# ETSI TS 129 244 V17.7.1 (2023-01)

**LTE;**
**5G;**
**Interface between the Control Plane and the User Plane nodes**
**(3GPP TS 29.244 version 17.7.1 Release 17)**

Reference
RTS/TSGC-0429244vh71

Keywords
5G,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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

***Important notice***

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

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

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

***Notice of disclaimer & limitation of liability***

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

***Copyright Notification***

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2023.
All rights reserved.

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

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

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

# Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 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

Intellectual Property Rights ..... 2
Legal Notice ..... 2
Modal verbs terminology ..... 2
Foreword ..... 15
1 Scope ..... 17
2 References ..... 17
3 Definitions, symbols and abbreviations ..... 20
3.1 Definitions ..... 20
3.2 Abbreviations ..... 20
4 Protocol Stack ..... 22
4.1 Introduction ..... 22
4.2 UDP Header and Port Numbers ..... 23
4.2.1 General ..... 23
4.2.2 Request Message ..... 23
4.2.3 Response Message ..... 23
4.3 IP Header and IP Addresses ..... 23
4.3.1 General ..... 23
4.3.2 Request Message ..... 23
4.3.3 Response Message ..... 24
4.4 Layer 2 ..... 24
4.5 Layer 1 ..... 24
5 General description ..... 24
5.1 Introduction ..... 24
5.2 Packet Forwarding Model ..... 24
5.2.1 General ..... 24
5.2.1A Packet Detection Rule Handling ..... 27
5.2.1A.1 General ..... 27
5.2.1A.2 PDI Optimization ..... 28
5.2.1A.2A Provisioning of SDF filters ..... 28
5.2.1A.3 Bidirectional SDF Filters ..... 29
5.2.1A.4 Application detection with PFD ..... 29
5.2.2 Usage Reporting Rule Handling ..... 29
5.2.2.1 General ..... 29
5.2.2.2 Provisioning of Usage Reporting Rule in the UP function ..... 30
5.2.2.2.1 General ..... 30
5.2.2.2.2 Credit pooling (for EPC) ..... 34
5.2.2.3 Reporting of Usage Report to the CP function ..... 35
5.2.2.3.1 General ..... 35
5.2.2.3.2 Credit pooling ..... 39
5.2.2.3.3 Traffic Usage Reporting with Redundant Transmission ..... 40
5.2.2.4 Reporting of Linked Usage Reports to the CP function ..... 40
5.2.2.5 End Marker Reception Reporting ..... 40
5.2.3 Forwarding Action Rule Handling ..... 41
5.2.3.1 General ..... 41
5.2.4 Buffering Action Rule Handling ..... 43
5.2.4.1 General ..... 43
5.2.4.2 Provisioning of Buffering Action Rule in the UP function ..... 43
5.2.5 QoS Enforcement Rule Handling ..... 44
5.2.5.1 General ..... 44
5.2.5.2 Provisioning of QoS Enforcement Rule in the UP function ..... 44
5.2.5.3 Reflective QoS (for 5GC) ..... 44
5.2.6 Combined SGW/PGW Architecture ..... 44
5.2.7 Multi-Access Rule Handling (for 5GC) ..... 45

5.2.7.1 General ..... 45
5.2.8 Session Reporting Rule Handling ..... 46
5.2.8.1 General ..... 46
5.2.8.2 Provisioning of Session Reporting Rule in the UP function ..... 46
5.2.8.2.1 General ..... 46
5.2.8.3 Reporting of Session Report to the CP function ..... 46
5.2.8.3.1 General ..... 46
5.2.9 Handling of Rules that cannot be activated ..... 46
5.3 Data Forwarding between the CP and UP Functions ..... 47
5.3.1 General ..... 47
5.3.2 Sending of End Marker Packets ..... 48
5.3.3 Forwarding of Packets Subject to Buffering in the CP Function ..... 48
5.3.3.1 General ..... 48
5.3.3.2 Forwarding of Packets from the UP Function to the CP Function ..... 49
5.3.3.3 Forwarding of Packets from the CP Function to the UP Function ..... 49
5.3.4 Data Forwarding between the CP and UP Functions with one PFCP-u Tunnel per UP Function or PDN ..... 50
5.3.4.1 General ..... 50
5.3.4.2 Forwarding of Packets from the UP Function to the CP Function ..... 50
5.3.4.3 Forwarding of Packets from the CP Function to the UP Function ..... 50
5.3.5 Forwarding of user data using Control Plane CIoT 5GS Optimisation (for 5GC) ..... 51
5.3.5.1 General ..... 51
5.3.5.2 Forwarding of Packets from the UP Function to the CP Function ..... 51
5.3.5.3 Forwarding of Packets from the CP Function to the UP Function ..... 51
5.4 Policy and Charging Control ..... 51
5.4.1 General ..... 51
5.4.2 Service Detection and Bearer/QoS Flow Binding ..... 52
5.4.3 Gating Control ..... 52
5.4.4 QoS Control ..... 53
5.4.5 DL Flow Level Marking for Application Detection ..... 54
5.4.6 Usage Monitoring ..... 54
5.4.7 Traffic Redirection ..... 54
5.4.8 Traffic Steering ..... 55
5.4.9 Provisioning of Predefined PCC/ADC Rules ..... 56
5.4.10 Charging ..... 57
5.4.11 (Un)solicited Application Reporting ..... 58
5.4.12 Service Identification for Improved Radio Utilisation for GERAN ..... 59
5.4.13 Transport Level Marking ..... 59
5.4.14 Deferred PDR activation and deactivation ..... 59
5.4.15 Packet Rate enforcement ..... 60
5.4.15.1 General ..... 60
5.4.15.2 Packet rate enforcement over Sxb and N4 interfaces ..... 60
5.4.15.3 PGW and SMF behaviour ..... 61
5.4.16 QoS differentiation for Stand-alone Non-Public Network (SNPN) ..... 62
5.4.16.1 General ..... 62
5.4.16.2 Access to PLMN services via SNPN ..... 62
5.4.16.3 Access to SNPN services via PLMN ..... 62
5.5 F-TEID Allocation and Release ..... 63
5.5.1 General ..... 63
5.5.2 Void ..... 63
5.5.3 F-TEID allocation in the UP function ..... 63
5.6 PFCP Session Handling ..... 64
5.6.1 General ..... 64
5.6.2 Session Endpoint Identifier Handling ..... 64
5.6.3 Modifying the Rules of an Existing PFCP Session ..... 64
5.7 Support of Lawful Interception ..... 64
5.7.1 General ..... 64
5.7.2 Lawful Interception in EPC ..... 64
5.7.3 Lawful Interception in 5GC ..... 65
5.8 PFCP Association ..... 65
5.8.1 General ..... 65
5.8.2 Behaviour with an Established PFCP Association ..... 66

5.8.3 Behaviour without an Established PFCP Association ..... 66
5.9 Usage of Vendor-specific IE ..... 67
5.10 Error Indication Handling ..... 67
5.11 User plane inactivity detection and reporting ..... 67
5.11.1 General ..... 67
5.11.2 User plane inactivity detection and reporting per PDN connection or PDU session ..... 67
5.11.3 User plane inactivity detection and reporting per PDR ..... 68
5.12 Suspend and Resume Notification procedures ..... 68
5.13 Ethernet traffic (for 5GC) ..... 68
5.13.1 General ..... 68
5.13.2 Address Resolution Protocol or IPv6 Neighbour Solicitation Response by SMF ..... 69
5.13.3 Address Resolution Protocol or IPv6 Neighbour Solicitation Response by UPF ..... 70
5.13.3A Provisioning of MAC addresses and SDF filters in Ethernet Packet Filters ..... 70
5.13.4 Bidirectional Ethernet Filters ..... 70
5.13.5 Reporting of UE MAC addresses to the SMF ..... 71
5.13.6 Ethernet PDU session anchor relocation ..... 71
5.14 Support IPv6 Prefix Delegation ..... 72
5.15 Signalling based Trace (De)Activation ..... 72
5.16 Framed Routing ..... 72
5.17 5G UPF (for 5GC) ..... 73
5.17.1 Introduction ..... 73
5.17.2 Uplink Classifier and Branching Point ..... 73
5.17.3 Data forwarding during handovers between 5GS and EPS ..... 73
5.18 Enhanced PFCP Association Release ..... 74
5.18.1 General ..... 74
5.18.2 UP Function Initiated PFCP Session Release ..... 75
5.19 Activation and Deactivation of Pre-defined PDRs ..... 75
5.20 Support of Access Traffic Steering, Switching and Splitting for 5GC ..... 76
5.20.1 General ..... 76
5.20.2 MPTCP functionality ..... 77
5.20.2.1 General ..... 77
5.20.2.2 Activate MPTCP functionality and Exchange MPTCP Parameters ..... 77
5.20.2.3 Control of Multipath TCP Connection Establishment by MPTCP Proxy ..... 77
5.20.2.4 Traffic Steering and IP Translation by MPTCP Proxy ..... 78
5.20.3 ATSSS-LL functionality ..... 78
5.20.3.1 Activate ATSSS-LL functionality and Exchange ATSSS-LL Parameters ..... 78
5.20.4 Handling of GBR traffic of a MA PDU session ..... 79
5.20.4.1 General ..... 79
5.20.4.2 Access Availability Reporting ..... 79
5.20.5 Access type of an MA PDU session becoming (un)available ..... 79
5.20.6 PMFP message handling in UPF ..... 79
5.21 UE IP address/prefix Allocation and Release ..... 80
5.21.1 General ..... 80
5.21.2 UE IP address/prefix allocation in the CP function ..... 81
5.21.2.1 General ..... 81
5.21.2.2 UE IP Address/prefix allocation using DHCP or AAA server ..... 81
5.21.3 UE IP address/prefix allocation in the UP function ..... 81
5.21.3.1 General ..... 81
5.21.3.2 Reporting UE IP Address Usage to the CP function ..... 82
5.22 PFCP sessions successively controlled by different SMFs of an SMF set (for 5GC) ..... 83
5.22.1 General ..... 83
5.22.2 With one PFCP association per SMF Set and UPF ..... 83
5.22.3 With one PFCP association per SMF and UPF ..... 84
5.22.4 Restoration of PFCP Sessions associated with an FQ-CSID, Group ID or PGW-C/SMF IP Address ..... 86
5.23 5G VN Group Communication (for 5GC) ..... 86
5.24 Support of Ultra Reliable Low Latency Communication for 5GC ..... 87
5.24.1 General ..... 87
5.24.2 Redundant Transmission on N3/N9 interfaces ..... 88
5.24.2.1 General ..... 88
5.24.2.2 GTP-U tunnel setup for redundant transmission ..... 88
5.24.2.3 Duplicating downlink packets for redundant transmission ..... 89
5.24.2.4 Eliminating duplicated uplink packets ..... 89

5.24.3 Redundant Transmission at transport layer ..... 89
5.24.4 Per QoS Flow Per UE QoS Monitoring ..... 89
5.24.4.1 General ..... 89
5.24.4.2 QoS Monitoring Control ..... 90
5.24.4.3 QoS Monitoring Reporting ..... 90
5.24.5 Per GTP-U Path QoS Monitoring ..... 91
5.24.5.1 General ..... 91
5.24.5.2 GTP-U path monitoring ..... 91
5.24.5.3 QoS monitoring of a PDU session based on GTP-U path monitoring ..... 92
5.24.5.4 QoS Monitoring Reporting ..... 92
5.25 Support of IPTV (for 5GC) ..... 92
5.26 Support of Time Sensitive Communications and Time Synchronization (for 5GC) ..... 94
5.26.1 General ..... 94
5.26.2 5GS Bridge management ..... 94
5.26.3 Transfer of 5GS bridge and port management information ..... 94
5.26.4 Reporting clock drift between External and 5GS times from UPF to SMF ..... 95
5.27 Inter-PLMN User Plane Security ..... 95
5.28 Downlink data delivery status with UPF buffering (for 5GC) ..... 96
5.28.1 General ..... 96
5.29 Support Reliable Data Service ..... 96
5.30 Notifying Start Pause of Charging ..... 97
5.31 Support of L2TP ..... 98
5.31.1 General ..... 98
5.31.2 L2TP Tunnel and L2TP Session Setup ..... 98
5.31.3 L2TP Session and L2TP Tunnel Release ..... 99
5.32 Support of Uplink packets buffering ..... 100
5.32.1 General ..... 100
5.32.2 Uplink packets buffering for on-line charging ..... 100
5.32.3 Uplink packets buffering during EAS relocation ..... 100
5.33 Support of enhancement of Edge Computing (for 5GC) ..... 100
5.33.1 General ..... 100
5.33.2 Uplink packet buffering for low packet loss during EAS relocation ..... 100
5.33.3 Edge Relocation using EAS IP address and Port number Replacement ..... 100
5.33.4 EAS Discovery procedure with Local DNS Server/Resolver ..... 101
5.33.5 Direct Reporting of QoS monitoring events to Local NEF or AF ..... 101
5.34 Support of 5G Multicast and Broadcast Service ..... 101
5.34.1 General ..... 101
5.34.2 N4mb requirements ..... 102
5.34.2.1 General ..... 102
5.34.2.2 Instructing the MB-UPF to forward MBS data using multicast and/or unicast transport ..... 102
5.34.2.3 Detecting and reporting user plane (in)activity of an MBS session ..... 103
5.34.2.4 Activation and Deactivation of a Multicast MBS session ..... 103
5.34.3 N4 requirements ..... 104
5.34.3.1 General ..... 104
5.34.3.2 Instructing the UPF to forward (or stop forwarding) multicast MBS data to associated PDU sessions ..... 104
5.34.3.3 Instructing a combined UPF/MBS-UPF to forward multicast MBS data to associated PDU sessions ..... 106
5.35 Support of Per Slice UP Resource Allocation and Usage Reporting by the UP Function ..... 107
5.35.1 General ..... 107
5.36 Paging Policy Indicator Provisioning ..... 108
5.36.1 General ..... 108
5.36.2 Enhanced Paging Policy Indicator Provisioning ..... 108
6 Procedures ..... 109
6.1 Introduction ..... 109
6.2 PFCP Node Related Procedures ..... 109
6.2.1 General ..... 109
6.2.2 Heartbeat Procedure ..... 109
6.2.2.1 General ..... 109
6.2.2.2 Heartbeat Request ..... 109
6.2.2.3 Heartbeat Response ..... 109

6.2.3 Load Control Procedure ..... 109
6.2.3.1 General ..... 109
6.2.3.2 Principles ..... 110
6.2.3.3 Load Control Information ..... 110
6.2.3.3.1 General Description ..... 110
6.2.3.3.2 Parameters ..... 111
6.2.3.3.3 Frequency of Inclusion ..... 111
6.2.4 Overload Control Procedure ..... 112
6.2.4.1 General ..... 112
6.2.4.2 Principles ..... 112
6.2.4.3 Overload Control Information ..... 113
6.2.4.3.1 General Description ..... 113
6.2.4.3.2 Parameters ..... 113
6.2.4.3.3 Frequency of Inclusion ..... 115
6.2.4.4 Message Throttling ..... 115
6.2.4.4.1 General ..... 115
6.2.4.4.2 Throttling algorithm – "Loss" ..... 116
6.2.4.5 Message Prioritization ..... 116
6.2.4.5.1 Description ..... 116
6.2.4.5.2 Based on the Message Priority Signalled in the PFCP Message ..... 117
6.2.5 PFCP PFD Management Procedure ..... 117
6.2.5.1 General ..... 117
6.2.5.2 CP Function Behaviour ..... 117
6.2.5.3 UP Function Behaviour ..... 117
6.2.6 PFCP Association Setup Procedure ..... 118
6.2.6.1 General ..... 118
6.2.6.2 PFCP Association Setup Initiated by the CP Function ..... 118
6.2.6.2.1 CP Function Behaviour ..... 118
6.2.6.2.2 UP Function behaviour ..... 119
6.2.6.3 PFCP Association Setup Initiated by the UP Function ..... 119
6.2.6.3.1 UP Function Behaviour ..... 119
6.2.6.3.2 CP Function Behaviour ..... 120
6.2.7 PFCP Association Update Procedure ..... 120
6.2.7.1 General ..... 120
6.2.7.2 PFCP Association Update Procedure Initiated by the CP Function ..... 120
6.2.7.2.1 CP Function Behaviour ..... 120
6.2.7.2.2 UP Function Behaviour ..... 120
6.2.7.3 PFCP Association Update Procedure Initiated by UP Function ..... 121
6.2.7.3.1 UP Function Behaviour ..... 121
6.2.7.3.2 CP Function Behaviour ..... 121
6.2.8 PFCP Association Release Procedure ..... 122
6.2.8.1 General ..... 122
6.2.8.2 CP Function Behaviour ..... 122
6.2.8.3 UP Function behaviour ..... 122
6.2.9 PFCP Node Report Procedure ..... 122
6.2.9.1 General ..... 122
6.2.9.2 UP Function Behaviour ..... 122
6.2.9.3 CP Function behaviour ..... 122
6.3 PFCP Session Related Procedures ..... 123
6.3.1 General ..... 123
6.3.2 PFCP Session Establishment Procedure ..... 123
6.3.2.1 General ..... 123
6.3.2.2 CP Function Behaviour ..... 123
6.3.2.3 UP Function Behaviour ..... 123
6.3.3 PFCP Session Modification Procedure ..... 123
6.3.3.1 General ..... 123
6.3.3.2 CP Function behaviour ..... 124
6.3.3.3 UP Function Behaviour ..... 124
6.3.4 PFCP Session Deletion Procedure ..... 124
6.3.4.1 General ..... 124
6.3.4.2 CP Function Behaviour ..... 124
6.3.4.3 UP Function Behaviour ..... 125

6.3.5 PFCP Session Report Procedure ..... 125
6.3.5.1 General ..... 125
6.3.5.2 UP Function Behaviour ..... 125
6.3.5.3 CP Function Behaviour ..... 125
6.4 Reliable Delivery of PFCP Messages ..... 125
6.5 PFCP messages bundling ..... 126

7 Messages and Message Formats ..... 127
7.1 Transmission Order and Bit Definitions ..... 127
7.2 Message Format ..... 127
7.2.1 General ..... 127
7.2.1A PFCP messages bundled in one UDP/IP packet ..... 127
7.2.2 Message Header ..... 128
7.2.2.1 General Format ..... 128
7.2.2.2 PFCP Header for Node Related Messages ..... 128
7.2.2.3 PFCP Header for Session Related Messages ..... 129
7.2.2.4 Usage of the PFCP Header ..... 129
7.2.2.4.1 General ..... 129
7.2.2.4.2 Conditions for Sending SEID=0 in PFCP Header ..... 130
7.2.3 Information Elements ..... 130
7.2.3.1 General ..... 130
7.2.3.2 Presence Requirements of Information Elements ..... 130
7.2.3.3 Grouped Information Elements ..... 131
7.2.3.4 Information Element Type ..... 132
7.3 Message Types ..... 132
7.4 PFCP Node Related Messages ..... 133
7.4.1 General ..... 133
7.4.2 Heartbeat Messages ..... 133
7.4.2.1 Heartbeat Request ..... 133
7.4.2.2 Heartbeat Response ..... 134
7.4.3 PFCP PFD Management ..... 134
7.4.3.1 PFCP PFD Management Request ..... 134
7.4.3.2 PFCP PFD Management Response ..... 135
7.4.4 PFCP Association messages ..... 136
7.4.4.1 PFCP Association Setup Request ..... 136
7.4.4.1.1 General ..... 136
7.4.4.1.2 Clock Drift Control Information IE within PFCP Association Setup Request ..... 138
7.4.4.1.3 GTP-U Path QoS Control Information IE within PFCP Association Setup Request ..... 139
7.4.4.2 PFCP Association Setup Response ..... 141
7.4.4.3 PFCP Association Update Request ..... 144
7.4.4.3.1 UE IP Address Usage Information IE within PFCP Association Update Request ..... 146
7.4.4.4 PFCP Association Update Response ..... 148
7.4.4.5 PFCP Association Release Request ..... 148
7.4.4.6 PFCP Association Release Response ..... 148
7.4.4.7 PFCP Version Not Supported Response ..... 148
7.4.5 PFCP Node Report Procedure ..... 149
7.4.5.1 PFCP Node Report Request ..... 149
7.4.5.1.1 General ..... 149
7.4.5.1.2 User Plane Path Failure Report IE within PFCP Node Report Request ..... 149
7.4.5.1.3 User Plane Path Recovery Report IE within PFCP Node Report Request ..... 150
7.4.5.1.4 Clock Drift Report IE within PFCP Node Report Request ..... 150
7.4.5.1.5 GTP-U Path QoS Report IE within PFCP Node Report Request ..... 150
7.4.5.1.6 QoS Information in GTP-U Path QoS Report IE ..... 151
7.4.5.1.7 Peer UP Restart Report IE within PFCP Node Report Request ..... 151
7.4.5.1.7 Peer UP Restart Report IE within PFCP Node Report Request ..... 151
7.4.5.2 PFCP Node Report Response ..... 152
7.4.5.2.1 General ..... 152
7.4.6 PFCP Session Set Deletion ..... 152
7.4.6.1 PFCP Session Set Deletion Request ..... 152
7.4.6.2 PFCP Session Set Deletion Response ..... 152
7.4.7 PFCP Session Set Modification ..... 153
7.4.7.1 PFCP Session Set Modification Request ..... 153

7.4.7.2 PFCP Session Set Modification Response ..... 154
7.5 PFCP Session Related Messages ..... 155
7.5.1 General ..... 155
7.5.2 PFCP Session Establishment Request ..... 155
7.5.2.1 General ..... 155
7.5.2.2 Create PDR IE within PFCP Session Establishment Request ..... 161
7.5.2.3 Create FAR IE within PFCP Session Establishment Request ..... 168
7.5.2.4 Create URR IE within PFCP Session Establishment Request ..... 174
7.5.2.5 Create QER IE within PFCP Session Establishment Request ..... 179
7.5.2.6 Create BAR IE within PFCP Session Establishment Request ..... 183
7.5.2.7 Create Traffic Endpoint IE within PFCP Session Establishment Request ..... 183
7.5.2.8 Create MAR IE within PFCP Session Establishment Request ..... 186
7.5.2.9 Create SRR IE within PFCP Session Establishment Request ..... 187
7.5.2.10 Provide ATSSS Control Information IE within PFCP Session Establishment Request ..... 190
7.5.2.11 Provide RDS Configuration Information IE within PFCP Session Establishment Request ..... 190
7.5.3 PFCP Session Establishment Response ..... 190
7.5.3.1 General ..... 190
7.5.3.2 Created PDR IE within PFCP Session Establishment Response ..... 193
7.5.3.3 Load Control Information IE within PFCP Session Establishment Response ..... 194
7.5.3.4 Overload Control Information IE within PFCP Session Establishment Response ..... 194
7.5.3.5 Created Traffic Endpoint IE within PFCP Session Establishment Response ..... 194
7.5.3.6 Created Bridge Info for TSC IE within PFCP Session Establishment Response ..... 195
7.5.3.7 ATSSS Control Parameters IE within PFCP Session Establishment Response ..... 195
7.5.3.8 Void ..... 196
7.5.4 PFCP Session Modification Request ..... 197
7.5.4.1 General ..... 197
7.5.4.2 Update PDR IE within PFCP Session Modification Request ..... 202
7.5.4.3 Update FAR IE within PFCP Session Modification Request ..... 203
7.5.4.4 Update URR IE within PFCP Session Modification Request ..... 206
7.5.4.5 Update QER IE within PFCP Session Modification Request ..... 210
7.5.4.6 Remove PDR IE within PFCP Session Modification Request ..... 213
7.5.4.7 Remove FAR IE within PFCP Session Modification Request ..... 213
7.5.4.8 Remove URR IE within PFCP Session Modification Request ..... 213
7.5.4.9 Remove QER IE PFCP Session Modification Request ..... 213
7.5.4.10 Query URR IE within PFCP Session Modification Request ..... 214
7.5.4.11 Update BAR IE within PFCP Session Modification Request ..... 214
7.5.4.12 Remove BAR IE within PFCP Session Modification Request ..... 214
7.5.4.13 Update Traffic Endpoint IE within PFCP Session Modification Request ..... 215
7.5.4.14 Remove Traffic Endpoint IE within PFCP Session Modification Request ..... 217
7.5.4.15 Remove MAR IE within PFCP Session Modification Request ..... 217
7.5.4.16 Update MAR IE within PFCP Session Modification Request ..... 217
7.5.4.17 Create PDR/FAR/URR/QER/BAR/MAR IEs within PFCP Session Modification Request ..... 219
7.5.4.18 TSC Management Information IE within PFCP Session Modification Request ..... 219
7.5.4.19 Remove SRR IE within PFCP Session Modification Request ..... 219
7.5.4.20 Update SRR IE within PFCP Session Modification Request ..... 219
7.5.4.21 Ethernet Context Information within PFCP Session Modification Request ..... 220
7.5.4.22 Query Packet Rate Status IE within PFCP Session Modification Request ..... 220
7.5.5 PFCP Session Modification Response ..... 221
7.5.5.1 General ..... 221
7.5.5.2 Usage Report IE within PFCP Session Modification Response ..... 224
7.5.5.3 TSC Management Information IE within PFCP Session Modification Response ..... 224
7.5.5.4 Packet Rate Status Report IE within PFCP Session Modification Response ..... 225
7.5.5.5 Updated PDR IE within PFCP Session Modification Response ..... 225
7.5.6 PFCP Session Deletion Request ..... 226
7.5.7 PFCP Session Deletion Response ..... 226
7.5.7.1 General ..... 226
7.5.7.2 Usage Report IE within PFCP Session Deletion Response ..... 228
7.5.8 PFCP Session Report Request ..... 228
7.5.8.1 General ..... 228
7.5.8.2 Downlink Data Report IE within PFCP Session Report Request ..... 230
7.5.8.3 Usage Report IE within PFCP Session Report Request ..... 231
7.5.8.4 Error Indication Report IE within PFCP Session Report Request ..... 234

7.5.8.5 TSC Management Information IE within PFCP Session Report Request....234
7.5.8.6 Session Report IE within PFCP Session Report Request....235
7.5.9 PFCP Session Report Response....236
7.5.9.1 General....236
7.5.9.2 Update BAR IE within PFCP Session Report Response....238
7.6 Error Handling....238
7.6.1 Protocol Errors....238
7.6.2 Different PFCP Versions....239
7.6.3 PFCP Message of Invalid Length....239
7.6.4 Unknown PFCP Message....239
7.6.5 Unexpected PFCP Message....239
7.6.6 Missing Information Elements....239
7.6.7 Invalid Length Information Element....240
7.6.8 Semantically incorrect Information Element....240
7.6.9 Unknown or unexpected Information Element....240
7.6.10 Repeated Information Elements....241

8 Information Elements....241
8.1 Information Elements Format....241
8.1.1 Information Element Format....241
8.1.2 Information Element Types....242
8.2 Information Elements....249
8.2.1 Cause....249
8.2.2 Source Interface....252
8.2.3 F-TEID....252
8.2.4 Network Instance....253
8.2.5 SDF Filter....253
8.2.6 Application ID....255
8.2.7 Gate Status....255
8.2.8 MBR....256
8.2.9 GBR....256
8.2.10 QER Correlation ID....256
8.2.11 Precedence....257
8.2.12 Transport Level Marking....257
8.2.13 Volume Threshold....257
8.2.14 Time Threshold....258
8.2.15 Monitoring Time....258
8.2.16 Subsequent Volume Threshold....259
8.2.17 Subsequent Time Threshold....259
8.2.18 Inactivity Detection Time....260
8.2.19 Reporting Triggers....260
8.2.20 Redirect Information....261
8.2.21 Report Type....262
8.2.22 Offending IE....263
8.2.23 Forwarding Policy....263
8.2.24 Destination Interface....263
8.2.25 UP Function Features....264
8.2.26 Apply Action....268
8.2.27 Downlink Data Service Information....269
8.2.28 Downlink Data Notification Delay....270
8.2.29 DL Buffering Duration....270
8.2.30 DL Buffering Suggested Packet Count....270
8.2.31 PFCPSMReq-Flags....271
8.2.32 PFCPSRRsp-Flags....271
8.2.33 Sequence Number....272
8.2.34 Metric....272
8.2.35 Timer....272
8.2.36 Packet Detection Rule ID (PDR ID)....273
8.2.37 F-SEID....273
8.2.38 Node ID....274
8.2.39 PFD Contents....274
8.2.40 Measurement Method....276

8.2.41 Usage Report Trigger....277
8.2.42 Measurement Period....278
8.2.43 Fully qualified PDN Connection Set Identifier (FQ-CSID)....279
8.2.44 Volume Measurement....280
8.2.45 Duration Measurement....280
8.2.46 Time of First Packet....281
8.2.47 Time of Last Packet....281
8.2.48 Quota Holding Time....281
8.2.49 Dropped DL Traffic Threshold....282
8.2.50 Volume Quota....282
8.2.51 Time Quota....283
8.2.52 Start Time....283
8.2.53 End Time....283
8.2.54 URR ID....284
8.2.55 Linked URR ID IE....284
8.2.56 Outer Header Creation....284
8.2.57 BAR ID....286
8.2.58 CP Function Features....286
8.2.59 Usage Information....287
8.2.60 Application Instance ID....288
8.2.61 Flow Information....288
8.2.62 UE IP Address....288
8.2.63 Packet Rate....289
8.2.64 Outer Header Removal....291
8.2.65 Recovery Time Stamp....292
8.2.66 DL Flow Level Marking....293
8.2.67 Header Enrichment....293
8.2.68 Measurement Information....294
8.2.69 Node Report Type....295
8.2.70 Remote GTP-U Peer....295
8.2.71 UR-SEQN....296
8.2.72 Activate Predefined Rules....296
8.2.73 Deactivate Predefined Rules....297
8.2.74 FAR ID....297
8.2.75 QER ID....297
8.2.76 OCI Flags....297
8.2.77 PFCP Association Release Request....298
8.2.78 Graceful Release Period....298
8.2.79 PDN Type....299
8.2.80 Failed Rule ID....299
8.2.81 Time Quota Mechanism....300
8.2.82 Void....301
8.2.83 User Plane Inactivity Timer....301
8.2.84 Multiplier....301
8.2.85 Aggregated URR ID IE....301
8.2.86 Subsequent Volume Quota....301
8.2.87 Subsequent Time Quota....302
8.2.88 RQI....302
8.2.89 QFI....303
8.2.90 Query URR Reference....303
8.2.91 Additional Usage Reports Information....303
8.2.92 Traffic Endpoint ID....304
8.2.93 MAC address....304
8.2.94 C-TAG (Customer-VLAN tag)....304
8.2.95 S-TAG (Service-VLAN tag)....305
8.2.96 Ethertype....306
8.2.97 Proxying....306
8.2.98 Ethernet Filter ID....306
8.2.99 Ethernet Filter Properties....307
8.2.100 Suggested Buffering Packets Count....307
8.2.101 User ID....307
8.2.102 Ethernet PDU Session Information....309

8.2.103 MAC Addresses Detected ..... 309
8.2.104 MAC Addresses Removed ..... 310
8.2.105 Ethernet Inactivity Timer ..... 310
8.2.106 Subsequent Event Quota ..... 311
8.2.107 Subsequent Event Threshold ..... 311
8.2.108 Trace Information ..... 311
8.2.109 Framed-Route ..... 312
8.2.110 Framed-Routing ..... 312
8.2.111 Framed-IPv6-Route ..... 312
8.2.112 Event Quota ..... 312
8.2.113 Event Threshold ..... 313
8.2.114 Time Stamp ..... 313
8.2.115 Averaging Window ..... 313
8.2.116 Paging Policy Indicator (PPI) ..... 314
8.2.117 APN/DNN ..... 314
8.2.118 3GPP Interface Type ..... 314
8.2.119 PFCPSRReq-Flags ..... 315
8.2.120 PFCPAUReq-Flags ..... 316
8.2.121 Activation Time ..... 316
8.2.122 Deactivation Time ..... 317
8.2.123 MAR ID ..... 317
8.2.124 Steering Functionality ..... 317
8.2.125 Steering Mode ..... 318
8.2.126 Weight ..... 318
8.2.127 Priority ..... 318
8.2.128 UE IP address Pool Identity ..... 319
8.2.129 Alternative SMF IP Address ..... 319
8.2.130 Packet Replication and Detection Carry-On Information ..... 320
8.2.131 SMF Set ID ..... 320
8.2.132 Quota Validity Time ..... 321
8.2.133 Number of Reports ..... 321
8.2.134 PFCPASRsp-Flags ..... 321
8.2.135 CP PFCP Entity IP Address ..... 322
8.2.136 PFCPSEReq-Flags ..... 322
8.2.137 IP Multicast Address ..... 322
8.2.138 Source IP Address ..... 323
8.2.139 Packet Rate Status ..... 324
8.2.140 Create Bridge Info for TSC IE ..... 325
8.2.141 DS-TT Port Number ..... 325
8.2.142 NW-TT Port Number ..... 325
8.2.143 5GS User Plane Node ..... 326
8.2.144 Port Management Information Container ..... 326
8.2.145 Requested Clock Drift Information ..... 326
8.2.146 Time Domain Number ..... 327
8.2.147 Time Offset Threshold ..... 327
8.2.148 Cumulative rateRatio Threshold ..... 327
8.2.149 Time Offset Measurement ..... 328
8.2.150 Cumulative rateRatio Measurement ..... 328
8.2.151 SRR ID ..... 328
8.2.152 Requested Access Availability Information ..... 329
8.2.153 Access Availability Information ..... 329
8.2.154 MPTCP Control Information ..... 330
8.2.155 ATSSS-LL Control Information ..... 330
8.2.156 PMF Control Information ..... 330
8.2.157 MPTCP Address Information ..... 331
8.2.158 UE Link-Specific IP Address ..... 331
8.2.159 PMF Address Information ..... 332
8.2.160 ATSSS-LL Information ..... 333
8.2.161 Data Network Access Identifier ..... 333
8.2.162 Average Packet Delay ..... 333
8.2.163 Minimum Packet Delay ..... 334
8.2.164 Maximum Packet Delay ..... 334

8.2.165 QoS Report Trigger ....334
8.2.166 GTP-U Path Interface Type ....335
8.2.167 Requested Qos Monitoring ....335
8.2.168 Reporting Frequency ....336
8.2.169 Packet Delay Thresholds ....336
8.2.170 Minimum Wait Time ....337
8.2.171 QoS Monitoring Measurement ....337
8.2.172 MT-EDT Control Information ....338
8.2.173 DL Data Packets Size ....338
8.2.174 QER Control Indications ....338
8.2.175 NF Instance ID ....339
8.2.176 S-NSSAI ....339
8.2.177 IP version ....339
8.2.178 PFCPASReq-Flags ....339
8.2.179 Data Status ....340
8.2.180 RDS Configuration Information ....340
8.2.181 MPTCP Applicable Indication ....341
8.2.182 User Plane Node Management Information Container ....341
8.2.183 Number of UE IP Addresses ....341
8.2.184 Validity Timer ....342
8.2.185 Offending IE Information ....342
8.2.186 RAT Type ....342
8.2.187 L2TP User Authentication ....343
8.2.188 LNS Address ....344
8.2.189 Tunnel Preference ....344
8.2.190 Calling Number ....344
8.2.191 Called Number ....344
8.2.192 L2TP Session Indications ....345
8.2.193 DNS Server Address ....345
8.2.194 NBNS Server Address ....345
8.2.195 Maximum Receive Unit ....346
8.2.196 Thresholds ....346
8.2.197 Steering Mode Indicator ....346
8.2.198 Group Id ....347
8.2.199 CP IP Address ....347
8.2.200 IP Address and Port Number Replacement ....348
8.2.201 DNS Query Filter ....348
8.2.202 Event Notification URI ....349
8.2.203 Notification Correlation ID ....349
8.2.204 Reporting Flags ....349
8.2.205 Predefined Rules Name ....350
8.2.206 MBS Session Identifier ....350
8.2.207 Multicast Transport Information ....351
8.2.208 MBSN4mbReq-Flags ....351
8.2.209 Local Ingress Tunnel ....352
8.2.210 MBS Unicast Parameters ID ....353
8.2.211 MBSN4Resp-Flags ....353
8.2.212 Tunnel Password ....353
8.2.213 Area Session ID ....354
8.2.214 DSCP to PPI Mapping Information ....354
8.2.215 PFCPSDRsp-Flags ....354
8.2.216 QER Indications ....355
8.2.217 Vendor-Specific Node Report Type ....355
8.2.218 Configured Time Domain ....356

**Annex A (Informative): PFCP Load and Overload Control Mechanism ....357**

A.1 Throttling Aalgorithms ....357
A.1.1 "Loss" Throttling Algorithm ....357
A.1.1.1 Example of Possible Implementation ....357

**Annex B (Normative): CP and UP Selection Functions with Control and User Plane Separation ..... 358**

B.1 CP Selection Function ..... 358
B.1.1 General ..... 358

B.2 UP Selection Function ..... 358
B.2.1 General ..... 358
B.2.2 SGW-U Selection Function ..... 358
B.2.3 PGW-U Selection Function ..... 359
B.2.4 Combined SGW-U/PGW-U Selection Function ..... 359
B.2.5 TDF-U selection function ..... 360
B.2.6 UP Selection Function Based on DNS ..... 360
B.2.6.1 General ..... 360
B.2.6.2 SGW-U Selection Function Based on DNS ..... 360
B.2.6.3 PGW-U Selection Function Based on DNS ..... 360
B.2.6.4 Combined SGW-U/PGW-U Selection Function Based on DNS ..... 361

**Annex C (Informative): Examples scenarios ..... 362**

C.1 General ..... 362

C.2 Charging Support ..... 362
C.2.1 Online Charging ..... 362
C.2.1.1 Online Charging Call Flow – Normal Scenario ..... 362
C.2.1.2 Online Charging Call Flow with Credit Pooling ..... 364
C.2.1.2.1 General ..... 364
C.2.1.2.2 Example Call Flow 1 ..... 364
C.2.1.2.3 Example Call Flow 2 ..... 366

**Annex D (Normative): Use of PFCP over N16a for the support of traffic offload by UPF controlled by I-SMF ..... 369**

D.1 General ..... 369

D.2 Procedures ..... 370
D.2.1 Addition of PSA and UL CL/BP controlled by I-SMF ..... 370
D.2.2 Removal of PSA and UL CL/BP ..... 373
D.2.3 Change of PSA ..... 374
D.2.4 Traffic Usage Reporting ..... 374
D.2.5 Updating N4 information towards I-SMF ..... 374
D.2.6 PDU session release ..... 374
D.2.7 Simultaneous change of UL CL/BP and PSA controlled by I-SMF ..... 375
D.2.8 Simultaneous change of UL CL/BP and PSA controlled by different I-SMFs ..... 377

**Annex E (Informative): Procedures Related to MPTCP Functionality ..... 380**

E.1 General ..... 380

E.2 Multipath TCP Connection Setup ..... 380
E.2.1 General ..... 380
E.2.2 Outgoing Multipath TCP Connection Setup ..... 380
E.2.3 Incoming Multipath TCP Connection Setup ..... 380
E.2.4 MPTCP Session Entry Stored in MPTCP Proxy ..... 381

E.3 IP Translation Procedure ..... 381
E.3.1 General ..... 381
E.3.2 IP Translation on Uplink IP Packets ..... 382
E.3.3 IP Translation on Downlink IP Packets ..... 382

**Annex F (Informative): Change history ..... 383**

History ..... 391

# 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.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 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.

PFCP shall be used over:

- the Sxa, Sxb, Sxc and the combined Sxa/Sxb reference points specified in 3GPP TS 23.214 [2].
- 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].
- the N4 interface specified in 3GPP TS 23.501 [28] and 3GPP TS 23.502 [29].
- the N4mb interface specified in 3GPP TS 23.247 [72].

In this specification the term CP function applies to control plane nodes such as SGW-C, PGW-C, TDF-C, SMF and MB-SMF.

In this specification the term UP function applies to user plane nodes such as SGW-U, PGW-U, TDF-U, UPF and MB-UPF.

The prefix PFCP in message and procedure names is used to indicate that messages and procedures are common and used on Sx, N4 and N4mb reference points. A PFCP session refers to both Sx and/or N4 sessions, or to an N4mb session. A PFCP association is established between a CP function and a UP function, i.e., for EPC, between an SGW-C/PGW-C/TDF-C and an SGW-U/PGW-U/TDF-U, and for 5GC, between an SMF and a UPF or between an MB-SMF and MB-UPF.

In the related stage 2 specifications the prefix Sx, N4 and N4mb is used for these common procedures realised by PFCP.

Clauses or paragraphs that only apply to EPC or 5GC are indicated by the label "for EPC" or "for 5GC".

# 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".

[28] 3GPP TS 23.501:"System Architecture for the 5G System"

[29] 3GPP TS 23.502:"Procedures for the 5G System"

[30] IEEE 802.1Q: "Virtual Bridged Local Area Networks"

[31] IEEE 802.3: "IEEE Standard for Ethernet"

[32] IETF RFC 826: "An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses".

[33] IETF RFC 4861: "Neighbor Discovery for IP version 6 (IPv6)". .

[34] 3GPP TS 38.415: "NG-RAN; PDU Session User Plane Protocol".

[35] 3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace; Trace control and configuration management".

[36] IETF RFC 4282: "The Network Access Identifier".

[37] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".

[38] IETF RFC 3162: "RADIUS and IPv6".

[39] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[40] 3GPP TS 23.527: "5G System; Restoration procedures".

[41] 3GPP TS 29.512: "5G System; Session Management Policy Control Service; Stage 3".

[42] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[43] 3GPP TS 29.510: "5G System; Network Function Repository Services; Stage 3".

[44] 3GPP TS 23.503:"Policy and Charging Control Framework for the 5G System".

[45] 3GPP TS 32.255: "Telecommunication management; Charging management; 5G data connectivity domain charging; Stage 2".

[46] 3GPP TS 29.512: "Session Management Policy Control Service, Stage 3".

[47] 3GPP TS 33.127: "Security; Lawful Interception (LI) architecture and functions".

[48] 3GPP TS 23.003: "Numbering, addressing and identification".

[49] 3GPP TS 29.561: "5G System; Interworking between 5G Network and external Data Networks; Stage 3".

[50] 3GPP TS 29.502: "5G System, Session Management Services; Stage 3".

[51] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[52] IETF RFC 2236: "Internet Group Management Protocol, Version 2".

[53] IETF RFC 3376: "Internet Group Management Protocol, Version 3".

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

[55] IETF RFC 2710: "Multicast Listener Discovery (MLD) for IPv6".

[56] Void

[57] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[58] IEEE Std 802.1AS-2020: "IEEE Standard for Local and metropolitan area networks--Timing and Synchronization for Time-Sensitive Applications".

[59] 3GPP TS 24.193: "Access Traffic Steering, Switching and Splitting; Stage 3".

[60] IETF RFC 8803: "0-RTT TCP Convert Protocol".

[61] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[62] IETF RFC 8684: "TCP Extensions for Multipath Operation with Multiple Addresses".

[63] 3GPP TS 24.539: "5G System (5GS); Network to TSN translator (TT) protocol aspects; Stage 3".

[64] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[65] 3GPP TS 24.250: "Protocol for Reliable Data Service; Stage 3".

[66] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[67] IETF RFC 2661: Layer Two Tunneling Protocol "L2TP"

[68] IETF RFC 2868: RADIUS Attributes for Tunnel Protocol Support

[69] 3GPP TS 23.548: "5G System Enhancements for Edge Computing; Stage 2".

[70] Void

[71] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax".

[72] 3GPP TS 23.247:" Architectural enhancements for 5G multicast-broadcast services; Stage 2".

[73] 3GPP TS 29.564: "5G System; User Plane Function Services; Stage 3".

[74] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

# 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].

**Associated PDU Session:** A PDU Session associated to a multicast session that is used for 5GC Individual MBS traffic delivery method and for signalling related to a user's participation in a multicast session such as join and leave requests.

**Associated QoS Flow:** A unicast QoS Flow that belongs to the associated PDU Session and is used for 5GC Individual MBS traffic delivery method. The associated QoS Flow is mapped from a multicast QoS Flow in a multicast MBS session.

**CP function**: A node with a Control Plane function (see 3GPP TS 23.214 [2]) supporting one or more PFCP entities. A Control Plane function, i.e. a Control Plane Node, is identified by the Node ID that is set to either an FQDN or an IP address.

**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.

**Node:** Either a CP function or an UP function supporting one or more PFCP entities. A Node is identified by the Node ID, which is set to either an FQDN or an IP address.

**PFCP Entity**: An endpoint in a CP (or UP) function supporting PFCP, that is identified by the IP address. The IP address of a PFCP entity may or may not be the IP address included in the Node ID.

**UP function**: A node with a User Plane function (see 3GPP TS 23.214 [2]) supporting one or more PFCP entities. A User Plane function, i.e. a User Plane Node, is identified by the Node ID that is set to either a FQDN or an IP address.

## 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 |
| ATSSS | Access Traffic Steering, Switching, Splitting |
| ATSSS-LL | ATSSS Low Layer |
| BAR | Buffering Action Rule |
| BP | Branching Point |

| | |
|---|---|
| CP | Control Plane |
| DDoS | Distributed Denial of Service |
| DEI | Drop Eligible Indicator |
| DNAI | Data Network Access Identifier |
| DSCP | Differentiated Services Code Point |
| DS-TT | Device-Side TSN Translator |
| eMPS | enhanced Multimedia Priority Service |
| FAR | Forwarding Action Rule |
| F-SEID | Fully Qualified SEID |
| F-TEID | Fully Qualified TEID |
| IP | Internet Protocol |
| IPUPS | Inter-PLMN User Plane Security |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| I-SMF | Intermediate SMF |
| L2TP | Layer 2 Tunneling Protocol |
| LAC | L2TP Access Concentrator |
| LMISF | LI Mirror IMS State Function |
| LNS | L2TP Network Server |
| MA | Multi-Access |
| MA | Multi-Access |
| MAR | Multi-Access Rule |
| MBS | Multicast/Broadcast Service |
| MB-SMF | Multicast/Broadcast Session Management Function |
| MB-UPF | Multicast/Broadcast User Plane Function |
| MBSF | Multicast/Broadcast Service Function |
| MBSTF | Multicast/Broadcast Service Transport Function |
| MPTCP | Multi-Path TCP Protocol |
| MT-EDT | Mobile Terminated Early Data TransmissionNR New Radio |
| NPN | Non-Public Network |
| NW-TT | Network-side TSN Translator |
| PCC | Policy and Charging Control |
| PCP | Priority Code Point |
| 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 |
| PMF | Performance Measurement Function |
| PMIC | Port Management Information Container |
| PSA | PDU Session Anchor |
| PTP | Precision Time Protocol |
| QER | QoS Enforcement Rule |
| RDS | Reliable Data Service |
| 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 |
| SMF | Session Management Function |
| SNPN | Stand-alone Non-Public Network |
| SRR | Session Reporting Rule |
| 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 |
| TMGI | Temporary Mobile Group Identity |

| | |
|---|---|
| ToS | Type of Service |
| TSC | Time Sensitive Communication |
| TSCTSF | Time Sensitive Communication and Time Synchronization function |
| TSSF | Traffic Steering Support Function |
| UDP | User Datagram Protocol |
| UL CL | Uplink Classifier |
| UMIC | User Plane Node Management Information Container |
| UP | User Plane |
| UPF | User Plane Function |
| URR | Usage Reporting Rule |
| VID | VLAN Identifier |

# 4 Protocol Stack

## 4.1 Introduction

The protocol stack for the control plane over the Sxa, Sxb, Sxc, combined Sxa/Sxb, N4 and N4mb reference points shall be as depicted in Figure 4.1-1. Clauses 4.2 and 4.3 further specify the related UDP and IP requirements.

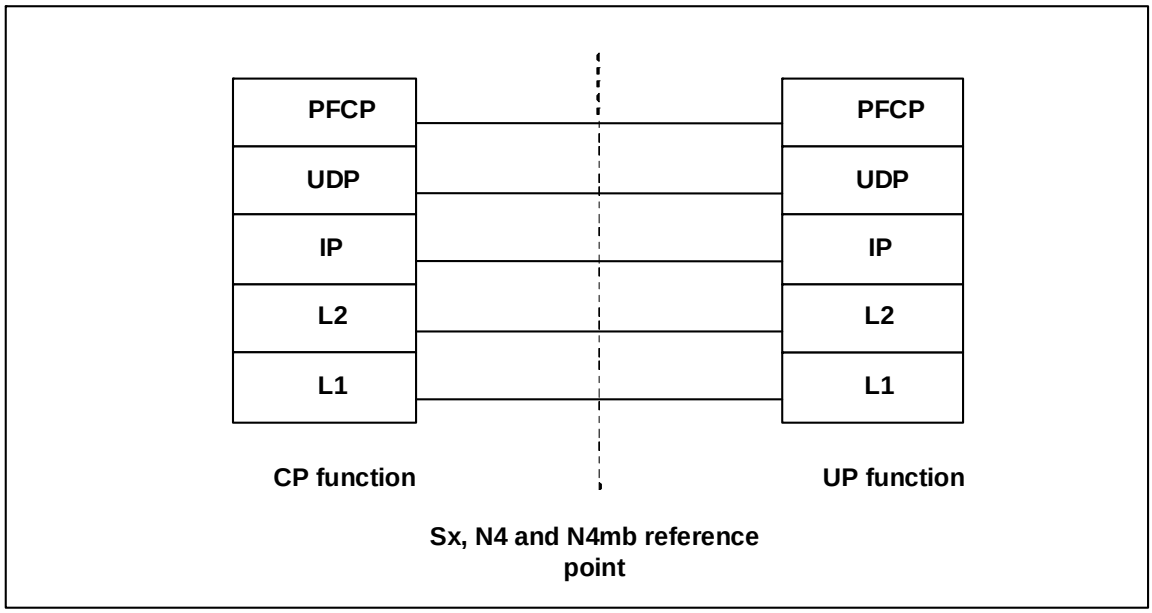



**Figure 4.1-1: Control Plane stack over Sxa, Sxb, Sxc, combined Sxa/Sxb, N4 and N4mb**

The protocol stack for the user plane over the Sxa, Sxb and N4reference points (see clause 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.

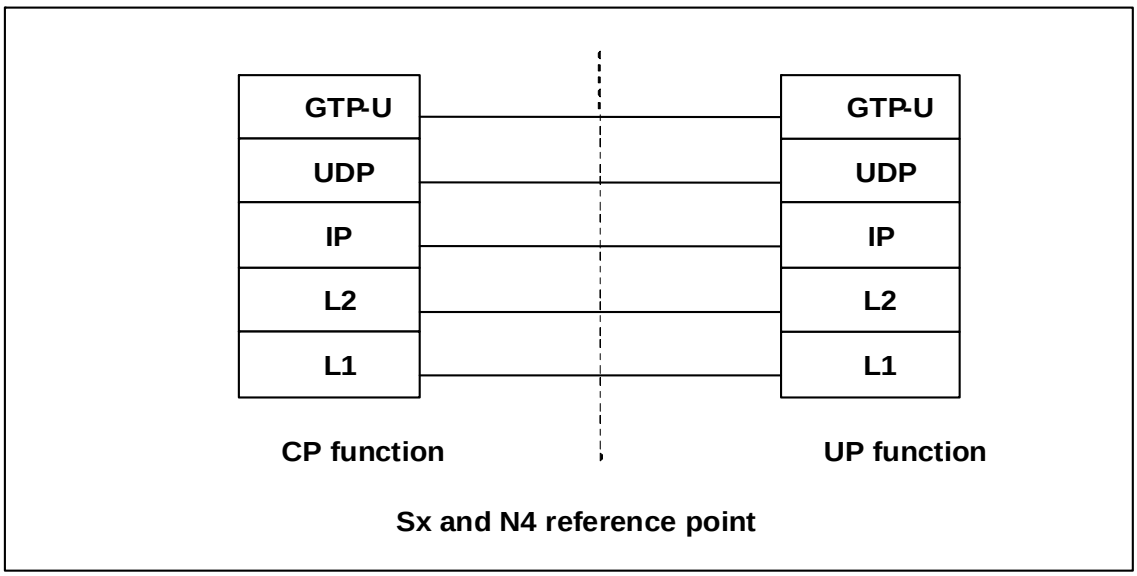



**Figure 4.1-2: User Plane stack over Sxa, Sxb, combined Sxa/Sxb and N4**

# 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 clause, "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 a PFCP 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 PFCP Session. The CP and the UP functions may change this IP address subsequently during a PFCP 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 clause 4.2 of 3GPP TS 23.214 [2].

The architecture reference model with SMF and UPF of 5GC nodes is described in clause 4.2 of 3GPP TS 23.501 [28].

The architecture reference model with MB-SMF and MB-UPF of 5GC nodes is described in clause 6.7 of 3GPP TS 23.247 [72].

This clause specifies the high level principles of the PFCP protocol and describe how 3GPP functionalities are realised on the Sxa, Sxb, Sxc, N4 and N4mb 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 packet forwarding scenarios supported over the N4 reference point are specified in 3GPP TS 23.501 [28] and 3GPP TS 23.502 [29].

The packet forwarding scenarios supported over the N4mb reference point are specified in 3GPP TS 23.247 [72].

The CP function controls the packet processing in the UP function by establishing, modifying or deleting PFCP Session contexts and by provisioning (i.e. adding, modifying or deleting) PDRs, FARs, QERs, URRs, BAR and/or MAR or by activating/deactivating pre-defined PDRs, FARs, QERs, URRs, per PFCP session context, whereby a PFCP session context may correspond:

- for EPC, 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.

- for 5GC, to an individual PDU session, a standalone PFCP session not tied to any PDU session or an MBS session.

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 or more FARs, 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;

    - accept or deny UE requests to join an IP multicast group;

    - forward, duplicate, drop or buffer the UL packet; or

    - forward the MBS session data to a Low Layer Source Specific Multicast (LL SSM) address (using multicast transport) and/or forward and replicate the MBS session data to multiple GTP-u peers (using unicast transport).

  - 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 PFCP 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 clause 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.

- zero or one MAR, which contains instructions related to Access Traffic Steering, Switching and Splitting (ATSSS) for the downlink traffic of a Multi-Access (MA) PDU session. See clause 5.2.7.

NOTE 2: A downlink PDR can be associated with two FARs for an N4 session established for an MA PDU session as an MAR contains two FARs for 3GPP and non-3GPP respectively.

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

The QoS Enforcement Rule Correlation ID shall be assigned by the CP function to correlate QERs from multiple PFCP 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 PFCP 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 PFCP sessions shall be provisioned, with the same QER contents, in each of these PFCP sessions. The QoS Enforcement Rule Correlation ID shall be only used to enforce the APN-AMBR when the UE is in EPC, it may be provided by the CP function over N4 to the UP function for a PDU session may move to EPC in a later stage.

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

- Every PDR provisioned for a PFCP session shall allow to identify the PFCP session, i.e. every PDR shall contain the information element(s) to identify the PFCP session, which is either a Traffic Endpoint Identifier (if the PDI Optimization feature is supported) or equivalent information, e.g. UE IP address, Local F-TEID, Frame-Route, in the PDI IE.

- 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 PFCP 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 PFCP sessions, not including the Packet Replication and Detection Carry-On Information IE, shall not overlap, i.e. PDRs in each PFCP session shall differ 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 PFCP session;

- 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 PFCP session, to control how the UP function shall process packets unmatched by any PDRs of any other PFCP 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.

- different PDRs of different PFCP sessions, including the Packet Replication and Detection Carry-On Information IE, may overlap. The Detection Carry-On Indication indicates that the UP function shall proceed with the look-up of other PDRs of other PFCP sessions matching the packet. This is used for broadcast traffic forwarding in 5G VN Group Communication.

- different downlink PDRs of different PFCP sessions, with a PDI including the IP multicast IP address IE, may overlap. The UP function shall proceed with the look-up of other PDRs of other PFCP sessions matching the packet. This is used for downlink IP multicast traffic for IPTV service (see clause 5.25).

- different downlink PDRs of different PFCP sessions, with a PDI including the MBS Session Identifier, may overlap. The UPF shall proceed with the look-up of other PDRs of other PFCP sessions with the same MBS Session Identifier matching the packets. This is used for multicast MBS services in 5GS using 5GC Individual Traffic Delivery (see clause 5.34).

On receipt of a user plane packet, the UP function shall perform a lookup of the provisioned PDRs in the UP function to identify only one PDR in a PFCP session according to the following steps:

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

- find the first PDR matching the incoming packet, among all the PDRs provisioned for this PFCP 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 which are identified with different IE type in the PDI of the PDR are matching the corresponding packet header fields unless specified otherwise. 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. If a match field has multiple instances, i.e. there are several IEs with the same IE type, a packet matches this match field if any instance is matching the corresponding packet header field.

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).

NOTE 3: A DL PDR can be provisioned with a UE IP address together with a Framed-Route or a Framed-IPv6-Rotue either in the PDI IE or in the Create Traffic Endpoint IE; in such case, the PDR is matched if the packet matches either the UE IP address or the Framed-Route (Framed-IPv6-Route).

When one or more pre-defined PDR(s) are activated for a given PDR (see clause 5.19), an incoming packet matches the PDR if it matches one of activated pre-defined PDR(s).

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.

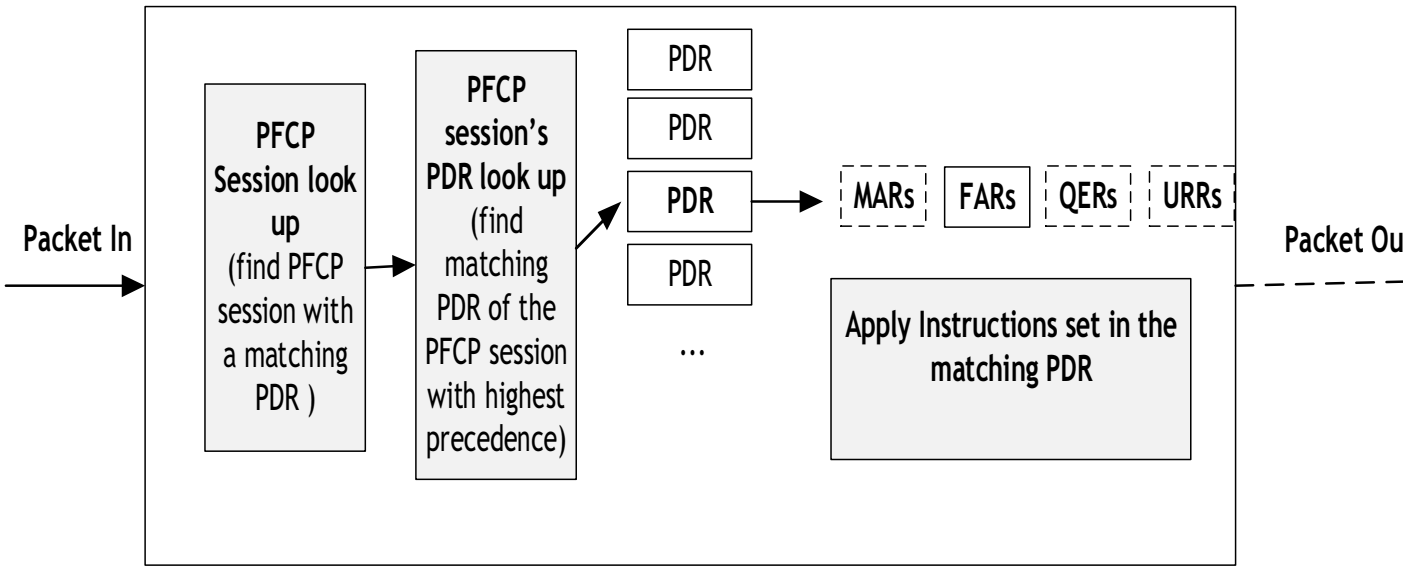



**Figure 5.2.1-1: Packet processing flow in the UP function**

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

NOTE 4: Deleting a QER in one PFCP session does not result in deleting another QER in another PFCP 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, URR or MAR is uniquely identifying a rule of the corresponding rule type within a session.

For an MA-PDU session, IP addresses translation for MPTCP traffic (see Annex E.3) is independent from the handling of URR/QER/BAR, but it shall be performed before applying the FAR (e.g. before creating the outer header and forwarding the packet).

## 5.2.1A Packet Detection Rule Handling

### 5.2.1A.1 General

When provisioning a PDR in the UP function, the CP function shall provide the PDI with the following information:

- the source interface of the incoming packets;
- a combination of the parameters, that incoming packets are requested to match, among: Local F-TEID, Network Instance, UE IP address(es), SDF Filter(s) and/or Application ID. For 5GC, the PDI may additionally contain one or more QFI(s) to detect traffic pertaining to specific QoS flow(s), Ethernet Packet Filter(s), Ethernet PDU Session Information (see clause 5.13.1) and/or DNS Query Filter(s).

The requirements for provisioning an SDF filter in the PDI are specified in clauses 5.2.1A.2A and 5.2.1A.3.

The CP function may provision the parameters, that incoming packets are requested to match, in the UP function by:

- providing the parameters individually in each PDI of the PFCP session; or
- optionally, if the PDI Optimization feature is supported by the UP function, by providing the parameters which may be common to multiple PDIs of a same PFCP session in a Traffic Endpoint IE and by referencing this Traffic Endpoint in the PDI(s) of the PFCP session. See clause 5.2.1A.2. A Traffic Endpoint may include a Local F-TEID, Network Instance, UE IP address(es) and/or Ethernet PDU Session Information (see clause 5.13.1).

NOTE: A Traffic Endpoint can correspond to a GTP-u endpoint, an SGi or an N6 endpoint.

### 5.2.1A.2 PDI Optimization

The PDI Optimization feature should be supported by CP and UP functions complying with this release of the specification. This feature allows the CP function to optimize the signaling towards the UP function by creating the information that are common to multiple PDRs as a Traffic Endpoint with a Traffic Endpoint ID and then referring to this common information from multiple PDRs. The Traffic Endpoint ID shall be unique within a PFCP session. If MTE feature is supported, one PDI may refer to more than one Traffic Endpoints. When a PDI refers to a Traffic Endpoint, the parameters that are in the Traffic Endpoint shall not be once again provided in the PDI. The CP function may update the Traffic Endpoint at any time.

If a Traffic Endpoint is updated, all the PDRs that refer to this Traffic Endpoint in the UP function shall use the updated information.

The UP function shall allocate and store the F-TEID associated to the Traffic Endpoint. When the UP function provides the allocated F-TEID to the CP function in the PFCP Session Establishment response or PFCP Session Modification response message, the CP function shall update the Traffic Endpoint information stored in the CP function with the received F-TEID.

The CP function should use a Traffic Endpoint ID created in a different PFCP message only after getting the confirmation from the UP function of the Traffic Endpoint ID creation.

If the CP function deletes a Traffic Endpoint, the UP Function shall delete all the PDRs that refer to this Traffic Endpoint.

NOTE 1: The requirements specified in clause 5.2.2.3.1 for reporting usage reports to the CP function also apply if the deletion of the Traffic Endpoint results in deleting the last PDR associated to a URR.

NOTE2: For EPC, the Remove Traffic Endpoint IE can be used to delete a bearer for which multiple PDRs exist (with the same Traffic Endpoint ID).

### 5.2.1A.2A Provisioning of SDF filters

When provisioning an SDF Filter in a PDI, the CP function shall:

- copy the Flow Description if it is received from the PCRF (or PCF), in the corresponding PDI of a PDR regardless of whether the PDR is for matching uplink or downlink traffic;

NOTE 1 The Flow Description received from the PCRF (or PCF) is set assuming downlink flows only, see clause 5.4.2 of 3GPP TS 29.212 [8]. The CP function uses the Flow-Direction AVP received from the PCRF (or PCF) to determine the actual direction and thus the source interface of the packet flows described in the Flow Description.

- for traffic from CP-function or SGi-LAN:
  - If the traffic is intended to be forwarded to the UE, the CP function shall provision the Flow Description with IPFilterRule "source" parameters set to correspond to the CP function or SGi-LAN and the IPFilterRule "destination" parameters correspond to the UE;
  - If the traffic is intended to be forwarded to the PDN, the CP function shall provision the Flow Description with IPFilterRule "source" parameters set to correspond to the CP function or SGi-LAN and the IPFilterRule "destination" parameters correspond to the PDN.

The UP function shall apply the SDF filter based on the Source Interface of the PDR as follows (see also clause 8.2.5):

- when the Source Interface is CORE, this indicates that the filter is for downlink data flow, so the UP function shall apply the Flow Description as is;
- when the Source Interface is ACCESS, this indicates that the filter is for uplink data flow, so the UP function shall swap the source and destination address/port in the Flow Description;
- when the Source Interface is CP-function or SGi-LAN, the UP function shall use the Flow Description as is.

#### 5.2.1A.3 Bidirectional SDF Filters

The CP function may provision bidirectional SDF Filters in the UP function (see clause 8.2.5), i.e. SDF Filters that may be associated to both uplink and downlink PDRs of a same PFCP/N4 session, as follows:

- when provisioning a bidirectional SDF Filter the first time for a PFCP/N4 session, the CP function shall provision the SDF filter definition together with a SDF Filter ID uniquely identifying the SDF Filter among all the SDF Filters provisioned for a given PFCP/N4 Session;
- the CP function may then provision a PDR for the same PFCP/N4 session but the opposite direction, by provisioning the SDF Filter ID in the SDF filter ID field of the PDI, without provisioning again the SDF filter definition;
- the UP function shall apply any modification of a bidirectional SDF Filter to all PDRs of the PFCP/N4 session making use of this SDF Filter;
- upon deletion of a PDR making use of a bidirectional SDF Filter, the UP function shall still apply the SDF Filter for any other PDR making use of the SDF Filter.

The requirements specified for provisioning SDF filters in clause 5.2.1A.2A shall also apply when provisioning bidirectional SDF Filters.

#### 5.2.1A.4 Application detection with PFD

The detection information for a given application may be provisioned by the CP function to the UP function via PFD management procedure. See clause 6.2.5.

The PFDE (PFD Enhancement) feature may be optionally supported by the CP function and UP function. When the feature is supported in both the CP function and UP function, the CP function may provision a PFD Contents IE including a property (i.e. either flow description, or URL or Domain Name/Domain Name Protocol) with multiple values.

NOTE 1: It is assumed, when the PFDE feature is not supported, a PFD Contents can only include a property with one value.

When the UP function attempts to detect the traffic pertaining to an application by using the application's PFDs (see clause 7.4.3.1 and 8.2.39), the UP function shall consider:

- the application is detected if the incoming traffic matches at least one PFD Contents;
- one PFD Contents is matched if the incoming traffic matches every property contained in the corresponding PFD Contents IE;
- the incoming traffic matches one property (i.e. flow description, URL and Domain Name/Domain Name Protocol) if it matches at least one value of the property.

NOTE 2: Interpretation of the Custom PFD Content is implementation specific.

### 5.2.2 Usage Reporting Rule Handling

#### 5.2.2.1 General

The CP function shall provision URR(s) for a PFCP session in a PFCP Session Establishment Request or a PFCP 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 or when an immediate report is requested within a PFCP Session Modification Request.

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

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

#### 5.2.2.2.1 General

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 PFCP 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 (or only allow forwarding of some limited user plane traffic, based on operator policy in the UP function) 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: For EPC, 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]). For 5GC, the Dropped DL Traffic Threshold can be armed in a UPF for triggering the SMF Pause of Charging feature (see 3GPP TS 23.502 [29]).

- 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 enforcement, e.g. bitrate enforcement for QoS, Gate control enforcement (as specified in clause 5.4.3) or packets dropped as requested by the FAR;

- a Measurement Information with the 'Measurement of Number of Packets' flag set to "1", to request the UP function to measure the number of packets be transferred in UL/DL/Total in addition to the measurement in octets, if the UP function supports the MNOP feature.

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 (or only allow forwarding of some limited user plane traffic, based on operator policy in the UP function) and, if no Time Threshold is provisioned, to also generate a usage report, when the measured traffic reaches the quota;

- a Measurement Information with the "Immediate Start Time Metering" flag set to "1", to request the UP function to start time metering immediately at receiving the flag; otherwise, the UP function shall start time metering when the first packet is received; 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 until a new non-zero Inactivity Detection Time is received or the time-based usage measurement is stopped. See Figure 5.2.2.2-1:

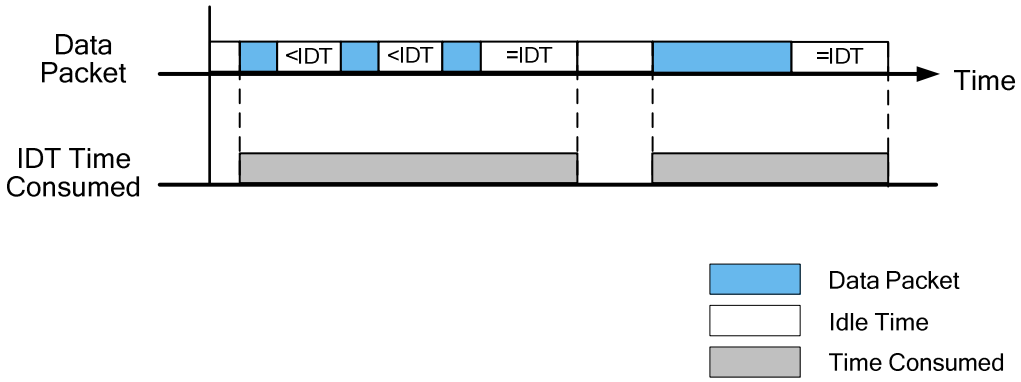



**Figure 5.2.2.2-1: IDT based charging**

NOTE 2: The Inactivity Detection Time can be set to the Quota Consumption Timer if received. The Inactivity Detection Time is not used to control when the time metering starts.

- For EPC, 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 clause 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:

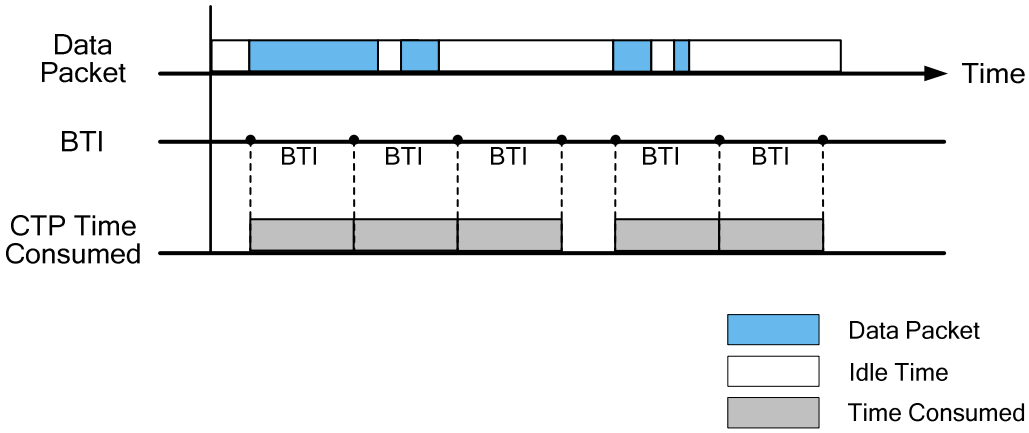



**Figure 5.2.2.2-2: CTP based charging**

- 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:

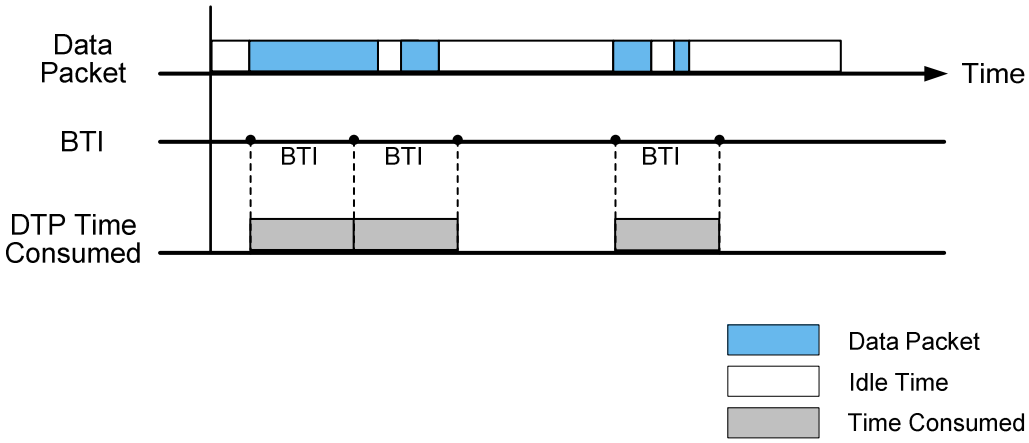



**Figure 5.2.2.2-3: DTP based charging**

When the time-based measurement method applies, and when the Envelope Reporting is required for EPC, 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 set the Reduced Application Detection Information flag in the Measurement Information of the URR, when requesting the detection of start and stop of an application solely for the purpose of envelope reporting for EPC.

The CP function may provision a Volume Threshold IE, a Volume Quota IE, or both (and/or respectively a Time/Event Threshold IE, a Time/Event Quota IE, or both). In such a case, the CP function may set the reporting trigger for threshold (VOLTH/TIMTH/EVETH) and/or the reporting trigger for quota (VOLQU/TIMQU/EVEQU)) in the Reporting Triggers IE.

When both a Volume (or Time or Event) Threshold IE and a Volume (or Time or Event) Quota IE are provisioned and only the reporting trigger for threshold (VOLTH/TIMTH/EVETH) is set, the UP function shall send a usage report only when reaching the Volume (or Time or Event) Threshold. When subsequently reaching the Volume (or Time or Event) Quota, the UP function shall stop forwarding packets (or only allow forwarding of some limited user plane traffic, based on operator policy in the UP function) without sending a new usage report to the CP function.

If both a Volume (or Time or Event) Threshold IE and a Volume (or Time or Event) Quota IE are provisioned and both of the respective Threshold and Quota reporting triggers are set, the UP function shall send a usage report when reaching the Volume (or Time or Event) Threshold and also later on when subsequently reaching the Volume (or Time or Event) Quota.

NOTE 3: A UP Function complying with Release 14 or Release 15 of the specification only sends one usage report when the threshold is reached, even if both reporting triggers (for the threshold and the quota) are set.

NOTE 4: After sending a usage report on reaching a threshold, the UP function typically gets a new quota before the earlier provisioned quota exhausts. This implies that the UP function typically sends a quota report when reaching the final quota.

NOTE 5: 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 6: 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 (or only allow forwarding of some limited user plane traffic, based on operator policy in the UP function), without sending a second usage report, when the granted volume (or time) quota is exhausted.

For event based measurement method, the CP function may provision:

- the Event Threshold IE, to request the UP function to generate a usage report when the number of events reaches the event threshold;

- the Event Quota IE, to request the UP function to stop forwarding packets applicable to the event (or only allow forwarding of some limited user plane traffic, based on operator policy in the UP function) and, if no Event threshold is provisioned, to also generate a usage report, when the number of events reaches the event quota;

NOTE 7: An event is preconfigured with one or more event detection logic in the UPF. Each event detection logic is associated with an Application ID. The CP function activates the detection and reporting of an event by provisioning PDR(s) with the PDI set to an Application ID and by provisioning a URR with an event threshold or event quota reporting trigger. The CP function identifies an event reported in a Usage Report by the URR ID.

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 (or only allow forwarding of some limited user plane traffic, based on operator policy in the UP function) when no packets have been received for the duration indicated in this parameter;

NOTE 8: 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 Quota Validity Time, if the VTIME feature is supported by UP function, to request the UP function to send a usage report after the validity duration is over. After Quota validity timer expiry, if packets are received on UPF, the UPF shall stop forwarding packets or only allow forwarding of limited user plane traffic, based on operator's policy in the UP function;

NOTE 9: After sending the usage report triggered by the QUHTI or QUVTI (i.e. the Quota Holding Time or Quota Validity Time expires), any remaining quota for the URR is discarded in the UP function.

- a Monitoring Time IE and zero or more Additional Monitoring IEs, 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/or time, and/or event thresholds at the monitoring time. The CP function may additionally provision a Subsequent Volume (or Time or Event) Threshold IE and/or a Subsequent Volume (or Time or Event) Quota IE, for a volume (or time or event) 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 or Event) Threshold IE, if provisioned in the URR, or to the remaining value of the Volume (or Time or Event) 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 separate usage reports as specified in clause 5.2.2.3.1;

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

- an User Plane Inactivity Timer, to request the UP function to send an usage report when no packets have been received for any of the PDRs associated to the URR for the duration indicated in this parameter.

If the UP function indicated support of the Quota Action feature in the UP Function Features IE, when the CP function provisions a Volume Quota or Time Quota or Event Quota in a URR, the CP function may also provision the "FAR ID for Quota Action" IE identifying the substitute FAR the UP function shall apply, for the traffic identified by the PDR to which the URR is associated, when exhausting any of these quotas. This FAR may require the UP function to drop the packets or buffer the packets or redirect the traffic towards a redirect destination as specified in clause 5.4.7.

If the UP function has indicated support of the QUASF feature as specified in clause 8.2.25, and when the CP function provisions a Volume Quota, Time Quota, or Event Quota in a URR, the CP function may also provision the Exempted Application ID for Quota Action IE or the Exempted SDF Filter for Quota Action IE, to instruct the UP function, that traffic matching the associated PDR(s) and matching the Application ID(s) or SDF Filter(s) shall be handled based on the FAR associated with the PDR as normal, even when the quota has been exhausted.

NOTE 10: The traffic forwarded after the quota has been exhausted need not to be measured.

NOTE 11: A PDR can be associated with multiple URRs. If one of these URRs requires the UP function to drop the user data packets, e.g. when the Quota has been exhausted, the other URRs associated to the PDR need also to stop their measurements, except for URRs including the Measurement Information with the 'Measurement Before QoS Enforcement' flag set to "1".

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

NOTE 12: This can be used in a PGW-U for the PGW Pause of Charging procedure (see 3GPP TS 23.401 [14]).

When the NSPOC feature as specified in clause 5.30 is supported by the CP and UP function, the CP function may provision:

- an Measurement Information with the 'Send Start Pause of Charging' Flag set to "1", to request the UP function (SGW-U or I/V-UPF) to send a Start Pause of Charging indication to the upstream GTP-U entity(s) when the Dropped DL Traffic Threshold is reached.

- an Measurement Information with the 'Applicable for Start of Pause of Charging' Flag set to "1", to indicate the UP function to stop the usage measurement for the URR when receiving Start Pause of Charging indication from the peer downstream GTP-U entity.

When the NSPOC feature is supported by the CP and UP functions, the CP function may use the "SUMPC" and "RUMUC" flags in the PFCPSMReq-Flags IE, and the "SUMPC" flag in the PFCPSEReq-Flags IE, to request the UP function to stop or resume the usage measurement for all URRs with the ASPOC flag set to "1". The CP function may set the "CIAM" flag in the Measurement Information IE in a Create URR or a Update URR IE to request the UP function to stop or resume the usage measurement according to the value of the Inactive Measurement flag for a specific URR with the "ASPOC" flag set to "1" if necessary. See also clause 5.30.

The CP function may request the UP function to measure network resources usage and generate the corresponding Usage Reports only for a number of times, by provisioning the "Number of Reports" IE in a URR, if the UP function supports the NORP feature (see clause 8.2.25-1). If so, the URR shall become inactive in the UP function after the requested "Number of Reports" have been reported.

The CP function may resume the measurement for an inactive URR by setting the Inactive Measurement flag of the Measurement Information IE of the URR to "0" in the Update URR IE in a PFCP Session Modification Request message, with or without the Number of Report IE if the URR was deactivated by setting the Inactive Measurement flag of the Measurement Information IE of the URR to from "0" to "1".

For any other cases, i.e. the URR becoming inactive, which is not caused by changing the Inactive Measurement flag from "0" to "1", the CP may resume the URR:

- by provisioning a Number of Report IE with a (new) non-zero value (to receive the corresponding number of usage reports) or with a null length (to request UP function to perform continous measurement) when the requested Number of Reports has been reached;

- by setting the CIAM flag to "1" and the INAM flag to "0" if the URR was provisioned with ASPOC bit set to "1" in the Update URR (for the URR) when the CP function has requested to stop usage measurement for pause of charging by setting the SUMPC flag to "1"; or

- by associating (new) PDR(s) with the URR when the last PDR associated with the URR has been removed.

If the CP function wishes the UP function to perform continuous measurement for a URR which was provisioned with a Number of Reports (i.e. to no longer limit the number of reports to be generated), the CP function shall provide the Number of Reports IE in the Update URR with a null length to delete the limit on the number of reports to be generated.

NOTE 13: The Number of Reports can be provisioned in an URR regardless which Measurement Method is used.

#### 5.2.2.2.2 Credit pooling (for EPC)

For EPC, when the Credit Pool feature is supported and the CP function (e.g. PGW-C) is instructed to handle a Credit Pool for a given Gy Session, the CP function shall create a URR for the Credit Pool, and in this URR, the CP function:

- shall include one Aggregated URR ID IE per URR sharing the credit pool, including the URR ID of the URR sharing the credit pool and the associated Multiplier to measure the abstract service units the corresponding traffic consumes from the credit pool;

- shall set the Time or Volume Threshold or Quota IE to the value calculated as specified in IETF RFC 4006 [16] according to the Measurement Method.

  NOTE 1: The value can be calculated using the following formula:

  S = Q1*M1 + Q2*M2 + ... + Qn*Mn,
  where the S is the quota for the credit pool, Qn is the quota and Mn is the multiplier for each Rating Group (RG) which are provided via the Multiple Services Credit Control from the OCS.
  An URRn is defined for each of RG.

  NOTE 2: When the Measurement Method is set to the combined volume/duration, the Time and Volume Threshold or Quota are calculated independently.

- may set the Reporting Trigger to reporting upon reaching a volume or time threshold or quota;

- may set the Measurement Method to the data volume, duration (i.e. time), combined volume/duration according to the Measurement Method set in the URRs in the Credit Pool.

NOTE 3: The UP function is instructed to handle a Credit Pool when a G-S-U-Pool-Reference AVP is included within a Multiple Services Credit Control from the OCS. A Credit Pool is identified by the G-S-U-Pool-Identifier AVP. See clause 6.3.11, 6.4.3 and 6.4.4 of 3GPP TS 32.299 [18].

In addition, the CP function shall also include the Linked URR IE, set to the Credit Pool URR ID, in all the URRs which are sharing the credit pool (i.e. which are associated with RGs sharing the Credit Pool).

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

#### 5.2.2.3.1 General

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 PFCP 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 set to "0" for the first Usage Report and incremented for every subsequent 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 an 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 all the thresholds (Volume/Time/Event Threshold) provisioned for the related URR, if the usage report was triggered due to one of the thresholds being reached, i.e. upon the reporting triggers VOLTH/TIMTH/EVETH; otherwise, if the usage report was triggered for other reporting triggers, adjust the thresholds (Volume/Time/Event Threshold) respectively by subtracting the (volume/time/event) reported usage in the usage report to determine when to generate the next report for reporting triggers VOLTH/TIMTH/EVETH;

- when the quota (Volume/Time/Event Quota) is provisioned in the URR:

  - adjust the quota for volume/time/event respectively by subtracting the (volume/time/event) reported usage in the usage report and use it when applying quota related handling, e.g. to drop or buffer the packets, or apply FAR ID for Quota Action (if provisioned) when the quota becomes "0" and to generate the relevant usage report if the corresponding reporting trigger(s)(VOLQU/TIMQU/EVEQU) is set;

  - consider no quota left for the URR when the usage report was triggered for the reporting triggers QUHTI and QUVTI; and

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

When receiving a new threshold and/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 and/or quota to determine when to send its next usage report to the CP function or to apply quota handling, i.e. the UP function shall discard any remaining quota.

At receiving a quota with value set to zero, the UP function shall:

- handle packets based on the FAR associated with the PDR, if the packets match the Application ID(s) or the SDF Filter(s) provisioned in the IE Exempted Application ID for Quota Action or the Exempted SDF Filter for Quota Action;

- apply the FAR identified in the FAR ID for Quota Action IE if the CP function has provisioned it, otherwise the UP function shall stop forwarding packets (or only allow forwarding of some limited user plane traffic, based on operator policy in the UP function); and

- report in a usage report the network resources usage measurement since the last usage report for that URR, if applicable.

When the UP function receives a non-zero quota for the same URR in one subsequent PFCP Session Modification Request message, the UP function shall apply the (normal) FAR associated with the PDR (detecting the application traffic) for the buffered traffic if the FAR ID for Quota Action was set to buffer the application traffic at zero quota (either be provisioned with zero quota earlier or the quota has been exhausted).

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.

NOTE 2: When receiving a new threshold or quota from the CP function for a measurement that is already ongoing in the UP function and if the UP function has already generated the usage report but had not sent it, the UP function can send the usage report before performing the update of the URR.

NOTE 3: A URR with the quota set to 0 can be provisioned when a service data flow is not allowed to start before quota is allocated to the service. See clause 5.4.11.

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. PFCP 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. For a URR, when multiple (Additional) Monitoring Time IEs are provisioned, or a new Monitoring Time is provisioned after the previous Monitoring Time has passed, the UP function may not be able to send the usage report with the Usage Information set to "AFT" for the previous Monitoring Time if there is no Reporting Trigger armed before the next Monitoring Time is reached; in such case, the UP function may send multiple usage reports with the Usage Information set to "BEF", together with one usage report with the Usage Information set to "AFT".

NOTE 4: 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 PFCP 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. PFCP 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.

For the volume-based measurement method, the UP function shall include all the counters (Total, Uplink and Downlink) of the URR in the Volume Measurement IE in the Usage Report IE; the UP function shall also include the

number of packets counted for Total, Uplink, Downlink in the Volume Measurement IE if requested by the CP function and if the UP function supports the MNOP feature.

An usage report triggered only due to the Dropped DL Traffic Threshold (DROTH) or Start of Traffic (START), or MAC Address Reporting (MACAR), or IP Multicast Join/Leave (IPMJL) shall not contain any measurement information, i.e. either the Volume/Duration Measurement set to zero or Volume/Duration Measurement IE is not present.

When being instructed to remove a URR or the last PDR associated to a URR, the UP function shall stop its ongoing measurements for the URR and include a Usage Report in the PFCP Session Modification Response or in an additional PFCP Session Report Request if there are non-null measurements to report for the URR. When being instructed to remove the last PDR associated to a URR, the UP function shall keep the URR and reset any measurement for the URR.

NOTE 5: A URR provisioned in a PFCP session can be provisioned/kept in the UP function without being associated with any PDR and the URR can be associated with a PDR in a later stage. The UP function will not remember any remaining quota and will consider the quota (if provisioned) as it was provisioned.

When being instructed to deactivate a network resources usage measurement via the Inactive Measurement flag of the Measurement Information IE of the URR, the UP function shall stop measuring the network resources usage (against the volume/time/event threshold/quota) and store the current measurement counts which will be resumed when the URR is activated again. The UP function shall not generate a usage report upon the deactivation of the URR and it shall send a usage report during the period when the URR is deactivated for the following scenarios:

- if the Quota Holding Time is expired and if the reporting trigger QUHTI is set;
- if the Quota Validity Time is expired and if the reporting trigger QUVTI is set;

NOTE 6: The Quota Holding Time can have been started before the URR is deactivated or starts from the moment when the URR is deactivated since no quota will be consumed.

- if it is the time for a periodic reporting and if the reporting trigger PERIO is set;
- if it is required to send a usage report for this URR when a usage report is reported for a linked URR and if the reporting trigger LIUSA is set;
- if it is required to send an immeditate report upon a query for the URR, or the URR is removed, dissociated from the last PDR;

NOTE 7: Multiple usage reports can be required to be reported to the CP function when deleting a PDR that is the last one to be associated to multiple URRs.

- if the User Plane Inactivity Timer is expired and if the reporting trigger UPINT is set.

NOTE 8: The User Plane Inactivity Timer can have been started before the URR is deactivated.

The CP function may request the UP function, in a PFCP Session Modification Request, to report its ongoing network resources measurement for one or multiple URRs of the PFCP session. In this case, the UP function shall:

- generate usage report(s) (based on the existing definition of any URR(s) included in the PFCP Session Modification Request message before any update) for the URR(s) being queried and for any associated linked usage reports (see clause 5.2.2.4) for which there are non-null measurements to report;
- include them in the PFCP Session Modification Response or in additional PFCP Session Report Request messages; and
- proceed as specified above upon generating a usage report for a URR towards the CP function, with the following additions:
    - if the PFCP Session Modification Request includes the Update URR IE (for the URR being queried) with a Volume or Time Threshold, the UP function shall re-apply the threshold received in the request;
    - otherwise, if a threshold and/or a quota had been set for the URR that is queried, since the usage report is not triggered due to the threshold being reached, the UP function shall adjust the threshold and/or quota by subtracting the time/volume reported in the usage report to determine when to generate the next report.

NOTE 9: Upon reaching a threshold that was adjusted due to a URR query as specified above, the UP function re-applies then the threshold that was provisioned in the URR (i.e. not the value of the adjusted threshold).

NOTE 10: The CP function can query a URR without including a Volume or Time Threshold in the PFCP Session Modification Request e.g. when it needs to close a traffic volume/service container (see clause 5.2.3.10.3 of 3GPP TS 32.251 [17]).

NOTE 11: The CP function can query a URR including a Volume or Time Threshold in the PFCP Session Modification Request e.g. when it needs to close a CDR (see clause 5.2.3.10.3 of 3GPP TS 32.251 [17]). In such a case, the CP function can include the same threshold for the URR being queried in the Update URR IE in the PFCP Session Modification Request message to trigger the UP function to re-apply the threshold.

NOTE 12: 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 PFCP session. As an exception, the UP function always generates an immediate report when being instructed to remove a URR.

When additional usage reports need to be sent in additional PFCP Session Report Request messages, i.e. when not all usage reports can be included in the PFCP Session Modification Response message, the UP function shall indicate, in the PFCP Session Modification Response message, either:

- that more usage reports will follow, by setting the AURI flag to 1 in the Additional Usage Reports Information IE (see clause 8.2.91); or

- the total number of additional usage reports that will be sent in all the additional PFCP Session Report Request messages (i.e. that will be sent after the PFCP Session Modification/Deletion Response message), by setting this value in the Additional Usage Reports Information IE (see clause 8.2.91).

In the former case (i.e. if the UP function indicates in the PFCP Session Modification Response message that more usage reports will follow), the UP function shall indicate, in one of the additional PFCP Session Report Request message, the total number of additional usage reports to be sent after the PFCP Session Modification Response message, by setting this value in the Additional Usage Reports Information IE. In both cases, the UP function may set the AURI flag to 1 in every additional PFCP Session Report Request message but the last one, to indicate that more usage reports will follow.

Besides, if the PFCP Session Modification Request included the Query URR Reference IE, usage reports sent in response to the query in the PFCP Session Modification Response and/or additional PFCP Session Report Request messages shall include the Query URR Reference IE set to the same value as received in the PFCP Session Modification Request.

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;

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

When the UP function supports the NORP feature and if a URR is provisioned with a "Number of Reports" IE, the number of Usage Reports generated according to the Reporting Trigger(s) defined in the URR shall not be more than the value of "Number of Reports". If the UP function is requested to resume the measurement for an inactive URR, the UP function shall generate a maximum number of Usage Reports equal to the new value of the Number of Reports IE received in the Update URR if any, or equal to the value of the Number of Reports IE previously provisioned in the URR if any; if no Number of Reports IE was provisioned before, there is no limit on the number of reports to send. If the CP function provisions a "Number of Reports" IE together with a Monitoring Time and/or a Measurement Information where the "Measurement Before QoS Enforcement' flag is set to "1" in a URR, the UP function shall generate usage reports as required by the Monitoring Time and/or the Measurement Information where the "Measurement Before QoS Enforcement' flag is set to "1" in a URR, which may lead UP function to generate more usage reports than the value of the "Number of Reports" IE.

NOTE 14: If the CP function expects to receive the exact number of usage reports as requested in the Number of Reports, it can abstain from provisioning a Number of Report IE together with a Monitoring Time and/or a Measurement Information where the "Measurement Before QoS Enforcement' flag is set to "1" in a URR.

At the PFCP session termination, the UP function shall indicate to the CP function, in the PFCP Session Deletion Response, the resources that have been consumed for each URR that was provisioned in the PFCP session since the last usage report (respective to each URR). A CP function may indicate support of Additional Usage Reports in PFCP Session Deletion Request by setting the ARDR flag in the CP Function Features IE (see clause 8.2.58). When additional PFCP Session Report Request messages need to be sent:

- the UP function shall:
  - set the cause to "More Usage Report to send" in the PFCP Session Deletion Response;
  - include the Additional Usage Reports Information IE in PFCP Session Deletion Response with either the AURI flag set to "1" or indicating the total number of additional usage reports that will be sent in all the additional PFCP Session Report Request messages; as described above:
    - in the former case, the UP function shall indicate in one additional PFCP Session Report Request message the total number of additional usage reports that will be sent after the PFCP Session Deletion Response;
    - in both cases, the UP function may set the AURI flag to 1 in every additional PFCP Session Report Request message but the last one, to indicate that more usage reports will follow.
  - set the PSDBU flag to 1 in the last PFCP Session Report Request message.
- when the CP function receives a PFCP Session Deletion Response with the Cause set to "More Usage Report to send", the CP function shall not delete the PFCP session until it receives a PFCP Session Report Request message with the PSDBU flag set to "1" (that indicates this is the last report), or it has received the number of usage reports indicated in the Additional Usage Reports Information IE in PFCP Session Deletion Response, or until an implementation specific timer expires otherwise.

