8 - Spare, for future use and set to 0.

Either the V4 or the V6 bit shall be set to "1".

Octets "m to (m+3)" and/or "p to (p+15)" (IPv4 address / IPv6 address fields), if present, shall contain the respective address values.

## 8.2.71 UR-SEQN

The UR-SEQN (Usage Report Sequence Number) IE identifies the order in which a usage report is generated for a given URR. It shall be encoded as shown in Figure 8.2.71-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 104 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | UR-SEQN | | | | | | | |

**Figure 8.2.71-1: UR-SEQN**

The UR-SEQN value shall be encoded as an Unsigned32 binary integer value.

## 8.2.72 Activate Predefined Rules

The Activate Predefined Rules IE type shall be coded as shown in Figure 8.2.72-1. It shall indicate a Predefined Rules Name, referring to one or more predefined rules which need to be activated in the UP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 106 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Predefined Rules Name | | | | | | | |

**Figure 8.2.72-1: Activate Predefined Rules**

The Predefined Rules Name field shall be encoded as an OctetString.

## 8.2.73 Deactivate Predefined Rules

The Deactivate Predefined Rules IE type shall be coded as shown in Figure 8.2.73-1. It shall indicate a Predefined Rules Name, referring to one or more predefined rules which need to be deactivated in the UP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 107 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Predefined Rules Name | | | | | | | |

**Figure 8.2.73-1: Deactivate Predefined Rules**

The Predefined Rules Name field shall be encoded as an OctetString.

## 8.2.74 FAR ID

The FAR ID IE type shall be encoded as shown in Figure 8.2.74-1. It shall contain a Forwarding Action Rule ID.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 108 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | FAR ID value | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.74-1: FAR ID**

The FAR ID value shall be encoded as an Unsigned32 binary integer value.

The bit 8 of octet 5 is used to indicate if the Rule ID is dynamically allocated by the CP function or predefined in the UP function. If set to 0, it indicates that the Rule is dynamically provisioned by the CP Function. If set to 1, it indicates that the Rule is predefined in the UP Function.

## 8.2.75 QER ID

The QER ID IE type shall be encoded as shown in Figure 8.2.75-1. It shall contain a QoS Enforcement Rule ID.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 109 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | QER ID value | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.75-1: QER ID**

The QER ID value shall be encoded as an Unsigned32 binary integer value.

The bit 8 of octet 5 is used to indicate if the Rule ID is dynamically allocated by the CP function or predefined in the UP function. If set to 0, it indicates that the Rule is dynamically provisioned by the CP Function. If set to 1, it indicates that the Rule is predefined in the UP Function.

## 8.2.76 OCI Flags

The OCI Flags IE shall contain the flags for overload control related information. It shall be encoded as shown in Figure 8.2.76-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 110 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | AOCI |
| s to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.76-1: OCI Flags**

The following flags are coded within Octet 5:

- Bit 1 – AOCI: Associate OCI with Node ID: The UP function shall set this flag to 1 if it has included the "Overload Control Information" and if this information is to be associated with the Node ID (i.e. FQDN or the IP address used during the UP function selection) of the serving UP function. This flag shall be set to 1 by the UP function, if the "Overload Control Information" is included in the Sx Session Establishment Response and the Cause IE is set to a rejection cause value.

- Bit 2 to 8: Spare, for future use and set to 0.

## 8.2.77 Sx Association Release Request

The Sx Association Release Request IE shall be encoded as shown in Figure 8.2.77-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 111 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | SARR |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.77-1: Sx Association Release Request**

The following flags are coded within Octet 5:

- Bit 1 – SARR (Sx Association Release Request): If this bit is set to "1", then the UP function requests the release of the Sx association.

- Bit 2 to 8: Spare, for future use and set to 0.