At the PFCP session termination, the UP function shall set the PURU flag to "1" in the PFCP Session Deletion Response if it has pending PFCP Session Report Request messages which have not been acknowledged yet. This indicates that the CP function should wait for some time before deleting the PFCP Session.

Upon receiving the Usage Report from the UP function, the CP function may initiate PFCP Session Modification procedure as result of the communication with the PCRF or OCS, as described in clause 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 PFCP session.

#### 5.2.2.3.2 Credit pooling

When a URR is received with at least one Aggregated URRs IE included, the UP function:

- shall calculate the traffic usage of the URR by applying the Multiplier(s) and aggregating the traffic usage from all URRs indicated in the Aggregated URRs IE(s), as specified in IETF RFC 4006 [16];

NOTE 1: The usage of this URR is calculated using the following formula:

C1*M1 + C2*M2 + ... + Cn*Mn = U,
where U is the usage counted by this URR, Cn is the usage counted by each aggregated URR (i.e. URR for each RG sharing the credit pool), and Mn is the multiplier for each aggregrated URR.

- shall generate a report when the counted usage exceeds the threshold;

- shall generate a report if the threshold is not provided, and stop packets forwarding (or only allow forwarding of some limited user plane traffic, based on operator policy in the UP function) for all Aggregated URRs when the counted usage exceeds the quota.

NOTE 2: The handling of the aggregated URR(s), e.g. generating a Usage Report upon the Reporting Trigger(s) is not impacted by handling of this URR for the Credit Pool.

#### 5.2.2.3.3 Traffic Usage Reporting with Redundant Transmission

The following requirements shall apply when using Redundant Transmission on N3/N9 interfaces or Redundant Transmission at transport layer:

- the UPF shall not count redundant packets in Usage Reports (e.g. Volume Measurement), i.e. it shall count the traffic only once in Usage Reports;

- the SMF shall provide the quota for the non-redundant transmission (i.e. not counting redundant traffic).

### 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 1: 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").

NOTE 2: This can be used by the CP function e.g. to request the UP function to report a Usage Report for a RG (i.e. URR "X") when the UP function reports a Usage Report for a credit pool to which this RG pertain (i.e. URR "Y").

When a usage report is to be generated for the URR "Y", regardless of the condition which triggers the report, 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.

NOTE 3: This also applies e.g. when an immediate usage report is requested for the URR "Y"within a PFCP session Modification Request.

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

A RG level URR may be linked to IP-CAN bearer level URR as well as IP-CAN Session level URR to enable the CP function to generate a CDR on the different level. In such case, a URR "X" may link to more URRs than just URR "Y".

### 5.2.2.5 End Marker Reception Reporting

The CP function may request the UP function to report the End Marker reception during UE Triggered Service Request with, or without I-SMF insertion/change/removal procedures (see clauses 4.2.3.2 and 4.23.4.3 in 3GPP TS 23.502 [29]):

- If a new I-UPF is selected by the SMF to replace the old I-UPF, the SMF may provide two PDRs to the new I-UPF, e.g. PDR-1 for DL data from the PSA UPF, where the Apply Action IE in FAR-1 associated with PDR-1 is set to BUFF; and e.g. PDR-2 for receiving the buffered DL data from the old I-UPF, where the Apply Action IE in FAR-2 associated with PDR-2 is set to FORW. In this case, the SMF shall indicate to the new I-UPF to report the reception of the End Marker packet from the old I-UPF, by providing a URR related to PDR-2 with REEMR flag set to 1 in the Reporting Triggers IE, which is included in a Create URR IE within PFCP Session Establishment Request.

- If the SMF removes the old I-UPF but does not replace it with a new I-UPF, then the SMF may provide two PDRs to the PSA UPF, e.g. PDR-3 for receiving DL data across N6, where the Apply Action IE in FAR-3 associated with PDR-3 is set to BUFF; and e.g. PDR-4 for receiving the buffered DL data from the old I-UPF, where the Apply Action IE in FAR-4 associated with PDR-4 is set to FORW. The SMF shall indicate to the PSA UPF to report the reception of the End Marker packet from the old I-UPF, by providing a URR related to PDR-4

with REEMR flag set to 1 in the Reporting Triggers IE which is included in a Create URR IE within PFCP Session Modification Request.

Once the End Marker packet is received from the old I-UPF, the UPF (either new I-UPF or the PSA UPF) shall inform the SMF about this by sending the PFCP Session Report Request with the Usage Report IE containing the usage measurement as instructed in the URR, where EMRRE flag shall be set to 1 in a Usage Report Trigger IE and shall discard the End Marker packet(s). The SMF shall instruct the UPF to start sending the buffered DL data identified by PDR-1 or PDR-3 by sending a PFCP Session Modification Request message, where the Apply Action IE in the FAR-1/FAR-3 related to PDR-1/PDR-3 shall be changed from BUFF to FORW.

## 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 a PFCP 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 clause 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;
- forward the MBS session data:
  - using multicast transport, by setting the FSSM flag together with the MBS Multicast Parameters to forward the packets to a Low Layer source specific multicast address; and/or
  - using unicast transport by setting the MBSU flag together with one or more MBS Unicast Parameters to forward and replicate the packets towards one or more GTP-U DL tunnels terminated at PSA UPF(s) and/or NG-RAN(s).
- buffer downlink or uplink 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;
- notify the CP function about the first discarded DL packet for each service data flow identified by a PDR, when the CP function requests the UP function to buffer DL packets but the DL Buffering Duration or the DL Buffering Suggested Packet Count is exceeded, or when the CP function requests the UP function to drop DL packets and a packet is discarded directly, by setting the DDPN flag, if the UP function supports the DDDS feature;
- notify the CP function about first buffered DL packet for each service data flow identified by a PDR, by setting the BDPN flag, if the UP function supports the DDDS feature;
- duplicate the packets, by setting the DUPL flag and by provisioning the Duplicating Parameters providing instructions on how to forward the duplicated packets;
- accept or deny UE requests to join an IP multicast group (see clause 5.25), by setting the IPMA or IPMD flag;
- duplicate the packets for redundant transmission (see clause 5.24.2), by setting the DFRT flag and by provisioning the Redundant Transmission Forwarding Parameters IE providing instructions on how to forward the duplicated packets for redundant transmission;
- eliminate duplicate packets used for redundant transmission (see clause 5.24.2), by setting the EDRT flag and by provisioning the Redundant Transmission Detection Parameters IE providing instructions on how to detect the duplicated packets for redundant transmission.

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

The CP function may request the UP function to forward the packets and duplicate the packets for redundant transmission.

The CP function may request the UP function to forward the packets and eliminate duplicate packets used for redundant transmission.

The CP function may provision one or more FAR(s) per PFCP session. Different FARs of a same PFCP 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 (in EPC), or when it receives a first downlink packet for each QoS flow for a given FAR (in 5GC), by sending a PFCP 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 PFCP Session Report Request messages for the same PFCP session.

NOTE 3: Receipt of downlink packets pertaining to different QoS flows associated to the same FAR can result in sending multiple PFCP Session Report Request messages for the same PFCP session. The CP function identifies the QFI based on the PDR ID (when different PDRs are used for different QoS flows) or based on the Downlink Data Service Information IE.

NOTE 4: The end marker packet is not considered as DL data packet so that it does not trigger the UP function to notify the CP function about the arrival of a DL packet. The UP function can discard the received end marker packet(s) silently, when it is not possible to be forwarded.

If the UP function indicated support of Header Enrichment of UL traffic (see clause 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 5: 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 clause 4.3.17.8.3.3.3 of 3GPP TS 23.401 [14]) for Non-IP PDN connections.

If the UP function indicated support of PDI optimisation (see clause 8.2.25), the CP function may include in the forwarding parameters of the FAR the Linked Traffic Endpoint ID, if it is available, identifying the traffic Endpoint allocated for this PFCP session to receive the traffic in the reverse direction.

NOTE 6: This information can enable an SGW-U or PGW-U to correlate the UL and DL traffic (i.e. PDRs) sent over a same bearer.

Assuming for instance a PFCP session provisioned in a PGW-U with:

- an UL PDR 1 (for an S5/S8 bearer 1) with Source Interface "Access" associated to an UL Traffic Endpoint ID "1" (comprising the IP address, a local TEID and optionally a network instance),

- a DL PDR 1 with Source Interface "Core", UE IP address and SDF 1,

the CP function sets the Linked Traffic Endpoint in the DL FAR 1 (associated to DL PDR 1) to the UL Traffic Endpoint "1", which allows the PGW-U to correlate the uplink and downlink PDRs for the same bearer (i.e. that UL PDR 1 associated to UL Traffic Endpoint "1", and DL PDR1 associated to DL FAR 1 with Linked Traffic Endpoint set to UL Traffic Endpoint "1", use the same S5/S8 bearer).

NOTE 7: The Linked Traffic Endpoint can possibly refer to a Traffic Endpoint in the reverse direction requested to be created in the same PFCP request.

## 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 PFCP 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 a PFCP session and associate it to the FAR(s) of the PFCP session in a PFCP Session Establishment Request or a PFCP 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 a PFCP Session Modification Request (for EPC); or
- the Downlink Data Notification Delay (for EPC), DL Buffering Duration and/or DL Buffering Suggested Packet Count in a PFCP Session Report Response message.

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

If the UP Function has indicated support of the feature UL/DL Buffering Control (UDBC), the CP function may provide the Suggested Buffering Packet Count IE in a BAR which is created during a PFCP Session Establishment procedure or a PFCP Session Modification procedure, and the CP function may modify it in a subsequent PFCP Session Modification Request, and/or a PFCP Session Report Response message. The same BAR may be associated with all the FARs in a PFCP session to indicate that all Service Data Flows in the PFCP Session share the same buffer in the UP function for the PFCP Session.

If the SGW-U has indicated support of the feature MT-EDT, the CP function may provide the MT-EDT (Mobile Terminated Early Data Transmission) Control Information IE in a BAR when it is created and modified, to request the SGW-U to report the sum of DL Data Packets Size in byte when sending Downlink Data Report.

In this release of the specification, at most one BAR may be created per PFCP 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:

- For EPC, the Downlink Data Notification Delay IE, to request the UP function to delay the sending of a PFCP 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 clause 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 clause 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 Suggested Buffering Packet Count IE if the UP Function has indicated support of the feature UDBC, to indicate the number of packets (including both uplink or downlink) that the CP function suggests to be buffered in the UP function, until it receives new instructions from the CP function, e.g. when the new Quota is granted.

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.

The UP function shall stop applying buffering when new instruction is received from the CP function. The buffered packets shall be either dropped or forwarded following the packet forwarding model specified in clause 5.2.1 and taking into consideration that the buffered Packets have been already processed earlier.

## 5.2.5 QoS Enforcement Rule Handling

### 5.2.5.1 General

The CP function shall provision QER(s) for a PFCP session in a PFCP Session Establishment Request or a PFCP 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 clause 5.4.3;
- QoS Control, i.e. MBR, GBR or Packet Rate enforcement, as specified in clause 5.4.4;
- DL flow level marking for application detection, as specified in clause 5.4.5;
- SCI (Service Class Indicator) marking for service identification for improved radio utilisation for GERAN, as specified in clause 5.4.12;
- for 5GC reflective QoS for uplink traffic.

### 5.2.5.3 Reflective QoS (for 5GC)

The 5GS may support Reflective QoS functionality (see clauses 5.7.5 in 3GPP TS 23.501 [28]).

When the 5GC determines to use Reflective QoS for a specific SDF, the SMF shall set the Reflective QoS Indication (RQI) bit to 1 in the QER associated to the DL PDR for this SDF in a PFCP Session Establishment Request or PFCP Session Modification Request message.

The SMF may also provision the UPF to perform uplink QoS flow binding verification for the specific SDF as specified in clause 5.4.2.

When the 5GC determines to no longer use Reflective QoS for a specific SDF, the SMF shall request the UPF to stop applying Reflective QoS for the corresponding downlink traffic, e.g. by setting the Reflective QoS Indication (RQI) bit to 0 in the QER that is associated to the DL PDR or by dissociating the QER from the DL PDR (as appropriate) in a PFCP Session Modification Request message.

If the SMF had provisioned the UPF to perform uplink QoS flow binding verification for the specific SDF, after an operator configurable time, the SMF shall update the UL PDR(s) to no longer perform uplink QoS flow binding verification for the corresponding uplink traffic and QFI.

## 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 clause 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 PFCP 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 PFCP session;
- the CP function may provision concurrently parameters in a message or for the PFCP session that are applicable to Sxa and Sxb.

## 5.2.7 Multi-Access Rule Handling (for 5GC)

### 5.2.7.1 General

The UP function (i.e. the UPF) shall support the Multi-Access Rule (MAR) if it supports the ATSSS feature (see MPTCP and ATSSS-LL flags in UP Function Features, Table 8.2.25-1).

The CP function (i.e. the SMF) shall provision in the UP function acting as the PDU Session Anchor (PSA) and supporting the ATSSS feature, one and only one MAR for every downlink PDR corresponding to non-GBR traffic of a PFCP session that is established for a Multi-Access (MA) PDU session.

The MAR provides instructions to the UP function on how to forward the packets matching the PDR over 3GPP and non-3GPP accesses. See clauses 5.8.2.11.8 and 5.32.8 in 3GPP TS 23.501 [28].

In an MAR, the CP function (i.e. the SMF) shall:

- instruct the UPF which traffic steering functionality to use, i.e. MPTCP or ATSSS-LL, using the Steering Functionality IE (see clause 8.2.124);
- set the Steering Mode to instruct how the packets shall be distributed across 3GPP and non-3GPP accesses, e.g. Active-Standby, Smallest Delay, Load Balancing and Priority Based (see clause 8.2.125);
- provision access specific forwarding action information including:
  - a FAR ID which control the packets forwarding either to 3GPP access or non-3GPP access;
  - a Weight to indicate the proportion of traffic to be forwarded by the given FAR when the Steering Mode is set to "Load Sharing";
  - a Priority to indicate at which condition the traffic is to be forwarded by the given FAR when the Steering Mode is set to "Active-Standby" or "Priority-Based";
  - a list of URR IDs to enable the SMF to request separate usage report for different accesses.

As specified in clause 5.32.8 of 3GPP TS 23.501 [28], in an MAR, the CP function (i.e. the SMF) may:

- provision Threshold values, including RTT and/or Packet Loss Rate, if the Steering Mode is Load Balancing with fixed split percentages or Priority-based;
- include a Steering Mode Indicator to indicate that the default steering parameters provided in the Steering Mode may be adjusted:
  - set autonomous load-balance flag to allow the UPF to adjust the traffic steering based on its own decisions when the Steering Mode is Load Balancing; or
  - set UE-assistance flag to allow the UPF to adjust the traffic steering based on the UE Assistance Data from UE when the Steering Mode is Load Balancing.

NOTE: The autonomous load-balance flag and the UE-assistance flag can not be set to "1" at the same time.

The CP function may provision one or more MAR(s) (for different PDRs) per PFCP session. Different MARs of a same PFCP session may be provisioned with a different steering functionality and/or a different steering mode. Different MARs of a same PFCP session may be associated with the same FAR(s).

If a UE indicates it supports MPTCP and ATSSS-LL, and if the network determines to apply both MPTCP functionality and ATSSS-LL functionality for the UE's PDU session, the CP function shall provision separate downlink PDRs for MPTCP traffic and for Non-MPTCP traffic. Correspondingly, different MARs shall be provisioned and associated with the separate downlink PDRs. The steering functionality shall be set to ATSSS-LL for the MAR associated with the downlink PDR for non MPTCP traffic.

The UP function shall distribute the downlink traffic across the two access networks (and the two N3/N9 tunnels) according to the instructions received in the MAR and feedback information received from the UE via the user plane (e.g. access network Unavailability or Availability reports for ATSSS-LL received by PMF, see 3GPP TS 24.193 [59]).

If the autonomous load-balance is set in the Steering Mode Indicator, the Weight shall be treated as the default percentages, and the UPF may autonomously determine its own percentages for traffic splitting to maximize the aggregated bandwidth in the downlink direction. If the UE-assistance is set in the Steering Mode Indicator, the UE may inform the UPF on how it decided to distribute the UL traffic of the matching SDF.

## 5.2.8 Session Reporting Rule Handling

### 5.2.8.1 General

The CP function may provision SRR(s) for a PFCP session in a PFCP Session Establishment Request or a PFCP Session Modification Request to request the UP function to detect and report events for a PFCP session that are not related to specific PDRs of the PFCP session or that are not related to traffic usage measurement.

- Change of 3GPP or non-3GPP access availability, for an MA PDU session (see clause 5.20.4.2).
- Reporting the per QoS flow per UE QoS Monitoring Report, as specified in clause 5.33.3.2 of 3GPP TS 23.501 [28].

### 5.2.8.2 Provisioning of Session Reporting Rule in the UP function

#### 5.2.8.2.1 General

When provisioning an SRR, the CP function shall provide control information identifying the events that the UPF is requested to detect and report. If Direct Reporting of QoS monitoring events to Local NEF or AF is supported and required, the CP function shall also provide Direct Reporting Information in the SRR (see clause 5.33.5).

The CP function may modify an SRR in the PFCP Session Modification Request message.

The CP function may request the UP function to stop the detection and reporting of specific events by removing the SRR or, if the SRR is used to control different types of events, by updating the SRR with a control information IE for the events to stop with a null length. When so instructed, the UP function shall stop detecting and reporting the corresponding events.

### 5.2.8.3 Reporting of Session Report to the CP function

#### 5.2.8.3.1 General

When detecting that a provisioned event to report occurs, the UP function shall generate a Session Report for the related SRR and send it to the CP function by initiating the PFCP Session Report procedure, unless Direct Reporting of QoS monitoring events to Local NEF or AF applies (see clause 5.33.5).

Upon generating a session report for an SRR towards the CP function or towards the Local NEF or AF if Direct Reporting of QoS monitoring event applies, the UP function shall continue to apply all the provisioned SRR(s), until getting any further instruction from the CP function.

## 5.2.9 Handling of Rules that cannot be activated

The CP function shall indicate support of the Partial Success (PSUCC) feature (see clause 8.2.58) during the PFCP association setup or update procedure, if it supports PFCP session establishment or modification with Partial Success, i.e. with the UP function partially accepting a PFCP session establishment or modification request when some rules requested to be created or modified cannot be applied, e.g. when a pre-defined rule name or pre-defined rule ID is not configured in the UP function.

If the CP function indicated support of the the PSUCC feature, and if this feature is also supported by the UP function, the UP function should partially accept a PFCP session establishment or modification request, if possible, even when it fails to create or modify one or more rules. In such a case, the UP function shall set the cause to "Request partially accepted" in the response and include the Partial Failure Information IE identifying the rules that the UP function could not activate and the cause of the failure.

NOTE: Partial acceptance of a request is not possible in some cases, when the failure to activate a rule would result in a PFCP session state that is not consistent, e.g. if no PDR or FAR would end up being activated for the PFCP session. Details on the conditions when a request can be partially accepted or not are left to UP function implementation.

Upon receipt of a PFCP session establishment or modification response indicating a partial acceptance of the request, the CP function shall consider that not all rules were successfully activated in the UP function and determine those which failed to be activated based on the Partial Failure Information IE in the response.

If the CP function or the UP function does not support the PSUCC feature, the UP function shall reject a PFCP session establishment or modification request if at least one rule fails to be applied.

# 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] for EPC and 3GPP TS 23.501 [28] for 5GC).

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

| | Scenario description | Data forwarding direction | For EPC applicable to | For 5GC 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 | UPF to SMF<br>SMF to UPF |
| 2 | Forwarding of packets between the CP function and the external PDN (over SGi) / DN (over N6). | UP to CP function<br>CP to UP function | PGW | UPF to SMF<br>SMF to UPF |
| 3 | Forwarding of packets subject to buffering in the CP function. | UP to CP function<br>CP to UP function | SGW | UPF to SMF<br>SMF to UPF |
| 4 | Forwarding of End Marker Packets constructed by the CP function to a downstream node. | CP to UP function | SGW, PGW | SMF to UPF |
| 5 | Forwarding of user data using Control Plane CIoT 5GS Optimisation | UP to CP function<br>CP to UP function | - | UPF to SMF<br>SMF to UPF |

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 PFCP 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 PFCP 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 PFCP 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.

For EPC PFCP 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.

For 5GC PFCP session contexts may correspond to individual PDU sessions or standalone sessions not tied to any PDU sessions used e.g. for forwarding RADIUS, Diameter or DHCP signalling between the SMF and the DN or for forwarding End Marker packets from the SMF to a downstream UPF or NG-RAN.

For EPC 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.

For 5GC the CP function may establish one N4-u tunnel per:

- PDU session e.g. for the data forwarding scenarios 1, 3 and 5;
- UP function or DN 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 clause 5.3.3.

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

Requirements for forwarding user data using Control Plane CIoT 5GS Optimisation between the UP and CP functions (scenario 5) are further specified in clause 5.3.5.

## 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 clause 5.8 of 3GPP TS 23.214 [2] for EPC and in clause 5.8.2.9 of 3GPP TS 23.501 [28] for 5GC. The support of End Marker packets by the UP function is optional.

A UP function complying with this release of the specification shall support constructing End Marker packets in the UP function and shall indicate so to the CP function by setting the EMPU flag in the UP Function Features (see clause 8.2.25).

A CP function complying with this release of the specification should request the UP function to construct End Marker packets. If so, 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 PFCP 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 or NG-u UPF F-TEID);
- encapsulate the constructed GTP-U End Marker packets in GTP-U packets according to the principles specified in clause 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 PFCP session, after receipt of the PFCP Session Modification Response indicating that the UP function has switched to a new F-TEID.

Upon receipt of a PFCP 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 clause 5.3.1.

The CP function shall establish one Sx-u tunnel per bearer of a PDN connection / one N4-u tunnel per PDU session when applying the data forwarding scenario 3.

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

For EPC, 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.

For 5GC, 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 an PSA-UPF, or G-PDUs (i.e. T-PDU plus a GTP-U header) for an I-UPF, 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 N4-u tunnel corresponding to the PDU session of the PDN connection.

NOTE 2: An I-UPF receiving G-PDUs from an N9 GTPU tunnel forwards the same G-PDUs towards the SMF but with the IP address and TEID in the GTP-U header changed to the SMF IP address and TEID of the corresponding N4-u tunnel.

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

- for EPC, 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;

- for 5GC, a PDR per PDU session, matching the received downlink user plane packets and for an I-UPF, 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 3: The PDR can be provisioned in the UP function before applying data forwarding to the CP function.

For EPC, 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.

For 5GC, G-PDUs sent from the UP function to the CP function over the N4-u tunnel shall include any GTP-U extension header(s):

- possibly received by the UP function over the N9 PDU sessions 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:

- for EPC, 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;

- for 5GC, over N4-u as G-PDUs with the GTP-U header set to the IP address and TEID uniquely assigned in the UP function for the N4-u tunnel set up for the corresponding PDU session.

G-PDUs sent over Sx-u / N4-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 (for EPC) or per PDU session (for 5GC), with an IP address and TEID uniquely assigned in the UP function for the Sx-u / N4-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 PFCP-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 PFCP-u tunnel per UP function or PDN, in addition to the requirements specified in clause 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 / N6 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 PFCP-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:

- for supporting data forwarding scenario "1" as specified in clause 5.3.1, an additional PDR for a PFCP session established for a PDN connection or a PDU session which requires such data forwarding, matching the received user plane packets from uplink direction. The Outer Header Removal IE shall not be present if the complete G-PDU is required to be forwarded, otherwise the Outer Header Removal IE shall be present and set to "0" or "1" for IPv4 or IPv6 respectively;

- for supporting data forwarding scenario "2" as specified in clause 5.3.1, a PDR matching the received user plane packets from downlink direction;

- 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" for IPv4 or IPv6 respectively, and the Outer GTP-U header set to the IP address and TEID uniquely assigned in the CP function for the Sx-u tunnel.

### 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 PFCP-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 PFCP-u tunnel set up for the UP function or PDN or DN for traffic to be sent towards SGi or N6; 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 PFCP-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, I-UPF) 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 PFCP-u tunnel, and with the field Outer Header Removal Description in the Outer Header Removal IE set to "0" or "1";

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

### 5.3.5 Forwarding of user data using Control Plane CIoT 5GS Optimisation (for 5GC)

#### 5.3.5.1 General

The following requirements shall apply to the data forwarding scenario 5 of Table 5.3.1-1 in addition to the requirements specified in clause 5.3.1.

The CP function shall establish one one N4-u tunnel per PDU session when applying the data forwarding scenario 5.

#### 5.3.5.2 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]) from N6 or G-PDUs (i.e. T-PDU plus a GTP-U header) received from N9, 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 N4-u tunnel corresponding to the PDU session.

NOTE: A UPF receiving G-PDUs from N9 forwards the G-PDUs towards the SMF but with the IP address and TEID in the GTP-U header changed to the SMF IP address and TEID of the corresponding N4-u tunnel.

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

- a PDR per PDU session, matching the received downlink user plane packets, and for traffic received from N9, 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 perform GTP-U/UDP/IPv4 or GTP-U/UDP/IPv6 encapsulation.

NOTE: 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 N4-u tunnel shall include any GTP-U extension header(s):

- possibly received by the UP function over the N9 interface and stored during the Outer Header Removal;

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

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

Likewise, when sending the uplink traffic received in the CP function to the UP function, the uplink traffic shall be forwarded over N4-u as G-PDUs with the GTP-U header set to the IP address and TEID uniquely assigned in the UP function for the N4-u tunnel set up for the corresponding PDU session.

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

a PDR per PDU session, with an IP address and TEID uniquely assigned in the UP function for the N4-u tunnel, and with the field Outer Header Removal Description in the Outer Header Removal IE set to "0" or "1";

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

## 5.4 Policy and Charging Control

### 5.4.1 General

This clause describe how Policy and Charging Control requirements are supported over the Sxa, Sxb, Sxc and N4 reference points.

## 5.4.2 Service Detection and Bearer/QoS Flow Binding

Service detection refers to the process that identifies the packets belonging to a service data flow or application. For EPC, see clauses 6.2.2.2 and 6.8.1 of 3GPP TS 23.203 [7]. For 5GC, see clause 6.2.2.2 of 3GPP TS 23.503 [44].

For EPC, bearer binding is the procedure that associates service data flow(s) 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 clauses 6.1.1.4 and 6.2.2.2 of 3GPP TS 23.203 [7].

For 5GC, QoS flow binding is the procedure that associates service data flow(s) to a QoS flow deemed to transport the service data flow. UL QoS flow binding verification refers to the process of discarding uplink packets due to no matching QoS flow for the uplink direction. See clause 6.1.3.2.4 of 3GPP TS 23.503 [44] and clause 5.7.1.7 of 3GPP TS 23.501 [28].

For 5MBS, QoS flow binding is the procedure that associates a PCC rule to a QoS Flow within an MBS Session. See clause 6.10 in 3GPP TS 23.247 [72].

Service detection is controlled over the Sxa, Sxb, Sxc and N4 reference points by configuring Packet Detection Information in PDRs to match the intended service data flows or application.

For EPC, 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).

For 5GC, the mapping of DL traffic to QoS flows is achieved by configuring QERs with QFI(s) for the QoS flow marking and associating FARs to the downlink PDRs, with FARs set to forward the packets to the appropriate downstream GTP-U tunnel (N9 or N3).

For EPC, 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(s) or the Application ID. As a result, uplink packets received on the uplink bearer but that do not match the SDF filter(s) or Application detection filter associated to the uplink PDRs are discarded.

For 5GC, uplink QoS flow binding verification (see clause 5.7.1.7 of 3GPP TS 23.501 [28]) is achieved by configuring Packet Detection Information in uplink PDRs containing the local F-TEID of the uplink PDU session, the UE IP address (source IP address to match for the incoming packet), the QFI of the QoS flow and the SDF filter(s) or the Application ID. As a result, uplink packets received on the uplink PDU session but that do not match the SDF filter(s) or Application detection filter and QFI 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 clauses 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.

NOTE 4: The UPF can be provisioned with a PDR (with low precedence) which contains the CN tunnel info, QFI and filter information that can detect any unwanted/unauthorized traffic with this QFI so that such traffic can be dropped with or without being counted before.

## 5.4.3 Gating Control

Gating control refers to the process within the user plane function (i.e. PGW-U and TDF-U for EPC, UPF for 5GC) 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 (for EPC see clause 4.3.2 of 3GPP TS 23.203 [7] and for 5GC see clause 4.3.3.1 of 3GPP TS 23.503 [44]).

The PGW-C and TDF-C (for EPC) and the SMF (for 5GC) controls the gating in the PGW-U and TDF-U (for EPC) and in the UPF (for 5GC) 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 (for EPC) and the UPF (for 5GC) 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 (for EPC) and the UPF (for 5GC) shall apply UL and DL gating accordingly.

The UP function shall discard packets matching a PDR if the PDR is associated with at least one QER provisioned with the Gate Status set to CLOSED.

### 5.4.4 QoS Control

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

- for EPC,
  - 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.
- for 5GC,
  - at the session level (Session-AMBR or UL and DL Packet Rate of a PDU session);
  - at the QoS Flow level;
  - at the service data flow (SDF) or application level.

See clause 4.3.3 of 3GPP TS 23.203 [7] clause 4.5.5 of 3GPP TS 29.212 [8] and clause 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, QoS Flow (for 5GC), 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;
- creating QERs for the QoS enforcement of the aggregate of SDFs with the same GBR QFI (for 5GC);
- 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 CP function 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 clauses 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 PFCP 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, TDF-U or UPF for the accumulated usage of network resources per:

- individual or group of service data flows;
- individual or group of applications;
- PDU session, possibly excluding an individual SDF or a group of service data flow(s) (for 5GC);
- IP-CAN session, possibly excluding an individual SDF or a group of service data flow(s) (for EPC); and/or
- TDF session, possibly excluding an individual application or a group of application(s) (for EPC).

For EPC, see clauses 4.4, 6.2.2.3 and 6.6 of 3GPP TS 23.203 [7] and clauses 4.5.16, 4.5.17, 4b.5.6, 4b.5.7 of 3GPP TS 29.212 [8].

For 5GC, see clauses 4.3.4 and 6.2.2.3 of 3GPP TS 23.503 [44] and clauses 4.2.2.10, 4.2.3.11, 4.2.4.10, 4.2.6.2.5, 4.2.6.5.3 of 3GPP TS 29.512 [41].

Usage Monitoring Control is supported over the Sxb, Sxc and N4 reference points by activating in the UP function the reporting of usage information towards the CP function, as specified in clauses 5.3 and 7.8.4 of 3GPP TS 23.214 [2] and in clause 5.8.2.6.2 of 3GPP TS 23.501 [28].

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 PFCP 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 PFCP 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, TDF or UPF, towards a redirect destination, e.g. redirect some HTTP flows to a service provisioning page. For EPC, see clause 6.1.13 of

3GPP TS 23.203 [7] and clauses 4.5.2.6 and 4b.5.1.4 of 3GPP TS 29.212 [8]. For 5GC, see clause 6.1.3.12 of 3GPP TS 23.503 [44] and clause 4.2.6.2.4 of 3GPP TS 29.512 [46].

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

For EPC and5GC, the traffic redirection shall be enforced 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 clause 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 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;
    - For HTTP traffic redirection, the Redirection Address Type shall be set to "URL" and the CP function shall set the Destination Interface IE in the FAR to "Access" (to forward the HTTP response message with a status code indicating redirect). For other types of traffic redirection, the Destination Interface IE in the FAR may be set to "Core";

  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 PFCP 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), or a specific N6-LAN traffic steering policy in the UPF (PDU Session Anchor), 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 or N6-LAN, per service data flows level or applications level.

Application Function influencing traffic routing (see clause 5.6.7 of 3GPP TS 23.501 [28]) also uses traffic steering for the purpose of steering the subscriber's traffic over N6, e.g. to a local access to a Data Network.

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

Traffic Steering is supported over the Sxb, Sxc and N4 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. Traffic steering is alternatively supported over the N4 reference point by instructing the UP function to route packets according to N6 routing information in the FAR (e.g. providing an IP address in the Outer Header Creation).

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 or N6-LAN.

See 3GPP TS 23.203 [7], 3GPP TS 29.212 [8] and 3GPP TS 23.501 [28].

The CP function shall control Traffic Steering towards SGi-LAN, N6-LAN or N6 in the UP function by:

- creating the necessary PDRs to represent the service data flows or applications to be steered;

- creating a FAR with the Forwarding Policy IE including the Forwarding Policy Identifier set to the Traffic Steering Policy Identifier, or creating a FAR with a Outer Header Creation with the destination IP address; and

- associating the FAR to the above PDRs of the PFCP session.

The CP function shall control the processing of the traffic received from the (S)Gi-LAN or N6-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/N6-LAN". The UP function shall distinguish packets coming from (S)Gi-LAN/N6-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 (for EPC) or SMF (for 5GC). Predefined PCC rules can be activated or deactivated by the PCRF/PCF at any time. The Predefined PCC rules may be grouped allowing the PCRF/PCF to dynamically activate a set of PCC rules.

For EPC 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.

For the definition of PCC and ADC rules see clauses 4.3.1 and 4b.3.2 of 3GPP TS 29.212 [8] and clause 5.6.2.6 of 3GPP TS 29.512 [41].

The CP function may enforce an activated predefined PCC or ADC rule by the PCRF/PCF 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 (for EPC) or QoS flow binding (for 5GC) 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 common to many PFCP sessions (i.e. predefined PDR(s) / 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 or by including predefined FAR/URR/QER ID(s) (of which the most significant bit is set to "1") within:

- the Create PDR IE in an PFCP Session Establishment Request; or

- the Update PDR IE in an PFCP Session Modification Request.

If the CP function activates the traffic handling policies by including predefined FAR/URR/QER ID(s), i.e. where bit 8 is set to "1", then Create/Update FAR/URR/QER IE(s) that shares the same ID shall not be present.

If the received Create/Update PDR IE contains both the Activate Predefined Rules IE and a predefined FAR/URR/QER ID (bit 8 set to "1"), it is an implementation matter how the UPF handles the message. The UPF shall either overwrite the FAR/URR/QER referenced by the Activate Predefined Rules IE with those referenced by the received FAR/URR/QER ID, or reject the message with the Cause value "Rule creation/modification Failure" and the Failed Rule ID IE (see clause 8.2.1).

NOTE 1: The Create/Update PDR IE can contain only dynamic FAR/URR/QER ID. Such dynamic rules provision the UPF with information that was not preconfigured, e.g. with a remote GTP-U F-TEID.

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 clause 5.2.2.

NOTE 2: The URR IDs used in reports triggered by a predefined rule in UP function are also pre-configured at the CP function.

The URR ID used in the usage report may be a predefined URR ID or a URR ID dynamically provisioned by the CP function.

For deactivating predefined rules which have been activated in the UP function using a Predefined Rule Name, the CP function shall include the Deactivate Predefined Rules IE in the Update PDR IE in a PFCP Session Modification Request to inform the UP function to deactivate the corresponding predefined rules for the related PDR.

For deactivating predefined FAR(s) /URR(s) / QER(s) which have been activated in the UP function by including predefined FAR/URR/QER ID(s) in the Create PDR IE or Update PDR IE, the CP function may include Remove FAR IE(s), Remove URR IE(s) and/or Remove QER IE(s) to delete the corresponding predefined FAR/URR/QER ID in an PFCP Session Modification Request message.

NOTE 3: Using Remove FAR IE(s), Remove URR IE(s) and Remove QER IE(s) does not result in any change to predefined rules that was activated using the Activate Predefined Rules IE. Such predefined rules continue to apply if still activated for the PDR.

### 5.4.10 Charging

For EPC, 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.

For 5GC, the charging requirements for online and offline charging in the 5G data connectivity domain are specified in 3GPP TS 32.255 [45].

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:

- for EPC:
  - 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;
- for 5GC:
  - PDU session and/or individual or group of service data flows, for an SMF;
  - QoS Flow, for an SMF.

See clauses 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 PFCP 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 clause 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 clause 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 and zero or more Additional Monitoring IEs 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. clause 6.3.7.1 of 3GPP TS 32.299 [18]).

## 5.4.11 (Un)solicited Application Reporting

For EPC, (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].

For 5GC, solicited Application Reporting refers to the process of reporting the start or stop of applications by the SMF to the PCF. See 3GPP TS 23.503 [44] and 3GPP TS 29.512 [41]. Unsolicited application reporting is not applicable for 5GC.

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;
    - the CP function may include a zero quota together with a FAR ID for Quota Action IE in the URR to instruct the UP function to drop or buffer the packets pertaining to the detected application traffic before the quota is granted in the subsequent PFCP Session Modification Request message. The FAR identified by the FAR ID for Quota Action shall be provisioned according to the "sdfHandl" instruction received from the PCF or the local policies as specified in 3GPP TS 29.512 [41].

NOTE 1: The (normal) FAR associated with the PDR detecting the application traffic is used when the URR is later on provisioned with a non-zero quota.

- associating the URR to the PDR.

For unsolicited application reporting, a PFCP 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 PFCP 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 2: 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.

The UP function shall only report the Application ID when detecting the start or stop of an application and the Reduced Application Detection Information flag is set in the Measurement Information of the URR, e.g. for envelope reporting.

## 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 clause 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 PFCP 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.

## 5.4.13 Transport Level Marking

For EPC, transport level marking is performed on a per EPS bearer basis in the SGW and PGW. Transport level marking refers to the process of marking traffic with a DSCP value based on the locally configured mapping from the QCI and optionally the ARP priority level.

For 5GC, transport level marking is performed on a per QoS flow basis. Transport level marking refers to the process of marking traffic at the UPF/MB-UPF with a DSCP value based on the mapping from the 5QI, the Priority Level (if explicitly signalled) and optionally the ARP priority level configured at the SMF/MB-SMF.

Transport level marking shall be controlled by the CP function by providing the DSCP in the ToS or Traffic Class within the Transport Level Marking IE in the FAR that is associated to the PDR matching the traffic to be marked. The UP function shall perform the transport level marking for the detected traffic and sends the marked packet to the peer entity.

The CP function may change transport level marking by changing the Transport Level Marking IE in the related FAR.

## 5.4.14 Deferred PDR activation and deactivation

As specified in clause 6.3.2 of 3GPP TS 23.203 [7] and clauses 4.5.13 and 4a.5.13 of 3GPP TS 29.212 [8], Policy and charging control rule operations can be also performed in a deferred mode. To support such deferred PCC rule activation or deactivation, the CP function and UP function may optionally support the Deferred PDR activation and deactivation (DPDRA) as described below.

If the feature DPDRA is supported in both CP function and UP function, and when a PCC rule is provisioned in a deferred mode, i.e. with a Rule-Activation-Time and/or Rule-Deactivation-Time, the CP function shall provision the corresponding PDR using Create PDR IE or Update PDR together with an Activation Time and/or Deactivation Time to enable the PDR being activated or deactivated at requested time.

Without being provisioned together with an Activation Time or a Deactivation Time, a PDR shall be active immediately when it is received. When the status of a PDR is changed from active to inactive, the UP function shall keep storing the inactive PDR together with its associated FAR, URR(s) and QER(s), and then UP function shall apply the same behavior as if the PDR is deleted.

The CP function shall control at what time the status of a PDR rule changes using Activation Time and/or Deactivation Time as exactly as being instructed by the PCRF using a Rule-Activation-Time and/or Rule-Deactivation-Time, as specified in clause 4.5.13 of 3GPP TS 29.212 [8].

1) If only Activation Time is specified and has not yet occurred, then the UP function shall set the PDR rule inactive and make it active at that time. If Activation Time has passed, then the UP function shall immediately set the PDR rule active.

2) If only Deactivation Time is specified and has not yet occurred, then the UP function shall set the PDR rule active and make it inactive at that time. If Deactivation Time has passed, then the UP function shall immediately set the PDR rule inactive.

3) If both Activation Time and Deactivation Time are specified, and the Activation Time occurs before the Deactivation Time, and also when the PDR rule is provided before or at the time specified in the Deactivation Time, the UP function shall handle the rule as defined in 1) and then as defined in 2).

4) If both Activation Time and Deactivation Time are specified, and the Deactivation Time occurs before the Activation Time, and also when the PDR rule is provided before or at the time specified in the Activation Time, the UP function shall handle the rule as defined in 2) and then as defined in 1).

5) If both Activation Time and Deactivation Time are specified but time has already occurred for both, and the Activation Time occurs before the Deactivation Time, then the UP function shall immediately set the PDR rule inactive.

NOTE 1: If the CP function receives both Rule-Activation-Time and Rule-Deactivation-Time from the PCRF, but time has already occurred for both, and the Rule-Activation-Time occurs before the Rule-Deactivation-Time, as alternative to above, the CP function can deactivate the corresponding PDR rule by provisioning a Deactivation Time which has occurred or removing the corresponding PDR rule.

6) If both Activation Time and Deactivation Time are specified but time has passed for both, and the Deactivation Time occurs before the Activation Time, then the UP function shall immediately set the PDR rule active.

NOTE 2: If the CP function receives both Rule-Activation-Time and Rule-Deactivation-Time from the PCRF, but time has passed for both, and the Rule-Deactivation-Time occurs before the Rule-Activation-Time, as alternative to above, the CP function can activate the corresponding PDR rule by provisioning a activation Time which has occurred in the Update PDR IE, or create the corresponding PDR rule if the PDR is not provisioned yet.

## 5.4.15 Packet Rate enforcement

### 5.4.15.1 General

Packet rate enforcement refers to the process of limiting the rate of uplink and/or downlink packets allowed to be sent for a PDN connection or a PDU session.

Packet rate enforcement shall be used to support:

- APN rate control for UE's all PDN connections for a given APN in EPC, see 3GPP TS 23.401 [14] and 3GPP TS 23.502 [29]. APN rate control is enforced across N4 interface only for 5GC interworking with EPC scenario (see clause 4.3 in 3GPP TS 23.501 [28]);

- Small data rate control for a PDU session in 5GC, see 3GPP TS 23.501 [28] and 3GPP TS 23.502 [29];

- Serving PLMN rate control, for downlink traffic, see 3GPP TS 23.401 [14] and 3GPP TS 23.501 [28].

### 5.4.15.2 Packet rate enforcement over Sxb and N4 interfaces

The CP function may instruct the UP function to perform packet rate enforcement, during the establishment or the modification of a PFCP session, over the Sxb and N4 reference points.

The CP function shall control packet rate enforcement in the UP function by:

1) creating the necessary PDR(s) to represent the uplink or downlink traffic to be enforced, if not already existing;

2) creating QER(s) containing the Packet Rate IE with one or more of the following enforcement rules and information:

   - Maximum Uplink/Downlink Packet Rates (i.e. Number of Uplink/Downlink Packets Allowed and Time units that determine the time periods for limiting the packet rates);

   - Additional Maximum Uplink/Downlink Packet Rates (i.e. Number of Additional Uplink/Downlink Packets Allowed and Time units that determine the time periods for limiting the packet rates), if additional packets are allowed to be sent beyond the maximum Uplink/Downlink Packet Rates;

   The QER may also contain the Packet Rate Status IE to indicate remaining numbers of allowed packets until a given time.

The QER may also contain the QER Control Indications IE with the Rate Control Status Reporting (RCSR) flag, indicating the UP function shall report to the CP function the status of the packet rate usage when the PFCP session is released.

3) associating the QER(s) to the UL and/or DL PDRs of the traffic for which packet rate enforcement is required.

When so instructed, the UP function shall proceed as follows:

1) the UP function shall count UL/DL packets within the time period (e.g. per minute, per day, etc.) and if the 'maximum allowed rate' is reached, the UP function shall discard or delay further packets.

2) If 'Additional Maximum Uplink/Downlink Packet Rates' are provided, the UPF shall consider 'maximum allowed rate' is equal to the 'number of packets per time unit' plus the 'number of additional allowed exception report packets per time unit'. Otherwise, the UPF shall consider 'maximum allowed rate' is equal to the 'number of packets per time unit'.

3) If the CP function has requested to report the rate control status, the UP function shall send to the CP function the Packet Rate Status IE, when the PFCP session is released. Otherwise, the UP function shall not send the Packet Rate Status IE to the CP function during the release of the PFCP session.

4) If the CP function provided Packet Rate Status information, then the UP function shall first enforce the rules in the Packet Rate Status IE until either the packet rate limits are reached, or the validity time expires. Only after this shall the UP function enforce the rules in the Packet Rate IE.

### 5.4.15.3 PGW and SMF behaviour

A PGW, SMF or SMF/PGW shall apply APN rate control, Small Data Rate Control and Serving PLMN rate control by instructing the UP function to perform packet rate enforcement as described in clause 5.4.15.2 with the following additions:

- Serving PLMN rate control:
  - the Maximum Downlink Packet Rate shall be set to the DL rate permitted by the Serving PLMN rate control parameters;
  - the CP function shall indicate to the UP function to not report the status of the packet rate usage.

NOTE 1: Serving PLMN rate control applies only to control plane PDU sessions and PDN connections. Uplink rate for Serving PLMN rate control is enforced by the MME or SMF, so it does not require support from the UP function.

- Small Data Rate Control:
  - the CP function shall indicate to the UP function to report the status of the packet rate usage;
  - the QER shall be associated to all the DL/UL PDRs of the PDU session;
- APN rate control:
  - the CP function shall indicate to the UP function to report the status of the packet rate usage;
  - the QER shall be associated to all the PDRs of all the PDN connections of the UE to the same APN, using the QER Correlation ID (see clause 5.2.1).

If both Serving PLMN rate control and Small Data Rate Control are applied in 5GS, or both Serving PLMN rate control and APN rate control are applied in EPS, the SMF/PGW-C may control packet rate enforcement in the UP function by provisioning:

- a QER for Small Data Rate Control/APN rate control, and by associating DL/UL PDRs to the QER; or
- alternatively, different QERs for Serving PLMN rate control and for Small Data Rate Control/APN rate control, and by associating DL PDRs to both of the QER(s).

APN rate control and Small Data Rate Control are distinct functionalities that apply in EPS and 5GS respectively. For PDU sessions supporting interworking with EPC, the SMF/PGW-C shall start APN rate control (if required for the UE's

PDN connections to the APN) and stop Small Data Rate Control (if this was performed for the PDU session) upon 5GS to EPS mobility, and vice-versa upon EPS to 5GS mobility, e.g. by:

- updating the information of the QER associated to the UL/DL PDRs with the packet rates and packet rate status (if available) applicable for APN rate control or Small Data Rate Control respectively, if the same QER is associated to UL/DL PDRs when the UE is in EPC and in 5GC; in this case, the SMF/PGW-C shall also request the UPF/PGW-U to report immediately the packet rate status at the time of the mobility between 5GS and EPS by including the Query Packet Rate Status IE in the PFCP Session Modification Request; or

NOTE 2: Requesting the UPF/PGW-U to report immediately the packet rate status enables to retrieve the current rate status applicable to the source system before the UPF/PGW-U overwrites the QER parameters with the packet rates and packet rate status (if available) applicable to the target system.

- provisioning different QERs for APN rate control and for Small Data Rate Control, and by associating UL/DL PDRs to the appropriate QER, when the UE is in EPC or in 5GC. In this case, when releasing the PFCP session, the UP function shall include the packet rate status for every QER for which this information has been requested in the corresponding QER Control Indications IE.

Besides, if the SMF/PGW-C set up additional PDRs in the UP function for S5/S8 tunnels for a PDU session supporting interworking with EPS, these PDRs shall not be associated to the QER used to perform Small Data Rate Control.

## 5.4.16 QoS differentiation for Stand-alone Non-Public Network (SNPN)

### 5.4.16.1 General

Support of QoS differentiation for SNPN is described in clause 5.30.2.7 and clause 5.30.2.8 of 3GPP TS 23.501 [28].

QoS differentiation procedures as described in the following clauses are optional and may be used when:

- UE access to PLMN services via SNPN;
- UE access to SNPN services via PLMN.

### 5.4.16.2 Access to PLMN services via SNPN

The SMF in PLMN shall provide DSCP(s) within the Transport Level Marking IE(s) in the FAR(s) that is associated to the PDR(s) matching the traffics to be marked to the UPF in PLMN.

UPF in PLMN shall perform the DSCP marking for the detected traffic and sends the marked packet to the N3IWF.

The SMF in SNPN shall provide PDR to the UPF in SNPN, based on the mapping rules including the mapping between the DSCP markings for the IPsec child SAs on NWu and the corresponding QoS requirement of the PLMN. The PDR may include specific DSCP and N3IWF IP address to enable UPF to detect the DL traffic.

The SMF in SNPN may provide the QER associated to the PDR to ensure the QoS for the DL traffic if the related QoS Flow has been established in the SNPN. Otherwise, the SMF in SNPN may provide the URR associated to the PDR to request the reporting of the detected DL traffic, which may be used by the SMF in SNPN to trigger the PDU session modification procedure to establish the DL traffic related QoS Flow in SNPN. The URR may include the Reporting trigger "Start of application" to enable the UPF sending Usage report with the usage report trigger "START" to the SMF upon detection of the DL traffic with such DSCP and N3IWF IP address.

The SMF in SNPN may also provide DSCP within the Transport Level Marking IE in the FAR that is associated to the PDR. UPF in SNPN shall perform the DSCP re-marking for the detected traffic and sends the marked packet to the NG-RAN.

### 5.4.16.3 Access to SNPN services via PLMN

The SMF in SNPN shall provide DSCP(s) within the Transport Level Marking IE(s) in the FAR(s) that is associated to the PDR(s) matching the traffics to be marked to the UPF in SNPN.

UPF in SNPN shall perform the DSCP marking for the detected traffic and sends the marked packet to the N3IWF.

The SMF in PLMN shall provide PDR to the UPF in PLMN, based on the mapping rules including the mapping between the DSCP markings for the IPsec child SAs on NWu and the corresponding QoS requirement of the SNPN. The PDR may include specific DSCP and N3IWF IP address to enable UPF to detect the DL traffic.

The SMF in PLMN may provide the QER associated to the PDR to ensure the QoS for the DL traffic if the related QoS Flow has been established in the PLMN. Otherwise, the SMF in PLMN may provide the URR associated to the PDR to request the reporting of the detected DL traffic, which may be used by the SMF in PLMN to trigger the PDU session modification procedure to establish the DL traffic related QoS Flow in PLMN. The URR may include the Reporting trigger "Start of application" to enable the UPF sending Usage report with the usage report trigger "START" to the SMF upon detection of the DL traffic with such DSCP and N3IWF IP address.

The SMF in PLMN may also provide DSCP within the Transport Level Marking IE in the FAR that is associated to the PDR. UPF in PLMN shall perform the DSCP re-marking for the detected traffic and sends the marked packet to the NG-RAN.

# 5.5 F-TEID Allocation and Release

## 5.5.1 General

For EPC and 5GC, F-TEID shall be only allocated by the UP function, see clause 5.8.2.3 of 3GPP TS 23.501 [28].

The UP function shall set the FTUP feature flag in the UP Function Features IE (see clause 8.2.25) and the CP function shall request the UP function to allocate the F-TEID. The UP function shall reject a request to establish a new PDR with an F-TEID allocation in the CP function option, with the cause "Invalid F-TEID allocation option". As an exception, the UP Function shall accept the PFCP Session Establishment Request message with a PDR including an existing F-TEID to re-establish a PFCP session during a restoration procedure as specified in clause 4.3.2 of 3GPP TS 23.527 [40] and clauses 16.1A.4 and 17.1A.4 of 3GPP TS 23.007 [24].

## 5.5.2 Void

## 5.5.3 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 PFCP Session Establishment Request or PFCP 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;

or, if the UP function indicated support of the PDI optimization (see clause 8.2.25), by:

- including the Local F-TEID IE only in the Create Traffic Endpoint IE and by setting the CHOOSE flag in the Local F-TEID IE of this IE; and
- including the Traffic Endpoint ID in all the PDRs to be created with the same F-TEID.

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

Upon receiving a request to remove a PDR or a Traffic Endpoint, or to delete a PFCP session, the UP function shall free the F-TEID(s) that was assigned to the PDR if there is no more PDR with the same F-TEID, to the Traffic Endpoint or to the PFCP Session.

When using redundant GTP-U transmission on N3/N9 interfaces (see clause 5.24.2), the CP function shall request the UP function to allocate the F-TEID for the redundant GTP-U tunnel following the same requirements as specified in this clause, using the "Local F-TEID for Redundant Transmission" IE instead of the "Local F-TEID" IE.

# 5.6 PFCP Session Handling

## 5.6.1 General

The following clauses provide details on PFCP Sessions handling.

## 5.6.2 Session Endpoint Identifier Handling

The SEID uniquely identifies a PFCP 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 PFCP session via the "F-SEID" IE.

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

## 5.6.3 Modifying the Rules of an Existing PFCP Session

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

When modifying an existing PFCP 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 PFCP 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 PFCP 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 PFCP Session Modification Request with the IE(s) to be removed with a null length. For an IE with multiple occurrences, e.g. when the description of the IE contains the text "several IEs with the same IE type may be present", one occurrence of such an IE with a null length shall result in removing all the IEs with the same IE type.

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

Upon receipt of a PFCP Request which modifies an existing PFCP 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

## 5.7.1 General

This clause specifies lawful interception with PFCP in EPC.

## 5.7.2 Lawful Interception in EPC

Requirements for support of Lawful Interception with a split SGW or PGW are specified in clauses 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 clause 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.

### 5.7.3 Lawful Interception in 5GC

Requirements for support of Lawful Interception with SMF and UPF are specified in clause 6.2.3 of 3GPP TS 33.127 [47]. The PFCP protocol is not used for Lawful Interception in 5GC.

## 5.8 PFCP Association

### 5.8.1 General

A PFCP Association shall be set up between the CP function and the UP function prior to establishing PFCP sessions on that UP function. Only one PFCP association shall be setup between a given pair of CP and UP functions, even if the CP and/or UP function exposes multiple IP addresses. A single PFCP association may also be setup between a SMF set and a UPF (see clause 5.22.2).

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

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

In PFCP signaling, a CP function or a UP function shall be identified by a unique Node ID. A Node ID may be set to an FQDN or to an IP address (either IPv4 or IPv6, see clause 8.2.38). When set to an IP address, it indicates that the CP/UP function only exposes one IP address for the PFCP Association signalling. Once a PFCP association is set up between a CP function and a UP function, the same Node ID as signaled respectively by the CP function and the UP function during the PFCP association setup procedure shall be used in all subsequent PFCP node related messages (other than Heartbeat messages) until the PFCP association is released.

NOTE 1: The control of a PFCP session can be taken over by a new SMF in an SMF set as specified in clause 5.22. When using the MPAS feature (see clause 5.22.3), when a different SMF takes over the control of the PFCP session, the UP function receives the NODE ID of the new SMF that is different from the NODE ID of the SMF that was handling the PFCP session earlier.

The PFCP entities shall accept any new IP address allocated as part of F-SEID other than the one(s) communicated in the Node Id.

NOTE 2: The source IP address to send PFCP Association Setup request can not be used as the destination IP address when the peer sends a PFCP Association Update Request message, e.g. for a scenario when a NAT is deployed in the network.

Prior to establishing a PFCP Association, the function responsible for establishing the PFCP Association (e.g. CP function) shall look up a peer function (e.g. UP function), e.g. using DNS procedures (see 3GPP TS 29.303 [25]), NRF procedures (see 3GPP TS 29.510 [43]) or local configuration. If the peer function is found to support multiple IP addresses (in the look up information), one of these addresses (any one) shall be used as destination IP address to send the PFCP Association Setup Request. Once the PFCP Association is established, any of the IP addresses of the peer function (found during the look-up) may then be used to send subsequent PFCP node related messages and PFCP session establishment requests for that PFCP Association.

NOTE 3: The look up information (e.g. in DNS, NRF or local configuration of the function responsible for establishing the PFCP association) needs to be configured consistently with the addressing information of the peer function. If a FQDN is configured to identify a function in DNS or NRF, then the Node ID of that function included in PFCP messages need to be set to the same FQDN. For instance, if the CP function is responsible for establishing the PFCP association, a UP function that exposes multiple IP addresses (for PFCP node related messages and PFCP session establishment requests) needs to be configured in the look up information as one (single) UP function that is associated to multiple IP addresses. The Node ID needs to be set to an SMF set FQDN when a single association is setup between an SMF set and UPF (see clause 5.22.2).

NOTE 4: PFCP session related messages for sessions that are already established are sent to the IP address received in the F-SEID allocated by the peer function or to the IP address of an alternative SMF in the SMF set (see clause 5.22). The former IP address needs not be configured in the look up information. See clauses 4.3.2 and 4.3.3.

## 5.8.2 Behaviour with an Established PFCP Association

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

- shall provision node related parameters (i.e. parameters that apply to all PFCP 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 clause 6.2.2;
- may establish PFCP sessions on that UP function;
- shall refrain from attempting to establish new PFCP sessions on the UP function, if the UP function has indicated it will shut down gracefully.

When a PFCP 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;
- shall accept PFCP 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 clause 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;
- may report UE IP address usage information to the CP function, if UE IP addresses are allocated by the UP function and the UE IP Address Usage Reporting feature is supported by the CP function (see clause 5.21.3.2).

## 5.8.3 Behaviour without an Established PFCP Association

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

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

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

- shall reject any incoming PFCP Session related messages from that CP function, with a cause indicating that no PFCP 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 an 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 PFCP message relevant to the PFCP Association Setup procedure to learn which vendor specific enhancements are supported by the peer.

Vendor-specific IE may be sent with any PFCP message. Vendor-specific IE may be added directly to a PFCP message, or by embedding it into a grouped IE.

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 PFCP session for which the message is received; and
- shall initiate a PFCP Session Report procedure, towards the CP function controlling this PFCP 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 clause 7.3.1 of 3GPP TS 29.281 [3]).

For EPC, 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 clauses 21.7 and 21.8 of 3GPP TS 23.007 [24], i.e.:

- modify the PFCP session to instruct the UP function to buffer DL packets;
- modify the PFCP session to delete the PDR and FAR, when having to delete a bearer; or
- delete the PFCP session, when having to delete the PDN connection.

For 5GC, upon receipt of an Error Indication Report, the SMF shall proceed as specified in clause 5.3 of 3GPP TS 23.527 [40].

# 5.11 User plane inactivity detection and reporting

## 5.11.1 General

This clause specifies the support of user plane inactivity detection and reporting.

## 5.11.2 User plane inactivity detection and reporting per PDN connection or PDU session

Clause 5.4.4.1 of 3GPP TS 23.401 [14] requires the PGW to initiate the release of an inactive emergency PDN connection.

Clauses 4.3.7 and 4.3.2.2.2 of 3GPP TS 23.502 [29] require the SMF to be able to initiate the deactivation of the UP connection of an existing PDU session without user plane activity for a given inactivity period, except for the H-SMF for the home routed roaming scenario or except for an always-on PDU session as described in clause 5.6.8 of 3GPP TS 23.501 [28].

Clauses 4.3.5.7, 4.23.9.4 and 4.23.9.5 of 3GPP TS 23.502 [29] requires the SMF to be able to initiate the deactivation of the UP connection of an existing PDU session in source UL CL or source UPF (e.g. PSA2) if no active traffic over the N9 forwarding tunnel is detected and reported by the Source UL CL. Clause 4.23.9.4 of 3GPP TS 23.502 [29] also requires the SMF to release the N9 forwarding tunnel of an existing PDU session in the target UL CL/BP if no active traffic over the N9 forwarding tunnel is detected and reported by the Source UL CL.

Clause 7.2.5.3 of 3GPP TS 23.247 [72] requires the MB-SMF to be able to initiate the deactivation of an MBS session without user plane activity.

The CP function may request the UP function to detect and report when no user plane packets are received for a PFCP session, by provisioning the User Plane Inactivity Timer IE in the PFCP Session Establishment Request or PFCP Session Modification Request.

Upon being provisioned with this IE, the UP function shall monitor the user plane activity of the PFCP session and report any user plane inactivity exceeding the duration indicated by this IE by sending a PFCP Session Report Request with the Report Type set to UPIR (User Plane Inactivity Report). The UP function shall then continue to process any further user plane packets as instructed by the rules provisioned for the PFCP session, until receiving any new instruction from the CP function.

### 5.11.3 User plane inactivity detection and reporting per PDR

Clause 4.23.9.5 of 3GPP TS 23.502 [29] requires the target I-SMF to be able to initiate the release of the N9 forwarding tunnel of an existing PDU session in the target UL CL/BP if no active traffic over the N9 forwarding tunnel is detected and reported by the target UL CL/BP.

When both the CP function and the UP function support the UPIDP feature (see clause 8.2.25), the CP function may request the UP function to detect and report when no user plane packets are received for one or more PDRs, by provisioning a URR including the User Plane Inactivity Timer IE and by associating this URR with the PDR(s) in a PFCP Session Establishment Request or PFCP Session Modification Request.

Upon being provisioned with this URR, the UP function shall monitor the user plane activity of all the PDR(s) associated with the URR and report user plane inactivity when no traffic has been received for any PDR(s) associated with the URR for the duration indicated in the User Plane Inactivity Timer IE by sending a PFCP Session Report Request with the Report Type set to USAR (Usage Report) and with the Usage Report Trigger IE set to UPINT (User Plane Inactivity Timer).

## 5.12 Suspend and Resume Notification procedures

Upon receipt of a Suspend Notification message, the PGW-C should request the PGW-U to discard packets received for the suspended PDN connection by:

- setting the DROP flag in the Apply Action IE of the FARs of the corresponding PFCP session; or
- setting the gate fields in the Gate Status IE of QERs to the value CLOSED.

Upon being requested to resume the PDN connection, the PGW-C should re-allow the PGW-U to forward the packets for the PDN connection (unless not permitted for other reasons) by:

- setting the FORW flag in the Apply Action IE of the FARs of the corresponding PFCP session; or
- setting the gate fields in the Gate Status IE of QERs to the value OPEN.

## 5.13 Ethernet traffic (for 5GC)

### 5.13.1 General

An SMF and UPF may support Ethernet PDU sessions, as specified in clause 5.6.10.2 of 3GPP TS 23.501 [28].

A combined PGW-C/SMF and PGW-U/UPF may support Ethernet PDU sessions as specified in clause 4.3.17.8a of 3GPP TS 23.401 [14] and clause 5.6.10.2 of 3GPP TS 23.501 [28]. In this case, the PGW-C/SMF and PGW-U/UPF shall follow, respectively, the requirements specified for the SMF and UPF by this clause.

For a PFCP session set up for an Ethernet PDU session, the SMF shall:

- include the PDN Type IE set to "Ethernet" in the PFCP Session Establishment Request;

- provision PDR(s), for uplink and/or downlink traffic, with Ethernet Packet Filter(s), based on at least any combination of:

  - Source/destination MAC address;

  - Ethertype as defined in IEEE 802.3 [31];

  - Customer-VLAN tag (C-TAG) and/or Service-VLAN tag (S-TAG) VID fields as defined in IEEE 802.1Q [30];

  - Customer-VLAN tag (C-TAG) and/or Service-VLAN tag (S-TAG) PCP/DEI fields as defined in IEEE 802.1Q [30];

  - IP Packet Filter Set, in case Ethertype indicates IPv4/IPv6 payload;

  - Ethernet PDU Session Information, only possible for a DL PDR, that identifies all (DL) Ethernet packets matching the PDU session as follows, based on the N6 Ethernet configuration in the UPF for the associated Network Instance (see clause 5.6.10.2 of 3GPP TS 23.501 [28]):

- DL traffic based on the MAC address(es) and/or C-TAG and/or S-TAG used by the UE for the UL traffic, for configurations where more than one PDU Session to the same DNN (e.g. for more than one UE) corresponds to the same N6 interface;

- DL traffic from the N6 interface associated to the PDU session, for configurations where there is a one-to-one relationship between a PDU Session and a N6 interface (in which case the UPF does not need to be aware of MAC addresses and/or C-TAG and/or S-TAG used by the UE in order to route down-link traffic).

NOTE 1: For instance, the SMF can provision a DL PDR with just an "Ethernet PDU Session Information", in a Traffic Endpoint ID or in a PDI, or Ethernet Packet Filters in a PDI, or both an "Ethernet PDU Session Information" in a Traffic Endpoint ID and Ethernet Packet Filters in a PDI.

The SMF may also request a UPF, acting as a PDU session anchor, to:

- redirect Address Resolution Protocol (ARP) (see IETF RFC 826 [32]) or IPv6 Neighbour Solicitation traffic (see IETF RFC 4861 [33]) to the SMF as specified in clause 5.13.2, or to respond to ARP or IPv6 Neighbour Solicitation based on the local cache information as specified in clause 5.13.3;

- report the MAC (Ethernet) addresses and possibly associated VLAN tag(s) used as source address of frames sent UL by the UE, as specified in clause 5.13.5;

- update its list of MAC addresses and possibly associated VLAN tag(s) associated to the PDU session, during an Ethernet PDU session anchor relocation, as specified in clause 5.13.6.

For a PFCP session set up for an Ethernet PDU session, the UPF shall:

- detect Ethernet traffic, based on Ethernet Packet Filter(s) provisioned in PDR(s) by the SMF, and process the Ethernet traffic as instructed in the FAR, QER(s) and URR(s) associated to the PDR(s);

- forward Address Resolution Protocol (see IETF RFC 826 [32]) or IPv6 Neighbour Solicitation messages (see IETF RFC 4861 [33]) to the SMF, as specified in clause 5.13.2, if so required by the SMF;

- respond to Address Resolution Protocol (see IETF RFC 826 [32]) or IPv6 Neighbour Solicitation (see IETF RFC 4861 [33]) based on the local cache information, as specified in clause 5.13.3, if so required by the SMF.

NOTE 2: Ethernet Preamble and Start of Frame delimiter are not sent over 5GS.

NOTE 3: How the UPF/SMF builds the ARP or the IPv6 Neighbour cache is not specified in this release and is implementation specific.

### 5.13.2 Address Resolution Protocol or IPv6 Neighbour Solicitation Response by SMF

If the SMF requests the UPF to forward all Address Resolution Protocol (ARP) (see IETF RFC 826 [32]) or IPv6 Neighbour Solicitation (see IETF RFC 4861 [33]) traffic to the SMF to respond to the ARP or IPv6 Neighbour

Solicitation based on the local cache information for Ethernet PDU sessions, the SMF shall provision a PDR in the UPF with:

- an Ethernet Packet Filter containing EtherType 2054 (hexadecimal 0x0806) and associate the PDR with a FAR, for forwarding ARP traffic to the SMF; and/or

- a PDI containing an application ID such that the identified application ID matches against EtherType 34525 (hexadecimal 0x86DD), IPv6 Next Header type as 58 and ICMP Field Type as 135 and associate the PDR with a FAR, for forwarding IPv6 Neighbour Solicitation traffic to the SMF.

In this case, the user plane packets shall be forwarded between the CP and UP functions by encapsulating the user plane packets using GTP-U encapsulation (see clause 5.3.1).

The SMF shall respond to ARP and/or IPv6 Neighbour Solicitation as specified in 3GPP TS 23.501 [28], clause 5.6.10.2 in this case.

### 5.13.3 Address Resolution Protocol or IPv6 Neighbour Solicitation Response by UPF

If the SMF requests the UPF to respond to Address Resolution Protocol (ARP) (see IETF RFC 826 [32]) or IPv6 Neighbour Solicitation (see IETF RFC 4861 [33]) based on the local cache information for an Ethernet PDU session, the SMF shall provision a PDR in the UPF with:

- an Ethernet Packet Filter containing EtherType 2054 (hexadecimal 0x0806) and associate the PDR with a FAR that has the ARP bit in Proxying IE of the Forwarding Parameters IE set to "1"; or

- a PDI containing an application ID such that the identified application ID matches against EtherType 34525 (hexadecimal 0x86DD), IPv6 Next Header type as 58 and ICMP Field Type as 135 and associate the PDR with a FAR that has the INS bit in Proxying IE of the Forwarding Parameters IE set to "1".

The UPF shall respond to ARP and/or IPv6 Neighbour Solicitation as specified in 3GPP TS 23.501 [28], clause 5.6.10.2 in this case.

### 5.13.3A Provisioning of MAC addresses and SDF filters in Ethernet Packet Filters

The provisioning of an SDF Filter in an Ethernet Packet Filter shall follow the requirements specified for provisioning an SDF Filter in clause 5.2.1A.2A.

Likewise, the source and destination MAC addresses information, when provisioned, shall be set as for downlink Ethernet flows. The UP function shall apply source and destination MAC addresses information based on the Source Interface of the PDR, according to the same principles as specified in clause 5.2.1A.2A, e.g. swapping the source and destination MAC addresses information if the Source Interface is ACCESS, and applying them as provisioned if the Source Interface is CORE.

### 5.13.4 Bidirectional Ethernet Filters

The CP function may provision bidirectional Ethernet Filters in the UP function (see table 7.5.2.2-3), i.e. Ethernet filters that may be associated to both uplink and downlink PDRs of a same PFCP session, as follows:

- when provisioning a bidirectional Ethernet Filter the first time for a PFCP session, the CP function shall set the BIDE (Bidirectional Ethernet Filter) flag in the Ethernet Filter Properties IE and provision the Ethernet filter definition together with a Ethernet Filter ID uniquely identifying the Ethernet Filter among all the Ethernet Filters provisioned for a given PFCP session; the source and destination MAC addresses information, in a bidirectional Ethernet filter, shall be set as for downlink Ethernet flows;

- the CP function may then provision a PDR for the same PFCP session but the opposite direction, by provisioning the Ethernet Filter ID in the Ethernet filter ID field of the PDI, without provisioning again the Ethernet Filter Properties and Ethernet filter definition.;

- when being provisioned with a bidirectional Ethernet Filter in a PDR, the UP function shall apply the Ethernet filter according to the direction of the PDR as specified in clause 5.13.3A, i.e. the UP function shall apply the

Ethernet filter parameters provisioned for the Ethernet filter ID, but with swapping the source and destination MAC addresses, and the source and destination IP addresses if any, if the PDR is set for uplink Ethernet flows;

- the UP function shall apply any modification of a bidirectional Ethernet Filter to all PDRs of the PFCP session making use of this Ethernet Filter;

- upon deletion of a PDR making use of a bidirectional Ethernet Filter, the UP function shall still apply the Ethernet Filter for any other PDR making use of the Ethernet Filter.

The requirements specified for provisioning of MAC addresses and SDF Filters in clause 5.13.A shall also apply when provisioning bidirectional Ethernet Filters.

## 5.13.5 Reporting of UE MAC addresses to the SMF

In a PFCP Session Establishment Request or a PFCP Session Modification Request, the SMF may request the UPF to start or stop (in a PFCP Sesssion Modification Request only) reporting the UE MAC addresses, i.e. the different MAC (Ethernet) addresses used as source address of frames sent UL by the UE in a PDU Session, by:

- creating a URR requesting the UPF to report Ethernet traffic information (i.e. with the Reporting Trigger set to 'MAC Addresses Reporting'); and

- associating the URR to the PDR provisioned for the UL traffic of the PDU session.

The SMF may additionally request the UPF to detect and report when no user plane packets are received for an UE MAC address, by provisioning the Ethernet Inactivity Timer IE in the URR.

When being requested to start reporting the UE MAC addresses, the UPF shall:

- report immediately any UE MAC addresses (and possibly their associated VLAN tags) known to be associated to the PDU session (e.g. if the request to start monitoring of traffic is received after the PFCP session establishment and if the UPF monitors the UE MAC addresses for the routing of DL traffic);

- report new UE MAC addresses (and possibly their associated VLAN tags) that are detected subsequently;

- report UE MAC addresses (and possibly their associated VLAN tags) that are removed subsequently from the PDU session, based on the detection of absence of traffic during the Ethernet Inactivity Timer, if this timer is provisioned in the URR.

NOTE: Numerous UE MAC addresses can be used by a same PDU session. The UP function can defer a bit the reporting of newly detected or removed UE MAC addresses to allow the reporting of multiple UE MAC addresses in a same usage report. Details are implementation specific.

## 5.13.6 Ethernet PDU session anchor relocation

The UPF (PSA) of an Ethernet PDU session may be relocated as specified in clause 4.3.5.8 of 3GPP TS 23.502 [29].

A UPF that supports the Ethernet PDU session relocation procedure shall set the ETHAR bit in the UP Function Features (see clause 8.2.25).

If the UPF indicated support of Ethernet PDU session anchor relocation, the SMF may request the UPF to update its list of MAC addresses and possibly associated VLAN tag(s) associated to the PDU session, during an Ethernet PDU session relocation procedure, by sending a PFCP Session Modification Request with Ethernet context information including the MAC addresses (and possibly associated VLAN tag(s)) received from the old Ethernet PDU session anchor.

Upon receipt of such information, the UPF shall consider these MAC addresses (and possibly associated VLAN tag(s)) as associated to the PDU session and the UPF may assist in the update of Ethernet forwarding tables of Ethernet switches in the DN as specified in clause 4.3.5.8 of 3GPP TS 23.502 [29].

## 5.14 Support IPv6 Prefix Delegation

Clause 5.3.1.2.6 of 3GPP TS 23.401 [14] and clause 4.6.2.3 of 3GPP TS 23.316 [57] specify requirements for IPv6 Prefix Delegation via DHCPv6, that allow assigning a single network prefix shorter than the default /64 prefix to a PDN connection or a PDU session.

The CP function shall assign, or request the UP function to assign (if the UP function indicates support of the UEIP feature, see clause 8.2.25), the network prefix shorter than the default /64 prefix by provisioning the UE IP Address IE in the UP function with:

- the IPv6D flag set to "1" and the IPv6 Prefix Delegation Bits field indicating the length of IPv6 Prefix for delegation (see clause 8.2.62); or

- the IP6PL flag set to "1" and the IPv6 Prefix Length field indicating the length of IPv6 Prefix for delegation (see clause 8.2.62), if the UP function supports the IP6PL feature (see clauses 5.21.1 and 8.2.25).

When UP function is requested to perform UE IP address allocation and IPv6 prefix delegation is used, the IPv6 prefix length may be determined by the CP function or the UP function:

- if it is determined by the CP function, the IPv6 Prefix Delegation Bits or IPv6 Prefix Length fields shall be set according to the desired IPv6 prefix length by the CP function;

- or if the IPv6 prefix length is determined by the UP function, the CP function shall set the IPv6 Prefix Delegation Bits or IPv6 Prefix Length fields to "0".

NOTE: The IPv6 prefix shorter than the default /64 prefix for IPv6 Prefix Delegation can include the /64 default prefix used for IPv6 stateless autoconfiguration (in EPS and 5GS) or not (5GS). In the latter case, the total IPv6 address space available for the PDU Session cannot be aggregated into one single IPv6 prefix; support of this latter case requires support of the IP6PL feature (see clauses 5.21.1 and 8.2.25).

When assigning additional IPv6 prefixes (i.e. prefixes in addition to the default prefix) to a UE, the CP function shall provision/update the UE IP Address IE in the PDI which may be as part of a Create PDR IE or a Update PDR IE, or in the Create Traffic EndPoint IE or Update Traffic EndPoint IE to the UP function as described above.

## 5.15 Signalling based Trace (De)Activation

The UP function shall set the TRACE feature flag in the UP Function Features IE if it supports Trace (see 3GPP TS 32.422 [35]).

If the UP function indicated support of Trace, the CP function may activate a trace session during a PFCP session establishment or a PFCP session modification procedure, by including the Trace Information IE in the PFCP Session Establishment Request or PFCP Session Modification Request.

The CP function may deactivate an on-going trace session by including the Trace Information IE with a null length in a PFCP Session Modification Request.

There shall be at most one trace session activated per PFCP session at a time.

## 5.16 Framed Routing

Framed routing allows to support an IP network behind a UE, such that a range of IP addresses or IPv6 prefixes is reachable over a single PDU session, e.g. for enterprise connectivity. Framed routes are IP routes behind the UE. The UPF advertizes relevant IP routes to receive packets destined to these destination IP addresses or IPv6 prefixes and to forward these packets over the PDU session. See clause 5.6.14 of 3GPP TS 23.501 [28], IETF RFC 2865 [37], IETF RFC 3162 [38]) and the Framed-Route, Framed-Routing and Framed-IPv6-Route AVPs specified in 3GPP TS 29.061 [39] and 3GPP TS 29.561 [49].

Framed routing is defined only for PDN connections and PDU sessions of the IP type (IPv4, IPv6, IPv4v6).

A UPF may indicate support of framed routing by setting the FRRT flag in the UP Function Features IE. If so, the CP function may include Framed-Route IEs, the Frame-Routing IE and Framed-IPv6-Route IEs in PDRs to describe framed routes associated to the PDU session.

The UP function shall:

- match the source IP address of packets with IP Address(es) or IPv6 prefixes as indicated in the the Framed-Route IE or Framed-IPv6-Route IE if it is provisioned in a UL PDRs;
- match the destination IP address of packets with IP Address(es) or IPv6 prefixes as indicated in the the Framed-Route IE or Framed-IPv6-Route IE if it is provisioned in a DL PDRs.

# 5.17 5G UPF (for 5GC)

## 5.17.1 Introduction

The following clauses describe the 5GS specific functionalities of a UP function.

## 5.17.2 Uplink Classifier and Branching Point

The Uplink Classifier and Branching Point functionalities refer to the capability of the UPF to route uplink traffic flows of the same PFCP session (PDU session) to two or more PDU Sessions Anchors, and to route the downlink traffic flows from these PDU Session Anchors on the tunnel towards the UE. They are defined in 3GPP TS 23.501 [28] and 3GPP TS 23.502 [29].

Uplink Classifier is supported for PDU sessions of type IPv4, IPv6, IPv4v6 or Ethernet. The routing of the uplink traffic flows to different PDU Session Anchors is based e.g. on the destination IP address/Prefix of the uplink packets for an IP PDU session.

Branching Point is supported for multi-homed PDU sessions of type IPv6, i.e. PDU sessions with multiple IPv6 prefixes. The routing of the uplink traffic flows to different PDU Session Anchors is based on the source IP prefix of the uplink packets.

The SMF may insert an Uplink Classifier or Branching Point, during a PDU session establishment or modification, by provisioning:

- two or more UL PDRs, with the appropriate Packet Detection Information, and with corresponding FARs to route the uplink traffic flows towards the appropriate PDU Session Anchors;
- two or more DL PDRs, with the appropriate Packet Detection Information, and with one (or more FARs) to route the downlink traffic flows on the tunnel towards the UE.

NOTE 1: This uses the generic functionalities of the PFCP protocol described in this specification, with two or more DL PDRs (for the traffic coming from the different PDU session anchors).

NOTE 2: A UPF acting as an Uplink Classifier or Branching Point can also behave as a PDU Session Anchor for the PDU session.

The SMF may remove an Uplink Classifier or Branching Point, during a PDU session modification, by removing the UL (or modifying the FAR associated to the UL PDR) and DL PDRs that were setup for the traffic to/from the PDU Session Anchor(s) to be removed.

## 5.17.3 Data forwarding during handovers between 5GS and EPS

Downlink data may be forwarded during an inter-system handover between 5GS and EPS using direct or indirect data forwarding.

NOTE: Uplink data is not forwarded during an inter-system handover between 5GS and EPS in this release of the specification.

Direct data forwarding is performed directly between the source and target RAN, without the involvement of any UPF to forward the data.

Indirect data forwarding during handovers between 5GS and EPS is supported as follows (see 3GPP TS 38.300 [42]):

- For 5G to 4G handover, the source NG-RAN node sends one or several end markers including one QFI of those QoS flows mapped to the same E-RAB and sends the end marker packets to the UPF over the PDU session tunnel. UPF removes the QFI and maps to an appropriate E-RAB tunnel towards SGW.

- For 4G to 5G handover, the source eNB forwards the received end markers in the EPS bearer tunnel to the SGW which forwards them to the UPF. The UPF adds one QFI among the QoS flows mapped to that E-RAB to the end markers and sends those end markers to the target NG-RAN node in the per PDU session tunnel.

To forward data (G-PDUs and End Marker packets) during a 5GS to EPS handover, the SMF shall:

- provision one PDR per E-RAB (that supports data forwarding for at least one QoS flow), with the list of QFIs that are mapped to the E-RAB;

- request the UPF to remove the GTP-U PDU Session Container extension header (including the QFI) from the data by including the GTP-U Extension Header Deletion field set to 'PDU Session Container' in the Outer Header Removal IE of the PDR(s);

- associate to each PDR a FAR to forward the data to the GTP-U tunnel of the corresponding E-RAB, i.e. with an Outer Header Creation IE containing the F-TEID of the (forwarding) SGW for the corresponding forwarding GTP-U tunnel.

To forward data (G-PDUs and End Marker packets) during an EPS to 5GS handover, the SMF shall:

- provision one PDR per E-RAB (that supports data forwarding for at least one QoS flow);

- create and associate one QER with each PDR, including the QFI IE set to the QFI value of one of the QoS flows mapped to the E-RAB, to request the UPF to insert a GTP-U PDU Session Container extension header including the QFI;

- create one FAR for each data forwarding tunnel in 5GS (i.e. per PDU session), with an Outer Header Creation IE containing the F-TEID of the target NG-RAN for the corresponding forwarding GTP-U tunnel;

- associate each PDR to the corresponding FAR (i.e. to forward the data of each E-RAB to the data forwarding tunnel of the corresponding PDU session).

# 5.18 Enhanced PFCP Association Release

## 5.18.1 General

To ensure no loss of usage reports and signalling efficiency, during a PFCP Association Release procedure, which is either initiated by CP function, or upon request from the UP function, the CP function and UP function may support the Enhanced PFCP Association Release feature (EPFAR) as described below.

When both the CP function and the UP function support the EPFAR feature, and when the CP (or UP) function determines that the PFCP association is to be released, the CP (or UP) function shall send a PFCP Association Update Request message with a "PFCP Association Release Preparation Start" flag to inform the peer UP (or CP) function that the PFCP Association is going to be released and the final non-zero usage reports are to be collected for these PFCP sessions which will be affected by PFCP association release.

The CP function should stop establishing new PFCP sessions in the UP function after receiving or sending a PFCP Association Release Preparation Start indication. The CP(or UP) function shall send a PFCP Association Update Response with a successful cause value to the peer.

Then the UP function shall initiate the PFCP Session Release procedure as specified in clause 5.18.2 by sending one or more PFCP Session Report Request messages for the PFCP sessions affected by the release of the PFCP association and that have non-zero usage reports to be reported. In the PFCP Session Report Request message, the UP function shall:

- set the Usage Report Trigger to TEBUR (Termination By UP function Report) for the usage reports being reported; and

- set the PSDBU (PFCP Session Deleted By the UP function) flag to "1" to indicate to the CP function that the PFCP Session is being deleted in the UP function and the usage reports included in the message are the final

usage reports for the given PFCP Session, if this is the last PFCP Session Report Request message sent for the PFCP session.

When the UP function has sent all the non-zero usage reports for the PFCP sessions affected by the release of the PFCP Association, the UP function shall send a PFCP Association Update Request with the flag URSS (non-zero Usage Reports for the affected PFCP Sessions Sent) set to "1" to indicate to the CP function that all non-zero usage reports for the affected PFCP sessions have been sent to the CP function and the corresponding PFCP sessions in the UP function have been locally deleted. The CP function shall then send a PFCP Association Update Response with a successful cause to the peer to indicate the PFCP Association Update Request is handled successfully.

The CP function shall then send a PFCP Association Release Request to release the PFCP Association as specified in clause 6.2.8.

### 5.18.2 UP Function Initiated PFCP Session Release

When the UP function needs delete a PFCP sesssion, e.g. during the Enhanced PFCP Association Release as described in clause 5.18.1 or when it detects an error or partial failure, the UP function shall:

- send one or more PFCP Session Report Request messages for this PFCP session;
- set the Report Type to "USAR" (Usage Report) if there is non-zero usage report for the PFCP session, or set the Report Type to "UISR" if there is no usage report to send (e.g. for a session without an URR provisioned or with an URR provisioned but with only null usage measurements);
- set the Usage Report Trigger to "TEBUR" for non-zero usage report(s), if usage reports are included in the PFCP Session Report Request message(s); and
- set the PSDBU flag to "1" to indicate to the CP function that the PFCP session is being deleted, in the last PFCP Session Report Request message sent for that PFCP session.

NOTE: The UP Function can release one or more PFCP Sessions (without tearing down the entire PFCP Association) when there is a partial failure in the UP Function.

## 5.19 Activation and Deactivation of Pre-defined PDRs

To reduce the signalling overhead for establishing a PFCP session (for a PDU session or a PDN connection) and improve the signalling efficiency, the CP and UP functions may support the Activation and Deactivation of a Pre-defined PDR (ADPDP) feature as described below.

When both the CP function and the UP function support the ADPDP feature, the CP function may activate one or more pre-defined PDRs for a PFCP session during a PFCP Session Establishment or a PFCP Session Modification procedure. A pre-defined PDR shall be configured in the UP function before it can be activated in a PFCP session.

A pre-defined PDR may contain all the necessary packets detection information to identify a service data flow or application traffic which may be common to many PFCP sessions, and it may be configured in the UPF associated with a pre-defined FAR, one or more pre-defined QER(s), and/or one or more pre-defined URR(s).

Any PFCP session specific information, e.g. traffic endpoint information, may not be part of a pre-defined PDR and is provisioned before or during the activation of the pre-defined PDR.

To activate one or more pre-defined PDR(s), the CP function shall provide one or more Activate Predefined Rules IE(s) in a Create PDR IE in a PFCP Session Establishment Request, or in a Create PDR IE or an Update PDR IE in a PFCP Session Modification Request message, that references a pre-defined PDR configured in the UP function, with the following information in the Create PDR or Update PDR IE:

- the traffic endpoint that the traffic shall match (e.g. Local F-TEID, UE IP Address or Traffic Endpoint ID);
- optionally the QFI that the traffic shall match, e.g. for a UL PDR where UL QoS flow binding verification is required (see clause 5.4.2);
- the precedence to be applied by the UP function among all PDRs of the PFCP session;

- optionally, an FAR containing instructions related to the processing of the packets matching the pre-defined PDR(s); when present, the UP function shall enforce it instead of the one defined in the pre-defined PDR(s) if any;

- optionally, one or more URRs to be used in addition to any URR(s) specified in the pre-defined PDR(s) (e.g. for session level Usage Monitoring);

- optionally, one or more QERs to be applied in addition to any QER(s) specified in the pre-defined PDR (e.g. for APN-AMBR enforcement).

When a pre-defined PDR is activated for a given PDR, an incoming packet matches the PDR if it matches the traffic endpoint, and the QFI if provisioned and one of the activated pre-defined PDR(s).

The CP function may update the use of pre-defined PDRs that are already activated in a PFCP session by including one or more Activate Predefined Rules IE(s) or Deactivate Predefined Rules IE(s) in a PFCP Session Modification Request and/or by updating the parameters provisioned in the PDR.

NOTE: The CP function cannot change a pre-defined PDR via PFCP session related procedure.

The CP function may deactivate a pre-defined PDR that is already activated in a PFCP session by including the Deactivate Predefined Rules IE in a PFCP Session Modification Request requesting to deactivate the predefined PDR(s).

In addition, this feature allows to define a group of pre-defined PDRs which can be activated, updated, and deactivated together. This allows the CP function to further optimize the signaling towards the UP function.

To activate, update, or deactivate a group of pre-defined PDRs, the CP shall follow the same procedure as for activating, updating, and deactivating a pre-defined PDR, but it shall use an Activate Predefined Rules IE that refers to a group of pre-defined PDRs.

# 5.20 Support of Access Traffic Steering, Switching and Splitting for 5GC

## 5.20.1 General

The Access Traffic Steering, Switching and Splitting (ATSSS) feature enables the support of Multi-Access (MA) PDU sessions, using one 3GPP access network or one non-3GPP access network at a time, or simultaneously using one 3GPP access network and one non-3GPP access network as defined in clauses 4.2.10 and 5.32 of 3GPP TS 23.501 [28].

A Multi-Access (MA) PDU session may support:

- both 3GPP access and non-3GPP access connected to 5GC, as specified in clause 4.22.2.1 and 4.22.2.2 of 3GPP TS 23.502 [29];

- 3GPP access connected to EPC while non-3GPP access is connected to 5GC, as specified in clause 4.22.2.3 of 3GPP TS 23.502 [29], subject to corresponding support by the UE.

The non-3GPP access network may be an untrusted non-3GPP access network, a trusted non-3GPP access network or a wireline 5G access network. The support of the ATSSS feature is optional for the SMF and the UPF.

When establishing a PFCP session for an MA PDU session, the SMF (H-SMF for a HR PDU session) shall select a PSA (UPF) supporting ATSSS (see MPTCP and ATSSS-LL flags in UP Function Features, Table 8.2.25-1), i.e. ATSSS-LL, MPTCP or both, and it shall provision in the PSA one Multi-Access Rule (MAR) for every downlink PDR matching non-GBR traffic sent towards the UE. See clause 5.2.7 for the handling of an MAR.

Distinct N3/N9 tunnels shall be established for each access network of the MA PDU session if the UE is registered to both 3GPP and non 3GPP access by:

- providing two UL PDRs to the PSA UPF in PFCP Session Establishment Request or PFCP Session Modification Request message, e.g. PDR-1 for UL data from 3GPP access and PDR-2 for UL data from non-3GPP access, to trigger the PSA UPF to allocate two N3/N9 UL CN tunnels as specified in clause 4.22.2.1 and clause 4.22.3.2 of 3GPP TS 23.502 [29];

- providing two FARs in one MAR associated to the DL PDR to the PSA UPF in PFCP Session Establishment Request or PFCP Session Modification Request message, e.g. FAR-1 for DL data forwarding to 3GPP access and FAR-2 for DL data forwarding to non-3GPP access.

## 5.20.2 MPTCP functionality

### 5.20.2.1 General

The SMF shall instruct the UPF(PSA) to activate MPTCP steering functionality for a given MA-PDU session if MPTCP needs to be used for TCP traffic flows.

The UPF(PSA) shall allocate resources for MPTCP steering functionality (e.g. MPTCP Proxy address, UE link-specific multipath IP addresses, etc.), and perform traffic steering, switching and splitting according to the instructions from the SMF.

### 5.20.2.2 Activate MPTCP functionality and Exchange MPTCP Parameters

If MPTCP steering functionality is required for a Multi-Access PDU session, the SMF shall send MPTCP Control Information to the UPF in PFCP Session Establishement Request, to instruct the UPF to activate the MPTCP functionality for this PFCP session. The SMF may also request to activate the PMF functionality for this PFCP session by sending PMF Control Information to the UPF. As a result, the UPF(PSA) shall allocate necessary resources for MPTCP and PMF and return the corresponding MPTCP and PMF Parameters (e.g. MPTCP IP address and port, UE link-specific multipath IP addresses, PMF IP address and port, etc.) to the SMF in PFCP Session Establishement Response.

The SMF may send MPTCP Control Information and/or PMF Control Information to the UPF in PFCP Session Modification Request, with updated value, e.g. if the SMF receives updated ATSSS rules from the PCF.

NOTE 1: Such MPTCP Parameters received by the SMF are sent to the UE together with the ATSSS rules, as specified in 3GPP TS 24.193 [59].

When provisioning an UL PDR for user plane traffic for which MPTCP is applicable, the SMF shall include an MPTCP Applicable Indication IE in the Create PDR IE.

NOTE 2: This indication can be used by the UPF to prepare itself for the reception of MPTCP traffic for the PDU session.

### 5.20.2.3 Control of Multipath TCP Connection Establishment by MPTCP Proxy

When MPTCP steering functionality is utilized, TCP connection establishment and data exchange between an UE and a remote host shall be proxide by the MPTCP Proxy in the UPF (PSA), using the mechanism specified in IETF RFC 8684 [62] and IETF RFC 8803 [60].

Once Multipath TCP connection is set up, the MPTCP Proxy shall store the MPTCP session entry which includes the following information:

- UE link-specific multipath IP addresses and its TCP port;
- UE's MA-PDU session IP address and its TCP port, if the MA-PDU session IP address is used by the MPTCP Proxy for IP translation;
- the N6 routable IP address and its TCP port, if N6 routable IP address is used by the MPTCP Proxy for IP translation;
- the remote host IP address and its TCP port.

The stored MPTCP session entry is used by MPTCP Proxy for subsequent IP translation when receiving uplink or downlink MPTCP traffic.

An UPF implementation may use N6 routable IP address instead of UE's MA-PDU session IP address for IP translation.

NOTE: The DL PDR from the SMF for MPTCP traffic carries the UE's MA-PDU session IP address. If the UPF uses a different N6 routable IP address, it is UPF implementation specific how to match DL PDRs for MPTCP traffic with downlink MPTCP traffic received with the destination address set to the N6 routable IP address.

#### 5.20.2.4 Traffic Steering and IP Translation by MPTCP Proxy

Once traffic for which MPTCP is applicable is detected by the UPF, the UPF shall internally forward this traffic to the MPTCP Proxy for IP translation. The MPTCP Proxy shall use the stored information in MPTCP session entry to perform IP translation to the detected MPTCP IP packets, e.g. replace the source IP address+port and/or destination IP address+port accordingly.

The UPF may detect the uplink IP packets for which MPTCP is applicable by checking whether the UL PDR matching the user plane traffic is set with an MPTCP Applicable Indication, or (UPF implementation choice) by checking whether the source or destination IP address of the user plane packets (after removing the GTP-U header) correspond to UE link-specific multipath IP address(es) and the MPTCP proxy IP address.

The UPF may detect the downlink IP packets for which MPTCP is applicable, by checking the information in the associated MAR (e.g. checking if the steering functionality is set to MPTCP) or by checking the destination IP address.

### 5.20.3 ATSSS-LL functionality

#### 5.20.3.1 Activate ATSSS-LL functionality and Exchange ATSSS-LL Parameters

If ATSSS-LL steering functionality is required for a Multi-Access PDU session, the SMF shall send ATSSS-LL Control Information to the UPF in PFCP Session Establishment Request, to instruct the UPF to activate the ATSSS-LL functionality for this PFCP session. The SMF may also request to activate the PMF functionality for this PFCP session by sending PMF Control Information to the UPF.

If PMF functionality is required to be activated for this MA PDU session, the SMF shall set the PMFI flag to 1 in the PMF Control Information IE, regardless whether per QoS flow access performance measurement is required. In addition, if the SMF determines that per QoS flow access performance measurements shall be applied for the MA PDU session, e.g. the threshold value(s) are received from PCF for the UL and/or DL traffic of the QoS flow, the SMF shall set the PQPM flag to 1 together with a list of QFI values for the QoS flows for which access performance measurements may be performed in the PMF Control Information IE.

Upon receiving the request from the SMF with indicating ATSSS-LL Control Information IE and PMF Control Information IE, the UPF(PSA) shall allocate necessary resources for ATSSS-LL and PMF and return the corresponding ATSSS-LL and PMF Parameters (e.g. PMF IP address and port, etc) to the SMF in PFCP Session Establishment Response:

- If per access performance measurements are required, i.e. PMFI flag set to 1 in the PMF Control Information IE, the UPF(PSA) shall allocate a default pair of access specific UDP ports (i.e. for IP PDU sessions) or MAC addresses (i.e. for Ethernet PDU sessions) and report them to the SMF in the PMF Address Information IE of a PMF Parameters IE not including the QoS flow identifier IE.

- If per QoS flow access performance measurements are required, i.e. PQPM flag is set to 1 in addition and a list of QFIs are indicated in the PMF Control Information IE, the UPF(PSA) shall allocate access specific UDP ports (i.e. for IP PDU sessions) or MAC addresses (i.e. for Ethernet PDU sessions) for each QoS flow indicated in the PMF Control Information and, for each QoS flow, report them to the SMF in the PMF Address Information IE of a PMF Parameters IE including the QoS flow identifier IE set to the corresponding QFI.

If the SMF provisions the UPF to apply ATSSS-LL in downlink with "Smallest Delay" steering mode, the UE does not support PMF RTT measurements (see clause 5.32.2 of 3GPP TS 23.501 [28]) and the UPF supports RTT measurements without PMF, the SMF should instruct the UPF to not use PMF RTT measurements by setting the DRTTI flag to "1" in the PMF Control Information.

NOTE 1: The UPF can measure RTT without using the PMF protocol by using other means not defined by 3GPP such as using the RTT measurements of MPTCP if there is an MPTCP connection established between the UE and UPF.

The SMF may send ATSSS-LL Control Information and/or PMF Control Information to the UPF in PFCP Session Modification Request, with updated value, e.g. if the SMF receives updated ATSSS rules from the PCF.

NOTE 2: Such ATSSS-LL Parameters received by the SMF are sent to the UE together with the ATSSS rules, as specified in 3GPP TS 24.193 [59].

## 5.20.4 Handling of GBR traffic of a MA PDU session

### 5.20.4.1 General

Traffic splitting of a GBR traffic is not supported (see clause 5.32.4 of 3GPP TS 23.501 [28]). Besides, switching GBR traffic from one access to another access requires the SMF to send N1/N2 messages to the UE and AN.

DL PDRs corresponding to GBR traffic shall be associated with DL FARs (i.e. no MAR).

### 5.20.4.2 Access Availability Reporting

For an MA PDU session using the ATSSS Low Layer (ATSSS-LL) or MPTCP steering functionality, the SMF may request the UPF to report when it cannot send downlink GBR traffic over its on-going access, e.g. based on access availability and unavailability report from the UE, by provisioning an SRR with an Access Availability Control Information IE requesting the UPF to report when an access (3GPP or non-3GPP access) becomes available or unavailable.

If so instructed, when detecting a change in an access availability, the UPF shall send an Access Availability Report to the SMF, indicating the access type and whether the access has become available or unavailable.

## 5.20.5 Access type of an MA PDU session becoming (un)available

The access type of an MA PDU session may become unavailable permanently (e.g. when the UE de-registers from one access) or transiently (e.g. when the UE has lost coverage of the 3GPP access or non-3GPP access).

When an access type of an MA PDU session becomes permanently unavailable, the SMF shall send a PFCP Session Modification Request with an Update MAR IE removing the Access Forwarding Information IE corresponding to the unavailable access. As a result, the UPF shall not send any more traffic on this access type.

Reversely, when a new access type becomes available for an MA PDU session, e.g. when the UE registers on another access and requests to establish user plane resources for that access, the SMF shall send a PFCP Session Modification Request with an Update MAR IE adding the Access Forwarding Information IE corresponding to the new available access type.

When an access type of an MA PDU session becomes transiently unavailable, the SMF shall notify the UPF that the access type has become unavailable by sending a PFCP Session Modification Request with the Access Availability Information IE indicating so. The SMF should then also notify the UPF when the access type becomes available again.

When being notified by the SMF that an access type has become transiently unavalaible, the UPF should stop sending DL traffic on this access until it receives the indication that the access becomes available again from the UE (i.e. PMF access available report) or the SMF.

## 5.20.6 PMFP message handling in UPF

The access performance measurement supports the following procedures, as specified in clause 5.32.5.1 of 3GPP TS 23.501 [28]:

- RTT measurement procedure initiated by the UE, or the UPF;
- Packet Loss Rate measurement procedure initiated by the UE, or the UPF;
- Access available/unavailable report procedure from the UE to the UPF;
- UE Assistance Data provisioning procedure from the UE to the UPF.

The per QoS flow access performance measurement procedure includes the RTT measurement and the Packet Loss Rate measurement, which may be initiated by the UE or the UPF(PSA).

PMFP messages are used by the PMF functionality in the UE and the PMF functionality in the UPF (PSA) to perform the access performance measurement procedures, as specified in 3GPP TS 24.193 [59].

PMFP messages shall be exchanged between the UE and the UPF via the default QoS flow or a dedicated QoS flow, as specified in 3GPP TS 23.501 [28]. To support this, the UPF shall learn the QFI identifying the QoS flow on which PMFP messages from the UE are transmitted, and shall send downlink PMFP messages on that QoS flow when needed.

Once an uplink PMFP message is detected, the UPF shall internally forward the PMFP message to the PMF functionality in the UPF, for subsequent handling.

The PMF functionality in the UPF shall learn the UE's address information for PMFP from the received PMFP message, e.g. to detect the IP address and UDP port of the PMF in the UE (for IP PDU sessions) or the MAC address of the PMF in the UE (for Ethernet PDU sessions), and set the source and destination addresses of PMFP messages sent to the UE accordingly, as specified in clause 5.32.5.1A of 3GPP TS 23.501 [28].

If the Steering mode is set to Load-Balancing and the UE Assistance Indicator is set, when the UPF receives a PMF message with UE Assistance Data (i.e. PMF-UAD message) from the UE, the UPF may apply the split percentages in the UE Assistance Data to all DL traffic for which the SMF has enabled the UE assistance operation. Meanwhile, the UPF shall store the original split percentage (i.e. the weight included in 3GPP/Non-3GPP Access Forwarding Action Information IE in the MAR) provisioned by the SMF, and apply these when the UE assistance mode is terminated, i.e. when the UPF receives a PMF message indicating the termination of UE assistance mode (i.e. PMF-UAT message).

# 5.21 UE IP address/prefix Allocation and Release

## 5.21.1 General

Stage 2 requirements for UE IP address allocation in the EPC and 5GC are specified in clause 5.3.1 of 3GPP TS 23.401 [14], clause 5.8.2.2 of 3GPP TS 23.501 [28] and clause 4.6.2 of 3GPP TS 23.316 [57]. The following types of UE IP addresses may be assigned over N4 or Sxb:

- IPv4 address;
- /64 IPv6 Prefix;
- IPv6 prefix other than default /64, including individual /128 IPv6 address, if the UPF indicates supports of the IP6PL feature (see clause 8.2.25), for IPv6 address allocation using DHCPv6 specified in clause 4.6.2.2 of 3GPP TS 23.316 [57];
- IPv6 prefix shorter than the default /64 prefix for support of IPv6 prefix delegation as specified in clause 4.6.2.3 of 3GPP TS 23.316 [57] and clause 5.14.

More than one UE IP address may be assigned to a PDU session, if the UPF indicates supports of the IP6PL feature (see clause 8.2.25), by provisioning multiple instances of the UE IP Address IE in a same PDI or Traffic Endpoint, or by provisioning multiple PDIs or Traffic Endpoints with a different UE IP Address, where the UE IP addresses may correspond e.g. to:

- multiple /128 IPv6 addresses; or
- an /64 default prefix used for IPv6 stateless autoconfiguration and an IPv6 prefix shorter than the default /64 prefix for IPv6 Prefix Delegation not including the /64 IPv6 Prefix (i.e. when the total IPv6 address space available for the PDU Session cannot be aggregated into one single IPv6 prefix); the IPv6 prefix shorter than the default /64 prefix may be assigned by setting either the IPv6D flag or the IP6PL flag as specified in clause 5.14.

A UE IPv4 address or IPv6 prefix may be allocated by the CP function or the UP function. A given IP address pool shall be controlled by a unique entity (either the SMF/PGW-C or the UPF/PGW-U or an external server).

The support of UE IP address/prefix allocation by the CP function is mandatory. The support of UE IP address/prefix allocation by the UP function is optional. See clause 5.8.2.2 of 3GPP TS 23.501 [28]. A UPF supporting the SSET feature (see clause 5.22.2) or the MPAS feature (see clause 5.22.3) shall support UE IP address/prefix allocation in the UP function.

The UP function shall set the UEIP feature flag in the UP Function Features IE if it supports UE IP address/prefix allocation in the UP function (see clause 8.2.25). If so, the CP function shall determine whether UE IP address or prefix is allocated by the CP function or the UP function based on network configuration.

If the SSET feature (see clause 5.22.2) or the MPAS feature (see clause 5.22.3) is supported, the SMFs in an SMF set may decide that the CP function should allocate the UE IP address or prefix. In such a case, the SMFs in the SMF set may query a DHCP or AAA server for UE IP address or prefix allocation as specified in clause 5.21.2.2.

## 5.21.2 UE IP address/prefix allocation in the CP function

### 5.21.2.1 General

When performing UE IP address allocation in the CP function, the CP function shall assign the UE IP address/prefix and provide the assigned address/prefix to the UP function in the UE IP Address IE of the PDR IE (see Table 7.5.2.2-1) or of the Traffic Endpoint (see Table 7.5.2.7-1). The CP function shall always provide a full list of assigned address(es)/prefix(es) to the UP function in the PDI or Create/Update Traffic Endpoint IE.

### 5.21.2.2 UE IP Address/prefix allocation using DHCP or AAA server

When performing the UE IP address allocation by an SMF set, the SMFs in the SMF set may be configured to use DHCP or AAA server to allocate the UE IP address/prefix as specified in clause 10 of 3GPP TS 29.561 [49] and clauses 11 and clauses 12 of 3GPP TS 29.561 [49], with the following additions:

- one (or more) DHCPv4 or DHCPv6 server or one (or more) AAA server may be deployed within the 5GC for resiliency;

- different SMFs of an SMF set may request, renew and release the IP address assigned to a given PDU session, e.g. when the PDU session is taken over by a different SMF during the lifetime of the PDU session.

The lease time assigned by the DHCP or AAA server for IP addresses may be set by the operator to a long time to minimize the need for IP address renewal. When the lease time is approaching expiry, the SMF should request the DHCP server to renew the IP address (keeping the IP address unchanged) or the SMF should initiate a AAA re-authorization to renew the IP address (keeping the IP address unchanged).

NOTE: The lease time is stored in the PDU session context (which is shared by the SMFs of the SMF set). So any SMF in the SMF set taking over the control of the PDU session can determine whether the lease time is approaching expiry.

## 5.21.3 UE IP address/prefix allocation in the UP function

### 5.21.3.1 General

When performing UE IP address/prefix allocation in the UP function, the CP function shall request the UP function to allocate the UE IP address/prefix by:

- setting the CHOOSE flags (CHOOSE IPV4 and/or CHOOSE IPV6) in the UE IP Address IE of the PDR IE (see Table 7.5.2.2-1) or of the Traffic Endpoint (see Table 7.5.2.7-1); the IPv6 prefix length shall be indicated in the UE IP Address if an IPv6 prefix other than default /64 and other than for IPv6 prefix delegation (see clause 5.14) is to be assigned and the UPF indicated support of the IP6PL feature (see clause 8.2.25); and

- including the Network Instance IE to indicate the IP address pool from which the UE IP address/prefix is to be assigned.

- optionally including the UE IP address Pool Identity from which the UE IP address shall be allocated by the UP function.

The CP function may request the UP function to allocate the same UE IP address/prefix to several PDRs to be created (i.e. using Create PDR) within one single PFCP Session Establishment Request or PFCP Session Modification Request, or to several PDRs to be modified (i.e. using Update PDR) within one single PFCP Session Modification Request by:

- setting the CHOOSE flags (CHOOSE IPV4 and/or CHOOSE IPV6) in the UE IP Address IE of each PDR to be created with a new UE IP address/prefix or each PDR to be modified;

or, if the UP function indicated support of the PDI optimization (see clause 8.2.25), by:

- including the UE IP Address IE in the Create Traffic Endpoint IE or Update Traffic Endpoint IE, and by setting the CHOOSE flags (CHOOSE IPV4 and/or CHOOSE IPV6) in that UE IP Address IE; and

- including the Traffic Endpoint ID in all the PDRs to be created with the same UE IP address or all PDRs to be modified with additional UE IP address(es).

If the PDR(s) is created or modified successfully or the Traffic Endpoint(s) is created or modified successfully, the UP function shall always return the full list of UE IP address/prefix in the UE IP Address IE(s) it has assigned to the PDR(s) or to the Traffic Endpoint(s) in the PFCP Session Establishment Response or PFCP Session Modification Response.

Upon receiving a request to delete a PFCP session, to remove a Traffic Endpoint associated with the UE IP address/prefix, or to remove the last PDR associated with the UE IP address/prefix, the UP function shall release the UE IP address/prefix that was assigned to the PFCP session, to the Traffic Endpoint, or to the PDR.

NOTE 1: When the CP function requests additional UE IP Address in the Update PDR or Update Traffic Endpoint IE, it needs not include any existing UE IP Address(es).

If the UP Function supports the "Per Slice UP Resource management" feature and if the feature is enabled in the UP Function, the UP Function shall take the S-NSSAI associated with the PFCP session into account when allocating UE IP address, together with other information present (e.g. Network Instance, UE IP address Pool Identity).

### 5.21.3.2 Reporting UE IP Address Usage to the CP function

The UE IP Address Usage Reporting feature (see clause 8.2.58) is an optional feature. The following requirements shall apply if UE IP addresses are allocated by the UP function and both the CP function and UP function support the UE IP Address Usage Reporting feature.

The UP Function should report UE IP address usage information to the CP function for network instances and/or IP address pools whose ratio of occupied (i.e. already assigned) IP addresses to the configured IP addresses in the UP Function exceeds a configurable threshold. If the UP Function supports the "Per Slice UP Resource management" feature and if the feature is enabled in the UP Function, the UP Function shall additionally indicate the S-NSSAI associated with the UE IP address usage information. The UP function shall do so by sending one or more PFCP Association Update Request messages to the CP function, including a UE IP Address Usage Information IE per network instance and/or IP address pool. Each UE IP Address Usage Information IE shall include a validity timer that informs the CP function for how long the UE IP address Usage Information shall be considered as valid. Each UE IP Address Usage Information shall also contain a UE IP Address Usage Sequence Number, which enables the CP function to determine the latest UE IP Address Usage Information generated by the UP function for a given network instance and/or IP address pool.

The UP function may update the UE IP address usage information reported to the CP function if needed, by sending subsequent PFCP Association Update Request/Response messages, including updated UE IP address Usage Information IEs with a (new) validity timer. The UP function shall increment the UE IP Address Usage Sequence Number when updating UE IP address usage information. The UP function shall also increment the UE IP Address Usage Sequence Number when the IP address usage has not changed but the validity timer needs to be renewed.

NOTE 1: The threshold value in the UP function needs to be selected in such way that it avoids frequent UE IP address usage reporting for network instances and/or UE IP address pools with low usage.

The CP function shall use the latest updated UE IP address Usage Information received for a given network instance and/or UE IP Address Pool. The CP function shall ignore a UE IP Address Usage Information IE received for a given network instance and/or IP address pool with a UE IP Address Usage Sequence Number smaller or equal to the UE IP Address Usage Sequence Number of an already received and stored information.

If the validity timer has not expired, the CP function shall keep the latest updated UE IP Address Usage Information received for a given Network Instance and/or UE IP Address Pool if it receives a PFCP Association Update Request/Response not including a UE IP Address Usage Information IE for this network instance and/or UE IP Address Pool.

NOTE 2: The UE IP Address Usage Information IE may be absent e.g. if the PFCP Association Update Request/Response is sent for other regular purposes, or if the ratio remains the same, or if the ratio has not changed enough to justify being reported again.

The CP function shall delete UE IP Address Usage Information if its validity period has expired.

# 5.22 PFCP sessions successively controlled by different SMFs of an SMF set (for 5GC)

## 5.22.1 General

A PFCP session may be controlled by different SMFs of an SMF Set using either one PFCP association per SMF Set and UPF as described in clause 5.22.2 (called SSET feature), or with each SMF of the SMF set establishing its own PFCP association with the UPF as described in clause 5.22.3 (called MPAS feature).

A UPF complying with this version of the specification and that supports being controlled by an SMF set shall support the procedures specified in clauses 5.22.3 (i.e. MPAS feature) and may support the procedures specified in clause 5.22.2 (i.e. SSET feature).

The requirements specified in this clause for the UPF, SMF and SMF set shall also apply to:

- combined PGW-U/UPF, combined PGW-C/SMF and combined PGW-C/SMF Set respectively;
- MB-SMF and MB-UPF, for MB-SMFs deployed in an MB-SMF set; and
- combined SMF/MB-SMF, combined UPF/MB-UPF for combined SMF/MB-SMFs Set.

An SMF supporting the SSET feature or the MAPS feature shall be ready to take over the control of a PFCP session from another SMF within the same SMF SET, upon receiving a request from a UPF requiring an SMF change, if possible.

## 5.22.2 With one PFCP association per SMF Set and UPF

When a UPF supports that a PFCP session can be successively controlled by different SMF(s) in the same SMF set, the following applies:

1) One SMF in the SMF set shall establish one single PFCP Association with the UPF for the SMF set; the Node ID in the PFCP Association Setup Request shall be set to an FQDN representing the SMF set.

   The SMF shall indicate that it supports the SSET feature in the CP Function Features IE (see clause 8.2.58); this indicates to the UPF that the PFCP sessions established with this PFCP association can be successively controlled by different SMFs of an SMF set according to the procedure defined in this clause.

   The SMF may also indicate the IP addresses of alternative SMFs within the SMF Set and the IP addresses of alternative PFCP entities pertaining to the same SMF in the Alternative SMF IP Address IE(s) in the PFCP Association Setup Request and in the subsequent PFCP Association Update Request messages. Those Alternative SMF IP Address IE(s) with the PPE (Preferred PFCP Entity) flag set to "1" are alternative PFCP entities that the UPF shall select preferably when such reselection is required as specified in the following bullet 4.

NOTE 1: Those Alternative SMF IP Address IE(s) with the PPE flag set to "1" are PFCP entities in the preferred binding entity corresponding to the binding level in the Binding Indication of the resource context created for the PDU session when binding procedures are supported in the SMF as specified in clause 6.12 of 3GPP TS 29.500 [74].

2) When establishing a PFCP session, the SEID that the SMF assigns in the CP F-SEID of the PFCP Session Establishment Request may be unique or not within the SMF set. However the assigned CP F-SEID shall be unique within the SMF set.

NOTE 2: The UPF does not (need to) know whether the SEID in the CP F-SEID is uniquely assigned in the SMF set or not.

3) Any SMF in the SMF set may issue requests to modify or delete the PFCP session, or to update or release the PFCP association. The UPF shall allow the related PFCP request to come from any other SMF from the same SMF set.

4) The UPF shall initiate PFCP session related requests (e.g. PFCP Session Report Request) towards another PFCP entity pertaining to the same SMF or another SMF of the SMF Set, if the IP address included in the CP F-SEID assigned to the PFCP session is not responsive, or if the UPF receives a GTP-U Error Indication from the SMF over the N4-u tunnel assigned to the N4 session for data forwarding if any.

   The UPF shall firstly use the IP addresses included in those Alternative SMF IP Address IE(s) with the PPE flag set to "1" (if available) whenever possible, then it may use the IP addresses included in the Alternative SMF IP Address IE(s) without the PPE flag set to "1", to contact an alternative PFCP entity. Otherwise the UPF shall use the SMF set FQDN in the CP Node ID to discover alternative SMFs within the SMF Set, e.g. by querying the DNS or by performing a discovery request towards the NRF.

   When sending the request to another PFCP entity pertaining to the same SMF or to the new SMF, the UPF shall set the SEID field to zero in the PFCP header of the PFCP request and include the CP F-SEID assigned by the previous SMF in the request.

5) When receiving a request from a UPF with the SEID field set to zero and CP F-SEID assigned by previous SMF, the SMF shall take over the control of the PFCP session from the previous SMF, unless it is needed to redirect the request to a different SMF (e.g. due to high load or because the corresponding session context has already been taken over by a different SMF in the same SMF set).

   An SMF may redirect a UPF initiated PFCP session related request to another PFCP entity pertaining to the same SMF or to a different SMF in the SMF set by rejecting the request with the cause "Redirection Requested" and with the IP address of the new entity to contact. When sending the redirected request to the new entity, the UPF shall set the SEID field to zero in the header of the PFCP request and include the CP F-SEID assigned by the previous SMF in the request.

   Alternatively, an SMF may forward the UPF request to another PFCP entity pertaining to the same SMF or to a new SMF in the SMF set; the new PFCP entity or the new SMF answers to the UPF, including the CP F-SEID IE with the IPv4 or IPv6 address of the new entity respectively and the same or a modified SEID, and optionally including the N4-u F-TEID that the UPF shall use for sending data towards the new entity.

NOTE 3: This allows to address cases where a different SMF would have been reselected in the 5GC for the PFCP session, e.g. by an AMF.

6) An SMF may also update, at any time, a PFCP session by including the CP F-SEID with the IPv4 or IPv6 address of a new SMF and/or a new SEID assigned by the new SMF in a PFCP Session Modification Request.

7) The UPF shall not trigger the restoration procedures specified in 3GPP TS 23.527 [40] for a PFCP session that can be controlled by different SMFs of an SMF set when a heartbeat failure is detected for the IP address of the assigned CP F-SEID. Restoration procedures shall be triggered only if heartbeat procedures fail with all the IP addresses of all the SMFs in the SMF set.

NOTE 4: The above requirements enable all SMFs of a same SMF set to successively control a given PFCP session without causing extra signalling over the N4 interface.

8) A UPF supporting the SSET feature shall support UE IP address/prefix allocation in the UP function (see clause 5.21).

### 5.22.3 With one PFCP association per SMF and UPF

If multiple PFCP associations are setup between an UPF and the SMFs in an SMF set, the following applies:

1) Each SMF in the SMF set shall establish its own PFCP association with the UPF and shall provide the Node ID IE set to an FQDN or IP address of the SMF and the SMF Set ID IE set to an FQDN representing the SMF set. All SMFs of an SMF set shall indicate the same SMF Set ID. Alternatively, if PFCP Association Setup is initiated by UPF as defined in clause 6.2.6.3, each SMF in the SMF set shall provide this information in PFCP Association Setup Response message.

   The SMF shall indicate that it supports the MPAS feature (Multiple PFCP Associations to the SMFs in an SMF set) in the CP Function Features IE (see clause 8.2.58); this indicates to the UPF that the PFCP sessions established with this PFCP association can be successively controlled by different SMFs of the same SMF set according to the procedure defined in this clause.

The SMF may also provide a list of alternative IP addresses of PFCP entities pertaining to the same SMF in the Alternative SMF IP Address IE in the PFCP Association Setup Request message and in the subsequent PFCP Association Update Request messages. Those Alternative SMF IP Address IE(s) with the PPE flag set to "1" are alternative PFCP entities that the UPF shall select preferably when such reselection is required as specified in the following bullet 6.

The UPF and SMF shall identify the PFCP association by the Node ID of the SMF and UPF respectively.

Likewise, when an SMF is added or removed from the SMF set, this SMF shall establish or tear down its PFCP association with the UPF. Alternatively, when an SMF updates its SMF SET ID using the PFCP Association Update procedure, the UPF shall maintain the existing PFCP sessions served by this SMF and use the new SMF Set ID of the SMF if the UPF needs to later reselect a different SMF instance for these PFCP sessions (as defined in step 6).

2) When establishing a PFCP session, the SEID that the SMF assigns in the CP F-SEID of the PFCP Session Establishment Request may be unique or not within the SMF set. However the assigned CP F-SEID shall be unique within the SMF set.

NOTE 1: The UPF does not (need to) know whether the SEID in the CP F-SEID is uniquely assigned in the SMF set or not. The SMF and the UPF identifies the PFCP session by its own CP F-SEID and UP F-SEID respectively.

3) Any SMF in the SMF set may issue requests to modify or delete the PFCP session. When the SMF controlling a PFCP session changes, the SMF that takes over the control of the PFCP session shall provide its own Node ID and may provide a new CP F-SEID.

   The UPF shall allow the PFCP session modification or deletion request to come from any other PFCP association from the same SMF set.

4) At any time, an SMF may update a PFCP session by including the CP F-SEID with the IPv4 or IPv6 address of a new SMF and/or a new SEID assigned by the new SMF in a PFCP Session Modification Request.

5) When receiving a request from a UPF with the SEID field set to zero and CP F-SEID assigned by previous SMF, the SMF shall take over the control of the PFCP session from the previous SMF, unless it is needed to redirect the request to a different SMF in the same SMF set (e.g. due to high load or because the corresponding session context has already been taken over by a different SMF in the same SMF set).

   An SMF may redirect a UPF initiated PFCP session related request to another PFCP entity pertaining to the same SMF or to a different SMF in the SMF set by rejecting the request with the cause "Redirection Requested" and with the IP address of the new entity to contact. When sending the redirected request to another PFCP entity pertaining to the same SMF or to the new SMF, the UPF shall set the SEID field to zero in the header of the PFCP request and include the CP F-SEID assigned by the previous SMF in the request.

   Alternatively, an SMF may forward the UPF request to another PFCP entity pertaining to the same SMF or another SMF in the SMF set; the new PFCP entity or the new SMF answers to the UPF, including the CP F-SEID IE with the IPv4 or IPv6 address of the new entity respectively and the same or a modified SEID, and optionally including the N4-u F-TEID that the UPF shall use for sending data towards the new entity.

NOTE 2: This allows to address cases where a different SMF would have been reselected in the 5GC for the PFCP session, e.g. by an AMF.

6) The UPF shall initiate PFCP session related requests (e.g. PFCP Session Report Request) towards another PFCP entity pertaining to the same SMF or to another SMF in the SMF set with which the UPF has established associations with the same SMF Set ID, if the IP address included in the CP F-SEID assigned to the PFCP session is not responsive, heartbeat failure towards IP address of the CP F-SEID assigned to the PFCP session, or if the UPF receives a GTP-U Error Indication from the SMF over the N4-u tunnel assigned to the N4 session for data forwarding.

   The UPF shall firstly use the IP addresses included in those Alternative SMF IP Address IE(s) with the PPE flag set to "1" (if available) whenever possible, then it may use the IP addresses included in the Alternative SMF IP Address IE(s) without the PPE flag set to "1", to contact an alternative PFCP entity.

   When sending the request to the new entity, the UPF shall set the SEID field to zero in the PFCP header of the PFCP request and include the CP F-SEID assigned by the previous SMF in the request.

7) The UPF shall not trigger the restoration procedures specified in 3GPP TS 23.527 [40] for a PFCP session that can be controlled by different SMFs of an SMF set when a heartbeat failure is detected. Restoration procedures shall be triggered only if heartbeat procedures fail with all of the SMFs in the SMF set (i.e. the SMFs with which the UPF has established associations with the same SMF Set ID).

8) If an SMF or UPF fails, the peer PFCP node that detects that error shall remove the PFCP association locally.

9) A UPF supporting the MPAS feature shall support UE IP address/prefix allocation in the UP function (see clause 5.21).

### 5.22.4 Restoration of PFCP Sessions associated with an FQ-CSID, Group ID or PGW-C/SMF IP Address

As specified in clause 31.6 of 3GPP TS 23.007 [24] and clause 4.6 of 3GPP TS 23.527[40], for deployments with PGW-C/SMF Set, the CP function (e.g. a PGW-C or a SMF) and the UP function (a PGW-U or a UPF) may support the feature "Restoration of PFCP Sessions associated with one or more PGW-C/SMF FQ-CSID(s), Group Id(s) or PGW-C/SMF IP address(es)". A CP function and a UP function that supports this feature shall behave as specified in clause 5.22.2 or 5.22.3 with the following additional requirements:

1) A UP function that supports this feature shall indicate so to the CP function by setting the RESPS feature bit in the UP Function Feature IE (see clause 8.2.25).

2) The PGW-C/SMF in a PGW-C/SMF Set may allocate a globally unique Group Id to a PFCP session, in the PFCP Session Establishment Request message during the PFCP session establishment procedure and may update the Group Id associated to the PFCP session in a PFCP Session Modification Request message if necessary. The UP function shall store the Group Id associated to a PFCP session. At most one Group ID may be associated to a PFCP session.

3) Alternatively, if partial failure handling is supported, the PGW-C/SMF may assign an FQ-CSID to a PFCP session as specified in clause 31 of 3GPP TS 23.007 [24] and clause 4.6 of 3GPP TS 23.527 [40].

4) The PGW-C/SMF (either the PGW-C/SMF serving the PFCP sessions or another PGW-C/SMF in the same Set taking over the control of the PFCP sessions) may send a PFCP Session Set Modification Request message to the PGW-U/UPF(s), including either one or more PGW-C/SMF FQ-CSID IE(s) allocated earlier, or one or more Group Id IE(s) allocated earlier, or one or more CP (PGW-C/SMF) IP Addresses and an Alternative SMF IP Address IE, to request the PGW-U/UPF(s) to send subsequent PFCP Session Report Request messages to the same or an alternative PGW-C/SMF (as indicated in the Alternative SMF IP Address IE) for the PFCP Sessions which are associated with the PGW-C/SMF FQ-CSID(s) or the Group Id IEs, or which have their F-SEID containing the CP IP Address. The PGW-C/SMF may instruct the UP function to move sessions associated with different PGW-C/SMF FQ-CSID(s), Group Ids or CP IP Addresses, to different PGW-C/SMF addresses.

5) When the PGW-U or UPF sends subsequent PFCP Session Report Request message to the indicated alternative PGW-C/SMF address, the PGW-U or UPF may receive either a new PGW-C/SMF FQ-CSID or a new Group Id for that PFCP session in the PFCP Session Report Response message from the new PGW-C/SMF.

NOTE: The above procedure enables a PGW-C/SMF to move groups of sessions to one or more different PGW-C/SMF instances, e.g. during a partial failure in a PGW-C/SMF or when a PGW-C/SMF is shutting down (e.g. scale-in operation), in one signal PFCP message. This allows the PGW-C/SMF to control how PFCP sessions are re-distributed in the SMF set.

## 5.23 5G VN Group Communication (for 5GC)

Stage 2 requirements for the support of 5G VN communication are specified in clauses 4.4.6 and 5.8.2.13 of 3GPP TS 23.501 [28].

The 5G VN group communication includes one to one communication and one to many communication.

One to one communication supports forwarding of unicast traffic between two UEs within a 5G VN, or between a UE and a device on the DN.

One to many communication supports forwarding of multicast traffic and broadcast traffic from one UE (or device on the DN) to many/all UEs within a 5G VN and devices on the DN.

5G VN Group Communication is optional to support. The SMF may instruct the UPF to forward unicast and/or broadcast traffic as described below if the UPF has indicated support of 5G VN Group Communication (see feature GCOM in clause 8.2.25).

There are 3 different traffic forwarding methods, i.e. UPF local switching, N6-based forwarding and N19-based forwarding, to forward traffic within the 5G VN group.

For all methods, traffic forwarding within the 5G VN group is realized by using a UPF internal interface ("5G VN Internal") and a two-step detection and forwarding process. In the first step, the packets received from any 5G VN group member (via it's PDU Session, via N6 or via N19) are forwarded to the UPF internal interface (i.e. Destination Interface set to "5G VN Internal"). In the second step, PDRs installed at the UPF internal interface (i.e. Source Interface set to "5G VN Internal") detect the packet and forward it to the respective 5G VN group member (via it's PDU Session, via N6 or via N19). If more than one 5G VN group has to be supported, the Network Instance set to a value representing the 5G VN group is used in addition to the UPF internal interface to enable isolation of the 5G VN group communication during the packet detection and forwarding process.

When N19-based forwarding is used, the SMF may correlate all the PDU sessions for the 5G VN Group members to generate the PDR and FAR corresponding to the group level N4-session for UPF as specified in clause 5.29.3 of 3GPP TS 23.501 [28].

For Ethernet unicast traffic on 5G VN Group Communication, the SMF may either explicitly configure DL PDR with the MAC addresses detected by the UPF on PDU Sessions supporting a 5G VN group, or rely on MAC address learning in UPF related with a 5G VN group by setting the Ethernet PDU Session Information indication in the DL PDR of the "5G VN internal" interface as specified in clause 5.8.2.13.0 of 3GPP TS 23.501 [28].

To enable IP or Ethernet type broadcast traffic forwarding of a 5G VN Group, the SMF may provide the PDRs related to the group level N4-session and each 5G VN group member' N4 Session to the UPF as specified in clause 5.8.2.13.3 of 3GPP TS 23.501 [28].

The details of the PDR and FAR setting over N4 for unicast traffic forwarding within a 5G VN are specified in clauses 5.8.2.13.1 and 5.8.2.13.2 of 3GPP TS 23.501 [28].

The details of the PDR and FAR setting over N4 for broadcast traffic forwarding within a 5G VN are specified in clause 5.8.2.13.3 of 3GPP TS 23.501 [28].

# 5.24 Support of Ultra Reliable Low Latency Communication for 5GC

## 5.24.1 General

Stage 2 requirements for the support of Ultra Reliable Low Latency Communication (URLLC) are specified in clause 5.33 of 3GPP TS 23.501 [28].

NOTE 1: In this release of specification redundant transmission on N3/N9 interfaces for URLLC is not supported for PDU Sessions involving an I-SMF. See 3GPP TS 23.501 [28] clauses 5.34, 5.33.2.2 and 3GPP TS 23.502 [29] clause 4.24.

Redundant transmission is applied for supporting the highly reliable URLLC services, there are three different methods: dual connectivity based end to end redundant user plane paths, redundant transmission on N3/N9 interfaces or redundant transmission at transport layer.

NOTE 2: Dual connectivity based end to end redundant user plane paths has no impact to N4 interface.

QoS Monitoring is applied for packet delay measurement. The packet delay between UE and PSA UPF is a combination of the uplink or downlink packet delay on Uu interface and uplink or downlink packet delay between NG-RAN and PSA UPF. The QoS Monitoring on uplink or downlink packet delay between NG-RAN and PSA UPF can be performed on different levels of granularities, i.e. per QoS Flow per UE level, or per GTP-U path level.

Support of the URLLC feature is an optional for the SMF and UPF, for 5GC.

## 5.24.2 Redundant Transmission on N3/N9 interfaces

### 5.24.2.1 General

Stage 2 requirements for support of Redundant Transmission on N3/N9 interfaces for high reliability communication are specified in clause 5.33.2.2 of 3GPP TS 23.501 [28].

This requires duplicating downlink and uplink packets of QoS flows requiring redundant transmission of a PDU session via two independent N3 or N9 tunnels between the RAN and the UPF (PSA).

The following requirements shall apply for QoS flows requiring redundant transmission. Requirements in clause 5.2.2.3.3 shall also apply for traffic usage reporting.

### 5.24.2.2 GTP-U tunnel setup for redundant transmission

The SMF shall request the UPF (PSA) to establish two N3 or N9 tunnels for a PDU session with one or more Service Data Flows associated with QoS flow(s) requiring redundant transmission as follows:

- when provisioning an UL PDR in the UPF (PSA), the SMF shall request the UPF to assign two Local F-TEIDs for the PDR, by provisioning the PDI or the Traffic Endpoint with the Redundant Transmission Detection Parameters IE. The SMF may provide two different Network Instances for these two F-TEIDs to achieve disjoint transport layer paths;

- alternatively, the SMF may request the UPF to assign one Local F-TEID for the related Network Instance when creating the UL PDR, and later request the UPF to assign another Local F-TEID with the same or a different Network Instance when updating the PDR, if the redundant transmission tunnels are not established during the PDU session establishment;

- when provisioning DL FAR in the UPF (PSA) corresponding to QoS flows requiring redundant transmission, the SMF shall request the UPF to duplicate the downlink packets for redundant transmission and the SMF shall provide two F-TEIDs of remote GTP-U tunnel endpoints in the FAR, as described in clause 5.24.2.3;

- alternatively, the SMF may provide one remote endpoint F-TEID when creating the FAR and later provide another remote endpoint F-TEID when updating the FAR, if the redundant transmission tunnels are not established during the PDU session establishment.

NOTE: To forward downlink packets pertaining to service data flows not requiring redundant transmission, the SMF can create a separate FAR not requiring to duplicate the packets.

The PSA UPF shall assign the local F-TEID(s) for establishing the redundant tunnel and include the Local F-TEID(s) for Redundant Transmission IE in the PFCP Session Establishment Response or the PFCP Session Modification Response to the SMF if the Redundant Transmission Detection Parameters IE was received in the corresponding request message.

The SMF shall request the UPF (PSA) to remove one N3 or N9 tunnel used for redundant transmission if redundant transmission is no longer needed as follows:

- request the UPF to remove the local F-TEID for redundant transmission by updating the PDI or the Traffic Endpoint in UL PDR with a null length Redundant Transmission Detection Parameters IE;

- request the UPF to remove the F-TEID of remote GTP-U tunnel endpoint for redundant transmission by updating the FAR in DL PDR with a null length Redundant Transmission Forwarding Parameters IE;

- set the DFRT and EDRT flags to 0 in the FAR associated to the corresponding UL and DL PDRs, to stop duplicating packets and eliminating duplicate packets.

When so instructed, the PSA UPF shall remove the local F-TEID for redundant transmission and the F-TEID of remote GTP-U tunnel endpoint for redundant transmission, stop duplicating packets and stop detecting/eliminating duplicate packets accordingly.

#### 5.24.2.3 Duplicating downlink packets for redundant transmission

If redundant transmission is required for a QoS flow, the SMF shall instruct the PSA UPF to replicate each downlink packet of the QoS Flow and to assign a sequence number to them by provisioning a FAR with the following information in a PFCP Session Establishment Request or PFCP Session Modification Request:

- the Redundant Transmission Forwarding Parameters IE including an Outer Header Creation IE set to the remote F-TEID of the redundant GTP-U tunnel, and if the GTP-U tunnel for redundant transmission uses a different network instance than the primary GTP-U tunnel, the Network Instance to be used for redundant transmission;
- the Apply Action IE with both the FORW and the DFRT flags set to "1".

When so instructed, the PSA UPF shall replicate downlink packets associated to such a FAR and construct the duplicated downlink packets using the information included in the Redundant Transmission Forwarding Parameters IE and other information included in the Forwarding Parameters IE for information that is not part of the Redundant Transmission Forwarding Parameters IE. The PSA UPF shall add the same sequence number in the PDU Session Container extension header of the downlink packet and the related duplicated downlink packets as specified in 3GPP TS 38.415 [34].

#### 5.24.2.4 Eliminating duplicated uplink packets

For QoS flows for which redundant transmission is required, the SMF shall also instruct the PSA UPF to eliminate the duplicated uplink packets of the QoS Flow, based on their sequence numbers in the PDU Session Container extension header by setting the EDRT flag and the FORW flag in the Apply Action IE in the FAR IE to request the UPF to eliminate the duplicated uplink packets based on the sequence number, i.e. to forward the uplink packets and to drop duplicated uplink packets. When so instructed, the PSA UPF shall forward the only one copy of the uplink packets and drop duplicate uplink packets.

### 5.24.3 Redundant Transmission at transport layer

Stage 2 requirements for support of Redundant Transmission at transport layer for high reliability communication are specified in clause 5.33.2.3 of 3GPP TS 23.501 [28].

If it supports the redundant transmission at transport layer, the UP function shall set the RTTL feature flag in the UP Function Features IE (see clause 8.2.25). If so, during the UE requested PDU session establishment procedure, the CP function may select the UPF that supports redundant transmission at transport layer for the PDU session.

Requirements in clause 5.2.2.3.3 shall apply for traffic usage reporting.

NOTE: How the UPF perform the redundant transmission at transport layer is left up to UPF implementation.

### 5.24.4 Per QoS Flow Per UE QoS Monitoring

#### 5.24.4.1 General

Stage 2 requirements for support of per QoS flow per UE QoS monitoring are specified in clause 5.33.3.2 of 3GPP TS 23.501 [28].

The UPF shall set the QFQM feature flag in the UP Function Features IE if it supports per QoS flow per UE QoS monitoring (see clause 8.2.25). If so, the SMF may request the UPF to perform the per QoS flow per UE QoS monitoring during a PFCP session establishment or a PFCP session modification procedure.

The SMF shall provision one or more QoS Monitoring per QoS flow control Information IEs to instruct the UPF to monitor the packet delay(s) of QoS flows as specified in clause 5.24.4.2. The SMF may request the UPF to stop the on-going QoS monitoring as specified in clause 5.24.4.2, when needed.

The UPF shall report the QoS monitoring result of the QoS flows to the SMF by sending QoS Monitoring Report IEs to the SMF as specified in clause 5.24.4.3, or by reporting the QoS monitoring events directly to the Local NEF or AF (see clause 5.33.5).

### 5.24.4.2 QoS Monitoring Control

If the per QoS Flow per UE QoS monitoring is required, the SMF may provision the following IEs included in the QoS Monitoring per QoS flow Control Information IE:

- one or more QFI IEs indicating the QoS flow(s) required for the QoS monitoring;
- a Requested QoS Monitoring IE indicating a request to monitor the downlink packet delay, uplink packet delay, and/or the round trip packet delay between the UPF (PSA) and UE;
- a Reporting Frequency IE indicating the frequency for the reporting, such as event triggered, periodic, and/or when the PDU Session is released;
- a Packet Delay Thresholds IE indicating thresholds for the downlink packet delay, uplink packet delay, and/or the round trip packet delay to generate the QoS monitoring reports to the CP function, if the Event Triggered QoS monitoring reporting is required in the reporting frequency.
- a Minimum Wait Time IE, to indicate the minimum waiting time between two consecutive reports, if the Event Triggered QoS monitoring reporting is required in the reporting frequency;
- a Measurement Period IE, indicating the period to generate periodic usage reports to the CP function if the periodic QoS monitoring reporting is required in the reporting frequency.

The SMF may require the UPF to stop the on-going QoS monitoring, by sending a PFCP Modification Request with the Remove SRR IE, or by sending a PFCP Modification Request with the Update SRR IE within which the previous QoS Monitoring per QoS flow Control IE is removed. Upon receiving such a PFCP Modification Request message, the UPF shall stop the on-going QoS monitoring.

### 5.24.4.3 QoS Monitoring Reporting

If the UPF is requested to perform QoS Monitoring (i.e. it receives one or more QoS Monitoring per QoS flow Control Information IEs from the SMF), the UPF shall select one or more downlink payload packets pertaining to every requested QoS flow(s) whenever available or create one or more dummy downlink GTP-U packets (i.e. G-PDU messages without a T-PDU as specified in clause 5.2.2.7 of 3GPP TS 29.281 [3]) otherwise, and insert the time stamp, and set the QoS Monitoring Packet (QMP) flag to "1" and the corresponding QoS Flow Identifer (for the requested QoS flow) into the GTP-U PDU Session Container extension header (see 3GPP TS 38.415 [34]) of these downlink packets.

When receiving the uplink packet related to the requested QoS flow(s), the UPF shall measure the packet delay(s) based on the time stamp(s) and packet delay(s) included in the GTP-U PDU Session Container extension header (see 3GPP TS 38.415 [34]) of the uplink packet, and generate a QoS monitoring report towards the SMF, if the packet delay(s) exceeds the defined Packet Delay Thresholds and Event Triggered QoS monitoring reporting is required in the reporting frequency. The UPF may send a next report only after the minimum waiting time indicated by the SMF.

NOTE: The dummy GTP-U packet(s) are not forwarded to the UE neither to the Packet Data Network, thus they are not measured for usage reporting. An Intermediate UPF between the PSA UPF and the NG-RAN forwards any received dummy GTP-U packets together with the GTP-U PDU Session Container extension header to the next GTP-U entity.

If the Periodic QoS monitoring reporting is required in the reporting frequency, the UPF shall generate QoS monitoring report based on the Measurement Period.

The UPF shall send QoS Monitoring Report IE to the SMF in PFCP Session Report Request; several QoS Monitoring Report IEs may be present to report the packet delay(s) for multiple QoS flows. The UPF shall include the delay value (Downlink, Uplink and/or Round trip) in the QoS Monitoring Measurement IE in the QoS Monitoring Report IE. See clause 5.33.5 for reporting the QoS monitoring events directly to the Local NEF or AF.

The UPF shall continue to apply all the provisioned SRR(s) and perform the related QoS monitoring measurement(s), until getting any further instruction from the CP function.

When receiving a new threshold (Packet Delay Thresholds, Minimum Wait Time and/or Measurement Period) from the SMF for a measurement that is already ongoing in the UPF, the UPF shall consider its ongoing measurements against the new threshold to determine when to send its next QoS monitoring report to the SMF or to the Local NEF or AF (if direct reporting of QoS monitoring event applies, see clause 5.33.5).

When receiving instruction from the SMF to stop the on-going QoS monitoring, the UPF shall generate a QoS monitoring report to the SMF or to the Local NEF or AF (if direct reporting of QoS monitoring event applies, see clause 5.33.5), to report the detected packet delay(s).

At the PFCP session termination, the UPF shall include a QoS Monitoring Report IE in the PFCP Session Deletion Response or the UPF shall send a QoS monitoring event directly to the Local NEF or AF (if direct reporting of QoS monitoring event applies, see clause 5.33.5), if the reporting frequency requests a report to be generated at the PFCP session termination.

If the Event Triggered QoS monitoring reporting is required in the reporting frequency, and no time stamp is received in uplink packet for a delay exceeding the Packet Delay Thresholds, the UPF shall generate a QoS monitoring report indicating a packet delay measurement failure to the SMF or to the Local NEF or AF (if direct reporting of QoS monitoring event applies, see clause 5.33.5).

If the Periodic QoS monitoring reporting is required in the reporting frequency, and no time stamp is received in uplink packet for a delay exceeding the Measurement Period, the UPF shall generate a QoS monitoring report indicating a packet delay measurement failure to the SMF or to the Local NEF or AF (if direct reporting of QoS monitoring event applies, see clause 5.33.5).

## 5.24.5 Per GTP-U Path QoS Monitoring

### 5.24.5.1 General

Stage 2 requirements for support of per GTP-U path QoS monitoring are specified in clause 5.33.3.3 of 3GPP TS 23.501 [28].

The UPF shall set the GPQM feature flag in the UP Function Features IE if it supports per GTP-U Path QoS monitoring (see clause 8.2.25).

### 5.24.5.2 GTP-U path monitoring

If the UPF is known to support this feature (e.g. by the UP Function Features IE), the SMF may request the UPF to measure the packet delay for transport paths towards remote GTP-U peers during a PFCP association setup or a PFCP association update procedure, by provisioning GTP-U Path QoS Control Information including:

- the identification of the GTP-U paths to be monitored, i.e.:
  - the IP destination address of one or more remote GTP-U peers, and if available, the network instance used to reach each remote GTP-U peer and the DSCP value(s) to measure the packet delay; or
  - the interface type(s) (i.e. N9 and/or N3) of the GTP-U paths;
- the values of the DSCP in the TOS/Traffic Class field to measure the packet delay, if available;
- the conditions and QoS parameters for the UPF to report measurements to the SMF, i.e. one or more of:
  - immediate report;
  - periodic report, with the reporting time period; and/or
  - event triggered report, when the average, minimum and/or maximum packet delay on a GTP-U path exceeds corresponding thresholds.

If so instructed, the UPF shall perform an estimation of the RTT for the GTP-U paths requested to be monitored, by sending Echo Request messages (with each requested DSCP value, if any) and measuring the time that elapses between the transmission of the Echo Request message and the reception of the Echo Response message. The UPF shall compute the packet delay by adding RTT/2 and the UPF internal processing time, thus the measured delay represents an estimated elapsed time for the GTP-U path (since a user plane packet entered the UPF and its reception by the next downstreams or upstreams GTP-U peer). The UPF shall send QoS reports to the SMF by including GTP-U Path QoS Report IE(s) in a PFCP Node Report Request message.

If the GTP-U paths to be monitored are identified by their interface types (e.g. N9 and/or N3), the UPF shall monitor all GTP-U paths of all PFCP sessions established with a FAR including a matching Destination Interface Type.

For event triggered reporting, the UPF shall send a first report when a reporting threshold is exceeded and a minimum waiting time shall be applied for the subsequent report for the same type of measurement (e.g. maximum packet delay) and the same remote GTP-U peer (if the threshold is exceeded after the waiting time).

### 5.24.5.3 QoS monitoring of a PDU session based on GTP-U path monitoring

The SMF may request the UPF (PSA) to monitor the Uplink, Downlink or Round-Trip delay per QoS flow per UE, as specified in clause 5.24.4.2 with the following addition:

- In the QoS Monitoring per QoS flow Control Information IE, the SMF shall indicate that QoS monitoring is performed based on GTP-U path monitoring by setting the GTPUM flag to 1 in the Requested Qos Monitoring IE.

Additionally, for the UPF (PSA) and for any intermediate UPF in the path of the PDU session, the SMF (or I-SMF) shall request the UPF:

- to measure the one-way delay of the GTP-U path with the preceding uplink GTP-U entity; this corresponds to the N3 path for a UPF connected to the RAN, and to a N9 path for a UPF connected to an intermediate UPF;
- to add this delay to the "N3/N9 Delay Result" field received in the GTP-U PDU Session Container extension header (see 3GPP TS 38.415 [34]) of the uplink packet; and
- for an intermediate UPF, to send the resulting value in the "N3/N9 Delay Result" field in the GTP-U PDU Session Container extension header (see 3GPP TS 38.415 [34]) of the uplink packet it forwards (towards the PSA).

The SMF shall request the above to the UPF (PSA or I-UPF) by including the Transport Delay Reporting IE in the UL PDR(s) associated to the corresponding QoS flow to be monitored. Multiple QoS flows may be monitored for a given PDU session as specified in clause 5.24.5.4.

When so requested, each UPF shall, for UL GTP-U packets with the PDU Session Container extension header including the RAN Uplink and/or Downlink fields, add the delay of the GTP-U path with the preceding uplink GTP-U entity.

NOTE: The "N3/N9 Delay Result" field is computed by the intermediate UPF(s) and UPF (PSA). The RAN does not report the N3 path delay. The intermediate UPF connected to the RAN adds the N3 delay; the next intermediate UPF (if any) adds the N9 delay with the first intermediate UPF and the PSA adds the N9 delay of the last GTP-U path towards the PSA. If the PSA is directly connected to the RAN, the PSA measures the N3 delay.

The SMF may request the UPF to stop the on-going QoS monitoring (based on GTP-U path monitoring) for a PDU session, by sending a PFCP Modification Request with the Remove SRR IE, or by sending a PFCP Modification Request with the Update SRR IE within which the previous QoS Monitoring per QoS flow Control IE is removed. Upon receiving such a PFCP Modification Request message, the UPF shall stop the on-going QoS monitoring.

### 5.24.5.4 QoS Monitoring Reporting

QoS monitoring reporting by the PSA shall be performed as specified in clause 5.24.4.3, with the following modifications.

The UP function shall not insert time stamps into the GTP-U PDU Session Container extension header (see 3GPP TS 38.415 [34]) of downlink packets.

When receiving the uplink packet related to the requested QoS flow(s), the PSA shall measure the Uplink or Downlink delay by computing the sum of the end to end accumulated transport delay (computed as defined in clause 5.24.5.3) and the RAN UL or DL delay included in the GTP-U PDU Session Container extension header (see 3GPP TS 38.415 [34]) of the uplink packet.

## 5.25 Support of IPTV (for 5GC)

IPTV service is defined in clause 4.9.1 of of 3GPP TS 23.316 [51]. Stage 2 procedures to support IPTV service are defined in clauses 4.6 and 7.7.1 of 3GPP TS 23.316 [51].

Support of IPTV service is optional for the SMF and UPF. The following requirements shall apply for IPTV service if the UPF supports the IPTV feature (see clause 8.2.25).

This requires the UPF (PSA) to support:

- terminating and managing IGMP or MLD messages received from the UE;
- acting as a Multicast Router as defined in in IETF RFC 2236 [52] and IETF RFC 3376 [53];
- replicating IP multicast traffic received from the N6 interface over PDU sessions having joined the corresponding IP multicast group;
- notifying the SMF when a PDU session has joined or left a multicast group, if so requested by the SMF.

NOTE: In this specification, "IGMP" refers to IGMPv2 and IGMPv3 and "MLD" refers to MLDv1 and MLDv2, unless specified otherwise.

For a PDU session used for IPTV service, the SMF shall provision the following rules in the UPF to control the UL IGMP/MLD traffic and the DL IP multicast traffic as follows:

- for the control of UL IGMP or MLD traffic:
  - a PDR that shall identify IGMPv2 (see IETF RFC 2236 [52]), IGMPv3 (see IETF RFC 4604 [54]), MLD (see IETF RFC 2710 [55]) and/or MLD2 (see IETF RFC 4604 [54]) signalling, i.e.:

- with a PDI containing an SDF filter with a Flow Description identifying packets with IP Protocol number of 2, or with a pre-defined PDR matching the same, for IGMP traffic;

- with a pre-defined PDR matching traffic with IPv6 Next Header type value 58 and ICMP Field Type value 131 or 143, for MLD traffic.

  - this PDR may also contain IP Multicast Addressing Info IE(s) identifying (ranges of) IP multicast group(s); if no IP Multicast Addressing Info IE is included, the PDR is meant to match any IP multicast group.
  - an associated FAR containing the Apply Action IE with the IPMA (IP Multicast Accept) or the IPMD (IP Multicast Deny) flag set in order to request the UPF to accept or deny the UE requests to join the corresponding IP multicast group(s);

- for the control of DL IP multicast traffic
  - a PDR including IP Multicast Addressing Info IE(s), identifying (ranges of) IP multicast addresses (DL IP multicast flows) or indicating any IP multicast address by the A (Any) flag set to "1";
  - an associated FAR containing the Apply Action IE set to forward or buffer the packets, and in the former case with the Outer Header Creation IE set to add the remote N3 or N9 GTP-U tunnel IP address and TEID related with the PDU session;
  - optionally an associated QER indicating the QoS to use for the PDU session for the IP Multicast traffic that has been replicated.

The UPF shall add or remove the PDU session to/from the DL replication tree associated with an IP Multicast flow, when the UE request to join the IP Multicast flow is accepted or when the UE requests to leave the IP Multicast flow. When receiving downlink IP multicast traffic, the UPF shall replicate the traffic towards each PDU session that has joined the corresponding IP multicast group and that is provisioned with a DL PDR enabling the forwarding of the corresponding IP multicast traffic.

Additionally, the SMF may provision a URR, associated with the UL PDR controlling the IGMP or MLD traffic, with a Reporting trigger set to "IP multicast join/leave" to request the UPF to report to the SMF when it adds or remove the PDU session to/from the DL replication tree associated with an IP Multicast flow. Corresponding reports shall contain the Multicast IP address of the DL multicast flow and, if available, the Source specific IP address(es) of the DL IP multicast flow.

# 5.26 Support of Time Sensitive Communications and Time Synchronization (for 5GC)

## 5.26.1 General

The SMF may request the UPF to measure and report the clock drift between the TSN time and 5GS time for one or more TSN time domains (see clause 5.27.2 of 3GPP TS 23.501 [28]), by provisioning one or more Clock Drift Control Information IE(s) in a PFCP Association Setup Request or a PFCP Association Update Request, with the following information:

- TSN Time Domain Number IE(s), identifying the TSN working time domain(s), e.g. PTP (Precision Time Protocol) "domainNumber", for which clock drift needs to be measured and reported (see clause 5.27.1.3 of 3GPP TS 23.501 [28]). This may be present if the Configured Time Domain IE is omitted. The SMF may omit the Time Domain Number IE in the request; if neither the Time Domain Number IE nor the Configured Time Domain IE is included, the UPF shall report the clock drift for all Time domains the UPF is connected to;

- Configured Time Domain IE with the CTDI (Configured Time Domain Indicator) flag set to "1", to indicate that clock drift needs to be measured and reported for the Time Domain Number configured in the NW-TT(s). This may be present if the Time Domain Number IE is omitted;

- the requested Clock Drift Information, indicating a request to report when the Time Offset Reporting Threshold is exceeded and/or when the cumulative RateRatio Reporting Thresholds is exceeded;

- the Time offset reporting threshold (i.e. the maximum time offset between the TSN time and 5G system time), if Time Offset Reporting is requested;

- the Cumulative rateRatio measurement threshold (i.e. related to cumulative rateRatio calculated at NW-TT)), if Cumulative RateRatio Reporting is requested.

If so requested, when detecting either of the clock drift offset triggers exceeding the defined threshold, the UPF shall send a PFCP Node Report Request to the SMF, including one or more Clock Drift Reports, with the corresponding TSN Time Domain Number(s), measurement information and Network Instance (if available) and the combination of DNN and S-NSSAI (if available).

## 5.26.2 5GS Bridge management

5GS Bridge information reporting is defined in Annex F.1 of 3GPP TS 23.502 [29]; this procedure enables the SMF to report 5GS Bridge/User Plane Node information of a PDU session established for Time Sensitive Communication (TSC) to the TSN AF or TSCTSF via the PCF.

Identities of 5GS Bridge/User Plane Node and UPF/NW-TT ports may be pre-configured in the UPF based on deployment. When establishing the PFCP session for the PDU session for TSC, the SMF shall provide the Network Instance IE and it may provide the APN/DNN IE and S-NSSAI IE to the UPF to enable the UPF to respond with the proper User Plane Node ID or Bridge ID based on configuration information associated with the network instance or DNN and S-NSSAI pair. The 5GS User Plane Node IE shall contain the Bridge ID in case of IEEE TSN.

In order to establish a PDU Session for TSC, the SMF shall send a PFCP Session Establishment Request to the UPF to establish the corresponding PFCP session as specified in this specification. Additionally, the SMF shall request the UPF to allocate the port number for DS-TT and provide the related 5GS User Plane Node by including the Create Bridge Info for TSC IE with the Bridge Information Indication (BII) bit set to "1", in the PFCP Session Establishment Request. If so requested, the UPF shall provide corresponding information to the SMF in the Created Bridge Info for TSC IE in the PFCP Session Establishment Response message.

NOTE: The port number for DS-TT and Bridge ID are not meant to be used in PDRs.

## 5.26.3 Transfer of 5GS bridge and port management information

5GS User Plane Node and port information configuration is defined in clause 5.28.3 of 3GPP TS 23.501 [28] and in Annex F of 3GPP TS 23.502 [29]; this procedure enables the SMF to relay transparently bridge and/or port related information between the TSN AF or TSCTSF and the NW-TT (and DS-TT).

Port management information shall be transferred between the SMF and UPF in a Port Management Information Container (PMIC). If the NW-TT supports several ports, and port management information needs to be sent for several ports, a separate PMIC shall be used for each port.

User Plane Node management information shall be transferred between the SMF and UPF in a User Plane Node Management Information Container (UMIC).

The SMF and UPF may send a PMIC or a UMIC using PFCP session related procedures of any PFCP session associated with the 5GS bridge.

The SMF may provide NW-TT related UMIC and/or PMIC(s) to the UPF by sending a PFCP Session Modification Request to the UPF including the TSC Management Information IE.

For a PDU session established for TSC, the UPF may send NW-TT related UMIC and/or PMIC(s) to the SMF by sending a PFCP Session Modification Response or a PFCP Session Report Request including the TSC Management Information IE.

The details of the User Plane Node and Port Management Container communication between NW-TT and TSN AF or TSCTSF is defined in the 3GPP TS 24.539 [63].

### 5.26.4 Reporting clock drift between External and 5GS times from UPF to SMF

The SMF may request the UPF to measure and report the clock drift between the external time and 5GS time for one or more external time domains (see clause 5.27.2.4 of 3GPP TS 23.501 [28]), by provisioning one or more Clock Drift Control Information IE(s) in a PFCP Association Setup Request or a PFCP Association Update Request, with the following information:

- Time Domain Number IE(s), identifying the working time domain(s), e.g. PTP (Precision Time Protocol) "domainNumber", for which clock drift needs to be measured and reported. This may be present if the Configured Time Domain IE is omitted. The SMF may omit the Time Domain Number IE in the request; if neither the Time Domain Number IE nor the Configured Time Domain IE is included, the UPF shall report the clock drift for all Time domains the UPF is connected to;

- Configured Time Domain IE with the CTDI (Configured Time Domain Indicator) flag set to "1", to indicate that clock drift needs to be measured and reported for the Time Domain Number configured in the NW-TT(s). This may be present if the Time Domain Number IE is omitted.

- the requested Clock Drift Information, indicating a request to report when the Time Offset Reporting Threshold is exceeded and/or when the cumulative RateRatio Reporting Thresholds is exceeded;

- the Time offset reporting threshold (i.e. the maximum time offset between the external time and 5G system time), if Time Offset Reporting is requested;

- the Cumulative rateRatio measurement threshold (i.e. related to cumulative rateRatio calculated at NW-TT)), if Cumulative RateRatio Reporting is requested.

If so requested, when detecting either of the clock drift offset triggers exceeding the defined threshold, the UPF shall send a PFCP Node Report Request to the SMF, including one or more Clock Drift Reports, with the corresponding Time Domain Number(s), measurement information and Network Instance (if available) and the combination of DNN and S-NSSAI (if available).

## 5.27 Inter-PLMN User Plane Security

Stage 2 requirements for support of the Inter-PLMN User Plane Security (IPUPS) functionality are defined in clauses 4.2.4, 5.8.2.14, 6.2.3, and 6.3.3.3 of 3GPP TS 23.501 [28], and in clauses 4.2.2 and 5.9.3.4 of 3GPP TS 33.501 [64].

The IPUPS functionality shall be activated for the user plane traffic received over N9 interface across PLMNs, according to operator's policy. The SMF shall provision UL/DL PDR(s) to identify the user plane traffic received at the local F-TEID in the UPF and provision UL/DL FAR(s) to forward the user plane traffic to the remote F-TEID in the

GTP-U peer. User plane packets not matching any PDR shall be dropped, using mechanisms defined in this specification, see e.g. clause 5.2.1.

During a PFCP Association Setup procedure, an UPF, which is configured to be used for IPUPS shall indicate this with the UPF configured for IPUPS (UUPSI) flag, as specified in clause 7.4.4.2.

NOTE: Any UPF can support the IPUPS functionality. In network deployments where specific UPFs are used to provide IPUPS, UPFs configured for providing IPUPS services (i.e. reporting the UUPSI flag) are selected to provide IPUPS function.

# 5.28 Downlink data delivery status with UPF buffering (for 5GC)

## 5.28.1 General

Stage 2 requirements for the support of Downlink data delivery status notification with UPF buffering are specified in clause 5.8.3.2 of 3GPP TS 23.501 [28] and clauses 4.15.3.2.8 and 4.15.3.2.9 of 3GPP TS 23.502 [29].

If the UP function supports the Downlink data delivery status notification with UPF buffering, the UP function shall set the DDDS feature flag in the UP Function Features IE (see clause 8.2.25). If so, the CP function may request the UP function to notify the first buffered DL packet and / or the first discarded DL packet for the traffic matching the downlink PDR by set the BUFF flag, BDPN flag and DDPN flag in the Apply Action IE of the FAR. The CP function may also provide the DL Buffering Duration IE and DL Buffering Suggested Packet Count IE in the related BAR to the UP function.

The UP function shall report the first buffered DL packet for each service data flow identified by a PDR, by sending a PFCP Session Report Request including a Downlink Data Report IE identifying the PDR(s) for which downlink packets have been received. The UP function shall also report the first discarded DL packet for each service data flow identified by a PDR if the DL Buffering Duration or DL Buffering Suggested Packet Count is exceeded. DL Data Status IE shall be included in the Downlink Data Report IE to indicate the report is triggered by the Downlink data delivery status with UPF buffering when the first DL packet is buffered or discarded.

NOTE The CP function can request the UP function to report the first buffered DL packet by setting the BDPN flag and / or the NOCP flag in the Apply Action IE of the FAR. If the BDPN flag is set, the UP function reports the first buffered DL packet for each service data flow identified by a PDR associated to the FAR. If the NOCP flag is set, the UP function reports the first buffered DL packet of any PDR associated to the FAR, i.e. if there are subsequent DL packets (pertaining to different service data flow identified by other PDRs associated to the FAR), there is no new report sent to the CP function.

If the UP function supports the Downlink data delivery status notification with UPF buffering, the CP function may also request the UP function to drop the DL packets directly and send a notification for the traffic matching the downlink PDR by set the DROP flag and DDPN flag in the Apply Action IE of the FAR.

The UP function shall report the dropped DL packets for each service data flow identified by a PDR, by sending a PFCP Session Report Request including a Downlink Data Report IE identifying the PDR(s) for which downlink packets have been received.

# 5.29 Support Reliable Data Service

Clause 5.31.6 of 3GPP TS 23.501 [28], clause 4.3.2 of 3GPP TS 23.502 [29] and clause 4.5.14.3 of 3GPP TS 23.682 [66], specify that The Reliable Data Service (RDS) may be used between the UE and UP function when using a PDU Session of PDU Type 'Unstructured' in 5GS or using PDN Connection of PDN Type 'Non-IP' in EPS. The service is enabled or disabled based on DNN and NSSAI Configuration per SLA in 5GS or APN Configuration per SLA in EPS.

If the UE indicates its capability of supporting RDS in the Protocol Configuration Options (PCO) and if the UP function indicated support of the RDS feature, the CP function may request the UP fuction to apply the RDS functionality for the PDU session by sending "Provide RDS Configuration Information" IE within PFCP Session Establishment Request message (see clause 7.5.2.11).

If the UP function supports and accepts RDS, it should respond to CP function by setting RDS flag in "RDS Configuration Information" IE within PFCP Session Establishment Response message (see clause 7.5.3.8), and the UP

function should place unstructed DL data from N6/SGi in the payload of RDS protocol and then insert it as GTP-U payload, and vice versa for UL data.

Then the CP function should indicate to the UE, in the PCO, that the RDS shall be used if enabled in the DNN and NSSAI configuration in 5GS or APN configuration in EPS. The Reliable Data Service is enabled afterwards.

Reliable Data Service protocol is defined in 3GPP TS 24.250 [65].

# 5.30 Notifying Start Pause of Charging

The requirements for PGW Pause of Charging in EPC are specified in clause 5.3.6A of 3GPP TS 23.401 [14] and the requirements for SMF Pause of Charging feature for 5GC are specified in clause 4.4.4 of 3GPP TS 23.502 [29].

To reduce the charging discrepancy between SGW-C and PGW-C, or between I/V-SMF and (h)SMF due to the signalling latency to notify start pause of charging, the CP function (SGW-C and PGW-C for EPC, I/V-SMF and (H-)SMF for 5GC) and UP function (SGW-U and PGW-U for EPC, I/V-UPF and PSA UPF) may support the Notify Start Pause of Charging via user plane feature (NSPOC) as described below.

When both the CP function and the UP function support the NSPOC feature, and the peer CP function (PGW-C or (H-)SMF) and peer UP function (PGW-U or PSA UPF) are known to support the NSPOC feature as specified in 3GPP TS 29.274 [9] and 3GPP TS 29.502 [50], the CP function (SGW-C, or I/V-SMF) may set the SSPOC bit to "1" in the Measurement Information included in the URR when the Dropped DL Traffic Threshold is provisioned, to request the UP function (SGW-C, I/V-UPF) to send a Start Pause of Charging indication via one or more GTP-U Tunnel Status message to the upstream GTP-U entity(s) when the Dropped DL Traffic Threshold is reached.

When both the CP function and the UP function support the NSPOC feature, the CP function (PGW-C, or (H-)SMF) may set the ASPOC bit to "1" in the Measurement Information included in the URR if the URR is intended for charging, to request the UP function to stop the usage measurement for the URR when receiving Start Pause of Charging indication from the peer downstream GTP-U entity, so that the UP function shall behave as if the Inactive Measurement flag had been set for the URR when it receives a Tunnel Status message with the Start Pause of Charging indication is set to "1" from the downstream peer GTP-U entity.

Regardless of whether the NSPOC feature is supported and used, the procedures specified in clause 5.3.6A of 3GPP TS 23.401 [14] and clause 4.4.4 of 3GPP TS 23.502 [29] for starting and stopping Pause of Charging for EPC and 5GC respectively shall be performed, i.e. the UP function (SGW-U or I/V-UPF) shall still be instructed to generate a usage report when the Dropped DL Traffic Threshold is reached, the SGW-C or V/I-SMF shall request the PGW-C or (H-)SMF to start or stop charging, and the PGW-C or (H-)SMF shall instruct the UP function (PGW-U or PSA UPF) to inactivate or activate measurement for URR(s) applicable for charging.

When the NSPOC feature is supported and used, the CP function (PGW-C or (H-)SMF) may:

- set the "SUMPC" flag in PFCPSMReq-Flags IE to "1" to request the UP function to stop the usage measurement for all URRs with the "ASPOC" flag set to "1", e.g. when the CP function is informed to start Pause of Charging via control plane;

- set the "RUMUC" flag in PFCPSMReq-Flags IE to "1" to request the UP function to resume the usage measurement for all URRs with the "ASPOC" flag set to "1", e.g. when the CP function is informed to stop Pause of Charging via control plane;- set the "CIAM" flag together with Inactive Measurement flag in the Measurement Information IE in the Create URR IE or Update URR IE to stop or resume the usage measurement for a specific URR with the "ASPOC" flag set to "1".

The UP function shall stop or resume the usage measurement for all the URRs with the "ASPOC" flag set to "1" upon receipt of a PFCP Session Establishment Request or PFCP Session Modification Request with the "SUMPC" or "RUMUC" flag set respectively, regardless the current value of the Inactive Measurement flag for a given URR.

The UP function shall start the usage measurement for a URR with the "ASPOC" flag set to "1" unless both the "CIAM" and "INAM" flags are set to "1" or unless the "SUMPC" flag is set to 1 in the same message, when the URR is provisioned in a Create URR IE.

NOTE 1: Only the "SUMPC" flag can be set in the PFCP Session Establishment Request message, e.g. during a restoration procedure for a UPF failure.

The UP function shall stop or resume the usage measurement for a specific URR with the "ASPOC" flag set to "1" upon receipt of a PFCP Session Modification Request including an Update URR IE with the Measurement

Information IE, according to the value of the "INAM" flag, if the "CIAM" flag is set to 1. If the "CIAM" flag is set to 0, the UP function shall ignore the "INAM" flag received in the Measurement Information for a URR with the "ASPOC" flag set to "1".

NOTE 2: Notifying Start Pause of Charging via GTP-U fastens the triggering of charging pause in the PGW-U or UPF (PSA). If the GTP-U Tunnel Status messages are lost, charging is paused when receiving the corresponding instruction from the PGW-C/SMF.

NOTE 3: The UP function will forward Tunnel Status message to the upstream GTP-U entity(s) if it is not a PSA UPF or PGW-U connecting to N6 or SGi interface. If the UP function is a UL/CL or BP, it needs send or forward the Tunnel Status message to all of PSA UPFs.

NOTE 4: The UP function resumes the usage measurement for all URRs with the "ASPOC" flag set to "1" regardless if the usage measurement was stopped by the CP function using the "SUMPC" flag or using the Inactive Measurement flag per URR, or upon being notified by the downstream GTP-U entity using Tunnel Status message.

NOTE 5: When the CP function uses Inactive Measurement flag to stop the usage measurement for a given URR, it can set the "ASPOC flag" to "0" if the CP function doesn't want that the usage measurement is resumed when applying "RUMUC".

# 5.31 Support of L2TP

## 5.31.1 General

Stage 2 requirements for the support of Layer 2 Tunneling Protocol (L2TP) are specified in clause 5.8.2.16 of 3GPP TS 23.501 [28], clause 4.3.2.4 of 3GPP TS 23.502 [29] and clause 5.5 of 3GPP TS 23.214 [2].

It is optional for both the CP function and the UP function to support the L2TP feature.

L2TP is specified in IETF RFC 2661 [67]. An L2TP Tunnel is setup between a L2TP Access Concentrator (LAC) and a L2TP Network Server (LNS) pair controlling the connection, that may contain one or more L2TP Sessions. More than one L2TP tunnel can be established between a LAC-LNS pair.

The UP function shall act as the LAC.

The CP function may request the UPF to setup an L2TP Session for a PDN connection or PDU session between the LAC and the LNS in the Data Network.

One L2TP tunnel between the UP Function and the L2TP server may be shared by multiple PDN connection / PDU session using the same N6/SGi network instance and L2TP parameters (e.g. LNS address). A single L2TP tunnel may be shared by multiple PDN connections / PDU sessions created by the same CP Function or by different CP Functions.

## 5.31.2 L2TP Tunnel and L2TP Session Setup

When both the CP function and the UP function support the L2TP feature (see clause 8.2.25), if an L2TP session is required to support the PDN connection/PDU session, the CP function shall send a PFCP Session Establishment Request message including the following L2TP related IEs, to request the UP Function to setup an L2TP session towards the LNS:

- one L2TP Session Information IE to control the L2TP session setup. The L2TP Session Information may include:
  - the Called Number, Calling Number and the MRU (Maximum Receive Unit in LCP/PPP, to be set as the value of the MTU received from the UE or that may be configured in the CP function);
  - the L2TP Session Indications IE to indicate that the UP function shall request the LNS to allocate an IP address for the PDN session/PDN connection, to provide DNS server address(es) and/or NBNS server address(es) for the session;

- the L2TP User Authentication IE including parameters such as authentication type, Username and Password, Challenge and Challenge Response which may either be sent by the UE through PCO or be configured in the CP0.

- One or more L2TP Tunnel Information IEs to provide parameters to control the establishment of a L2TP tunnel if such information is available in the CP function, e.g. if it is received from an AAA/Radius server or locally configured in the CP function. This IE shall include LNS IPv4/IPv6 address, and it may include Tunnel Password for L2TP tunnel authentication, Tunnel Preference if multiple L2TP Tunnel Information IEs are sent, as specified in 3GPP TS 29.061 [39] and 3GPP TS 29.561 [49].

NOTE 1: Multiple L2TP Tunnel Information IEs can be sent to provide the UP Function with a list of possible L2TP tunnels that can be used to establish the L2TP session. This can be used to ensure that the session is established even if a specific LNS is temporarily unavailable, or to load balance the setup of L2TP sessions over different LNS's. A given L2TP Tunnel Information IE includes Tunnel attributes, e.g. Tunnel-Server-Endpoint and Tunnel-Password, received over N6/SGi with the same Tag value (see IETF RFC 2868 [68]). See also 3GPP TS 29.061 [39] and 3GPP TS 29.561 [49].

NOTE 2: If the UE IP address is to be allocated by the UP function (or the LNS), the CP function indicates this in the UE IP Address IE in the Create PDR or Create Traffic Endpoint IE, regardless of whether the UE IP address is to be assigned by the LNS or the UPF.

NOTE 3: If the L2TP tunnel parameters are configured in the UP Function, the UP Function determines how to establish the L2TP tunnel based on its local configuration.

NOTE 4: An L2TP session cannot be modified once established as specified in IETF RFC 2661 [67].

Upon receiving the PFCP Session Establishment Request from the CP function, the UP function shall determine whether to use an already established L2TP tunnel (if any appropriate one has already been established) or establish a new L2TP tunnel. The UP function may have already established L2TP tunnel(s), e.g. based on locally configured L2TP Tunnel Information. If an existing L2TP Tunnel is used, the UP function shall only setup a new L2TP session within the existing L2TP tunnel. Otherwise, the UP function shall perform both L2TP tunnel and L2TP session setup.

The UP function shall send a PFCP Session Establishment Response to the CP function, carrying the Created L2TP Session IE containing information about the established L2TP session, e.g. the used LNS Address, that may be used for statistics or diagnostics. The Cause IE in the response message may carry additional L2TP specific failure information to the CP function if the L2TP tunnel or L2TP session establishment failed.

The PFCP Session Establishment Response message may also include the DNS Server Address IE(s) and/or NBNS Server Address IE(s) containing the DNS server and/or NBNS Server information, if this information was requested.

If the UE IP address was allocated by the UP Function (or the LNS), the UP function shall provide the allocated IP address to the CP function in the UE IP Address IEs in the Created PDR IE and/or Created Traffic Endpoint IE (as specified in this specification).

Upon receiving uplink user plane traffic pertaining to the PFCP session with a L2TP session established, the UP function shall forward the traffic via the L2TP tunnel towards the LNS server.

### 5.31.3 L2TP Session and L2TP Tunnel Release

Upon receiving a PFCP Session Deletion Request message from the CP function, the UP function shall release the corresponding L2TP session. The UP function may release the L2TP tunnel if there is no other L2TP session using the L2TP tunnel.

NOTE 1: The UPF can alternatively retain the L2TP tunnel when all L2TP sessions are terminated.

When the LNS terminates a L2TP session or an L2TP tunnel, the following applies:

- If the LNS terminates an L2TP session, the UP function shall terminate the PFCP session and report to the CP Function that the PFCP session is deleted by sending a PFCP Session Report Request message to the CP function as described in clause 5.18.2, with the Cause indicating the reason for the termination.

- If the LNS terminates an L2TP tunnel, the UP function shall terminate all the PFCP sessions using the L2TP tunnel and report to all the CP functions controlling at least one such PFCP session that the respective PFCP

sessions have been deleted by sending a PFCP Session Report Request message to the CP function for each affected PFCP session, as described in clause 5.18.2, with the Cause indicating the reason for the termination.

- If the UP function detects that the connectivity with an LNS is lost, the UP function shall terminate the PFCP sessions using the L2TP tunnel(s) towards that LNS and report to the CP that all the PFCP sessions affected have been deleted by sending a PFCP Session Report Request message to the CP function for each affected PFCP session, as described in clause 5.18.2, with the Cause indicating the reason for the termination.

# 5.32 Support of Uplink packets buffering

## 5.32.1 General

This clause specifies the support of uplink packets buffering.

## 5.32.2 Uplink packets buffering for on-line charging

If the UP function indicated support of the Quota Action (QUOAC) feature in the UP Function Features IE and the FAR ID for Quota Action was set to buffer the application traffic at zero quota, the UP function shall buffer the related uplink packets if it is provisioned with zero quota earlier or the quota has been exhausted, as specified in clause 5.2.2.2.1. In addition, if the UP Function has indicated support of the feature UL/DL Buffering Control (UDBC), the UP function shall buffer the number of packets (including both uplink or downlink) based on the Suggested Buffering Packet Count IE in a BAR provided by the SMF, until it receives new instructions from the CP function, e.g. when the new Quota is granted.

## 5.32.3 Uplink packets buffering during EAS relocation

If the UP function supports uplink packets buffering during EAS relocation, the UP function shall set the UPBER bit in the UP Function Features (see clause 8.2.25).

The SMF shall request the UPF (PSA) to buffer the uplink packets related to one or more Service Data Flows sent to the new EAS by setting the BUFF flag in Apply Action IE of the related FAR. The SMF shall set the FORW flag in Apply Action IE when the EAS relocation has been performed.

# 5.33 Support of enhancement of Edge Computing (for 5GC)

## 5.33.1 General

Stage 2 requirements for support of enhancement of Edge Computing are specified in 3GPP TS 23.548 [69].

## 5.33.2 Uplink packet buffering for low packet loss during EAS relocation

Support of uplink packets buffering for low packet loss during EAS relocation as specified in clause 6.3.5 of 3GPP TS 23.548 [69] is defined in clause 5.32.3.

## 5.33.3 Edge Relocation using EAS IP address and Port number Replacement

To support Edge Relocation using EAS IP address and Port number replacement as specified in clause 6.3.3 of 3GPP TS 23.548 [69], the SMF shall instruct the UPF to replace:

- for the UL traffic, the destination IP address and/or port number of the outgoing IP packet with the Target EAS IP address and/or port number, by provisioning an UL FAR with an IP Address and Port Number Replacement IE containing the Target EAS IP address and/or port number; and

- for the DL traffic, the source IP address and/or port number of the incoming packet with the Source EAS IP address and/or port number, by provisioning a DL FAR with an IP Address and Port Number Replacement IE containing the Source EAS IP address and/or port number.

A UPF that supports replacing the source and destination IP address and Port Number of an (inner) IP packet shall set the IPREP flag in the UP Function Features IE (see clause 8.2.25) and shall replace the source or destination IP address and/or Port Number of an (inner) IP packet as instructed by the SMF.

### 5.33.4 EAS Discovery procedure with Local DNS Server/Resolver

Clause 6.2.3.2.3 of 3GPP TS 23.548 [69] specifies two options (C and D) for scenarios where the DNS message is to be handled by a Local DNS server/resolver.

In Option C, the SMF shall provision UL PDR(s) on the UL CL (including e.g. the Local DNS server address) or the BP (e.g. with the source IP prefix set to the IP prefix address assigned by the Local PSA) and associated FAR(s) to route traffic destined to the L-DN including the DNS query messages to the L-PSA, as specified in clause 5.17.2.

In Option D, if the SMF has been configured that DNS Queries for an FQDN (range) query can be locally routed on the UL CL, the SMF shall instruct:

- the UL CL to locally route DNS queries for the FQDN (range) to the Local DNS server, by provisioning an UL PDR with one or more DNS Query Filters or with a pre-defined PDR matching the requested DNS traffic and by associating a FAR to the UL PDR to forward the traffic towards the Local PSA. A UPF supporting this option shall indicate that it supports steering DNS traffic based on the target domain of the DNS Query by setting the DNSTS flag in the UP Function Features IE (see clause 8.2.25); and

- the Local PSA to send the DNS traffic to the Local DNS server, by provisioning a UL PDR with one or more DNS Query Filters, as described above for the UL CL, and by associating a FAR to the UL PDR to forward the traffic to the Local DNS server via tunneling (with the FAR including the Outer Header Creation IE) or via IP address replacement (with the FAR including the IP Address and Port number Replacement IE containing the IP address and/or port of the Local DNS server).

### 5.33.5 Direct Reporting of QoS monitoring events to Local NEF or AF

A UPF may be instructed to report QoS monitoring events directly to a local NEF or AF as specified in clause 6.4 of 3GPP TS 23.548 [69].

A UPF that supports this feature shall set the DRQOS (Direct Reporting of QoS monitoring events) flag in the UP Function Feature IE (see clause 8.2.25).

An SMF shall instruct an UPF that supports the DRQOS feature to report Per QoS Flow Per UE QoS Monitoring events directly to a local NEF or AF by applying the requirements specified in clauses 5.24.4 or 5.24.5.3, and by additionally including a Direct Reporting Information IE in the SRR as specified in clause 5.2.8.2.

The Direct Reporting Information shall include the Event Notification URI towards which events shall be sent, and if available, the Notification Correlation ID to be included in these events. If the events need to be sent both directly to the local NEF or AF and to the SMF, the Direct Reporting Information IE shall also include the Reporting Flags IE with the DUPL flag set to "1".

An UPF that supports this feature shall send the Per QoS Flow Per UE QoS Monitoring events to the SMF if the SRR does not contain the Direct Reporting Information IE, or directy to the Local NEF or AF using the notification URI received in the Direct Reporting Information IE, or both if the Direct Reporting Information IE is provided with the DUPL flag set to "1", as specified in clause 5.24.4.3.

The UPF shall report QoS monitoring events directly to the Local NEF or AF using the UPF Event Exposure service specified in 3GPP TS 29.564 [73].

## 5.34 Support of 5G Multicast and Broadcast Service

### 5.34.1 General

This clause specifies N4mb and N4 specific requirements to support 5G Multicast and Broadcast Service.

Stage 2 requirements for the support of 5G Multicast and Broadcast Service is specified in clause 6.7 of 3GPP TS 23.247 [72] and clause 5.8.2.11 of 3GPP TS 23.501 [28].

## 5.34.2 N4mb requirements

### 5.34.2.1 General

This clause specifies N4mb specific requirements to support 5G Multicast and Broadcast Service.For a location dependent MBS service (see clause 6.2.3 of 3GPP TS 23.247 [72]), the MB-SMF shall establish one PFCP session per MBS session and MBS Session Area, following the requirements specified in clause 5.34.2.2.

NOTE: A Location dependent MBS service enables distribution of different content data to different MBS service areas. The same MBS Session ID is used but a different Area Session ID is used for each MBS service area.

### 5.34.2.2 Instructing the MB-UPF to forward MBS data using multicast and/or unicast transport

When the MB-SMF receives an MBS Session Create Request from a NEF/MBSF to configure an MBS session, the MB-SMF shall select an MB-UPF and request that MB-UPF to allocate relevant user plane resource for the MBS session, or for the MBS session and MBS Service Area for a location dependent MBS service; to do so, the MB-SMF shall send a PFCP Session Establishment Request message to the MB-UPF to setup a PFCP session for the MBS Session, or for the MBS session and MBS Service Area for a location dependent MBS service, including the following information in the PFCP Session Establishment Request message:

- the MBS Session Identifier identifying the MBS session (i.e. TMGI or SSM address);
- the Area Session ID, for a location dependent MBS service;
- a JMBSSM (Join MBS Session SSM) indication in the MBSN4mbReq-Flags IE to request the MB-UPF to join the multicast tree towards the Source Specific Multicast (SSM) address information provided by AF/AS or MBSTF for the MBS Session where the SSM is provided in the IP Multicast Addressing Info IE in the corresponding downlink PDR, if multicast transport applies over N6mb (i.e. if no N6mb ingress tunnel is requested to be allocated);
- a PLLSSM (Provide Low Layer Source Specific Multicast address) indication in the MBSN4mbReq-Flags IE to request the MB-UPF to provide a lower layer SSM address (i.e. multicast destination address and related source IP address) and a GTP-U Common Tunnel EndPoint Identifier (C-TEID), if multicast transport applies over N3mb or N19mb. During a restoration procedure for an MB-UPF restart however the MB-SMF shall not set the PLLSSM flag (see clause 8.2.2 in 3GPP TS 23.527 [40]);
- for each MBS QoS flow:
  - a Create PDR IE to provision a downlink PDR with PDI or a Create Tunnel Endpoint IE containing either:
    - a "Local Ingress Tunnel" IE with the CHOOSE bit set to "1" to request the MB-UPF to allocate an ingress tunnel for Nmb9, or for N6mb if unicast transport is used over N6mb (MB-UPF shall assign a single ingress tunnel address, regardless of the number of MBS QoS flows); or
    - an IP Multicast Addressing Info IE to request the MB-UPF to retrieve the MBS session data from the IP Multicast Address, when using multicast transport over N6mb.
  - a Create QER IE to provision a QER (associated with the PDR including the above PDI or Traffic EndPoint ID) instructing the MB-UPF to insert the QFI of the MBS QoS flow in user plane packets and possibly requesting the MB-UPF to apply specific QoS treatments; the IQFISN (Insert DL MBS QFI Sequence Number) flag in the Create QER IE shall be set to "1" to request the MB-UPF to insert the DL MBS QFI Sequence Number in the PDU session container in user plane packets;
  - a Create FAR IE to provision a FAR (associated with the PDR including the above PDI or Traffic EndPoint ID) with the Apply Action set to "FSSM" with an MBS Multicast Parameters IE, when multicast transport is used over N3mb or N19mb, to forward the packets to the low layer SSM address when it is allocated; otherwise, the apply action shall be set to "DROP".

The MBS Session Identifier, Area Session ID (for a location dependent MBS service) and the MBSN4mbReq-Flags are included in the group IE "MBS Session N4mb Control Information" at the PFCP message level.

The MB-UPF shall return the allocated ingress tunnel information in the Created PDR IE or Created Traffic Endpoint IE and provide the Low Layer SSM address if requested.

For an MBS session using unicast transport over N3mb or N19mb, when one or more NG-RAN node(s) and/or PSA UPF(s) provides a downlink GTP-U F-TEID (i.e. IP address and tunnel endpoint identifier) to receive the MBS session data, the MB-SMF shall send a PFCP Session Modification Request or a PFCP Session Establishment Request message to change the FAR with the Apply Action set to "MBSU" together with one or more Add MBS Unicast Parameters to instruct the MB-UPF to forward and replicate MBS Session data towards the one or more GTP-U DL tunnels terminating at the NG-RAN(s) and/or PSA UPF(s).

NOTE: FAR with the Apply Action set to "MBSU" together with one or more Add MBS Unicast Parameters is sent with a PFCP Session Establishment Request message during the restoration procedures, as specified in 3GPP TS 23.527 [40], see e.g. clauses 8.2.2 and 8.2.3.

For an MBS session using multicast transport over N3mb or N19mb, if the "FSSM" flag is set in the Apply Action, the MB-UPF shall forward the MBS session data using the Low Layer Source Specific Multicast address (i.e. destination IP multicast address and related source IP address) and C-TEID it allocated to the MBS session.

Both the "FSSM" and "MBSU" flags shall be set in the Apply Action IE if the MB-UPF is requested to forward MBS data using both multicast and unicast transport over N3mb or N19mb.

### 5.34.2.3 Detecting and reporting user plane (in)activity of an MBS session

As specified in clauses 7.2.5.2 and 7.2.5.3 of 3GPP TS 23.247 [72], the MB-SMF may instruct the MB-UPF to detect and report when user plane inactivity or activity is detected for an MBS session, in order to deactive or activate the MBS session (see also clause 5.34.2.4).

User plane inactivity detection and reporting for an MBS session shall be supported as specified in clause 5.11.

User plane activity detection and reporting for an MBS session shall be supported as specified in clauses 5.2.3.1, i.e. by setting the NOCP flag in the Apply Action IE of the FAR and by the MB-UPF sending a PFCP Session Report Request including a Downlink Data Report IE identifying the PDR(s) for which downlink packets have been received.

### 5.34.2.4 Activation and Deactivation of a Multicast MBS session

Activation and Deactivation of a Multicast MBS session is specified in clauses 7.2.5.2 and 7.2.5.3 of 3GPP TS 23.247 [72].At deactivation of a Multicast MBS Session, e.g. triggered by receiving an user plane inactivity report from the MB-UPF, or by receiving an MBS session deactivation request from the AF, the MB-SMF shall send a PFCP Session Modification Request message to request the MB-UPF:

- to stop forwarding the MBS session data and:
  - to report the receipt of subsequent DL MBS session data, by setting the Apply Action IE from "FSSM and/or MBSU" to "BUFF and NOCP" in the FAR of the PFCP session corresponding to the MBS session, if the activation of the MBS session is to be triggered upon receiving DL data report from the MB-UPF; or
  - to change the Apply Action IE from "FSSM and/or MBSU" to "DROP" or "BUFF" in the FAR of the PFCP session corresponding to the MBS session, if the deactivation is requested by the AF;
- optionally, to delete all unicast DL N3mb F-TEIDs and all unicast DL N19mb F-TEIDs, i.e. to delete all the information earlier received in all the Add MBS Unicast Parameters IEs, by setting the "DETEID" flag to "1" in the PFCPSMReq-Flags, if the MB-SMF stores N3mb F-TEIDs and N19mb F-TEIDs and does not want to keep these F-TEIDs in the MB-UPF when the MBS session is deactivated. Otherwise, MB-UPF will keep all unicast DL N3mb F-TEIDs and all unicast DL N19mb F-TEIDs when the MBS session is deactivated.