## 8.2.78 Graceful Release Period

The purpose of the Graceful Release Period IE is to specify a specific time for a graceful release. The Graceful Release Period IE shall be encoded as shown in Figure 8.2.78-1 and table 8.2.78.1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 112 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Timer unit | | | Timer value | | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.78-1: Graceful Release Period**

**Table 8.2.78.1: Graceful Release Period information element**

| |
|---|
| Timer value<br>Bits 5 to 1 represent the binary coded timer value.<br><br>Timer unit<br>Bits 6 to 8 defines the timer value unit for the timer as follows:<br>Bits<br>**8 7 6**<br>0 0 0 value is incremented in multiples of 2 seconds<br>0 0 1 value is incremented in multiples of 1 minute<br>0 1 0 value is incremented in multiples of 10 minutes<br>0 1 1 value is incremented in multiples of 1 hour<br>1 0 0 value is incremented in multiples of 10 hours<br>1 1 1 value indicates that the timer is infinite<br><br>Other values shall be interpreted as multiples of 1 minute in this version of the protocol.<br><br>Timer unit and Timer value both set to all "zeros" shall be interpreted as an indication that the timer is stopped. |

## 8.2.79 PDN Type

The PDN Type IE shall be encoded as shown in Figure 8.2.79-1. It indicates the type of a PDN connection (IP or Unstructured).

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 113 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | PDN Type | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.79-1: PDN Type**

**Table 8.2.79-1: PDN Type**

| PDN Type | Value (Decimal) |
|---|---|
| IPv4 | 1 |
| IPv6 | 2 |
| IPv4v6 | 3 |
| Non-IP | 4 |
| For future use. Shall not be sent. | 0, 5 to 7 |

## 8.2.80 Failed Rule ID

The Failed Rule ID IE type shall be encoded as shown in Figure 8.2.80-1. It shall identify the Rule which failed to be created or modified.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 114 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | Rule ID Type | | | | |
| 6 to p | Rule ID value | | | | | | | |
| (p+1) to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.80-1: Failed Rule ID**

The Rule ID Type shall be encoded as a 5 bits binary integer value as specified in Table 8.2.80-1.

**Table 8.2.80-1: Rule ID Type**

| Rule ID Type | Value (Decimal) |
|---|---|
| PDR | 0 |
| FAR | 1 |
| QER | 2 |
| URR | 3 |
| BAR | 4 |
| For future use. Shall not be sent. If received, shall be interpreted as the value "1". | 5 to 31 |

The length and the value of the Rule ID value field shall be set as specified for the PDR ID, FAR ID, QER ID, URR ID and BAR ID IE types respectively.

## 8.2.81 Time Quota Mechanism

The Time Quota Mechanism type shall be encoded as shown in Figure 8.2.81-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 115 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | BTIT |
| m to (m+3) | Base Time Interval | | | | | | | |
| w to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.81-1: Time Quota Mechanism**

BTIT (Base Time Interval Type) indicates the type of the interval to be provided in the Base Time Interval field.

**Table 8.2.81-1: Base Time Interval Type**

| Base Time Interval Type | Value (Decimal) |
|---|---|
| CTP | 0 |
| DTP | 1 |
| Spare, for future use. | 2 to 3 |

The Base Time Interval, shall be encoded as Unsigned32 as specified in subclause 7.2.29 of 3GPP TS 32.299 [18].

## 8.2.82 User Plane IP Resource Information

The User Plane IP Resource Information IE type shall be encoded as shown in Figure 8.2.82-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 116 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | ASSONI | TEIDRI | | | V6 | V4 |
| 6 | TEID Range | | | | | | | |
| m to (m+3) | IPv4 address | | | | | | | |
| p to (p+15) | IPv6 address | | | | | | | |
| k to l | Network Instance | | | | | | | |
| (l+1) to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.82-1: User Plane IP Resource Information**

The following flags are coded within Octet 5:

- Bit 1 – V4: If this bit is set to "1", then the IPv4 address field shall be present, otherwise the IPv4 address field shall not be present.

- Bit 2 – V6: If this bit is set to "1", then the IPv6 address field shall be present, otherwise the IPv6 address field shall not be present.