At the (re)activation of a Multicast MBS Session, e.g. triggered by receiving the DL data report from the MB-UPF, or by receiving an MBS session activation request from the AF, the MB-SMF shall send a PFCP Session Modification Request message:

- requesting the MB-UPF to forward the MBS session data towards NG-RANs and/or UPFs, by setting the Apply Action IE from "BUFF" (with or without NOCP") or "DROP" to "FSSM and/or MBSU" in the FAR of the PFCP session;

- provisioning all unicast NG-RAN DL N3mb F-TEIDs and UPF N19mb F-TEID (which are stored and were possibly updated in the MB-SMF) in the Add MBS Unicast Parameters IEs to request the MB-UPF to forward one copy of the MBS session data to these DL tunnels when the unicast transport is used, if all the DL N3mb and N19mb F-TEIDs were deleted during the MBS session deactivation procedure; and

- optionally including a User Plane Inactivity Timer IE to provision or update the user plane inactivity timer to request the MB-UPF to report user plane inactivity, if the deactivation of the MBS session is to be triggered upon user plane inactivity report from the MB-UPF.

## 5.34.3 N4 requirements

### 5.34.3.1 General

This clause specifies the N4 requirements for the support of multicast MBS services using 5GC Individual MBS traffic delivery. The MBS data may be delivered from the MB-UPF to the UPF using multicast or unicast transport. It is optional for both the SMF and the UPF to support the multicast MBS service. The following requirements shall apply if the SMF and UPF support the MBSN4 feature (see clause 8.2.25).

NOTE 1: There is no impact on N4 to support broadcast MBS services in the 5GS.

NOTE 2: For an MBS session (or an MBS session towards an MBS service area for location dependent MBS), there is only one MB-SMF (set) and one MB-UPF.

For a given multicast MBS session, or for a given multicast MBS session and MBS Service Area for a location dependent MBS service, only a single copy of MBS Session data is delivered from the MB-UPF to the UPF. The UPF shall allocate only one N19mb downlink tunnel to receive the MBS session data for the MBS session, or for the MBS session and MBS Service Area for a location dependent MBS service, if unicast transport applies over N19mb or the UPF shall join the multicast group to receive MBS session data if multicast transport applies over N19mb.

### 5.34.3.2 Instructing the UPF to forward (or stop forwarding) multicast MBS data to associated PDU sessions

When a PDU session needs to be associated with an MBS session (e.g. when a UE requests to join a multicast MBS session, 5GC Individual MBS traffic delivery is used and the request is accepted by the SMF), the SMF shall associate the PDU session with the multicast MBS session by sending a PFCP Session Establishment or Modification Request message to the UPF, for the PFCP session corresponding to the PDU session, with the following information:

- the MBS Session N4 Control Information IE including the MBS Session Identifier, the Area Session ID, for a location dependent MBS service and, if IP multicast transport applies over N19mb (i.e. a multicast transport address has been received from the MB-SMF):

  - the Multicast Transport Information IE for the given MBS session containing the Low Layer Source Specific Multicast address, i.e. the Multicast address and the source IP address and the GTP-U Common TEID which have been allocated by the MB-UPF for the MBS session, when the SMF considers it is the first PDU session to be associated with the MBS session (or with the MBS session and Area Session ID for a location dependent MBS service) in this UPF; the SMF may provide this information even if there are already other PDU sessions associated with the MBS session (or with the MBS session and Area Session ID for a location dependent MBS service) in this UPF;

- one or more new DL PDR(s) including:

  - the MBS Session Identifier, the Area Session ID (for a location dependent MBS service), or a Traffic Endpoint IE which is including the MBS Session Identifier, and the Area Session ID (for a location dependent MBS service); this information shall be used by the UPF to:

    - determine whether the UPF already receives the MBS session data, or if instead it needs to allocate a new N19mb DL tunnel (when using IP unicast transport over N19mb) or send an IGMP JOIN request to join the multicast tree (when using IP multicast transport over N19mb) to receive the MBS session data; the UPF shall allocate the same N19mb DL Tunnel ID when the SMF requests the UPF to allocate a DL F-TEID for N19mb and multiple UE/PDU sessions are already associated with the MBS session (or with the MBS session and Area Session ID for a location dependent MBS service) in the UPF (e.g. PDU

sessions controlled by other SMFs, or when multiple PDU sessions served by the same SMF need to be associated concurrently with the MBS session).

- identify the list of PDU sessions (served by the UPF) towards which any DL packet received for this MBS session shall be distributed;

- if unicast transport is used over N19mb:

  - a local F-TEID to be allocated at the UPF, with the CHOOSE flag set to "1" in the "Local F-TEID" IE in the PDI IE or Create Traffic Endpoint IE, if the SMF has no "N19mb DL F-TEID" information available for the MBS Session, e.g. for the first PDU Session in the SMF to be associated with the MBS session (or with the MBS session and Area Session ID for a location dependent MBS service); otherwise

  - the Local F-TEID set to the "N19mb DL F-TEID" for the MBS Session (or for the MBS session and Area Session ID for a location dependent MBS service) which is known by the SMF.

- multiple DL PDRs may be provisioned and associated with different QERs to apply different QoS treaments for different multicast QoS flows within the MBS session. For each multicast QoS flow, the SMF may instruct the UPF to modify the QFI of downlink packets of the multicast QoS flow (received from the MB-UPF) to the QFI assigned by the SMF for the Associated (unicast) QoS flow, by associating a DL PDR including the QFI of the multicast QoS flow with a QER including the QFI IE set to the QFI of the Associated QoS flow.

- the new DL PDR(s) may be associated with an (existing) Forwarding Action Rule to forward the received MBS session data to the UE via existing downlink N3/N9 tunnel, or with a new Forwarding Action Rule with the Apply Action set to "Drop" if the SMF wishes to maintain the MBS data reception over N19mb but suspends the delivery of the data to the UE's PDU session, e.g. when the UE is switching between 5GC Individual MBS traffic delivery and 5GC Shared MBS traffic delivery due to the UE moving back and forth between MBS non-supporting NG-RAN and MBS supporting NG-RAN.

The UPF shall respond with a PFCP Session Establishment or Modification Response message to the SMF, and the UPF shall include an MBS Session N4 Information IE if any of the following information needs to be reported:

- the allocated "N19mb DL Tunnel ID" if it was requested;

- an NN19DT (New N19mb Downlink Tunnel) indication in the MBSN4Resp-Flags IE indicating if the N19mb DL F-TEID has been newly allocated by the UPF or if a N19mb DL F-TEID had already been allocated by the UPF for the MBS session (or for the MBS session and Area Session ID for a location dependent MBS service), when the "N19mb DL Tunnel ID" is present; this information allows the SMF to determine if it needs to report this N19mb DL Tunnel ID to the MB-SMF;

- an indication "JMTI"(Joined N19mb Multicast Tree Indication) in the MBSN4Resp-Flags IE indicating if the UPF has joined the multicast tree from MB-UPF, if the Multicast Transport Information was included in the request message.

NOTE: The indications "JMTI" and "NN19DT" are defined to help the SMF to determine if it needs to communicate with the MB-SMF, e.g., to report the newly allocated N19mb DL TEID in order to let the MB-SMF inform the MB-UPF to send a copy of MBS Session data to the UPF. The indication "JMTI" indicates to the SMF that no N19mb DL TEID needs to be allocated.

If unicast transport is used over N19mb and if the NN19DT (New N19mb Downlink Tunnel) indication is not set in the MBSN4Resp-Flags IE within the PFCP Session Establishment or Modification Response (i.e. if the MBSN4Resp-Flags IE is present and the NN19DT indication is not set, or if the MBSN4Resp-Flags IE is absent), the SMF shall assume that the UPF had already allocated the N19mb DL TEID earlier than the PFCP Session Establishment or Modification Request.

When a PDU Session should be no longer be associated with the MBS session, or with the MBS session and Area Session ID for a location dependent MBS service, (e.g. the PDU session leaves the MBS session, or when switching to 5GC Shared MBS traffic delivery), or when the MBS session to which the PDU session is associated is being deactivated, the SMF shall send a PFCP Session Modification Request message to remove the DL PDR(s) that were created to receive the MBS session data, unless the SMF decides to keep the UPF receiving MBS Session data from N19mb, in which case the PDR shall be associated with a FAR set to drop packets. In the former case, when all the DL PDR(s) that were created to receive the MBS session data have been removed, the UPF shall consider that the PFCP

session (PDU session) is no longer associated with the MBS session (i.e. the UPF shall delete, from its PFCP session context, the MBS Session N4 Control Information corresponding to the MBS session).

In the PFCP Session Modification Response message, the UPF shall include the indication "N19DTR" (N19mb Downlink Tunnel Removal) in the MBSN4Resp-Flags IE indicating the N19mb DL Tunnel is to be removed if the UPF was requested to remove the DL PDRs of the MBS session for the PFCP session and this was the last PFCP session associated with the N19mb DL Tunnel in the UPF. This tells the SMF that it shall request the MB-SMF to inform the MB-UPF to stop sending MBS Session data towards this N19mb DL Tunnel.

The UPF shall also set the indication "N19DTR" (N19mb Downlink Tunnel Removal) in the MBSN4Resp-Flags IE indicating the N19mb DL Tunnel is to be removed in the PFCP Session Deletion Response message when the SMF deleted the last PFCP session who was associated with the N19mb DL Tunnel in the UPF.

When the MBS session to which the PDU session is associated is being re-activated, the SMF shall send a PFCP Session Modification Request message to the UPF:

- including the MBS Session N4 Control Information IE and re-creating the DL PDR(s) of the MBS QoS flows, following the same requirements as described above for associating the PDU session with the MBS session, if the SMF removed the DL PDR(s) that were created to receive the MBS session data when the MBS session was deactivated; or

- associating the DL PDR(s) of the MBS QoS flows with the FAR provisioned with the N3 DL F-TEID to forward packets, if the SMF decided to keep the UPF receiving MBS Session data from N19mb by associating these DL PDR(s) with a FAR set to drop packets when the MBS session was deactivated.

During a restoration procedure for an MB-UPF failure without Restart (see clause 8.2.3 of 3GPP TS 23.527 []), if multicast transport is used over N19mb:

- the SMF shall instruct the UPF to use the new Low Layer Source Specific Multicast address, i.e. the Multicast address and the source IP address and the GTP-U Common TEID which have been allocated by the new MB-UPF for the MBS session, by sending a PFCP Session Modification Request message with the MBS Session N4 Control Information IE including the MBS Session Identifier, the Area Session ID (for a location dependent MBS service) and the Multicast Transport Information IE containing the new LL SSM address and GTP-U Common TEID;

- upon receipt of such a request, the UPF shall send an IGMP JOIN request to join the multicast tree to receive the MBS session data from the new MB-UPF and it shall leave delivery from the previous multicast address that was in use for the MBS session. The UPF shall set the indication "JMTI"(Joined N19mb Multicast Tree Indication) in the MBSN4Resp-Flags IE in the PFCP Session Modification Response to indicate that the UPF has joined the multicast tree from MB-UPF.

When receiving the MBS session data for a given MBS session, or for a given MBS session and Area Session ID for a location dependent MBS service, either from the N19mb DL Tunnel allocated for this MBS Session (where the packets shall be identified by N19mb DL TEID) when unicast transport is used, or from the low layer Multicast transport address (where the packets shall be identified by the low layer Multicast transport address) when multicast transport is used, the UPF shall replicate the MBS Session data to all PFCP sessions which are associated with the MBS Session, or with the MBS session and Area Session ID for a location dependent MBS service.

The UPF shall forward the MBS DL QFI Sequence Number in the PDU Session Container (see 3GPP TS 38.415 [34]) of MBS data packets received from the MB-UPF unmodified.

#### 5.34.3.3 Instructing a combined UPF/MBS-UPF to forward multicast MBS data to associated PDU sessions

The procedures and requirements to instruct a combined UPF/MB-UPF to associate a PDU session with an MBS session (or with the MBS session and Area Session ID for a location dependent MBS service) for which it serves as the MB-UPF shall be as specified in clauses 5.34.2.2 and 5.34.3.2, with the following additions:

- the combined UPF/MB-UPF may determine that the PDU session is being associated with an MBS session (or with an MBS session and Area Session ID for a location dependent MBS service) for which it serves as MB-UPF by determining whether a specific PFCP session has been established for the MBS session (or with the MBS session and Area Session ID for a location dependent MBS service), as specified in clause 5.34.2.2;

- the SMF shall instruct the combined UPF/MB-UPF to associate the PDU session with the MBS session (or with the MBS session and Area Session ID for a location dependent MBS service) as specified in clause 5.34.3.2, as if the UPF and MB-UPF were not combined; this means in particular that the DL PDR of the PFCP session of the PDU session to be associated with the MBS session (or with the MBS session and Area Session ID for a location dependent MBS service) shall not contain an N6mb / Nmb9 address or IP multicast addressing information;

NOTE 1: Only the PFCP session created for the MBS session (or for the MBS session and Area Session ID for a location dependent MBS service) as specified in clause 5.34.2.2 can contain a N6mb / Nmb9 address or IP multicast addressing information.

- it is an implementation choice for such combined UPF/MB-UPF to allocate a (possibly virtual / internal) N19mb DL Tunnel ID (i.e. IP address and TEID) or to indicate to the SMF that it has joined the low layer multicast group assigned by the MB-UPF for the MBS session (or for the MBS session and Area Session ID for a location dependent MBS service), and the combined UPF/MB-UPF shall respond to the SMF accordingly, as if it is the UPF and MB-UPF were not combined;

- if the combined UPF/MB-UPF returns a N19mb DL Tunnel ID with the NN19DT (New N19mb Downlink Tunnel) indication set to 1, the SMF shall request the MB-SMF to (or the combined SMF/MB-SMF shall) instruct the MB-UPF to forward and replicate MBS Session data towards the (possibly virtual / internal) N19mb DL Tunnel ID as specified in clause 5.34.2.2, as if the UPF and MB-UPF were not combined.

NOTE 2: The SMF, MB-SMF or a combined SMF/MB-SMF need not implement any additional logic when communicating with a combined UPF/MB-UPF.

# 5.35 Support of Per Slice UP Resource Allocation and Usage Reporting by the UP Function

## 5.35.1 General

A UP Function may serve PDU sessions belonging to different network slices (i.e. S-NSSAIs).

UP resources allocation per network slice may be achieved by:

a) the UP function allocating UP resources based on the Network Instance IE (and other N4 information such as PDU session type, IP Address Pool ID, ATSSS Control Information), with distinct Network Instance values being configured in the CP function and UP Function for different network slices; or

NOTE 1: The above behavior does not require support of any specific PFCP protocol extension and can be supported by UP function implementations complying with earlier releases of the specification.

b) the UP function allocating UP resources based on the Network Instance IE and S-NSSAI IE (and other N4 information such as PDU session type, IP Address Pool ID, ATSSS Control Information), if the feature "Per Slice UP Resource Management" is supported by the UP function and if the UP function is configured to do so by operator policy.

A UP function that supports allocating UP resources based on the Network Instance IE and S-NSSAI IE (and other N4 information) and that is configured to do so by operator policy, shall:

- indicate support of the feature "Per Slice UP Resource Management" in the UP Function Features IE during the PFCP association setup procedure; and

- allocate resources in the UP function using the Network Instance and, if available, the S-NSSAI.

A UP function that does not support allocating UP resources based on the Network Instance IE and S-NSSAI IE or that is not configured to do so by operator policy shall allocate UP resources based on the Network Instance IE (and other N4 information).

If the UP function supports the UE IP Address Usage Reporting feature (see clause 5.21.3.2), the UP function shall report the UP IP address usage as specified in clause 5.21.3.2, by reporting the UE IP address usage:

a) per Network Instance, if the UP function does not support allocating UP resources based on the Network Instance IE and S-NSSAI IE or it is is not configured to do so by operator policy; or

NOTE 2: This allows to report UE IP address usage per network slice when using a distinct Network Instance value per network slice.

b) per Network Instance and S-NSSAI, if the UP function supports allocating UP resources based on the Network Instance IE and S-NSSAI IE and is configured to do so by operator policy. In this case, the UP Function shall report the UE IP address usage information associated with a specific S-NSSAI, as specified in clause 5.21.3.

NOTE 3: If the UP function indicates that it supports the "Per Slice UP Resource Management" feature and if this feature is also supported by the CP function, the CP function can instruct the UP function to allocate UP resource taking into account the network slice by including the Network Instance IE and S-NSSAI IE in the PFCP session establishment procedure. Otherwise, a separate Network Instance needs to be configured for each S-NSSAI if support of multiple slices is needed.

# 5.36 Paging Policy Indicator Provisioning

## 5.36.1 General

Stage 2 requirements for Paging Policy Differentiation are specified in clause 5.4.3.2 of 3GPP TS 23.501 [28].

For a UE in RRC Inactive state the NG-RAN can be required to enforce specific paging policies in the case of NG-RAN paging, based on 5QI, ARP and PPI associated with an incoming DL PDU. To support this, the SMF shall instruct the UPF to detect the DSCP in the TOS (IPv4) / TC (IPv6) value in the IP header of the DL PDU and insert the corresponding PPI as described below. When Paging Policy Differentiation is enabled in the network and a PPI needs to be inserted into DL PDU, the SMF shall:

- provision a PDR for each PPI containing one or more DSCP code(s) to be matched against the DSCP in the TOS (IPv4) / TC (IPv6) value in the IP header of the DL PDUs, where these DSCP code(s) are to be mapped to the same PPI, in the PDI together with or without the service data flow detection information;

NOTE 1: When service data flow level packet detection is not required, e.g. for an I/V-UPF, the PDR can be provisioned with one or more DSCP(s) to be matched in the PDI without any service data flow detection information.

NOTE 2: When service data flow level packet detection is required, several PDRs with the same service data flow detection information but with different (set of) DSCP(s) (which are mapped to different PPI) need to be provisioned.

- associate the PDR with a QER with the Paging Policy Indicator set to the mapped PPI to instruct UPF to insert the corresponding PPI into the GTP-U PDU Session Container extension header of outgoing packets.

## 5.36.2 Enhanced Paging Policy Indicator Provisioning

To reduce the number of PDRs/QERs to be provisioned (in order to support NG-RAN paging using Paging Policy Indicator (PPI)), the SMF and the UPF may support the Enhanced Provisioning Paging Policy Indicator (EPPPI) feature as specified below.

During a PFCP session establishment/modification procedure, if both the SMF and the UPF support the EPPPI feature, the SMF may include a DSCP to PPI Control Information in the PFCP Session Establishment/Modification Request message to instruct the UPF to insert a PPI in the GTP-U PDU Session Container extension header of downlink GTP-U packets encapsulating payload packets (to be sent to the UE). When the DSCP to PPI Control Information IE is present, the SMF may:

- include one or more DSCP to PPI Mapping Information to instruct the UPF to insert the corresponding PPI for downlink GTP-U packets, where the DSCP of its payload packet is matching one of DSCP codes in the DSCP to PPI Mapping Information;

- include one or more QFIs to instruct UPF to insert PPI only for the downlink packets received on the requested QFI(s);

# 6 Procedures

## 6.1 Introduction

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

## 6.2 PFCP Node Related Procedures

### 6.2.1 General

The following clauses specify either node level or PFCP entity level procedures over the Sxa, Sxb, Sxc and N4 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

PFCP Heartbeat is a PFCP entity level procedure.

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] for EPC, and in clause 4 of 3GPP TS 23.527 [40] for 5GC.

#### 6.2.2.2 Heartbeat Request

An PFCP entity of a CP or UP function may send a Heartbeat Request to a PFCP entity of a peer node to find out if the peer PFCP entity is alive. If multiple PFCP entities pertain to the same CP or UP function, each PFCP entity may send Heartbeat Request messages towards each PFCP entity pertaining to the peer node with which a PFCP control association is established.

NOTE 1: If the UP function supports the MPAS feature and connected to an SMF set, each PFCP entity of the UP function can send heartbeat Requests towards each PFCP entity of every SMF with which a PFCP control association is established.

NOTE 2: If the UP function supports the SSET feature and connected to an SMF set, each PFCP entity of the UP function can send heartbeat Requests towards each PFCP entity pertaining to the same SMF or the SMFs in the SMF set with which a PFCP control association is established.

A CP function or UP function shall be prepared to receive a Heartbeat Request at any time (even from unknown peers) and it shall reply with a 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 a node level procedure.

Load Control is an optional feature defined over the Sxa, Sxb, Sxc and N4 reference points.

Load control enables the UP function to send its load information to the CP function to adaptively balance the PFCP 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 PFCP 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 clause 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 clause 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 a node level procedure.

Overload Control is an optional feature defined over the Sxa, Sxb, Sxc and N4 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 clause 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 clause 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 PFCP 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 clause 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 occurring, 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 clause 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 PFCP 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 clause 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 clause 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 clause 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 PFCP PFD Management Procedure

### 6.2.5.1 General

PFCP PFD Management is a node level procedure.

The PFCP PFD Management procedure may be used by the CP function and UP function to provision PFDs (e.g. received from the PFDF as specified in clauses 5.11.4 and 6.5.2 of 3GPP TS 23.214 [2]) to the UP function, for one or more Application Identifiers.

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 clause 8.2.25).

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

NOTE: Application identifiers preconfigured in the UP function, if any, need to be distinct from application identifiers provisioned via PFD management procedure.

### 6.2.5.2 CP Function Behaviour

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

The CP function:

- shall send the PFCP 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 a PFCP 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 a PFCP 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) provisioned via the PFD Management Procedure;
- 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 a PFCP PFD Management Response with the cause "success", if the above operations were performed successfully;
- if a PFD is removed/modified and this PFD was used to detect application traffic related to an application identifier in a PDR created/activated for a PFCP session and the UP function has reported the application start to the CP function for the application or the application instance corresponding to this PFD as defined in clause 5.4.11 ((Un)solicited Application Reporting), the UP function shall report the application stop to the CP function for the corresponding application or the corresponding application instance identifier as defined in clause 5.4.11 if the removed/modified PFD in UP results in the stop of the application or the application instance is not being able to be detected. See clause 5.11.4 of 3GPP TS 23.214 [2].

NOTE: Multiple PFDs can be associated with the application identifier. When the removed/modified PFD is the last one which is used to detect traffic identified by application id, the UPF reports application stop.

## 6.2.6 PFCP Association Setup Procedure

### 6.2.6.1 General

PFCP Association Setup is a node level procedure.

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

The setup of a PFCP association may be initiated by the CP function (see clause 6.2.6.2) or the UP function (see clause 6.2.6.3).

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

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

#### 6.2.6.2.1 CP Function Behaviour

The CP function shall initiate the PFCP Association Setup procedure to request to setup a PFCP association towards a UP function prior to establishing a first PFCP session on this UP function.

The CP function shall retrieve an IP address of the UP function to send the PFCP Association Setup Request, as specified in clause 5.8.1, and shall send a PFCP Association Setup Request to the UP function with:

- the Node ID of the CP function;
- the list of optional features the CP function supports which may affect the UP function behaviour, if any;
- optionally, the PFCP Session Retention Information IE (see figure 7.4.4.1-2) to request the UP function to retain all or part of the existing PFCP sessions if a PFCP association already exists in the UP function for the same Node ID.

The CP function shall only initiate PFCP Session related signalling procedures toward a UP function after it receives the PFCP 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 a PFCP 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 PFCP association;
  - shall send a PFCP Association Setup Response including:

- a successful cause;
- its Node ID;
- information of all supported optional features in the UP function;
- optionally one or more UE IP address Pool Information IE which contains a list of UE IP Address Pool Identities per Network Instance, S-NSSAI and IP version;
- optionally the NF Instance ID of the UPF if available.

  - shall send a PFCP 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 a PFCP Association Setup Response with an appropriate error cause if the request is rejected.

If the PFCP Association Setup Request contains a Node ID for which a PFCP association was already established, the UP function shall:

- proceed with establishing the new PFCP association (regardless of the Recovery Timestamp received in the request), overwriting the existing association;
- retain the PFCP sessions that were established with the existing PFCP association and that are requested to be retained, if the PFCP Session Retention Information IE was received in the request; otherwise, delete the PFCP sessions that were established with the existing PFCP association;
- set the PSREI (PFCP Session Retained Indication) flag to "1" in the PFCP Association Setup Response, if the PFCP Session Retention Information IE was received in the Request and the requested PFCP sessions have been retained.

If the UPF is configured to be used for IPUPS, the UPF shall set the UUPSI (UPF configured for IPUPS Indication) flag to "1" in the PFCP Association Setup Response message.

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

#### 6.2.6.3.1 UP Function Behaviour

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

The UP function:

- shall retrieve an IP address of the CP function, e.g. based on local configuration in the UP function;
- shall send the PFCP Association Setup Request including:
  - the Node ID of the UP function;
  - information of all supported optional features in the UP function;
  - optionally one or more UE IP address Pool Information IE which contains a list of UE IP Address Pool Identities per a given Network Instance, S-NSSAI and IP version;
  - optionally the NF Instance ID of the UPF if available.

- the UUPSI (UPF configured for IPUPS Indication) flag set to "1" if the UPF is configured to be used for IPUPS.

#### 6.2.6.3.2 CP Function Behaviour

When receiving a PFCP 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 PFCP association;
  - shall send a PFCP Association Setup Response with a successful cause, its Node ID, and information of the list of optional features the CP function supports which may affect the UP function behaviour, if any;
- shall send a PFCP 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 a PFCP Association Setup Response with an appropriate error cause if the request is rejected.

The CP function shall only initiate PFCP Session related signalling procedures toward a UP function after it has sent the PFCP 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 PFCP Association Update Procedure

### 6.2.7.1 General

PFCP Association Update is a node level procedure.

The PFCP Association Update procedure shall be used to modify an existing PFCP 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 PFCP Association Update Procedure Initiated by the CP Function

#### 6.2.7.2.1 CP Function Behaviour

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

When both the CP function and UP function support the EPFAR feature, the CP function may send a PFCP Association Update Request with the "PFCP Association Release Preparation Start" flag set to "1" when the CP function decides to release the PFCP association and request the UP function to report all non-zero usage reports for the PFCP session affected by the release of the PFCP association, as specified in clause 5.18.

#### 6.2.7.2.2 UP Function Behaviour

When receiving a PFCP Association Update Request, the UP function:

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

When both the CP function and UP function support the EPFAR feature, and the CP function has set the "PFCP Association Release Preparation" set to "1" in the PFCP Association Update Request message, the UP function shall

send the PFCP Association Update Response to CP function with successful cause value and then send PFCP Session Report Request messages to report non-zero usage reports (at least one message per PFCP Session) for the PFCP Sessions affected by the release of the PFCP association, as specified in clause 5.18.

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

#### 6.2.7.3.1 UP Function Behaviour

The UP function initiates the PFCP Association Update procedure to report changes to the PFCP association to the CP function, e.g. change of optional features, an indication to request to release the PFCP association, change of the UE IP Address Pool Identifies configured in the UP function.

The UP function may send a PFCP Association Update Request to request the CP function to perform the release of the PFCP association, optionally providing a Graceful Release Period.

When the Enhanced PFCP Association Release feature (EPFAR) (see clause 5.18) is supported by both the CP function and UP function, the UP function:

- may send a PFCP Association Update Request with the flag "PFCP Association Release Preparation" set to "1" when the UP function decides to release the PFCP association and thus inform the CP function that all non-zero usage reports for those PFCP session affected by the release of the PFCP association will be reported;
- shall then send a PFCP Association Update Request, with the URSS flag set to "1" once all non-zero usage reports for all the PFCP Sessions affected by the release of PFCP Association have been sent to the CP function.

After reception of the PFCP Association Update Response, the UP function shall consider that the PFCP association is still setup until receiving a PFCP Association Release Request. When the UP function requests to release the PFCP Association and sends a PFCP Association Update Request message with a Graceful Release Period or with the URSS flag set, if no PFCP Association Release Request is received before the Graceful Release Period or a configurable timer (when the URSS flag is set) expires, the UP function may locally release the association, behaving as if the PFCP Association Release Request had been received.

#### 6.2.7.3.2 CP Function Behaviour

When receiving a PFCP Association Update Request, the CP function:

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

If the UP function has requested to release the PFCP association in the PFCP Association Update Request, the CP function should initiate a PFCP Association Release Request to release the PFCP association, as soon as possible if no Graceful Release Period was included in the request or before the expiry of the Graceful Release Period. The CP function should stop creating new PFCP sessions in the UP function during the Graceful Release Period. When the final usage report(s) for a PFCP Session (upon being deleted) is required, e.g. based on operator policies, the CP function should initiate a PFCP Session Deletion Procedure to collect the usage reports per PFCP Session affected by the release of PFCP Association before the Graceful Release Period is expired.

When both the CP function and UP function support the EPFAR feature, and if the UP function has set the URSS flag to "1" in the PFCP Association Update Request message, the CP function shall send the PFCP Association Update Response with successful cause value to indicate the PFCP Association Update Request is handled successfully and then immediately initiate the PFCP Association Release Procedure, as specified in clause 5.18.

If the UP function has included UE IP address Pool Identity IE in the PFCP Association Update Request message, the CP function shall use it to overwrite the UE IP address Pool Identity previously received from the UP function.

## 6.2.8 PFCP Association Release Procedure

### 6.2.8.1 General

PFCP Association Release is a node level procedure.

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

When the final usage report(s) for a PFCP Session is required, e.g. based on the operator policies, the CP function should retrieve the final usage reports for the PFCP Sessions affected by the release of PFCP Association, i.e. by initiating a PFCP Session Deletion Procedure towards the UP function for every PFCP session, before it initiates PFCP Association Release Request.

### 6.2.8.2 CP Function Behaviour

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

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

### 6.2.8.3 UP Function behaviour

When the UP function receives a PFCP Association Release Request, the UP function:

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

NOTE: The UP function always accepts a PFCP Association Release Request.

## 6.2.9 PFCP Node Report Procedure

### 6.2.9.1 General

PFCP Node Report Procedure is a node level procedure.

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

### 6.2.9.2 UP Function Behaviour

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

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

When the UP function receives a PFCP 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 a PFCP Node Report Request message, it shall:

- process the information being reported as appropriate and send a PFCP Node Report Response with the cause "success";

- otherwise return an appropriate error cause value.

# 6.3 PFCP Session Related Procedures

## 6.3.1 General

The following clauses describe the session related procedures over the Sxa, Sxb, Sxc and N4 reference points. The behaviour of the CP function and UP function when sending and receiving session related messages is described.

## 6.3.2 PFCP Session Establishment Procedure

### 6.3.2.1 General

The PFCP Session Establishment procedure shall be used to setup a PFCP 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 PFCP Session Establishment procedure to create a PFCP session for a PDN connection or a PDU session, 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 PFCP Session Establishment Request message with a new PFCP F-SEID together with Rules to be created;

- may include its current Recovery Time Stamp as specified in clause 19A of TS 3GPP TS 23.007 [24].

When the CP function receives a PFCP Session Establishment Response with the cause "Request accepted (success)", the CP function shall continue with the procedure which triggered the PFCP Session Establishment procedure. If the CP function indicated support of the PSUCC feature (see clause 8.2.58) during the PFCP association setup or update procedure, and if the cause in the response indicates "Request partially accepted", the CP function shall behave as specified in clause 5.2.9.

### 6.3.2.3 UP Function Behaviour

When the UP function receives a PFCP Session Establishment Request message:

- the UP function shall store and apply the rules received in the request and send a PFCP Session Establishment Response with cause "success", if all rules in the PFCP Session Establishment Request are stored and applied;

- Otherwise, if at least one rule failed to be stored or applied:

  - the UP function shall 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 PFCP session context, if the CP function or the UP function does not support the PSUCC feature (see clause 5.2.9); or

  - alternatively, if the CP function indicated support of the PSUCC feature (see clause 8.2.58) during the PFCP association setup or update procedure, and if this feature is also supported by the UP function, the UP function should accept the request partially, if possible, and return a response indicating a partial acceptance of the request as specified in clause 5.2.9.

## 6.3.3 PFCP Session Modification Procedure

### 6.3.3.1 General

The PFCP Session Modification procedure shall be used to modify an existing PFCP 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 PFCP Session Modification procedure to modify an existing PFCP session, e.g. triggered by a modification of PDN connection, PDU session, 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.

The CP function shall not include multiple updates in a PFCP Modification Request message, e.g. Create PDR, Update PDR and Remove PDR, for the same rule identified by the Rule ID.

When the CP function receives a PFCP Session Modification Response with the cause "Request accepted (success)", it shall continue with the procedure which has initiated the PFCP Session Modification procedure. If the CP function indicated support of the PSUCC feature (see clause 8.2.58) during the PFCP association setup or update procedure, and if the cause in the response indicates "Request partially accepted", the CP function shall behave as specified in clause 5.2.9.

#### 6.3.3.3 UP Function Behaviour

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

- send the PFCP Session Modification Response message with a rejection cause value set to "Session context not found" if the F-SEID included in the PFCP Session Modification Request message is unknown;
- reject a modification request which would relate to a rule not existing in the UP function;
- discard any updates on the PFCP session context included in the PFCP Session Modification Request message if the request is rejected and send a PFCP 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 PFCP session context for the PFCP session as if the PFCP 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 PFCP Session Modification Response with the cause "Request accepted (success)", if all the requested modifications are accepted and performed successfully;
- send the PFCP Session Modification Response with the cause "Request partially accepted", if the CP function indicated support of the PSUCC feature (see clause 8.2.58) during the PFCP association setup or update procedure, if this feature is also supported by the UP function, and if the UP function could accept the request partially as specified in clause 5.2.9.

### 6.3.4 PFCP Session Deletion Procedure

#### 6.3.4.1 General

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

#### 6.3.4.2 CP Function Behaviour

The CP function initiates a PFCP Session Deletion procedure towards the UP function to delete an existing PFCP session e.g. when the corresponding PDN connection or PDU session is deleted.

The CP shall:

- send a PFCP Session Deletion Request with the F-SEID identifying the PFCP session.

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

#### 6.3.4.3 UP Function Behaviour

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

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

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

### 6.3.5 PFCP Session Report Procedure

#### 6.3.5.1 General

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

#### 6.3.5.2 UP Function Behaviour

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

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

If the Enhanced PFCP Association Release feature (EPFAR) is supported by both the CP function and UP function, the UP function may send a PFCP Session Report Request message with the flag PSDBU being set to "1" to the CP function to report that the PFCP session is being deleted in the UP function, as specified in clause 5.18, e.g. to report remaining non-zero usage reports for all URRs in the PFCP Session before the PFCP Session is locally deleted in the UP function during an Enhanced PFCP Association Release procedure.

When the UP function receives a PFCP 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 a PFCP Session Report Request message, it shall:

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

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

- otherwise return an appropriate error cause value.

If the Enhanced PFCP Association Release feature (EPFAR) is supported by both the CP function and UP function, the CP function shall consider that a PFCP Session is locally deleted in the UP function upon receiving a PFCP Session Report Request message from the UP function with the flag PSDBU being set to "1".

## 6.4 Reliable Delivery of PFCP Messages

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

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.

## 6.5 PFCP messages bundling

PFCP messages bundling is an optional procedure that may be supported by the CP function and the UP function.

PFCP messages bundling may be used if both the CP function and the UP function have indicated support of the corresponding feature (see clauses 8.2.25 and 8.2.58) during the PFCP Association Setup or Update procedure. If so, the following requirements shall apply.

Several PFCP session related requests and/or responses messages, related to the same PFCP session or to different PFCP sessions handled by the same peer PFCP entity (i.e. with the peer's F-SEID having the same IP address, or with the same peer's IP address for PFCP Session Establishment Requests), may be bundled together in a single UDP/IP packet as specified in clause 7.2.1A, when being sent to that peer PFCP entity. PFCP messages may be bundled towards a PFCP entity of a UP function or of a CP function, independently.

NOTE 1: If the CP function bundles few PFCP session related requests in one UDP/IP packet it sends to a UP function, the UP function can return responses in separate UDP/IP packets or it can bundle some of the responses together with other PFCP session related messages.

NOTE 2: Bundling PFCP messages in a single UDP/IP packet enable to enhance performance and scalability (reduced CPU and memory cost thanks to reducing the number of packets to be packetized, exchanged and processed over N4).

PFCP session related messages handled by different peer PFCP entities (i.e. with the peer's F-SEID having different IP addresses) shall not be bundled together. PFCP node related messages shall not be bundled either.

The procedures specified in the rest of this specification shall apply for each PFCP message that is bundled in a UDP/IP packet, as if the PFCP message was sent in its own individual UDP/IP packet, i.e. PFCP messages bundling shall not incur any change to the PFCP protocol other than what is described in this clause.

NOTE 3: Each PFCP message bundled in a single UDP/IP packet has its own sequence number. Besides, if a UDP/IP packet carrying bundled PFCP messages is lost, retransmitted PFCP messages do not need to be bundled in the same manner as when sent originally.

# 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.

### 7.2.1A PFCP messages bundled in one UDP/IP packet

When applying PFCP messages bundling (see clause 6.5), PFCP messages shall be bundled in one UDP/IP packet as depicted in Figure 7.2.1A-1.

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

**Figure 7.2.1A-1: PFCP messages bundled in one UDP/IP packet**

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

The FO" (Follow On) flag in the PFCP message header of each PFCP message bundled in the UDP/IP packet, except the last PFCP message, shall be set to "1" to indicate that another PFCP message follows in the UDP/IP packet. See clause 7.2.2.

## 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 | FO | 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 clause 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 clause 7.2.2.4.1).
- Bit 3 represents the "FO" flag (see clause 7.2.2.4.1).
- Bit 4 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.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| 1 | Version | | | Spare | Spare | FO=0 | 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

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 | FO | 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 clause 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 PFCP 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 relative priority of the PFCP message. It shall be encoded as the binary value of the Message Priority and it may take any value between 0 and 15, where 0 corresponds to the highest priority and 15 the lowest priority.

- Bit 3 represents the "FO" (Follow On) flag. If the "FO" flag is set to "1", then another PFCP message follows in the UDP/IP packet (see clauses 6.5 and 7.2.1A).

- 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 clause 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:

- PFCP Session Establishment Request message on Sxa/Sxb/Sxc/N4;

- 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".

- When the UP function sends PFCP Session Report Request message over N4 towards another SMF or another PFCP entity in the SMF as specified in clause 5.22.2 and clause 5.22.3.

## 7.2.3 Information Elements

### 7.2.3.1 General

The format of PFCP Information Elements are defined in clause 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 clause 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 clause 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 clause 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 a PFCP 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 clause 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 within the same message level, these IEs shall have different IE types.

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

Assigning the same IE type to grouped IEs which don't have the same content is not recommended, even if these grouped IEs are in different message levels.

#### 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, Sxc, N4 and N4mb reference points are defined in Table 7.3-1.

**Table 7.3-1: Message Types**

| Message Type value (Decimal) | Message | Applicability | | | | |
|---|---|---|---|---|---|---|
| | | Sxa | Sxb | Sxc | N4 | N4 mb |

| | | | | | | |
|---|---|---|---|---|---|---|
| 0 | Reserved | | | | | |
| | **PFCP Node related messages** | | | | | |
| 1 | PFCP Heartbeat Request | X | X | X | X | X |
| 2 | PFCP Heartbeat Response | X | X | X | X | X |
| 3 | PFCP PFD Management Request | - | X | X | X | - |
| 4 | PFCP PFD Management Response | - | X | X | X | - |
| 5 | PFCP Association Setup Request | X | X | X | X | X |
| 6 | PFCP Association Setup Response | X | X | X | X | X |
| 7 | PFCP Association Update Request | X | X | X | X | X |
| 8 | PFCP Association Update Response | X | X | X | X | X |
| 9 | PFCP Association Release Request | X | X | X | X | X |
| 10 | PFCP Association Release Response | X | X | X | X | X |
| 11 | PFCP Version Not Supported Response | X | X | X | X | X |
| 12 | PFCP Node Report Request | X | X | X | X | X |
| 13 | PFCP Node Report Response | X | X | X | X | X |
| 14 | PFCP Session Set Deletion Request | X | X | - | X | - |
| 15 | PFCP Session Set Deletion Response | X | X | - | X | - |
| 16 | PFCP Session Set Modification Request | - | X | - | X | - |
| 17 | PFCP Session Set Modifcation Response | - | X | - | X | - |
| 18 to 49 | For future use | | | | | |
| | **PFCP Session related messages** | | | | | |
| 50 | PFCP Session Establishment Request | X | X | X | X | X |
| 51 | PFCP Session Establishment Response | X | X | X | X | X |
| 52 | PFCP Session Modification Request | X | X | X | X | X |
| 53 | PFCP Session Modification Response | X | X | X | X | X |
| 54 | PFCP Session Deletion Request | X | X | X | X | X |
| 55 | PFCP Session Deletion Response | X | X | X | X | X |
| 56 | PFCP Session Report Request | X | X | X | X | X |
| 57 | PFCP Session Report Response | X | X | X | X | X |
| 58 to 99 | For future use | | | | | |
| | **Other messages** | | | | | |
| 100 to 255 | For future use | | | | | |

# 7.4 PFCP Node Related Messages

## 7.4.1 General

This clause specifies either node level or PFCP entity level messages used over the Sxa, Sxb, Sxc, N4 and N4mb reference points (see clause 6.2).

## 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 | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Recovery Time Stamp | M | This IE shall contain the time stamp when the PFCP entity was started see clause 19A of 3GPP TS 23.007 [24]. | X | X | X | X | X | Recovery Time Stamp |
| Source IP Address | O | This IE may be included when a Network Address Translation device is deployed in the network. See clause 19a in 3GPP TS 23.007 [24]. | X | X | X | X | X | Source IP Address |

### 7.4.2.2 Heartbeat Response

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Recovery Time Stamp | M | This IE shall contain the time stamp when the PFCP entity was started see clause 19A of 3GPP TS 23.007 [24]. | X | X | X | X | X | Recovery Time Stamp |

## 7.4.3 PFCP PFD Management

### 7.4.3.1 PFCP PFD Management Request

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Application ID's PFDs | C | This IE shall contain an Application Identifier and the associated PFDs to be provisioned in the UP function.<br>Several IEs with the same IE type may be present to provision PFDs for multiple Application IDs.<br>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 | X | - | Application ID's PFDs |
| Node ID | O | When present, this IE shall contain the unique identifier of the sending Node. | - | X | X | X | - | Node ID |

**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** | **N4** | **N4 mb** | |
| Application ID | M | This IE shall identify the Application ID for which PFDs shall be provisioned in the UP function. | - | X | X | X | - | Application ID |
| PFD context | C | This IE shall be present if the PFD needs to be provisioned in the UP function.<br>When present, it shall describe the PFD to be provisioned in the UP function.<br>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 | X | - | PFD context |

**Table 7.4.3.1-3: PFD context**

| Octet 1 and 2 | PFD context IE Type = 59 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 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. (NOTE 1) | - | X | X | X | - | PFD Contents |
| NOTE 1 The CP function shall only provision a PFD Contents including a property with multiple values if the UP function supports PFDE feature. See clauses 8.2.25 and 8.2.39. | | | | | | | | |

### 7.4.3.2 PFCP PFD Management Response

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| 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 |
| Node ID | O | When present, this IE shall contain the unique identifier of the sending Node. | - | X | X | X | - | Node ID |

## 7.4.4 PFCP Association messages

### 7.4.4.1 PFCP Association Setup Request

#### 7.4.4.1.1 General

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | X | X | Node ID |
| Recovery Time Stamp | M | This IE shall contain the time stamp when the CP or UP function was started, see clause 19A of 3GPP TS 23.007 [24]. (NOTE) | X | X | X | X | X | 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. | X | X | X | X | X | 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. | X | X | X | X | X | CP Function Features |
| Alternative SMF IP Address | O | This IE may be present if the (MB-)SMF advertises the support of the SSET and/or MPAS feature in the CP Function Features IE (see clause 8.2.58).<br><br>When present, this IE shall contain an IPv4 and/or IPv6 address of an alternative (MB-)SMF or an alternative PFCP entity in the same (MB-)SMF when SSET feature is used, or an alternative PFCP entity in the same (MB-)SMF when MPAS feature is used.<br>Several IEs with the same IE type may be present to represent multiple alternative (MB-)SMF IP addresses. | - | - | - | X | X | Alternative SMF IP Address |
| SMF Set ID | C | This IE shall be present if the (MB-)SMF advertises the support of the MPAS feature in the CP Function Features IE (see clause 5.22.3).<br><br>When present, this IE shall contain an FQDN representing the (MB-)SMF set to which the (MB-)SMF belongs. | - | - | - | X | X | SMF Set ID |
| PFCP Session Retention Information | O | This IE may be present to request the UP function to keep all or part of the existing PFCP sessions upon receipt of a PFCP association setup request with a Node ID for which a PFCP association was already established. See clause 6.2.6.2.1. | X | X | X | X | X | PFCP Session Retention Information |
| UE IP address Pool Information | O | This IE may be present when the UP function sends this message, if UE IP Address Pools are configured in the UP function.<br><br>Several IE with the same IE type may be present to represent multiple UE IP address Pool Information. | - | X | - | X | - | UE IP address Pool Information |
| GTP-U Path QoS Control Information | C | This IE may be present, if the CP function sends this message, to request the UPF to monitor the QoS on GTP-U paths (see clause 5.24.5).<br>Several IEs with the same IE type may be present to represent multiple GTP-U paths (with different parameters) to monitor. | - | - | - | X | - | GTP-U Path QoS Control Information |
| Clock Drift Control Information | O | This IE may be present, if the CP function sends this message, to request the UPF to report clock drift between the external time and 5GS time for working domains (see clause 5.26.4).<br>Several IEs with the same IE type may be present for multiple Time domains (with different parameters). | - | - | - | X | - | Clock Drift Control Information |
| UPF Instance ID | O | This IE may be present if the UP function is a 5G UP function and if available, and if the message is sent by the UP function. | - | - | - | X | X | NF Instance ID |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| PFCPASReq-Flags | O | This IE shall be included if at least one of the flags is set to "1":<br><br>- UUPSI (UPF configured for IPUPS): when the message is sent by a UPF, the UP function shall set this flag to "1" if the UPF is configured to be used for IPUPS. See clause 5.27. | - | - | - | X | - | PFCPASReq-Flags |
| NOTE: A PFCP function shall ignore the Recovery Timestamp received in the PFCP Association Setup Request message. | | | | | | | | |

**Table 7.4.4.1-2: PFCP Session Retention Information IE within PFCP Association Setup Request**

| Octet 1 and 2 | PFCP Session Retention Information IE Type = 183 (decimal) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| CP PFCP Entity IP Address | O | This IE may be present to indicate the IP address of a CP PFCP entity for which the UP function shall retain the existing PFCP sessions, upon receipt of a PFCP association setup request with a Node ID for which a PFCP association was already established. See clause 6.2.6.2.1<br><br>Several IEs with the same IE type may be present to represent multiple CP PFCP entities for which PFCP sessions shall be retained.<br><br>If no CP PFCP Entity IP Address IE is present in the PFCP Session Retention Information IE, all existing PFCP sessions shall be kept upon receipt of a PFCP association setup request with a Node ID for which a PFCP association was already established. | X | X | X | X | X | CP PFCP Entity IP Address |

**Table 7.4.4.1-3: UE IP address Pool Information IE within PFCP Association Setup Request**

| Octet 1 and 2 | UE IP address Pool Information IE Type = 233 (decimal) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| UE IP address Pool Identity | M | When present, this IE shall contain an UE IP address Pool Identity<br><br>Several IEs with the same IE type may be present to represent multiple UE IP address Pool Identities. | - | X | - | X | - | UE IP address Pool Identity |
| Network Instance | O | The IE may be present to indicate for which DNN/APN the UE IP Address Pool Identifies are configured. | - | X | - | X | - | Network Instance |
| S-NSSAI | O | The IE may be present to indicate for which S-NSSAI the UE IP Address Pool Identities are configured.<br>Several IEs with the same IE type may be present to represent multiple S-NSSAIs. | - | - | - | X | - | S-NSSAI |
| IP version | O | The IE may be present to indicate for which IP version the UE IP Address Pool Identities are configured. | - | - | - | X | - | IP version |

### 7.4.4.1.2 Clock Drift Control Information IE within PFCP Association Setup Request

The Clock Drift Control Information grouped IE shall be encoded as shown in Table 7.4.4.1.2-1.

**Table 7.4.4.1.2-1: Clock Drift Control Information within PFCP Association Setup Request**

| Octet 1 and 2 | Clock Drift Control Information IE Type = 203 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Requested Clock Drift Information | M | This IE shall indicate the requested clock drift information. | - | - | - | X | - | Requested Clock Drift Information |
| Time Domain Number | C | When present, this IE shall identifiy the external time domain(s) for which clock drift information is requested.<br><br>More than one IE with this type may be included to represent multiple Time Domain Numbers.<br><br>This IE may be included if the Configured Time Domain IE is not included. (NOTE) | - | - | - | X | - | Time Domain Number |
| Configured Time Domain | C | When present with the CTDI (Configured Time Domain Indicator) flag set to "1", this IE indicates that the request targets the external time domain that is configured to the NW-TT(s) in the UPF.<br><br>This IE may be included if the Time Domain Number IE is not included. (NOTE) | - | - | - | X | - | Configured Time Domain |
| Time Offset Threshold | C | This IE shall be present if Time Offset Reporting is requested.<br>When present, it shall indicate the threshold to report the time offset, i.e. the offset shall be reported only when it exceeds the threshold compared to the previous report. | - | - | - | X | - | Time Offset Threshold |
| Cumulative rateRatio Threshold | C | This IE shall be present if Cumulative RateRatio Reporting is requested.<br>When present, it shall indicate the threshold to report the cumulative rateRatio, i.e. the cumative rateRatio shall be reported only when it exceeds the threshold compared to the previous report. | - | - | - | X | - | Cumulative rateRatio Threshold |
| NOTE: If neither the Time Domain Number IE nor the Configured Time Domain IE is included, this indicates that the request targets all the external time domains the UPF is connected to. | | | | | | | | |

### 7.4.4.1.3 GTP-U Path QoS Control Information IE within PFCP Association Setup Request

The GTP-U Path QoS Control Information grouped IE shall be encoded as shown in Table 7.4.4.1.3-1.

**Table 7.4.4.1.3-1: GTP-U Path QoS Control Information within PFCP Association Setup Request**

| Octet 1 and 2 | GTP-U Path QoS Control Information IE Type = 239 (decimal) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Remote GTP-U Peer | C | When present, this IE shall include the IP address of the remote GTP-U peer for which QoS information is to be reported, and the network instance used towards the remote GTP-U peer if available.<br>Several IEs with the same IE type may be present to represent multiple remote GTP-U peers.<br>(NOTE) | - | - | - | X | - | Remote GTP-U Peer |
| GTP-U Path Interface Type | C | When present, this IE shall include the Interface Type of the GTP-U paths for which QoS information is to be reported.<br>(NOTE) | - | - | - | X | - | GTP-U Path Interface Type |
| QoS Report Trigger | M | This IE shall indicate the trigger for reporting QoS information to the SMF. | - | - | - | X | - | QoS Report Trigger |
| DSCP | C | This IE shall be present, if available. When present, it shall contain the value of the DSCP in the TOS/Traffic Class field to measure the packet delay.<br><br>Several IEs with the same IE type may be present to represent multiple DSCP values to use for QoS monitoring. | - | - | - | X | - | Transport Level Marking |
| Measurement Period | C | This IE shall be present if the QoS Report Trigger indicates periodic reporting. When present, it shall contain the time period for the QoS reports towards the SMF. | - | - | - | X | - | Measurement Period |
| Average Packet Delay Threshold | C | This IE may be present if the QoS Report Trigger indicates reporting based on thresholds. | - | - | - | X | - | Average Packet Delay |
| Minimum Packet Delay Threshold | C | This IE may be present if the QoS Report Trigger indicates reporting based on thresholds. | - | - | - | X | - | Minimum Packet Delay |
| Maximum Packet Delay Threshold | C | This IE may be present if the QoS Report Trigger indicates reporting based on thresholds. | - | - | - | X | - | Maximum Packet Delay |
| Minimum Waiting Time | C | This IE may be present if the QoS Report Trigger indicates reporting based on thresholds. When present, it shall contain the minimum waiting time between two consecutive reports for the same type of measurement and the same remote GTP-U peer. | - | - | - | X | - | Timer |
| NOTE: At least one Remote GTP-U Peer IE or GTP-U Path Interface Type IE shall be present. | | | | | | | | | |

### 7.4.4.2 PFCP Association Setup Response

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | X | X | Node ID |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | X | X | X | Cause |
| Recovery Time Stamp | M | This IE shall contain the time stamp when the CP or UP function was started, see clause 19A of 3GPP TS 23.007 [24]. (NOTE) | X | X | X | X | X | 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. | X | X | X | X | X | 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. | X | X | X | X | X | CP Function Features |
| Alternative SMF IP Address | O | This IE may be present if the (MB-)SMF advertises the support of the SSET and/or MPAS feature in the CP Function Features IE (see clause 8.2.58).<br><br>When present, this IE shall contain an IPv4 and/or IPv6 address of an alternative (MB-)SMF or an alternative PFCP entity in the same (MB-)SMF when SSET feature is used, or an alternative PFCP entity in the same (MB-)SMF when MPAS feature is used.<br>Several IEs with the same IE type may be present to represent multiple alternative (MB-)SMF IP addresses. | - | - | - | X | X | Alternative SMF IP Address |
| SMF Set ID | C | This IE shall be present if the CP function sends this message and (MB-)SMF advertises the support of the MPAS feature in the CP Function Features IE (see clause 5.22.3).<br><br>When present, this IE shall contain an FQDN representing the (MB-)SMF set to which the (MB-)SMF belongs. | - | - | - | X | X | SMF Set ID |
| PFCPASRsp-Flags | O | This IE shall be included if at least one of the flags is set to "1":<br>- PSREI (PFCP Session Retained Indication): the UP function shall set this flag to "1" if the PFCP Session Retention Information IE was received in the Request, an existing PFCP association was already established for the same Node ID and the requested PFCP sessions have been retained. See clause 6.2.6.2.2.<br><br>- UUPSI (UPF configured for IPUPS): the UP function shall set this flag to "1" if the UPF is configured to be used for IPUPS. See clause 5.27. | X<br><br>- | X<br><br>- | X<br><br>- | X<br><br>X | X<br><br>- | PFCPASRsp-Flags |
| Clock Drift Control Information | C | This IE may be present, if the CP function sends this message, to request the UPF to report clock drift between the external time and 5GS time for external working domains (see clause 5.26.4).<br>Several IEs with the same IE type may be present to represent multiple external time domains (with different parameters).<br>See Table 7.4.4.1.2-1. | - | - | - | X | - | Clock Drift Control Information |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| UE IP address Pool Information | O | This IE may be present when the UP function sends this message, if UE IP Address Pools are configured in the UP function.<br><br>Several IE with the same IE type may be present to represent multiple UE IP address Pool Information.<br><br>The IE shall be encoded as in Table 7.4.4.1-3. | - | X | - | X | - | UE IP address Pool Information |
| GTP-U Path QoS Control Information | C | This IE may be present, if the CP function sends this message, to request the UPF to monitor the QoS on GTP-U paths (see clause 5.24.5). Several IEs with the same IE type may be present to represent multiple GTP-U paths to monitor.<br>See Table 7.4.4.1.3-1. | - | - | - | X | - | GTP-U Path QoS Control Information |
| UPF Instance ID | O | This IE may be present if the UP function is a 5G UP function and if available, and if the message is sent by the UP function. | - | - | - | X | X | NF Instance ID |
| NOTE: A PFCP function shall ignore the Recovery Timestamp received in PFCP Association Setup Response message. | | | | | | | | |

### 7.4.4.3 PFCP Association Update Request

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | X | X | Node ID |
| UP Function Features | O | If present, this IE shall indicate the supported Features when the sending node is the UP function. | X | X | X | X | X | UP Function Features |
| CP Function Features | O | If present, this IE shall indicate the supported Features when the sending node is the CP function. | X | X | X | X | X | CP Function Features |
| PFCP Association Release Request | C | This IE shall be present if the UP function requests the CP function to release the PFCP association. | X | X | X | X | X | PFCP Association Release Request |
| Graceful Release Period | C | This IE shall be present if the UP function requests a graceful release of the PFCP association. | X | X | X | X | X | Graceful Release Period |
| PFCPAUReq-Flags | O | This IE shall be included if at least one of the flags is set to "1".<br>- PARPS (PFCP Association Release Preparation Start): if both the CP function and UP function support the EPFAR feature, the CP or UP function may set this flag to "1" to indicate that the PFCP association is to be released and all non-zero usage reports for those PFCP Sessions affected by the release of the PFCP association shall be reported. | X | X | X | X | - | PFCPAUReq-Flags |
| Alternative SMF IP Address | O | This IE may be present if the (MB-)SMF advertises the support of the SSET and/or MPAS feature in the CP Function Features IE (see clause 8.2.58).<br><br>When present, this IE shall contain an IPv4 and/or IPv6 address of an alternative (MB-)SMF or an alternative PFCP entity in the same (MB-)SMF when SSET feature is used, or an alternative PFCP entity in the same (MB-)SMF when MPAS feature is used.<br><br>Several IEs with the same IE type may be present to represent multiple alternative (MB-)SMF IP addresses. | - | - | - | X | X | Alternative SMF IP Address |
| SMF Set ID | O | This IE may be present if the CP function sends this message and (MB-)SMF advertises the support of the MPAS feature in the CP Function Features IE (see clause 5.22.3), and there is a change in FQDN representing the (MB-)SMF set to which the (MB-)SMF belongs. | - | - | - | X | X | SMF Set ID |
| Clock Drift Control Information | C | This IE shall be present if the Clock Drift Control Information needs to be modified (see clause 5.26.4).<br>Several IEs with the same IE type may be present to represent TSN domains.<br><br>When present, the UPF shall replace any Clock Drift control information received earlier with the new received information.<br><br>A Clock Drift Control Information with a null length indicates that clock drift reporting shall be stopped.<br><br>See Table 7.4.4.1.2-1. | - | - | - | X | - | Clock Drift Control Information |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| UE IP address Pool Information | O | This IE may be present when the UP function sends this message, if UE IP Address Pools are configured in the UP function.<br><br>Several IE with the same IE type may be present to represent multiple UE IP address Pool Information.<br><br>The IE shall be encoded as in Table 7.4.4.1-3. | - | X | - | X | - | UE IP address Pool Information |
| GTP-U Path QoS Control Information | C | This IE shall be present if the GTP-U Path QoS Control Information needs to be modified (see clause 5.24.5).<br>Several IEs with the same IE type may be present to represent multiple GTP-U paths to monitor.<br><br>When present, the UPF shall replace any GTP-U path control information received earlier with the new received information.<br><br>A GTP-U Path QoS Control Information with a null length indicates that QoS monitoring of GTP-U paths shall be stopped.<br><br>See Table 7.4.4.1.3-1. | - | - | - | X | - | GTP-U Path QoS Control Information |
| UE IP Address Usage Information | O | The UP function may include this IE if both UP and CP functions support the UE IP Address Usage Reporting feature.<br>See Table 7.4.4.3.1-1<br><br>Several IEs with the same type may be present to represent UE IP Address Usage Information for different UE IP Address Pools and/or Network Instances.<br><br>See clause 5.21.3. | - | X | - | X | - | UE IP Address Usage Information |

### 7.4.4.3.1 UE IP Address Usage Information IE within PFCP Association Update Request

The UE IP Address Usage Information grouped IE shall be encoded as shown in Figure 7.4.4.3.1-1.

**Table 7.4.4.3.1-1: UE IP Address Usage Information IE within PFCP Association Update Request**

| Octet 1 and 2 | | UE IP Address Usage Information IE Type = 267 (decimal) | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | | Length = n | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| UE IP Address Usage Sequence Number | M | This IE shall be used by the CP function to properly collate out-of-order UE IP Address Usage Information received for a given network instance and/or UE IP Address pool, e.g. due to PFCP retransmissions. This IE shall also be used by the receiver to determine whether the newly received UE IP Address Usage Information has changed compared to UE IP Address Usage Information previously received from the same node earlier. | - | X | - | X | - | Sequence Number |
| UE IP Address Usage Metric | M | This IE shall represent the current ratio of occupied UE IP addresses in the UP function for the Network Instance indicated in the Network Instance IE, or for the Network Instance indicated in the Network Instance IE and the UE IP address Pool indicated by the UE IP Address Pool Id IE when this IE is present. The value shall be expressed as a percentage within the range of 0 to 100, where 0 means no or 0% usage and 100 means maximum or 100% usage reached (i.e. it is not desirable to receive further PFCP Session Establishment Requests). | - | X | - | X | - | Metric |
| Validity Timer | M | This IE shall represent the period of time during which the UE IP Address Usage Information shall be considered as valid. | - | X | - | X | - | Validity Timer |
| Number of UE IP Addresses | M | This IE shall indicate the total number of UE IP addresses configured for the Network Instance or also for the IP address Pool, when this IE is present. (NOTE) | - | X | - | X | - | Number of UE IP Addresses |
| Network Instance | M | This IE shall identify the associated Network instance. | - | X | - | X | - | Network Instance |
| UE IP Address Pool Id | O | This IE may be present if UE IP Addresses Pools are configured in the UPF.<br><br>When present, this IE shall contain the identity of the associated UE IP address Pool. | - | X | - | X | - | UE IP address Pool Identity |
| S-NSSAI | O | This IE may be present if the feature "Per slice UP resource management" is supported by the UP Function. When present, it shall indicate the S-NSSAI for which the UE IP addresses usage information is reported. | - | X | - | X | - | S-NSSAI |
| NOTE: When reporting the number of IPv6 UE Addresses for a specific Network Instance and/or IP address pool, the number of default /64 prefixes is reported by default, unless configured otherwise. | | | | | | | | |

### 7.4.4.4 PFCP Association Update Response

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | X | X | Node ID |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | X | X | X | Cause |
| UP Function Features | O | If present, this IE shall indicate the supported Features when the sending node is the UP function. | X | X | X | X | X | UP Function Features |
| CP Function Features | O | If present, this IE shall indicate the supported Features when the sending node is the CP function. | X | X | X | X | X | CP Function Features |
| UE IP Address Usage Information | O | The UP function may include if both UP and CP functions support the UE IP Address Usage Reporting feature.<br>See Table 7.4.4.3.1-1.<br><br>Several IEs with the same type may be present to represent UE IP Address Usage Information for different UE IP Address Pools and/or Network Instances.<br><br>See clause 5.21.3. | - | X | - | X | - | UE IP Address Usage Information |

### 7.4.4.5 PFCP Association Release Request

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | X | X | Node ID |

### 7.4.4.6 PFCP Association Release Response

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | X | X | Node ID |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | X | X | X | Cause |

### 7.4.4.7 PFCP 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 PFCP 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 PFCP Node Report Procedure

### 7.4.5.1 PFCP Node Report Request

#### 7.4.5.1.1 General

The PFCP Node Report Request shall be sent over the Sxa, Sxb, Sxc, N4 and N4mb interface by the UP function to report information to the CP function that is not specific to a PFCP session.

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | X | X | Node ID |
| Node Report Type | M | This IE shall indicate the type of the report. | X | X | X | X | X | Node Report Type |
| Vendor-Specific Node Report Type | C | This IE shall be present if the Node Report Type IE indicates a Vendor-Specific Report. When present, this IE shall indicate the type of the Vendor-Specific Report. | X | X | X | X | X | Vendor-Specific 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 | - | X | X | User Plane Path Failure Report |
| User Plane Path Recovery Report | C | This IE shall be present if the Node Report Type indicates a User Plane Path Recovery Report. | X | X | - | X | X | User Plane Path Recovery Report |
| Clock Drift Report | C | This IE shall be present if the Node Report Type indicates a Clock Drift Report.<br>More than one IE with this type may be included to send Clock Drift Reports for different Time Domain Numbers. | - | - | - | X | - | Clock Drift Report |
| GTP-U Path QoS Report | C | This IE shall be present if the Node Report Type indicates a GTP-U Path QoS Report.<br>More than one IE with this type may be included to represent multiple remote GTP-U peers for which QoS information is reported. | - | - | - | X | - | GTP-U Path QoS Report |
| Peer UP Restart Report | C | This IE shall be present if the Node Report Type Indicates a Peer GTP-U entity has restarted as specified in clause 20.3.4a of 3GPP TS 23.007 [24] and in clause 5.5 of 3GPP TS 23.527 [40]. | X | X | - | X | - | Peer UP Restart Report |

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

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

| Octet 1 and 2 | User Plane Path Failure Report IE Type = 102 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| 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 | - | X | X | Remote GTP-U Peer |

#### 7.4.5.1.3 User Plane Path Recovery Report IE within PFCP Node Report Request

**Table 7.4.5.1.3-1: User Plane Path Recovery Report IE within PFCP Node Report Request**

| Octet 1 and 2 | User Plane Path Recovery Report IE Type = 187 (decimal) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Remote GTP-U Peer | M | This IE shall include the IP address of the remote GTP-U peer towards which user plane path failure was reported and then the path has recovered within an operator configurable maximum path failure duration (see clause 20.3.4 in 3GPP TS 23.007 [24] and clause 5.4 in 3GPP TS 23.527 [40]).<br>More than one IE with this type may be included to represent multiple remote GTP-U peers towards which a user plane path has recovered. | X | X | - | X | X | Remote GTP-U Peer |

#### 7.4.5.1.4 Clock Drift Report IE within PFCP Node Report Request

**Table 7.4.5.1.4-1: Clock Drift Report IE within PFCP Node Report Request**

| Octet 1 and 2 | Clock Drift Report IE Type = 205 (decimal) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Time Domain Number | M | This IE shall identify the Time Domain Number for which measurements are reported. | - | - | - | X | - | Time Domain Number |
| Time Offset Measurement | O | When present, this IE shall contain the time offset measurement. | - | - | - | X | - | Time Offset Measurement |
| Cumulative rateRatio Measurement | O | When present, this IE shall contain the cumulative rateRatio measurement. | - | - | - | X | - | Cumulative rateRatio Measurement |
| Time Stamp | O | When present, this IE shall provide the timestamp when the collection of the information in this report was generated. | - | - | - | X | - | Time Stamp |
| Network Instance | C | This IE shall be present, when available (NOTE). | - | - | - | X | - | Network Instance |
| APN/DNN | C | This IE shall be present, when available (NOTE). | - | - | - | X | - | APN/DNN |
| S-NSSAI | C | This IE shall be present, when available (NOTE). | - | - | - | X | - | S-NSSAI |
| NOTE: The UPF shall provide the Network Instance and DNN/S-NSSAI (if available) to the CP function, to enable SMF to associate the report with the corresponding PFCP sessions and NW-TT, when the UPF supports more than one NW-TT. | | | | | | | | | |

#### 7.4.5.1.5 GTP-U Path QoS Report IE within PFCP Node Report Request

**Table 7.4.5.1.5-1: GTP-U Path QoS Report IE within PFCP Node Report Request**

| Octet 1 and 2 | GTP-U Path QoS Report IE Type = 239 (decimal) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Remote GTP-U Peer | M | This IE shall include the IP address of the remote GTP-U peer for which QoS information is reported, and the network instance used towards the remote GTP-U peer if available. | - | - | - | X | - | Remote GTP-U Peer |
| GTP-U Path Interface Type | C | This IE shall be present, if available. When present, it shall indicate the interface type of the GTP-U path towards the remote GTP-U peer. | - | - | - | X | - | GTP-U Path Interface Type |
| QoS Report Trigger | M | This IE shall indicate the trigger for this report. | - | - | - | X | - | QoS Report Trigger |
| Time Stamp | M | This shall shall provide the timestamp when the collection of the information in this report was generated. | - | - | - | X | - | Time Stamp |
| Start Time | C | This shall shall provide the timestamp when the collection of the information in this report was started. | - | - | - | X | - | Start Time |
| QoS Information | M | This IE shall contain the measured QoS information. More than one IE with this type may be included to represent multiple QoS Information, e.g. for different DSCP values. | - | - | - | X | - | QoS Information |

#### 7.4.5.1.6 QoS Information in GTP-U Path QoS Report IE

**Table 7.4.5.1.6-1: QoS Information in GTP-U Path QoS Report IE**

| Octet 1 and 2 | QoS Information IE Type = 240 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Average Packet Delay | M | This IE shall indicate the average packet delay of the related GTP-U path. | - | - | - | X | - | Average Packet Delay |
| Minimum Packet Delay | C | This IE shall indicate the minimum packet delay of the related GTP-U path, if available. | - | - | - | X | - | Minimum Packet Delay |
| Maximum Packet Delay | C | This IE shall indicate the maximum packet delay of the related GTP-U path, if available. | - | - | - | X | - | Maximum Packet Delay |
| DSCP | C | This IE shall be present, if available. When present, it shall contain the value of the DSCP in the TOS/Traffic Class field used in Echo messages to measure the packet delay. | - | - | - | X | - | Transport Level Marking |

#### 7.4.5.1.7 Peer UP Restart Report IE within PFCP Node Report Request

#### 7.4.5.1.7 Peer UP Restart Report IE within PFCP Node Report Request

**Table 7.4.5.1.7-1: Peer UP Restart Report IE within PFCP Node Report Request**

| Octet 1 and 2 | Peer UP Restart Report Type = 315 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Remote GTP-U Peer | M | This IE shall include the IP address of the remote GTP-U peer which has restarted.<br><br>More than one IE with this type may be included to represent that multiple peer GTP-U entities restart. | X | X | - | X | X | Remote GTP-U Peer |

### 7.4.5.2 PFCP Node Report Response

#### 7.4.5.2.1 General

The PFCP Node Report Response shall be sent over the Sxa, Sxb; Sxc, N4 and N4mb interface by the CP function to the UP function as a reply to the PFCP Node Report Request.

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | X | X | Node ID |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | 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 | X | X | Offending IE |

## 7.4.6 PFCP Session Set Deletion

### 7.4.6.1 PFCP Session Set Deletion Request

The PFCP Session Set Deletion Request shall be sent over the Sxa, Sxb or N4 interface by the CP function to request the UP function to delete the PFCP sessions affected by a partial failure.

The PFCP Session Set Deletion Request shall be also sent over the Sxa, Sxb or N4 interface by the UP function to request the CP function to delete the PFCP sessions affected by a partial failure.

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Node ID | M | This IE shall contain the node identity of the originating node of the message. | X | 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/SMF FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24] and clause 4.6 of 3GPP TS 23.527 [40]. | X | X | - | X | - | FQ-CSID |
| PGW-U/SGW-U/ UPF FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24] and clause 4.6 of 3GPP TS 23.527 [40]. | X | X | - | 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 PFCP Session Set Deletion Response

The PFCP Session Set Deletion Response shall be sent over the Sxa, Sxb or N4 interface by the UP function or the CP function as a reply to the PFCP Session Set Deletion Request.

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 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 an conditional or mandatory IE missing or faulty. | X | X | - | X | - | Offending IE |

## 7.4.7 PFCP Session Set Modification

### 7.4.7.1 PFCP Session Set Modification Request

The PFCP Session Set Modification Request shall be sent over the Sxb or N4 interface by the CP function to request the UP function to send any subsequent PFCP Session Report Request messages for the PFCP sessions which are identified by either FQ-CSID(s) or Group Id(s), or the CP IP Address in their F-SEIDs, towards an (alternative) SMF/PGW-C, e.g. when those PFCP sessions are affected by a partial PGW-C/SMF failure or are controlled by a PGW-C/SMF that is shutting down.

This procedure shall only be performed if the UP function indicated support of the RESPS feature (see clause 8.2.25).

**Table 7.4.7.1-1: Information Elements in a PFCP Session Set Modification Request**

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| Node ID | M | This IE shall contain the node identity of the originating node of the message. | - | X | - | X | - | Node ID |
| PFCP Session Change Info | M | This IE shall identify the FQ-CSID(s), Group Id(s) or CP IP address(es) of the PFCP sessions for which the PGW-U/UPF shall send subsequent PFCP Session Report Request messages to an Alternative SMF/PGW-C IP Address.<br><br>Several IEs with the same IE type may be present to request the PGW-U/UPF to move PFCP sessions associated with different FQ-CSIDs, Group Ids or CP IP addresses to different PGW-C/SMFs. | - | X | - | X | - | PFCP Session Change Info |

**Table 7.4.7.1-2: PFCP Session Change Info IE within PFCP Session Set Modification Request**

| Octet 1 and 2 | PFCP Session Change Info IE Type = 290 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| PGW-C/SMF FQ-CSID | C | This IE shall identify the PGW-C/SMF FQ-CSID of the PFCP sessions for which the UPF shall send subsequent PFCP Session Report Request messages to the Alternative SMF/PGW-C IP Address.<br><br>See also clause 31.6 of 3GPP TS 23.007 [24] and clause 4.7 of 3GPP TS 23.527 [40].<br><br>Several IEs with the same IE type may be present to represent several FQ-CSIDs of PFCP sessions that need to be moved to the same Alternative SMF/PGW-C IP Address. | - | X | - | X | - | FQ-CSID |
| Group Id | C | This IE shall identify the Group Id of the PFCP sessions for which the UPF shall send subsequent PFCP Session Report Request messages to the Alternative SMF/PGW-C IP Address.<br><br>See also clause 31.6 of 3GPP TS 23.007 [24] and clause 4.7 of 3GPP TS 23.527 [40].<br><br>Several IEs with the same IE type may be present to represent several Group Ids of PFCP sessions that need to be moved to the same Alternative SMF/PGW-C IP Address. | - | X | - | X | - | Group-Id |
| CP IP Address | C | This IE shall identify the IP address in the CP F-SEID of the PFCP sessions for which the UPF shall send subsequent PFCP Session Report Request messages to the Alternative SMF/PGW-C IP Address.<br><br>Several IEs with the same IE type may be present to represent several CP IP addresses of PFCP sessions that need to be moved to the same Alternative SMF/PGW-C IP Address. | - | X | - | X | - | CP IP Address |
| Alternative SMF/PGW-C IP Address | M | This IE shall include the alternative SMF/PGW-C IP Address to be used by the UP function to send subsequent PFCP Session Report Request messages for the PFCP Sessions associated with the PGW-C/SMF FQ-CSID(s), Group Id(s) or CP IP address(es).<br><br>When present, this IE shall contain an IPv4 and/or IPv6 address of the same or an alternative SMF/PGW-C. | - | X | | X | - | Alternative SMF IP Address |

## 7.4.7.2 PFCP Session Set Modification Response

The PFCP Session Set Modification Response shall be sent over the Sxb or N4 interface by the UP function to the CP function as a reply to the PFCP Session Set Modification Request.

**Table 7.4.2.2-1: Information Elements in a PFCP Session Set Modification Response**

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| 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 a conditional or mandatory IE missing or faulty. | - | X | - | X | - | Offending IE |

# 7.5 PFCP Session Related Messages

## 7.5.1 General

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

## 7.5.2 PFCP Session Establishment Request

### 7.5.2.1 General

The PFCP Session Establishment Request shall be sent over the Sxa, Sxb, Sxc, N4 and N4mb interface by the CP function to establish a new PFCP session context in the UP function.

**Table 7.5.2.1-1: Information Elements in a PFCP Session Establishment Request**

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sxa | Sxb | Sxc | N4 | N4 mb | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | 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 | X | X | F-SEID |
| Create PDR | M | This IE shall be present for at least one PDR to be associated to the PFCP session.<br><br>Several IEs with the same IE type may be present to represent multiple PDRs.<br>See Table 7.5.2.2-1. | X | X | X | X | X | Create PDR |
| Create FAR | M | This IE shall be present for at least one FAR to be associated to the PFCP session.<br><br>Several IEs with the same IE type may be present to represent multiple FARs.<br>See Table 7.5.2.3-1. | X | X | 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 PFCP 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 | X | - | Create URR |
| Create QER | C | This IE shall be present if a QoS enforcement or QoS marking action shall be applied to packets matching one or more PDR(s) of this PFCP 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 | 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 PFCP 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 | - | - | X | - | Create BAR |
| Create Traffic Endpoint | C | This IE may be present if the UP function has indicated support of PDI optimization.<br>Several IEs within the same IE type may be present to represent multiple Traffic Endpoints.<br>See Table 7.5.2.7-1. | X | X | X | X | X | Create Traffic Endpoint |
| PDN Type | C | This IE shall be present if the PFCP session is setup for an individual PDN connection or PDU session (see clause 5.2.1).<br>When present, this IE shall indicate whether this is an IP or non-IP PDN connection/PDU session or, for 5GC, an Ethernet PDU session. See NOTE 3. | X | 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/SMF FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24] and clause 4.6 of 3GPP TS 23.527 [40]. | X | 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 |
| User Plane Inactivity Timer | O | This IE may be present to request the UP function to send a User Plane Inactivity Report when no user plane packets are received for this PFCP session for a duration exceeding the User Plane Inactivity Timer. When present, it shall contain the duration of the inactivity period after which a User Plane Inactivity Report shall be generated. | - | X | X | X | X | User Plane Inactivity Timer |
| User ID | O | This IE may be present, based on operator policy. It shall only be sent if the UP function is in a trusted environment.<br>See NOTE 1. | X | X | X | X | - | User ID |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Trace Information | O | When present, this IE shall contain the trace instructions to be applied by the UP function for this PFCP session. | X | X | X | X | - | Trace Information |
| APN/DNN | O | This IE may be present, if related functionalities in the UP function require the APN/DNN information. See NOTE 2. | X | X | - | X | X | APN/DNN |
| Create MAR | C | This IE shall be present for a N4 session established for a MA PDU session.<br><br>Several IEs with the same IE type may be present to represent multiple MARs.<br>See Table 7.5.2.8-1. | - | - | - | X | - | Create MAR |
| PFCPSEReq-Flags | C | This IE shall be included if at least one of the flags is set to "1".<br>- RESTI (Restoration Indication): this bit shall be set to "1" if the CP function re-establishes an existing PFCP session and the allocation of GTP-U F-TEID and/or UE IP address is performed by the UP function. (NOTE 4)<br><br>- SUMPC (Stop Usage Measurement to Pause Charging): the CP function, e.g. PGW-C or (H-)SMF, shall set this flag if the usage measurement for the URRs which are applicable for charging (i.e. with the "ASPOC" flag set to "1") shall be stopped in the UP function. | X | X | - | X | - | PFCPSEReq-Flags |
| Create Bridge Info for TSC | C | This IE shall be present for a PFCP session established for TSC to request the UPF to provide Bridge information for TSC. | - | - | - | X | - | Create Bridge Info for TSC |
| Create SRR | O | This IE may be present to request the UPF to detect and report events not related to specific PDRs.<br>Several IEs within the same IE type may be present to represent multiple SRRs.<br>See Table 7.5.2.9-1. | - | - | - | X | - | Create SRR |
| Provide ATSSS Control Information | C | This IE shall be present for N4 session establishment for a MA PDU session.<br>When present, this IE shall contain the required ATSSS functionalities for this MA PDU session.<br>See Table 7.5.2.10-1. | - | - | - | X | - | Provide ATSSS Control Information |
| Recovery Time Stamp | O | This IE may be included to contain the time stamp when the CP function was started. (See clause 19A of 3GPP TS 23.007 [24].) | X | X | X | X | - | Recovery Time Stamp |
| S-NSSAI | O | This IE may be present, if related functionalities in the UP function require the S-NSSAI information. (NOTE 2, NOTE 5)<br>When present, it shall indicate the S-NSSAI of the PDU session or MBS session. | - | - | - | X | X | S-NSSAI |
| Provide RDS configuration information | O | When present, this IE shall contain the RDS configuration information to be applied by the UP function for this PFCP session. | - | X | - | X | - | Provide RDS configuration information |
| RAT Type | O | This IE may be present to provide the UP Function the current RAT Type for the PDN connection/PDU session to which this PFCP Session is corresponding for statistics purpose if the PFCP session is not established for a MA PDU session. | X | X | - | X | - | RAT Type |
| L2TP Tunnel Information | C | This IE shall be present if L2TP tunnel information is received from an AAA server, e.g. Radius/Diameter server or if it is configured in the CP function.<br><br>Several IE with the same IE type may be present to provide L2TP Tunnel Information for alternative LNS. | - | X | - | X | - | L2TP Tunnel Information |
| L2TP Session Information | C | This IE shall be present to include the information to establish a L2TP session, if an L2TP session needs to be established for this PFCP session. | - | X | - | X | - | L2TP Session Information |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Group Id | O | This IE may be included by the CP function to indicate the group identifier to which the PFCP session pertains (see clause 5.22). | - | X | - | X | - | Group Id |
| MBS Session N4mb Control Information | M | This IE shall identify the MBS session, or the MBS session and Area Session ID for a location dependent MBS service, and it may contain further control information for the MB-UPF. | - | - | - | - | X | MBS Session N4mb Control Information |
| MBS Session N4 Control Information | C | This IE shall be included if the correspond PDU session shall be associated with an MBS session, or with an MBS session and Area Session ID for a location dependent MBS service.<br><br>Several IEs with the same IE type may be present to provide N4 control information for several MBS sessions, e.g., when the UE requests to join several MBS sessions. | - | - | - | X | - | MBS Session N4 Control Information |
| DSCP to PPI Control Information | O | This IE may be present if the UPF is required to insert the Paging Policy Indicator (PPI) in the GTP-U PDU Session Container extension header of outgoing GTP-U packets (encapsulating payload packets) based on the DSCP in the TOS/Traffic Class field in the IP header of payload packet and if the UPF supports the EPPPI feature as specified in clause 5.36.2.<br><br>Several IEs with the same IE type may be present to provide different DSCP to PPI Control Information for different set of QFI(s). | - | - | - | X | - | DSCP to PPI Control Information |

NOTE 1: This can be used for troubleshooting problems in the UP function affecting a subscriber.
NOTE 2: The CP function may provide additional information (e.g. APN/DNN, S-NSSAI) to the UP function, e.g. used by the forwarding rules pre-defined in UP function (some forwarding rules are APN specific), used by the UP function for performance measurement, used by the UP function for resource management, or used by the UPF to include a proper User plane node/Bridge ID in the response message during a PFCP session establishment for a PDU session for TSC.
NOTE 3: The SGW-C may set PDN type as Non-IP for an Ethernet PDN to allow interworking with a legacy SGW-U.
NOTE 4: The UP function shall accept the CP function allocated GTP-U F-TEID and/or UE IP address in the PFCP Session Establishment Request message with the RESTI flag set to "1", if the requested GTP-U F-TEID and/or UE IP address are available. If the GTP-U F-TEID or UE IP address provided by the CP function is not available at the UP function, the UP function shall reject the PFCP Session Establishment Request with the cause "PFCP session restoration failure due to requested resource not available" (see clause 8.2.1).
NOTE 5: A UPF shall support allocating resources using the Network Instance IE and the UPF may additionally support allocating resources using the Network Instance IE and S-NSSAI IE (see clause 5.35).

**Table 7.5.2.1-2: L2TP Tunnel Information IE in the PFCP Session Establishment Request message**

| Octet 1 and 2 | L2TP Tunnel Information IE Type = 276 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| LNS Address | M | This IE shall be present to include the Tunnel Server Endpoint, i.e. LNS IP address. | - | X | - | X | - | LNS Address |
| Tunnel Password | O | This IE may be present to include the password to be used to authenticate to a remote server. | - | X | - | X | - | Tunnel Password |
| Tunnel Preference | C | This IE shall be present if multiple L2TP Tunnel Information IEs are included in the message.<br><br>If present this IE indicates the order in which the L2TP Tunnel Information IEs shall be used when trying to establish the L2TP session. | - | X | - | X | - | Tunnel Preference |

**Table 7.5.2.1-3: L2TP Session Information IE in the PFCP Session Establishment Request message**

| Octet 1 and 2 | L2TP Session Information IE Type = 277 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Calling Number | O | This IE may be present, e.g. to include an MSISDN of the UE. | - | X | - | X | - | Calling Number |
| Called Number | O | This IE may be present, e.g. to include an APN/DNN. | - | X | - | X | - | Called Number |
| Maximum Receive Unit | O | This IE may be present to include Maximum Receive Unit for LCP/PPP which may be set to the value of the MTU received from the UE or may be configured in the CP function. | - | X | - | X | - | Maximum Receive Unit |
| L2TP Session Indications | C | This IE shall be present if the CP function requests the UP function to get a UE IP Address, and/or DNS server information, and/or NBNS server information from the LNS. | - | X | - | X | - | L2TP session Indications |
| L2TP User Authentication | O | This IE may be present to include the authentication information to be used during L2TP session establishment. | - | X | - | X | - | L2TP User Authentication |
| NOTE: The Tunnel Password and L2TP User Authentication IE are transferred with plain text, a Network Domain Security/IP based security mechanism may be deployed between the CP function and the UP function if required by the local policies. | | | | | | | | |

**Table 7.5.2.1-4: MBS Session N4mb Control Information IE within PFCP Session Establishment Request**

| Octet 1 and 2 | MBS Session N4mb Control Information IE Type = 300 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| MBS Session Identifier | M | | - | - | - | - | X | MBS Session Identifier |
| Area Session ID | C | This IE shall be present for a location dependent MBS service. When present, it shall contain the Area Session ID, which together with the MBS Session Identifier, uniquely identify the service area part of the content data of the MBS service. | - | - | - | - | X | Area Session ID |
| MBSN4mbReq-Flags | C | This IE shall be included if at least one of the flags is set to "1".<br><br>- PLLSSM (Provide Lower Layer SSM): the MB-SMF shall set this flag to "1" to request the MB-UPF to allocate a LL SSM (i.e. multicast destination address and related source IP address) and a GTP-U Common Tunnel EndPoint Identifier (C-TEID), if multicast transport is used over N3mb and/or N19mb. See clause 5.34.2.2.<br><br>- JMBSSM (Join MBS Session SSM): the MB-SMF shall set this flag to "1" to request the MB-UPF to join the multicast tree towards the Source Specific Multicast (SSM) address information provided by AF/AS for the MBS Session, if multicast transport is used over N6mb.<br><br>- MBS RESTI (MBS Restoration Indication): this bit shall be set to "1" if the MB-SMF re-establishes an existing PFCP session. (NOTE) | - | - | - | - | X | MBSN4mbReq-Flags |
| Multicast Transport Information for N3mb and/or N19mb | C | This IE shall be present during the restoration of a PFCP session of an MBS session after an MB-UPF restart, as defined in clause 8.2.2 of 3GPP TS 23.527 [40].<br><br>When present, it shall include the low layer source specific multicast address information (i.e. multicast destination address and related source IP address) and the GTP-U Common Tunnel EndPoint Identifier (C-TEID) that the MB-SMF requests the MB-UPF to allocate for multicast transport over N3mb and/or N19mb, if possible. (NOTE) | - | - | - | - | X | Multicast Transport Information |
| NOTE: The MB-UPF shall accept the MB-SMF allocated N3mb/N19mb and/or the N6mb/Nmb9 address in the PFCP Session Establishment Request message with the MBS RESTI flag set to "1", if the requested addresses are available. If one requested address is not available at the MB-UPF, the MB-UPF shall reject the PFCP Session Establishment Request with the cause "PFCP session restoration failure due to requested resource not available" (see clause 8.2.1). | | | | | | | | |

**Table 7.5.2.1-5: MBS Session N4 Control Information IE within PFCP Session Establishment Request**

| Octet 1 and 2 | MBS Session N4 Control Information IE Type = 310 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| MBS Session Identifier | M | | - | - | - | X | - | MBS Session Identifier |
| Area Session ID | C | This IE shall be present for a location dependent MBS service. When present, it shall contain the Area Session ID, which together with the MBS Session Identifier, uniquely identify the service area part of the content data of the MBS service. | - | - | - | X | - | Area Session ID |
| Multicast Transport Information | C | This IE shall be present to include a low layer source specific multicast address information (i.e. multicast destination address and related source IP address) and a GTP-U Common Tunnel EndPoint Identifier (C-TEID) which was allocated by the MB-UPF, if IP multicast transport is used over N19mb. | - | - | - | X | - | Multicast Transport Information |

**Table 7.5.2.1-6: DSCP to PPI Control Information IE within PFCP Session Establishment Request**

| Octet 1 and 2 | DSCP to PPI Control Information IE Type = 316 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| DSCP to PPI Mapping Information | M | This IE shall be present to instruct the UPF to insert the corresponding PPI for the downlink GTP-U packet, where the DSCP of its payload packet is matching one of DSCP codes in the DSCP to PPI Mapping Information.<br><br>Several IEs with the same IE type may be present to provide different DSCP to PPI mapping information. | - | - | - | X | - | DSCP to PPI Mapping Information |
| QFI | O | This IE may be present to request the UPF to only insert PPI for those packets pertain to the requested QoS flow(s).<br><br>Several IEs with the same IE type may be present to provide a list of QFIs.<br><br>(NOTE 1) | - | - | - | X | - | QFI |
| NOTE 1: The absence of QFI(s) indicates that insertion of the corresponding PPI shall be applied for all DL packets (matching the DSCP(s) of the DSCP to PPI Mapping Information IE) pertaining to all QoS flows of the PFCP session. | | | | | | | | |

## 7.5.2.2 Create PDR IE within PFCP 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 PFCP 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** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| PDR ID | M | This IE shall uniquely identify the PDR among all the PDRs configured for that PFCP session. | X | X | 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 PFCP session, when looking for a PDR matching an incoming packet. | - | X | X | 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 | 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 | - | 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, and if the MAR ID is not included. This IE may be present if the CP function activated a predefined rule name with a predefined FAR but the CP function wishes to overwrite the predefined FAR by another FAR. (NOTE 2)<br>When present this IE shall contain the FAR ID to be associated to the PDR. | X | X | 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 | X | - | URR ID |
| QER ID | C | This IE shall be present if a QoS enforcement or QoS marking 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 | X | X | QER ID |
| Activate Predefined Rules | C | This IE shall be present if Predefined Rule(s) shall be activated for this PDR. When present this IE shall contain one Predefined Rules name.<br>Several IEs with the same IE type may be present to represent multiple "Activate Predefined Rules" names. | - | X | X | X | - | Activate Predefined Rules |
| Activation Time | O | This IE may be present if the PDR activation shall be deferred. (NOTE 1) | - | X | X | X | - | Activation Time |
| Deactivation Time | O | This IE may be present if the PDR deactivation shall be deferred. (NOTE 1) | - | X | X | X | - | Deactivation Time |
| MAR ID | C | This IE shall be present if the PDR is provisioned to match the downlink traffic of non-GBR QoS flows towards the UE for a PFCP session established for a MA PDU session. | - | - | - | X | - | MAR ID |
| Packet Replication and Detection Carry-On Information | C | This IE shall be present if the PDR is provisioned to match a broadcast packet. When present, it contains the information to instruct the UPF to replicate the packet and to carry-on the look-up of other PDRs of other PFCP sessions matching the packet (see clause 5.2.1). | - | - | - | X | - | Packet Replication and Detection Carry-On Information |
| IP Multicast Addressing Info | O | This IE may be present in an UL PDR controlling UL IGMP/MLD traffic (see 5.25).<br>When present, it shall contain a (range of) IP multicast address(es), and optionally source specific address(es), identifying a set of IP multicast flows. See Table 7.5.2.2-4.<br>Several IEs with the same IE type may be present to represent multiple IP multicast flows. | - | - | - | X | - | IP Multicast Addressing Info |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| UE IP address Pool Identity | O | This IE may be present if UE IP Addresses Pools are configured in the UPF.<br><br>When present, this IE shall contain the identity of a UE IP address Pool configured in the UPF.<br>Two IEs with the same IE type shall be present to represent UE IPv4 Address Pool Identity and UE IPv6 Address Pool Identity if different pool identities are used for UE IPv4 address and UE IPv6 address and both an UE IPv4 and an UE IPv6 address are requested to be assigned for the PFCP session. In this case, the UE IPv4 Address Pool Identity shall be encoded before the UE IPv6 Address Pool Identity. | - | X | - | X | - | UE IP address Pool Identity |
| MPTCP Applicable Indication | C | This IE shall be present if the PDR is used to detect UL user plane traffic for which MPTCP is applicable. | - | - | - | X | - | MPTCP Applicable Indication |
| Transport Delay Reporting | C | This IE shall be present to request the UPF to add the delay of the GTP-U path with the preceding uplink GTP-U entity to the "N3/N9 Delay Result received in the GTP-U PDU Session Container extension header (see 3GPP TS 38.415 [34]) of the uplink packet, when monitoring the QoS of a PDU session based on GTP-U path monitoring (see clause 5.24.5.3). See Table 7.5.2.2-6. | - | - | - | X | - | Transport Delay Reporting |
| RAT Type | O | This IE may be present to provide the UP Function the current RAT Type for the UL PDR for statistics purpose if the PFCP session is established for a MA PDU session. | - | - | - | X | - | RAT Type |
| NOTE 1: When the Activation Time and Deactivation Time are not present, the PDR shall be activated immediately at receiving the message.<br>NOTE 2: If a predefined FAR is or has been activated using a predefined rule name, it is UP function implementation specific whether this predefined FAR can be overwritten by a FAR ID pointing to another predefined FAR (i.e. with the most significant bit set to 1). If not, the UP function shall reject such a request if received from the CP function. | | | | | | | | |

**Table 7.5.2.2-2: PDI IE within PFCP 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** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Source Interface | M | This IE shall identify the source interface of the incoming packet. | X | X | X | X | X | Source Interface |
| Local F-TEID | O | This IE shall not be present if Traffic Endpoint ID is present.<br>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 CP function requests the UP function to assign a local F-TEID to the PDR. | X | X | - | X | - | F-TEID |
| Local Ingress Tunnel | C | This IE shall not be present if Traffic Endpoint ID is present.<br>If present, this IE shall identify the IP address and the UDP port for a UDP/IP tunnel.<br><br>The CP function shall set the CHOOSE (CH) bit to 1 if the CP function requests the UP function to assign a local ingress tunnel to the PDR. | - | - | - | - | X | Local Ingress Tunnel |
| Network Instance | O | This IE shall not be present if Traffic Endpoint ID is present. It shall be present if the CP function requests the UP function to allocate a UE IP address/prefix and the Traffic Endpoint ID is not present.<br>If present, this IE shall identify the Network instance to match for the incoming packet. See NOTE 1, NOTE2. | X | X | X | X | X | Network Instance |
| Redundant Transmission Detection Parameters | O | If present, this IE shall contain the information used for the reception of redundant uplink packets on N3/N9 interfaces. | - | - | - | X | - | Redundant Transmission Detection Parameters |
| UE IP address | O | This IE shall not be present if Traffic Endpoint ID is present.<br>If present, this IE shall identify the UE IP address as the source or destination IP address to match for the incoming packet. (NOTE 5).<br><br>The CP function shall set the CHOOSE IPV4 (CHV4) and/or the CHOOSE IPV6 (CHV6) bits to 1 if the UP function supports the allocation of UE IP address/ prefix and the CP function requests the UP function to assign a UE IP address/prefix to the PDR.<br><br>This IE may also present to identify the IP address of the CP function as the destination IP address to match for the incoming packet, e.g. Radius, Diameter or DHCP signalling packet. (NOTE 8).<br><br>In the 5GC, several IEs with the same IE type may be present to represent multiple UE IP addresses, if the UPF indicated support of the IP6PL feature (see clause 5.21). | - | X | X | X | - | UE IP address |
| Traffic Endpoint ID | C | This IE may be present if the UP function has indicated the support of PDI optimization.<br>If present, this IE shall uniquely identify the Traffic Endpoint for that PFCP session.<br><br>Several IEs with the same IE type may be present to provision several Traffic Endpoints with different Traffic Endpoint IDs, from which the UPF may receive packets pertaining to the same service data flow, which is subject for the same FAR, QER and URR, if the UPF has indicated it supports MTE feature as specified in clause 8.2.25. See NOTE 6. | X | X | X | X | X | Traffic Endpoint ID |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| SDF Filter | O | If present, this IE shall identify the SDF filter to match for the incoming packet. Several IEs with the same IE type may be present to provision a list of SDF Filters. The full set of applicable SDF filters, if any, shall be provided during the creation or the modification of the PDI.<br>See NOTE 3. | - | X | X | X | X | SDF Filter |
| Application ID | O | If present, this IE shall identify the Application ID to match for the incoming packet. | - | X | X | X | X | Application ID |
| Ethernet PDU Session Information | O | This IE may be present to identify all the (DL) Ethernet packets matching an Ethernet PDU session (see clause 5.13.1). | - | - | - | X | - | Ethernet PDU Session Information |
| Ethernet Packet Filter | O | If present, this IE shall identify the Ethernet PDU to match for the incoming packet.<br>Several IEs with the same IE type may be present to represent a list of Ethernet Packet Filters.<br>The full set of applicable Ethernet Packet filters, if any, shall be provided during the creation or the modification of the PDI. | - | - | - | X | - | Ethernet Packet Filter |
| QFI | O | This IE shall not be present if Traffic Endpoint ID is present and the QFI(s) are included in the Traffic Endpoint.<br>If present, this IE shall identify the QoS Flow Identifier to match for the incoming packet.<br>Several IEs with the same IE type may be present to provision a list of QFIs. When present, the full set of applicable QFIs shall be provided during the creation or the modification of the PDI. | - | - | - | X | - | QFI |
| Framed-Route | O | This IE may be present for a PDR if the UPF indicated support of Framed Routing (see clauses 8.2.25 and 5.16). If present, this IE shall describe a framed route.<br>Several IEs with the same IE type may be present to provision a list of framed routes. (NOTE 5) | - | X | - | X | - | Framed-Route |
| Framed-Routing | O | This IE may be present for a DL PDR if the UPF indicated support of Framed Routing (see clauses 8.2.25 and 5.16). If present, this IE shall describe the routing method for the UP function for the IP route related to Framed-Routes or Framed-IPv6-Routes. (NOTE 7) | - | X | - | X | - | Framed-Routing |
| Framed-IPv6-Route | O | This IE may be present for a PDR if the UPF indicated support of Framed Routing (see clauses 8.2.25 and 5.16). If present, this IE shall describe a framed IPv6 route.<br>Several IEs with the same IE type may be present to provision a list of framed IPv6 routes. (NOTE 5) | - | X | - | X | - | Framed-IPv6-Route |
| Source Interface Type | O | This IE may be present to indicate the 3GPP interface type of the source interface, if required by functionalities in the UP Function, e.g. for performance measurements. | X | X | - | X | X | 3GPP Interface Type |
| IP Multicast Addressing Info | O | This IE may be present in a DL PDR controlling DL IP multicast traffic (see clause 5.25).<br>When present, it shall contain a (range of) IP multicast address(es), and optionally source specific address(es), identifying a set of IP multicast flows. See Table 7.5.2.2-4.<br>This IE shall be present over N4mb, if multicast transport is used over N6mb and if Traffic Endpoint ID is not present.<br>Several IEs with the same IE type may be present to represent multiple IP multicast flows. | - | - | - | X | X | IP Multicast Addressing Info |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| DNS Query Filter | O | This IE may be present for an UL PDR if the UPF indicated support of DNS traffic steering based on FQDN in the DNS Query message.<br>If present, this IE shall identify the DNS Query filter to match for the incoming DNS Query packets.<br>Several IEs with the same IE type may be present to provision a list of DNS Query Filters. The full set of applicable DNS Query filters, if any, shall be provided during the creation or the modification of the PDI. | - | - | - | X | - | DNS Query Filter |
| MBS Session Identifier | C | This IE shall be present when the PDR is created to receive MBS session data. (NOTE 9) | - | - | - | X | - | MBS Session Identifier |
| Area Session ID | C | This IE shall be present for a location dependent MBS service. When present, it shall contain the Area Session ID, which together with the MBS Session Identifier, uniquely identify the service area part of the content data of the MBS service. (NOTE 9) | - | - | - | X | - | Area Session ID |

NOTE 1: The Network Instance parameter is needed e.g. in the following cases:
- PGW/TDF UP function supports multiple PDNs with overlapping IP addresses;
- SGW UP function is connected to PGWs in different IP domains (S5/S8);
- PGW UP function is connected to SGWs in different IP domains (S5/S8);
- SGW UP function is connected to eNodeBs in different IP domains;
- UPF is connected to 5G-ANs in different IP domains;
- Separation of multiple 5G VN groups communication in the UPF;
- Indirect data forwarding.

NOTE 2: When a Local F-TEID is provisioned in the PDI, the Network Instance shall relate to the IP address of the F-TEID. Otherwise, the Network Instance shall relate to the UE IP address if provisioned or the destination IP address in the SDF filter if provisioned

NOTE 3: SDF Filter IE(s) shall not be present if Ethernet Packet Filter IE(s) is present.

NOTE 4: When several SDF filter IEs are provisioned, the UP function shall consider that the packets are matched if matching any SDF filter. The same principle shall apply for Ethernet Packet Filters and QFIs.

NOTE 5: If both the UE IP Address and the Framed-Route (or Framed-IPv6-Route) are present, the packets which are considered being matching the PDR shall match at least one of them.

NOTE 6: Maximum two Traffic Endpoint ID containing different Local TEIDs per PDI may be provisioned over the N4 interface for a PFCP session which is established for a PDU session subject for 5G to EPS mobility with N26 supported. Several Traffic Endpoint ID containing different UE IP Addresses may be provisioned over the N4 interface for a PFCP session if the UPF also indicated support of the IP6PL feature (see clause 5.21.1).

NOTE 7: In this release of specification, the UP function shall announce the IP route(s) for Framed-Route(s) or Framed-IPv6-Route(s) to the PDN regardless of the value of the Framed-Routing.

NOTE 8: The IP address of the CP function is needed e.g. perform Router Advertisements and match the destination IP address of the incoming packet if the Radius, Diameter or DHCP signaling packets between the SMF and the external DN is forwarded by the UPF.

NOTE 9: The Inclusion of the MBS Session Identifier, or MBS Session Identifier and Area Session ID for a location dependent MBS session, enables the UPF to allocate the same N19mb tunnel for the same MBS Session, or for the same MBS session and Area Session ID for a location dependent MBS session, when receiving multiple PFCP Session Establishment or Modification Request messages for different PFCP sessions being associated with the same MBS session, or with the same MBS session and Area Session ID for a location dependent MBS session, and also helps the UPF to identify the PFCP sessions associated with a MBS Session, or with the same MBS session and Area Session ID for a location dependent MBS session.

**Table 7.5.2.2-3: Ethernet Packet Filter IE within PFCP Session Establishment Request**

| Octet 1 and 2 | Ethernet Packet Filter IE Type = 132 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Ethernet Filter ID | C | This shall be present if Bidirectional Ethernet filter is required. This IE shall uniquely identify an Ethernet Filter among all the Ethernet Filters provisioned for a given PFCP session. | - | - | - | X | - | Ethernet Filter ID |
| Ethernet Filter Properties | C | This IE shall be present when provisioning a bidirectional Ethernet Filter the first time (see clause 5.13.4). | - | - | - | X | - | Ethernet Filter Properties |
| MAC address | O | If present, this IE shall identify the MAC address.<br>This IE may be present up to 16 times. | - | - | - | X | - | MAC address |
| Ethertype | O | If present, this IE shall identify the Ethertype. | - | - | - | X | - | Ethertype |
| C-TAG | O | If present, this IE shall identify the Customer-VLAN tag. | - | - | - | X | - | C-TAG |
| S-TAG | O | If present, this IE shall identify the Service-VLAN tag. | - | - | - | X | - | S-TAG |
| SDF Filter | O | If packet filtering is required, for Ethernet frames with Ethertype indicating IPv4 or IPv6 payload, this IE shall describe the IP Packet Filter Set.<br>Several IEs with the same IE type may be present to represent a list of SDF filters. | - | - | - | X | - | SDF Filter |

**Table 7.5.2.2-4: IP Multicast Addressing Info IE within PFCP Session Establishment Request**

| Octet 1 and 2 | IP Multicast Addressing Info IE Type = 188 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |
| IP Multicast Address | M | This IE shall contain the IP multicast address(es) of the DL multicast flow(s) or indicate "any" IP multicast address.<br><br>For N4mb, the IP Multicast Address shall be set to the value of IP Multicast Address in the SSM for the MBS Session. | - | - | - | X | X | IP Multicast Address |
| Source IP Address | O | When present, this IE shall contain the source specific IP address of the DL multicast flow.<br>Several IEs with the same IE type may be present to represent multiple source specific addresses.<br>If this IE is not present, this indicates "any" source IP address. | - | - | - | X | | Source IP Address |
| | M | This IE shall be set to the value of the IP Source Address in the SSM for the MBS Session. | - | - | - | - | X | |

**Table 7.5.2.2-5: Redundant Transmission Detection Parameters IE in PDI**

| Octet 1 and 2 | Redundant Transmission Detection Parameters IE Type = 255 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Local F-TEID for Redundant Transmission | M | This IE shall identify the local F-TEID to match for an incoming packet for redundant transmission.<br>The CP function shall set the CHOOSE (CH) bit to 1 if it requests the UP function to assign a local F-TEID to the PDR. | - | - | - | X | - | F-TEID |
| Network Instance for Redundant Transmission | C | This IE shall be included if the Local F-TEID for Redundant Transmission uses a different network Instance than the Network Instance used for the Local F-TEID for the primary GTP-U tunnel. | - | - | - | X | - | Network Instance |

**Table 7.5.2.2-6: Transport Delay Reporting IE in Create PDR IE**

| Octet 1 and 2 | Transport Delay Reporting IE Type = 271 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Preceding UL GTP-U Peer | M | This IE shall identify the preceding UL GTP-U peer. | - | - | - | X | - | Remote GTP-U Peer |
| DSCP | O | If present, this IE shall contain the DSCP to use to measure the GTP-U path delay with the preceding UL GTP-U peer. | - | - | - | X | - | Transport Level Marking |

## 7.5.2.3 Create FAR IE within PFCP 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 PFCP 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** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| FAR ID | M | This IE shall uniquely identify the FAR among all the FARs configured for that PFCP session. | X | X | X | X | X | FAR ID |
| Apply Action | M | This IE shall indicate the action to apply to the packets, See clauses 5.2.1 and 5.2.3. | X | X | 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 | 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><br>Several IEs with the same IE type may be present to represent to duplicate the packets to different destinations. See NOTE 1.<br><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. | X | - | - | X | - | BAR ID |
| Redundant Transmission Forwarding Parameters | C | This IE shall be present when the Apply Action requests the packets to be duplicated for redundant transmission and the Forwarding Parameters IE is included. 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 for redundant transmission. Except for the parameters included in the Redundant Transmission Parameters IE, the duplicated packets shall apply the same parameters as those indicated in the Forwarding Parameters IE.<br><br>See table 7.5.2.3-4. | - | - | - | - | - | Redundant Transmission Forwarding Parameters |
| MBS Multicast Parameters | C | This IE shall be present when the Apply Action is set to "FSSM". This requests the MB-UPF to forward the MBS session data to a Low Layer SSM. | - | - | - | - | X | MBS Multicast Parameters |
| Add MBS Unicast Parameters | C | This IE shall be present when the Apply Action is set to "MBSU". This requests the MB-UPF to forward the MBS session data to a remote GTP-U peer for unicast transport.<br><br>Several IEs with the same IE type may be present to request the MB-UPF to forward the MBS session data to multiple remote GTP-U peers. | - | - | - | - | X | Add MBS Unicast Parameters |
| NOTE 1: The same user plane packets may be required, according to operator's policy and configuration, to be duplicated to different SX3LIFs. | | | | | | | | |

**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** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Destination Interface | M | This IE shall identify the destination interface of the outgoing packet. | X | 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 | 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 | 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/or Port Number when adding a UDP/IP header or an IP header or the C-TAG/S-TAG (for 5GC). See NOTE 2. | X | 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 for EPC, 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 clause 5.10 of 3GPP TS 23.214 [2]. When present for 5GC, it shall contain the value of the DSCP in the TOS/Traffic Class field set based on the 5QI, the Priority Level (if explicitly signalled), and optionally the ARP priority level, of the associated QoS flow, as described in clause 5.8.2.7 of 3GPP TS 23.501 [28], | X | 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 / N6-LAN. It may be present if the Destination Interface is set to Core, Access, or CP-Function. See NOTE 2.<br>When present, it shall contain an Identifier of the Forwarding Policy locally configured in the UP function. | - | X | 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 | X | - | Header Enrichment |
| Linked Traffic Endpoint ID | C | This IE may be present, if it is available and the UP function indicated support of the PDI optimisation feature, (see clause 8.2.25). When present, it shall identify the Traffic Endpoint ID allocated for this PFCP session to receive the traffic in the reverse direction (see clause 5.2.3.1). | X | X | - | X | - | Traffic Endpoint ID |
| Proxying | C | This IE shall be present if proxying is to be performed by the UP function.<br><br>When present, this IE shall contain the information that the UPF shall respond to Address Resolution Protocol and / or IPv6 Neighbour Solicitation based on the local cache information for the Ethernet PDUs. | - | - | - | X | - | Proxying |
| Destination Interface Type | O | This IE may be present to indicate the 3GPP interface type of the destination interface, if required by functionalities in the UP Function, e.g. for performance measurements. | X | X | - | X | - | 3GPP Interface Type |
| Data Network Access Identifier | C | This IE shall be present over N16a to link the UL FAR in an UL CL or BP towards a specific local PSA, if more than one local PSA has been inserted by an I-SMF. It may be present over N16a otherwise. This IE shall not be sent over N4.<br>When present, it shall be set to the DNAI associated to the local PSA towards which the UL traffic shall be forwarded. | - | - | - | - | - | Data Network Access Identifier |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| IP Address and Port Number Replacement | C | This IE shall be present if the UP function indicated support of replacing the source and destination IP address and Port Number of an (inner) IP packet, and if the source or destination IP address and/or port number of the (Inner) IP packet shall be modified, e.g. for Edge Relocation using EAS IP address and Port number Replacement (see clause 5.33.3).<br><br>This IE shall also be present if the destination IP address and/or port number of the (Inner) IP packet shall be modified, e.g. for EAS Discovery procedure with Local DNS Server/Resolver using Local DNS Server/Resolver IP address and Port number Replacement (see clause 5.33.4).<br>(NOTE 3) | - | - | - | X | - | IP Address and Port Number Replacement |
| 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>- PGW UP function is connected to SGWs in different IP domains (S5/S8);<br>- SGW UP function is connected to eNodeBs in different IP domains;<br>- UPF is connected to 5G-ANs in different IP domains;<br>- Separation of multiple 5G VN groups communication in the UPF;<br>- Indirect data forwarding.<br>NOTE 2: If the Outer Header Creation and Forwarding Policy are present, the UP function shall put the user plane packets in the user plane tunnel by applying Outer Header Creation, after enforcing the required Forwarding Policy.<br>NOTE 3: As opposed to the Outer Header Creation IE, this IE does not result in adding any outer header to the outgoing packet. | | | | | | | | |

**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** | **N4** | **N4 mb** | |
| 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. See NOTE 1. | 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 |
| NOTE 1: If the Outer Header Creation and Forwarding Policy are present, the UP function shall put the user plane packets in the user plane tunnel by applying Outer Header Creation, after enforcing the required Forwarding Policy. | | | | | | | | |

**Table 7.5.2.3-4: Redundant Transmission Forwarding Parameters IE in FAR**

| Octet 1 and 2 | Redundant Transmission Forwarding Parameters IE Type = 270 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Outer Header Creation | M | This IE shall be present if the UP function is required to perform the redundant transmission of the outgoing packet.<br>If present, it shall contain the F-TEID of the remote GTP-U peer for redundant transmission. | - | - | - | X | - | Outer Header Creation |
| Network Instance for Redundant Transmission | C | This IE shall be included if the GTP-U tunnel used for redundant transmission uses a different network Instance than the Network Instance used for the primary GTP-U tunnel. | - | - | - | X | - | Network Instance |

**Table 7.5.2.3-5: MBS Multicast Parameters IE in the Create FAR IE**

| Octet 1 and 2 | MBS Multicast Parameters IE Type = 301 (decimal) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |
| Destination Interface | M | This IE shall identify the destination interface of the outgoing packet. | - | - | - | - | X | Destination Interface |
| Network Instance | O | When present, this IE shall identify the Network instance towards which to send the outgoing packet. | - | - | - | - | X | Network Instance |
| Outer Header Creation | M | This IE shall instruct the MB-UPF to create a GTP-U header using the Low Layer SSM and the C-TEID allocated to the MBS session. | - | - | - | - | 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 | Transport Level Marking |
| Destination Interface Type | O | This IE may be present to indicate the 3GPP interface type of the destination interface, if required by functionalities in the UP Function, e.g. for performance measurements.<br><br>Several IEs with the same IE type may be present to represent multiple destination interface types (e.g. N3mb and N19mb). | - | - | - | - | X | 3GPP Interface Type |

**Table 7.5.2.3-6: Add MBS Unicast Parameters IE in the Create FAR IE**

| Octet 1 and 2 | Add MBS Unicast Parameters IE Type = 302 (decimal) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Destination Interface | M | This IE shall identify the destination interface of the outgoing packet. | - | - | - | - | X | Destination Interface |
| MBS Unicast Parameters ID | M | This IE shall identify the MBS Unicast Parameters IE. | - | - | - | - | X | MBS Unicast Parameters ID |
| Network Instance | O | When present, this IE shall identify the Network instance towards which to send the outgoing packet. | - | - | - | - | X | Network Instance |
| Outer Header Creation | M | This IE shall be present to request the MB-UPF to add one outer header to the outgoing packet. It shall contain the F-TEID of the remote GTP-U peer when adding a GTP-U/UDP/IP header. | - | - | - | - | 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 | Transport Level Marking |
| Destination Interface Type | O | This IE may be present to indicate the 3GPP interface type of the destination interface, if required by functionalities in the UP Function, e.g. for performance measurements. | - | - | - | - | X | 3GPP Interface Type |

### 7.5.2.4 Create URR IE within PFCP 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 PFCP 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** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| URR ID | M | This IE shall uniquely identify the URR among all the URRs configured for this PFCP session. | X | 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 | 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, or when an SMF instructs an UPF to report the reception of the End Marker packet from the old I-UPF during a Service Request procedure (see clauses 4.2.3.2 and 4.23.4.3 in 3GPP TS 23.502 [29]). | X | 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 | 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 | 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 clause 5.2.2.2)<br>When present, it shall indicate the Volume Quota value. | - | X | X | X | - | Volume Quota |
| Event Threshold | C | This IE shall be present if event-based measurement is used and reporting is required upon reaching an event threshold. When present, it shall indicate the number of events after which the UP function shall report to the CP function for this URR. | - | X | X | X | - | Event Threshold |
| Event Quota | C | This IE shall be present if event-based measurement is used and the CP function needs to provision an Event Quota in the UP function (see clause 5.2.2.2)<br>When present, it shall indicate the Event Quota value. | - | X | X | X | - | Event 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 | 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 clause 5.2.2.2)<br>When present, it shall indicate the Time Quota value | - | X | 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.<br>When present, it shall contain the duration of the inactivity period. | - | X | 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.<br>When present, it shall contain the threshold of the DL traffic being dropped. | X | - | - | X | - | Dropped DL Traffic Threshold |
| Quota Validity Time | C | This IE shall be present if reporting is required when the Quota Validity time for a given Quota is over. | - | X | - | X | - | Quota Validity Time |
| 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 | 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.<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 | 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.<br>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 | X | X | - | Subsequent Time Threshold |
| Subsequent Volume Quota | O | This IE may be present if Monitoring Time IE is present and volume-based measurement is used (see clause 5.2.2.2).<br>When present, it shall indicate the Volume Quota value which the UP function shall use for this URR for the period after the Monitoring Time. | - | X | X | X | - | Subsequent Volume Quota |
| Subsequent Time Quota | O | This IE may be present if Monitoring Time IE is present and time-based measurement is used (see clause 5.2.2.2)<br>When present, it shall indicate the Time Quota value which the UP function shall use for this URR for the period after the Monitoring Time. | - | X | X | X | - | Subsequent Time Quota |
| Subsequent Event Threshold | O | This IE may be present if the Monitoring Time IE is present and event-based measurement is used.<br>When present, it shall indicate the number of events after which the UP function shall report to the CP function for this URR for the period after the Monitoring Time. | - | X | X | X | - | Subsequent Event Threshold |
| Subsequent Event Quota | O | This IE may be present if Monitoring Time IE is present and event-based measurement is used (see clause 5.2.2.2).<br>When present, it shall indicate the Event Quota value which the UP function shall use for this URR for the period after the Monitoring Time. | - | X | X | X | - | Subsequent Event Quota |
| 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 | 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 clause 5.2.2.4).<br>Several IEs with the same IE type may be present to represent multiple linked URRs which are related with this URR. | - | X | 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>- Reduced Application Detection Information Flag: this flag may be set to "1", if the Reporting Triggers request to report the start or stop of application, to request the UP function to only report the Application ID in the Application Detection Information, e.g. for envelope reporting.<br>- Immediate Start Time Metering Flag: this flag may be set to "1" if time-based measurement is used and the UP function is requested to start the time metering immediately at receiving the flag. .<br>- Measurement of Number of Packets Flag: this flag may be set to "1" when the Volume-based measurement applies, to request the UP function to report the number of packets in UL/DL/Total in addition to the measurement in octet.<br>- Send Start Pause of Charging Flag: this flag may be set to "1" by the CP function if the UP Function is requested to send a Start Pause of Charging indication to the upstream GTP-U entity(s) when the Dropped DL Traffic Threshold is reached.<br>- Applicable for Start of Pause of Charging Flag: this flag may be set to "1" if the URR is applicable for Start of Pause of Charging, so that the UP function shall stop the usage measurement for the URR when receiving Start Pause of Charging indication from the peer downstream GTP-U entity.<br>- Control of Inactive Measurement Flag: the flag shall be set to "1" if the CP function requests the UP function to stop or resume the usage measurement for the URR with the "ASPOC" flag set to "1" according to the value of Inactive Measurement Flag. | -<br>-<br>-<br>-<br>X<br>X<br>-<br>- | X<br>X<br>X<br>X<br>X<br>-<br>X<br>X | X<br>-<br>-<br>X<br>X<br>-<br>-<br>- | X<br>X<br>X<br>X<br>X<br>X<br>X<br>X | -<br>-<br>-<br>-<br>-<br>-<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 |
| Aggregated URRs | C | This IE shall be included if the URR is used to support a Credit Pool.<br><br>Several IEs with the same IE type may be present to provide multiple aggregated URRs. | - | X | - | - | - | Aggregated URRs |
| FAR ID for Quota Action | C | This IE may be present if the Volume Quota IE and/or the Time Quota IE and/or Event Quota IE is provisioned in the URR and the UP Function indicated support of the Quota Action feature.<br>When present, it shall contain the identifier of the substitute FAR the UP function shall apply, for the traffic associated to this URR, when exhausting any of these quotas. See NOTE 1, NOTE 3. | - | X | X | X | - | FAR ID |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Ethernet Inactivity Timer | C | This IE shall be present if Ethernet traffic reporting is used and the SMF requests the UP function to also report inactive UE MAC addresses.<br>When present, it shall contain the duration of the Ethernet inactivity period. | - | - | - | X | - | |
| Additional Monitoring Time | O | When present, this IE shall contain the time at which the UP function shall re-apply the volume or time or event threshold/quota provisioned in the IE.<br><br>Several IEs with the same IE type may be present to provide multiple Monitoring Times. | X | X | X | X | - | Additional Monitoring Time |
| Number of Reports | O | This IE may be present if the UP function supports the NORP feature. When present, it shall indicate the number of usage reports to be generated by the URR. See also clauses 5.2.2.2.1 and 5.2.2.3.1. See NOTE 2. | X | X | X | X | - | Number of Reports |
| Exempted Application ID for Quota Action | O | This IE may be present if the Volume Quota IE and/or the Time Quota IE and/or Event Quota IE is provisioned in the URR and the UP Function has indicated support of the QUASF feature as specified in clause 8.2.25.<br><br>When present, it shall contain an Application ID matching packets that shall be exempted from applying the FAR ID for Quota Action when the quota has been exhausted.<br><br>Several IEs with the same IE type may be present to provide multiple Application IDs.<br><br>See NOTE 4. | - | X | X | X | - | Application ID |
| Exempted SDF Filter for Quota Action | O | This IE may be present if the Volume Quota IE and/or the Time Quota IE and/or Event Quota IE is provisioned in the URR and the UP Function has indicated support of the QUASF feature as specified in clause 8.2.25.<br><br>When present, it shall contain an SDF Filter matching packets that shall be exempted from applying the FAR ID for Quota Action when the quota has been exhausted.<br><br>Several IEs with the same IE type may be present to provide multiple SDF Filters.<br><br>See NOTE 4. | - | X | X | X | - | SDF Filter |
| User Plane Inactivity Timer | C | This IE shall be present, for a time, volume or event-based measurement, if reporting is required when no packets are received for any PDR(s) associated with the URR during a given inactivity period. See clause 5.11.3.<br>When present, it shall contain the duration of the inactivity period. | - | - | - | X | - | User Plane Inactivity Timer |

NOTE 1: The substitute FAR used when exhausting a Volume Quota or Time Quota may be set to drop the packets or redirect the traffic towards a redirect destination as specified in clause 5.4.7.

NOTE 2: This IE may be provisioned and set to "1" e.g. for a URR with the Dropped DL Traffic Threshold used for the Pause of Charging feature, if the UP function supports the NORP feature.

NOTE 3: If the FAR as indicated in the FAR ID for Quota Action is removed after being provisioned, the UP function shall behave as if the FAR ID for Quota Action is not provisioned and shall apply the default behaviour per local configuration when the quota is exhausted.

NOTE 4: The Exempted Application ID for Quota Action IE or Exempted Filter ID for Quota Action IE may be provisioned as the Restricted-Filter-Rule AVP or Filter ID AVP which is included in Final-Unit-Indication AVP from the online charging system when the Final-Unit-Action AVP is set to "REDIRECT" or "RESTRICT_ACCESS". See also 3GPP TS 32.299 [18].

**Table 7.5.2.4-2: Aggregated URRs**

| Octet 1 and 2 | Aggregated URRs = 118 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | | **Appl.** | | | | **IE Type** |
| | | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Aggregated URR ID | M | This IE shall be present for the aggregated URR ID of the URR sharing the credit pool. | - | X | - | - | - | Aggregated URR ID |
| Multiplier | M | This IE shall be included to measure the abstract service units the traffic of the corresponding aggregated URR consumes from the credit pool. | - | X | - | - | - | Multiplier |

**Table 7.5.2.4-3: Additional Monitoring Time**

| Octet 1 and 2 | Additional Monitoring Time = 147 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | | **Appl.** | | | | **IE Type** |
| | | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Monitoring Time | M | This IE shall be present and contain the time at which the UP function shall re-apply the volume or time threshold/quota. | X | X | 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 | 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 | X | X | - | Subsequent Time Threshold |
| Subsequent Volume Quota | O | This IE may be present if Monitoring Time IE is present and volume-based measurement is used (see clause 5.2.2.2). When present, it shall indicate the Volume Quota value which the UP function shall use for this URR for the period after the Monitoring Time. | - | X | X | X | - | Subsequent Volume Quota |
| Subsequent Time Quota | O | This IE may be present if Monitoring Time IE is present and time-based measurement is used (see clause 5.2.2.2) When present, it shall indicate the Time Quota value which the UP function shall use for this URR for the period after the Monitoring Time. | - | X | X | X | - | Subsequent Time Quota |
| Subsequent Event Threshold | O | This IE may be present if the Monitoring Time IE is present and event-based measurement is used. When present, it shall indicate the number of events after which the UP function shall report to the CP function for this URR for the period after the Monitoring Time. | - | X | X | X | - | Event Threshold |
| Subsequent Event Quota | O | This IE may be present if Monitoring Time IE is present and event-based measurement is used (see clause 5.2.2.2). When present, it shall indicate the Event Quota value which the UP function shall use for this URR for the period after the Monitoring Time. | - | X | X | X | - | Event Quota |

### 7.5.2.5 Create QER IE within PFCP 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 PFCP 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** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| QER ID | M | This IE shall uniquely identify the QER among all the QER configured for that PFCP session | - | X | X | 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 PFCP sessions, for APN-AMBR enforcement/APN rate control of multiple UE's PDN connections to the same APN. | - | X | - | 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 | 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>For EPC, 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><br>For 5GC, this IE may be set to the value of:<br>- the Session-AMBR, for a QER that is referenced by all the PDRs of the non-GBR QoS flows of a PDU session;<br>- the QoS Flow MBR, for a QER that is referenced by all the PDRs of a QoS Flow;<br>- the SDF MBR, for a QER that is referenced by all the PDRs of a SDF. | - | X | X | 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 QoS Flow GBR, for a QER that is referenced by all the PDRs of a QoS Flow (for 5GC);<br>- the SDF GBR, for a QER that is referenced by all the PDRs of a SDF. | - | X | X | 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, or belonging to the PDU session (5GC) using CIoT EPS Optimizations as described in 3GPP TS 23.401 [2] and 3GPP TS 23.501 [28], respectively;<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 all PDN connections to the same APN, or for Small Data Rate Control (5GC) for a QER related to the PDU session using CIoT EPS Optimizations as described in 3GPP TS 23.401 [2] and 3GPP TS 23.501 [28], respectively. | - | X | - | X | - | Packet Rate |
| Packet Rate Status | C | This IE may be present during the UE requested PDU session establishment, or UE requested PDN connection establishment.<br>When present, the UP function shall first enforce these rules. Only after that shall the UP function enforce the rules in the Packet Rate IE. | - | X | - | X | - | Packet Rate Status |
| DL Flow Level Marking | C | This IE shall be set if the UP function is required to mark the packets for QoS purposes:<br>- by the TDF-C, for DL flow level marking for application indication (see clause 5.4.5);<br>- by the PGW-C, for setting the GTP-U Service Class Indicator extension header for service indication towards GERAN (see clause 5.4.12). | - | X | X | - | - | DL Flow Level Marking |
| QoS flow identifier | C | This IE shall be present if the QoS flow identifier shall be inserted or modified by the UPF or shall be inserted by the MB-UPF. (NOTE 2) | - | - | - | X | X | QFI |
| Reflective QoS | C | This IE shall be present if the UP function is required to insert a Reflective QoS Indicator to request reflective QoS for uplink traffic. | - | - | - | X | - | RQI |
| Paging Policy Indicator | C | This IE shall be present if the UPF is required to set the Paging Policy Indicator (PPI) in outgoing packets (see clause 5.4.3.2 of 3GPP TS 23.501 [28]).<br>When present, it shall be set to the PPI value to set. | - | - | - | X | - | Paging Policy Indicator |
| Averaging Window | O | This IE may be present if the UP function is required to use a different Averaging window than the default one. (NOTE 1) | - | - | - | X | - | Averaging Window |
| QER Control Indications | C | This IE shall be included if the CP function needs to provide the QoS enforcement control information:<br>- RCSR (Rate Control Status Reporting): the CP function shall set this bit "1" to request the UP function to report the rate control status when the PFCP session is released. | - | X | - | X | - | QER Control Indications |
| QER Indications | C | This IE shall be included if at least one of the flags is set to "1".<br>- IQFISN (Insert DL MBS QFI Sequence Number): this IE shall be set to "1" to request the MB-UPF to insert the DL MBS QFI Sequence Number in the PDU Session Container of the MBS data packets (see 3GPP TS 38.415 [34]). | - | - | - | - | X | QER Indications |

NOTE 1: As 5QI is not signalled over N4, one default averaging window shall be pre-configured in the UPF.
NOTE 2: The SMF may request the UPF to modify the QFI of downlink packets of a multicast QoS flow received from the MB-UPF to the QFI assigned by the SMF for the Associated QoS flow. See clause 5.34.3.2.

### 7.5.2.6 Create BAR IE within PFCP 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 PFCP 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** | **N4** | **N4 mb** | |
| BAR ID | M | This IE shall uniquely identify the BAR provisioned for that PFCP session. | X | - | - | 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 clause 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 |
| Suggested Buffering Packets Count | C | This IE may be present if the UP Function indicated support of the feature UDBC.<br><br>When present, it shall contain the number of packets that are suggested to be buffered when the Apply Action parameter requests to buffer the packets. The packets that exceed the limit shall be discarded. | - | X | X | X | - | Suggested Buffering Packets Count |
| MT-EDT Control Information | O | This IE may be included to request the SGW-U to report the sum of DL Data Packets Size. | X | - | - | - | - | MT-EDT Control Information |

### 7.5.2.7 Create Traffic Endpoint IE within PFCP Session Establishment Request

The Create Traffic Endpoint grouped IE shall be encoded as shown in Figure 7.5.2.7-1.

**Table 7.5.2.7-1: Create Traffic Endpoint IE within PFCP Session Establishment Request**

| Octet 1 and 2 | Create Traffic Endpoint IE Type = 127(decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Traffic Endpoint ID | M | This IE shall uniquely identify the Traffic Endpoint for that PFCP session. | X | X | X | X | X | Traffic Endpoint ID |
| 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 CP function requests the UP function to assign a local F-TEID to the Traffic Endpoint. | X | X | - | X | - | F-TEID |
| Network Instance | O | This IE shall be present if the CP function requests the UP function to allocate a UE IP address/prefix.<br>If present, this IE shall identify the Network instance to match for the incoming packet. See NOTE 1, NOTE 2. | X | X | X | X | X | Network Instance |
| Redundant Transmission Detection Parameters | O | If present, this IE shall contain the information used for the reception of redundant uplink packets on N3/N9 interfaces.<br>See Table 7.5.2.2-5. | - | - | - | X | - | Redundant Transmission Detection Parameters |
| UE IP address | O | If present, this IE shall identify the UE IP address as the source or destination IP address to match for the incoming packet. (NOTE 3).<br><br>The CP function shall set the CHOOSE IPV4 (CHV4) and/or CHOOSE IPV6 (CHV6) bits to 1 if the UP function supports the allocation of UE IP address/ prefix and the CP function requests the UP function to assign a UE IP address/prefix to the Traffic Endpoint.<br><br>This IE may also present to identify the IP address of the CP function as the destination IP address to match for the incoming packet, e.g. Radius, Diameter or DHCP signalling packet. (NOTE 6).<br><br>In the 5GC, several IEs with the same IE type may be present to represent multiple UE IP addresses, if the UPF indicated support of the IP6PL feature (see clause 5.21). | - | X | X | X | - | UE IP address |
| Ethernet PDU Session Information | O | This IE may be present to identify all the (DL) Ethernet packets matching an Ethernet PDU session (see clause 5.13.1). | - | - | - | X | - | Ethernet PDU Session Information |
| Framed-Route | O | This IE may be present for a PDR if the UPF indicated support of Framed Routing (see clauses 8.2.25 and 5.16). If present, this IE shall describe a framed route.<br><br>Several IEs with the same IE type may be present to provision a list of framed routes. (NOTE 3) | - | X | - | X | - | Framed-Route |
| Framed-Routing | O | This IE may be present for a DL PDR if the UPF indicated support of Framed Routing (see clauses 8.2.25 and 5.16). If present, this IE shall describe the routing method for the UP function for the IP route related to Framed-Routes or Framed-IPv6-Routes. (NOTE 5) | - | X | - | X | - | Framed-Routing |
| Framed-IPv6-Route | O | This IE may be present for a PDR if the UPF indicated support of Framed Routing (see clauses 8.2.25 and 5.16). If present, this IE shall describe a framed IPv6 route.<br>Several IEs with the same IE type may be present to provision a list of framed IPv6 routes. (NOTE 3) | - | X | - | X | - | Framed-IPv6-Route |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| QFI | O | This IE may be present if the UPF has indicated it supports MTE feature as specified in clause 8.2.25.<br><br>If present, this IE shall identify the QoS Flow Identifier to match for the incoming packet received from the traffic endpoint.<br><br>Several IEs with the same IE type may be present to provision a list of QFIs. When present, the full set of applicable QFIs shall be provided. | - | - | - | X | - | QFI |
| Source Interface Type | O | This IE may be present to indicate the 3GPP interface type of the source interface, if required by functionalities in the UP Function, e.g. for performance measurements.<br>(NOTE 4) | X | X | - | X | X | 3GPP Interface Type |
| Local Ingress Tunnel | C | This IE shall be present over N4mb, for Nmb9, or for N6mb if unicast transport is used over N6mb, if Traffic Endpoint ID is present in the DL PDR.<br><br>If present, this IE shall identify the IP address and the UDP port for a UDP/IP tunnel.<br><br>The CP function shall set the CHOOSE (CH) bit to 1 if the CP function requests the UP function to assign a local ingress tunnel to the PDR. | - | - | - | - | X | Local Ingress Tunnel |
| IP Multicast Addressing Info | C | This IE shall be present over N4mb, if multicast transport is used over N6mb, if Traffic Endpoint ID is present in the DL PDR.<br>See Table 7.5.2.2-4. | - | - | - | - | X | IP Multicast Addressing Info |
| MBS Session Identifier | C | This IE shall be present when the PDR is created to receive MBS session data. (NOTE 7) | - | - | - | X | - | MBS Session Identifier |
| Area Session ID | C | This IE shall be present for a location dependent MBS service. When present, it shall contain the Area Session ID, which together with the MBS Session Identifier, uniquely identify the service area part of the content data of the MBS service.<br>(NOTE 7) | - | - | - | X | - | Area Session ID |
| RAT Type | O | This IE may be present to provide the UP Function the current RAT Type for the UL PDR(s) for statistics purpose if the PFCP session is established for a MA PDU session. | - | - | - | X | - | RAT Type |

NOTE 1: The Network Instance parameter is needed e.g. in the following cases:
- PGW/TDF UP function supports multiple PDNs with overlapping IP addresses;
- SGW UP function is connected to PGWs in different IP domains (S5/S8);
- PGW UP function is connected to SGWs in different IP domains (S5/S8);
- SGW UP function is connected to eNodeBs in different IP domains;
- UPF is connected to 5G-ANs in different IP domains;
- Separation of multiple 5G VN groups communication in the UPF.

NOTE 2: When a Local F-TEID is provisioned in the Traffic Endpoint, the Network Instance shall relate to the IP address of the F-TEID. Otherwise, the Network Instance shall relate to the UE IP address.

NOTE 3: If both the UE IP Address and the Framed-Route (or Framed-IPv6-Route) are present, the packets which are considered being matching the PDR shall match at least one of them.

NOTE 4: If the Source Interface Type is provisioned at the traffic endpoint, it shall not be provisioned in individual PDRs associated to the traffic endpoint.

NOTE 5: In this release of specification, the UP function shall announce the IP route(s) for Framed-Route(s) or Framed-IPv6-Route(s) to the PDN regardless of the value of the Framed-Routing.

NOTE 6: The CP IP Address parameter is needed e.g. perform Router Advertisements and match the destination IP address of the incoming packet if the Radius, Diameter or DHCP signaling packets between the SMF and the external DN is forwarded by the UPF.

NOTE 7: The Inclusion of the MBS Session Identifier, or MBS Session Identifier and Area Session ID for a location dependent MBS session, enables the UPF to allocate the same N19mb tunnel for the same MBS Session, or for the same MBS Session Identifier and Area Session ID for a location dependent MBS session, when receiving multiple PFCP Session Establishment or Modification Request messages for different PFCP sessions being associated with the same MBS session, or with the same MBS session and Area Session ID for a location dependent MBS session, and also helps the UPF to identify the PFCP sessions associated with a MBS Session, or with the same MBS session and Area Session ID for a location dependent MBS session.

### 7.5.2.8 Create MAR IE within PFCP Session Establishment Request

The Create MAR grouped IE shall be encoded as shown in Figure 7.5.2.8-1.

**Table 7.5.2.8-1: Create MAR IE within PFCP Session Establishment Request**

| Octet 1 and 2 | Create MAR IE Type = 165 (decimal) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| MAR ID | M | This IE shall uniquely identify the MAR among all the MARs configured for that PFCP session. | - | - | - | X | - | MAR ID |
| Steering Functionality | M | This IE shall be present to indicate the applicable traffic steering functionality. | - | - | - | X | - | Steering Functionality |
| Steering Mode | M | This IE shall be present to indicate the steering mode. | - | - | - | X | - | Steering Mode |
| 3GPP Access Forwarding Action Information | C | This IE shall be present to provision 3GPP access specific forwarding action information if the UE is registered for 3GPP access, except when steering mode is set to "Active-Standby", Non-3GPP access is the active access and 3GPP access is not used as Standby access. In the latter case, this IE may be present.<br>(NOTE) | - | - | - | X | - | 3GPP Access Forwarding Action Information |
| Non-3GPP Access Forwarding Action Information | C | This IE shall be present to provision non-3GPP access specific forwarding action information if the UE is registered for non-3GPP access, except when steering mode is set to "Active-Standby", 3GPP access is the active access and Non-3GPP access is not used as Standby access. In the latter case, this IE may be present.<br>(NOTE 1) | - | - | - | X | - | Non-3GPP Access Forwarding Action Information |
| Threshold Values | C | This IE shall be present if the steering mode is "Load Balancing" with fixed split percentages or "Priority-based" and if available.<br><br>When present, this IE shall contain the RTT and/or a Packet Loss Rate.<br>(NOTE 2) | - | - | - | X | - | Thresholds |
| Steering Mode Indicator | C | This IE shall be included if at least one of the flags is set to "1":<br>- ALBI (Autonomous Load Balancing Indicator): this flag shall be set to "1" if the SMF allows the UPF to apply autonomous load-balance when the Steering Mode is Load-Balancing;<br><br>- UEAI (UE Assistance Indicator): this flag shall be set to "1" if the SMF allows UE assistant load-balance when the Steering Mode is Load-Balancing.<br><br>(NOTE 2) | - | - | - | X | - | Steering Mode Indicator |

NOTE 1: For the "Active-Standby" steering mode, if the network determines to not define a Standby access (as specified in clause 5.32.8 of 3GPP TS 23.501 [28]), the SMF shall either set the Priority IE within (Non-)3GPP Access Forwarding Action Information IE to the value "No Standby" or not include the (Non-)3GPP Access Forwarding Action Information IE for that access not defined as Standby access.
NOTE 2: The Threshold Values IE and the Steering Mode Indicator IE shall not be present together.

**Table 7.5.2.8-2: 3GPP Access Forwarding Action Information IE in the Create MAR IE**

| Octet 1 and 2 | 3GPP Access Forwarding Action Information 1 IE Type = 166 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| FAR ID | M | This IE shall uniquely identify the FAR among all the FARs configured for this PFCP session. | - | - | - | X | - | FAR ID |
| Weight | C | This IE shall be present if steering mode is set to "Load Balancing" to identify the weight of the FAR. (NOTE 1) | - | - | - | X | - | Weight |
| Priority | C | This IE shall be present if the steering mode is set to "Active-Standby" or "Priority-based". (NOTE 2) | - | - | - | X | - | Priority |
| URR ID | C | This IE shall uniquely identify the URR among all the URRs configured for the PFCP session. This enables the SMF to request separate usage reports for different FARs (i.e. different accesses) (NOTE 3)<br><br>Several IEs within the same IE type may be present to represent a list of URRs to be associated to the FAR. | - | - | - | X | - | URR ID |
| RAT Type | O | This IE may be present to provide the UP Function the current RAT Type for the DL FAR for statistics purpose. | - | - | - | X | - | RAT Type |

NOTE 1: The weights for all FARs included in both 3GPP Access Forwarding Action Information and Non 3GPP Access Forwarding Action Information need to sum up to 100. If the autonomous load balance operation is allowed, the Weights shall be treated as the default percentages.

NOTE 2: The Priority value shall be set to "Active", "Standby" or "No Standby" if the Steering Mode is set to "Active-Standby"; the Priority value shall be set to "High" or "Low" if the Steering Mode is set to "Priority-based". The 3GPP Access Forwarding Action Information and Non 3GPP Access Forwarding Action Information shall set different values.

NOTE 3: One or more URRs may still be provisioned in the Create PDR IE when an MAR ID is present, while the URR(s) provisioned in this IE shall present a different set of URR(s) to request separate usage reports.

**Table 7.5.2.8-3: Non-3GPP Access Forwarding Action Information IE in the Create MAR IE**

| Octet 1 and 2 | Non-3GPP Access Forwarding Action Information IE Type = 167 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Same IEs and requirements as defined in Table 7.5.2.8-2 | | | | | | | | |

## 7.5.2.9 Create SRR IE within PFCP Session Establishment Request

The Create SRR grouped IE shall be encoded as shown in Figure 7.5.2.9-1.

**Table 7.5.2.9-1: Create SRR IE within PFCP Session Establishment Request**

| Octet 1 and 2 | Create SRR IE Type = 212 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| SRR ID | M | This IE shall uniquely identify the SRR among all the SRRs configured for this PFCP session. | - | - | - | X | - | SRR ID |
| Access Availability Control Information | C | This IE shall be present if the UPF needs to report when an access type becomes available or not available (see clause 5.20.4.2). | - | - | - | X | - | Access Availability Control Information |
| QoS Monitoring per QoS flow Control Information | C | This IE shall be present if the per QoS Flow per UE QoS monitoring reporting is triggered.<br>Several IEs within the same IE type may be present to represent a list of QoS Monitoring per QoS flow Control Information for different QoS flows. | - | - | - | X | - | QoS Monitoring per QoS flow Control Information |
| Direct Reporting Information | C | This IE shall be present if the UPF indicated support of the DRQOS feature and if the QoS monitoring events shall be reported by the UPF directly to a Local NEF or AF, or both to the SMF and Local NEF/AF (see clause 5.33.5).<br>(NOTE) | - | - | - | X | - | Direct Reporting Information |
| NOTE: In this release of the specification, the Direct Reporting Information shall only be used for direct reporting of QoS monitoring per QoS flow. | | | | | | | | |

The Access Availability Control Information IE shall be encoded as shown in Table 7.5.2.9-2.

**Table 7.5.2.9-2: Access Availability Control Information**

| Octet 1 and 2 | Access Availability Control Information = 216 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Requested Access Availability Information | M | This IE shall indicate the requested information to be reported. | - | - | - | X | - | Requested Access Availability Information |

The QoS Monitoring per QoS flow Control Information IE shall be encoded as shown in Table 7.5.2.9-3.

**Table 7.5.2.9-3: QoS Monitoring per QoS flow Control Information**

| Octet 1 and 2 | QoS Monitoring per QoS flow Control Information = 242 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| QFI | M | This IE shall identify the QoS Flow Identifier for which QoS monitoring is required.<br>Several IEs within the same IE type may be present to represent different QoS flows. | - | - | - | X | - | QFI |
| Requested QoS Monitoring | M | This IE shall indicate whether the uplink, downlink and/or round trip packet delay between the UE and the UPF (PSA) shall be monitored, and whether QoS monitoring is performed based on GTP-U path monitoring. | - | - | - | X | - | Requested QoS Monitoring |
| Reporting Frequency | M | This IE shall indicate the frequency for the reporting, i.e. event triggered, periodic, or when the PDU Session is released. | - | - | - | X | - | Reporting Frequency |
| Packet Delay Thresholds | C | This IE shall be present if event triggered QoS monitoring reporting is used and reporting is required upon reaching a delay threshold. When present, it shall indicate the packet delay after which the UP function shall report QoS monitoring result to the CP function or Local NEF or AF for this SRR.<br>(NOTE 1) | - | - | - | X | - | Packet Delay Thresholds |
| Minimum Wait Time | C | This IE shall be present if event triggered QoS monitoring reporting is required. When present, it shall indicate the minimum waiting time between two consecutive reports after which the UP function may report new QoS monitoring result to the CP function or Local NEF or AF for this SRR. | - | - | - | X | - | Minimum Wait Time |
| Measurement Period | C | This IE shall be present if the periodic QoS monitoring reporting is required. When present, it shall indicate the period for generating and reporting QoS monitoring reports.<br>(NOTE 2) | - | - | - | X | - | Measurement Period |
| NOTE 1: If no time stamp is received in uplink packet for a delay exceeding the Packet Delay Thresholds, the UP function shall generate a QoS monitoring report indicating a packet delay measurement failure to the CP function or Local NEF or AF.<br>NOTE 2: If no time stamp is received in uplink packet for a delay exceeding the Measurement Period, the UP function shall generate a QoS monitoring report indicating a packet delay measurement failure to the CP function or Local NEF or AF. | | | | | | | | |

The Direct Reporting Information IE shall be encoded as shown in Table 7.5.2.9-4.

**Table 7.5.2.9-4: Direct Reporting Information**

| Octet 1 and 2 | Direct Reporting Information = 295 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Event Notification URI | M | This IE shall contain the notification URI to be used for sending the UPF event notifications. | - | - | - | X | - | Event Notification URI |
| Notification Correlation ID | C | This IE shall indicate the notification correlation id to be included in the UPF event notifications. It shall be present if it is available. | - | - | - | X | - | Notification Correlation ID |
| Reporting Flags | | This IE shall be included if at least one of the flags is set to "1".<br>- DUPL (Duplicate notification): this IE shall be set to "1" if event notifications shall be sent over N4 and directly to the notification URI indicated in the Event Notification URI IE. When this flag is set to "0", this indicates that the UPF shall only send the event notifications directly to the notification URI indicated in the Event Notification URI IE. | - | - | - | X | - | Reporting Flags |

### 7.5.2.10 Provide ATSSS Control Information IE within PFCP Session Establishment Request

The Provide ATSSS Control Information grouped IE shall be encoded as shown in Figure 7.5.2.10-1.

**Table 7.5.2.10-1: Provide ATSSS Control Information IE within PFCP Session Establishment Request**

| Octet 1 and 2 | Provide ATSSS Control Information IE Type = 220 (decimal) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| MPTCP Control Information | C | This IE shall be present if the PDU session is an MA PDU session and the MPTCP functionality is required. | - | - | - | X | - | MPTCP Control Information |
| ATSSS-LL Control Information | C | This IE shall be present if the PDU session is an MA PDU session and the ATSSS-LL functionality is required. | - | - | - | X | - | ATSSS-LL Control Information |
| PMF Control Information | C | This IE shall be present if the PDU session is an MA PDU session and the PMF functionality is required. | - | - | - | X | - | PMF Control Information |

### 7.5.2.11 Provide RDS Configuration Information IE within PFCP Session Establishment Request

The Provide RDS Configuration Information IE shall be encoded as shown in Figure 7.5.2.11-1.

**Table 7.5.2.11-1: Provide RDS Configuration Information IE within PFCP Session Establishment Request**

| Octet 1 and 2 | Provide RDS Configuration Information IE Type = 261 (decimal) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| RDS Configuration Information | O | When present, this IE indicates if the RDS mechanism is supported. | - | X | - | X | - | RDS Configuration Information |

## 7.5.3 PFCP Session Establishment Response

### 7.5.3.1 General

The PFCP Session Establishment Response shall be sent over the Sxa, Sxb, Sxc and N4 interface by the UP function to the CP function as a reply to the PFCP Session Establishment Request.

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

| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
|---|---|---|---|---|---|---|---|---|
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | X | X | Node ID |
| Cause | M | This IE shall indicate the acceptance, partial acceptance or rejection of the corresponding request message. | X | X | 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 | X | X | Offending IE |
| UP F-SEID | C | This IE shall be present if the cause is set to "Request accepted (success)". When present, it shall contain the unique identifier allocated by the UP function identifying the session. | X | X | 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 a local F-TEID or a UE IP address/prefix for the PDR.<br>When present, this IE shall contain the PDR information associated to the PFCP session. There may be several instances of this IE.<br>See table 7.5.3.2-1. | X | X | - | 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 | 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 | X | X | Overload Control Information |
| PGW-U/SGW-U /UPF FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24] and clause 4.6 of 3GPP TS 23.527 [40]. | X | X | - | 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 | X | X | Failed Rule ID |
| Created Traffic Endpoint | C | This IE shall be present if the cause is set to "success" and the UP function was requested to allocate a local F-TEID or a UE IP address/prefix in a Create Traffic Endpoint IE. When present, it shall contain the local F-TEID or UE IP address/prefix to be used for this Traffic Endpoint.<br>There may be several instances of this IE. | X | X | - | X | X | Created Traffic Endpoint |
| Created Bridge Info for TSC | C | This IE shall be present if the UPF was requested to provide Bridge information for TSC in the PFCP Session Establishment Request. When present, it shall contain the Bridge information for TSC for the PFCP session.<br>See Table 7.5.3.6-1. | - | - | - | X | - | Created Bridge Info for TSC |
| ATSSS Control Parameters | C | This IE shall be present if ATSSS functionality is required in the request message and the UPF allocates the resources and parameters corresponding to the required ATSSS functionality.<br>See Table 7.5.3.7-1. | - | - | - | X | - | ATSSS Control Parameters |
| RDS configuration information | O | When present, this IE shall contain the RDS configuration information the UP function supported for this PFCP session. | - | X | - | X | - | RDS configuration information |
| Partial Failure Information | C | This IE shall be present if the Cause IE indicates partial acceptance of the request to provide failure information related to a failed rule. See Table 7.5.3.1-2.<br>Several IEs within the same IE type may be present to report failures to apply multiple rules. | - | X | X | X | X | Partial Failure Information |
| Created L2TP Session | O | This IE may be present to include information for the Created L2TP session if the Cause IE indicates a success. | - | X | - | X | - | Created L2TP Session |
| MBS Session N4mb Information | C | This IE shall be present if any IE in this grouped IE needs to be included. | - | - | - | - | X | MBS Session N4mb Information |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| MBS Session N4 Information | C | This IE shall be included if any IE in this grouped IE needs to be included as specified in clause 5.34.1.<br><br>Several IE with the same IE type may be present to contain N4 Information for several MBS Sessions respectively. | - | - | - | X | - | MBS Session N4 Information |

**Table 7.5.3.1-2: Information Elements in a Partial Failure Information**

| Octet 1 and 2 | Partial Failure Information IE Type = 272 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |
| Failed Rule ID | M | This IE shall indicate the rule that failed to be applied. | - | X | X | X | X | Failed Rule ID |
| Failure Cause | M | This IE shall indicate the reason why the rule could not be applied. | - | X | X | X | X | Cause |
| Offending IE Information | M | This IE shall be included to report the offending IE which caused the rule activation failure, e.g. an unknown predefined rule name included in Activate Predefined Rules IE or an unknown Application ID in the PDI.<br>Several IEs within the same IE type may be present to report multiple offending IEs. | - | X | X | X | X | Offending IE Information |

**Table 7.5.3.1-3: Created L2TP Session IE in the PFCP Session Establishment Response message**

| Octet 1 and 2 | Created L2TP Session IE Type = 279 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| DNS Server Address | O | This IE may be present to include a DNS server address.<br><br>Several IEs with the same IE type may be present to represent multiple DNS server addresses.<br><br>The order of the IEs in the message indicates the priority, i.e. the first IE shall contain the primary DNS server address and the second IE shall contain the secondary DNS server address. | - | X | - | X | - | DNS Server Address |
| NBNS Server Address | O | This IE may be present to include an NBNS server address.<br>Several IEs with the same IE type may be present to represent multiple NBNS server addresses.<br><br>The order of the IEs in the message indicates the priority, i.e. the first IE shall contain the primary NBNS server address and the second IE shall contain the secondary NBNS server address. | - | X | - | X | - | NBNS Server Address |
| LNS Address | O | This IE may be present to include the used Tunnel Server Endpoint, i.e., the LNS IP address, for the PFCP Session. | - | X | - | X | - | LNS Address |

**Table 7.5.3.1-4: MBS Session N4mb Information IE within PFCP Session Establishment Response**

| Octet 1 and 2 | MBS Session N4 Information IE Type = 303 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Multicast Transport Information | C | This IE shall be present to include a low layer source specific multicast address information (i.e. multicast destination address and related source IP address) and a GTP-U Common Tunnel EndPoint Identifier (C-TEID) if the CP function has requested to allocate such information for multicast transport over N3mb and/or N19mb. | - | - | - | - | X | Multicast Transport Information |

**Table 7.5.3.1-5: MBS Session N4 Information IE within PFCP Session Establishment Response**

| Octet 1 and 2 | MBS Session N4 Information IE Type = 311 (decimal) | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |
| MBS Session Identifier | M | | - | - | - | X | - | MBS Session Identifier |
| Area Session ID | C | This IE shall be present for a location dependent MBS service. When present, it shall contain the Area Session ID, which together with the MBS Session Identifier, uniquely identify the service area part of the content data of the MBS service. | - | - | - | X | - | Area Session ID |
| N19mb DL Tunnel ID | C | This IE shall be present when the SMF has requested the UPF to allocate a Local F-TEID in the PDI or in the Create Traffic Endpoint IE. (NOTE 1) | - | - | - | X | - | F-TEID |
| MBSN4Resp-Flags | C | This IE shall be included if at least one of the flags is set to "1". NOTE 2.<br>- NN19DT (New N19mb Downlink Tunnel): the UPF shall set this flag if it has allocated a new N19mb DL TEID for the MBS session;<br>- JMTI (Joined N19mb Multicast Tree Indication): the UPF shall set this flag if it has joined the multicast tree from the MB-UPF;<br>- N19DTR (N19mb Downlink Tunnel Removal): the UPF shall set this flag if it is about to remove the N19mb DL Tunnel for receiving the MBS session data. | - | - | - | X | - | MBSN4Resp-Flags |
| NOTE 1: The UPF need not include Created PDR or Created Traffic Endpoint to return the newly allocated N19mb DL TEID.<br>NOTE 2: Clause 5.34.3.2 explains what is indicated by the absence of the MBSN4Resp-Flags. | | | | | | | | | |

## 7.5.3.2 Created PDR IE within PFCP 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 PFCP 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** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| PDR ID | M | | X | X | - | 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 | - | X | - | F-TEID |
| Local F-TEID for Redundant Transmission | C | This IE shall be present and shall contain the local F-TEID used for this PDR for the reception of redundant uplink packets on N3/N9 interfaces, if the CP function requested a Local F-TEID to be assigned for redundant transmission. | - | - | - | X | - | F-TEID |
| UE IP Address | C | If the UP function allocates the UE IP address/prefix, this IE shall be present and shall contain the UE IP address/ prefix assigned by the UP function.<br>In the 5GC, several IEs with the same IE type may be present to represent multiple UE IP addresses, if the UPF indicated support of the IP6PL feature (see clause 5.21). | - | X | - | X | - | UE IP Address |
| Local Ingress Tunnel | C | If the UP function allocates the Local Ingress Tunnel, this IE shall be present and shall contain the Local Ingress Tunnel to be used for this PDR. | - | - | - | - | X | Local Ingress Tunnel |

### 7.5.3.3 Load Control Information IE within PFCP 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 PFCP Session Establishment Response**

| Octet 1 and 2 | Load Control Information IE Type = 51 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Load Control Sequence Number | M | See clause 6.2.3.3.2 for the description and use of this parameter. | X | X | X | X | X | Sequence Number |
| Load Metric | M | See clause 6.2.3.3.2 for the description and use of this parameter. | X | X | X | X | X | Metric |

### 7.5.3.4 Overload Control Information IE within PFCP 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 PFCP 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** | **N4** | **N4 mb** | |
| Overload Control Sequence Number | M | See 6.2.4.3.2 for the description and use of this parameter. | X | X | X | X | X | Sequence Number |
| Overload Reduction Metric | M | See clause 6.2.4.3.2 for the description and use of this parameter. | X | X | X | X | X | Metric |
| Period of Validity | M | See clause 6.2.4.3.2 for the description and use of this parameter. | X | X | 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 | X | X | OCI Flags |

### 7.5.3.5 Created Traffic Endpoint IE within PFCP Session Establishment Response

The Created Traffic Endpoint grouped IE shall be encoded as shown in Figure 7.5.3.5-1.

**Table 7.5.3.5-1: Created Traffic Endpoint IE within PFCP Session Establishment Response**

| Octet 1 and 2 | Created Traffic Endpoint IE Type = 128 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4mb** | |
| Traffic Endpoint ID | M | This IE shall uniquely identify the Traffic Endpoint for that PFCP session. | X | X | - | X | X | Traffic Endpoint 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 Traffic Endpoint. | X | X | - | X | - | F-TEID |
| Local F-TEID for Redundant Transmission | C | This IE shall be present and shall contain the local F-TEID to be used for this PDR for the reception of redundant uplink packets on N3/N9 interfaces, if the CP function requested a Local F-TEID to be assigned for redundant transmission. | - | - | - | X | - | F-TEID |
| UE IP Address | C | If the UP function allocates the UE IP address/prefix, this IE shall be present and shall contain the UE IP address/ prefix assigned by the UP function.<br>In the 5GC, several IEs with the same IE type may be present to represent multiple UE IP addresses, if the UPF indicated support of the IP6PL feature (see clause 5.21). | - | X | - | X | - | UE IP Address |
| Local Ingress Tunnel | C | If the UP function allocates the Local Ingress Tunnel, this IE shall be present and shall contain the Local Ingress Tunnel to be used for this PDR. | - | - | - | - | X | Local Ingress Tunnel |

### 7.5.3.6 Created Bridge Info for TSC IE within PFCP Session Establishment Response

The Created Bridge Info for TSC grouped IE shall be encoded as shown in Figure 7.5.3.6-1.

**Table 7.5.3.6-1: Created Bridge Info for TSC IE within PFCP Session Establishment Response**

| Octet 1 and 2 | Created Bridge Info for TSC IE Type = 195 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4mb** | |
| DS-TT Port Number | C | If the BII bit was set to "1" in the Create Bridge Info for TSC IE, this IE shall be present and shall contain the DS-TT Port Number assigned by the UP function. | - | - | - | X | - | DS-TT Port Number |
| 5GS User Plane Node | C | If the BII bit was set to "1" in the Create Bridge Info for TSC IE, this IE shall be present and shall contain the 5GS User Plane Node assigned by the UP function. | - | - | - | X | - | 5GS User Plane Node |

### 7.5.3.7 ATSSS Control Parameters IE within PFCP Session Establishment Response

The ATSSS Control Parameters grouped IE shall be encoded as shown in Figure 7.5.3.7-1.

**Table 7.5.3.7-1: ATSSS Control Parameters IE within PFCP Session Establishment Response**

| Octet 1 and 2 | ATSSS Control Parameters IE Type = 221 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| MPTCP Parameters | C | This IE shall be present if the TCI flag in the MPTCP Control Information IE is set to "1" in the Request message and the UPF allocated resources for MPTCP. | - | - | - | X | - | MPTCP Parameters |
| ATSSS-LL Parameters | C | This IE shall be present if the LLI flag in ATSSS-LL Control Information IE is set to "1" in the Request message and the UPF allocated resources for ATSSS-LL. | - | - | - | X | - | ATSSS-LL Parameters |
| PMF Parameters | C | This IE shall be present if the PMFI flag in the PFM Control Information IE is set to "1" in the Request message and the UPF allocated resources for PMF. Several IEs with the same IE type may be present to provide multiple PMF Parameters. | - | - | - | X | - | PMF Parameters |

The MPTCP Parameters grouped IE shall be encoded as shown in Figure 7.5.3.7-2.

**Table 7.5.3.7-2: MPTCP Parameters IE within PFCP Session Establishment Response**

| Octet 1 and 2 | MPTCP Parameters IE Type = 225 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| MPTCP Address Information | M | This IE shall carry the information of allocated MPTCP address. | - | - | - | X | - | MPTCP Address Information |
| UE Link-Specific IP Address | M | This IE shall carry the information of allocated UE link-specific IP address for MPTCP. | - | - | - | X | - | UE Link-Specific IP Address |

The ATSSS-LL Parameters grouped IE shall be encoded as shown in Figure 7.5.3.7-3.

**Table 7.5.3.7-3: ATSSS-LL Parameters IE within PFCP Session Establishment Response**

| Octet 1 and 2 | ATSSS-LL Parameters IE Type = 226 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| ATSSS-LL Information | M | This IE shall indicate that resources have been allocated to the ATSSS functionality. | - | - | - | X | - | ATSSS-LL Information |

The PMF Parameters grouped IE shall be encoded as shown in Figure 7.5.3.7-4.

**Table 7.5.3.7-4: PMF Parameters IE within PFCP Session Establishment Response**

| Octet 1 and 2 | PMF Parameters IE Type = 227 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| PMF Address Information | M | This IE shall contain the PMF Address Information. | - | - | - | X | - | PMF Address Information |
| QoS flow identifier | O | If present, this IE shall identify the QoS Flow Identifier of the QoS flow related to the PMF address information. | - | - | - | X | - | QFI |

### 7.5.3.8 Void

## 7.5.4 PFCP Session Modification Request

### 7.5.4.1 General

The PFCP Session Modification Request is used over the Sxa, Sxb, Sxc, N4 and N4mb interface by the CP function to request the UP function to modify the PFCP session.

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CP F-SEID | C | This IE shall be present if the CP function decides to change its F-SEID for the PFCP session. The UP function shall use the new CP F-SEID for subsequent PFCP Session related messages for this PFCP Session. See Note 2. | X | X | 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 7.5.4-6-1. Several IEs within the same IE type may be present to represent a list of PDRs to remove. | X | X | 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 7.5.4-7-1. Several IEs within the same IE type may be present to represent a list of FARs to remove. | X | X | X | X | X | Remove FAR |
| Remove URR | C | When present, this shall contain the URR Rule which is requested to be removed. See Table 7.5.4-8-1. Several IEs within the same IE type may be present to represent a list of URRs to remove. | X | 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 7.5.4-9-1. Several IEs within the same IE type may be present to represent a list of QERs to remove. | - | X | X | 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 | - | - | X | - | Remove BAR |
| Remove Traffic Endpoint | C | When present, this IE shall contain the Traffic Endpoint ID identifying the traffic endpoint to be removed, if the UP function has indicated support of PDI optimization. All the PDRs that refer to the removed Traffic Endpoint shall be deleted. See Table 7.5.4.14-1. Several IEs within the same IE type may be present to represent a list of Traffic Endpoints to remove. | X | X | X | X | X | Remove Traffic Endpoint |
| Create PDR | C | This IE shall be present if the CP function requests the UP function to create a new PDR. See Table 7.5.2.2-1. Several IEs within the same IE type may be present to represent a list of PDRs to create. | X | X | 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. Several IEs within the same IE type may be present to represent a list of FARs to create. | X | X | 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. Several IEs within the same IE type may be present to represent a list of URRs to create. | X | 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. Several IEs within the same IE type may be present to represent a list of QERs to create. | - | X | X | 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. See Table 7.5.2.6-1. | X | - | - | X | - | Create BAR |
| Create Traffic Endpoint | C | When present this IE shall contain the information associated with the Traffic Endpoint to be created, if the UP function has indicated support of PDI optimization. See Table 7.5.2.7-1. Several IEs within the same IE type may be present to represent a list of Traffic Endpoints to create. | X | X | X | X | X | Create Traffic Endpoint |
| Update PDR | C | This IE shall be present if a PDR previously created for the PFCP session need to be modified. See Table 7.5.4.2-1. Several IEs within the same IE type may be present to represent a list of PDRs to update. | X | X | X | X | X | Update PDR |
| Update FAR | C | This IE shall be present if a FAR previously created for the PFCP session need to be modified. See Table 7.5.4.3-1. Several IEs within the same IE type may be present to represent a list of FARs to update. | X | X | X | X | X | Update FAR |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Update URR | C | This IE shall be present if URR(s) previously created for the PFCP 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.<br>See Table 7.5.4.4-1. | X | X | X | X | - | Update URR |
| Update QER | C | This IE shall be present if QER(s) previously created for the PFCP 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 7.5.4.5-1. | - | X | X | X | X | Update QER |
| Update BAR | C | This IE shall be present if a BAR previously created for the PFCP session needs to be modified.<br>A previously created BAR that is not modified shall not be included.<br>See Table 7.5.4.11-1. | X | - | - | X | - | Update BAR |
| Update Traffic Endpoint | C | When present this IE shall contain the information associated with the traffic endpoint to be updated, if the UP function has indicated support of PDI optimization.<br><br>All the PDRs that refer to the Traffic Endpoint shall use the updated Traffic Endpoint information.<br>See Table 7.5.4.13-1.<br>Several IEs within the same IE type may be present to represent a list of Traffic Endpoints to update. | X | X | X | X | X | Update Traffic Endpoint |
| PFCPSMReq-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 PFCP 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 PFCP session (see NOTE 3).<br>- SUMPC (Stop Usage Measurement to Pause Charging): the CP function, e.g. PGW-C or (H-)SMF, shall set this flag if the usage measurement for the URRs which are applicable for charging (i.e. with the "ASPOC" flag set to "1") shall be stopped in the UP function.<br>- RUMUC (Resume Usage Measurement to Un-pause Charging): the CP function, e.g. PGW-C or (H-)SMF, shall set this flag if the usage measurement for the URRs which are applicable for charging (i.e. with the "ASPOC" flag set to "1") shall be resumed in the UP function.<br>- DETEID (Delete All DL N3mb and/or N19mb F-TEIDs): the MB-SMF shall set this flag to "1" if it requests the MB-UPF to delete all NG-RAN N3mb DL F-TEIDs and all UPF N19mb DL F-TEIDs for the MBS session when the Apply Action is changed from the "FSSM and/or MBSU" to the "BUFF" (with or without "NOCP"), or to "DROP" (see clause 5.34.2.4). | X<br>X<br>-<br>-<br>- | -<br>X<br>X<br>X<br>X | -<br>X<br>-<br>-<br>- | X<br>X<br>X<br>X<br>X | -<br>-<br>-<br>-<br>- | PFCPSMReq-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 | X | - | Query URR |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| PGW-C/SMF FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24] and clause 4.6 of 3GPP TS 23.527 [40]. | X | 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 |
| User Plane Inactivity Timer | C | This IE shall be present if it needs to be changed. | - | X | X | X | X | User Plane Inactivity Timer |
| Query URR Reference | O | This IE may be present if the Query URR IE is present or the QAURR flag is set to "1". When present, it shall contain a reference identifying the query request, which the UP function shall return in any usage report sent in response to the query. | X | X | X | X | - | Query URR Reference |
| Trace Information | O | When present, this IE shall contain the trace instructions to be applied by the UP function for this PFCP session. A Trace Information with a null length indicates that the trace session shall be deactivated. | X | X | X | X | - | Trace Information |
| Remove MAR | C | When present, this IE shall contain the MAR Rule which is requested to be removed. See Table 7.5.4.15-1. Several IEs within the same IE type may be present to represent a list of MARs to remove. | - | - | - | X | - | Remove MAR |
| Update MAR | C | This IE shall be present if an MAR previously created for the PFCP session needs to be modified. See Table 7.5.4.16-1.<br><br>Several IEs within the same IE type may be present to represent a list of MARs to update. | - | - | - | X | - | Update MAR |
| Create MAR | C | This IE shall be present if the CP function requests the UP function to create a new MAR for a new PDR. See Table 7.5.2.8-1.<br><br>Several IEs within the same IE type may be present to represent a list of MARs to create. | - | - | - | X | - | Create MAR |
| Node ID | C | This IE shall be present if a new SMF in an SMF Set, with one PFCP association per SMF and UPF (see clause 5.22.3), takes over the control of the PFCP session. When present, it shall contain the unique identifier of the new SMF. | - | - | - | X | X | Node ID |
| TSC Management Information | C | This IE shall be present if the SMF needs to send TSC Management information to the UPF. Several IEs within the same IE type may be present to transfer PMICs for different NW-TT ports. (NOTE 6). | - | - | - | X | - | TSC Management Information |
| Remove SRR | C | When present, this shall indicate the SRR Rule which is requested to be removed. See Table 7.5.4-19-1. Several IEs within the same IE type may be present to represent a list of SRRs to remove. | - | - | - | X | - | Remove SRR |
| Create SRR | C | This IE shall be present if the CP function requests the UP function to create a new SRR. See Table 7.5.2.9-1. Several IEs within the same IE type may be present to represent a list of SRRs to create. | - | - | - | X | - | Create SRR |
| Update SRR | C | This IE shall be present if SRR(s) previously created for the PFCP session need to be modified. Several IEs within the same IE type may be present to represent a list of modified SRRs. Previously SRRs that are not modified shall not be included. See Table 7.5.4.20-1. | - | - | - | X | - | Update SRR |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Provide ATSSS Control Information | C | This IE shall be present for PFCP session modification for an MA PDU session, if the ATSSS Control Information changes.<br>When present, this IE shall contain the required ATSSS functionalities for this MA PDU session.<br>The UPF shall replace any value received previously by the new information received in this IE. See Note 4.<br>See Table 7.5.2.10-1. | - | - | - | X | - | Provide ATSSS Control Information |
| Ethernet Context Information | C | This IE shall be present to update the list of MAC addresses associated to the PDU session during an Ethernet PDU session anchor relocation. | - | - | - | X | - | Ethernet Context Information |
| Access Availability Information | O | This IE may be present for an MA PDU session to signal that an access type has become transiently unavailable or has become available again (see clause 5.20.5).<br>Two IEs with the same IE type may be present to report changes of access availability for both 3GPP and non-3GPP accesses. | - | - | - | X | - | Access Availability Information |
| Query Packet Rate Status | C | This IE shall be present if the CP function requests immediate packet rate status report(s) to the UP function.<br>Several IEs within the same IE type may be present to represent a list of QERs for which an immediate packet rate status report is requested.<br>See Table 7.5.4.22-1. | - | X | - | X | - | Query Packet Rate Status |
| S-NSSAI | O | This IE may be present to indicate the S-NSSAI of the PDU session or MBS session, if the S-NSSAI of the PDU Session or MBS session has been provided previously to the UP function and the S-NSSAI has changed. (NOTE 5) | - | - | - | X | X | S-NSSAI |
| RAT Type | | This IE shall be present if there is a RAT change and the CP function wants to inform the UP Function about the new RAT Type if the PFCP session is not established for a MA PDU session. | X | X | - | X | - | RAT Type |
| Group Id | C | This IE shall be included by the CP function to indicate the new group identifier to which the PFCP session pertains, if it has been changed (see clause 5.22.4).<br><br>When present, the UP function shall replace any earlier value associated to the PFCP session with the new value. | - | X | - | X | - | Group Id |
| MBS Session N4 Control Information | C | This IE shall be included if:<br>- the correspond PDU session is being associated with an MBS session, or with an MBS session and Area Session ID for a location dependent MBS service; or<br><br>- the PDU session is already associated with an MBS session, or with an MBS session and Area Session ID for a location dependent MBS service, and the N19mb multicast transport information has changed. In this case, the Multicast Transport Information IE shall contain the new multicast transport information to use to receive MBS session data from the MB-UPF.<br><br>Several IEs with the same IE type may be present to provide N4 control information for several MBS sessions, e.g. when the UE requests to join several MBS sessions.<br><br>See Table 7.5.2.1-5 for encoding. | - | - | - | X | - | MBS Session N4 Control Information |
| DSCP to PPI Control Information | C | This IE shall be present if the DSCP to PPI Control Information needs to be changed. The UPF shall replace any value received previously by the new information received in this IE.<br><br>See Table 7.5.2.1-6 for encoding. | - | - | - | X | - | DSCP to PPI Control Information |

NOTE 1: The CP function may request the UP function to drop the packets currently buffered for the PFCP 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 a PFCP 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 PFCP session to request the UP function to start buffering the downlink data packets with notifying the arrival of subsequent downlink data packets. See clause 5.9.3 of 3GPP TS 23.214 [2].

NOTE 2: When changing the CP F-SEID of an established PFCP Session, the CP function shall be able to handle any incoming PFCP 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 PFCPSMReq-Flags IE and the Query URR IE are exclusive from each other in a PFCP Session Modification Request.

NOTE 4: If the ATSSS resources have already been allocated to the PFCP session previously, e.g. during the PFCP session establishment, the UPF shall not allocate new values for such resources (e.g. UE Link-Specific IP Address).

NOTE 5: S-NSSAI for the PDU session may be updated after PDU session establishment, i.e. during EPS to 5GS handover procedure, the initial AMF may use configured S-NSSAI for interworking to create the PDU session in 5GS. For home routed PDU session, if the S-NSSAI in serving PLMN (mapped from S-NSSAI in HPLMN) is different from the configured S-NSSAI for interworking and V-SMF reselection is not needed, the AMF will update V-SMF with S-NSSAI in serving PLMN for the PDU session, as specified in clause 4.11.1.3.3 of 3GPP TS 23.502 [29]. The S-NSSAI may also be updated by SMF+PGW-C during EPS to 5GS handover in non-roaming or roaming-with-LBO case. The S-NSSAI may be used by the UP function for performance measurement.

NOTE 6: When transferring port and user plane node management information between the TSN AF or the TSCTSF and the NW-TT, since the NW-TT may support multiple ports, there may be several instances of the TSC Management Information IEs containing a Port Management Information Container together with a NW-TT Port Number, and only one instance of the TSC Management Information IE containing a User Plane Node Management Information Container that may also contain a Port Management Information Container together with a NW-TT Port Number.

### 7.5.4.2 Update PDR IE within PFCP 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 PFCP 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** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| PDR ID | M | This IE shall uniquely identify the PDR among all the PDRs configured for that PFCP session. | X | X | X | X | X | PDR ID |
| Outer Header Removal | C | This IE shall be present if it needs to be changed. | X | X | - | 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 PFCP session, when looking for a PDR matching an incoming packet. | - | X | X | 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 | X | X | PDI |
| FAR ID | C | This IE shall be present if it needs to be changed | X | X | 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 | 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 | 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. When present this IE shall contain one Predefined Rules name.<br>Several IEs with the same IE type may be present to represent multiple "Activate Predefined Rules" names. | - | X | 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. When present this IE shall contain one Predefined Rules name.<br>Several IEs with the same IE type may be present to represent multiple "Activate Predefined Rules" names. | - | X | X | X | - | Deactivate Predefined Rules |
| Activation Time | O | This IE may be present if the PDR activation time shall be changed. (NOTE 2) | - | X | X | X | - | Activation Time |
| Deactivation Time | O | This IE may be present if the PDR deactivation time shall be changed. (NOTE 2) | - | X | X | X | - | Deactivation Time |
| IP Multicast Addressing Info | O | This IE may be present in an UL PDR controlling UL IGMP/MLD traffic (see clause 5.25), if it needs to be changed<br>When present, it shall contain a (range of) IP multicast address(es), and optionally source specific address(es), identifying a set of IP multicast flows. See Table 7.5.2.2-4.<br>Several IEs with the same IE type may be present to represent multiple IP multicast flows.<br>When present, the UPF shall replace any IP multicast address(es) previously stored for this PDR by the IP multicast address(es) received in this IE. | - | - | - | X | - | IP Multicast Addressing Info |
| Transport Delay Reporting | C | This IE shall be present if Transport Delay Reporting needs to be changed (e.g. transport delay reporting needs to be activated or deactivated). See Table 7.5.2.2-6. | - | - | - | X | - | Transport Delay Reporting |
| RAT Type | O | This IE may be present if there is a RAT change for the UL PDR if the PFCP session is established for a MA PDU session. | - | - | - | X | - | RAT Type |
| NOTE1: 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.<br>NOTE2: When the Activation Time and Deactivation Time are not present, the PDR shall keep its current activation status, either active or inactive. | | | | | | | | |

### 7.5.4.3 Update FAR IE within PFCP 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 PFCP 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** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4mb** | |
| FAR ID | M | This IE shall identify the FAR to be updated. | X | X | X | X | X | FAR ID |
| Apply Action | C | This IE shall be present if it is changed. | X | X | 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 | X | - | Update Forwarding Parameters |
| Update Duplicating Parameters | C | This IE shall be present if it is changed. See table 7.5.4.3-3.<br>Several IEs with the same IE type may be present to request to duplicate the packets to different destinations. | X | X | - | - | - | Update Duplicating Parameters |
| Redundant Transmission Forwarding Parameters | C | This IE shall be present if it is changed. See table 7.5.2.3-4. | - | - | - | X | - | Redundant Transmission Forwarding Parameters |
| BAR ID | C | This IE shall be present if the BAR ID associated to the FAR needs to be modified. | X | - | - | X | - | BAR ID |
| Add MBS Unicast Parameters | C | This IE shall be present when the Apply Action is set to "MBSU" to request the MB-UPF to forward the MBS session data to a remote GTP-U peer for unicast transport, if no remote GTP-U peers are provisioned yet in the MB-UPF, or if additional GTP-U peers need to be provisioned. (NOTE).<br><br>Several IEs with the same IE type may be present to represent multiple remote GTP-U peers.<br><br>See Table 7.5.2.3-6. | - | - | - | - | X | Add MBS Unicast Parameters |
| Remove MBS Unicast Parameters | C | This IE shall be present when the MB-SMF to request the MB-UPF to delete a remote GTP-U peer to stop forwarding the MBS session data to that remote GTP-U peer for unicast transport.<br><br>Several IEs with the same IE type may be present to represent to delete multiple remote GTP-U peers. | - | - | - | - | X | Remove MBS Unicast Parameters |
| NOTE: When the Apply Action is changed to “MBSU” during an MBS session reactivation, remote GTP-U peers may already be provisioned in the MB-UPF if the MB-SMF did not request the MB-UPF to delete the N3mb/N19mb DL F-TEIDs when the MBS session was deactivated (see clause 5.34.2.4). | | | | | | | | |

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

| 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** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 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 | X | - | Destination Interface |
| Network instance | C | This IE shall only be provided if it is changed. | X | 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 | X | - | Redirect Information |
| Outer Header Creation | C | This IE shall only be provided if it is changed.<br>See NOTE 1. | X | X | - | X | - | Outer Header Creation |
| Transport Level Marking | C | This IE shall only be provided if it is changed | X | X | - | X | - | Transport Level Marking |
| Forwarding Policy | C | This IE shall only be provided if it is changed.<br>See NOTE 1. | - | X | X | X | - | Forwarding Policy |
| Header Enrichment | C | This IE shall only be provided if it is changed | - | X | X | X | - | Header Enrichment |
| PFCPSMReq-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 | - | X | - | PFCPSMReq-Flags |
| Linked Traffic Endpoint ID | C | This IE may be present, if it is changed and the UP function indicated support of the PDI optimization feature, (see clause 8.2.25). When present, it shall identify the Traffic Endpoint ID allocated for this PFCP session to receive the traffic in the reverse direction (see clause 5.2.3.1). | X | X | - | X | - | Traffic Endpoint ID |
| Destination Interface Type | C | This IE shall be present to indicate the 3GPP interface type of the destination interface, if the value has changed. | X | X | - | X | - | 3GPP Interface Type |
| Data Network Access Identifier | C | This IE shall be provided over N16a if it is changed. This IE shall not be sent over N4. | - | - | - | - | - | Data Network Access Identifier |
| IP Address and Port Number Replacement | C | This IE shall only be provided if it is changed. | - | - | - | X | - | IP Address and Port Number Replacement |
| NOTE 1: If the Outer Header Creation and Forwarding Policy are present, the UP function shall put the user plane packets in the user plane tunnel by applying Outer Header Creation, after enforcing the required Forwarding Policy. | | | | | | | | |

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

| 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** | **N4** | **N4 mb** | |
| 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 | - | - | - | Destination Interface |
| Outer Header Creation | C | This IE shall only be provided if it is changed.<br>See NOTE 1. | 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.<br>See NOTE 1. | - | X | - | - | - | Forwarding Policy |
| NOTE 1: If the Outer Header Creation and Forwarding Policy are present, the UP function shall put the user plane packets in the user plane tunnel by applying Outer Header Creation, after enforcing the required Forwarding Policy. | | | | | | | | |

**Table 7.5.4.3-4: Remove MBS Unicast Parameters IE in the Update FAR IE**

| Octet 1 and 2 | Remove MBS Unicast Parameters Type = 304 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sxa** | **Sxb** | **Sxc** | **N4** | **N4 mb** | |
| MBS Unicast Parameters ID | M | This IE shall identify the MBS Unicast Parameters IE to be removed. | - | - | - | - | X | MBS Unicast Parameters ID |

## 7.5.4.4 Update URR IE within PFCP 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 PFCP 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** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| URR ID | M | This IE shall uniquely identify the URR among all the URRs configured for that PFCP session | X | 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 | 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, or when an SMF instructs an UPF to report the reception of the End Marker packet from the old I-UPF during a Service Request procedure (see clauses 4.2.3.2 and 4.23.4.3 in 3GPP TS 23.502 [29]). | X | 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 | 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 | 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 | 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 | 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 | X | - | Time Quota |
| Event Threshold | C | This IE shall be present if Event Threshold needs to be modified.<br>When present, it shall indicate the number of events after which the UP function shall report to the CP function for this URR. | - | X | X | X | - | Event Threshold |
| Event Quota | C | This IE shall be present if Event Quota needs to be modified.<br>When present, it shall indicate the Event Quota value. | - | X | X | X | - | Event 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 | 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 | - | - | X | - | Dropped DL Traffic Threshold |
| Quota Validity Time | C | This IE shall be present if Quota Validity time was not sent earlier or quota validity time value needs to be modified. | - | X | - | X | - | Quota Validity Time |
| 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 | 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 | 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 | X | X | - | Subsequent Time Threshold |
| Subsequent Volume Quota | C | This IE shall be present if the Subsequent Volume Quota needs to be modified.<br>When present, it shall indicate the Volume Quota value which the UP function shall use for this URR for the period after the Monitoring Time. | - | X | X | X | - | Subsequent Volume Quota |
| Subsequent Time Quota | C | This IE shall be present if the Subsequent Time Quota needs to be modified.<br>When present, it shall indicate the Time Quota value which the UP function shall use for this URR for the period after the Monitoring Time. | - | X | X | X | - | Subsequent Time Quota |
| Subsequent Event Threshold | O | This IE shall be present if the Subsequent Event Threshold needs to be modified.<br>When present, it shall indicate the number of events after which the UP function shall report to the CP function for this URR for the period after the Monitoring Time. | - | X | X | X | - | Subsequent Event Threshold |
| Subsequent Event Quota | O | This IE shall be present if the Subsequent Event Quota needs to be modified.<br>When present, it shall indicate the Event Quota value which the UP function shall use for this URR for the period after the Monitoring Time. | - | X | X | X | - | Subsequent Event Quota |
| 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 | 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 clause 5.2.2.4).<br><br>Several IEs with the same IE type may be present to represent multiple linked URRs which are related with this URR. | - | X | X | X | - | Linked URR ID |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Measurement Information | C | This IE shall be included if any of the following flag is set to "1" or if the change of flag(s) from "1" to "0" results in the IE becoming set to all zeros.<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.<br>- Reduced Application Detection Information Flag: this flag may be set to "1", if the Reporting Triggers request to report the start or stop of application, to request the UP function to only report the Application ID in the Application Detection Information, e.g. for envelope reporting.<br>- Immediate Start Time Metering Flag: this flag may be set to "1" if time-based measurement is used and the UP function is requested to start the time metering immediately at receiving the flag.<br>- Send Start Pause of Charging Flag: this flag may be set to "1" by the CP function if the UP Function is requested to send a Start Pause of Charging indication to the upstream GTP-U entity(s) when the Dropped DL Traffic Threshold is reached.<br>- Applicable for Start of Pause of Charging Flag: this flag may be set to "1" if the URR is applicable for Start of Pause of Charging, so that the UP function shall stop the usage measurement for the URR when receiving Start Pause of Charging indication from the peer downstream GTP-U entity.<br>- Control of Inactive Measurement Flag: the flag shall be set to "1" if the CP function requests the UP function to stop or resume the usage measurement for the URR with the "ASPOC" flag set to "1" according to the value of Inactive Measurement Flag. | - | X | - | X | - | Measurement Information |
| | | | X | - | - | X | X | |
| | | | - | X | X | X | - | |
| | | | - | X | - | X | - | |
| | | | - | X | - | X | - | |
| 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 |
| Aggregated URRs | C | This IE shall be included if the Aggregated URRs IE needs to be modified. See Table 7.5.2.4-2.<br><br>Several IEs with the same IE type may be present to provision multiple aggregated URRs.<br><br>When present, this IE shall provide the complete list of the aggregated URRs. | - | X | - | - | - | Aggregated URRs |
| FAR ID for Quota Action | C | This IE shall be present if the FAR ID for Quota Action IE needs to be modified. This IE may be present if the Volume Quota IE or the Time Quota IE or Event Quota IE is newly provisioned in the URR and the UP Function indicated support of the Quota Action.<br>When present, it shall contain the identifier of the substitute FAR the UP function shall apply, for the traffic associated to this URR, when exhausting any of these quotas. See NOTE 1, NOTE 2. | - | X | X | X | - | FAR ID |
| Ethernet Inactivity Timer | C | This IE shall be present if the Ethernet Inactivity Timer needs to be modified. When present, it shall contain the duration of the Ethernet inactivity period. | - | - | - | X | - | Ethernet Inactivity Timer |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Additional Monitoring Time | O | This IE shall be present if the additional 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 or event threshold/quota. See Table 7.5.2.4-3.<br>The CP function shall provide the full set of Additional Monitoring Times IE(s). The UP function shall replace any Additional Monitoring Times IE(s) provisioned earlier by the new set of received IE(s). | X | X | X | X | - | Additional Monitoring Time |
| Number of Reports | O | This IE may be present if the Number of Reports need to be changed. When present, it shall indicate the number of usage reports to be generated by the URR. See also clauses 5.2.2.2.1 and 5.2.2.3.1. | X | X | X | X | - | Number of Reports |
| Exempted Application ID for Quota Action | C | This IE shall be present if Application ID for Quota Action needs to be changed.<br><br>When present, it shall contain an Application ID matching packets that shall be exempted from applying the FAR ID for Quota Action when the quota has been exhausted.<br><br>Several IEs with the same IE type may be present to provide multiple Application IDs.<br><br>The CP function shall always provide a complete list of Application IDs.<br><br>See NOTE 3. | - | X | X | X | - | Application ID |
| Exempted SDF Filter for Quota Action | C | This IE shall be present if the SDF Filter for Quota Action needs to be changed.<br><br>When present, it shall contain a SDF Filter matching packets that shall be exempted from applying the FAR ID for Quota Action when the quota has been exhausted.<br><br>Several IEs with the same IE type may be present to provide multiple SDF Filters.<br><br>The CP function shall always provide a complete list of SDF Filters.<br><br>See NOTE 3. | - | X | X | X | - | SDF Filter |
| User Plane Inactivity Timer | C | This IE shall be present if the User Plane Inactivity Timer needs to be modified.<br>When present, it shall contain the duration of the User Plane Inactivity Timer. | - | - | - | X | - | User Plane Inactivity Timer |

NOTE 1: The substitute FAR used when exhausting a Volume Quota or Time Quota may be set to drop the packets or redirect the traffic towards a redirect destination as specified in clause 5.4.7.