- Bit 3-5 – TEID Range Indication (TEIDRI): the value of this field indicates the number of bits in the most significant octet of a TEID that are used to partition the TEID range, e.g. if this field is set to "4", then the first 4 bits in the TEID are used to partition the TEID range.

- Bit 6 – Associated Network Instance (ASSONI): if this bit is set to "1", then the Network Instance field shall be present, otherwise the Network Instance field shall not be present, i.e. User Plane IP Resource Information provided can be used by CP function for any Network Instance of GTP-U user plane in the UP function.

- Bit 7 to 8: Spare, for future use and set to 0.

At least one of the V4 and V6 flags shall be set to "1", and both may be set to "1".

Octet 6 (TEID Range) shall be present if the TEID Range Indication is not set to zero and shall contain a value of the bits which are used to partition the TEID range. E.g. if the TEID Range Indication is set to "4", then Octet 6 shall be one of values between 0 and 15. When TEID Range Indication is set to zero, the Octet 6 shall not be present, the TEID is not partitioned, i.e. all TEID values are available for use by the CP function.

Octets "m to (m+3)" and/or "p to (p+15)" (IPv4 address / IPv6 address fields), if present, shall contain the respective IP address values.

Octets "k to l", if present, shall contain a Network Instance value as encoded in octet "5 to n+4" of the Figure 8.2.4-1 in subclause 8.2.4, identifying a Network Instance with which the IP address or TEID Range is associated.

# Annex A (Informative): PFCP Load and Overload Control Mechanism

## A.1 Throttling Aalgorithms

### A.1.1 "Loss" Throttling Algorithm

#### A.1.1.1 Example of Possible Implementation

This subclause provides an example of a possible implementation of the "Loss" algorithm, amongst other possible methods.

It is possible to make use of a statistical loss function (e.g., random selection of messages to throttle based on the indicated percentage) to decide if the given message can be sent or need to be throttled. For example, the source node generates a random number between (0, 100) for each message which is a potential candidate for throttling. To realize 10% throttling, messages with a random number 10 or less are throttled and hence this achieves approximately a 10% reduction in the overall traffic. The actual traffic reduction might vary slightly from the requested percentage, albeit by an insignificant amount.

The algorithm can select certain messages to throttle in priority. For example, implementations can distinguish between higher-priority and lower-priority messages, and drop the lower-priority messages in favour of dropping the higher priority messages, as long as the total reduction in traffic conforms to the requested reduction in effect at the time. For example, in the 50-50 distribution of high priority and low priority messages, 20% reduction to low priority messages and 0% reduction to high priority messages need to be applied in order to achieve the effective reduction in traffic by 10% towards the overloaded node.

# Annex B (Normative): CP and UP Selection Functions with Control and User Plane Separation

## B.1 CP Selection Function

### B.1.1 General

The SGW-C and PGW-C selection function shall follow the principles specified in 3GPP TS 29.303 [25] for the SGW and PGW selection functions without Control and User Plane Separation.

The following additional considerations apply with Control and User Plane Separation:

1. At most one SGW-C shall be selected per user at any time.
2. The service area of an SGW-C function shall be aligned with the service area of the corresponding SGW-U functions (see subclause 4.3.4 of 3GPP TS 23.214 [2]. All the SGW-U functions in the service area shall have a full meshed connectivity with all the eNBs of TAs and/or all RNCs/BSCs of RAs served by that service area.
3. The SGW dynamic load reported to the MME/SGSN and the PGW dynamic load reported to the MME/SGSN or TWAN/ePDG should take into account the operating status of the CP and UP functions' resources that the SGW-C/PGW-C is controlling. See subclause 6.2.3 for how the CP function obtains load control information from the UP function.
4. For Dedicated Core Networks (see subclause 5.8 of 3GPP TS 29.303 [25]), an SGW-C or PGW-C function shall be declared in DNS as dedicated to certain mapped UE usage types if the CP function or if all the UP functions it controls are dedicated to certain mapped UE usage types. In this case, the CP function shall be provisioned in DNS with all the mapped UE usage types that both the CP function and its UP functions support.