NOTE 2: If the FAR as indicated in the FAR ID for Quota Action is removed after being provisioned, the UP function shall behave as if the FAR ID for Quota Action is not provisioned and shall apply the default behaviour per local configuration when the quota is exhausted.

NOTE 3: The Exempted Application ID for Quota Action IE or Exempted Filter ID for Quota Action IE may be provisioned as the Restricted-Filter-Rule AVP or Filter ID AVP which is included in Final-Unit-Indication AVP from the online charging system when the Final-Unit-Action AVP is set to "REDIRECT" or "RESTRICT_ACCESS". See also 3GPP TS 32.299 [18].

### 7.5.4.5 Update QER IE within PFCP 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 PFCP 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** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| QER ID | M | This IE shall uniquely identify the QER among all the QRs configured for that PFCP session | - | X | X | 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 | - | 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 | 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>For EPC, 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><br>For 5GC, this IE may be set to the value of:<br>- the Session-AMBR, for a QER that is referenced by all the PDRs of the non-GBR QoS flows of a PDU session;<br>- the QoS Flow MBR, for a QER that is referenced by all the PDRs of a QoS Flow;<br>- the SDF MBR, for a QER that is referenced by all the PDRs of a SDF.<br><br>See NOTE 1. | - | X | X | 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 QoS Flow GBR, for a QER that is referenced by all the PDRs of a QoS Flow (for 5GC);<br>- the SDF GBR, for a QER that is referenced by all the PDRs of a SDF.<br>See NOTE 1. | - | X | X | 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 | - | 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 |
| QoS flow identifier | C | This IE shall be present if it needs to be modified. | - | - | - | X | X | QFI |
| Reflective QoS | C | This IE shall be present if the state of the Reflective QoS needs to be modified (activate if inactive, or deactivate the active Reflective QoS). | - | - | - | X | - | RQI |
| Paging Policy Indicator | C | This IE shall be present if it needs to be modified. | - | - | - | X | - | Paging Policy Indicator |
| Averaging Window | O | This IE may be present if the UP function is required to modify the Averaging Window. (NOTE 2) | - | - | - | X | - | Averaging Window |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| QER Control Indications | C | This IE shall be included if the CP function need to provide the updated QoS enforcement control information:<br>- RCSR (Rate Control Status Reporting): the CP function shall set this bit "1" to request the UP function to report the rate control status when the PFCP session is released. | - | X | - | X | - | QER Control Indications |
| 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.<br>NOTE 2: As 5QI is not signalled over N4, one default averaging window shall be pre-configured in the UPF. | | | | | | | | |

## 7.5.4.6 Remove PDR IE within PFCP Session Modification Request

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

R grouped IE shall be encoded as shown in Figure 7.5.4.6-1.

**Table 7.5.4.6-1: Remove PDR IE within PFCP 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** | **N4** | **N4 mb** | |
| PDR ID | M | This IE shall identify the PDR to be deleted. | X | X | X | X | X | PDR ID |

## 7.5.4.7 Remove FAR IE within PFCP 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 PFCP 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** | **N4** | **N4 mb** | |
| FAR ID | M | This IE shall identify the FAR to be deleted. | X | X | X | X | X | FAR ID |

## 7.5.4.8 Remove URR IE within PFCP 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 PFCP 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** | **N4** | **N4 mb** | |
| URR ID | M | This IE shall identify the URR to be deleted. | X | X | X | X | - | URR ID |

## 7.5.4.9 Remove QER IE PFCP Session Modification Request

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

**T Table 7.5.4.9-1: Remove QER IE PFCP 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** | **N4** | **N4 mb** | |
| QER ID | M | This IE shall identify the QER to be deleted. | - | X | X | X | X | QER ID |

## 7.5.4.10 Query URR IE within PFCP 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 PFCP 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** | **N4** | |
| URR ID | M | This IE shall identify the URR being queried. | X | X | X | X | URR ID |

## 7.5.4.11 Update BAR IE within PFCP 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 PFCP 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** | **N4** | **N4 mb** | |
| BAR ID | M | This IE shall identify the BAR Rule to be modified. | X | - | - | 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 clause 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 | - | - | X | - | Downlink Data Notification Delay |
| Suggested Buffering Packets Count | C | This IE may be present if the UP Function indicated support of the feature UDBC.<br><br>When present, it shall contain the number of packets that are suggested to be buffered when the Apply Action parameter requests to buffer the packets. The packets that exceed the limit shall be discarded. | | X | X | X | - | Suggested Buffering Packets Count |
| MT-EDT Control Information | O | This IE may be included to request the SGW-U to report the sum of DL Data Packets Size. | X | - | - | - | - | MT-EDT Control Information |

## 7.5.4.12 Remove BAR IE within PFCP 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 PFCP 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** | **N4** | **N4 mb** | |
| BAR ID | M | This IE shall identify the BAR to be deleted. | X | - | - | X | - | BAR ID |

## 7.5.4.13 Update Traffic Endpoint IE within PFCP Session Modification Request

The Update Traffic Endpoint grouped IE shall be encoded as shown in Figure 7.5.4.13-1.

**Table 7.5.4.13-1: Update Traffic Endpoint IE within PFCP Session Modification Request**

| Octet 1 and 2 | | Update Traffic Endpoint Type = 129 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Traffic Endpoint ID | M | This IE shall uniquely identify the Traffic Endpoint to be modified for that PFCP session. | X | X | X | X | X | Traffic Endpoint ID |
| Local F-TEID | C | This IE shall be present if it needs to be changed.<br>The CP function shall set the CHOOSE (CH) bit to 1 if the CP function requests the UP function to assign a local F-TEID to the PDR.<br>See NOTE. | X | - | - | X | - | F-TEID |
| Network Instance | O | If present, this IE shall identify the Network instance to match for the incoming packet. See NOTE. | X | X | X | X | X | Network Instance |
| Redundant Transmission Detection Parameters | C | This IE shall be present if it needs to be changed See Table 7.5.2.2-5.<br>See NOTE. | - | - | - | X | - | Redundant Transmission Detection Parameters |
| UE IP address | C | This IE shall be present if it needs to be changed.<br>In the 5GC, several IEs with the same IE type may be present to represent multiple UE IP addresses, if the UPF indicated support of the IP6PL feature (see clause 5.21).<br>When present, the UE IP address(es) present in this IE shall replace the UE IP address(es) stored in the UP function for this traffic endpoint.<br>See NOTE. | - | X | X | X | - | UE IP address |
| Framed-Route | C | This IE shall be present for a PDR if the UPF indicated support of Framed Routing (see clauses 8.2.25 and 5.16) and it needs to be changed. If present, this IE shall describe a framed route.<br><br>Several IEs with the same IE type may be present to provision a list of framed routes. | - | X | - | X | - | Framed-Route |
| Framed-Routing | C | This IE shall be present for a DL PDR if the UPF indicated support of Framed Routing (see clauses 8.2.25 and 5.16) and it needs to be changed. If present, this IE shall describe the routing method for the UP function for the IP route related to Framed-Routes or Framed-IPv6-Routes. (NOTE 2) | - | X | - | X | - | Framed-Routing |
| Framed-IPv6-Route | C | This IE shall be present for a PDR if the UPF indicated support of Framed Routing (see clauses 8.2.25 and 5.16) and it needs to be changed. If present, this IE shall describe a framed IPv6 route.<br>Several IEs with the same IE type may be present to provision a list of framed IPv6 routes. | - | X | - | X | - | Framed-IPv6-Route |
| QFI | C | This IE shall be present if QFI(s) applicable for the traffic endpoints need to be changed and if the UPF has indicated it supports MTE feature as specified in clause 8.2.25.<br><br>If present, this IE shall identify the QoS Flow Identifier to match for the incoming packet.<br>Several IEs with the same IE type may be present to provision a list of QFIs. When present, the full set of applicable QFIs shall be provided. | - | - | - | X | - | QFI |
| Source Interface Type | C | This IE shall be present if the 3GPP interface type of the traffic endpoint needs to be changed. | X | X | - | X | X | 3GPP Interface Type |
| RAT Type | O | This IE may be present if there is a RAT change for the UL PDR(s) if the PFCP session is established for a MA PDU session. | - | - | - | X | - | RAT Type |

NOTE 1: The IEs which do not need to be modified shall not be included in the Update Traffic Endpoint IE. The UP function shall continue to behave according to the values previously received for IEs not present in the Update Traffic Endpoint IE. F-TEID may be changed if the SGW-C has received the "Change F-TEID support Indication" over the S11/S4 interface (for an IDLE state UE initiated TAU/RAU procedure to allow the SGW changing the GTP-U F-TEID).

NOTE 2: In this release of specification, the UP function shall announce the IP route(s) for Framed-Route(s) or Framed-IPv6-Route(s) to the PDN regardless of the value of the Framed-Routing.

### 7.5.4.14 Remove Traffic Endpoint IE within PFCP Session Modification Request

The Remove Traffic Endpoint grouped IE shall be encoded as shown in Figure 7.5.4.14-1.

**Table 7.5.4.14-1: Remove Traffic Endpoint IE within PFCP Session Modification Request**

| Octet 1 and 2 | Remove Traffic Endpoint IE Type = 130 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Traffic Endpoint ID | M | This IE shall identify the Traffic Endpoint to be deleted. | X | X | X | X | X | Traffic Endpoint ID |

### 7.5.4.15 Remove MAR IE within PFCP Session Modification Request

The Remove MAR grouped IE shall be encoded as shown in Figure 7.5.4.15-1.

**Table 7.5.4.15-1: Remove MAR IE within PFCP Session Modification Request**

| Octet 1 and 2 | Remove MAR IE Type = 168 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| MAR ID | M | This IE shall identify the MAR to be deleted. | - | - | - | X | - | MAR ID |

### 7.5.4.16 Update MAR IE within PFCP Session Modification Request

The Update MAR grouped IE shall be encoded as shown in Figure 7.5.4.16-1.

**Table 7.5.4.16-1: Update MAR IE within PFCP Session Modification Request**

| Octet 1 and 2 | Update MAR IE Type = 169 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| MAR ID | M | This IE shall identify the MAR to be updated. | - | - | - | X | - | MAR ID |
| Steering Functionality | C | This IE shall be present if it is changed. | - | - | - | X | - | Steering Functionality |
| Steering Mode | C | This IE shall be present if it is changed. | - | - | - | X | - | Steering Mode |
| Update 3GPP Access Forwarding Action Information | C | This IE shall be present if the 3GPP Access Forwarding Action Information was provisioned previously and if any of IEs is to be changed.<br><br>This IE shall also be present to remove 3GPP Access Forwarding Action Information that was provisioned previously if the UE deregisters from the corresponding access. This shall be done by including this IE with a null length. | - | - | - | X | - | Update 3GPP Access Forwarding Action Information |
| Update Non-3GPP Access Forwarding Action Information | C | This IE shall be present if the Non-3GPP Access Forwarding Action Information was provisioned previously and if any of IEs is to be changed.<br><br>This IE shall also be present to remove the Non-3GPP Access Forwarding Action Information that was provisioned previously if the UE deregisters from the corresponding access. This shall be done by including this IE with a null length. | - | - | - | X | - | Update Non-3GPP Access Forwarding Action Information |
| 3GPP Access Forwarding Action Information | C | This IE shall be present to provision 3GPP access specific forwarding action information when this access is added, i.e. when the UE registers to 3GPP access.<br><br>See Table 7.5.2.8-2. | - | - | - | X | - | 3GPP Access Forwarding Action Information |
| Non-3GPP Access Forwarding Action Information | C | This IE shall be present to provision Non-3GPP access specific forwarding action information when this access is added, i.e. when the UE registers to non-3GPP access. See Table 7.5.2.8-3. | - | - | - | X | - | Non-3GPP Access Forwarding Action Information |
| Threshold values | C | This IE shall be present if it is changed. | - | - | - | X | - | Thresholds |
| Steering Mode Indicator | C | This IE shall be included if any of the following flag is set to "1" or if the change of flag(s) from "1" to "0" results in the IE becoming set to all zeros.<br>Applicable flags are:<br>- ALBI (Autonomous Load Balancing Indicator): this flag shall be set to "1" if the SMF allows the UPF to apply autonomous load-balance when the Steering Mode is Load-Balancing;<br><br>- UEAI (UE Assistance Indicator): this flag shall be set to "1" if the SMF allows UE assistant load-balance when the Steering Mode is Load-Balancing. | - | - | - | X | - | Steering Mode Indicator |

**Table 7.5.4.16-2: Update 3GPP Access Forwarding Action Information IE in Update MAR IE**

| Octet 1 and 2 | Update 3GPP Access Forwarding Action Information IE Type = 175 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| FAR ID | C | This IE shall be present if it is changed. | - | - | - | X | - | FAR ID |
| Weight | C | This IE shall be present if it is changed. | - | - | - | X | - | Weight |
| Priority | C | This IE shall be present if it is changed. | - | - | - | X | - | Priority |
| URR ID | C | This IE shall be present if a measurement action shall be applied or no longer applied to packets for this access.<br><br>When present, this IE shall contain the list of all the URR IDs to be associated to this access. | - | - | - | X | - | URR ID |
| RAT Type | O | This IE may be present if it is changed. | - | - | - | X | - | RAT Type |

**Table 7.5.4.16-3: Update Non-3GPP Access Forwarding Action Information IE in Update MAR IE**

| Octet 1 and 2 | Update Non-3GPP Access Forwarding Action Information IE Type = 176 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Same IEs and requirements as defined in Table 7.5.4.16-2 | | | | | | | | |

## 7.5.4.17 Create PDR/FAR/URR/QER/BAR/MAR IEs within PFCP Session Modification Request

PFCP Session Modification Request message may conditionally include Create PDR IE, Create FAR IE, Create URR IE, Create QER IE, Create BAR IE and Create MAR IE. The encoding of these IEs are specified within PFCP Session Establishment Request message (see clauses 7.5.2.2 – 7.5.2.8).

## 7.5.4.18 TSC Management Information IE within PFCP Session Modification Request

The TSC Management Information grouped IE shall be encoded as shown in Table 7.5.4.18-1.

**Table 7.5.4.18-1: TSC Management Information IE within PFCP Session Modification Request**

| Octet 1 and 2 | TSC Management Information IE Type = 199 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Port Management Information Container | O | When present, this IE shall contain a Port Management Information container. | - | - | - | X | - | Port Management Information Container |
| User Plane Node Management Information Container | O | When present, this IE shall contain an User Plane Node Management Information container. | - | - | - | X | - | User Plane Node Management Information Container |
| NW-TT Port Number | C | When PMIC IE is present, this IE shall contain the related NW-TT Port Number. | - | - | - | X | - | NW-TT Port Number |

## 7.5.4.19 Remove SRR IE within PFCP Session Modification Request

The Remove SRR grouped IE shall be encoded as shown in Table 7.5.4.19-1.

**Table 7.5.4.19-1: Remove SRR IE within PFCP Session Modification Request**

| Octet 1 and 2 | Remove SRR IE Type = 211 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| SRR ID | M | This IE shall identify the SRR to be deleted. | - | - | - | X | - | SRR ID |

## 7.5.4.20 Update SRR IE within PFCP Session Modification Request

The Update SRR grouped IE shall be encoded as shown in Table 7.5.4.20-1.

**Table 7.5.4.20-1: Update SRR IE within PFCP Session Modification Request**

| Octet 1 and 2 | Update SRR IE Type = 213 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| SRR ID | M | This IE shall uniquely identify the SRR among all the SRRs configured for that PFCP session | - | - | - | X | - | SRR ID |
| Access Availability Control Information | C | This IE shall be present if the Access Availability Control Information needs to be modified. See Table 7.5.2.9-2.<br><br>The CP function shall provide the full Access Availability Control Information IE. The UP function shall replace the Access Availability Control Information IE provisioned earlier, if any, by the new received IE. | - | - | - | X | - | Access Availability Control Information |
| QoS Monitoring per QoS flow Control Information | C | This IE shall be present if the QoS Monitoring per QoS flow Control Information needs to be modified. See Table 7.5.2.9-3.<br>The CP function shall provide the full set of QoS Monitoring per QoS flow Control Information IE(s). The UP function shall replace any QoS Monitoring per QoS flow Control Information IE(s) provisioned earlier by the new set of received IE(s).<br>Several IEs within the same IE type may be present to represent a list of QoS Monitoring per QoS flow Control Information for different QoS flows. | - | - | - | X | - | QoS Monitoring per QoS flow Control Information |
| Direct Reporting Information | C | This IE shall be present if the Direct Reporting Information IE needs to be modified. See Table 7.5.2.9-4. | - | - | - | X | - | Direct Reporting Information |

## 7.5.4.21 Ethernet Context Information within PFCP Session Modification Request

The Ethernet Context Information grouped IE shall be encoded as shown in Table 7.5.4.21-1.

**Table 7.5.4.21-1: Ethernet Context Information IE within PFCP Session Modification Request**

| Octet 1 and 2 | Ethernet Context Information IE Type = 254 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| MAC Addresses Detected | M | This IE shall be present if one or more MAC addresses need to be associated to the PDU session.<br>Several IEs with the same IE type may be present to provision multiple lists of MAC addresses (e.g. with different V-LAN tags). | - | - | - | X | - | MAC Addressed Detected |

## 7.5.4.22 Query Packet Rate Status IE within PFCP Session Modification Request

The Query Packet Rate Status grouped IE shall be encoded as shown in Table 7.5.4.22-1.

**Table 7.5.4.22-1: Query Packet Rate Status IE within PFCP Session Modification Request**

| Octet 1 and 2 | Query Packet Rate Status IE Type = 263 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| QER ID | M | This IE shall identify the QER being queried for its Packet Rate Status | - | X | - | X | - | QER ID |

## 7.5.5 PFCP Session Modification Response

### 7.5.5.1 General

The PFCP Session Modification Response shall be sent over the Sxa, Sxb, Sxc and N4 interface by the UP function to the CP function as a reply to the PFCP Session Modification Request.

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sxa | Sxb | Sxc | N4 | N4mb | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Cause | M | This IE shall indicate the acceptance, partial acceptance or rejection of the corresponding request message. | X | X | 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 | 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 or a UE IP address/prefix for the PDR(s).<br>When present, this IE shall contain the PDR information associated to the PFCP session.<br>See Table 7.5.3.2-1.<br>Several IEs within the same IE type may be present to represent a list of created PDRs. | X | X | - | 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 | 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 | X | X | Overload Control Information |
| Usage Report | C | This IE shall be present if:<br>- the Query URR IE was present or the QAURR flag was set to "1" in the PFCP Session Modification Request,<br>- traffic usage measurements for that URR are available at the UP function, and<br>- the UP function decides to return some or all of the requested usage reports in the PFCP Session Modification Response.<br><br>This IE shall be also present if:<br>- a URR or the last PDR associated to a URR has been removed,<br>- non-null traffic usage measurements for that URR are available in the UP function, and<br>- the UP function decides to return some or all of the related usage reports in the PFCP Session Modification Response (see clause 5.2.2.3.1).<br><br>Several IEs within the same IE type may be present to represent a list of Usage Reports. | X | 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 | X | X | Failed Rule ID |
| Additional Usage Reports Information | C | This IE shall be included if the Query URR IE was present or the QAURR flag was set to "1" in the PFCP Session Modification Request, and usage reports need to be sent in additional PFCP Session Report Request messages (see clause 5.2.2.3.1).<br>When present, this IE shall either indicate that additional usage reports will follow, or indicate the total number of usage reports that need to be sent in PFCP Session Report Request messages. | X | X | X | X | - | Additional Usage Reports Information |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Created/Updated Traffic Endpoint | C | This IE shall be present if the cause is set to "success", Traffic Endpoint(s) were requested to be created or updated, and the UP function was requested to allocate the local F-TEID or a UE IP address/prefix for the Traffic Endpoint(s).<br><br>If the UP function allocates additional UE IP address/prefix (upon receiving a Create Traffic Endpoint or Update Traffic Endpoint in the corresponding PFCP Session Modification Request message from the CP function), this IE shall be present and shall contain the complete list of UE IP address / prefix assigned by the UP function for this PFCP session.<br><br>In the 5GC, several IEs with the same IE type may be present to represent multiple UE IP addresses, if the UPF indicated support of the IP6PL feature (see clause 5.21).<br><br>(NOTE 1)<br>When present, this IE shall contain the Traffic Endpoint information associated to the PFCP session.<br>See Table 7.5.3.5-1.<br><br>Several IEs within the same IE type may be present to represent a list of created/updated Traffic Endpoints. | X | X | - | X | X | Created Traffic Endpoint |
| TSC Management Information | C | This IE shall be present if the UPF needs to send TSC Management information to the SMF.<br>Several IEs within the same IE type may be present to transfer PMICs for different NW-TT ports. (NOTE 2). | - | - | - | X | - | TSC Management Information |
| ATSSS Control Parameters | C | This IE shall be present if ATSSS functionality is required in the request message, and the UPF allocates the resources and parameters corresponding to the required ATSSS functionality.<br>See Table 7.5.3.7-1. | - | - | - | X | - | ATSSS Control Parameters |
| Updated PDR | C | This IE shall be present if a Update PDR is present in the corresponding PFCP Session Modification Request and UP function is requested to allocate a new F-TEID, e.g. to support the redundant transmission on N3/N9 interfaces, or move the application traffic from a default bearer to a new dedicated bearer, or the UP function is requested to assign additional UE IP Address or Prefix, e.g. a shorter than /64 prefix delegation. See Table 7.5.5.5-1.<br>Several IEs within the same IE type may be present to represent a list of updated PDRs. | - | X | - | X | - | Updated PDR |
| Packet Rate Status Report | C | This IE shall be present if the CP function has requested to report an immediate packet rate status in the PFCP Session Modification Request and the UP function supports the CIOT feature (see clause 8.2.25).<br>Several IEs within the same IE type may be present to represent a list of Packet Rate Status Reports. | - | X | - | X | - | Packet Rate Status Report |
| Partial Failure Information | C | This IE shall be present if the Cause IE indicates partial acceptance of the request to provide failure information related to a failed rule.<br>Several IEs within the same IE type may be present to report failures to apply multiple rules.<br><br>See Table 7.5.3.1-2. | - | X | X | X | X | Partial Failure Information |
| MBS Session N4 Information | C | This IE shall be included if any IE in this grouped IE needs to be included as specified in clause 5.34.1.<br><br>Several IE with the same IE type may be present to contain N4 Information for several MBS Sessions.<br><br>See Table 7.5.3.1-5 for encoding. | - | - | - | X | - | MBS Session N4 Information |

NOTE 1: The UP function supporting the PDI optimization feature and the IP6PL feature (see clause 8.2.25) shall support providing the complete list of UE IP Address IEs in the Created/Updated Endpoint IE.
NOTE 2: When transferring port and user plane node management information between the TSN AF or the TSCTSF and the NW-TT, since the NW-TT may support multiple ports, there may be several instances of the TSC Management Information IEs containing a Port Management Information Container together with a NW-TT Port Number, and only one instance of the TSC Management Information IE containing a User Plane Node Management Information Container that may also contain a Port Management Information Container together with a NW-TT Port Number.

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

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

**Table 7.5.5.2-1: Usage Report IE within PFCP 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** | **N4** | **N4 mb** | |
| URR ID | M | This IE shall identify the URR for which usage is reported. | X | X | X | X | - | URR ID |
| UR-SEQN | M | This IE shall uniquely identify the Usage Report for the URR (see clause 5.2.2.3). | X | X | X | X | - | UR-SEQN |
| Usage Report Trigger | M | This IE shall identify the trigger for this report. | X | X | X | X | - | Usage Report Trigger |
| Start Time | C | This IE shall be present, except if the Usage Report Trigger indicates 'Start of Traffic', 'Stop of Traffic' or 'MAC Addresses Reporting'.<br>When present, this IE shall provide the timestamp when the collection of the information in this report was started. | X | X | X | X | - | Start Time |
| End Time | C | This IE shall be present, except if the Usage Report Trigger indicates 'Start of Traffic', 'Stop of Traffic' or 'MAC Addresses Reporting'.<br>When present, this IE shall provide the timestamp when the collection of the information in this report was generated. | X | X | X | X | - | End Time |
| Volume Measurement | C | This IE shall be present if a volume measurement needs to be reported. | X | X | X | X | - | Volume Measurement |
| Duration Measurement | C | This IE shall be present if a duration measurement needs to be reported. | X | 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 | X | - | Usage Information |
| Query URR Reference | C | This IE shall be present if this usage report is sent as a result of a query URR received in a PFCP Session Modification Request and the Query URR Reference IE was present in the PFCP Session Modification Request.<br>When present, it shall be set to the Query URR Reference value received in the PFCP Session Modification Request. | X | X | X | X | - | Query URR Reference |
| Ethernet Traffic Information | C | This IE shall be present if Ethernet Traffic Information needs to be reported. | - | - | - | X | - | Ethernet Traffic Information |

### 7.5.5.3 TSC Management Information IE within PFCP Session Modification Response

The TSC Management Information grouped IE shall be encoded as shown in Table 7.5.5.3-1.

**Table 7.5.5.3-1: TSC Management Information IE within PFCP Session Modification Response**

| Octet 1 and 2 | TSC Management Information IE Type = 200 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Port Management Information Container | O | When present, this IE shall contain a Port Management Information container. | - | - | - | X | - | Port Management Information Container |
| User Plane Node Management Information Container | O | When present, this IE shall contain an User Plane Node Management Information container. | - | - | - | X | - | User Plane Node Management Information Container |
| NW-TT Port Number | C | When PMIC IE is present, this IE shall contain the related NW-TT Port Number. | - | - | - | X | - | NW-TT Port Number |

## 7.5.5.4 Packet Rate Status Report IE within PFCP Session Modification Response

The Packet Rate Status Report grouped IE shall be encoded as shown in Table 7.5.5.4-1.

**Table 7.5.5.4-1: Packet Rate Status Report IE within PFCP Session Modification Response message**

| Octet 1 and 2 | Packet Rate Status Report IE Type = 264 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| QER ID | M | This IE shall uniquely identify a QER in a PFCP session. | - | X | - | X | - | QER ID |
| Packet Rate Status | M | This IE shall indicate the remaining validity time and the remaining number of UL/DL packets that still can be sent. | - | X | - | X | - | Packet Rate Status |

## 7.5.5.5 Updated PDR IE within PFCP Session Modification Response

The Updated PDR grouped IE shall be encoded as shown in Table 7.5.5.5-1.

**Table 7.5.5.5-1: Updated PDR IE in PFCP Session Modification Response**

| Octet 1 and 2 | Updated PDR IE Type = 256 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| PDR ID | M | This IE shall uniquely identify the PDR among all the PDRs configured for that PFCP session. | - | - | - | X | - | PDR ID |
| Local F-TEID for Redundant Transmission | C | This IE shall be present and shall contain the local F-TEID to be used for this PDR for the reception of redundant uplink packets on the N3/N9 interfaces. | - | - | - | X | - | F-TEID |
| 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 | - | - | - | F-TEID |
| UE IP Address | C | If the UP function allocates additional UE IP address/prefix (upon receiving a Update PDR in the corresponding PFCP Session Modification Request message from the CP function), this IE shall be present and shall contain the complete list of UE IP address / prefix assigned by the UP function for this PFCP session.<br><br>In the 5GC, several IEs with the same IE type may be present to represent multiple UE IP addresses, if the UPF indicated support of the IP6PL feature (see clause 5.21). | - | X | - | X | - | UE IP Address |

## 7.5.6 PFCP Session Deletion Request

The PFCP Session Deletion Request shall be sent over the Sxa, Sxb, Sxc and N4 interface by the CP function to request the UP function to delete the PFCP session. The PFCP Header for Session Related Messages shall contain the F-SEID identifying the PFCP session (see clause 6.3.4.2).

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |
| | | | | | | | | |

## 7.5.7 PFCP Session Deletion Response

### 7.5.7.1 General

The PFCP Session Deletion Response shall be sent over the Sxa, Sxb, Sxc and N4 interface by the UP function to the CP function as a reply to the PFCP Session Deletion Request.

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

| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
|---|---|---|---|---|---|---|---|---|
| | | | Sx a | Sx b | Sx c | N4 | N4 mb | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | 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 | 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 | 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 | 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 PFCP 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 | X | - | Usage Report |
| Additional Usage Reports Information | C | This IE shall be included if the usage reports need to be sent in additional PFCP Session Report Request messages (see clause 5.2.2.3.1). When present, this IE shall either indicate that additional usage reports will follow, or indicate the total number of usage reports that need to be sent in PFCP Session Report Request messages. | X | X | X | X | - | Additional Usage Reports Information |
| Packet Rate Status Report | C | This IE shall be present if the CP function has requested in a QER to report the packet rate status when the PFCP session is released and the UP function supports CIOT feature. (See clause 8.2.25) | - | X | - | X | - | Packet Rate Status Report |
| Session Report | C | This IE shall be present if a SRR for QoS monitoring had been provisioned in the UP function for the PFCP session being deleted and QoS monitoring measurements for that SRR are available at the UP function. See Table 7.5.8. 6-1. Several IEs within the same IE type may be present to represent a list of Session Reports. | - | - | - | X | - | Session Report |
| MBS Session N4 Information | C | This IE shall be included if any IE in this grouped IE needs to be included as specified in clause 5.34.1.<br><br>Several IE with the same IE type may be present to contain N4 Information for several MBS Sessions.<br><br>See Table 7.5.3.1-5 for encoding. | - | - | - | X | - | MBS Session N4 Information |
| PFCPSDRsp-Flags | C | This IE shall be included if at least one of the flags is set to "1".<br><br>- PURU (Pending Usage Reports Unacknowledged): the UP function shall set this flag if the UP function has pending PFCP Session Report Request messages which have not been acknowledged yet when it sends the PFCP Session Deletion Response message. | X | X | X | X | - | PFCPSDRsp-Flags |

**Table 7.5.7.1-2: Packet Rate Status Report IE within PFCP Session Deletion Response message**

| Octet 1 and 2 | Packet Rate Status Report IE Type = 252 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| QER ID | M | This IE shall uniquely identify a QER in a PFCP session. | - | X | - | X | - | QER ID |
| Packet Rate Status | M | This IE shall indicate the remaining validity time and the remaining number of UL/DL packets that still can be sent. | - | X | - | X | - | Packet Rate Status |

### 7.5.7.2 Usage Report IE within PFCP Session Deletion Response

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

**Table 7.5.7.2-1: Usage Report IE within PFCP 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** | **N4** | **N4 mb** | |
| URR ID | M | This IE shall identify the URR for which usage is reported. | | X | X | X | X | - | URR ID |
| UR-SEQN | M | This IE shall uniquely identify the Usage Report for the URR (see clause 5.2.2.3). | | X | X | X | X | - | UR-SEQN |
| Usage Report Trigger | M | This IE shall identify the trigger for this report. | | X | X | X | X | - | Usage Report Trigger |
| Start Time | C | This IE shall be present, except if the Usage Report Trigger indicates 'Start of Traffic', 'Stop of Traffic' or 'MAC Addresses Reporting'.<br>When present, this IE shall provide the timestamp when the collection of the information in this report was started. | | X | X | X | X | - | Start Time |
| End Time | C | This IE shall be present, except if the Usage Report Trigger indicates 'Start of Traffic', 'Stop of Traffic' or 'MAC Addresses Reporting'.<br>When present, this IE shall provide the timestamp when the collection of the information in this report was generated. | | X | X | X | X | - | End Time |
| Volume Measurement | C | This IE shall be present if a volume needs to be reported. | | X | X | X | X | - | Volume Measurement |
| Duration Measurement | C | This IE shall be present if a duration measurement needs to be reported. | | X | 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 | X | - | Usage Information |
| Ethernet Traffic Information | C | This IE shall be present if Ethernet Traffic Information needs to be reported. See Table 7.5.8.3-3. | | - | - | - | X | - | Ethernet Traffic Information |

## 7.5.8 PFCP Session Report Request

### 7.5.8.1 General

The PFCP Session Report Request shall be sent over the Sxa, Sxb, Sxc, N4 and N4mb interface by the UP function to report information related to a PFCP session to the CP function.

**Table 7.5.8.1-1: Information Elements in a PFCP Session Report Request**

| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
|---|---|---|---|---|---|---|---|---|
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Report Type | M | This IE shall indicate the type of the report. | X | X | X | X | X | Report Type |
| Downlink Data Report | C | This IE shall be present if the Report Type indicates a Downlink Data Report. | X | - | - | X | 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 | X | - | Usage Report |
| Error Indication Report | C | This IE shall be present if the Report Type indicates an Error Indication Report. | X | X | - | 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 | 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 | X | X | Overload Control Information |
| Additional Usage Reports Information | C | This IE shall be included in one of the additional PFCP Session Report Request messages, if the PFCP Session Modification Response or the PFCP Session Deletion Response indicated that more usage reports would follow (i.e. if the AURI flag was set to "1") (see clause 5.2.2.3.1).<br>When present, this IE shall indicate the total number of usage reports that need to be sent in all the additional PFCP Session Report Request messages.<br>This IE may also be included in every additional PFCP Session Report Request message but the last one, with the AURI flag set to 1, to indicate that more usage reports will follow in additional PFCP Session Report Request message. | X | X | X | X | - | Additional Usage Reports Information |
| PFCPSRReq-Flags | C | This IE shall be included if at least one of the flags is set to "1".<br>- PSDBU (PFCP Session Deleted By the UP function):<br>- if both the CP function and UP function support the EPFAR feature,the UP function may set this flag if the UP function needs to delete the PFCP session, e.g. to report all remaining non-zero usage reports for all URRs in the PFCP Session and the PFCP session is being deleted locally in the UP function.<br>- the UP function shall also set this flag when sending the last PFCP Session Report Request message after having received a PFCP Session Deletion Request (see clause 5.2.2.3.1). | X | X | X | X | - | PFCPSRReq-Flags |
| Old CP F-SEID | C | This IE shall be present if the UPF sends the PFCP Session Report Request to a different SMF in an SMF Set. See clauses 5.22.2 and 5.22.3.<br>When present, it shall indicate the CP F-SEID assigned by the previous SMF to the PFCP session. | - | - | - | X | X | F-SEID |
| Packet Rate Status Report | C | This IE shall be present if the EPFAR is used (see clause 5.18), UP function initiates a PFCP Session release and the CP function has requested in a QER to report the packet rate status when the PFCP session is released.<br>See Table 7.5.7.1-1. | - | X | - | X | - | Packet Rate Status Report |
| TSC Management Information | C | This IE shall be present if the Report Type indicates TSC Management Information Report.<br>Several IEs within the same IE type may be present to transfer PMICs for different NW-TT ports. (NOTE). | - | - | - | X | - | TSC Management Information |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Session Report | C | This IE shall be present if the Report Type indicates a Session Report. See Table 7.5.8.6-1.<br>Several IEs within the same IE type may be present to represent a list of Session Reports. | - | - | - | X | - | Session Report |
| Cause | O | This IE may be present to provide additional reason for sending the PFCP Session Report Request message, e.g. for a UP function initiated PFCP session deletion due to the corresponding L2TP session being terminated. | - | X | - | X | - | Cause |
| NOTE: When transferring port and user plane node management information between the TSN AF or the TSCTSF and NW-TT, since the NW-TT may support multiple ports, there may be several instances of the TSC Management Information IEs containing a Port Management Information Container together with a NW-TT Port Number, and only one instance of the TSC Management Information IE containing a User Plane Node Management Information Container that may also contain a Port Management Information Container together with a NW-TT Port Number. | | | | | | | | |

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

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

**Table 7.5.8.2-1: Downlink Data Report IE within PFCP 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** | **N4** | **N4 mb** | |
| PDR ID | M | This IE shall identify the PDR for which downlink data packets have been received or discarded at the UP function.<br><br>More than one IE with this type may be included to represent multiple PDRs having received or discarded downlink data packets. | X | - | - | X | X | PDR ID |
| Downlink Data Service Information | C | This IE shall be included for a PFCP session with an IP PDN type, if the UP function supports the Paging Policy Differentiation feature (see clause 4.9 of 3GPP TS 23.401 [14]) and clause 5.4.3.2 of 3GPP TS 23.501 [28]).<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>For 5GC, this IE shall also be included over N4, for each PDR and for each packet that triggers a Downlink Data Notification, if the QFI of the downlink data packet is available.<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 | - | - | X | - | Downlink Data Service Information |
| DL Data Packets Size | O | This IE may be present if the SGW-U supports the MT-EDT feature and is requested to report the sum of the DL Data Packets Size. | X | - | - | - | - | DL Data Packets Size |
| DL Data Status | O | This IE may be present if the first downlink data packet has been buffered or discarded at the UP function for downlink data delivery status notification. | - | - | - | X | - | Data Status |

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

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

**Table 7.5.8.3-1: Usage Report IE within PFCP 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** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| URR ID | M | This IE shall identify the URR for which usage is reported. | X | X | X | X | - | URR ID |
| UR-SEQN | M | This IE shall uniquely identify the Usage Report for the URR (see clause 5.2.2.3). | X | X | X | X | - | UR-SEQN |
| Usage Report Trigger | M | This IE shall identify the trigger for this report. | X | X | X | X | - | Usage Report Trigger |
| Start Time | C | This IE shall be present, except if the Usage Report Trigger indicates 'Start of Traffic', 'Stop of Traffic' or 'MAC Addresses Reporting'.<br>When present, this IE shall provide the timestamp when the collection of the information in this report was started. | X | X | X | X | - | Start Time |
| End Time | C | This IE shall be present, except if the Usage Report Trigger indicates 'Start of Traffic', 'Stop of Traffic' or ' MAC Addresses Reporting'.<br>When present, this IE shall provide the timestamp when the collection of the information in this report was generated. | X | X | X | X | - | End Time |
| Volume Measurement | C | This IE shall be present if a volume measurement needs to be reported. (NOTE 2) | X | X | X | X | - | Volume Measurement |
| Duration Measurement | C | This IE shall be present if a duration measurement needs to be reported. (NOTE 2) | X | X | X | X | - | Duration Measurement |
| Application Detection Information | C | This IE shall be present if application detection information needs to be reported. | - | X | 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 | 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 | 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 | X | - | Usage Information |
| Query URR Reference | C | This IE shall be present if this usage report is sent as a result of a query URR received in a PFCP Session Modification Request and the Query URR Reference IE was present in the PFCP Session Modification Request.<br>When present, it shall be set to the Query URR Reference value received in the PFCP Session Modification Request. | X | X | X | X | - | Query URR Reference |
| Event Time Stamp | C | This IE shall be present, if the report is related to an event.<br>When present, it shall be set to the time when the event occurs.<br>Several IEs with the same IE type may be present to report multiple occurrences for an event for this URR ID. | - | X | X | X | - | Time Stamp |
| Ethernet Traffic Information | C | This IE shall be present if Ethernet Traffic Information needs to be reported. See Table 7.5.8.3-3. | - | - | - | X | - | Ethernet Traffic Information |
| Join IP Muticast Information | C | This IE shall be present if the UPF needs to report that it has added the PDU session to the DL replication tree of a new IP multicast flow.<br>Several IEs with the same IE type may be present to report multiple IP multicast flows added to the PDU session. | - | - | - | X | - | Join IP Multicast Information |
| Leave IP Muticast Information | C | This IE shall be present if the UPF needs to report that it has removed the PDU session from the DL replication tree of an IP multicast flow.<br>Several IEs with the same IE type may be present to report multiple IP multicast flows removed from the PDU session. | - | - | - | X | - | Leave IP Multicast Information |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Predefined Rules Name | O | This IE may be present to identify a predefined rule if the usage report is generated for a predefined URR which was activated via a Activate Predefined Rules IE in a Create PDR IE or an Update PDR IE.<br><br>Several IEs with the same IE type may be present to represent multiple Predefined Rules with which the URR is associated. | - | X | - | X | - | Predefined Rules Name |
| 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.<br>NOTE 2: The UP function may send a Usage Report with the Volume/Duration Measurement set to zero. | | | | | | | | |

**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** | **N4** | **N4 mb** | |
| Application ID | M | This IE shall identify the Application ID for which a start or stop of traffic is reported. | - | X | 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 Reduced Application Detection Information flag was not set in the Measurement Information and if the flow information for the detected application is deducible. It shall be present, when reporting the stop of an application, if the Reduced Application Detection Information flag was not set in the Measurement Information and if it was provided when reporting the start of the application. | - | X | 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 Reduced Application Detection Information flag was not set in the Measurement Information and if the flow information for the detected application is deducible. | - | X | X | X | - | Flow Information |
| PDR ID | O | When present, it shall contain the PDR ID which the application traffic matches. | - | X | X | X | - | PDR ID |

**Table 7.5.8.3-3: Ethernet Traffic Information IE within Usage Report IE**

| Octet 1 and 2 | Ethernet Traffic Information IE Type = 143 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | | **Appl.** | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| MAC Addresses Detected | C | This IE shall be present if one or more new MAC addresses have been detected.<br>When present, it shall identify the MAC (Ethernet) addresses newly detected as source address of frames sent UL by the UE.<br>Several IEs with the same IE type may be present to to provision multiple lists of MAC addresses (e.g. with different V-LAN tags). | - | - | - | X | - | MAC Addresses Detected |
| MAC Addresses Removed | C | This IE shall be present if one or more new MAC addresses have been removed.<br>When present, it shall identify the MAC (Ethernet) addresses that have been inactive for a duration exceeding the Ethernet inactivity Timer.<br>Several IEs with the same IE type may be present to to provision multiple lists of MAC addresses (e.g. with different V-LAN tags). | - | - | - | X | - | MAC Addresses Removed |

**Table 7.5.8.3-4: Join IP Multicast Information IE within Usage Report IE**

| Octet 1 and 2 | Join IP Multicast Information IE Type = 189 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | | **Appl.** | | | | **IE Type** |
| | | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| IP Multicast Address | M | This IE shall contain the IP multicast address of the DL multicast flow added to the PDU session. | - | - | - | X | - | IP Multicast Address |
| Source IP Address | C | This IE shall contain the source specific IP address of the DL multicast flow added to the PDU session, if available. Several IEs with the same IE type may be present to represent multiple source specific addresses. | - | - | - | X | - | Source IP Address |

**Table 7.5.8.3-5: Leave IP Multicast Information IE within Usage Report IE**

| Octet 1 and 2 | Leave IP Multicast Information IE Type = 190 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | | **Appl.** | | | | **IE Type** |
| | | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| IP Multicast Address | M | This IE shall contain the IP multicast address of the DL multicast flow removed from the PDU session. | - | - | - | X | - | IP Multicast Address |
| Source IP Address | C | This IE shall contain the source specific IP address of the DL multicast flow removed from the PDU session, if available.<br>Several IEs with the same IE type may be present to represent multiple source specific addresses. | - | - | - | X | - | Source IP Address |

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

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

**Table 7.5.8.4-1: Error Indication Report IE within PFCP 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** | **N4** | **N4 mb** | |
| 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 | - | X | X | F-TEID |

### 7.5.8.5 TSC Management Information IE within PFCP Session Report Request

The TSC Management Information grouped IE shall be encoded as shown in Table 7.5.8.5-1.

**Table 7.5.8.5-1: TSC Management Information IE within PFCP Session Report Request**

| Octet 1 and 2 | TSC Management Information IE Type = 201 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Port Management Information Container | O | When present, this IE shall contain a Port Management Information container. | - | - | - | X | - | Port Management Information Container |
| User Plane Node Management Information Container | O | When present, this IE shall contain an User Plane Node Management Information container. | - | - | - | X | - | User Plane Node Management Information Container |
| NW-TT Port Number | C | When PMIC IE is present, this IE shall contain the related NW-TT Port Number. | - | - | - | X | - | NW-TT Port Number |

### 7.5.8.6 Session Report IE within PFCP Session Report Request

The Session Report grouped IE shall be encoded as shown in Table 7.5.8.6-1.

**Table 7.5.8.6-1: Session Report IE within PFCP Session Report Request**

| Octet 1 and 2 | Session Report IE Type = 214 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| SRR ID | M | This IE shall identify the SRR for which usage is reported. | - | - | - | X | - | SRR ID |
| Access Availability Report | C | This IE shall be present if change of access availability needs to be reported. When present, this IE shall indicate an access type and whether the access type has become available or unavailable. | - | - | - | X | - | Access Availability Report |
| QoS Monitoring Report | C | This IE shall be present if the Report Type indicates a QoS Monitoring Report.<br>Several IEs within the same IE type may be present to represent a list of QoS Monitoring Reports, e.g. for different QoS flows. | - | - | - | X | - | QoS Monitoring Report |

The Access Availability Report IE shall be encoded as shown in Table 7.5.8.2-2.

**Table 7.5.8.6-2: Access Availability Report IE**

| Octet 1 and 2 | Access Availability Report IE Type = 218 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| Access Availability Information | M | This IE shall indicate an access type and whether the access type has become available or not available.<br><br>Up to two IEs with the same IE type may be present to report access availability changes for 3GPP and non-3GPP accesses. | - | - | - | X | - | Access Availability Information |

The QoS Monitoring Report IE shall be encoded as shown in Table 7.5.8.6-3.

**Table 7.5.8.6-3: QoS Monitoring Report IE**

| Octet 1 and 2 | QoS Monitoring Report IE Type = 247 (decimal) | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Octets 3 and 4 | Length = n | | | | | | | |
| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |
| QFI | M | This IE shall identify the QoS Flow Identifier for which QoS monitoring is reported. | - | - | - | X | - | QFI |
| QoS Monitoring Measurement | M | This IE shall contain the measured packet delay(s). | - | - | - | X | - | QoS Monitoring Measurement |
| Time Stamp | M | This IE shall provide the timestamp when the collection of the information in this report was generated. | - | - | - | X | - | Time Stamp |
| Start Time | O | When present, this IE shall provide the timestamp when the collection of the information in this report was started. | - | - | - | X | - | Start Time |

## 7.5.9 PFCP Session Report Response

### 7.5.9.1 General

The PFCP Session Report Response shall be sent over the Sxa, Sxb, Sxc, N4 and N4mb interface by the CP function to the UP function as a reply to the PFCP Session Report Request.

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

| **Information elements** | **P** | **Condition / Comment** | **Appl.** | | | | | **IE Type** |
|---|---|---|---|---|---|---|---|---|
| | | | **Sx a** | **Sx b** | **Sx c** | **N4** | **N4 mb** | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | 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 | X | X | Offending IE |
| Update BAR | C | This IE shall be present if a BAR previously created for the PFCP 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 | - | - | X | - | Update BAR |
| PFCPSRRsp-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 PFCP session (see NOTE 1). | X | - | - | X | - | PFCPSRRsp-Flags |
| CP F-SEID | O | This IE may be set by the SMF if the UPF indicated support of PFCP sessions successively controlled by different SMFs of a same SMF Set and the Cause IE indicates "Request accepted (success)"(see clause 5.22).<br><br>When present, it shall be set to the new F-SEID that the UPF shall use for sending subsequent PFCP session related messages. | - | - | - | X | X | F-SEID |
| N4-u F-TEID | O | This IE may be set by the SMF if the UPF indicated support of PFCP sessions successively controlled by different SMFs of a same SMF Set and the Cause IE indicates "Request accepted (success)".<br><br>When present, it shall be set to the new N4-u F-TEID that the UPF shall use for data forwarding towards the SMF. | - | - | - | X | - | F-TEID |
| Alternative SMF IP Address | O | This IE may be set by the SMF if the UPF indicated support of PFCP sessions successively controlled by different SMFs of a same SMF Set and the Cause IE indicates "Redirection Requested" (see clause 5.22).<br><br>When present, it shall be set to the IP address of the new SMF to contact. | - | - | - | X | X | Alternative SMF IP Address |
| PGW-C/SMF FQ-CSID | O | This IE may be included by the alternative SMF or PGW-C to allocate a new PGW-C/SMF FQ-CSID for the PFCP session, during the restoration of PFCP sessions associated with one or more PGW-C/SMF FQ-CSID(s) (see clause 5.22.4), if the Cause IE indicates "Request accepted (success)".<br><br>When present, the UP function shall replace any earlier value associated to the PFCP session with the new value. | - | X | - | X | - | FQ-CSID |
| Group Id | C | This IE may be included by the alternative SMF or PGW-C to allocate a new Group Id for the PFCP session, during the restoration of PFCP sessions associated with one or more Group Id(s) (see clause 5.22.4), if the Cause IE indicates "Request accepted (success)".<br><br>When present, the UP function shall replace any earlier value associated to the PFCP session with the new value. | - | X | - | X | - | Group Id |
| Node ID | C | This IE should be present if the CP F-SEID IE is present.<br><br>When present, it shall be set to the Node ID of the SMF that has taken over the control of the PFCP session, i.e. that SMF has assigned the CP F-SEID. | - | - | - | X | - | Node ID |

NOTE 1: The CP function may request the UP function to drop the packets currently buffered for the PFCP session, when buffering is performed in the UP function, upon receipt of a PFCP 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 clause 5.9.3 of 3GPP TS 23.214 [2].

### 7.5.9.2 Update BAR IE within PFCP Session Report Response

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

**Table 7.5.9.2-1: Update BAR IE in PFCP 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** | **N4** | **N4 mb** | |
| BAR ID | M | This IE shall identify the BAR Rule to be modified. | X | - | - | 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 clause 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 | - | - | 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 clause 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 | - | - | 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 | - | - | X | - | DL Buffering Suggested Packet Count |
| Suggested Buffering Packets Count | C | This IE may be present if the UP Function indicated support of the feature UDBC.<br><br>When present, it shall contain the number of packets that are suggested to be buffered when the Apply Action parameter requests to buffer the packets. The packets that exceed the limit shall be discarded. | - | X | X | X | - | Suggested Buffering Packets 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 clauses 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 clauses.

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 clause 7.2.3.2.

The receiving PFCP entity shall apply the error handling specified in the subsequent clauses.

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 a PFCP 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 Heartbeat 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.

Additional information elements may be included in Response messages containing a rejection Cause value, see clause 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 clause 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.

| Octets | Bits 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.

| Octets | Bits 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 3rd column of this table specifies if the IE is either Extendable or has a variable length or a fixed length and a reference to the clause where the IE is specified:

- 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.

The 4th column of this table indicates the number of fixed Octets the IE contained when the IE was first defined in the specification, which shall be an integer value reflecting the minimum length of fixed octets defined for the IE.

An IE of any of the above types may have a null length as specified in clause 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 clause 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 (PFCP 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 / Clause 8.2.1 | 1 |
| 20 | Source Interface | Extendable / Clause 8.2.2 | 1 |
| 21 | F-TEID | Extendable / Clause 8.2.3 | 1 |
| 22 | Network Instance | Variable Length / Clause 8.2.4 | Not Applicable |
| 23 | SDF Filter | Extendable / Clause 8.2.5 | 2 |
| 24 | Application ID | Variable Length / Clause 8.2.6 | Not Applicable |
| 25 | Gate Status | Extendable / Clause 8.2.7 | 1 |
| 26 | MBR | Extendable / Clause 8.2.8 | 10 |
| 27 | GBR | Extendable / Clause 8.2.9 | 10 |
| 28 | QER Correlation ID | Extendable / Clause 8.2.10 | 4 |
| 29 | Precedence | Extendable / Clause 8.2.11 | 4 |
| 30 | Transport Level Marking | Extendable / Clause 8.2.12 | 2 |
| 31 | Volume Threshold | Extendable /Clause 8.2.13 | 1 |
| 32 | Time Threshold | Extendable /Clause 8.2.14 | 4 |
| 33 | Monitoring Time | Extendable /Clause 8.2.15 | 4 |
| 34 | Subsequent Volume Threshold | Extendable /Clause 8.2.16 | 1 |
| 35 | Subsequent Time Threshold | Extendable /Clause 8.2.17 | 4 |
| 36 | Inactivity Detection Time | Extendable /Clause 8.2.18 | 4 |
| 37 | Reporting Triggers | Extendable /Clause 8.2.19 | 2 |
| 38 | Redirect Information | Extendable /Clause 8.2.20 | 3 |
| 39 | Report Type | Extendable / Clause 8.2.21 | 1 |
| 40 | Offending IE | Fixed / Clause 8.2.22 | 2 |
| 41 | Forwarding Policy | Extendable / Clause 8.2.23 | 1 |
| 42 | Destination Interface | Extendable / Clause 8.2.24 | 1 |
| 43 | UP Function Features | Extendable / Clause 8.2.25 | 1 |
| 44 | Apply Action | Extendable / Clause 8.2.26 | 1 |
| 45 | Downlink Data Service Information | Extendable / Clause 8.2.27 | 1 |
| 46 | Downlink Data Notification Delay | Extendable / Clause 8.2.28 | 1 |
| 47 | DL Buffering Duration | Extendable / Clause 8.2.29 | 1 |
| 48 | DL Buffering Suggested Packet Count | Variable / Clause 8.2.30 | Not Applicable |
| 49 | PFCPSMReq-Flags | Extendable / Clause 8.2.31 | 1 |
| 50 | PFCPSRRsp-Flags | Extendable / Clause 8.2.32 | 1 |
| 51 | Load Control Information | Extendable / Table 7.5.3.3-1 | Not Applicable |
| 52 | Sequence Number | Fixed Length / Clause 8.2.33 | 4 |
| 53 | Metric | Fixed Length / Clause 8.2.34 | 1 |
| 54 | Overload Control Information | Extendable / Table 7.5.3.4-1 | Not Applicable |
| 55 | Timer | Extendable / Clause 8.2 35 | 1 |
| 56 | PDR ID | Extendable / Clause 8.2 36 | 2 |
| 57 | F-SEID | Extendable / Clause 8.2 37 | 9 |
| 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 / Clause 8.2.38 | 1 |
| 61 | PFD contents | Extendable / Clause 8.2.39 | 2 |

| | | | |
|---|---|---|---|
| 62 | Measurement Method | Extendable / Clause 8.2.40 | 1 |
| 63 | Usage Report Trigger | Extendable / Clause 8.2.41 | 2 |
| 64 | Measurement Period | Extendable / Clause 8.2.42 | 4 |
| 65 | FQ-CSID | Extendable / Clause 8.2.43 | 1 |
| 66 | Volume Measurement | Extendable / Clause 8.2.44 | 1 |
| 67 | Duration Measurement | Extendable / Clause 8.2.45 | 4 |
| 68 | Application Detection Information | Extendable / Table 7.5.8.3-2 | Not Applicable |
| 69 | Time of First Packet | Extendable / Clause 8.2.46 | 4 |
| 70 | Time of Last Packet | Extendable / Clause 8.2.47 | 4 |
| 71 | Quota Holding Time | Extendable / Clause 8.2.48 | 4 |
| 72 | Dropped DL Traffic Threshold | Extendable / Clause 8.2.49 | 1 |
| 73 | Volume Quota | Extendable / Clause 8.2.50 | 1 |
| 74 | Time Quota | Extendable / Clause 8.2.51 | 4 |
| 75 | Start Time | Extendable / Clause 8.2.52 | 4 |
| 76 | End Time | Extendable / Clause 8.2.53 | 4 |
| 77 | Query URR | Extendable / Table 7.5.4.10-1 | Not Applicable |
| 78 | Usage Report (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 / Clause 8.2.54 | 4 |
| 82 | Linked URR ID | Extendable / Clause 8.2.55 | 4 |
| 83 | Downlink Data Report | Extendable / Table 7.5.8.2-1 | Not Applicable |
| 84 | Outer Header Creation | Extendable / Clause 8.2.56 | 2 |
| 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 / Clause 8.2.57 | 1 |
| 89 | CP Function Features | Extendable / Clause 8.2.58 | 1 |
| 90 | Usage Information | Extendable / Clause 8.2.59 | 1 |
| 91 | Application Instance ID | Variable Length / Clause 8.2.60 | Not Applicable |
| 92 | Flow Information | Extendable / Clause 8.2.61 | 3 |
| 93 | UE IP Address | Extendable / Clause 8.2.62 | 1 |
| 94 | Packet Rate | Extendable / Clause 8.2.63 | 1 |
| 95 | Outer Header Removal | Extendable / Clause 8.2.64 | 1 |
| 96 | Recovery Time Stamp | Extendable / Clause 8.2.65 | 4 |
| 97 | DL Flow Level Marking | Extendable / Clause 8.2.66 | 1 |
| 98 | Header Enrichment | Extendable / Clause 8.2.67 | 1 |
| 99 | Error Indication Report | Extendable / Table 7.5.8.4-1 | Not Applicable |
| 100 | Measurement Information | Extendable / Clause 8.2.68 | 1 |
| 101 | Node Report Type | Extendable / Clause 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 / Clause 8.2.70 | 1 |
| 104 | UR-SEQN | Fixed Length / Clause 8.2.71 | 4 |
| 105 | Update Duplicating Parameters | Extendable / Table 7.5.4.3-3 | Not Applicable |
| 106 | Activate Predefined Rules | Variable Length / Clause 8.2.72 | Not Applicable |
| 107 | Deactivate Predefined Rules | Variable Length / Clause 8.2.73 | Not Applicable |
| 108 | FAR ID | Extendable / Clause 8.2.74 | 4 |
| 109 | QER ID | Extendable / Clause 8.2.75 | 4 |
| 110 | OCI Flags | Extendable / Clause 8.2.76 | 1 |
| 111 | PFCP Association Release Request | Extendable / Clause 8.2.77 | 1 |
| 112 | Graceful Release Period | Extendable / Clause 8.2.78 | 1 |
| 113 | PDN Type | Extendable / Clause 8.2.79 | 1 |
| 114 | Failed Rule ID | Extendable / Clause 8.2.80 | 1 |
| 115 | Time Quota Mechanism | Extendable / Clause 8.2.81 | 1 |
| 116 | Reserved | | |
| 117 | User Plane Inactivity Timer | Extendable /Clause 8.2.83 | 4 |
| 118 | Aggregated URRs | Extendable / Table 7.5.2.4-2 | Not Applicable |
| 119 | Multiplier | Fixed / Clause 8.2.84 | 12 |
| 120 | Aggregated URR ID | Fixed / Clause 8.2.85 | 4 |
| 121 | Subsequent Volume Quota | Extendable / Clause 8.2.86 | 1 |
| 122 | Subsequent Time Quota | Extendable / Clause 8.2.87 | 4 |
| 123 | RQI | Extendable / Clause 8.2.88 | 1 |

| | | | |
|---|---|---|---|
| 124 | QFI | Extendable / Clause 8.2.89 | 1 |
| 125 | Query URR Reference | Extendable / Clause 8.2.90 | 4 |
| 126 | Additional Usage Reports Information | Extendable / Clause 8.2.91 | 2 |
| 127 | Create Traffic Endpoint | Extendable / Table 7.5.2.7 | Not Applicable |
| 128 | Created Traffic Endpoint | Extendable / Table 7.5.3.5 | Not Applicable |
| 129 | Update Traffic Endpoint | Extendable / Table 7.5.4.13 | Not Applicable |
| 130 | Remove Traffic Endpoint | Extendable / Table 7.5.4.14 | Not Applicable |
| 131 | Traffic Endpoint ID | Extendable / Clause 8.2.92 | 1 |
| 132 | Ethernet Packet Filter | Extendable / Table 7.5.2.2-3 | Not Applicable |
| 133 | MAC address | Extendable / Clause 8.2.93 | 1 |
| 134 | C-TAG | Extendable / Clause 8.2.94 | 3 |
| 135 | S-TAG | Extendable / Clause 8.2.95 | 3 |
| 136 | Ethertype | Extendable / Clause 8.2.96 | 2 |
| 137 | Proxying | Extendable / Clause 8.2.97 | 1 |
| 138 | Ethernet Filter ID | Extendable / Clause 8.2.98 | 4 |
| 139 | Ethernet Filter Properties | Extendable / Clause 8.2.99 | 1 |
| 140 | Suggested Buffering Packets Count | Extendable / Clause 8.2.100 | 1 |
| 141 | User ID | Extendable / Clause 8.2.101 | 1 |
| 142 | Ethernet PDU Session Information | Extendable / Clause 8.2.102 | 1 |
| 143 | Ethernet Traffic Information | Extendable / Table 7.5.8.3-3 | Not Applicable |
| 144 | MAC Addresses Detected | Extendable / Clause 8.2.103 | 7 |
| 145 | MAC Addresses Removed | Extendable / Clause 8.2.104 | 7 |
| 146 | Ethernet Inactivity Timer | Extendable / Clause 8.2.105 | 4 |
| 147 | Additional Monitoring Time | Extendable / Table 7.5.2.4-3 | Not Applicable |
| 148 | Event Quota | Extendable / Clause 8.2.112 | 4 |
| 149 | Event Threshold | Extendable / Clause 8.2.113 | 4 |
| 150 | Subsequent Event Quota | Extendable / Clause 8.2.106 | 4 |
| 151 | Subsequent Event Threshold | Extendable / Clause 8.2.107 | 4 |
| 152 | Trace Information | Extendable / Clause 8.2.108 | 7 |
| 153 | Framed-Route | Variable Length / Clause 8.2.109 | Not Applicable |
| 154 | Framed-Routing | Fixed Length / Clause 8.2.110 | 4 |
| 155 | Framed-IPv6-Route | Variable Length / Clause 8.2.111 | Not Applicable |
| 156 | Time Stamp | Extendable / Clause 8.2.114 | 4 |
| 157 | Averaging Window | Extendable /Clause 8.2.115 | 4 |
| 158 | Paging Policy Indicator | Extendable / Clause 8.2.116 | 1 |
| 159 | APN/DNN | Variable Length / Clause 8.2.117 | Not Applicable |
| 160 | 3GPP Interface Type | Extendable / Clause 8.2.118 | 1 |
| 161 | PFCPSRReq-Flags | Extendable / Clause 8.2.119 | 1 |
| 162 | PFCPAUReq-Flags | Extendable / Clause 8.2.120 | 1 |
| 163 | Activation Time | Extendable / Clause 8.2.121 | 4 |
| 164 | Deactivation Time | Extendable / Clause 8.2.122 | 4 |
| 165 | Create MAR | Extendable / Table 7.5.2.8-1 | Not Applicable |
| 166 | 3GPP Access Forwarding Action Information | Extendable / Table 7.5.2.8-2 | Not Applicable |
| 167 | Non-3GPP Access Forwarding Action Information | Extendable / Table 7.5.2.8-3 | Not Applicable |
| 168 | Remove MAR | Extendable / Table 7.5.4.15-1 | Not Applicable |
| 169 | Update MAR | Extendable / Table 7.5.4.16-1 | Not Applicable |
| 170 | MAR ID | Extendable / Clause 8.2.123 | 2 |
| 171 | Steering Functionality | Extendable / Clause 8.2.124 | 1 |
| 172 | Steering Mode | Extendable / Clause 8.2.125 | 1 |
| 173 | Weight | Fixed / Clause 8.2.126 | 1 |
| 174 | Priority | Extendable / Clause 8.2.127 | 1 |
| 175 | Update 3GPP Access Forwarding Action Information | Extendable / Table 7.5.4.16-2 | Not Applicable |
| 176 | Update Non 3GPP Access Forwarding Action Information | Extendable / Table 7.5.4.16-3 | Not Applicable |
| 177 | UE IP address Pool Identity | Extendable / Clause 8.2.128 | 2 |
| 178 | Alternative SMF IP Address | Extendable / Clause 8.2.129 | 1 |
| 179 | Packet Replication and Detection Carry-On Information | Extendable / Clause 8.2.130 | 1 |
| 180 | SMF Set ID | Extendable / Clause 8.2.131 | Not applicable |
| 181 | Quota Validity Time | Extendable / Clause 8.2.132 | 4 |
| 182 | Number of Reports | Fixed / Clause 8.2.133 | 2 |

| | | | |
|---|---|---|---|
| 183 | PFCP Session Retention Information (within PFCP Association Setup Request) | Extendable / Table 7.4.4.1-2 | 1 |
| 184 | PFCPASRsp-Flags | Extendable / Clause 8.2.134 | 1 |
| 185 | CP PFCP Entity IP Address | Extendable / Clause 8.2.135 | 1 |
| 186 | PFCPSEReq-Flags | Extendable / Clause 8.2.136 | 1 |
| 187 | User Plane Path Recovery Report | Extendable / Table 7.4.5.1.3-1 | Not Applicable |
| 188 | IP Multicast Addressing Info within PFCP Session Establishment Request | Extendable / Clause 7.5.2.2-4 | Not Applicable |
| 189 | Join IP Multicast Information IE within Usage Report | Extendable / Table 7.5.8.3-4 | Not Applicable |
| 190 | Leave IP Multicast Information IE within Usage Report | Extendable / Table 7.5.8.3-5 | Not Applicable |
| 191 | IP Multicast Address | Extendable / Clause 8.2.137 | 1 |
| 192 | Source IP Address | Extendable / Clause 8.2.138 | 1 |
| 193 | Packet Rate Status | Extendable / Clause 8.2.139 | 1 |
| 194 | Create Bridge Info for TSC | Extendable / Clause 8.2.140 | 1 |
| 195 | Created Bridge Info for TSC | Extendable / Table 7.5.3.6-1 | Not Applicable |
| 196 | DS-TT Port Number | Fixed Length / Clause 8.2.141 | 4 |
| 197 | NW-TT Port Number | Fixed Length / Clause 8.2.142 | 4 |
| 198 | 5GS User Plane Node | Extendable / Clause 8.2.143 | Not Applicable |
| 199 | TSC Management Information IE within PFCP Session Modification Request | Extendable / Table 7.5.4.18-1 | Not Applicable |
| 200 | TSC Management Information IE within PFCP Session Modification Response | Extendable / Table 7.5.5.3-1 | Not Applicable |
| 201 | TSC Management Information IE within PFCP Session Report Request | Extendable / Table 7.5.8.5-1 | Not Applicable |
| 202 | Port Management Information Container | Variable Length / Clause 8.2.144 | Not Applicable |
| 203 | Clock Drift Control Information | Extendable / Table 7.4.4.1.2-1 | Not Applicable |
| 204 | Requested Clock Drift Information | Extendable / Clause 8.2.145 | 1 |
| 205 | Clock Drift Report | Extendable / Table 7.4.5.1.4-1 | Not Applicable |
| 206 | Time Domain Number | Extendable / Clause 8.2.146 | 1 |
| 207 | Time Offset Threshold | Extendable / Clause 8.2.147 | 8 |
| 208 | Cumulative rateRatio Threshold | Extendable / Clause 8.2.148 | 4 |
| 209 | Time Offset Measurement | Extendable / Clause 8.2.149 | 8 |
| 210 | Cumulative rateRatio Measurement | Extendable / Clause 8.2.150 | 4 |
| 211 | Remove SRR | Extendable/ Table 7.5.4.19-1 | Not applicable |
| 212 | Create SRR | Extendable/ Table 7.5.2.9-1 | Not applicable |
| 213 | Update SRR | Extendable/ Table 7.5.4.21-1 | Not applicable |
| 214 | Session Report | Extendable / Table 7.5.8.7-1 | Not Applicable |
| 215 | SRR ID | Extendable / Clause 8.2.151 | 1 |
| 216 | Access Availability Control Information | Extendable / Table 7.5.2.9-2 | Not applicable |
| 217 | Requested Access Availability Information | Extendable / Clause 8.2.152 | 1 |
| 218 | Access Availability Report | Extendable / Table 7.5.8.6-2 | Not applicable |
| 219 | Access Availability Information | Extendable / Clause 8.2.153 | 1 |
| 220 | Provide ATSSS Control Information | Extendable / Table 7.5.2.10-1 | Not Applicable |
| 221 | ATSSS Control Parameters | Extendable / Table 7.5.3.7-1 | Not Applicable |
| 222 | MPTCP Control Information | Extendable / Clause 8.2.154 | 1 |
| 223 | ATSSS-LL Control Information | Extendable / Clause 8.2.155 | 1 |
| 224 | PMF Control Information | Extendable / Clause 8.2.156 | 1 |
| 225 | MPTCP Parameters | Extendable / Table 7.5.3.7-2 | Not Applicable |
| 226 | ATSSS-LL Parameters | Extendable / Table 7.5.3.7-3 | Not Applicable |
| 227 | PMF Parameters | Extendable / Table 7.5.3.7-4 | Not Applicable |
| 228 | MPTCP Address Information | Extendable / Clause 8.2.157 | 4 |
| 229 | UE Link-Specific IP Address | Extendable / Clause 8.2.158 | 1 |
| 230 | PMF Address Information | Extendable / Clause 8.2.159 | 1 |
| 231 | ATSSS-LL Information | Extendable / Clause 8.2.160 | 1 |
| 232 | Data Network Access Identifier | Variable Length / Clause 8.2.161 | Not applicable |
| 233 | UE IP address Pool Information | Extendable / Table 7.4.4.1-3 | Not Applicable |
| 234 | Average Packet Delay | Extendable / Clause 8.2.162 | 4 |
| 235 | Minimum Packet Delay | Extendable / Clause 8.2.163 | 4 |
| 236 | Maximum Packet Delay | Extendable / Clause 8.2.164 | 4 |
| 237 | QoS Report Trigger | Extendable / Clause 8.2.165 | 1 |
| 238 | GTP-U Path QoS Control Information | Extendable / Table 7.4.4.1.3-1 | Not Applicable |

| | | | |
|---|---|---|---|
| 239 | GTP-U Path QoS Report (PFCP Node Report Request) | Extendable / Table 7.4.5.1.5-1 | Not Applicable |
| 240 | QoS Information in GTP-U Path QoS Report | Extendable / Table 7.4.5.1.6-1 | Not Applicable |
| 241 | GTP-U Path Interface Type | Extendable / Clause 8.2.166 | 1 |
| 242 | QoS Monitoring per QoS flow Control Information | Extendable / Table 7.5.2.9-3 | Not applicable |
| 243 | Requested QoS Monitoring | Extendable / Clause 8.2.167 | 1 |
| 244 | Reporting Frequency | Extendable / Clause 8.2.168 | 1 |
| 245 | Packet Delay Thresholds | Extendable / Clause 8.2.169 | 1 |
| 246 | Minimum Wait Time | Extendable / Clause 8.2.170 | 4 |
| 247 | QoS Monitoring Report | Extendable / Table 7.5.8.6-3 | Not applicable |
| 248 | QoS Monitoring Measurement | Extendable / Clause 8.2.171 | 1 |
| 249 | MT-EDT Control Information | Extendable / Clause 8.2.172 | 1 |
| 250 | DL Data Packets Size | Extendable / Clause 8.2.173 | 2 |
| 251 | QER Control Indications | Extendable / Clause 8.2.174 | 1 |
| 252 | Packet Rate Status Report | Extendable / Table 7.5.7.1-2 | Not applicable |
| 253 | NF Instance ID | Fixed / Clause 8.2.175 | 16 |
| 254 | Ethernet Context Information | Extendable / Table 7.5.4.21-1 | Not Applicable |
| 255 | Redundant Transmission Parameters | Extendable / Table 7.5.2.2-5, Table 7.5.2.3-4 | Not Applicable |
| 256 | Updated PDR | Extendable / Table 7.5.5.5-1 | Not Applicable |
| 257 | S-NSSAI | Fixed Length / Clause 8.2.176 | 4 |
| 258 | IP version | Extendable / Clause 8.2.177 | 1 |
| 259 | PFCPASReq-Flags | Extendable / Clause 8.2.178 | 1 |
| 260 | Data Status | Extendable / Clause 8.2.179 | 1 |
| 261 | Provide RDS configuration information | Extendable / Table 7.5.2.11-1 | Not Applicable |
| 262 | RDS configuration information | Extendable / Clause 8.2.180 | 1 |
| 263 | Query Packet Rate Status IE within PFCP Session Modification Request | Extendable / Table 7.5.4.22-1 | Not Applicable |
| 264 | Packet Rate Status Report IE within PFCP Session Modification Response | Extendable / Table 7.5.5.4-1 | Not Applicable |
| 265 | MPTCP Applicable Indication | Extendable / Clause 8.2.181 | 1 |
| 266 | Bridge Management Information Container | Variable Length / Clause 8.2.182 | Not Applicable |
| 267 | UE IP Address Usage Information | Extendable / Table 7.4.4.3.1-1 | Not Applicable |
| 268 | Number of UE IP Addresses | Extendable / Clause 8.2.183 | 1 |
| 269 | Validity Timer | Extendable / Clause 8.2.184 | 2 |
| 270 | Redundant Transmission Forwarding Parameters | Extendable / Table 7.5.2.3-4 | Not Applicable |
| 271 | Transport Delay Reporting | Extendable / Table 7.5.2.2-6 | Not Applicable |
| 272 | Partial Failure Information | Extendable / Table 7.5.3.1-2 | Not Applicable |
| 273 | Spare | | |
| 274 | Offending IE Information | Variable Length / Clause 8.2.152 | Not Applicable |
| 275 | RAT Type | Extendable / Table 8.2.186 | 1 |
| 276 | L2TP Tunnel Information | Extendable / Table 7.5.2.1-2 | Not Applicable |
| 277 | L2TP Session Information | Extendable / Table 7.5.2.1-3 | Not Applicable |
| 278 | L2TP User Authentication IE | Extendable / Clause 8.2.187 | 1 |
| 279 | Created L2TP Session | Extendable / Table 7.5.3.1-3 | Not Applicable |
| 280 | LNS Address | Extendable / Clause 8.2.188 | 1 |
| 281 | Tunnel Preference | Fixed Length / Clause 8.2.189 | 3 |
| 282 | Calling Number | Variable Length / Clause 8.2.190 | Not Applicable |
| 283 | Called Number | Variable Length / Clause 8.2.191 | Not Applicable |
| 284 | L2TP Session Indications | Extendable / Clause 8.2.192 | 1 |
| 285 | DNS Server Address | Extendable / Clause 8.2.193 | 1 |
| 286 | NBNS Server Address | Extendable / Clause 8.2.194 | 1 |
| 287 | Maximum Receive Unit | Fixed Length / Clause 8.2.195 | 2 |
| 288 | Thresholds | Extendable / Clause 8.2.196 | 1 |
| 289 | Steering Mode Indicator | Extendable / Clause 8.2.197 | 1 |
| 290 | PFCP Session Change Info | Extendable / Table 7.4.7.1-2 | Not Applicable |
| 291 | Group ID | Variable Length / Clause 8.2.198 | Not Applicable |
| 292 | CP IP Address | Variable / Clause 8.2.199 | Not Applicable |
| 293 | IP Address and Port number Replacement | Extendable / Clause 8.2.200 | 1 |
| 294 | DNS Query Filter | Extendable / Clause 8.2.201 | 2 |
| 295 | Direct Reporting Information | Extendable / Table 7.5.2.9-4 | Not applicable |

| | | | |
|---|---|---|---|
| 296 | Event Notification URI | Variable Length / Clause 8.2.202 | Not Applicable |
| 297 | Notification Correlation ID | Variable Length / Clause 8.2.203 | Not Applicable |
| 298 | Reporting Flags | Extendable / Clause 8.2.204 | Not Applicable |
| 299 | Predefined Rules Name | Variable Length / Clause 8.205 | Not Applicable |
| 300 | MBS Session N4mb Control Information | Extendable / Table 7.5.2.1-4 | Not Applicable |
| 301 | MBS Multicast Parameters | Extendable / Table 7.5.2.3-5 | Not Applicable |
| 302 | Add MBS Unicast Parameters | Extendable / Table 7.5.2.3-6 | Not Applicable |
| 303 | MBS Session N4mb Information | Extendable / Table 7.5.3.1-4 | Not Applicable |
| 304 | Remove MBS Unicast Parameters | Extendable / Table 7.5.4.3-4 | Not Applicable |
| 305 | MBS Session Identifier | Extendable Length / Clause 8.2.206 | 1 |
| 306 | Multicast Transport Information | Extendable Length / Clause 8.2.207 | 5 |
| 307 | MBSN4mbReq-Flags | Extendable Length / Clause 8.2.208 | 1 |
| 308 | Local Ingress Tunnel | Extendable / Clause 8.2.209 | 1 |
| 309 | MBS Unicast Parameters ID | Extendable / Clause 8.2.210 | 2 |
| 310 | MBS Session N4 Control Information | Extendable / Table 7.5.2.1-5 | Not Applicable |
| 311 | MBS Session N4 Information | Extendable / Table 7.5.3.1-5 | Not Applicable |
| 312 | MBSN4Resp-Flags | Extendable / Clause 8.2.211 | 1 |
| 313 | Tunnel Password | Variable Length / Clause 8.2.212 | Not Applicable |
| 314 | Area Session ID | Fixed Length / Clause 8.2.213 | 2 |
| 315 | Peer UP Restart Report | Extendable / Clause 7.4.5.1.7 | Not Applicable |
| 316 | DSCP to PPI Control Information | Extendable / Table 7.5.2.1-6 | Not Applicable |
| 317 | DSCP to PPI Mapping Information | Extendable / Clause 8.2.214 | 2 |
| 318 | PFCPSDRsp-Flags | Extendable / Clause 8.2.215 | 1 |
| 319 | QER Indications | Extendable / Clause 8.2.216 | 1 |
| 320 | Vendor-Specific Node Report Type | Extendable / Clause 8.2.217 | 1 |
| 321 | Configured Time Domain | Extendable / Clause 8.2.218 | 1 |
| 322 to 32767 | Spare. For future use. | | |
| 32768 to 65535 | Reserved for vendor specific IEs | | |

# 8.2 Information Elements

## 8.2.1 Cause

Cause IE is coded as depicted in Figure 8.2.1-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 19 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Cause value | | | | | | | |

**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 | More Usage Report to send | This cause shall be returned by the UP function in the PFCP Session Deletion Response message when it has more usage reports to send. (See clause 5.2.2.3.1) |
| | 3 | Request partially accepted | This cause shall be returned if the PSUCC feature is supported by the CP function and the UP function, when a PFCP Session Establishment Request or PFCP Session Modification Request is partially accepted. See clause 5.2.9. |
| | 4-63 | 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 PFCP 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 incorrect in a request message, e.g. the Mandatory IE is malformated or it carries an invalid or unexpected value. |
| | 70 | Invalid Forwarding Policy | This cause shall be used by the UP function in the PFCP Session Establishment Response or PFCP 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 PFCP Session Establishment Response or PFCP 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) and the Restoration Indication bit was not set to "1" in the request. |
| | 72 | No established PFCP Association | This cause shall be used by the CP function or the UP function if they receive a PFCP message other than the PFCP Association Setup Request and the Heartbeat Request message from a peer with which there is no established PFCP 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 PFCP 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. This cause may also be returned in Partial Failure Information to report that a rule cannot be applied due to a limitation of resources in the UP function. |
| | 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 | Redirection Requested | This cause may be returned to indicate a request to the UPF to redirect its PFCP request to a different SMF. |
| | 79 | All dynamic addresses are occupied | This cause may be returned if the UE IP address is to be assigned by the UP function but all UE IP addresses configured for a given Network Instance and/or IP address pool in the UP function are occupied. |
| | 80 | Unknown Pre-defined Rule | This cause may be returned in Partial Failure Information to report that a pre-defined rule cannot be applied since being unknown to the UP function. |
| | 81 | Unknown Application ID | This cause may be returned in Partial Failure Information to report that a rule cannot be applied due to the Application ID being unknown by the UP function. |
| | 82 | L2TP tunnel Establishment failure | This cause shall be returned if the UP function detects an L2TP tunnel failure in the PFCP Session Establishment Response. |
| | 83 | L2TP session Establishment failure | This cause shall be returned if the UP function detects an L2TP session failure in the PFCP Session Establishment Response. |
| | 84 | L2TP tunnel release | This cause may be returned by the UP function when the L2TP tunnel is released, e.g. in a PFCP Session Report Request message to delete the PFCP session if the corresponding L2TP session is terminated since to the LNS initiated the release of the L2TP tunnel or the LNS is failed. See clause 5.31.3. |
| | 85 | L2TP session release | This cause may be returned by the UP function when the L2TP session is released, e.g. in a PFCP Session Report Request message to delete the PFCP session if the corresponding L2TP session is terminated since the LNS initiated the release of the L2TP session. See clause 5.31.3. |
| | 86 | PFCP session restoration failure due to requested resource not available | This cause should be returned by:<br>- the UP function when the CP function requests the UP function to re-establish an existing PFCP session (i.e. the Restoration Indication bit set to "1" in the request) but the GTP-U F-TEID or UE IP address provided by the CP function is not available. See clauses 4.3.2 and 4.3.4 of 3GPP TS 23.527 [40].<br>- the MB-UPF when the MB-SMF requests the MB-UPF to re-establish an existing PFCP session (i.e. the MBS Restoration Indication bit is set to "1" in the request) but the N3mb/N19mb LL SSM address or N6mb/Nmb9 ingress tunnel address provided by the MB-SMF is not available. See clause 8.2.2 of 3GPP TS 23.527 [40].<br>The resource is not available means that it cannot be assigned to any PFCP session, due to e.g. the address having been decommissioned by OAM from the (MB-) UPF or e.g. the address being no longer operational due to a partial hardware failure at the (MB-)UPF. |
| | 87 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 64 "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/N6-LAN | 2 |
| CP-function | 3 |
| 5G VN Internal | 4 |
| Spare | 5 to 15 |

NOTE 1: The "Access" and "Core" values denote an uplink and downlink traffic direction respectively.
NOTE 2: For indirect data forwarding, the Source Interface in the PDR and the Destination Interface in the FAR shall both be set to "Access", in the forwarding SGW(s). The Interface value does not infer any traffic direction, in PDRs and FARs set up for indirect data forwarding, i.e. with both the Source and Destination Interfaces set to Access.

## 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 PFCP Session Establishment Request or PFCP 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" for both scenarios:

- when the CP function is providing F-TEID, i.e. both IPv4 address field and IPv6 address field may be present; or
- when the UP function is requested to allocate the F-TEID, i.e. when CHOOSE bit is set to "1", and the IPv4 address and IPv6 address fields are not present.

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 clause 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] clauses 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, i.e. a single IP flow packet filter.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 23 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | BID | 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 (w+3) | SDF Filter ID | | | | | | | |
| x 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 – BID (Bidirectional SDF Filter): If this bit is set to "1", then the SDF Filter ID shall be present, otherwise the SDF Filter ID shall not be present.

- Bit 6 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 clause 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 clause 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 clause 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 clause 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 clause 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.

The SDF Filter ID, when present, shall be encoded as an Unsigned32 binary integer value. It shall uniquely identify an SDF Filter among all the SDF Filters provisioned for a given PFCP Session. The source/destination IP address and port information, in a bidirectional SDF Filter, shall be set as for downlink IP flows. The SDF filter for the opposite direction has the same parameters, but having the source and destination address/port parameters swapped. When being provisioned with a bidirectional SDF filter in a PDR, the UP function shall apply the SDF filter as specified in clause 5.2.1A.2A.

## 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).

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **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.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **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 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 PFCP sessions. The QER Correlation ID shall be dynamically assigned by the CP function and provisioned by the CP function in different PFCP sessions to correlate QERs used in these PFCP sessions.

NOTE: A QER Correlation ID is not a Rule ID. It is only a correlation number to correlate QERs from different PFCP 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 a PFCP 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. The lower precedence values indicate higher precedence of the PDR, and the higher precedence values indicate lower precedence of the PDR when matching a packet.

## 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 DSCP value in the IPv4 Type-of-Service or the IPv6 Traffic-Class field and the second octet shall contain the ToS/Traffic Class mask field, which shall be set to "0xFC". See clause 5.3.15 of 3GPP TS 29.212 [8].

NOTE: The original ECN bits in the IP header of user plane packets are not changed after applying transport level marking.

## 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 clause 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 | QUVTI | IPMJL | EVEQU | EVETH | MACAR | ENVCL | TIMQU | VOLQU |
| 7 | Spare | Spare | Spare | Spare | Spare | Spare | UPINT | REEMR |
| 8 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 clause 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 clause 5.2.2.3).

- Bit 4 – MACAR (MAC Addresses Reporting): when set to "1", this indicates a request for reporting the MAC (Ethernet) addresses used as source address of frames sent UL by the UE.

- Bit 5 – EVETH (Event Threshold): when set to "1", this indicates a request for reporting when an event threshold is reached. .

- Bit 6 – EVEQU (Event Quota): when set to "1", this indicates a request for reporting when an Event Quota is reached. .

- Bit 7 – IPMJL (IP Multicast Join/Leave): when set to "1", this indicates a request for reporting when the UPF adds or removes the PDU session to/from the DL replication tree associated with an IP multicast flow.

- Bit 8: – QUVTI (Quota Validity Time): when set to "1", this indicates a usage report being reported for a URR due to the quota validity timer expiry.

Octet 7 shall be encoded as follows:

- Bit 1 – REEMR (REport the End Marker Reception): when set to "1", the SMF instructs the UPF to report the reception of the End Marker packet. See clause 5.2.2.2.1 and also clauses 4.2.3.2 and 4.23.4.3 in 3GPP TS 23.502 [29].

- Bit 2 – UPINT (User Plane Inactivity Timer): when set to "1", this indicates a request for reporting when no packets have been received for a period exceeding the User Plane Inactivity Timer.

- Bit 3 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-1) | Redirect Server Address | | | | | | | |
| p-(p+1) | Other Redirect Server Address Length=b | | | | | | | |
| (p+2)-(p+2+b-1) | Other Redirect Server Address | | | | | | | |
| m to (m+1) | Redirect Port | | | | | | | |
| s 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 |
| IPv4 and IPv6 addresses | 4 |
| Port | 5 |
| IPv4 address and Port | 6 |
| IPv6 address and Port | 7 |
| IPv4 and IPv6 addresses and Port | 8 |
| Spare, for future use. | 9 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 clauses 8.38 and 8.39 of IETF RFC 4006 [16].

If the Redirect Address type is set to "IPv4 and IPv6 address", the Redirect Information IE shall include an IPv4 address and an IPv6 address in the Redirect Server Address IE and Other Redirect Server Address.

The Redirection Address Type may be set to "Port", "IPv4 address and Port", "IPv6 address and Port", or "IPv4 and IPv6 addresses and Port" if the UP function has indicated its support of the RATP feature as specified in clause 8.2.25.

If the Redirect Address Type is set to Port, the Redirect Address Server Address shall not be present, the UP function shall keep the destination of IP address and only change the destination port to the port as indicated in Redirect Port field.

If the Redirect Address Type is set to "IPv4 address and Port", "IPv6 address and Port", or "IPv4 and IPv6 addresses and Port", the Redirect Address Server Address and Redirect Port shall be included. When Redirect Address Type is set to "IPv4 and IPv6 addresses and Port", the Other Redirect Server Address shall also be present.

## 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 | UISR | SESR | TMIR | UPIR | ERIR | USAR | DLDR |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.21-1: Report Type**

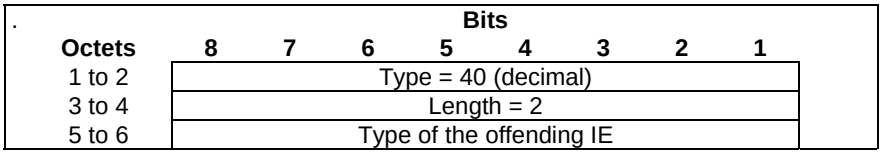
Octet 5 shall be encoded as follows:

- 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 – UPIR (User Plane Inactivity Report): when set to "1", this indicates a User Plane Inactivity Report.
- Bit 5 –TMIR (TSC Management Information Report): when set to "1", this indicates a TSC Management Information Report.
- Bit 6 – Session Report (SESR): when set to "1", this indicates a Session Report.
- Bit 7 – UISR (UP Initiated Session Request): when set to "1", this indicates it is a UP function initiated request for a reason which is indicated by the PFCPSRReq-Flags, for the PFCP session.
- 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".

## 8.2.22 Offending IE

Offending IE IE is coded as depicted in Figure 8.2.22-1.



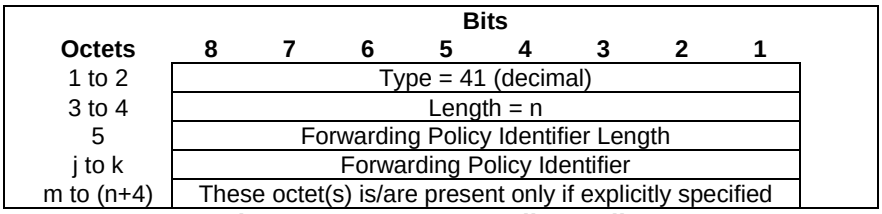
| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 40 (decimal) | | | | | | | |
| 3 to 4 | Length = 2 | | | | | | | |
| 5 to 6 | Type of the offending IE | | | | | | | |

**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 | | | | | | | |

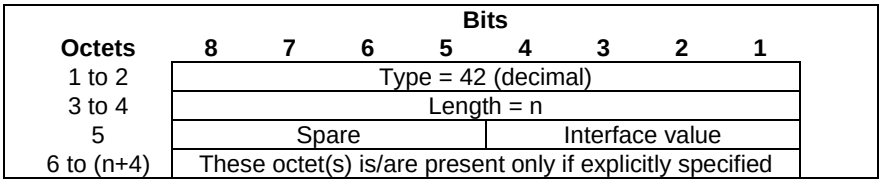
**Figure 8.2.23-1: Forwarding Policy**

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 (NOTE 1, NOTE 3, NOTE 4) | 0 |
| Core (see NOTE 1) | 1 |
| SGi-LAN/N6-LAN | 2 |
| CP- Function | 3 |
| LI Function (see NOTE 2) | 4 |
| 5G VN Internal | 5 |
| Spare | 6 to 15 |

NOTE 1: The "Access" and "Core" values denote a downlink and uplink traffic direction respectively.
NOTE 2: LI Function may denote an SX3LIF or an LMISF. See clause 5.7.
NOTE 3: For indirect data forwarding, the Source Interface in the PDR and the Destination Interface in the FAR shall both be set to "Access", in the forwarding SGW(s). The Interface value does not infer any traffic direction, in PDRs and FARs set up for indirect data forwarding, i.e. with both the Source and Destination Interfaces set to Access.
NOTE 4: For a HTTP redirection, the Source Interface in the PDR to match the uplink packets to be redirected and the Destination Interface in the FAR to enable the HTTP redirection shall both be set to "Access".

## 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.

| Octets | Bits 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 8 | Additional Supported-Features 1 |
| 9 to 10 | Additional Supported-Features 2 |
| 11 to 12 | Additional Supported-Features 3 |
| 13 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 | M/O | Description |
|---|---|---|---|---|
| 5/1 | BUCP | Sxa, N4 | O (NOTE 2) | Downlink Data Buffering in CP function is supported by the UP function. |
| 5/2 | DDND | Sxa, N4 | O | The buffering parameter 'Downlink Data Notification Delay' is supported by the UP function. |
| 5/3 | DLBD | Sxa, N4 | O | The buffering parameter 'DL Buffering Duration' is supported by the UP function. |
| 5/4 | TRST | Sxb, Sxc, N4 | O | Traffic Steering is supported by the UP function. |
| 5/5 | FTUP | Sxa, Sxb, N4 | M | F-TEID allocation / release in the UP function is supported by the UP function. |
| 5/6 | PFDM | Sxb, Sxc, N4 | O | The PFD Management procedure is supported by the UP function. |
| 5/7 | HEEU | Sxb, Sxc, N4 | O | Header Enrichment of Uplink traffic is supported by the UP function. |
| 5/8 | TREU | Sxb, Sxc, N4 | O (NOTE 3) | Traffic Redirection Enforcement in the UP function is supported by the UP function. |
| 6/1 | EMPU | Sxa, Sxb, N4 | M | Sending of End Marker packets supported by the UP function. |
| 6/2 | PDIU | Sxa, Sxb, Sxc, N4, N4mb | O (NOTE 4) | Support of PDI optimised signalling in UP function (see clause 5.2.1A.2). |
| 6/3 | UDBC | Sxb, Sxc, N4 | O | Support of UL/DL Buffering Control |
| 6/4 | QUOAC | Sxb, Sxc, N4 | O | The UP function supports being provisioned with the Quota Action to apply when reaching quotas. |
| 6/5 | TRACE | Sxa, Sxb, Sxc, N4 | O | The UP function supports Trace (see clause 5.15). |
| 6/6 | FRRT | Sxb, N4 | O | The UP function supports Framed Routing (see IETF RFC 2865 [37] and IETF RFC 3162 [38]). |
| 6/7 | PFDE | Sxb, N4 | O | The UP function supports a PFD Contents including a property with multiple values. |
| 6/8 | EPFAR | Sxa, Sxb, Sxc, N4 | O | The UP function supports the Enhanced PFCP Association Release feature (see clause 5.18). |
| 7/1 | DPDRA | Sxb, Sxc, N4 | O | The UP function supports Deferred PDR Activation or Deactivation. |
| 7/2 | ADPDP | Sxa, Sxb, Sxc, N4 | O | The UP function supports the Activation and Deactivation of Pre-defined PDRs (see clause 5.19). |
| 7/3 | UEIP | Sxb, N4 | O (NOTE 5) | The UP function supports allocating UE IP addresses or prefixes (see clause 5.21). |
| 7/4 | SSET | N4, N4mb | O | (MB-)UPF support of PFCP sessions successively controlled by different (MB-)SMFs of a same (MB-)SMF Set (see clause 5.22). |
| 7/5 | MNOP | Sxa, Sxb, Sxc, N4 | O | The UP function supports measurement of number of packets which is instructed with the flag 'Measurement of Number of Packets' in a URR. See also clause 5.2.2.2.1. |
| 7/6 | MTE | N4 | O | UPF supports multiple instances of Traffic Endpoint IDs in a PDI. |
| 7/7 | BUNDL | Sxa, Sxb, Sxc, N4, N4mb | O | PFCP messages bundling (see clause 6.5) is supported by the UP function. |
| 7/8 | GCOM | N4 | O | UPF support of 5G VN Group Communication. (See clause 5.23) |
| 8/1 | MPAS | N4, N4mb | O | (MB-)UPF support for multiple PFCP associations to the (MB-)SMFs in an (MB-)SMF set (see clause 5.22.3). |
| 8/2 | RTTL | N4 | O | UPF supports redundant transmission at transport layer. |
| 8/3 | VTIME | Sxb,N4 | O | UP function support of quota validity time feature. |
| 8/4 | NORP | Sxa, Sxb, Sxc, N4 | O | UP function support of Number of Reports as specified in clause 5.2.2.2. |
| 8/5 | IPTV | N4 | O | UPF support of IPTV service (see clause 5.25) |

| | | | | |
|---|---|---|---|---|
| 8/6 | IP6PL | N4 | O | UPF supports:<br>- UE IPv6 address(es) allocation with IPv6 prefix length other than default /64 (including allocating /128 individual IPv6 addresses), as specified in clause 4.6.2.2 of of 3GPP TS 23.316 [57]; and<br><br>- multiple UE IPv6 addresses allocation using multiple instances of the UE IP Address IE in a same PDI or Traffic Endpoint, or using multiple PDIs or Traffic Endpoints with a different UE IP Address as specified in clause 5.21.1. |
| 8/7 | TSCU | N4 | O | Time Sensitive Communication is supported by the UPF (see clause 5.26). |
| 8/8 | MPTCP | N4 | O | UPF support of MPTCP Proxy functionality (see clause 5.20) |
| 9/1 | ATSSS-LL | N4 | O | UPF support of ATSSS-LLL steering functionality (see clause 5.20) |
| 9/2 | QFQM | N4 | O | UPF support of per QoS flow per UE QoS monitoring (see clause 5.24.4). |
| 9/3 | GPQM | N4 | O | UPF support of per GTP-U Path QoS monitoring (see clause 5.24.5). |
| 9/4 | MT-EDT | Sxa | O | SGW-U support of reporting the size of DL Data Packets. (see clause 5.2.4.1). |
| 9/5 | CIOT | Sxb, N4 | O | UP function support of CIoT feature, e.g. small data packet rate enforcement. (see 5.4.15) |
| 9/6 | ETHAR | N4 | O | UPF support of Ethernet PDU Session Anchor Relocation (see clause 5.13.6). |
| 9/7 | DDDS | N4 | O | UPF support of reporting the first buffered / first discarded downlink data after buffering / directly dropped downlink data for downlink data delivery status notification. |
| 9/8 | RDS | Sxb, N4 | O | UP function support of Reliable Data Service (see clause 5.29). |
| 10/1 | RTTWP | N4 | O | UPF support of RTT measurements towards the UE Without PMF. |
| 10/2 | QUASF | Sxb, Sxc, N4 | O | The UP function supports being provisioned in a URR with an Exempted Application ID for Quota Action or an Exempted SDF Filter for Quota Action which is to be used when the quota is exhausted. See also clauses 5.2.2.2.1 and 5.2.2.3.1. |
| 10/3 | NSPOC | Sxa, Sxb, N4 | O | UP function supports notifying start of Pause of Charging via user plane. |
| 10/4 | L2TP | Sxb, N4 | O | UP function supports the L2TP feature as described in clause 5.31. |
| 10/5 | UPBER | N4 | O | UP function supports the uplink packets buffering during EAS relocation. |
| 10/6 | RESPS | Sxb, N4 | O | UP function supports Restoration of PFCP Sessions associated with one or more PGW-C/SMF FQ-CSID(s), Group Id(s) or CP IP address(es) (see clause 5.22.4) |
| 10/7 | IPREP | N4 | O | UP function supports IP Address and Port number replacement (see clause 5.33.3). |
| 10/8 | DNSTS | N4 | O | UP function support DNS Traffic Steering based on FQDN in the DNS Query message (see clause 5.33.4) |
| 11/1 | DRQOS | N4 | O | UP function supports Direct Reporting of QoS monitoring events to Local NEF or AF (see clause 5.33.5). |
| 11/2 | MBSN4 | N4 | O | UPF supports sending MBS multicast session data to associated PDU sessions using 5GC individual delivery. |
| 11/3 | PSUPRM | N4, N4mb | O | UP function supports Per Slice UP Resource Management (see clause 5.35). |

| | | | | |
|---|---|---|---|---|
| 11/4 | EPPPI | N4 | O | UP function supports Enhanced Provisioning of Paging Policy Indicator feature as specified in clause 5.36.2. |
| 11/5 | RATP | Sxb, N4 | O | UP function supports Redirection Address Types set to "Port", "IPv4 address and Port", "IPv6 address and Port", or "IPv4 and IPv6 addresses and Port". |
| 11/6 | UPIDP | N4 | O | UP function supports User Plane Inactivity Detection and reporting per PDR feature as specified in clause 5.11.3. |

NOTE 1: Features are defined as follows:
- Feature Octet / Bit: The octet and bit number within the Supported-Features IE, e.g. "5 / 1".
- Feature: A short name that can be used to refer to the octet / bit and to the feature.
- Interface: A list of applicable interfaces to the feature.
- M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O") for a UP function complying with this release of the specification.
A feature defined as mandatory in this release of the specification may not necessarily be defined or mandatory to support in earlier releases (see the respective specifications), therefore a CP function complying with this release of the specification shall be prepared to receive a UP Function Features IE with a mandatory feature bit set to "0".
- Description: A clear textual description of the feature.

NOTE 2: Downlink data should be buffered preferably in the UP function. Downlink data may be buffered in the CP function when desired, e.g. for UEs using power saving methods.

NOTE 3: 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.

NOTE 4: CP and UP functions complying with this release of the specification should support this feature.

NOTE 5: A UPF that supports the SSET or MPAS feature shall support this 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 | DFRT | IPMD | IPMA | DUPL | NOCP | BUFF | FORW | DROP |
| 6 | Spare | | | MBSU | FSSM | DDPN | BDPN | EDRT |
| 7 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 – IPMA (IP Multicast Accept): when set to "1", this indicates a request to accept UE requests to join an IP multicast group.
- Bit 7 – IPMD (IP Multicast Deny): when set to "1", this indicates a request to deny UE requests to join an IP multicast group.

- Bit 8 – DFRT (Duplicate for Redundant Transmission): when set to "1", this indicates a request to duplicate the packets for redundant transmission (see clause 5.24.2).

The octet 6 shall be encoded as follows:

- Bit 1 – EDRT (Eliminate Duplicate Packets for Redundant Transmission): when set to "1", this indicates a request to eliminate duplicate packets used for redundant transmission (see clause 5.24.2).

- Bit 2 – BDPN (Buffered Downlink Packet Notification): when set to "1", this indicates a request to notify the CP function about the first buffered DL packet for downlink data delivery status notification.

- Bit 3 – DDPN (Discarded Downlink Packet Notification): when set to "1", this indicates a request to notify the CP function about the first discarded DL packet for downlink data delivery status notification if the DL Buffering Duration or DL Buffering Suggested Packet Count is exceeded or it is discarded directly. See clause 5.2.3.1.

- Bit 4 - FSSM (Forward packets to lower layer SSM): when set to "1", this indicates a request to the MB-UPF to forward MBS session data towards a low layer SSM address allocated by the MB-UPF using multicast transport.

- Bit 5 – MBSU (Forward and replicate MBS data using Unicast transport): when set to "1", this indicates a request to forward and replicate MBS session data towards multiple remote GTP-U peers using unicast transport.

- Bit 6 to 8 – Spare, for future use and seto to "0".

One and only one of the DROP, FORW, BUFF, IPMA and IPMD flags shall be set to "1".

The NOCP flag and BDPN 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.

The DFRN flag may only be set if the FORW flag is set.

The EDRT flag may be set if the FORW flag is set.

The DDPN flag may be set with any of the DROP and BUFF flags.

Both the MBSU flag and the FSSM flag may be set (to require the MB-UPF to forward MBS session data using both multicast and unicast transports).

## 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.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 45 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | QFII | PPI |
| m | Spare | | Paging Policy Indication value | | | | | |
| p | Spare | | QFI | | | | | |
| q 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]).

The QFII flag in octet 5 indicates whether the QFI value in octet "p" shall be present. If QFII is set to "1", then the QFI value shall be present. If QFII is set to "0", then octet "p" shall not be present.

The QFI value, in octet "p", shall be encoded as the octet 5 of the QFI IE in clause 8.2.89.

## 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 PFCP 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 PFCPSMReq-Flags

The PFCPSMReq-Flags IE indicates flags applicable to the PFCP 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 | DETEID | RUMUC | SUMPC | QAURR | SNDEM | DROBU |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.31-1: PFCPSMReq-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 PFCP 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 PFCP session.

- Bit 4 - SUMPC (Stop of Usage Measurement to Pause Charging): if this bit is set to "1", it indicates that the UP function shall stop the usage measurement for all URRs with the "ASPOC" flag set to "1".

- Bit 5 - RUMUC (Resume of Usage Measurement to Un-pause of Charging): if this bit is set to "1", it indicates that the UP function shall resume the usage measurement for all URRs with the "ASPOC" flag set to "1".

- Bit 6 - DETEID (Delete All DL N3mb and/or N19mb F-TEIDs): if this bit is set to "1", it indicates that the MB-UPF shall delete all NG-RAN N3mb DL F-TEIDs and all UPF N19mb DL F-TEIDs which were provisioned in Add MBS Unicast Parameters IEs for the MBS session (see clause 5.34.2.4).

- Bit 7 to 8 – Spare, for future use, shall be set to"0" by the sender and discarded by the receiver.

Bits 4 and 5 shall not be set both to "1".

## 8.2.32 PFCPSRRsp-Flags

The PFCPSRRsp-Flags IE indicates flags applicable to the PFCP Session Report Response message. It is coded as depicted in Figure8.2.32-1.

| 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: PFCPSRRsp-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 PFCP 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<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. |

## 8.2.36 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 Table8.2.38-2.

**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 Type is set to an IPv4 address, then the Node ID value length shall be 4 Octets.

If the Node ID Type is set to an IPv6 address, then the Node ID value length shall be 16 Octets.

If the Node ID Type is set to an FQDN, then the Node ID value encoding shall be identical to the encoding of a FQDN within a DNS message of clause 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 | ADNP | AURL | AFD | DNP | 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 (w+1) | Length of Domain Name Protocol | | | | | | | |
| (w+2) to x | Domain Name Protocol | | | | | | | |
| y to (y+1) | Length of Additional Flow Description | | | | | | | |
| (y+2) to z | Additional Flow Description | | | | | | | |
| a to (a+1) | Length of Additional URL | | | | | | | |
| (a+2) to b | Additional URL | | | | | | | |
| c to (c+1) | Length of Additional Domain Name and Domain Name Protocol | | | | | | | |
| (c+2) to d | Additional Domain Name and Domain Name Protocol | | | | | | | |
| e 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 in the Figure 8.2.39-1:

- 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 – DNP (Domain Name Protocol): If this bit is set to "1", then the Length of Domain Name Protocol and the Domain Name Protocol shall be present, otherwise they shall not be present; and if this bit is set to "1", the Length of Domain Name and the Domain Name fields shall also be present.

- Bit 6 – AFD (Additional Flow Description): If this bit is set to "1", the Length of Additional Flow Description and the Additional Flow Description field shall be present, otherwise they shall not be present.

- Bit 7 – AURL (Additional URL): If this bit is set to "1", the Length of Additional URL and the Additional URL field shall be present, otherwise they shall not be present.

- Bit 8 – ADNP (Additional Domain Name and Domain Name Protocol): If this bit is set to "1", the Length of Additional Domain Name and Domain Name Protocol, and the Additional Domain Name and Domain Name Protocol field shall be present, otherwise they shall not be present.

The Flow Description field, when present, shall be encoded as an OctetString as specified in clause 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 clause 6.4.3.9 of 3GPP TS 29.251 [21].

The URL field, when present, shall be encoded as an OctetString as specified in clause 6.4.3.8 of 3GPP TS 29.251 [21].

The Domain Name Protocol field, when present, shall be encoded as an OctetString as specified in clause 6.4.3.9 of 3GPP TS 29.251 [21].

Additional instance(s) of the Flow Description shall be encoded as shown in Figure 8.2.39-2. The encoding of Flow Description 2, 3 up to m field are the same as the Flow Description field specified in clause 8.2.39.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| (y+2) to (y+3) | Length of Flow Description 2 | | | | | | | |
| (y+4) to i | Flow Description 2 | | | | | | | |
| j to (j+1) | Length of Flow Description 3 | | | | | | | |
| (j+2) to k | FlowDescription 3 | | | | | | | |
| | ... | | | | | | | |
| l to (l+1) | Length of Flow Description m | | | | | | | |
| (l+2) to z | Flow Description m | | | | | | | |

**Figure 8.2.39-2: Additional Flow Description field**

Additional instance(s) of the URL shall be encoded as shown in Figure 8.2.39-3. The encoding of URL 2, 3 up to m fields are the same as the URL field.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| (a+2) to (a+3) | Length of URL 2 | | | | | | | |
| (a+4) to o | URL 2 | | | | | | | |
| pa to (pa+1) | Length of URL 3 | | | | | | | |
| (pa+2) to pb | URL 3 | | | | | | | |
| | ... | | | | | | | |
| pc to (pc+1) | Length of URL m | | | | | | | |
| (pc+2) to b | URL m | | | | | | | |

**Figure 8.2.39-3: Additional URL field**

Additional instance(s) of the Domain Name and Domain Name Protocol shall be encoded as shown in Figure 8.2.39-4. The encoding of Domain Name 2, 3, up to m fields and Domain Name Protocol 2, 3 up to m fields are the same as the Domain Name field and Domain Name Protocol field respectively.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| (c+2) to (c+3) | Length of Domain Name 2 | | | | | | | |
| (c+4) to pd | Domain Name 2 | | | | | | | |
| pe to (pe+1) | Length of Domain Name Protocol 2 | | | | | | | |
| (pe+2) to pf | Domain Name Protocol 2 | | | | | | | |
| pg to (pg+1) | Length of Domain Name 3 | | | | | | | |
| (pg+2) to ph | Domain Name 3 | | | | | | | |
| pi to (pi+1) | Length of Domain Name Protocol 3 | | | | | | | |
| (pi+2) + pj | Domain Name Protocol 3 | | | | | | | |
| | ... | | | | | | | |
| pk to (pk+1) | Length of Domain Name m | | | | | | | |
| (pk+2) to pl | Domain Name m | | | | | | | |
| pm to (pm+1) | Length of Domain Name Protocol m | | | | | | | |
| (pm+2) to d | Domain Name Protocol m | | | | | | | |

**Figure 8.2.39-4: Additional Domain Name and Domain Name Protocol field**

## 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 | EVETH | MACAR | ENVCL | MONIT | TERMR | LIUSA | TIMQU | VOLQU |
| 7 | Spare | Spare | UPINT | EMRRE | QUVTI | IPMJL | TEBUR | EVEQU |
| 8 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 time 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 clause 5.2.2.4).
- Bit 4 – TERMR (Termination Report): when set to "1", this indicates a usage report being reported (in a PFCP Session Deletion Response) for a URR due to the termination of the PFCP session, or a usage report being reported (in a PFCP Session Modification Response) for a URR due to the removal of the URR or dissociated from the last PDR.
- 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 clause 5.2.2.3).
- Bit 7 – MACAR (MAC Addresses Reporting): when set to "1", this indicates a usage report to report MAC (Ethernet) addresses used as source address of frames sent UL by the UE.
- Bits 8: EVETH (Event Threshold): when set to "1", this indicates a usage report is generated when an event threshold is reached.

Octet 7 shall be encoded as follows:

- Bit 1 – EVEQU (Event Quota): when set to "1", this indicates that the Event Quota has been exhausted.
- Bit 2 – TEBUR (Termination By UP function Report): when set to "1", this indicates a usage report being reported for a URR due to the termination of the PFCP session which is initiated by the UP function.
- Bit 3 – IPMJL (IP Multicast Join/Leave): when set to "1", this indicates a usage report being reported for a URR due to the UPF adding or removing the PDU session to/from the DL replication tree associated with an IP multicast flow.
- Bit 4 – QUVTI (Quota Validity Time): when set to "1", this indicates a usage report being reported for a URR due to the quota validity timer expiry.
- Bit 5 – EMRRE (End Marker Reception REport): this indicates that the UP function has received End Marker from the old I-UPF. See clauses 4.2.3.2 and 4.23.4.3 in 3GPP TS 23.502 [29]).
- Bit 6 – UPINT (User Plane Inactivity Timer): when set to "1", this indicates that no packets have been received for a period exceeding the User Plane Inactivity Timer.
- Bit 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 or the periodic QoS monitoring 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, or a set of PDU sessions belonging to an arbitrary number of UEs on a SMF or UPF. The FQ-CSID is supported on the Sxa, Sxb and N4 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 | Spare \| Node Type |
| (q+3) 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, PGW-U, ePDG, TWAN , SMF or UPF.

Other values of Node-Address Type are reserved.

Values of Number of CSID greater than 1 shall only be employed in the PFCP Session Deletion Request. The value 0 shall be used in a PFCP Session Modification Request, with the FQ-CSID Node-ID Type and Node-Address fields set to all zeros, and with the Node Type indicating one node type, to remove an FQ-CSID previously provisioned for the PFCP session for the related node type.

NOTE: The CP function can remove all the FQ-CSIDs for all node types provisioned in the UP function for a given PFCP session by sending a PFCP Session Modification Request with one FQ-CSID IE with a null length.

The node that creates the FQ-CSID (i.e. SGW-C for SGW-C FQ-CSID, PGW-C or SMF for PGW-C/SMF FQ-CSID and PGW-U or SGW-U or UPF for PGW-U/SGW-U/UPF FQ-CSID) needs to ensure that the Node-ID is globally unique and the CSID value is unique within that node.

The Node Type field in bits 1 to 4 of octet (q+2) shall be encoded as defined in Table 8.2.43-2. Bits 5 to 8 of octet (q+2) shall be set to zero by the sender and ignored by the receiver.

**Table 8.2.43-2: Node Type**

| Node Type | Value (Decimal) |
|---|---|
| MME | 0 |
| SGW-C | 1 |
| PGW-C/SMF | 2 |
| ePDG | 3 |
| TWAN | 4 |
| PGW-U/SGW-U/UPF | 5 |
| Spare, for future use. | 6-15 |

## 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 | | DLNOP | ULNOP | TONOP | DLVOL | ULVOL | TOVOL |
| m to (m+7) | Total Volume | | | | | | | |
| p to (p+7) | Uplink Volume | | | | | | | |
| q to (q+7) | Downlink Volume | | | | | | | |
| r to (r+7) | Total Number of Packets | | | | | | | |
| s to (s+7) | Uplink Number of Packets | | | | | | | |
| t to (t+7) | Downlink Number of Packets | | | | | | | |
| z 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 – TONOP: If this bit is set to "1", then the Total Number of Packets field shall be present, otherwise the Total Number of Packets field shall not be present.
- Bit 5 – ULNOP: If this bit is set to "1", then the Uplink Number of Packets field shall be present, otherwise the Uplink Number of Packets field shall not be present.
- Bit 6 – DLNOP: If this bit is set to "1", then the Downlink Number of Packets field shall be present, otherwise the Downlink Number of Packets field shall not be present.
- Bit 7 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 clause 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 clause 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.

| Octets | Bits 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.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 72 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | DLBY | DLPA |
| m to (m+7) | Downlink Packets | | | | | | | |
| o to (o+7) | Number of Bytes of Downlink Data | | | | | | | |
| 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 – DLBY: If this bit is set to "1", then the Number of Bytes of Downlink Data field shall be present, otherwise the Number of Bytes of Downlink Data field shall not be present.
- Bit 3 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.

The Number of Bytes of Downlink Data fields shall be encoded as an Unsigned64 binary integer value. It shall contain the number of bytes of the downlink data.

## 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 clause 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 clause 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 to 6 | 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 |
| t to (t+2) | C-TAG |
| u to (u+2) | S-TAG |
| 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. It takes the form of a bitmask where each bit indicates the outer header to be created in the outgoing packet. Spare bits shall be ignored by the receiver.

**Table 8.2.56-1: Outer Header Creation Description**

| Octet / Bit | Outer Header to be created in the outgoing packet |
|---|---|
| 5/1 | GTP-U/UDP/IPv4 (NOTE 1), (NOTE 3) |
| 5/2 | GTP-U/UDP/IPv6 (NOTE 1), (NOTE 3) |
| 5/3 | UDP/IPv4 (NOTE 2, NOTE 5) |
| 5/4 | UDP/IPv6 (NOTE 2, NOTE 5) |
| 5/5 | IPv4 (NOTE 5) |
| 5/6 | IPv6 (NOTE 5) |
| 5/7 | C-TAG (see NOTE 4) |
| 5/8 | S-TAG (see NOTE 4) |
| 6/1 | N19 Indication (NOTE 6) |
| 6/2 | N6 Indication (NOTE 6) |
| 6/3 | Low Layer SSM and C-TEID (NOTE 7) |

NOTE 1: The SGW-U/I-UPF shall also create GTP-U extension header(s) if any has been stored for this packet, during a previous outer header removal (see clause 8.2.64).

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 clause 4.3.17.8.3.3.2 of 3GPP TS 23.401 [14]).

NOTE 3: The SGW-U/I-UPF shall set the GTP-U message type to the value stored during the previous outer header removal.

NOTE 4: This value may apply to UL packets sent by a UPF for Ethernet PDU sessions over N6 (see clause 5.8.2.11.6 of 3GPP TS 23.501 [28]).

NOTE 5: This value may apply e.g. to UL packets sent by a UPF (PDU Session Anchor) over N6, when explicit N6 traffic routing information is provided to the SMF (see clause 5.6.7 of 3GPP TS 23.501 [28]). The IPv4 or IPv6 address shall correspond to the IP address of the tunnel endpoint in the data network.

NOTE 6: When the "N19 Indication" or "N6 Indication" bit in the Outer Header Creation Description field is set to "1", the UPF shall associate an "N19 Indication" or "N6 Indication" internal flag with the packet to indicate that the packet has been received from a N19 or N6 interface respectively. This indication is further used to prevent the packet from being forwarded back over N19 or N6 respectively (see clause 8.2.130).

NOTE 7: When the "Low Layer SSM and C-TEID" bit in the Outer Header Creation Description field is set to "1", the MB-UPF shall create a GTP-U header with the C-TEID and set the destination IP address and the source IP address as the IP Multicast Distribution Address and the IP Source Address in the Multicast Transport Information IE, which is the Low Layer SSM allocated to the MBS session. In this case, the TEID, IPv4/IPv6 address and Port Number fields shall not be present.

At least one bit of the Outer Header Creation Description field shall be set to "1". Bits 5/1 and 5/2 may both be set to "1" if an F-TEID with both an IPv4 and IPv6 addresses has been assigned by the GTP-U peer. In this case, the UP function shall send the outgoing packet towards the IPv4 or IPv6 address.

The TEID field shall be present if the Outer Header Creation Description requests the creation of a GTP-U header, i.e. if in Octet 5 any of the bits 5/1 and 5/2 are set. 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 an IPv4 header, i.e. if in Octet 5 any of the bits 5/1, 5/3 and 5/5 are set. 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 an IPv6 header, i.e. if in Octet 5 any of the bits 5/2, 5/4 and 5/6 are set. 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. if in Octet 5 any of the bits 5/3 and 5/4 are set. 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.

The C-TAG field shall be present if the Outer Header Creation Description requests the setting of the C-Tag in Ethernet packet. Otherwise it shall not be present. When present, it shall contain the destination Customer-VLAN tag to set in the Customer-VLAN tag header of the outgoing packet.

The S-TAG field shall be present if the Outer Header Creation Description requests the setting of the S-Tag in Ethernet packet. Otherwise it shall not be present. When present, it shall contain the destination Service-VLAN tag to set in the Service-VLAN tag 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 7 | Additional Supported-Features 1 |
| 8 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 | M/O | Description |
|---|---|---|---|---|
| 5/1 | LOAD | Sxa, Sxb, Sxc, N4, N4mb | O | Load Control is supported by the CP function. |
| 5/2 | OVRL | Sxa, Sxb, Sxc, N4, N4mb | O | Overload Control is supported by the CP function. |
| 5/3 | EPFAR | Sxa, Sxb, Sxc, N4 | O | The CP function supports the Enhanced PFCP Association Release feature (see clause 5.18). |
| 5/4 | SSET | N4, N4mb | O | (MB-)SMF support of PFCP sessions successively controlled by different (MB-)SMFs of a same (MB-)SMF Set (see clause 5.22). |
| 5/5 | BUNDL | Sxa, Sxb, Sxc, N4, N4mb | O | PFCP messages bundling (see clause 6.5) is supported by the CP function. |
| 5/6 | MPAS | N4, N4mb | O | (MB-)SMF support for multiple PFCP associations from an (MB-)SMF set to a single (MB-)UPF (see clause 5.22.3). |
| 5/7 | ARDR | Sxb, N4 | O | CP function supports Additional Usage Reports in the PFCP Session Deletion Response (see clause 5.2.2.3.1). |
| 5/8 | UIAUR | Sxb, N4 | O | CP function supports the UE IP Address Usage Reporting feature, i.e. receiving and handling of UE IP Address Usage Information IE (see clause 5.21.3.2). |
| 6/1 | PSUCC | Sxb, Sxc, N4, N4mb | O | CP function supports PFCP session establishment or modification with Partial Success, i.e. with UP function reporting rules that cannot be activated. See clause 5.2.9. |
| 6/2 | RPGUR | Sxa, Sxb, N4, N4mb | O | CP function supports the Peer GTP-U Entity Restart Reporting as specified in clause 20.3.4a of 3GPP TS 23.007 [24] and in clause 5.5 of 3GPP TS 23.527 [40]. |

NOTE: Features are defined as follows:
- Feature Octet / Bit: The octet and bit number within the Supported-Features IE, e.g. "5 / 1".
- Feature: A short name that can be used to refer to the octet / bit and to the feature.
- Interface: A list of applicable interfaces to the feature.
- M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O") for a CP function complying with this release of the specification.
A feature defined as mandatory in this release of the specification may not necessarily be defined or mandatory to support in earlier releases (see the respective specifications), therefore a UP function complying with this release of the specification shall be prepared to receive a CP Function Features IE with a mandatory feature bit set to "0".
- 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 clause 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 | IP6PL | CHV6 | CHV4 | IPv6D | S/D | V4 | V6 |
| m to (m+3) | IPv4 address | | | | | | | |
| p to (p+15) | IPv6 address | | | | | | | |
| r | IPv6 Prefix Delegation Bits | | | | | | | |
| s | IPv6 Prefix Length | | | | | | | |
| 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 CHV6 bit shall not be set and 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 CHV4 bit sshall not be set and 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, Create Traffic Endpoint IE and Update Traffic Endpoint 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 – IPv6D: This bit is only applicable to the UE IP address IE in the PDI IE, Create Traffic Endpoint IE and Update Traffic Endpoint IE, when the V6 bit or CHV6 bit is set to "1". If this bit is set to "1", then the IPv6 Prefix Delegation Bits field shall be present, otherwise the UP function shall consider IPv6 prefix is default /64.

- Bit 5 – CHV4 (CHOOSE IPV4): If this bit is set to "1", then the V4 bit shall not be set, the IPv4 address shall not be present and the UP function shall assign an IPv4 address. This bit shall only be set by the CP function.

- Bit 6 – CHV6 (CHOOSE IPV6): If this bit is set to "1", then the V6 bit shall not be set, the IPv6 address shall not be present and the UP function shall assign an IPv6 address. This bit shall only be set by the CP function.

- Bit 7 – IP6PL (IPv6 Prefix Length): this bit is only applicable when the V6 bit or CHV6 bit is set to "1" and the "IPv6D" bit is set to "0", for an IPv6 prefix other than default /64, when the UP function supports the IP6PL feature as specified in clause 8.2.25. If this bit is set to "1", then the IPv6 Prefix Length field shall be present.

- Bit 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.

Octet r, if present, shall contain the number of bits allocated for IPv6 prefix delegation (relative to the default /64 IPv6 prefix), e.g. if /60 IPv6 prefix is used, the value shall be set to "4". When using UE IP address IE in a PDI to match packets, the UP function shall only use the IPv6 prefix part and ignore the interface identifier part. When the field is set to "0", the UP function shall determine a value based on the local configuration.

The IPv6 Prefix Length in octet s, when present, shall be encoded as an 8 bits binary integer, e.g. if /72 prefix is used, the value shall be set to to (decimal) 72, or if /56 prefix is used, the value shall be set to (decimal) 56. The prefix length value "128" indicates an individual /128 IPv6 address. When the field is set to "0", the UP function shall determine a value based on the local configuration.

## 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 | | | | | APRC | 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 | Spare | | | | | Additional Uplink Time Unit | | |
| (q+1) to (q+2) | Additional Maximum Uplink Packet Rate | | | | | | | |
| r | Spare | | | | | Additional Downlink Time Unit | | |
| (r+1) to (r+2) | Additional Maximum Downlink Packet Rate | | | | | | | |
| s 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 – APRC (Additional Packet Rate Control): If this bit is set to "1", then the presence of octets q to (r+2) is determined as follows:
  - If bit 1 (ULPR) is set to "1", then octets q to (q+2), the Additional Maximum Uplink Packet Rate shall be present. Otherwise, octets q to (q+2) shall not be present;
  - If bit 2 (DLPR) is set to "1", then octets r to (r+2), the Additional Maximum Downlink Packet Rate shall be present. Otherwise, octets r to (r+2) shall not be present.
- Bits 4 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.

When present, octets q to (q+2) indicate the additional maximum number of uplink packets allowed to be sent within the additional uplink time unit.

When present, octets r to (r+2) indicate the additional maximum number of downlink packets allowed to be sent within the additional downlink time unit.

The Additional Uplink/Downlink Time Unit shall be encoded as the Uplink/Downlink Time Unit, see Table 8.2.63.1.

**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.

The Additional Maximum Uplink/Downlink Packet Rate shall be encoded as an Unsigned16 binary integer value. They shall indicate the additional maximum number of uplink/downlink packets allowed to be sent in the indicated Additional uplink/downlink time unit respectively.

NOTE: The Serving PLMN rate control is only applicable to downlink packets with the value of Maximum Downlink Packet Rate set to equal to or higher than 10 and with the Downlink Time Unit set to 6 minutes. The Small Data Rate Control/APN rate control is applicable to both uplink/downlink packets with the Time Unit set to minute/hour/day/week.

## 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 | GTP-U Extension Header Deletion | | | | | | | |
| 7 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 (NOTE 1), (NOTE 2), (NOTE 8) | 0 |
| GTP-U/UDP/IPv6 (NOTE 1), (NOTE 2) | 1 |
| UDP/IPv4 (NOTE 3, NOTE 6) | 2 |
| UDP/IPv6 (NOTE 3, NOTE 6) | 3 |
| IPv4 (NOTE 6) | 4 |
| IPv6 (NOTE 6) | 5 |
| GTP-U/UDP/IP (NOTE 4) | 6 |
| VLAN TAG POP (i.e. removal of one VLAN tag, S-TAG or C-TAG) (See NOTE 5) | 7 |
| VLAN TAGs POP-POP (i.e. removal of 2 VLAN tags, S-TAG and C-TAG) (See NOTE 5) | 8 |
| Spare, for future use. (See NOTE 7) | 9 to 255 |
| NOTE 1: The SGW-U/I-UPF 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]) that are not requested to be deleted by the GTP-U Extension Header Deletion field.<br>NOTE 2: The SGW-U/I-UPF shall store the GTP-U message type for a GTP-U signalling message which is required to be forwarded, e.g. for an End Marker message.<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 clause 4.3.17.8.3.3.2 of 3GPP TS 23.401 [14]).<br>NOTE 4: The CP function shall use this value to instruct UP function to remove the GTP-U/UDP/IP header regardless it is IPv4 or IPv6.<br>NOTE 5: This value may apply to DL packets received by a UPF over N6 for Ethernet PDU sessions (see clause 5.8.2.11.3 of 3GPP TS 23.501 [28]). The VLAN POP operation removes the VLAN tag from the top of the VLAN stack (outer VLAN tag), i.e. it removes the S-TAG or C-TAG if the user plane packet contains only one VLAN tag, or it removes the S-TAG if the user plane packet contains both a C-TAG and an S-TAG.<br>NOTE 6: This value may apply e.g. to DL packets received by a UPF (PDU Session Anchor) over N6, when explicit N6 traffic routing information is provided to the SMF (see clause 5.6.7 of 3GPP TS 23.501 [28]).<br>NOTE 7: If the UP function receives an unknown value, it shall reject the request message with the cause set to "Mandatory IE incorrect" together with the Offending IE set to the IE type of Outer Header Removal IE.<br>NOTE 8: The PSA UPF shall store GTP-U extension header(s) required to be forwarded and that are not requested to be deleted by the GTP-U Extension Header Deletion field, e.g. the PDU Session Container received from the MB-UPF (for MBS session data) over N19mb interface, and modify it as instructed by the SMF, e.g. the PSA UPF may be instructed to modify the QFI field in the PDU Session Container extension header for the packets received from the MB-UPF. | |

The GTP-U Extension Header Deletion field (octet 6) shall be present if it is required to delete GTP-U extension header(s) from incoming GTP-PDUs. Octet 6 shall be absent if all GTP-U extension headers required to be forwarded shall be stored as indicated in NOTE 1 of Table 8.2.64-1.

The GTP-U Extension Header Deletion field, when present, shall be encoded as specified in Table 8.2.64-2. It takes the form of a bitmask where each bit provides instructions on the information to be deleted from the incoming GTP-PDU packet. Spare bits shall be ignored by the receiver.

**Table 8.2.64-2: GTP-U Extension Header Deletion**

| Octet / Bit | GTP-U Extension Header to be deleted from incoming packet |
|---|---|
| 6/1 | PDU Session Container (NOTE) |
| NOTE: This value shall be used for data forwarding during a 5GS to EPS handover for a UPF that supports EPS-5GS interworking (see clause 5.17.3). | |

## 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 PFCP entity 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 clause 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 clause 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 clause 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.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 100 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | CIAM | ASPOC | SSPOC | MNOP | ISTM | RADI | 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).
- Bit 3 – RADI (Reduced Application Detection Information): when set to "1", this indicates that the Application Detection Information reported to the CP function, upon detecting the start or stop of an application, shall only contain the Application ID.
- Bit 4 – ISTM (Immediate Start Time Metering): when set to "1", this indicates that time metering shall start immediately when the flag is received.
- Bit 5 – MNOP (Measurement of Number of Packets): when set to "1", this indicate a request to measure the number of packets transferred in UL/DL/Total in addition to the measurement in octets when Volume based measurement applies.
- Bit 6 – SSPOC (Send Start Pause of Charging): when set to "1", this indicate that the UP Function shall send a Start Pause of Charging indication to the upstream GTP-U entity(s) when the Dropped DL Traffic Threshold is reached.
- Bits 7 – ASPOC (Applicable for Start of Pause of Charging): when set to "1", this indicate that UP Function the the URR is applicable for Start of Pause of Charging, so that it shall stop the usage measurement for the URR when receiving Start Pause of Charging indication from the peer downstream GTP-U entity.
- Bits 8 – CIAM (Control of Inactive Measurement): when set to "1", this indicates that the UP function shall read the current value of the "INAM" flag and stop (if "INAM" is set to "1") or resume (if "INAM" is set to "0") the usage measurement accordingly for the given URR with the "APSOC" flag set to "1". If the "CIAM" flag is set to 0 for a URR with the "ASPOC" flag set to "1", the UP function shall ignore the "INAM" flag received in the Measurement Information. The "CIAM" flag shall be ignored for a URR without the ASPOC" flag set to "1".

At least one bit shall be set to "1". Several bits may be set to "1", e.g. both MBQE and MNOP bits are set to "1".

## 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.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 101 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | VSR | PURR | GPQR | CKDR | UPRR | 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 – UPRR (User Plane Path Recovery Report): when set to "1", this indicates a User Plane Path Recovery Report.

  Bit 3 – CKDR (Clock Drift Report): when set to "1", this indicates a Clock Drift Report.
- Bit 4 – GPQR (GTP-U Path QoS Report): when set to "1", this indicates a GTP-U Path QoS Report.
- Bit 5 – PURR (peer GTP-U entity Restart Report): when set to "1", this indicates a Peer GTP-U Restart report.
- Bit 6 – VSR (Vendor-Specific Report): when set to "1", this indicates a Vendor-Specific Report.
- Bit 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".

NOTE 1: If UPFR, UPRR and/or PURR bits are set to "1", the Remote GTP-U Peer IEs in the User Plane Path Failure Report IE, in the User Plane Path Recovery Report IE and/or Peer UP Restart Report IE are different.

NOTE 2: A Vendor-Specific Report can be used in the PFCP Node Report Request message by non-3GPP Standards Development Organizations for interfaces relying on PFCP as the protocol for Control and User Plane Separation, for reports not defined by 3GPP. See clauses 5.9 and 8.1.1 for the definition and usage of Vendor Specific IEs.

## 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 | | | | NI | DI | V4 | V6 |
| m to (m+3) | IPv4 address | | | | | | | |
| p to (p+15) | IPv6 address | | | | | | | |
| q to (q+1) | Length of Destination Interface field | | | | | | | |
| (q+2) to r | Destination Interface field | | | | | | | |
| s to (s+1) | Length of Network Instance field | | | | | | | |
| (s+2) to t | Network Instance field | | | | | | | |
| 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 – DI: If this bit is set to "1", then the Length of Destination Interface field and the Destination Interface field shall be present, otherwise both the Length of Destination Interface field and the Destination Interface field shall not be present.
- Bit 4 – NI: If this bit is set to "1", then the Length of Network Instance field and the Network Instance field shall be present, otherwise both the Length of Network Instance field and the Network Instance field shall not be present.
- Bit 5 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.

The Destination Interface field, when present, shall be encoded as the same as Destination Interface IE (from octet 5, i.e. excluding Type and Length) specified in clause 8.2.24.

The Network Instance field, when present, shall be encoded as the same as Network Instance IE (from octet 5, i.e. excluding Type and Length) specified in clause 8.2.4.

## 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 |
| 6 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 PFCP 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 PFCP Association Release Request

The PFCP 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 | | | | | | URSS | SARR |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.77-1: PFCP Association Release Request**

The following flags are coded within Octet 5:

- Bit 1 – SARR (PFCP Association Release Request): If this bit is set to "1", then the UP function requests the release of the PFCP association.

- Bit 2 – URSS (non-zero Usage Reports for the affected PFCP Sessions Sent): If this bit is set to "1", it indicates that the UP function has sent all the non-zero usage reports to the CP function for all PFCP essions affected by the PFCP Association Release.

- Bit 3 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, Ethernet or Unstructured).

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **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**

The PDN Type shall be encoded as a 3 bits binary integer value as specified in Table 8.2.79-1.

**Table 8.2.79-1: PDN Type**

| PDN Type | Value (Decimal) |
|---|---|
| IPv4 | 1 |
| IPv6 | 2 |
| IPv4v6 | 3 |
| Non-IP | 4 |
| Ethernet | 5 |
| For future use. Shall not be sent. | 0, 6, 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 |
| MAR | 5 |
| SRR | 6 |
| For future use. Shall not be sent. If received, shall be interpreted as the value "1". | 7 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 , BAR ID, MAR ID and SRR 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 clause 7.2.29 of 3GPP TS 32.299 [18].

## 8.2.82 Void

## 8.2.83 User Plane Inactivity Timer

The User Plane Inactivity Timer IE contains the inactivity time period, in seconds, to be monitored by the UP function. It shall be encoded as shown in Figure 8.2.83-1.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 117 (decimal) |
| 3 to 4 | Length = n |
| 5 to 8 | User Plane Inactivity Timer |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.83-1: User Plane Inactivity Timer**

The User Plane Inactivity Timer field shall be encoded as an Unsigned32 binary integer value. The timer value "0" shall be interpreted as an indication that user plane inactivity detection and reporting is stopped.

## 8.2.84 Multiplier

The Multiplier IE type shall be encoded as shown in Figure 8.2.84-1. It contains a Multiplier (see IETF RFC 4006 [16]) to measure the abstract service units the traffic of an aggregated URR consumes from the credit pool.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 119 (decimal) |
| 3 to 4 | Length = 12 |
| 5 to 12 | Value-Digits |
| 13 to 16 | Exponent |

**Figure 8.2.84-1: Multiplier**

The Value-Digit value and Exponent value shall be encoded as binary integer value, and set the value as in Value-Digit AVP and Exponent AVP as specified in 3GPP TS 32.299 [18].

## 8.2.85 Aggregated URR ID IE

The Aggregated URR ID IE type shall be encoded as shown in Figure 8.2.85-1. It contains a URR ID.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 120 (decimal) |
| 3 to 4 | Length = 4 |
| 5 to 8 | URR ID value |

**Figure 8.2.85-1: Aggregated URR ID**

Each URR ID value shall be encoded as an Unsigned32 binary integer value.

## 8.2.86 Subsequent Volume Quota

The Subsequent Volume Quota IE type shall be encoded as shown in Figure 8.2.86-1. It contains the volume quota to be monitored by the UP function after the Monitoring Time.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 121 (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 8.2.86-1: Subsequent 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.

## 8.2.87 Subsequent Time Quota

The Subsequent Time Quota IE type shall be encoded as shown in Figure 8.2.87-1. It contains the time quota to be monitored by the UP function after the Monitoring Time.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 122 (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 8.2.87-1: Subsequent Time Quota**

The Time Quota value shall be encoded as an Unsigned32 binary integer value. It contains a duration in seconds.

## 8.2.88 RQI

The Reflective QoS Indicator (RQI) IE shall be encoded as shown in Figure 8.2.88-1. It indicates if Reflective QoS applies for the UL.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 123 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | RQI |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.88-1: RQI**

The value of RQI flag shall be set as follows:

- RQI set to 0: deactivate Reflective QoS;
- RQI set to 1: activate Reflective QoS.

See also clause 5.5.3.4 of 3GPP TS 38.415 [34].

## 8.2.89 QFI

The QFI IE type shall be encoded as shown in Figure 8.2.89-1. It contains an QoS flow identifier identifying a QoS flow in a 5G system filter.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 124 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | QFI value | | | | |
| p to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.89-1: QFI**

The QFI value shall be encoded as binary integer value, as specified in clause 5.5.3.3 of 3GPP TS 38.415 [34].

## 8.2.90 Query URR Reference

The Query URR Reference IE type shall be encoded as shown in Figure 8.2.90-1. It shall contain the reference of a query request for URR(s).

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 125 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Query URR Reference value | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.90-1: Query URR Reference**

The Query URR Reference value shall be encoded as an Unsigned32 binary integer value.

## 8.2.91 Additional Usage Reports Information

The Additional Usage Reports Information IE type shall be encoded as shown in Figure 8.2.91-1. It shall either indicate that additional usage reports will follow, or contain the total number of usage reports that need to be sent in all the additional PFCP Session Report Request messages after the PFCP Session Modification Response or PFCP Session Deletion Response (see clause 5.2.2.3.1).

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 126 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | AURI | Number of Additional Usage Reports value | | | | | | |
| 6 | Number of Additional Usage Reports value | | | | | | | |
| 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.91-1: Additional Usage Reports Information**

The Number of Additional Usage Reports value shall be encoded as an unsigned binary integer value on 15 bits. Bit 7 of Octet 5 is the most significant bit and bit 1 of Octet 6 is the least significant bit.

The bit 8 of octet 5 shall encode the AURI (Additional Usage Reports Indication) flag:

- when set to "1", it indicates that additional usage reports will follow. In this case, the Number of Additional Usage Reports value shall be set to "0" by the sender and ignored by the receiver;
- when set to "0", the Number of Additional Usage Reports value shall be set to the total number of additional usage reports to be sent in PFCP Session Report Request messages.

## 8.2.92 Traffic Endpoint ID

The Traffic Endpoint ID IE type shall be encoded as shown in Figure 8.2.92-1. It shall contain a Traffic Endpoint ID.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 131 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Traffic Endpoint ID value | | | | | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.92-1: Traffic Endpoint ID**

The Traffic Endpoint ID value shall be encoded as a binary integer value within the range of 0 to 255.

## 8.2.93 MAC address

The MAC address IE shall be encoded as shown in Figure 8.2.93-1. It shall contain an MAC address value.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 133 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | spare | | | | UDES | USOU | DEST | SOUR |
| m to (m+5) | Source MAC address value | | | | | | | |
| n to (n+5) | Destination MAC address value | | | | | | | |
| o to (o+5) | Upper Source MAC address value | | | | | | | |
| p to (p+5) | Upper Destination MAC address value | | | | | | | |
| s to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.93-1: MAC address**

The following flags are coded within Octet 5:

- Bit 1 – SOUR (Source): If this bit is set to "1", then the source MAC address value is provided.
- Bit 2 – DEST (Destination): If this bit is set to "1", then the destination MAC address value is provided.
- Bit 3 – USOU (Source): If this bit is set to "1", then the source MAC address value contains the lower value and Upper Source MAC address value contains the upper value of an MAC address range.
- Bit 4 – UDES (Destination): If this bit is set to "1", then the destination MAC address value contains the lower value and Upper Destination MAC address value contains the upper value of an MAC address range.- Bit 5 to 8: Spare, for future use and set to "0".

Octets "m to (m+5)" or "n to (n+5)" and "o to (o+5)" or "p to (p+5)", if present, shall contain an MAC address value (12-digit hexadecimal numbers).

## 8.2.94 C-TAG (Customer-VLAN tag)

The C-TAG IE shall be encoded as shown in Figure 8.2.94-1. It shall contain the Customer-VLAN tag (C-TAG) as defined in IEEE 802.1Q [30].

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 134 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | VID | DEI | PCP |
| 6 | C-VID value | | | | DEI Flag | PCP value | | |
| 7 | C-VID Value | | | | | | | |
| 8 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.94-1: C-TAG (Customer-VLAN tag)**

The following flags are coded within Octet 5:

- Bit 1 – PCP: If this bit is set to "1", then PCP Value field shall used by the receiver, otherwise the PCP Value field shall be ignored.
- Bit 2 – DEI: If this bit is set to "1", then DEI flag field shall used by the receiver, otherwise the DEI flag field shall be ignored.
- Bit 3 – VID: If this bit is set to "1", then C-VID value field shall used by the receiver, otherwise the VID Value field shall be ignored.
- Bit 4 to 8 – spare and reserved for future use.

The PCP value, DEI flag and C-VID Value are specified in IEEE 802.1Q [30] tag format.

Octet 6 / Bit 3 shall contain the most significant bit of the PCP value.

Octet 6 / Bit 8 shall be the most significant bit of the C-VID value and Octet 7 / Bit 1 shall be the least significant bit (see clause 7.1).

NOTE: The encoding of the C-Tag in PFCP differs from the encoding of the C-Tag defined in IEEE 802.1Q [30].

## 8.2.95 S-TAG (Service-VLAN tag)

The S-TAG IE type shall be encoded as shown in Figure 8.2.95-1. It shall contain Service-VLAN tag (S-TAG) as defined in IEEE 802.1Q [30]

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 135 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | VID | DEI | PCP |
| 6 | S-VID value | | | | DEI Flag | PCP value | | |
| 7 | S-VID value | | | | | | | |
| 8 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.95-1: S-TAG (Service-VLAN tag)**

The following flags are coded within Octet 5:

- Bit 1 – PCP: If this bit is set to "1", then PCP Value field shall used by the receiver, otherwise the PCP Value field shall be ignored.
- Bit 2 – DEI: If this bit is set to "1", then DEI flag field shall used by the receiver, otherwise the DEI flag field shall be ignored.
- Bit 3 – VID: If this bit is set to "1", then VID value field shall used by the receiver, otherwise the VID Value field shall be ignored.
- Bit 4 to 8 – spare and reserved for future use.

The PCP value, DEI flag and S-VID Value are specified in IEEE 802.1Q [30] tag format.

Octet 6 / Bit 3 shall contain the most significant bit of the PCP value.

Octet 6 / Bit 8 shall be the most significant bit of the S-VID value and Octet 7 / Bit 1 shall be the least significant bit (see clause 7.1).

NOTE: The encoding of the S-Tag in PFCP differs from the encoding of the S-Tag defined in IEEE 802.1Q [30].

## 8.2.96 Ethertype

The Ethertype IE type shall be encoded as shown in Figure 8.2.96-1. It contains an Ethertype as defined in IEEE 802.3 [31].

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 136 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 6 | Ethertype | | | | | | | |
| 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.96-1: Ethertype**

## 8.2.97 Proxying

The Proxying IE shall be encoded as shown in Figure 8.2.97-1. It specifies if responding to Address Resolution Protocol (ARP) (see IETF RFC 826 [32]) and / or IPv6 Neighbour Solicitation (see IETF RFC 4861 [33]) as specified in clause 5.6.10.2 of 3GPP TS 23.501 [28], functionality for the Ethernet PDUs is performed in UPF.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 137 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | INS | ARP |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.97-1: Proxying**

The following flags are coded within Octet 5:

- Bit 1 – ARP: If this bit is set to "1", then responding ARP is performed in UPF based on local cache information.
- Bit 2 – INS: If this bit is set to "1", then responding to IPv6 Neighbour Solicitation is performed in UPF based on local cache information.
- Bit 3 to 8 – spare and reserved for future use.

## 8.2.98 Ethernet Filter ID

The Ethernet Filter ID IE type shall be encoded as shown in Figure 8.2.98-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 138 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Ethernet Filter ID value | | | | | | | |
| 10 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.98-1: Ethernet Filter ID**

The Ethernet Filter ID value shall be encoded as an Unsigned32 binary integer value.

## 8.2.99 Ethernet Filter Properties

The Ethernet Filter Properties IE type shall be encoded as shown in Figure 8.2.99-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 139 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | BIDE |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.99-1: Ethernet Filter Properties**

The following flags are coded within Octet 5:

- Bit 1 – BIDE (Bidirectional Ethernet Filter): If this bit is set to "1", then the Ethernet Filter identified by the Ethernet Filter ID is bidirectional.
- Bit 2 to 8 – spare and reserved for future use.

## 8.2.100 Suggested Buffering Packets Count

The Suggested Buffering Packets Count IE indicates the number of packets (including both UL and DL packets) that are suggested to be buffered by the UP function while waiting for the new instruction from the CP function. It is coded as depicted in Figure 8.2.100-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 140 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Packet Count value | | | | | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.100-1: Suggested Buffering Packets Count**

The Packet Count value is encoded in octet 5 and the range of the Packet Count value is from 0 to 255.

## 8.2.101 User ID

The User ID IE type shall be encoded as shown in Figure 8.2.101-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 141 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | PEIF | GPSIF | SUPIF | NAIF | MSISDNF | IMEIF | IMSIF |
| 6 | Length of IMSI | | | | | | | |
| 7 to a | IMSI | | | | | | | |
| b | Length of IMEI | | | | | | | |
| (b+1) to c | IMEI | | | | | | | |
| d | Length of MSISDN | | | | | | | |
| (d+1) to e | MSISDN | | | | | | | |
| f | Length of NAI | | | | | | | |
| (f+1) to g | NAI | | | | | | | |
| h | Length of SUPI | | | | | | | |
| (h+1) to i | SUPI | | | | | | | |
| j | Length of GPSI | | | | | | | |
| (j+1) to k | GPSI | | | | | | | |
| l | Length of PEI | | | | | | | |
| (l+1) to m | PEI | | | | | | | |
| p to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.101-1: User ID**

The following flags are coded within Octet 5:

- Bit 1 – IMSIF: If this bit is set to "1", then the Length of IMSI and IMSI fields shall be present, otherwise these fields shall not be present.
- Bit 2 – IMEIF: If this bit is set to "1", then the Length of IMEI and IMEI fields shall be present, otherwise these fields shall not be present.
- Bit 3 – MSISDNF: If this bit is set to "1", then the Length of MSISDN and MSISDN fields shall be present, otherwise these fields shall not be present.
- Bit 4 – NAIF: If this bit is set to "1", then the Length of NAI and NAI fields shall be present, otherwise these fields shall not be present.
- Bit 5 – SUPIF: If this bit is set to "1", then the Length of SUPI and SUPI fields shall be present, otherwise these fields shall not be present.
- Bit 6 – GPSIF: If this bit is set to "1", then the Length of GPSI and GPSI fields shall be present, otherwise these fields shall not be present.
- Bit 7 – PEIF: If this bit is set to "1", then the Length of PEI and PEI fields shall be present, otherwise these fields shall not be present.- Bit 8: Spare, for future use and set to "0".

One or more flags may be set to "1".

For 5GS User Identities:

- The SUPI field shall only be used for carrying a Global Cable Identifier (GCI) or a Global Line Identifier (GLI). The IMSI and NAI, if received by the SMF in the SUPI, shall be included in the IMSI and NAI field respectively.
- The GPSI field shall only be used for carrying an External Identifier. The MSISDN, if received by the SMF in the SUPI, shall be included in the MSISDN field.
- The PEI field shall only be used for carrying an MAC address or an Extended Unique Identifier. The IMEI, if received by the SMF in the PEI, shall be included in the IMEI field.

The coding of IMSI field, from octets 7 to 'a' shall be encoded as the octets 5 to n+4 of the IMSI IE type specified in clause 8.3 of 3GPP TS 29.274 [9].

The coding of IMEI field, in octets 'b+1' to 'c' shall be encoded as the octets 5 to n+4 of the MEI IE type specified in clause 8.10 of 3GPP TS 29.274 [9].

The coding of MSISDN field, in octets 'd+1' to 'e' shall be encoded as the octets 5 to n+4 of the MSISDN IE type specified in clause 8.11 of 3GPP TS 29.274 [9].

The coding of the SUPI field, in octets 'h+1' to 'i' shall be encoded as the Supi data type specified in clause 5.3.2 of 3GPP TS 29.571 [61].

The coding of the GPSI field, in octets 'j+1' to 'k' shall be encoded as the Gpsi data type specified in clause 5.3.2 of 3GPP TS 29.571 [61].

The coding of the PEI field, in octets 'l+1' to 'm' shall be encoded as the Pei data type specified in clause 5.3.2 of 3GPP TS 29.571 [61].

The NAI field, in octets 'f+1' to 'g' shall be encoded as an Octet String (see IETF RFC 4282 [36]).

## 8.2.102 Ethernet PDU Session Information

Ethernet PDU Session Indication is coded as depicted in Figure 8.2.102-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 142 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | ETHI |
| k to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.102-1: Ethernet PDU Session Information**

The following flags are coded within Octet 5:

- Bit 1 – ETHI (Ethernet Indication): This bit shall be set to "1". This refers to all the DL traffic matching the Ethernet PDU session (see clause 5.13.1).

- Bit 2 to 8 are spare and reserved for future use.

## 8.2.103 MAC Addresses Detected

The MAC Addresses Detected IE shall be encoded as shown in Figure 8.2.103-1. It shall contain a list of MAC address values.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 144 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Number of MAC addresses (k) | | | | | | | |
| 6 to 11 | MAC address value 1 | | | | | | | |
| o to (o+5) | MAC address value 2 | | | | | | | |
| p to (p+5) | … | | | | | | | |
| q to (q+5) | MAC address value k | | | | | | | |
| s | Length of C-TAG field | | | | | | | |
| (s+1) to t | C-TAG | | | | | | | |
| u | Length of S-TAG field | | | | | | | |
| (u+1) to v | S-TAG | | | | | | | |
| w to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.103-1: MAC addresses Detected**

Octet 5 shall encode the number of 48-bit MAC addresses.

MAC address values shall be encoded as 12-digit hexadecimal numbers.

The Length of C-TAG field shall indicate the length of the C-TAG field. It shall be set to 0 if the C-TAG field is absent.

When present, the C-TAG field shall be encoded as the Customer-VLAN tag defined in clause 8.2.94, excluding octets 1 to 4.

The Length of S-TAG field shall indicate the length of the S-TAG field. It shall be set to 0 if the S-TAG field is absent.

When present, the S-TAG field shall be encoded as the Service-VLAN Tag defined in clause 8.2.95, excluding octets 1 to 4.

## 8.2.104 MAC Addresses Removed

The MAC Addresses Removed IE shall be encoded as shown in Figure 8.2.104-1. It shall contain a list of MAC address values.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 145 (decimal) |
| 3 to 4 | Length = n |
| 5 | Number of MAC addresses (k) |
| 6 to 11 | MAC address value 1 |
| o to (o+5) | MAC address value 2 |
| p to (p+5) | … |
| q to (q+5) | MAC address value k |
| s | Length of C-TAG field |
| (s+1) to t | C-TAG |
| u | Length of S-TAG field |
| (u+1) to v | S-TAG |
| w to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.104-1: MAC addresses Removed**

Octet 5 shall encode the number of 48-bit MAC addresses.

MAC address values shall be encoded as 12-digit hexadecimal numbers.

The Length of C-TAG field shall indicate the length of the C-TAG field. It shall be set to 0 if the C-TAG field is absent.

When present, the C-TAG field shall be encoded as the Customer-VLAN tag defined in clause 8.2.94, excluding octets 1 to 4.

The Length of S-TAG field shall indicate the length of the S-TAG field. It shall be set to 0 if the S-TAG field is absent.

When present, the S-TAG field shall be encoded as the Service-VLAN Tag defined in clause 8.2.95, excluding octets 1 to 4.

## 8.2.105 Ethernet Inactivity Timer

The Ethenet Inactivity Timer IE contains the inactivity time period, in seconds, to be monitored by the UP function, to detect that a UE MAC address is inactive. It shall be encoded as shown in Figure 8.2.105-1.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 146 (decimal) |
| 3 to 4 | Length = n |
| 5 to 8 | Ethernet Inactivity Timer |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.105-1: Ethernet Inactivity Timer**

The Ethernet Inactivity Timer field shall be encoded as an Unsigned32 binary integer value.

## 8.2.106 Subsequent Event Quota

The Subsequent Event Quota IE type shall be encoded as shown in Figure 8.2.106-1. It contains the event quota to be monitored by the UP function.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 150 (decimal) |
| 3 to 4 | Length = n |
| 5 to 8 | Subsequent Event Quota |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.106-1: Subsequent Event Quota**

The Subsequent Event Quota field shall be encoded as an Unsigned32 binary integer value.

## 8.2.107 Subsequent Event Threshold

The Subsequent Event Threshold IE contains the Number of events after which the measurement report is to be generated by the UP function. It shall be encoded as shown in Figure 8.2.107-1.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 151 (decimal) |
| 3 to 4 | Length = n |
| 5 to 8 | Subsequent Event Threshold |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.107-1: Subsequent Event Threshold**

The Subsequent Event Threshold field shall be encoded as an Unsigned32 binary integer value.

## 8.2.108 Trace Information

The Trace Information IE type shall be encoded as shown in Figure 8.2.108-1. It contains the trace control and configuration parameters to apply for the PFCP session.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 152 (decimal) |
| 3 to 4 | Length = n |
| 5 | MCC digit 2 \| MCC digit 1 |
| 6 | MNC digit 3 \| MCC digit 3 |
| 7 | MNC digit 2 \| MNC digit 1 |
| 8 to10 | Trace ID |
| 11 | Length of Triggering Events |
| 12 to m | Triggering Events |
| m+1 | Session Trace Depth |
| m+2 | Length of List of Interfaces |
| (m+3) to p | List of Interfaces |
| p+1 | Length of IP Address of Trace Collection Entity |
| (p+2) to q | IP Address of Trace Collection Entity |
| (q+1) to (n-4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.108-1: Trace Information**

Octets 5 to 10 represent the Trace Reference parameter as defined in clause 5.6 of 3GPP TS 32.422 [35].

Triggering Events, Session Trace Depth, List of Interfaces and IP Address of Trace Collection Entity are specified in 3GPP TS 32.422 [35].

Octets "(p+2) to q" shall contain an IPv4 address value (4 octets) or IPv6 address value (16 octets).

See 3GPP TS 24.008 [5], clause 10.5.1.4, Mobile Identity, for the coding of MCC and MNC. If MNC is 2 digits long, bits 5 to 8 of octet 6 are coded as "1111".

## 8.2.109 Framed-Route

The Framed-Route IE describes a framed route. It shall be encoded as shown in Figure 8.2.109-1.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 153 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Framed-Route | | | | | | | |

**Figure 8.2.109-1: Framed-Route**

The Framed-Route field shall be encoded as an Octet String as the value part of the Framed-Routing AVP specified in IETF RFC 2865 [37].

## 8.2.110 Framed-Routing

The Framed-Routing IE describes the frame routing of a framed route. It shall be encoded as shown in Figure 8.2.110-1.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 154 (decimal) | | | | | | | |
| 3 to 4 | Length = 4 | | | | | | | |
| 5 to 8 | Framed-Routing | | | | | | | |

**Figure 8.2.110-1: Framed-Routing**

The Framed-Routing field shall be encoded as the value part of the Framed-Routing AVP specified in IETF RFC 2865 [37].

## 8.2.111 Framed-IPv6-Route

The Framed-IPv6-Route IE describes a framed IPv6 route. It shall be encoded as shown in Figure 8.2.111-1.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 155 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Framed-IPv6-Route | | | | | | | |

**Figure 8.2.111-1: Framed-IPv6-Route**

The Framed-IPv6-Route field shall be encoded as an Octet String as the value part of the Framed-IPv6-Route AVP specified in IETF RFC 3162 [38].

## 8.2.112 Event Quota

The Event Quota IE type shall be encoded as shown in Figure 8.2.112-1. It contains the event quota to be monitored by the UP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 148 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Subsequent Event Quota | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.112-1: Event Quota**

The Event Quota field shall be encoded as an Unsigned32 binary integer value.

## 8.2.113 Event Threshold

The Event Threshold IE contains the Number of events after which the measurement report is to be generated by the UP function. It shall be encoded as shown in Figure 8.2.113-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 149 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Event Threshold | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.113-1: Event Threshold**

The Event Threshold field shall be encoded as an Unsigned32 binary integer value.

## 8.2.114 Time Stamp

The Time Stamp IE indicates the time stamp when certain event occurs or certain operation occurs. It shall be encoded as shown in Figure 8.2.114-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 156 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Time Stamp | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.114-1: Time Stamp**

The Time Stamp 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 clause 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.

## 8.2.115 Averaging Window

The Averaging Window IE shall contain the duration over which the GFBR and MFBR is calculated (see clause 5.7.3.6 of 3GPP TS 23.501 [28]). It shall be encoded as shown in Figure 8.2.115-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 157 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Averaging Window | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.115-1: Averaging Window**

The Averaging Window field shall be encoded as an Unsigned32 binary integer value. It shall contain the duration in ms.

## 8.2.116 Paging Policy Indicator (PPI)

The Paging Policy Indicator (PPI) IE indicates a PPI value for paging policy differentation. It shall be encoded as shown in Figure 8.2.116-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 158 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | PPI value | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.116-1: Paging Policy Indicator (PPI)**

The PPI value shall be encoded as a value between 0 and 7, as specified in clause 5.5.3.7 of 3GPP TS 38.415 [34].

## 8.2.117 APN/DNN

Access Point Name (APN) / Data Network Name (DNN) is transferred from CP function to UP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 159 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | APN/DNN | | | | | | | |

**Figure 8.2.117-1: APN/DNN**

The encoding the APN/DNN field follows 3GPP TS 23.003 [2] clause 9.1. The content of the APN/DNN field shall be the full APN/DNN with both the APN/DNN Network Identifier and APN/DNN Operator Identifier being present as specified in 3GPP TS 23.003 [2] clauses 9.1.1 and 9.1.2, 3GPP TS 23.060 [19] Annex A and 3GPP TS 23.401 [14] clauses 4.3.8.1.

NOTE: The APN/DNN field is not encoded as a dotted string as commonly used in documentation.

## 8.2.118 3GPP Interface Type

The 3GPP Interface Type IE shall be encoded as shown in Figure 8.2.118-1. It indicates the 3GPP interface type of the Source Interface within the PDR IE, or the 3GPP interface type of the Destination Interface within the FAR IE.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 160 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | Interface Type value | | | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.118-1: 3GPP Interface Type**

The 3GPP Interface Type value shall be encoded as a 6 bits binary integer as specified in in Table 8.2.118-1.

**Table 8.2.118-1: Interface Type value**

| Interface value | Values (Decimal) |
|---|---|
| S1-U | 0 |
| S5 /S8-U (NOTE 1) | 1 |
| S4-U | 2 |
| S11-U | 3 |
| S12 | 4 |
| Gn/Gp-U (NOTE 2) | 5 |
| S2a-U | 6 |
| S2b-U | 7 |
| eNodeB GTP-U interface for DL data forwarding | 8 |
| eNodeB GTP-U interface for UL data forwarding | 9 |
| SGW/UPF GTP-U interface for DL data forwarding | 10 |
| N3 3GPP Access | 11 |
| N3 Trusted Non-3GPP Access | 12 |
| N3 Untrusted Non-3GPP Access | 13 |
| N3 for data forwarding | 14 |
| N9 (or N9 for non-roaming, see NOTE 3) | 15 |
| SGi | 16 |
| N6 | 17 |
| N19 | 18 |
| S8-U | 19 |
| Gp-U | 20 |
| N9 for roaming | 21 |
| Iu-U | 22 |
| N9 for data forwarding | 23 |
| Sxa-U | 24 |
| Sxb-U | 25 |
| Sxc-U | 26 |
| N4-U | 27 |
| SGW/UPF GTP-U interface for UL data forwarding | 28 |
| N6mb/Nmb9 | 29 |
| N3mb | 30 |
| N19mb | 31 |
| Spare | 32 to 63 |
| NOTE 1: If separation of roaming and non-roaming traffic is desired this value should only be used for the S5-U interface and "S8-U" (decimal 19) should be used for the S8-U interface.<br>NOTE 2: If separation of roaming and non-roaming traffic is desired this value should only be used for the Gn-U interface and "Gp-U" (decimal 20) should be used for the Gp-U interface.<br>NOTE 3: If separation of roaming and non-roaming traffic is desired, this value should only be used for N9 non-roaming interfaces and (decimal value "21") should be used for N9 roaming interfaces. | |

## 8.2.119 PFCPSRReq-Flags

The PFCPSRReq-Flags IE indicates flags applicable to the PFCP Session Report Request message. It is coded as depicted in Figure 8.2.119-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 161 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | Spare | Spare | PSDBU |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.199-1: PFCPSRReq-Flags**

The following bits within Octet 5 shall indicate:

- Bit 1 – PSDBU (PFCP Session Deleted By the UP function): if this bit is set to "1", it indicates that the UP function has reported all non-zero Usage Reports for all URRs in the PFCP Session and the PFCP Session is being deleted in the UP function locally.

- Bit 2 to 8 – Spare, for future use, shall be set to "0" by the sender and discarded by the receiver.

## 8.2.120 PFCPAUReq-Flags

The PFCPAUReq-Flags IE indicates flags applicable to the PFCP Association Update Request message. It is coded as depicted in Figure 8.2.120-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 162 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | Spare | Spare | PARPS |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.120-1: PFCPAUReq-Flags**

The following bits within Octet 5 shall indicate:

- Bit 1 – PARPS (PFCP Association Release Preparation Start): if this bit is set to "1", it indicates that the PFCP association is to be released and all non-zero usage reports for the PFCP Sessions affected by the release of the PFCP association shall be reported.

- Bit 2 to 8 – Spare, for future use, shall be set to "0" by the sender and discarded by the receiver.

## 8.2.121 Activation Time

The Activation Time IE indicates the time that the PDR shall be set to be active in the UP function. It shall be encoded as shown in Figure 8.2.121-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 163 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Activation Time | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.121-1: Activation Time**

The Activation Time field shall indicate the activation 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 clause 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.

## 8.2.122 Deactivation Time

The Deactivation Time IE indicates the time that the PDR shall be set to be inactive in the UP function. It shall be encoded as shown in Figure 8.2.122-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 164 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Deactivation Time | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.122-1: Deactivation Time**

The Deactivation Time field shall indicate the deactivation 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 clause 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.

## 8.2.123 MAR ID

The MAR ID IE type shall be encoded as shown in Figure 8.2.123-1. It shall contain a Multi-Access Rule ID.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 170 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 6 | MAR ID value | | | | | | | |
| 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.123-1: MAR ID**

The MAR ID value field shall be encoded as an Unsigned16 binary integer value.

## 8.2.124 Steering Functionality

The Steering Functionality IE type shall be encoded as shown in Figure 8.2.124-1. It indicates the steering functionality (ATSSS feature) to be used in a MAR.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 171 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | Steering Functionality Value | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.124-1: Steering Functionality**

The Steering Functionality value shall be encoded as a 4 bits binary integer as specified in Table 8.2.124-1.

**Table 8.2.124-1: Steering Functionality value**

| Steering Functionality Value | Values (Decimal) |
|---|---|
| ATSSS-LL | 0 |
| MPTCP | 1 |
| Spare | 2 to 15 |

## 8.2.125 Steering Mode

The Steering Mode IE type shall be encoded as shown in Figure 8.2.125-1. It indicates the steering mode to be used in a MAR.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 172 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | Steering Mode Value | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.125-1: Steering Mode**

The Steering Mode value shall be encoded as a 4 bits binary integer as specified in Table 8.2.125-1.

**Table 8.2.125-1: Steering Mode value**

| Steering Mode Value | Values (Decimal) |
|---|---|
| Active-Standby | 0 |
| Smallest Delay | 1 |
| Load Balancing | 2 |
| Priority-based | 3 |
| Spare | 4 to 15 |

## 8.2.126 Weight

The Weight IE shall be encoded as shown in Figure 8.2.126-1. It indicates the percentage of the traffic to be transferred over one access.

The Weight Value field shall take binary coded integer values from 0 up to 100. Other values shall be considered as 0.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 173 (decimal) | | | | | | | |
| 3 to 4 | Length = 1 | | | | | | | |
| 5 | Weight Value | | | | | | | |

**Figure 8.2.126-1: Weight**

## 8.2.127 Priority

The Priority IE type shall be encoded as shown in Figure 8.2.127-1. It indicates whether it is active or standby or no standby for a given access when the Steering Mode is set to Active-Standby, or whether it is high or low priority for a given access when the Steering Mode is set to Priority-based.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 174 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | Priority Value | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.127-1: Priority**

The Priority Value shall be encoded as a 4 bits binary integer as specified in Table 8.2.127-1.

**Table 8.2.127-1: Priority value**

| Priority Value | Values (Decimal) |
|---|---|
| Active | 0 |
| Standby | 1 |
| No Standby | 2 |
| High | 3 |
| Low | 4 |
| Spare | 5 to 15 |

The "No Standby" Priority value may be used when the network determines to not define a Standby access.

## 8.2.128 UE IP address Pool Identity

The User Plane UE IP Pool Identity IE type shall be encoded as shown in Figure 8.2.128-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 177 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 6 | UE IP address Pool Id Length | | | | | | | |
| 7 to k | UE IP address Pool Identity | | | | | | | |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.128-1: UE IP address Pool Identity**

Octets 7 to "k": The UE IP address Pool Identity shall be encoded as an OctetString (see the Framed-Ipv6-Pool and Framed-Pool in clause 12.6.3 of 3GPP TS 29.561 [49]); the value part of Framed-Pool or Framed-Ipv6-Pool is copied into the UE IP address Pool Identity field of the UE IP address Pool Identity IE if the CP function receives the corresponding information from an external server.

## 8.2.129 Alternative SMF IP Address

The Alternative SMF IP Address IE shall contain an IPv4 and/or IPv6 address. It shall be encoded as shown in Figure 8.2.129-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 178 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | PPE | V4 | V6 |
| p to (p+3) | IPv4 Address | | | | | | | |
| q to (q+15) | IPv6 Address | | | | | | | |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.129-1: Alternative SMF 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 Alternative SMF 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 Alternative SMF IP Address, otherwise the IPv4 address field shall not be present.
- Bit 3 – PPE (Preferred PFCP Entity): If this bit is set to "1", then the alternative SMF IP address shall be used by the UPF as a preferred address when reselecting a PFCP entity as specified in clauses 5.22.2 and 5.22.3.
- Bit 4 to 8 Spare, for future use and set to "0".

Octets "p to (p+3)" or "q to (q+15)" (IPv4 address / IPv6 address fields), if present, shall contain the address value.

## 8.2.130 Packet Replication and Detection Carry-On Information

The Packet Replication and Detection Carry-On Information IE shall be encoded as shown in Figure 8.2.130-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 179 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | DCARONI | PRIN6I | PRIN19I | PRIUEAI |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.130-1: Packet Replication and Detection Carry-On Information**

The following flags are coded within Octet 5:

- Bit 1 – PRIUEAI (Packet Replication Information – UE/PDU Session Address Indication): This bit shall be set to "1" to indicate that if the packet has been received from the UE's PDU session (e.g. the source IP address is set to the UE's PDU IP session address, or the source MAC address is an Ethernet MAC address associated to the PDU session for an Ethernet PDU session), the UP function shall neither create a copy of the packet nor apply the corresponding processing (i.e. FAR, QER, URR). Otherwise the UPF shall perform a copy of the packet and apply the corresponding processing (i.e. FAR, QER, URR).

- Bit 2 – PRIN19I (Packet Replication Information - N19 Indication): This bit shall be set to "1" to indicate that if the packet has been received from a N19 interface (i.e. a "N19 Indication" internal flag is associated with the packet, see clause 8.2.56)), the UP function shall neither create a copy of the packet nor apply the corresponding processing (i.e. FAR, QER, URR). Otherwise the UPF shall perform a copy of the packet and apply the corresponding processing (i.e. FAR, QER, URR).

- Bit 3 – PRIN6I (Packet Replication Information - N6 Indication): This bit shall be set to "1" to indicate that if the packet has been received from a N6 interface (i.e. a "N6 Indication" internal flag is associated with the packet, see clause 8.2.56)), the UP function shall neither create a copy of the packet nor apply the corresponding processing (i.e. FAR, QER, URR). Otherwise the UPF shall perform a copy of the packet and apply the corresponding processing (i.e. FAR, QER, URR).

- Bit 4 – DCARONI (Detection Carry-On Indication): This bit shall be set to "1" to request the UP function to continue the packet detection process, i.e. look up of other PDRs of other PFCP sessions matching the packet (see clause 5.2.1).

- Bit 5 to 8 are spare and reserved for future use.

## 8.2.131 SMF Set ID

The SMF Set ID IE shall contain an FQDN representing the SMF Set. It shall be encoded as shown in Figure 8.2.131-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 180 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | |
| 6 to m | FQDN | | | | | | | |
| (m+1) to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.131-1: SMF Set ID**

FQDN encoding shall be identical to the encoding of a FQDN within a DNS message of clause 3.1 of IETF RFC 1035 [27] but excluding the trailing zero byte.

NOTE: The FQDN field in the IE is not encoded as a dotted string as commonly used in DNS master zone files.

## 8.2.132 Quota Validity Time

The Quota Validity Time IE type shall be encoded as shown in Figure 8.2.132-1. It contains the quota validity time in seconds.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 181 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Validity Time value | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.132-1: Quota Validity Time**

The Quota Validity Time value shall be encoded as an Unsigned32 binary integer value.

## 8.2.133 Number of Reports

The Number of Reports IE shall be encoded as shown in Figure 8.2.133-1. It contains an Unigned16 binary integer value excluding the first value "0".

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 182 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 6 | Number of Reports | | | | | | | |

**Figure 8.2.133-1: Number of Reports**

## 8.2.134 PFCPASRsp-Flags

The PFCPASRsp-Flags IE indicates flags applicable to the PFCP Association Setup Response message. It is coded as depicted in Figure 8.2.134-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 184 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | UUPSI | PSREI |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.134-1: PFCPASRsp-Flags**

The following bits within Octet 5 shall indicate:

- Bit 1 – PSREI (PFCP Session Retained Indication): if this bit is set to "1", it indicates that an existing PFCP association was already established for the same Node ID and the requested PFCP sessions have been retained. See clause 6.2.6.2.2.
- Bit 2 – UUPSI (UPF configured for IPUPS Indication): if this bit is set to "1", it indicates that the UPF is configured to be used for IPUPS. See clause 5.27.
- Bit 3 to 8 – Spare, for future use, shall be set to "0" by the sender and discarded by the receiver.

## 8.2.135 CP PFCP Entity IP Address

The CP PFCP Entity IP Address IE shall contain an IPv4 and/or IPv6 address. It shall be encoded as shown in Figure 8.2.135-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 135 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | V4 | V6 |
| p to (p+3) | IPv4 Address | | | | | | | |
| q to (q+15) | IPv6 Address | | | | | | | |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.135-1: CP PFCP Entity 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 CP PFCP Entity 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 CP PFCP Entity IP Address, otherwise the IPv4 address field shall not be present.
- Bit 3 to 8 Spare, for future use and set to "0".

Octets "p to (p+3)" or "q to (q+15)" (IPv4 address / IPv6 address fields), if present, shall contain the address value.

## 8.2.136 PFCPSEReq-Flags

The PFCPSEReq-Flags IE indicates flags applicable to the PFCP Session Establishment Request message. It is coded as depicted in Figure 8.2.136-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 186 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | Spare | SUMPC | RESTI |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.136-1: PFCPSEReq-Flags**

The following bits within Octet 5 shall indicate:

- Bit 1 – RESTI (Restoration Indication): if this bit is set to "1", it indicates to the UP function that the PFCP session to be established is to restore an existing PFCP session.
- Bit 2 – SUMPC (Stop of Usage Measurement to Pause Charging): if this bit is set to "1", it indicates that the UP function shall stop the usage measurement for all URRs with the "ASPOC" flag set to "1".

## 8.2.137 IP Multicast Address

The IP Multicast Address IE type shall be encoded as shown in Figure 8.2.137-1. It contains an IP multicast address or a range of IP multicast addresses.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 191 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | A | R | V4 | V6 |
| m to (m+3) | (start) IPv4 address | | | | | | | |
| p to (p+15) | (start) IPv6 address | | | | | | | |
| q to (q+3) | (end) IPv4 address | | | | | | | |
| r to (r+15) | (end) IPv6 address | | | | | | | |
| k to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.137-1: IP Multicast Address**

The following flags are coded within Octet 5:

- Bit 1 – V6: If this bit is set to "1", then the (start) IPv6 address field shall be present, otherwise the (start) IPv6 address field shall not be present.
- Bit 2 – V4: If this bit is set to "1", then the (start) IPv4 address field shall be present, otherwise the (start) IPv4 address field shall not be present.
- Bit 3 – R (Range): If this bit is set to "1", this indicates that a range of addresses is included, i.e. that
  - the (start) IPv4 address and (end) IPv4 address fields shall be present if bit 2 (V4) is set to "1";
  - the (start) IPv6 address and (end) IPv6 address fields shall be present if bit 1 (V6) is set to "1",

otherwise (end) address fields shall not be present.

- Bit 4 – Any: If this bit is set to "1", this indicates any IP multicast address; in this case, no IP address field shall be included.
- Bit 5 to 8 Spare, for future use and set to "0".

One and only one of the V6, V4 and A flags shall be set to "1". The R flag may be set if the V6 or the V4 flag is set to "1".

Octets "m to (m+3)", "p to (p+15)", "q to (q+3)", "r to (r+15)" (IPv4 address / IPv6 address fields), if present, shall contain the address value.

## 8.2.138 Source IP Address

The Source IP Address IE type shall be encoded as shown in Figure 8.2.138-1

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 192 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | MPL | V4 | V6 |
| m to (m+3) | IPv4 address | | | | | | | |
| p to (p+15) | IPv6 address | | | | | | | |
| q | mask/prefix length | | | | | | | |
| k to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.138-1: Source 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, 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 – Mask/Prefix Length: If this bit is set to "1", then the mask (for IPv4) / prefix (for IPv6) length field shall be present, otherwise this field shall not be present.

- Bit 4 to 8 Spare, for future use and set to "0".

Octets "m to (m+3)", "p to (p+15)" (IPv4 address / IPv6 address fields), if present, shall contain the address value.

The mask/prefix length field, if present, shall be encoded as a 8 bits binary integer.

EXAMPLE 1: this field encodes the value 24 for the IPv4 subnet 192.0.2.10/24.

EXAMPLE 2: this field encodes the value 64 for the /64 IPv6 prefix.

## 8.2.139 Packet Rate Status

Packet Rate Status shall be encoded as shown in Figure 8.2.139-1.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 193 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | APR | DL | UL |
| a to (a+1) | Number of Remaining Uplink Packets Allowed | | | | | | | |
| b to (b+1) | Number of Remaining Additional Uplink Packets Allowed | | | | | | | |
| c to (c+1) | Number of Remaining Downlink Packets Allowed | | | | | | | |
| d to (d+1) | Number of Remaining Additional Downlink Packets Allowed | | | | | | | |
| e to (e+7) | Rate Control Status Validity Time | | | | | | | |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.139-1: Packet Rate Status**

The following flags are coded within Octet 5:

- Bit 1 – UL (remaining uplink packet limit): If this bit is set to "1", then octets 'a' to (a+1), the Number of Remaining Uplink Packets Allowed shall be present, otherwise these octets shall not present.

- Bit 2 – DL (remaining downlink packet limit): If this bit is set to "1", then octets 'c' to (c+1), the Number of Remaining Downlink Packets Allowed shall be present, otherwise these octets shall not present.

- Bit 3 – APR (Additional Packet Rates, i.e. remaining additional packet limit): If this bit is set to "1", then the presence of Number of Remaining Additional Uplink/Downlink Packets Allowed is determined as follows:

  - If bit 1 (UL) is set to "1", then octets b to (b+1), the Number of Remaining Additional Uplink Packets Allowed shall be present. Otherwise, octets b to (b+1) shall not be present;

  - If bit 2 (DL) is set to "1", then octets d to (d+1), the Number of Remaining Additional Downlink Packets Allowed shall be present. Otherwise, octets d to (d+1) shall not be present.

- Bits 4 to 8: Spare, for future use and set to "0".

If either bit 1 or bit 2 is set to '1', then octets 'e' to (e+7), the Rate Control Status Validity Time shall be present.

If present, the Number of Remaining Uplink Packets Allowed in octets 'a' to (a+1) shall indicate the number of uplink packets that are still allowed to be sent within the Rate Control Status Validity Time.

If present, the Number of Remaining Additional Uplink Packets Allowed in octets 'b' to (b+1) shall indicate the number of additional uplink packets that are still allowed to be sent within the Rate Control Status Validity Time.

If present, the Number of Remaining Downlink Packets Allowed in octets 'c' to (c+1) shall indicate the number of downlink packets that are still allowed to be sent within the Rate Control Status Validity Time.

If present, the Number of Remaining Additional Downlink Packets Allowed in octets 'd' to (d+1) indicate the number of additional downlink packets that are still allowed to be sent within the Rate Control Status Validity Time.

If present, the Rate Control Status Validity Time shall be coded as the time in seconds relative to 00:00:00 on 1 January 1900 (calculated as continuous time without leap seconds and traceable to a common time reference) where binary encoding of the integer part is in the 32 most significant bits and binary encoding of the fraction part in the 32 least significant bits. The fraction part is expressed with a granularity of 1 /2**32 second (see clause 8.135 in 3GPP TS 29.274 [9]).

## 8.2.140 Create Bridge Info for TSC IE

The Create Bridge Info for TSC IE shall be encoded as shown in Figure 8.2.140-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 194 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | BII |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.140-1: Create Bridge Info for TSC IE**

The following flags are coded within Octet 5:

- Bit 1 – BII (Bridge Information Indication): If this bit is set to "1", then the Bridge Information comprising a DS-TT port number and the related 5GS User Plane Node is requested to be provided.
- Bit 2 to 8 Spare, for future use and set to "0".

## 8.2.141 DS-TT Port Number

The DS-TT Port Number IE shall be encoded as shown in Figure 8.2.141-1. It shall contain one Port Number value.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 196 (decimal) | | | | | | | |
| 3 to 4 | Length = 4 | | | | | | | |
| 5 to 8 | Port Number value | | | | | | | |

**Figure 8.2.141-1: DS-TT Port Number**

The Port Number value may refer either to an Ethernet port or an IEEE PTP port and it shall be encoded as an Unsigned16 binary integer value in octets 7 and 8. Octets 5 and 6 shall be set to all zeros.

For Ethernet type PDU Sessions, it is assumed that the PTP port number is the same as the associated Ethernet port number.

## 8.2.142 NW-TT Port Number

The NW-TT Port Number IE shall be encoded as shown in Figure 8.2.142-1. It shall contain one Port Number value.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 197 (decimal) | | | | | | | |
| 3 to 4 | Length = 4 | | | | | | | |
| 5 to 8 | Port Number value | | | | | | | |

**Figure 8.2.142-1: NW-TT Port Number**

The Port Number value may refer either to an Ethernet port or an IEEE PTP port and it shall be encoded as an Unsigned16 binary integer in octets 7 and 8. Octets 5 and 6 shall be set to all zeros.

For Ethernet type PDU Sessions, it is assumed that the PTP port number is the same as the associated Ethernet port number.

## 8.2.143 5GS User Plane Node

The 5GS User Plane Node IE shall be encoded as shown in Figure 8.2.143-1.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 198 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | BID |
| m to (m+7) | User Plane Node value | | | | | | | |
| s to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.143-1: 5GS User Plane Node**

The following flags are coded within Octet 5:

- Bit 1 – BID: If this bit is set to "1", then theUser Plane Node value field shall be present.
- Bit 2 to 8: Spare, for future use and set to "0".

The User Plane Node value field shall be encoded as an Unsigned64 binary integer. To support IEEE TSN, the User Plane Node value field encodes the Bridge ID as defined in IEEE 802.1Q [30] clause 14.2.5. Without IEEE TSN, the User Plane Node ID may encode any value within the range.

## 8.2.144 Port Management Information Container

The Port Management Information Container IE shall be encoded as shown in Figure 8.2.144-1. It contains an opaque container of port management information.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 202 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Port Management Information | | | | | | | |

**Figure 8.2.144-1: Port Management Information Container**

The Port Management Information field shall be encoded as an Octet String. It shall encode an Ethernet port management message defined in clause 8 of 3GPP TS 24.539 [63].

## 8.2.145 Requested Clock Drift Information

The Requested Clock Drift Information IE shall be encoded as shown in Figure 8.2.145-1. It indicates the clock drift information to report to the CP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 204 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | RRCR | RRTO |
| 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.145-1: Requested Clock Drift Information**

Octet 5 shall be encoded as follows:

- Bit 1: (RRTO) Request to Report Time Offset: when set to "1", this indicates a request to report when the Time Offset Reporting Threshold is exceeded.
- Bit 2: (RRCR) Request to Report Cumulative RateRatio: when set to "1", this indicates a request to report when the cumulative RateRatio Reporting Thresholds is exceeded.
- Bits 3 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".

## 8.2.146 Time Domain Number

The Time Domain Number IE type shall be encoded as shown in Figure 8.2.146-1. It shall contain a external timing related Domain Number.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 206 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Time Domain Number value | | | | | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.146-1: Time Domain Number**

The Time Domain Number value field shall be encoded as a binary integer value.

## 8.2.147 Time Offset Threshold

The Time Offset Threshold IE type shall be encoded as shown in Figure 8.2.147-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 207 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 12 | Time Offset Threshold | | | | | | | |
| 13 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.147-1: Time Offset Threshold**

The Time Offset Threshold field shall be encoded as a signed64 binary integer value. It shall contain the Time Offset Threshold in nanoseconds.

## 8.2.148 Cumulative rateRatio Threshold

The Cumulative rateRatio Threshold IE type shall be encoded as shown in Figure 8.2.148-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 208 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Cumulative rateRatio Threshold | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.148-1: Cumulative rateRatio Threshold**

The Cumulative rateRatio Threshold field shall be encoded as the cumulativeRateRatio (Integer32) specified in clauses 14.4.2 and 15.6 of IEEE Std 802.1AS-2020 [58], i.e. the quantity "(rateRatio- 1.0)(2^41)".

## 8.2.149 Time Offset Measurement

The Time Offset Measurement IE type shall be encoded as shown in Figure 8.2.149-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 209 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 12 | Time Offset Measurement | | | | | | | |
| 13 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.149-1: Time Offset Measurement**

The Time Offset Measurement field shall be encoded as a signed64 binary integer value. It shall contain the Time Offset Measurement in nanoseconds. It shall contain the time offset between the 5GS clock and the clock of the external time domain.

## 8.2.150 Cumulative rateRatio Measurement

The Cumulative rateRatio Measurement IE type shall be encoded as shown in Figure 8.2.150-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 210 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Cumulative rateRatio Measurement | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.150-1: Cumulative rateRatio Measurement**

The Cumulative rateRatio Measurement field shall be encoded as the cumulativeRateRatio (Integer32) specified in clauses 14.4.2 and 15.6 of IEEE Std 802.1AS-2020 [58], i.e. the quantity "(rateRatio- 1.0)(2^41)". It shall be equal to the cumulative ratio of the frequency of the 5GS clock to the frequency of the clock of the external time domain.

## 8.2.151 SRR ID

The SRR ID IE type shall be encoded as shown in Figure 8.2.151-1. It contains a Session Reporting Rule ID.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 215 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | SRR ID value | | | | | | | |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.151-1: SRR ID**

The SRR ID value shall be encoded as a binary integer value.

## 8.2.152 Requested Access Availability Information

The Requested Access Availability Information IE shall be encoded as shown in Figure 8.2.152-1. It indicates the access availability information requested to be reported to the CP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 217 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | RRCA |
| 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.152-1: Requested Access Availability Information**

Octet 5 shall be encoded as follows:

- Bit 1: (RRCA) Request to Report Change in Access availability: when set to "1", this indicates a request to the UPF to report when an access (3GPP or non-3GPP access) becomes available or unavailable.
- Bits 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".

## 8.2.153 Access Availability Information

The Access Availability Information IE shall indicate an access type and whether the access type has become available or not available. It shall be encoded as shown in Figure 8.2.153-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 219 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | Availability Status | Access Type |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.153-1: Access Availability Information**

The Access Type shall be encoded as a 2 bits binary integer as specified in Table 8.2.153-1.

**Table 8.2.153-1: Access Type**

| Access Type | Values (Decimal) |
|---|---|
| 3GPP access type | 0 |
| Non-3GPP access type | 1 |
| Spare | 2 to 3 |

The Availability Status shall be encoded as a 2 bits binary integer as specified in Table 8.2.153-2.

**Table 8.2.153-2: Availability Status**

| Availability Status | Values (Decimal) |
|---|---|
| Access has become unavailable | 0 |
| Access has become available | 1 |
| Spare | 2 to 3 |

## 8.2.154 MPTCP Control Information

The MPTCP Control Information IE shall provide details of the required MPTCP functionality. It shall be encoded as shown in Figure 8.2.154-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 222 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | TCI |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.154-1: MPTCP Control Information**

The following flags are coded within Octet 5:

- Bit 1 – TCI (Transport Converter Indication): If this bit is set to "1", it indicates that the required MPTCP steering functionality is of type Transport Converter (see IETF RFC 8803 [60]) and the UPF shall allocate relevant resource as specified in clause 5.20.2.1.

- Bit 2 to 8 Spare, for future use and set to "0".

## 8.2.155 ATSSS-LL Control Information

The ATSSS-LL Control Information IE shall provide details of the required ATSSS-LL functionality. It shall be encoded as shown in Figure 8.2.155-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 223 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | LLI |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.155-1: ATSSS-LL Control Information**

The following flags are coded within Octet 5:

- Bit 1 – LLI: If this bit is set to "1", it indicates that the ATSSS-LL steering functionality is required.