## B.2 UP Selection Function

### B.2.1 General

The following requirements apply for the selection of the UP function:

- the SGW-C, PGW-C and TDF-C shall be responsible for the selection of the SGW-U, PGW-U and TDF-U respectively;
- an SGW-C may select different SGW-U functions for different PDN connections of a same user.

It is implementation specific how to support the UP selection function requirements specified in this clause. Subclause B.2.6 specifies one possible implementation.

### B.2.2 SGW-U Selection Function

The SGW-C shall be able to select the SGW-U considering the following parameters:

- the SGW-U location and the user 's location (i.e. ECGI, eNodeB ID or TAI for E-UTRAN, RAI or RNC-ID for UTRAN);
- the SGW-U's capabilities and the capabilities required for the particular UE session to establish;
- the mapped UE Usage Type (when dedicating SGW-U to specific Dedicated Core Networks);
- the SGW-U's dynamic load;

- the SGW-U's relative static capacity (versus other SGW-Us).

Based on local policy, if the user's location information is required to be used for selecting the UP function, the SGW-C shall determine the list of candidate SGW-Us taking into account the user 's location (ECGI, eNodeB ID or TAI for E-UTRAN, RAI or RNC-ID for UTRAN).

The SGW-C shall select, among the candidate SGW-U functions, an SGW-U function which supports all the capabilities required for the particular UE session, considering the information received during the Sx Association Setup.

## B.2.3 PGW-U Selection Function

The PGW-C shall be able to select the PGW-U considering the following parameters:

- the requested APN for the PDN connection;
- the PGW-U location and the user 's location;
- the PGW-U's capabilities and the capabilities required for the particular UE session to establish;
- the mapped UE Usage Type (when dedicating PGW-U to specific Dedicated Core Networks);
- the PGW-U's dynamic load;
- the PGW-U's relative static capacity (versus other PGW-Us);
- whether a PDN connection already exists for the same UE and APN, in which case the same PGW-U shall be selected (to enable APN-AMBR enforcement);

NOTE: The SGW-U and PGW-U location can be configured in the SGW-C and PGW-C or derived from DNS procedures as specified in subclause B.2.2.

If the PGW-C already assigned a PGW-U to the UE for the requested APN (e.g. UE with multiple PDN connections to the same APN), the PGW-C shall select the same PGW-U for the new PDN connection.

If a non-null IPv4 address and/or a IPv6 prefix is received in the PDN Address Allocation (PAA) IE in the Create Session Request, e.g. static address assignment in the user subscription, the PGW-C shall select a PGW-U which can support the requested UE's IP address and/or IPv6 prefix.

Otherwise, the PGW-C shall determine the list of candidate PGW-Us taking into account the requested APN.

The PGW-C shall select, among the candidate PGW-U functions, a PGW-U function which supports all the capabilities required for the particular UE session, considering the information received during the Sx Association Setup.

## B.2.4 Combined SGW-U/PGW-U Selection Function

A Combined SGW-C and PGW-C function shall be able to select a combined SGW-U and PGW-U function. This shall be possible for all the UE's PDN connections, as shown in Figure B.2.1-1.

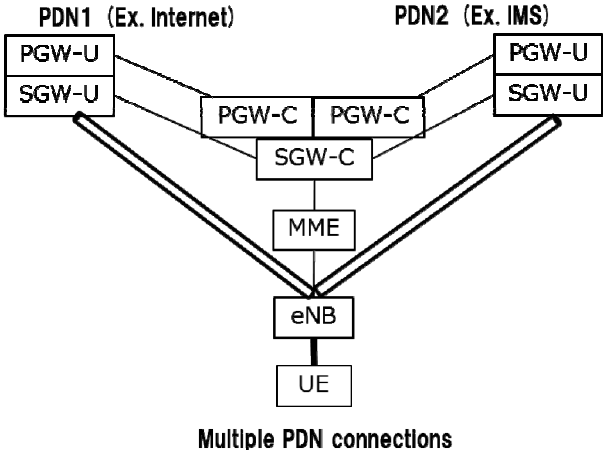


**Figure B.2.4 -1: SGW-U/PGW-U colocation with Control and User Plane Separation**

A combined SGW-C/PGW-C function shall select the SGW-U and PGW-U as defined respectively in B.2.2 and B.2.3, with the following additions:

- the combined SGW-C/PGW-C function shall select the best couple of SGW-U and PGW-U, for the requested APN, among all candidate couples of (SGW-U, PGW-U), instead of selecting independently the SGW-U and the PGW-U.

## B.2.5 TDF-U selection function

The TDF-C shall be able to select the TDF-U as specified in subclause 5.12.5 of 3GPP TS 23.214 [2].

## B.2.6 UP Selection Function Based on DNS

### B.2.6.1 General

This subclause specifies optional DNS procedures to select the SGW-U and PGW-U functions and the requirements which apply when these procedures are supported.

The relative static capacity of an SGW-U and PGW-U may be configured in the DNS.

The Node ID of an SGW-U and PGW-U may take the form of a canonical node name to allow the selection of a SGW-U and PGW-U with the best topological match.

### B.2.6.2 SGW-U Selection Function Based on DNS

The SGW-C shall retrieve the list of candidate SGW-Us using DNS procedures taking into account the user 's location (ECGI, eNodeB ID or TAI for E-UTRAN, RAI or RNC-ID for UTRAN), as specified in 3GPP TS 29.303 [25].

In non-roaming or LBO scenarios where the PGW-U is already selected (e.g. TAU with SGW change) and when it is preferred to select a collocated node or a topologically closer node, the SGW-C shall try to select an SGW-U collocated with the PGW-U.

### B.2.6.3 PGW-U Selection Function Based on DNS

The PGW-C shall retrieve the list of candidate PGW-Us using DNS procedures taking into account the requested APN, as specified in 3GPP TS 29.303 [25].

In non-roaming or LBO scenarios, when it is preferred to select a collocated node or a topologically closer node, i.e. when such preference is indicated in the canonical node names of the PGW-U functions in the DNS (using "topon" as the first label of canonical node name), the PGW-C shall give precedence to collocation of SGW-U and PGW-U, then to topological closeness (i.e. pairs of SGW-U and PGW-U with canonical node names with the highest number of matching labels). This requires the SGW-C to provide the SGW-U Node ID to the PGW-C.

### B.2.6.4 Combined SGW-U/PGW-U Selection Function Based on DNS

A combined SGW-C/PGW-C function shall select the SGW-U and PGW-U as defined respectively in B.2.4, B.2.6.2 and B.2.6.3.

# Annex C (Informative): Examples scenarios

## C.1 General

This clause provides example call flows illustrating how the CP function can provision the UP function to support certain functionalities.

This Annex is informative and the normative descriptions in this specification and in 3GPP TS 23.214 [2] prevail over the descriptions in this Annex if there is any difference.

## C.2 Charging Support

### C.2.1 Online Charging

#### C.2.1.1 Online Charging Call Flow – Normal Scenario

Figure C.2.1.1-1 illustrates the exchanges taking place over the Sxb or Sxc reference points when applying online charging. In this example, the OCS grants quotas by chunks of 100 Mbytes and requests the CP function to request new credits when the remaining credit falls below 10 Mbytes.

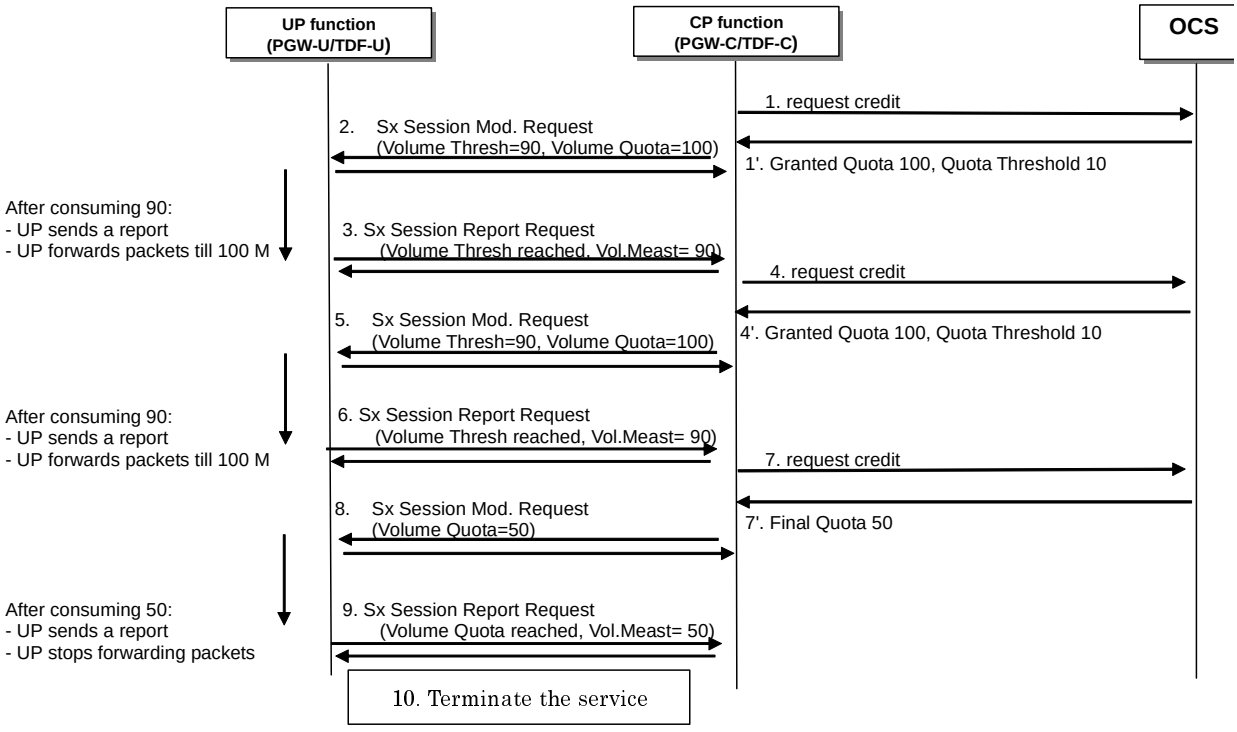


**Figure C.2.1.1-1: Online charging with intermediate and final quotas**

1. Upon the request from the CP function, the OCS grants an intermediate quota of 100 Mbytes and requests the CP function to request a new credit when the remaining credit falls below 10 Mbytes.

2. The CP function sends an Sx Session Modification Request to the UP function with an Update URR IE including the Volume Threshold IE set to 90 Mbytes and the Volume Quota IE set to 100 Mbytes.

3. Upon reaching the Volume Threshold (i.e. 90 Mbytes), the UP function sends an Sx Session Report Request to the CP function with a Usage Report IE including the Usage Report Trigger set to "Volume Threshold" and the

Volume Measurement set to 90 Mbytes. The UP function continues to pass on traffic until reaching the Volume Quota (i.e. an extra 10 Mbytes of traffic can be passed on).

4. Upon the request from the CP function, the OCS grants a new intermediate quota of 100 Mbytes and requests the CP function to request a new credit when the remaining credit falls below 10 Mbytes.

5. The CP function sends an Sx Session Modification Request to the UP function with an Update URR IE including the Volume Threshold IE set to 90 Mbytes and the Volume Quota IE set to 100 Mbytes. If the UP function had forwarded e.g. 5 Mbytes of traffic since the last usage report, the UP function knows that it shall send the next usage report upon passing on an extra 85 Mbytes of traffic.

6. Upon reaching the Volume Threshold (i.e. 90 Mbytes), the UP function sends an Sx Session Report Request to the CP function with a Usage Report IE including the Usage Report Trigger set to "Volume Threshold" and the Volume Measurement set to 90 Mbytes. The UP function continues to pass on traffic until reaching the Volume Quota (i.e. an extra 10 Mbytes of traffic can be passed on).

7. Upon the request from the CP function, the OCS grants a new final quota of 50 Mbytes and requests the CP function to terminate the service or to redirect the traffic towards a redirect destination when the quota is consumed.

8. The CP function sends an Sx Session Modification Request to the UP function with an Update URR IE including the Volume Quota IE set to 50 Mbytes. If the UP function had forwarded e.g. 5 Mbytes of traffic since the last usage report, the UP function knows that it shall send the next usage report upon passing on an extra 45 Mbytes of traffic.

9. Upon reaching the Volume Quota (i.e. 50 Mbytes), the UP function sends an Sx Session Report Request to the CP function with a Usage Report IE including the Usage Report Trigger set to "Volume Quota" and the Volume Measurement set to 50 Mbytes. The UP function stops passing on traffic.

10. Upon being notified that the final quota has been reached, the CP function terminates the service (e.g. by preventing the traffic of the corresponding SDF to further pass on in the UP function) or redirects the traffic towards a redirect destination by provisioning a Redirect Information IE within the FAR associated to the traffic.

# Annex D(Informative): Change history

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** |
| 2016-07 | CT4#74 | C4-164286 | | | First version after CT4#74 | 0.0.0 | 0.1.0 |
| 2016-10 | CT4#74bis | C4-165318 | | | Version after CT4#74bis | 0.1.0 | 0.2.0 |
| 2016-11 | CT4#75 | C4-166347 | | | Version after CT4#75 | 0.2.0 | 0.3.0 |
| 2017-01 | CT4#75bis | C4-170124 | | | Version after CT4#75bis | 0.3.0 | 0.4.0 |
| 2017-02 | CT4#76 | C4-171423 | | | Version after CT4#76 | 0.4.0 | 0.5.0 |
| 2017-03 | CT#75 | CP-170016 | | | This version was sent for information | 0.5.0 | 1.0.0 |
| 2017-04 | C4#77 | C4-172285 | | | Version after CT4#77 | 1.0.0 | 1.1.0 |
| 2017-05 | C4#78 | C4-173360 | | | Version after CT4#78 | 1.1.0 | 1.2.0 |
| 2017-06 | CT#76 | CP-171047 | | | This version was sent for approval | 1.2.0 | 2.0.0 |
| 2017-06 | CT#76 | CP-171183 | | | Editorial correction | 2.0.0 | 2.0.1 |
| 2017-06 | CT#76 | CP-171183 | | | Approved in CT#76 | 2.0.1 | 14.0.0 |
| 2017-09 | CT#77 | CP-172020 | 0001 | - | PDN Instance over Sx | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0002 | 1 | Transport Level Marking & DL Flow Level Marking | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0003 | 2 | Clarifications and corrections to Usage Reporting | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0004 | - | PDN Type over Sx | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0005 | 1 | Creating multiple PDRs in one Sx message with F-TEID allocation in UP function | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0006 | 1 | Message with a rejection cause | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0007 | - | Corrections to the number of Fixed Octets | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0008 | 1 | QER correlation ID | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0009 | 3 | Sx Protocol extension to support Envelope Reporting | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0010 | 1 | OCI Flags | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0011 | 2 | IP Address(es) and TEIDs of a UP function | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0012 | 1 | Clarification on bearer of a PDN connection and description on UP fucntion feature | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0013 | 2 | Clarification on Rule IDs | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0014 | 1 | Clarification on creating rules | 14.0.0 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0018 | 2 | URR and QER handling | 14.0.0 | 14.1.0 |

# History

| Document history | | |
|---|---|---|
| V14.0.0 | July 2017 | Publication |
| V14.1.0 | October 2017 | Publication |
| | | |
| | | |
| | | |