- Bit 2 to 8 Spare, for future use and set to "0".

## 8.2.156 PMF Control Information

The PMF Control Information IE shall provide details of the required PMF functionality. It shall be encoded as shown in Figure 8.2.156-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 224 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | PQPM | DRTTI | PMFI |
| 6 | Number of QFI (=p) | | | | | | | |
| 7 | value of QFI 1 | | | | | | | |
| 8 | value of QFI 2 | | | | | | | |
| ... | … | | | | | | | |
| 7-(7+p-1) | value of QFI p | | | | | | | |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.156-1: PMF Control Information**

The following flags are coded within Octet 5:

- Bit 1 – PMFI: If this bit is set to "1", it indicates that the PMF functionality is required and the UPF shall allocate relevant resource as specified in 5.20.3.1.
- Bit 2 – DRTTI (Disallow PMF RTT Indication): If this bit is set to "1", it indicates that PMF RTT measurements are not allowed. This bit shall be set to "1" if the UE does not support PMF RTT measurements (i.e. if the UE supports MPTCP with any steering mode and ATSSS-LL with only the Active-Standby steering mode, see clauses 5.32.2 and 5.32.5.1 of 3GPP TS 23.501 [28]).
- Bit 3 – PQPM (Per QoS flow Performance Measurement indication): If this bit is set to "1", it indicates that per QoS flow access performance measurement is applicable to this PDU session. A list of QFI values shall be present to indicate a list of QoS flows over which access performance measurement may be performed.
- Bit 4 to 8 Spare, for future use and set to "0".

The Number of QFI shall indicate the total number of the QFI values. Each subsequent Octet after the Number of QFI shall carry one QFI value (i.e. the Octet 5 of the QFI IE, as specified in clause 8.2.89).

## 8.2.157 MPTCP Address Information

The MPTCP Address Information IE shall carry the address information of MPTCP proxy in the UPF. It shall be encoded as shown in Figure 8.2.157-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 228 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | V6 | V4 |
| 6 | MPTCP Proxy Type | | | | | | | |
| 7 to 8 | MPTCP Proxy Port | | | | | | | |
| p to (p+3) | MPTCP Proxy IPv4 Address | | | | | | | |
| q to (q+15) | MPTCP Proxy IPv6 Address | | | | | | | |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.228-1: MPTCP Address Information**

The following flags are coded within Octet 5:

- Bit 1 – V4: If this bit is set to "1", then the MPTCP Proxy IPv4 Address field shall be present in the MPTCP Address Information IE.
- Bit 1 – V6: If this bit is set to "1", then the MPTCP IPv6 Address field shall be present in the MPTCP Address Information IE.
- Bit 3 to 8 Spare, for future use and set to "0".

Octets 6 shall indicate the MPTCP Proxy Type, with the value specified in clause 6.1.4 of 3GPP TS 24.193 [59].

Octets 7 to 8 shall indicate the allocated TCP port number of the MPTCP Proxy.

Octets "p to (p+3)" or "q to (q+15)" (IPv4 address / IPv6 address fields), if present, shall contain the address value.

## 8.2.158 UE Link-Specific IP Address

The UE Link-Specific IP Address IE shall carry link-specific IP address used for MPTCP steering function. It shall be encoded as shown in Figure 8.2.158-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 229 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | NV6 | NV4 | V6 | V4 |
| p to (p+3) | UE Link-Specific IPv4 Address for 3GPP Access | | | | | | | |
| q to (q+15) | UE Link-Specific IPv6 Address for 3GPP Access | | | | | | | |
| r to (r+3) | UE Link-Specific IPv4 Address for Non-3GPP Access | | | | | | | |
| s to (s+3) | UE Link-Specific IPv6 Adress for Non-3GPP Access | | | | | | | |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.158-1: UE Link-Specific IP Address**

The following flags are coded within Octet 5:

- Bit 1 – V4: If this bit is set to "1", then the UE Link-Specific IPv4 Address for 3GPP Access shall be present in the UE Link-Specific IP Address IE.
- Bit 2 – V6: If this bit is set to "1", then the UE Link-Specific IPv6 Address for 3GPP Access shall be present in the UE Link-Specific IP Address IE.
- Bit 3 – NV4: If this bit is set to "1", then the UE Link-Specific IPv4 Address for Non-3GPP Access shall be present in the UE Link-Specific IP Address IE.
- Bit 4 – NV6: If this bit is set to "1", then the UE Link-Specific IPv6 Address for Non-3GPP Access shall be present in the UE Link-Specific IP Address IE.
- Bit 5 to 8 Spare, for future use and set to "0".

Octets "p to (p+3)" or "q to (q+15)" (IPv4 address / IPv6 address fields), if present, shall contain the value for UE Link-Specific IP Address for 3GPP access.

Octets "r to (r+3)" or "s to (s+15)" (IPv4 address / IPv6 address fields), if present, shall contain the value for UE Link-Specific IP Address for Non-3GPP access.

## 8.2.159 PMF Address Information

The PMF Address Information IE shall contain the address information of Performance Measure Function (PMF). It shall be encoded as shown in Figure 8.2.159-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 230 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | MAC | V6 | V4 |
| p to (p+3) | PMF IPv4 Address | | | | | | | |
| q to (q+15) | PMF IPv6 Address | | | | | | | |
| r to (r+1) | PMF Port for 3GPP Access | | | | | | | |
| s to (s+1) | PMF Port for Non-3GPP Access | | | | | | | |
| t to (t+5) | PMF MAC Address for 3GPP Access | | | | | | | |
| u to (u+5) | PMF MAC Address for Non-3GPP Access | | | | | | | |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.159-1: PMF Addresss Information**

The following flags are coded within Octet 5:

- Bit 1 – V4: If this bit is set to "1", it indicates the PMF IPv4 Address filed shall be presend in the PMF Address Information IE, together with: PMF Port for 3GPP Access, PMF Port for Non-3GPP Access.
- Bit 2 – V6: If this bit is set to "1", it indicates the PMF IPv6 Address filed shall be presend in the PMF Address Information IE, together with: PMF Port for 3GPP Access, PMF Port for Non-3GPP Access.

- Bit 3 – MAC: If this bit is set to "1", it indicates the PMF MAC Address for 3GPP Access, PMF MAC Address for Non-3GPP Access filed shall be presend in the PMF Address Information IE.

- Bit 4 to 8 Spare, for future use and set to "0".

Octets "p to (p+3)" or "q to (q+15)" (IPv4 address / IPv6 address fields), if present, shall contain the value for PMF IP Address.

Octets "r to (r+1)" shall carry the allocated UDP port number associated with the 3GPP access network, for IP PDU session.

Octets "s to (s+1)" shall carry the allocated UDP port number associated with the Non-3GPP access network, for IP PDU session.

Octets "t to (t+5)" shall carry the allocated PMF MAC address for 3GPP access, for Ethernet PDU session.

Octets "u to (u+5)" shall carry the allocated PMF MAC address for Non-3GPP access, for Ethernet PDU session.

## 8.2.160 ATSSS-LL Information

The ATSSS-LL Information IE shall contain ATSSS-LL information. It shall be encoded as shown in Figure 8.2.160-1.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 231 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | LLI |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.160-1: ATSSS-LL Information**

The following flags are coded within Octet 5:

- Bit 1 – LLI: If this bit is set to "1", it indicates that resources for the ATSSS-LL steering functionality have been allocated.

- Bit 2 to 8 Spare, for future use and set to "0".

## 8.2.161 Data Network Access Identifier

The Data Network Access Identifier IE type shall be encoded as shown in Figure 8.2.161-1. It contains an identifier of a Data Network Access.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 232 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Data Network Access Identfier | | | | | | | |

**Figure 8.2.161-1: Data Network Access Identifier**

The Data Network Access Identifier field shall be encoded as an OctetString.

## 8.2.162 Average Packet Delay

The Average Packet Delay IE indicates the average packet delay experienced by user plane packets on a GTP-U path. It shall be coded as depicted in Figure 8.2.162-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 234 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Delay Value in milliseconds | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.162-1: Average Packet Delay**

The Delay Value shall be encoded as an Unsigned 32 binary integer value, in milliseconds.

## 8.2.163 Minimum Packet Delay

The Minimum Packet Delay IE indicates the minimum packet delay experienced by user plane packets on a GTP-U path. It shall be coded as depicted in Figure 8.2.163-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 235 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Delay Value in milliseconds | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.163-1: Minimum Packet Delay**

The Delay Value shall be encoded as an Unsigned 32 binary integer value, in milliseconds.

## 8.2.164 Maximum Packet Delay

The Maximum Packet Delay IE indicates the maximum packet delay experienced by user plane packets on a GTP-U path. It shall be coded as depicted in Figure 8.2.164-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 236 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Delay Value in milliseconds | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.164-1: Maximum Packet Delay**

The Delay Value shall be encoded as an Unsigned 32 binary integer value, in milliseconds.

## 8.2.165 QoS Report Trigger

The QoS Report Trigger IE shall be encoded as shown in Figure 8.2.165-1. It indicates the trigger of the QoS report.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 237 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | IRE | THR | PER |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.165-1: QoS Report Trigger**

Octet 5 shall be encoded as follows:

- Bit 1 – PER (Periodic Reporting): when set to "1", this indicates a periodic report.
- Bit 2 –THR (Event triggered based on Threshold): when set to "1", this indicates a report caused by QoS exceeding a threshold.
- Bit 3 – IRE (Immediate Report): when set to "1", this indicates an immediate report requested by CP function.
- Bit 4 to 8: Spare, for future use and set to "0".

## 8.2.166 GTP-U Path Interface Type

The GTP-U Path Interface Type IE shall be encoded as shown in Figure 8.2.166-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 241 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | N3 | N9 |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.166-1: GTP-U Path Interface Type**

Octet 5 shall be encoded as follows:

- Bit 1 – N9: when set to "1", this indicates the N9 interface type.
- Bit 2 –N3: when set to "1", this indicates the N3 interface type.
- Bit 3 to 8: Spare, for future use and set to "0".

## 8.2.167 Requested Qos Monitoring

The Requested Qos Monitoring IE shall be encoded as shown in Figure 8.2.167-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 243 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | GTPU PM | RP | UL | DL |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.167-1: Requested Qos Monitoring**

Octet 5 shall be encoded as follows:

- Bit 1 – DL (Downlink): when set to "1", this indicates a request for measuring the downlink packet delay from the UPF (PSA) to the UE.
- Bit 2 – UL (Uplink): when set to "1", this indicates a request for measuring the uplink packet delay from the UE to the UPF (PSA).
- Bit 3 – RP (Round Trip): when set to "1", this indicates a request for measuring the round trip packet delay between the UPF (PSA) and UE.
- Bit 4 – GTPUPM (GTP-U Path Monitoring):
  - when set to "1, this indicates that the Downlink, Uplink or Round Trip delay shall be measured by using GTP-U path monitoring, i.e. by the I-UPF reporting the one-way end to end accumulated transport delay in UL GTP-U packets towards the PSA; see clause 5.33.3.3 of 3GPP TS 23.501 [28];

- when set to "0", this indicates that the Downlink, Uplink or Round Trip delay shall be measured by using RAN and UPF time information in GTP-U packets; see clause 5.33.3.2 of 3GPP TS 23.501 [28].

- Bit 5 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".

## 8.2.168 Reporting Frequency

The Reporting Frequency IE shall be encoded as shown in Figure 8.2.168-1. It indicates the frequency for the UP function to send a QoS Monitoring report to the CP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 244 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | SESRL | PERIO | EVETT |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.19-1: Reporting Frequency**

Octet 5 shall be encoded as follows:

- Bit 1 – EVETT (Event Triggered QoS monitoring reporting): when set to "1", this indicates the delay for QoS monitoring is reported when the delay exceeds a threshold.

- Bit 2 – PERIO (Periodic QoS monitoring reporting): when set to "1", this indicates the delay for QoS monitoring is reported periodicly.

- Bit 3 – SESRL (Session Released QoS monitoring reporting): when set to "1", this indicates the delay for QoS monitoring is reported when the PDU session is released.

- 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".

## 8.2.169 Packet Delay Thresholds

The Packet Delay Thresholds IE contains a packet delay thresholds in milliseconds to be monitored by the UP function. It shall be encoded as shown in Figure 8.2.169-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 245 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | RP | UL | DL |
| m to (m+3) | Downlink packet delay threshold | | | | | | | |
| p to (p+3) | Uplink packet delay threshold | | | | | | | |
| q to (q+3) | Round trip packet delay threshold | | | | | | | |
| s to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.169-1: Packet Delay Thresholds**

The following flags are coded within Octet 5:

- Bit 1 – DL: If this bit is set to "1", then the Downlink packet delay threshold field shall be present, otherwise the Downlink packet delay threshold field shall not be present.

- Bit 2 – UL: If this bit is set to "1", then the Uplink packet delay threshold field shall be present, otherwise the Uplink packet delay threshold field shall not be present.

- Bit 3 – RP: If this bit is set to "1", then the Round trip packet delay threshold field shall be present, otherwise the Round trip packet delay threshold 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 Downlink packet delay threshold, Uplink packet delay threshold and Round trip packet delay threshold fields shall be encoded as an Unsigned32 binary integer value. They shall contain the downlink, uplink or round trip packet delay in milliseconds respectively.

## 8.2.170 Minimum Wait Time

The Minimum Wait Time IE contains the minimum waiting time between two consecutive reports for event triggered QoS monitoring reporting. It shall be encoded as shown in Figure 8.2.170-1.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 246 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | Minimum Wait Time | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.170-1: Minimum Wait Time**

The Minimum Wait Time field shall be encoded as an Unsigned32 binary integer value. It shall contain the duration in seconds.

## 8.2.171 QoS Monitoring Measurement

The QoS Monitoring Measurement IE contains the packet delay monitored by the UP function. It shall be encoded as shown in Figure 8.2.171-1.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 248 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | PLMF | RP | UL | DL |
| m to (m+3) | Downlink packet delay | | | | | | | |
| p to (p+3) | Uplink packet delay | | | | | | | |
| q to (q+3) | Round trip packet delay | | | | | | | |
| s to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.171-1: QoS Monitoring Measurement**

The following flags are coded within Octet 5:

- Bit 1 – DL (Downlink): If this bit is set to "1", then the Downlink packet delay field shall be present, otherwise the Downlink packet delay field shall not be present.

- Bit 2 – UL (Uplink): If this bit is set to "1", then the Uplink packet delay field shall be present, otherwise the Uplink packet delay field shall not be present.

- Bit 3 – RP (Round Trip): If this bit is set to "1", then the Round trip packet delay field shall be present, otherwise the Round trip packet delay field shall not be present.

- Bit 4 – PLMF (Packet Delay Measurement Failure): If this bit is set to "1", this indicates no timestamp is received in uplink packet for a delay exceeding the Packet Delay Thresholds or the Measurement Period.

- Bit 5 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 Downlink packet delay, Uplink packet delay and Round trip packet delay fields shall be encoded as an Unsigned32 binary integer value. They shall contain the downlink, uplink or round trip packet delay in milliseconds respectively.

## 8.2.172 MT-EDT Control Information

MT-EDT Control Information is coded as depicted in Figure 8.2.172-1.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 249 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | RDSI |
| k to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.172-1: MT-EDT Control Information**

The following flags are coded within Octet 5:

- Bit 1 – RDSI (Reporting DL data packets Size Indication): This bit shall be set to "1" if the UP function is requested to report the sum of DL data packets size.

- Bit 2 to 8 are spare and reserved for future use.

## 8.2.173 DL Data Packets Size

The DL Data Packets Size IE type shall be encoded as shown in Figure 8.2.173-1. It contains the sum of DL data packets size in byte which triggers to send Downlink Data Report.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 250 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 6 | DL Data Packets Size | | | | | | | |
| 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.173-1: DL Data Packets Size**

The DL Data Packets Size shall be encoded as an Unsigned16 binary integer value.

## 8.2.174 QER Control Indications

The QER Control Indications IE indicates flags applicable to a QER. It is coded as depicted in Figure 8.2.174-1.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 251 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | Spare | Spare | RCSR |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.174-1: QER Control Indications**

The following bits within Octet 5 shall indicate:

- Bit 1 – RCSR (Rate Control Status Reporting): If this bit is set to "1", then the UP function shall report the rate control status when the PFCP session is released. If this bit is set to "0", then the UPF shall not report the rate control status (see clause 5.4.15).

- Bit 2 to 8 – Spare, for future use, shall be set to "0" by the sender and discarded by the receiver.

## 8.2.175 NF Instance ID

The NF Instance ID IE type shall be encoded as shown in Figure 8.2.175-1. It contains the NF Instance ID of a UPF.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 253 (decimal) | | | | | | | |
| 3 to 4 | Length = 16 | | | | | | | |
| 5 to 20 | NF Instance ID | | | | | | | |

**Figure 8.2.175-1: NF Instance ID**

The NF Instance ID field shall be encoded as specified in 3GPP TS 29.571 [61].

## 8.2.176 S-NSSAI

The S-NSSAI IE indicates the S-NSSAI of a PDU session. It shall be encoded as shown in Figure 8.2.176-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 257 (decimal) | | | | | | | |
| 3 to 4 | Length = 4 | | | | | | | |
| 5 | SST | | | | | | | |
| 6 to 8 | SD | | | | | | | |

**Figure 8.2.176-1: S-NSSAI**

The SST (Slice/Service Type) and SD (Slice Differentiator) fields shall be encoded as defined in clause 28.4.2 of 3GPP TS 23.003 [2].

## 8.2.177 IP version

IP version shall be encoded as shown in Figure 8.2.177-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 258 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | V6 | V4 |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.177-1: IP version**

The following flags are coded within Octet 5:

- Bit 1 – V4: when set to "1", this indicate the IP version is V4;
- Bit 2 – V6: when set to "1", this indicate the IP version is V6;
- Bit 3 to 8: Spare, for future use and set to "0".

At least one of V4 and V6 shall be set to "1", and both may be set to "1".

## 8.2.178 PFCPASReq-Flags

The PFCPASReq-Flags IE indicates flags applicable to the PFCP Association Setup Request message. It is coded as depicted in Figure 8.2.178-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 259 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | UUPSI |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.178: PFCPASReq-Flags**

The following bits within Octet 5 shall indicate:

- Bit 1 – UUPSI (UPF configured for IPUPS Indication): if this bit is set to "1", it indicates that the UPF is configured to be used for IPUPS. See clause 5.27.
- Bit 2 to 8 – Spare, for future use, shall be set to "0" by the sender and discarded by the receiver.

## 8.2.179 Data Status

The Data Status IE indicates the status of the data packets in the UP function. It is coded as shown in Figure 8.2.179-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 260 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | BUFF | DROP |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.179-1: Data Status**

The following flags are coded within Octet 5:

- Bit 1 – DROP: when set to "1", this indicates first DL packet is discarded by the UP function.
- Bit 2 – BUFF: when set to "1", this indicates first DL packet is received and buffered by the UP function.
- Bit 3 to 8 Spare, for future use and set to "0".

## 8.2.180 RDS Configuration Information

The RDS Configuration Information IE shall provide details of the RDS Configuration Information. It shall be encoded as shown in Figure 8.2.180-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 262 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | RDS |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.180-1: RDS Configuration Information**

The following flags are coded within Octet 5:

- Bit 1 – RDS (Reliable Data Service): If this bit is set to "1", it indicates that the RDS is requested to be applied (in request) / applied (in response).
- Bit 2 to 8 Spare, for future use and set to "0".

## 8.2.181 MPTCP Applicable Indication

MPTCP Applicable Indication shall be coded as depicted in Figure 8.2.181-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 265 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | MAI |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.181-1: MPTCP Applicable Indication**

The following flags are coded within Octet 5:

- Bit 1 – MAI (MPTCP Applicable Indication): When this bit is set to "1", it indicates that the PDR is used to detect user plane traffic for which MPTCP is applicable (see clause 5.20.2.4).

- Bit 2 to 8 are spare and reserved for future use.

## 8.2.182 User Plane Node Management Information Container

The User Plane Node Management Information Container IE shall be encoded as shown in Figure 8.2.182-1. It contains an opaque container of User Plane Nodemanagement information.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 266 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | User Plane Node Management Information | | | | | | | |

**Figure 8.2.182 -1: User Plane NodeManagement Information Container**

The User Plane Node Management Information field shall be encoded as an Octet String. It shall encode a Bridge management message defined in clause 9 of 3GPP TS 24.539 [63].

## 8.2.183 Number of UE IP Addresses

Number of UE IP Addresses IE shall be coded as depicted in Figure 8.2.183-1. It contains an Unsigned32 binary integer value in octets "a to (a+3)" and "b to (b+3)".

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 268 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | Spare | IPv6 | IPv4 |
| a to (a+3) | Number of UE IPv4 Addresses | | | | | | | |
| b to (b+3) | Number of UE IPv6 Addresses | | | | | | | |
| k to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.183-1: Number of UE IP Addresses**

The following flags are coded within Octet 5:

- Bit 1 – IPv4: If this bit is set to "1", Number of UE IPv4 Addresses field shall be present. Otherwise the Number of UE IPv4 Addresses field shall not be present.

- Bit 2 – IPv6: If this bit is set to "1", Number of UE IPv6 Addresses field shall be present. Otherwise the Number of UE IPv6 Addresses field shall not be present.

Octets "a to (a+3)" and/or "b to (b+3)" shall be present if Bis 1 and/or Bit 2 in octet 5 is present. Otherwise, these octets shall not be present.

## 8.2.184 Validity Timer

Validity Timer IE shall be coded as depicted in Figure 8.2.184-1. It shall contain two octets long Unsigned16 binary integer value representing a time interval in seconds.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 269 (decimal) |
| 3 to 4 | Length = n |
| 5 to 6 | Validity Timer |
| k to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.184-1: Validity Timer**

## 8.2.185 Offending IE Information

Offending IE Information shall be coded as depicted in Figure 8.2.185-1.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 274 (decimal) |
| 3 to 4 | Length = n |
| 5 to 6 | Type of the offending IE |
| 7 to (n+4) | Value of the offending IE |

**Figure 8.2.185-1: Offending IE Information**

The Type of the offending IE field in octets 5 to 6 shall contain the IE type (as defined in clause 8.2.1) that caused the failure.

The Value of the offending IE field in octets 7 to (n+4) shall contain the value of the offending IE that caused the failure.

## 8.2.186 RAT Type

The RAT Type IE indicates the RAT type for the PFCP Session. The RAT Type IE type shall be encoded as shown in Figure 8.2.186-1.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 275 |
| 3 to 4 | Length = n |
| 5 | RAT Type |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.186-1: RAT Type IE**

RAT Type indicates the type of RAT for the PFCP Session. It shall be encoded as defined in Table 8.2.186-1.

**Table 8.2.186-1: RAT Type values**

| RAT Type | Values (Decimal) |
|---|---|
| <reserved> | 0 |
| UTRAN | 1 |
| GERAN | 2 |
| WLAN | 3 |
| GAN | 4 |
| HSPA Evolution | 5 |
| EUTRAN (WB-E-UTRAN) | 6 |
| Virtual | 7 |
| EUTRAN-NB-IoT | 8 |
| LTE-M | 9 |
| NR | 10 |
| Spare, for future use | 11-255 |

## 8.2.187 L2TP User Authentication

The L2TP User Authentication IE shall be encoded as shown in Figure 8.2.187-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 278 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 - 6 | Proxy Authen Type Value | | | | | | | |
| 7 | Spare | | | | PAI | PAR | PAC | PAN |
| 8 | Length of Proxy Authen Name | | | | | | | |
| 9 to a | Proxy Authen Name Value | | | | | | | |
| a+1 | Length of Proxy Authen Challenge | | | | | | | |
| (a+2) to b | Proxy Authen Challenge Value | | | | | | | |
| b+1 | Length of Proxy Authen Response | | | | | | | |
| (b+2) to c | Proxy Authen Response Value | | | | | | | |
| c+1 | Proxy Authen ID | | | | | | | |
| (c+2) to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.187-1: L2TP User Authentication**

The following flags are coded within Octet 7:

- Bit 1 – PAN: If this bit is set to "1", then the Length of Proxy Authen Name and Proxy Authen Name Value shall be present; otherwise, the Length of Proxy Authen Name and Proxy Authen Name Value shall not be present.
- Bit 2 – PAC: If this bit is set to "1", then the Length of Proxy Authen Challenge and Proxy Authen Challenge Value shall be present; otherwise, the Length of Proxy Authen Challenge and Proxy Authen Challenge Value shall not be present.
- Bit 3 – PAR: If this bit is set to "1", then the Length of Proxy Authen Response and Proxy Authen Response Value shall be present; otherwise, the Length of Proxy Authen Response and Proxy Authen Response Value shall not be present.
- Bit 4 – PAI: If this bit is set to "1", then the Proxy Authen ID shall be present; otherwise, the Proxy Authen ID shall not be present.

Proxy Authen Type Value, Proxy Authen Name Value, Proxy Authen Challenge Value, Proxy Authen Response Value and Proxy Authen ID shall be encoded as the Attribute Value field for the Proxy Authen Type AVP, Proxy Authen Name AVP, Proxy Authen Challenge AVP, Proxy Authen Response AVP and Proxy Authen ID respectively as specified in IETF RFC 2661 [67].

If Proxy Authen Type Value is 1, then the PAN and PAR flags shall be set.

If Proxy Authen Type Value is 2, then the PAN, PAC, PAR, and PAI flags shall be set.

If Proxy Authen Type Value is 3, then the PAN, PAR, and PAI flags shall be set.

If Proxy Authen Type Value is 5, then the PAN, PAC, PAR, and PAI flags shall be set.

## 8.2.188 LNS Address

The LNS Address IE shall contain an IPv4/IPv6 address. It shall be encoded as shown in Figure 8.2.188-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 280 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to o | LNS Address value | | | | | | | |
| m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.188-1: LNS Address**

If the LNS Address is an IPv4 address, the LNS Address value length shall be "4".

If the LNS Address is an IPv6 address, the LNS Address value length shall be "16".

## 8.2.189 Tunnel Preference

The Tunnel Preference IE type shall be encoded as shown in Figure 8.2.189-1. It contains a Tunnel Preference value which indicates the preference to be given to the L2TP tunnel to which it refers; higher preference is given to lower values, with 0x000000 being most preferred and 0xFFFFFF least preferred (see 3GPP TS 29.061 [39]).

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 281 (decimal) | | | | | | | |
| 3 to 4 | Length = 3 | | | | | | | |
| 5 to 7 | Tunnel Preference value | | | | | | | |

**Figure 8.2.189-1: Tunnel Preference**

The Tunnel Preference value shall be encoded as three octets binary integer value.

## 8.2.190 Calling Number

The Calling Number IE type shall be encoded as shown in Figure 8.2.190-1. It contains a Calling Number value which may contain a MSISDN (see 3GPP TS 29.061 [39]).

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 282 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Calling Number value | | | | | | | |

**Figure 8.2.190-1: Calling Number**

The Calling Number value shall be encoded in UTF8String format.

## 8.2.191 Called Number

The Called Number IE type shall be encoded as shown in Figure 8.2.191-1. It contains a Called Number value which may contain a DNN/APN. (see 3GPP TS 29.061 [39]).

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 283 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Called Number value | | | | | | | |

**Figure 8.2.191-1: Called Number**

The Called Number value shall be encoded in UTF8String format.

## 8.2.192 L2TP Session Indications

The L2TP Session Indications IE shall be encoded as shown in Figure 8.2.192-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 284 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | RENSA | REDSA | REUIA |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.192-1: L2TP Session Indications**

The following bits within Octet 5 shall indicate:

- Bit 1 – REUIA (Request UE IP Address): if this bit is set to "1", it indicates to the UP function that the UP function shall request the UE IP address from the LNS.
- Bit 2 – REDSA (Request DNS Server Address): if this bit is set to "1", it indicates to the UP function that the UP function shall request DNS Server Address from the LNS.
- Bit 3 – RENSA (Request NBNS Server Address): if this bit is set to "1", it indicates to the UP function that the UP function shall request NBNS Server Address from the LNS.
- Bit 4 to 8 – Spare, for future use, shall be set to "0" by the sender and discarded by the receiver.

NOTE: REDSA and RENSA are only applicable for PDN connections/PDU sessions with IPv4 address.

## 8.2.193 DNS Server Address

The DNS Server Address IE shall contain an IPv4 address. It shall be encoded as shown in Figure 8.2.193-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 285 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | DNS Server Address value | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.193-1: DNS Server Address**

## 8.2.194 NBNS Server Address

The NBNS Server Address IE shall contain an IPv4 address. It shall be encoded as shown in Figure 8.2.194-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 286 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 8 | NBNS Server Address value | | | | | | | |
| 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.194-1: NBNS Server Address**

## 8.2.195 Maximum Receive Unit

The Maximum Receive Unit shall be encoded as shown in Figure 8.2.195-1. The Maximum Receive Unit value shall contain the link MTU size value received from the UE via the Protocol Configuration Options (see 3GPP TS 24.008 [5]).

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 287 (decimal) | | | | | | | |
| 3 to 4 | Length = 2 | | | | | | | |
| 5 to 6 | Maximum Receive Unit value | | | | | | | |

**Figure 8.2.195-1: Maximum Receive Unit**

The Maximum Receive Unit value shall be encoded as two octet's binary integer value.

## 8.2.196 Thresholds

The Thresholds IE shall be encoded as shown in Figure 8.2.196-1. It indicates the RTT and/or a Packet Loss Rate.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 288 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | PLR | RTT |
| m to (m+1) | RTT value | | | | | | | |
| p | Packet Loss Rate value | | | | | | | |
| q to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.196.-1: Thresholds**

The following flags are coded within Octet 5:

- Bit 1 – RTT: If this bit is set to "1", then the RTT value field shall be present, otherwise the RTT value shall not be present.
- Bit 2 – PLR: If this bit is set to "1", then the Packet Loss Rate value field shall be present, otherwise the Packet Loss Rate value shall not be present.
- Bit 3 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 RTT value field shall be encoded as an Unsigned16 binary integer value. It shall contain the RTT in milliseconds.

The Packet Loss Rate value field shall indicate 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.

## 8.2.197 Steering Mode Indicator

The Steering Mode Indicator IE shall be encoded as shown in Figure 8.2.197-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 289 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | UEAI | ALBI |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.197.-1: Steering Mode Indicator**

The following flags are coded within Octet 5:

- Bit 1 –ALBI (Autonomous Load Balancing Indicator): If this bit is set to "1", the autonomous load-balance is allowed.
- Bit 2 –UEAI (UE Assistance Indicator): If this bit is set to "1", the UE-assistance operation is allowed.
- Bit 3 to 8 Spare, for future use and set to "0".

The ALBI and UEAI shall not be set to "1" at the same time.

## 8.2.198 Group Id

The Group Id IE type shall be encoded as shown in Figure 8.2.198-1. It shall contain an octet string as a global unique identifier for a group and it may be encoded using the same mechanism for the NfInstanceId as specified in 3GPP TS 29.571 [61].

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 291 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to n+4 | Group Id | | | | | | | |

**Figure 8.2.198-1: Group Id**

## 8.2.199 CP IP Address

The CP IP Address IE shall contain an IPv4 and/or IPv6 address. It shall be encoded as shown in Figure 8.2.199-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 292 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | V4 | V6 |
| p to (p+3) | IPv4 Address | | | | | | | |
| q to (q+15) | IPv6 Address | | | | | | | |

**Figure 8.2.199-1: CP 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 CP 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 CP IP Address, otherwise the IPv4 address field shall not be present.
- Bit 3 to 8 Spare, for future use and set to "0".

Octets "p to (p+3)" or "q to (q+15)" (IPv4 address / IPv6 address fields), if present, shall contain the address value.

## 8.2.200 IP Address and Port Number Replacement

The IP Address and Port Number Replacement IE type shall be encoded as shown in Figure 8.2.200-1. It contains instructions to modify the contents of the (inner) packet.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 293 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 6 | Spare | | SPN | SIPV6 | SIPV4 | DPN | DIPV6 | DIPV4 |
| p to (p+3) | Destination IPv4 Address | | | | | | | |
| q to (q+15) | Destination IPv6 Address | | | | | | | |
| r to (r+1) | Destination Port Number | | | | | | | |
| s to (s+3) | Source IPv4 Address | | | | | | | |
| t to (t+15) | Source IPv6 Address | | | | | | | |
| u to (u+1) | Source Port Number | | | | | | | |
| v to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.200-1: IP Address and Port Number Replacement**

The following flags are coded within Octet 5:

- Bit 1 – DIPV4: If this bit is set to "1", then the Destination IPv4 field shall be present, otherwise the Destination IPv4 field shall not be present.
- Bit 2 – DIPV6: If this bit is set to "1", then the Destination IPv6 field shall be present, otherwise the Destination IPv6 field shall not be present.
- Bit 3 – DPN: If this bit is set to "1", then the Destination Port Number field shall be present, otherwise the Destination Port Number field shall not be present.
- Bit 4 – SIPV4: If this bit is set to "1", then the Source IPv4 field shall be present, otherwise the Source IPv4 field shall not be present.
- Bit 5 – SIPV6: If this bit is set to "1", then the Source IPv6 field shall be present, otherwise the Source IPv6 field shall not be present.
- Bit 6 – SPN: If this bit is set to "1", then the Source Port Number field shall be present, otherwise the Source Port Number field shall not be present.
- Bit 7 to 8: Spare, for future use and set to "0".

When present, the Destination IPv4 Address field or the Source IPv4 Address field shall contain the destination or source IPv4 address respectively to set in the IPv4 header of the outgoing packet.

When present, the Destination IPv6 Address field or the Source IPv6 Address field shall contain the destination or source IPv6 address respectively to set in the IPv6 header of the outgoing packet.

When present, the Destination Port Number field or the Source Port Number field shall contain the destination or source Port Number respectively to set in the UDP header of the outgoing packet.

At least one IP address shall be present.

## 8.2.201 DNS Query Filter

The DNS Query Filter IE type shall be encoded as shown in Figure 8.2.201-1. It contains a DNS Query Filter.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 294 (decimal) |
| 3 to 4 | Length = n |
| 5 to 6 | Length of Domain Name Pattern |
| 7 to p | Domain Name Pattern |
| x to (n+4) | These octet(s) is/are present only if explicitly specified |

**Figure 8.2.201-1: DNS Query Filter**

The Domain Name Pattern field, in octets 7 to p, shall be encoded as Octetstring representing a JSON object defined as FqdnPatternMatchingRule data type specified in clause 5.2.4.23 of 3GPP TS 29.571 [61].

## 8.2.202 Event Notification URI

The Event Notification URI IE type shall be encoded as shown in Figure 8.2.202-1.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 296 (decimal) |
| 3 to 4 | Length = n |
| 5 to n+4 | Event Notification URI |

**Figure 8.2.202-1: Event Notification URI**

The Event Notification URI field in octets 5 to (n+4) shall contain an octet string representing the Event Notification URI (i.e. string providing an URI formatted according to IETF RFC 3986 [71]) to be used for sending the UPF event notifications.

## 8.2.203 Notification Correlation ID

The Notification Correlation ID IE type shall be encoded as shown in Figure 8.2.203-1.

| Octets | Bits 8 7 6 5 4 3 2 1 |
|---|---|
| 1 to 2 | Type = 297 (decimal) |
| 3 to 4 | Length = n |
| 5 to n+4 | Notification Correlation ID |

**Figure 8.2.203-1: Notification Correlation ID**

The Notification Correlation ID field in octets 5 to (n+4) shall contain an octet string representing the value of the Notification Correlation ID to be sent in UPF event notifications.

## 8.2.204 Reporting Flags

The Reporting Flags IE indicates flags providing additional information for direct event notification reporting. It is coded as depicted in Figure 8.2.204-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 298 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | Spare | Spare | DUPL |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.204-1: Reporting Flags**

The following bits within Octet 5 shall indicate:

- Bit 1 – DUPL (Duplicated notification): if this bit is set to "1", it indicates that the UP function shall also report the event notifications over N4 (in addition to reporting them directly to the Event Notification URI).

- Bit 2 to 8 – Spare, for future use, shall be set to"0" by the sender and discarded by the receiver.

## 8.2.205 Predefined Rules Name

The Predefined Rules Name IE type shall be coded as shown in Figure 8.2.205-1. It shall contain a Predefined Rules Name, referring to one or more predefined rules which are activated in the UP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 299 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Predefined Rules Name | | | | | | | |

**Figure 8.2.205-1: Predefined Rules Name**

The Predefined Rules Name field shall be encoded as an OctetString.

## 8.2.206 MBS Session Identifier

The MBS Session Identifier is used to identify a 5G MBS Session. It contains the Temporary Mobile Group Identity as defined in 3GPP TS 23.003 [2] or a Source Specific IP multicast address which consists of two IP addresses, one is an IP unicast address used as source address in IP packets for identifying the source of the multicast service (e.g. AF/AS), the other is an IP multicast address used as destination address in related IP packets for identifying a multicast service associated with the source.

It is coded as specified in Figure 8.2.206-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 305 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | NIDI | SSMI | TMGI |
| 6-11 | TMGI | | | | | | | |
| 12-m | Source Specific IP Multicast Address | | | | | | | |
| o to (o+5) | NID | | | | | | | |
| q-(n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.206-1: MBS Session Identifier**

The following bits within Octet 5 shall indicate:

- Bit 1 – TMGI: if this bit is set to "1", it indicates that the TMGI field shall be present, otherwise it shall not be present;

- Bit 2 – SSMI: if this bit is set to "1", it indicates that the Source Specific IP Multicast Address field shall be present, otherwise it shall not be present;

- Bit 3 – NIDI: if this bit is set to "1", it indicates that the Network Identifier (NID) field shall be present, otherwise it shall not be present;

- Bit 4 to 8 – Spare, for future use, shall be set to "0" by the sender and discarded by the receiver.

The TMGI field shall be encoded as octets 3 to octet 8 in the figure 10.5.154 of 3GPP TS 24.008 [5].

The Source Specific IP Multicast Address field shall be encoded the octets 10 to m of IE Multicast Transport Information as specified in 8.2.207.

The NID field shall be encoded with 11 hexadecimal digit, bit 8 to bit 5 of the octet "o" is the most significant digit and bit 8 to bit 5 of the octet "o+5" is the least significant digit, and bits 4 to 1 of octets (o+5) shall all be encoded as 0.

## 8.2.207 Multicast Transport Information

The Multicast Transport Information IE contains the Low Layer Source Specific IP Multicast Address allocated by the MB-UPF. It is coded as specified in Figure 8.2.207-1.

The IP Multicast Distribution Address and the IP Source Address fields contain the IPv4 or IPv6 address. The Address Type and Address Length fields shall be included in each field:

- The Address Type, which is a fixed length code (of 2 bits) identifying the type of address that is used in the Address field.

- The Address Length, which is a fixed length code (of 6 bits) identifying the length of the Address field.

- The Address, which is a variable length field shall contain either an IPv4 address or an IPv6 address.

Address Type 0 and Address Length 4 shall be used when Address is an IPv4 address.

Address Type 1 and Address Length 16 shall be used when Address is an IPv6 address.

Other combinations of values are not valid.

Common Tunnel Endpoint Identifier is allocated at the source Tunnel Endpoint and signalled to the destination Tunnel Endpoint. There is one Common Tunnel Endpoint Identifier allocated per MBS session.

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 306 (decimal) | | | | | | | |
| 3 to 4 | Length=n | | | | | | | |
| 5 | Spare | | | | | | | |
| 6 to 9 | Common Tunnel Endpoint Identifier | | | | | | | |
| 10 | Address Type | | Address Length | | | | | |
| 11 to K | IP Multicast Distribution Address (IPv4 or IPv6) | | | | | | | |
| K+1 | Address Type | | Address Length | | | | | |
| (k+2) to m | IP Source Address (IPv4 or IPv6) | | | | | | | |
| (m+1) to n | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.207-1: Multicast Transport Information**

## 8.2.208 MBSN4mbReq-Flags

The MBSN4mbReq-Flags IE indicates flags applicable to the PFCP Session Establishment Request. It is coded as depicted in Figure 8.2.208-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 307 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | MBS RESTI | JMBS SM | PLLS SM |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.208-1: MBSN4mbReq-Flags**

The following bits within Octet 5 shall indicate:

- Bit 1 – PLLSSM (Provide Lower Layer SSM): if this bit is set to "1", it indicates that the MB-UPF shall allocate a lower layer SSM (i.e. multicast destination address and related source IP address) and a GTP-U Common Tunnel EndPoint Identifier (C-TEID) in the Multicast Transport Address IE. See clause 5.34.2.2.

- Bit 2 – JMBSSM (Join MBS Session SSM): if this bit is set to "1", it indicates that the MB-UPF shall join the multicast tree towards the Source Specific Multicast (SSM) address information provided by AF/AS or MBSTF for the MBS Session.

- Bit 3 – MBS RESTI (MBS Restoration Indication): if this bit is set to "1", it indicates to the MB-UPF that the PFCP session to be established is to restore an existing PFCP session of an MBS session.

- Bit 4 to 8 – Spare, for future use, shall be set to "0" by the sender and discarded by the receiver.

## 8.2.209 Local Ingress Tunnel

The Local Ingress Tunnel IE type shall be encoded as shown in Figure 8.2.209-1. It indicates a UDP/IP tunnel.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 308 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | CH | V6 | V4 |
| 6-7 | UDP Port | | | | | | | |
| 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 8.2.209-1: Local Ingress Tunnel**

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 UDP Port, IPv4 address and IPv6 address fields shall not be present and the UP function shall assign a UDP Port 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 to 8: Spare, for future use and set to "0".

Only one of the V4 and V6 flags shall be set to "1".

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.

## 8.2.210 MBS Unicast Parameters ID

The MBS Unicast Parameters ID IE type shall be encoded as shown in Figure 8.2.210-1. It shall contain a MBS Unicast Parameters ID.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 309 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 6 | MBS Unicast Parameters ID value | | | | | | | |
| 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.210-1: MBS Unicast Parameters ID**

The MBS Unicast Parameters ID value field shall be encoded as an Unsigned16 binary integer value.

## 8.2.211 MBSN4Resp-Flags

The MBSN4Resp-Flags IE indicates flags applicable to the PFCP Session Establishment/Modification/Deletion Response message for a PFCP session that is associated with an MBS Session. It is coded as depicted in Figure 8.2.211-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 312 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | N19DTR | JMTI | NN19DT |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.211-1: MBSN4Resp-Flags**

The following bits within Octet 5 shall indicate:

- Bit 1 – NN19DT (New N19mb Downlink Tunnel): if this bit is set to "1", it indicates that the UPF has allocated a new N19mb DL Tunnel ID for the MBS Session;
- Bit 2 – JMTI (Joined N19mb Multicast Tree Indication): if this bit is set to "1", it indicates that the UPF has joined the multicast tree from MB-UPF;
- Bit 3 – N19DTR (N19mb Downlink Tunnel Removal): if this bit is set to "1", it indicates that the UPF is going to remove the N19mb DL Tunnel for receiving the MBS session data, because the PFCP session removing the PDR is the last PFCP session which was associated with the N19mb DL Tunnel in the UPF;
- Bit 4 to 8 – Spare, for future use, shall be set to "0" by the sender and discarded by the receiver.

NOTE: See clause 5.34.3.2 for further description of the setting and use of the bits in the MBSN4Resp-Flags.

## 8.2.212 Tunnel Password

The Tunnel Password IE type shall be encoded as shown in Figure 8.2.212-1. It contains the value of Tunnel Password (in plain text) to be used for the L2TP tunnel.

NOTE: The CP function obtains the plain text value of Tunnel Password after decoding and de-encrypting the Tunnel-Password AVP, which is received from AAA/Radius Server, as specified in clause 3.5 of IETF RFC 2868 [68].

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 313 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to (n+4) | Tunnel Password value | | | | | | | |

**Figure 8.2.212-1: Tunnel Password**

The Tunnel Password value shall be encoded in UTF8String format.

## 8.2.213 Area Session ID

The Area Session ID together with the MBS Session Identifier uniquely identifies the service area part of the content data of a location dependent MBS service (see clause 30.3 of 3GPP TS 23.003 [2]). It shall be coded as specified in Figure 8.2.213-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 314 (decimal) | | | | | | | |
| 3 to 4 | Length = 2 | | | | | | | |
| 5 to 6 | Area Session ID value | | | | | | | |

**Figure 8.2.213-1: Area Session ID**

The Area Session ID value shall be encoded as an Unsigned16 binary integer value.

## 8.2.214 DSCP to PPI Mapping Information

The DSCP to PPI Mapping Information IE shall be encoded as shown in Figure 8.2.214-1. It contains the mapping from DSCP(s) to a PPI.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 317 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | PPI Value | | |
| 6 | Spare | DSCP Value 1 | | | | | | |
| 7 | Spare | DSCP Value 2 | | | | | | |
| ... | Spare | ... | | | | | | |
| (5+x) | Spare | DSCP Value x | | | | | | |
| (6+x) to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.214-1: DSCP to PPI Mapping Information**

The PPI Value in octet 5 shall be encoded as a value between 0 and 7, as specified in clause 5.5.3.7 of 3GPP TS 38.415 [34].

The DSCP Value 1 to x, in octet 6 to octet (5+x), where X shall not be larger than 63, shall be encoded as the DSCP in TOS (IPv4) or TC (IPv6) information (see IETF RFC 2474 [13]).

## 8.2.215 PFCPSDRsp-Flags

The PFCPSDRsp-Flags IE indicates flags applicable to the PFCP Session Report Response message. It is coded as depicted in Figure8.2.215-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 318 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | Spare | Spare | PURU |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.215-1: PFCPSDRsp-Flags**

The following bits within Octet 5 shall indicate:

- Bit 1 – PURU (Pending Usage Reports Unacknowledged): if this bit is set to "1", it indicates that there are pending PFCP Session Report Request messages which have not been acknowledged yet.
- Bit 2 to 8 – Spare, for future use, shall be set to "0" by the sender and discarded by the receiver.

## 8.2.216 QER Indications

The QER Indications IE indicates flags applicable to a QER. It shall be coded as depicted in Figure 8.2.216-1.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 319 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | Spare | Spare | Spare | Spare | Spare | Spare | IQFISN |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.216-1: QER Indications**

The following bits within Octet 5 shall indicate:

- Bit 1 – IQFISN (Insert DL MBS QFI SN): If this bit is set to "1", then the MB-UPF shall insert the DL MBS QFI Sequence Number in the PDU Session Container of MBS data packets (see 3GPP TS 38.415 [34]).
- Bit 2 to 8 – Spare, for future use, shall be set to "0" by the sender and discarded by the receiver.

## 8.2.217 Vendor-Specific Node Report Type

The Vendor-Specific Node Report Type IE shall be encoded as shown in Figure 8.2.217-1. It indicates the type of the Vendor-Specific node report the UP function sends to the CP function.

| Octets | Bits 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 1 to 2 | Type = 320 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 to 6 | Enterprise ID | | | | | | | |
| 7 | Spare | Spare | Spare | Spare | Spare | Spare | Spare | Spare |
| 8 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.217-1: Vendor-Specific Node Report Type**

Octet 7 (and following octets if needed) shall be encoded as a bitmask, where each bit in the bitmask shall indicate a Vendor-Specific Node Report Type. The definition and semantic of the bits in the bitmask are out of scope of 3GPP.

Enterprise ID in octets 5 to 6 shall be encoded as defined in clause 8.1.1. The Enterprise ID may identify a Standards Development Organization. The report types indicated by octet 7 (and following octets if needed) are specific to the Standards Development Organization or enterprise identified by the Enterprise ID.

Spare bits are for future use and shall be set to "0".

At least one bit shall be set to "1".

NOTE: The Vendor-Specific Node Report Type IE in the PFCP Node Report Request message can be used by non-3GPP Standards Development Organizations for interfaces relying on PFCP as the protocol for Control and User Plane Separation, for identifying the type of vendor-specific node reports not defined by 3GPP. The definition and semantic of the bits within the bitmask are to be specified by each non-3GPP Standards Development Organization (without liaising with 3GPP CT4). See clauses 5.9 and 8.1.1 for the definition and usage of Vendor Specific IEs.

## 8.2.218 Configured Time Domain

The Configured Time Domain IE type shall be encoded as shown in Figure 8.2.218-1. It shall contain

| | Bits | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Octets** | **8** | **7** | **6** | **5** | **4** | **3** | **2** | **1** |
| 1 to 2 | Type = 321 (decimal) | | | | | | | |
| 3 to 4 | Length = n | | | | | | | |
| 5 | Spare | | | | | | | CTDI |
| 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | |

**Figure 8.2.218-1: Configured Time Domain**

Octet 5 shall be encoded as follows:

- Bit 1 (CTDI – Configured Time Domain Indicator): when set to "1", this indicates that the Time Domain Number configured to the NW-TT(s) is used.

- Bits 2 to 8: Spare, for future use and set to "0".

# 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 clause 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 clause 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 clause 6.2.3 for how the CP function obtains load control information from the UP function.
4. For Dedicated Core Networks (see clause 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.
5. The MME/SGSN shall be able to select an SGW-C and a PGW-C optimized for NR, e.g. for UEs indicating support of dual connectivity with NR in NAS signalling to the MME or SGSN and without subscription restriction to use NR as secondary RAT, according to the requirements specified in clause 5.12.2 of 3GPP TS 29.303 [25]. The SGW-C and the PGW-C optimized for NR may be a combined SGW-C/PGW-C function optimized for the NR.

## 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. Clause 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);
- the UP Function Selection Information Flags, indicating whether it is desired to select an SGW-U optimized for NR, as specified in 3GPP TS 29.274 [9].

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 PFCP 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);
- the UP Function Selection Information Flags, indicating whether it is desired to select a PGW-U optimized for NR, as specified in 3GPP TS 29.274 [9].

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 clause 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 an 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 PFCP Association Setup.

## B.2.4 Combined SGW-U/PGW-U Selection Function

A Combined SGW-C/PGW-C function shall be able to select a combined SGW-U/PGW-U function. This shall be possible for all the UE's PDN connections, as shown in Figure B.2.1-1.

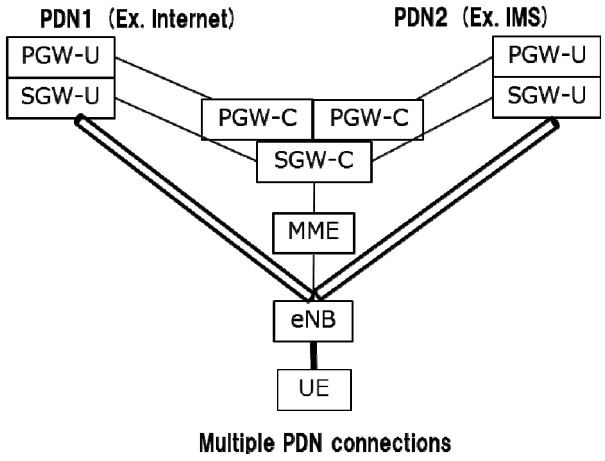



**Figure B.2.4 -1: SGW-U/PGW-U colocation with Control and User Plane Separation**

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 (e.g. the combined SGW-U/PGW-U function), 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 clause 5.12.5 of 3GPP TS 23.214 [2].

## B.2.6 UP Selection Function Based on DNS

### B.2.6.1 General

This clause 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.

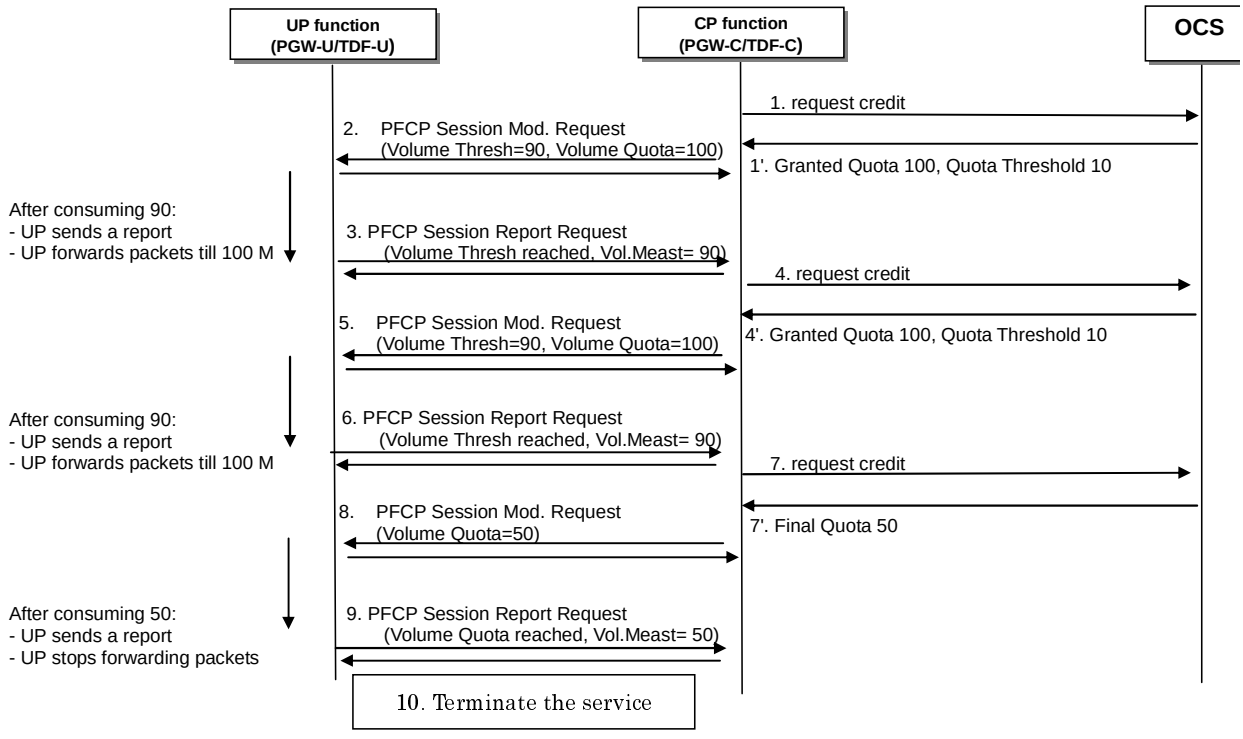



**Figure C.2.1.1-1: Online charging with intermediate and final quotas**

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 a PFCP 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 a PFCP 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 a PFCP 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 a PFCP 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 a PFCP 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 a PFCP 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.

Figure C.2.1.1-2 illustrates the exchanges taking place over the Sxb or Sxc reference points when applying online charging and the UP function supports being provisioned with the Quota Action to apply when reaching quotas. This example is similar to the previous one, but the CP function provisions the UP function with the action to apply when reaching the final quota.

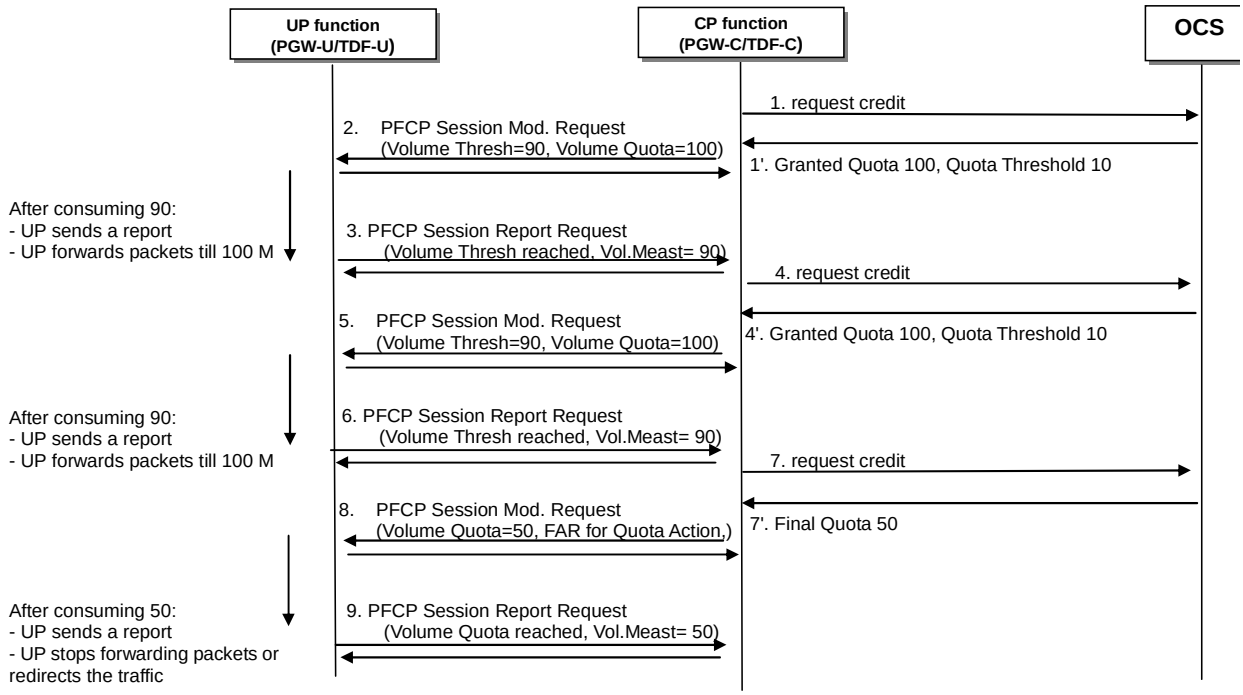



**Figure C.2.1.1-2: Online charging with Quota Action provisioned in the UP function**

1 to 7'. Same as for figure C.2.1.1-1.

8. The CP function sends a PFCP Session Modification Request to the UP function with a Create FAR IE provisioning the action the UP function shall apply when reaching the quota, and with an Update URR IE including the Volume Quota IE set to 50 Mbytes and the FAR ID for Quota Action IE set to the new FAR ID). 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 a PFCP 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.

10. The UP function applies the quota action provisioned at step 8, i.e. it stops forwarding packets or it redirects the traffic towards a redirect destination, according to the FAR identified in the FAR ID for Quota Action.

## C.2.1.2 Online Charging Call Flow with Credit Pooling

### C.2.1.2.1 General

Figure C.2.1.2-1 illustrates a signalling flow over the Sxb and Gy reference points when applying online charging, and when the CP function (i.e. PGW-C) is instructed by the OCS to handle a Credit Pool for a given Gy Session.

### C.2.1.2.2 Example Call Flow 1

In this example, the PGW-C is instructed by the OCS to handle a credit pool for two Rating Groups, RG1 and RG2. The PGW-C provisions two URRs, URR1 and URR2, for the two RGs respectively, and a URR3 for the Credit Pool. The PGW-C provisions the URR1 and URR2 with the quota received from the OCS respectively for RG1 and RG2 (like if there was no credit pooling).

This reflects one possible implementation option, whereby each quota remains managed independently from the others. This approach can result in extra usage reports being sent over Sxb for RG1 or RG2 before the credit pool is exhausted.

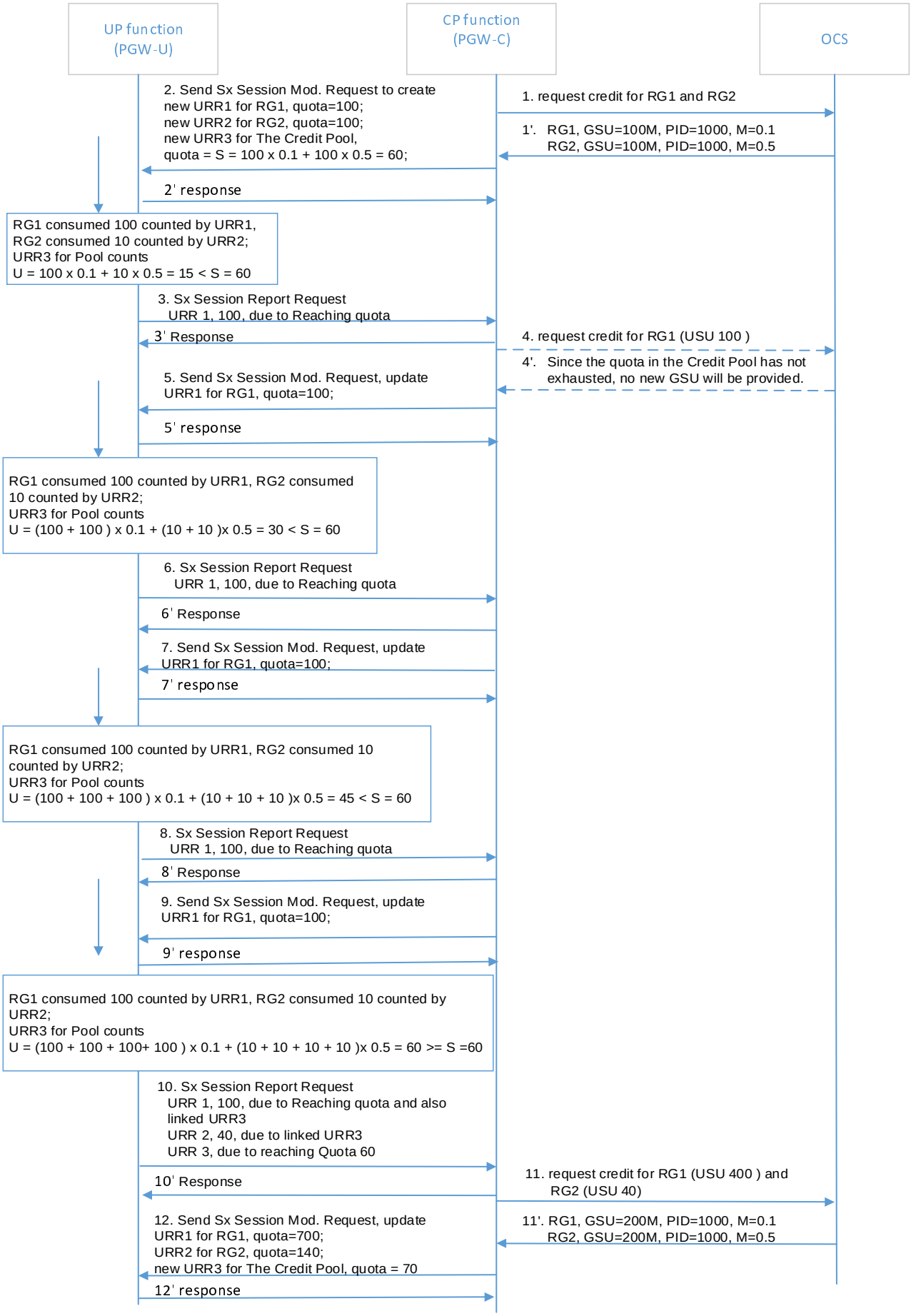



**Figure C.2.2.2-1: Online charging with Credit Pooling (alt 1)**

1. Upon the request from the CP function for RG1 and RG2, the OCS grants:

   RG1: quota 100 Mbytes, together with a G-S-U-Pool-Reference AVP included within the Multiple Services Credit Control (for RG1), where the G-S-U-Pool-Identifier AVP indicating the identifer (e.g. 1000) of the Credit Pool to which the RG1 pertains, the CC-Unit-Type AVP specifies the type of units for which credit is (e.g. total octets), the Unit-Value AVP specifies the multiplier (e.g. 0.1);

   RG2: quotas 100 Mbytes, together with a G-S-U-Pool-Reference AVP included within the Multiple Services Credit Control (for RG2), where the G-S-U-Pool-Identifier AVP indicating the identifer (e.g. 1000) of the Credit Pool to which the RG2 pertains, the CC-Unit-Type AVP specifies the type of units for which credit is (e.g. total octets), the Unit-Value AVP specifies the multiplier (e.g. 0.5);

2. The CP function sends a PFCP Session Modification Request to the UP function, to create:

   A new URR1 for RG1, quota=100, Linked URR = URR3;
   A new URR2 for RG2, quota=100, Linked URR = URR3;
   A new URR3 for Pool, quota = S = 100 x 0.1 + 100 x 0.5 = 60, Aggregated URRs: URR1 with Multiplier 0.1 and URR2 with Multiplier 0.5.

   The UP function accepts the request.

3. The RG1 has consumed 100 counted by URR1, RG2 consumed 10 counted by URR2; the URR3 for the Credit Pool counts U = 100 x 0.1 + 10 x 0.5 = 15 < S. The URR1 triggers sending a usage report towards the CP function due to reaching the Quota 100. So the UP function sends a PFCP Session Report Request, including the Usage Reports for the URR1. The CP function sends the response message.

4. Based on operator's policies, the CP function reports used quota for the RG1 to the OCS. The OCS does not grant any quota since the quota for the Credit Pool has not been consumed yet.

NOTE: This step is skipped in the rest flow.

5. The CP function sends a PFCP Session Modification Request to the UP function with the modified URR1, with new quota 100.

Step 6, 7, 8 and 9 repeats step 3 and 5.

10. The RG1 has consumed another 100 counted by URR1, RG2 consumed another 10 counted by URR2; the URR3 for the Credit Pool counts U = (100 + 100 + 100 + 100) x 0.1 + (10 +10 + 10 + 10) x 0.5 = 60 >= S = 60. So the UP function sends a PFCP Session Report Request, including the Usage Reports for:
    - the URR3, generated due to reaching quota (60),
    - for the URR1, generated due to that it is linked to the URR3 and it has reached the quota 100, and
    - for the URR2 generated due to that it is linked to the URR3.
    The CP function sends the response message.

11. The CP function requests new Quota for RG1 and RG2 to the OCS. The OCS grants 200M for RG1 and 100M for RG2, with the same pool ID and Multipliers.

12. The CP function sends a PFCP Session Modification Request to the UP function with the modified URRs, for URR1, URR2 and URR3.

#### C.2.1.2.3 Example Call Flow 2

In this example, the PGW-C is instructed by the OCS to handle a credit pool for two Rating Groups, RG1 and RG2. The PGW-C provisions two URRs, URR1 and URR2, for the two RGs respectively, and a URR3 for the Credit Pool. The PGW-C provisions the quotas for URR1 and URR2 taking into account the credit pool quota and the multipliers of the RGs.

This reflects another possible implementation option. This approach avoids extra usage reports being sent over Sxb for RG1 or RG2 before the credit pool is exhausted, and thus reduces Sxb signalling.

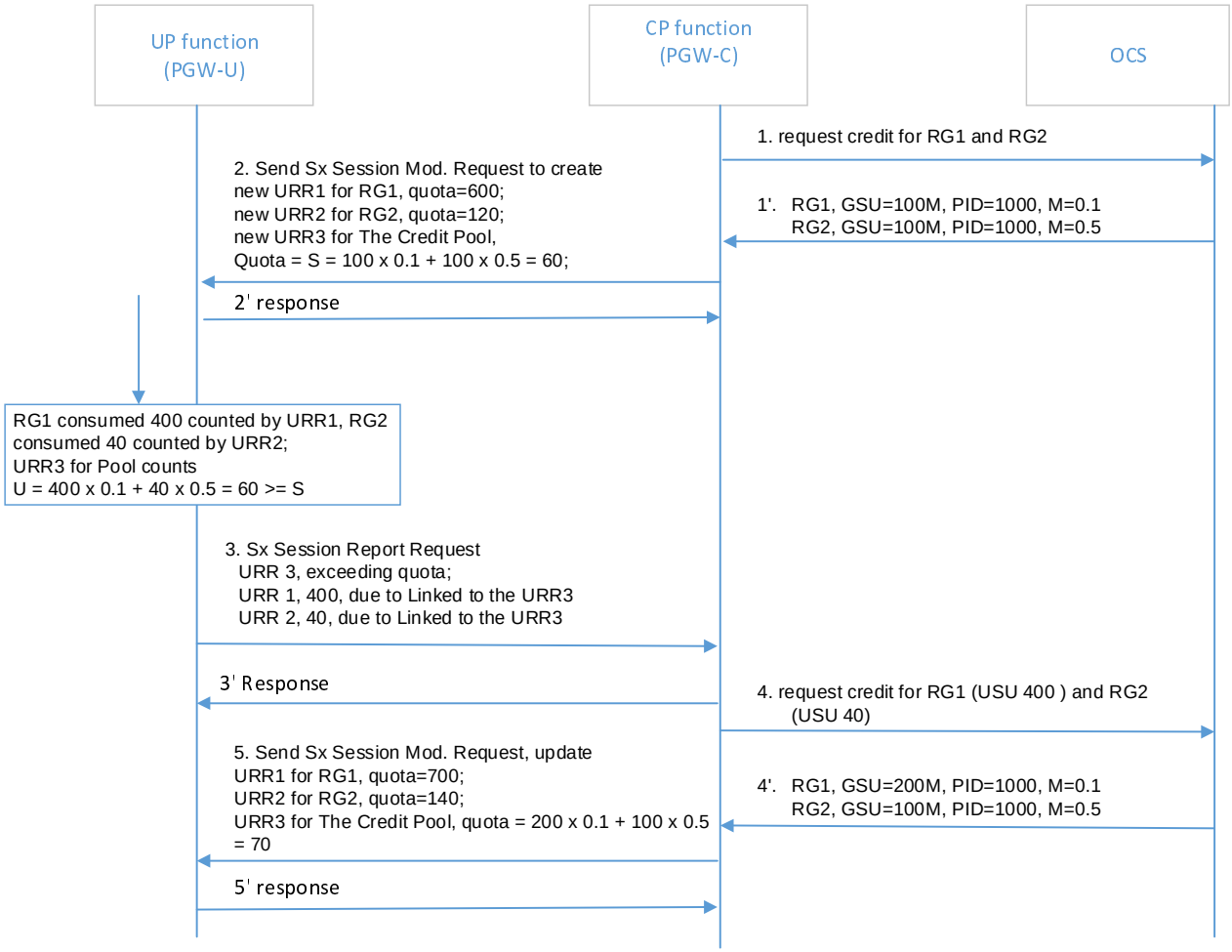



**Figure C.2.2.3-2: Online charging with Credit Pooling (alt 2)**

1. Upon the request from the CP function for RG1 and RG2, the OCS grants:

   RG1: quota 100 Mbytes, together with a G-S-U-Pool-Reference AVP included within the Multiple Services Credit Control (for RG1), where the G-S-U-Pool-Identifier AVP indicating the identifer (e.g. 1000) of the Credit Pool to which the RG1 pertains, the CC-Unit-Type AVP specifies the type of units for which credit is (e.g. total octets), the Unit-Value AVP specifies the multiplier (e.g. 0.1);

   RG2: quotas 100 Mbytes, together with a G-S-U-Pool-Reference AVP included within the Multiple Services Credit Control (for RG2), where the G-S-U-Pool-Identifier AVP indicating the identifer (e.g. 1000) of the Credit Pool to which the RG2 pertains, the CC-Unit-Type AVP specifies the type of units for which credit is (e.g. total octets), the Unit-Value AVP specifies the multiplier (e.g. 0.5);

2. The CP function sends a PFCP Session Modification Request to the UP function, to create:

   A new URR1 for RG1, quota=600, Linked URR = URR3;
   A new URR2 for RG2, quota=120, Linked URR = URR3;
   And new URR3 for Pool, quota = S = 100 x 0.1 + 100 x 0.5 = 60, Aggregated URRs: URR1 with Multiplier 0.1 and URR2 with Multiplier 0.5.

   The UP function accepts the request.

NOTE 1: To avoid receiving usage report upon exceeding the original Quota for RG1 or RG2, the quota can be set to 60 / 0.1 = 600 for RG1, assuming RG1 consumes the complete Quota for the pool; similarly, for RG2, the quota can be set to 60 / 0.5 = 120;

3. The URR3 always first reaches the Quota, e.g. when the URR1 has counted 400, and URR2 has counted 40, this results the counted usage for the Credit Pool U=400 x 0.1 + 40 x 0.5 = 60. So the UP function sends a PFCP Session Report Request, including the Usage Reports:

- for the URR3, generated due to that it has reached quota (60);
  - for the URR1, generated due to that it is linked to the URR3; and
  - for the URR2, generated due to that it is linked to the URR3.

The CP function sends the response message.

4. The CP function requests new Quota for RG1 and RG2 to the OCS. The OCS grants 200M for RG1 and 100M for RG2, with the same pool ID and Multipliers.

5. The CP function sends a PFCP Session Modification Request to the UP function with the modified URRs, for URR1, URR2 and URR3.

   URR1 for RG1, quota=70 / 0.1 = 700;

   URR2 for RG2, quota=70 / 0.5 = 140;

   URR3 for The Credit Pool, quota = 200 x 0.1 + 100 x 0.5 = 70.

# Annex D (Normative): Use of PFCP over N16a for the support of traffic offload by UPF controlled by I-SMF

## D.1 General

This Annex applies to PDU sessions involving an Intermediate SMF (I-SMF), when the I-SMF has inserted an Uplink Classifier (UL CL) or Banching Point (BP) into the data path of the PDU session and a local PDU Session Anchor (PSA) further called PSA2 in this Annex, for local traffic offload.

For such PDU sessions, PFCP session related messages shall be exchanged between the SMF and I-SMF for:

- the SMF to provide N4 information to the I-SMF regarding how the traffic shall be detected, enforced and monitored in the UPF(s) controlled by the I-SMF;
- the I-SMF to forward N4 information with traffic usage reporting to the SMF.

See clause 5.34.6 of 3GPP TS 23.501 [28].

Whether the UL CL or BP and PSA2 are supported by the same UPF or not shall be transparent to the SMF.

When exchanging N4 information over N16a, the SMF and I-SMF shall assume the model in Figure D.1-1 where the UL CL or BP and PSA2 are supported by separate UPFs, i.e. separate PFCP session related messages shall be exchanged over N4 for the UL CL/BP and for the PSA2.

NOTE 1: This allows the SMF and I-SMF to exchange unambiguous information on whether N4 information exchanged over N16a relates to the UL CL/BP or the PSA2, e.g. whether a QER is to be enforced in the UL CL/BP or PSA2.

NOTE 2: The UL CL/BP and PSA2 inserted by the I-SMF can be co-located or located on different UPFs, regardless of the model assumed over N16a for the exchange of N4 information.

NOTE 3: Only one local PSA (i.e. PSA2) is shown in this figure; in real deployment, more than one local PSAs can be inserted.

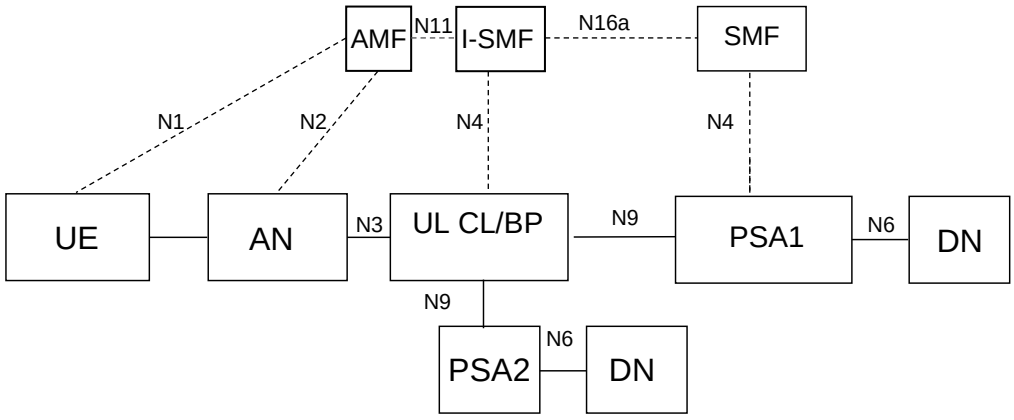



**Figure D.1-1: UL CL/BP and PSA2 model for N4 information exchanged over N16a**

The I-SMF shall translate the N4 information received from the SMF into appropriate N4 rules towards the UL CL/BP and the PSA2; the I-SMF shall merge the N4 information received for the UL CL/BP and the PSA2 if the UL CL/BP and PSA2 are located on the same UPF.

The N4 information exchanged over N16a shall only include the rules related to the UL and DL traffic to offload via PSA2, and not include the rules to the non-offload UL and DL traffic via PSA1. The I-SMF shall generate on its own

N4 rules towards the UL CL/BP for UL and DL traffic exchanged between the AN and PSA1. The PDR, FAR, URR, QER ID(s) allocated by the I-SMF and the SMF for the PFCP sessions between I-SMF and UL CL and between I-SMF and PSA2 shall be distinct; the Precedence of the PDRs set by the I-SMF and the SMF shall also be distinct (see clause D.2.1).

All the PFCP session related messages specified in clause 7.5 shall be supported over N16a. Unless specified otherwise in this Annex, the requirements specified in the rest of this specification for PFCP session related procedures and messages are also applicable to N16a.

None of the PFCP Node related messages specified in clause 7.4 shall be sent over N16a. PFCP Load and Overload control information shall not be exchanged over N16a.

Data forwarding procedures (see clause 5.3) shall not be used over N16a.

PFCP session related messages shall be sent over N16a in a binary body part of an HTTP multipart message using the Nsmf_PDUSession as specified in 3GPP TS 29.502 [50]. The Json body part of a HTTP multipart message shall indicate whether a given PFCP session related message relates to the UL CL/BP or to the PSA2. Presence of the DNAI IE indicates the PFCP session message relates to PSA2 and absence of the DNAI IE indicates the PFCP session message relates to UL CL/BP.

# D.2 Procedures

## D.2.1 Addition of PSA and UL CL/BP controlled by I-SMF

The corresponding stage 2 call flow is specified in clause 4.23.9.1 of 3GPP TS 23.502 [29].

When the I-SMF decides to select a new PSA2 and/or a UL CL/BP (replacing the current I-UPF) for the PDU session, e.g. using the list of DNAI(s) of interest for this PDU Session received from the SMF, it shall establish PFCP sessions towards UL CL/BP and/or PSA2 respectively.

The I-SMF shall allocate PDR/FAR/URR/QER ID not larger than 255 and shall set Precedence value not smaller than 65536. The SMF shall allocate PDR/FAR/URR/QER ID from 256 onwards and shall set Precedence value not larger than 65535.

NOTE 1: Since PDRs provided by the SMF to control the traffic via PSA2 have higher precedence than PDRs generated by the I-SMF, the I-SMF need not modify the PDRs generated by its own. See the example further down.

For the PFCP session established between I-SMF and UL CL/BP:

- the I-SMF shall create at least a UL PDR to identify the UL traffic received from AN and a UL FAR to forward the traffic towards PSA1;
- the I-SMF shall create a DL PDR to identify the DL traffic from the PSA1 and a DL FAR to forward the traffic towards the AN;

NOTE 2: The I-SMF needs to include DL N9 F-TEID in the SMF PDUSession Update Request sent to SMF as specified in 3GPP TS 29.502 [50].

For the PFCP session established between I-SMF and PSA2:

- the I-SMF shall create at least an UL PDR to identify the UL traffic received from UL CL/BP and a UL FAR to forward the traffic towards the DN;
- the I-SMF shall create a DL PDR to identify the DL traffic from the DN and a DL FAR to forward the traffic towards the UL CL/BP;

NOTE 3: If IPv6 multi-homing applies to the PDU session, a new IPv6 prefix can be allocated by the PSA2, which is sent in SMF PDUSession Update Request to SMF.

Upon successful establishment of the PFCP sessions, the I-SMF indicates to the SMF that it has inserted an UL CL/BP and PSA by sending a SMF PDUSession Update Request to the SMF (see step 4 clause 4.23.9.1 of 3GPP TS 23.502 [29]).

When the I-SMF indicates to the SMF that it has inserted an UL CL/BP and PSA, the SMF shall send two PFCP Session Establishment Requests towards the I-SMF, one targeting the UL CL/BP and another one targeting the PSA2, with the following information:

1) PFCP Session Establishment Request for the UL CL/BP:

- For the support of the UL traffic offloaded towards PSA2:

  - one Create Traffic Endpoint IE, just including a Traffic EndPoint ID; the UL traffic endpoint corresponds to the N3 endpoint of UL CL/BP; the UL traffic endpoint shall not contain information about the N3 interface, i.e. the Network Instance IE and the Local F-TEID IE shall not be included;

  - at least one Create PDR IE with:

- the Source Interface set to "Access";

- the Traffic Endpoint IE referring to the UL traffic endpoint;

- any additional Packet Detection Information to define the UL traffic to match (e.g. SDF Filter, Application ID, Ethernet Packet Filter);

- any applicable PDR information, e.g. FAR ID, URR ID, QER ID.

UL PDRs shall not contain the Outer Header Removal IE.

  - one UL FAR set to forward (or drop) the UL traffic, with the Destination Interface set to "Core". If more than one local PSA has been inserted by the I-SMF, the UL FAR shall indicate the Data Network Access Identifier associated to the local PSA towards which the UL traffic shall be forwarded; the UL FAR may do so otherwise.

- For the support of the DL traffic offloaded from PSA2:

  - one Create Traffic Endpoint IE, including a Traffic EndPoint ID; the DL traffic endpoint shall not contain information about the N9 interface, i.e. the Network Instance IE and the Local F-TEID IE shall not be included;

  - at least one Create PDR IE with:

- the Source Interface set to "Core";

- the Traffic Endpoint IE referring to the DL traffic endpoint;

- any applicable PDR information, e.g. FAR ID, URR ID, QER ID;

  - one DL FAR set to forward (or drop) the DL traffic to the access network, with the Destination Interface set to "Access"; the DL FAR shall not contain the Outer Header Creation IE;

NOTE 4: The I-SMF is responsible for all the N3 and N9 protocol aspects (e.g. Network Instance, Local F-TEID, outer header creation or removal).

- any applicable QERs and/or URRs.

2) PFCP Session Establishment Request for the PSA2:

- For the support of the UL traffic offloaded at PSA2:

  - one Create Traffic Endpoint IE, just including a Traffic EndPoint ID; the UL traffic endpoint shall not contain information about the N9 interface, i.e. the Network Instance IE and the Local F-TEID IE shall not be included;

  - at least one Create PDR IE with:

- the Source Interface set to " Access ";

- the Traffic Endpoint IE referring to the UL traffic endpoint;

- any applicable PDR information, e.g. FAR ID, URR ID, QER ID;

UL PDRs shall not contain the Outer Header Removal IE;

- one UL FAR set to forward (or drop) the UL traffic, with the Destination Interface set to "Core".

- For the support of the DL traffic offloaded at PSA2:

  - one Create Traffic Endpoint IE, including a Traffic EndPoint ID and any additional information to define the DL traffic endpoint (e.g. Network Instance IE, UE IP Address IE); the DL traffic endpoint corresponds to the N6 endpoint of PSA2;

  - at least one Create PDR IE with:

- the Source Interface set to "Core";

- the Traffic Endpoint IE referring to the DL traffic endpoint;

- any additional Packet Detection Information to define the DL traffic to match (e.g. SDF Filter, Application ID, Ethernet Packet Filter);

- any applicable PDR information, e.g. FAR ID, URR ID, QER ID;

  - one DL FAR set to forward (or drop) the DL traffic, with the Destination Interface set to " Access "; the DL FAR shall not contain the Outer Header Creation IE.

  NOTE 5: The I-SMF is responsible for all the N3 and N9 protocol aspects (e.g. Network Instance, Local F-TEID, outer header creation or removal).

  - Any applicable QERs and/or URRs.

In the PFCP Session Establishment Request for the UL CL/BP, the SMF shall not include any N4 rules for the UL and DL traffic via PSA1 (i.e. non-offload traffic exchanged between AN and PSA1).

The I-SMF shall translate the SMF instructions into N4 instructions to send to the UL CL/BP and PSA2, for the UL and DL traffic in one or more PFCP Session Modification Request message(s) (the I-SMF has already created a PFCP session in the UL CL/BP and PSA2 in steps 2 and 3 of Figure 4.23.9.1-1 of 3GPP TS 23.502 [29]). In particular:

- the I-SMF shall map the UL and DL traffic endpoints requested to be created by the SMF in the UL CL/BP and PSA2 respectively to the UL and DL traffic endpoints created in the UL CL/BP and in PSA2 for UL and DL traffic; the I-SMF shall update the DL traffic endpoint in PSA2 if necessary, e.g. with any Framed-Route or Framed-IPv6-Route information received from the SMF;

- the I-SMF shall add the Outer Header Removal IE to the UL PDR of the UL CL/BP;

- the I-SMF shall add an Outer Header Creation IE to DL PDR(s) of the UL CL/BP to add a GTP-U header set to the 5G-AN F-TEID, and to add a Network Instance IE if needed;

- the I-SMF shall update the UL FAR of the UL CL/BP and the DL FAR of the PSA2 with N9 protocol information, if the UL CL/BP and PSA2 are located on different UPFs; if more than one local PSA has been inserted by the I-SMF, the I-SMF shall derive the local PSA towards which the UL traffic shall be forwarded from the Data Network Access Identifier IE indicated in the UL FAR over N16a.

- the I-SMF shall overwrite the Apply Action IE of the DL FAR received from the SMF according to the User Plane connection state of the PDU session, e.g. to request the UPF to buffer packets if the PDU session is deactivated, or to forward the DL packets otherwise;

- the I-SMF shall merge the N4 information received for the UL CL/BP and the PSA2 if the UL CL/BP and PSA2 are located on the same UPF.

The I-SMF shall return two PFCP Session Establishment Response messages to the SMF for UL CL/BP and PSA2 respectively. In the PFCP Session Establishment Response messages, the I-SMF may set the Node ID IE and UP F-SEID IE to the ones provided by the UL CL/BP and the PSA2. The Created PDR and Created Traffic Endpoint shall not be included.

The I-SMF shall generate by itself the N4 rules to control the UL and DL traffic via PSA1 (i.e. non-offload traffic exchanged between AN and PSA1), and send such N4 rules to the UL CL/BP together with the N4 rules mapped from the N4 information sent by the SMF.

EXAMPLE: Example of addition of PSA2 and UL CL controlled by I-SMF:

1) in step 3 of clause 4.23.9.1 of 3GPP TS 23.502 [29], when establishing the PFCP session between I-SMF and UL CL/BP, the I-SMF can provide the following PDRs/FARs to the UL CL/BP:

   UL PDR1 (UL F-TEID 1 is allocated to receive UL traffic from NG-RAN ) and
   UL FAR1 (forward all traffic towards PSA1);

   DL PDR2 (N9 DL F-TEID is allocated to receive DL traffic from PSA1 which will be reported in SMF PDUSession Update Request towards SMF) and
   DL FAR2 (forward all traffic towards NG-RAN N3 F-TEID).

2) in step 2 of clause 4.23.9.1 of 3GPP TS 23.502 [29], when establishing the PFCP session between I-SMF and PSA2, the I-SMF can provide the following PDRs/FARs to PSA2:

   UL PDR1 (to receive traffic from UL CL, i.e. including the UL F-TEID of UL CL) and
   UL FAR1 (forward all traffic towards DN);

   DL PDR2 (to receive traffic from DN) and
   DL FAR2 (forward all traffic towards UL CL's N9 DL F-TEID).

3) in step 6 of clause 4.23.9.1 of 3GPP TS 23.502 [29], the SMF sends an SMF PDUSession Update Request to the I-SMF encapsulating binary encoded PFCP Session Establishment Request messages to request to offload service traffic towards PSA2, e.g. for a service which is identified by app-id 100;

   In the PFCP Session Establishment Request message for PSA2, the SMF includes:

   UL PDR 256 (where the PDI includes app-id =100) and
   UL FAR 256 (forward all traffic towards DN);

   DL PDR 257 (sending traffic to UL CL, where the PDI includes app-id=100) and
   DL FAR 257 (sending traffic to UL CL).

In the PFCP Session Establishment Request message for UL CL, the SMF includes:

   UL PDR 256 (where the PDI includes app-id =100) and
   UL FAR 256 (forward traffic towards PSA2);

   DL PDR 257 (identifying all traffic received from PSA2) and
   DL FAR 257 (forward traffic toward access);

4) in step 7 of clause 4.23.9.1 of 3GPP TS 23.502 [29], the I-SMF maps rules received in 3) in the PFCP Session Modification Request message to the PSA2, and the PDR1 and PDR2 provisioned earlier by I-SMF during the PFCP session establishment procedure will not be matched for the application traffic identified by app-id 100 due to a lower precedence.

5) in step 8 of clause 4.23.9.1 of 3GPP TS 23.502 [29], the I-SMF can maps rules received in 3) in the PFCP Session Modification Request message to the UL CL, the PDR1 (forwarding all traffic to PSA1) provisioned earlier by I-SMF during the PFCP session establishment procedure will not be matched for the application traffic identified by app-id 100 due to a lower precedence.

## D.2.2 Removal of PSA and UL CL/BP

The corresponding stage 2 call flow is specified in clause 4.23.9.2 of 3GPP TS 23.502 [29].

When the I-SMF indicates to the SMF that it is removing a UL CL/BP and PSA, the SMF shall send two PFCP Session Deletion Requests towards the I-SMF, one for the UL CL/BP and another one for the PSA2. The I-SMF shall return two PFCP Session Deletion Responses to the SMF (including usage reports if applicable, see clause 7.5.7.1).

## D.2.3 Change of PSA

The corresponding stage 2 call flow is specified in clause 4.23.9.3 of 3GPP TS 23.502 [29].

When the I-SMF indicates to the SMF a change of traffic offload, the SMF shall send a PFCP Session Establishment Request (for the new DNAI), a PFCP Session Deletion Request (for the old DNAI) towards the I-SMF, and a PFCP Session Modification Request for the UL CL/BP if needed. The I-SMF shall behave as described in clauses D.2.1 and D.2.2 and return a PFCP Session Establishment Response, a PFCP Session Deletion Response and a PFCP Session Modification Response if needed.

## D.2.4 Traffic Usage Reporting

The SMF may request the I-SMF to report traffic usage measurements as specified in the rest of this specification.

The I-SMF shall report traffic usage measurements to the SMF as specified in the rest of this specification, i.e. in PFCP Session Report Request, PFCP Session Modification Response and PFCP Session Deletion Response messages.

## D.2.5 Updating N4 information towards I-SMF

The SMF may send PFCP Session Modification Requests with updated PFCP rules (e.g. updated PDR, QER URR), targeting the UL CL/BP or PSA2, as specified in the rest of this specification. The I-SMF shall return PFCP Session Modification Responses accordingly.

## D.2.6 PDU session release

Corresponding stage 2 requirements are specified in clauses 4.23.3a and 4.23.5.2 of 3GPP TS 23.502 [29].

If an UL/CL or BP was inserted in the data path by the I-SMF:

- In scenarios where the I-SMF sends a Release Request to the SMF, e.g. UE deregistration procedure, the I-SMF shall first send a PFCP Session Deletion Request to the UL CL/BP and local PSA to retrieve non-zero traffic usage reports, before sending the Release Request over N16a to the SMF. If the I-SMF needs to report traffic usage measurements to the SMF for the UL CL/BP and/or for the local PSA, the I-SMF shall encapsulate one PFCP Session Report Request for the UL CL/BP and/or one PFCP Session Report Request for the local PSA in the Release Request sent over N16a to the SMF. The SMF shall encapsulate corresponding PFCP Session Report Response(s) in the Release Response.

  If more traffic usage measurements need to be reported to the SMF, the I-SMF shall send one or more Update Request(s) towards the SMF before sending a Release Request.

  Upon receiving the Release Request from the I-SMF, the SMF shall consider that the PFCP sessions between the I-SMF and UL CL/BP and local PSA have been deleted.

- In scenarios where the I-SMF sends an Update Request to the SMF, e.g. UE initiated PDU session release, if the I-SMF needs to report traffic usage measurements to the SMF for the UL CL/BP and/or for the local PSA, the I-SMF may encapsulate one PFCP Session Report Request for the UL CL/BP and/or one PFCP Session Report Request for the local PSA in the Update Request sent over N16a to the SMF (i.e. in step 3a of Figure 4.3.4.3-1 of 3GPP TS 23.502 [29])). If so, the SMF shall encapsulate corresponding PFCP Session Report Response(s) in the Update Response.

  The SMF shall then send two PFCP Session Deletion Requests towards the I-SMF, one for the UL CL/BP and another one for the local PSA, in the subsequent Update Request initiated by the SMF towards the I-SMF to trigger the release of the PDU session (i.e. in step 3a of Figure 4.3.4.3-1 of 3GPP TS 23.502 [29]). The I-SMF shall encapsulate corresponding PFCP Session Deletion Response(s) in the Update Response (i.e. in step 14 of Figure 4.3.4.3-1 of 3GPP TS 23.502 [29]), including usage reports if applicable, see clause 7.5.7.1. The PFCP Session Deletion Response may indicate that additional usage reports need to be signalled; if so, the I-SMF shall send additional Update Request(s) towards the SMF encapsulating PFCP Session Report Requests and the SMF shall return Update Response (s) encapsulating PFCP Session Report Responses. When the last usage report has

been received, the SMF shall notify the I-SMF that the PDU session is released (in step 16a of Figure 4.3.4.3-1 of 3GPP TS 23.502 [29]).

## D.2.7 Simultaneous change of UL CL/BP and PSA controlled by I-SMF

The corresponding stage 2 call flow is specified in clause 4.23.9.4 of 3GPP TS 23.502 [29]. Figure D.2.7-1 specifies the details of the signalling interactions between the SMF and the I-SMF, and between the I-SMF and the UL CL/BPs and PSAs.

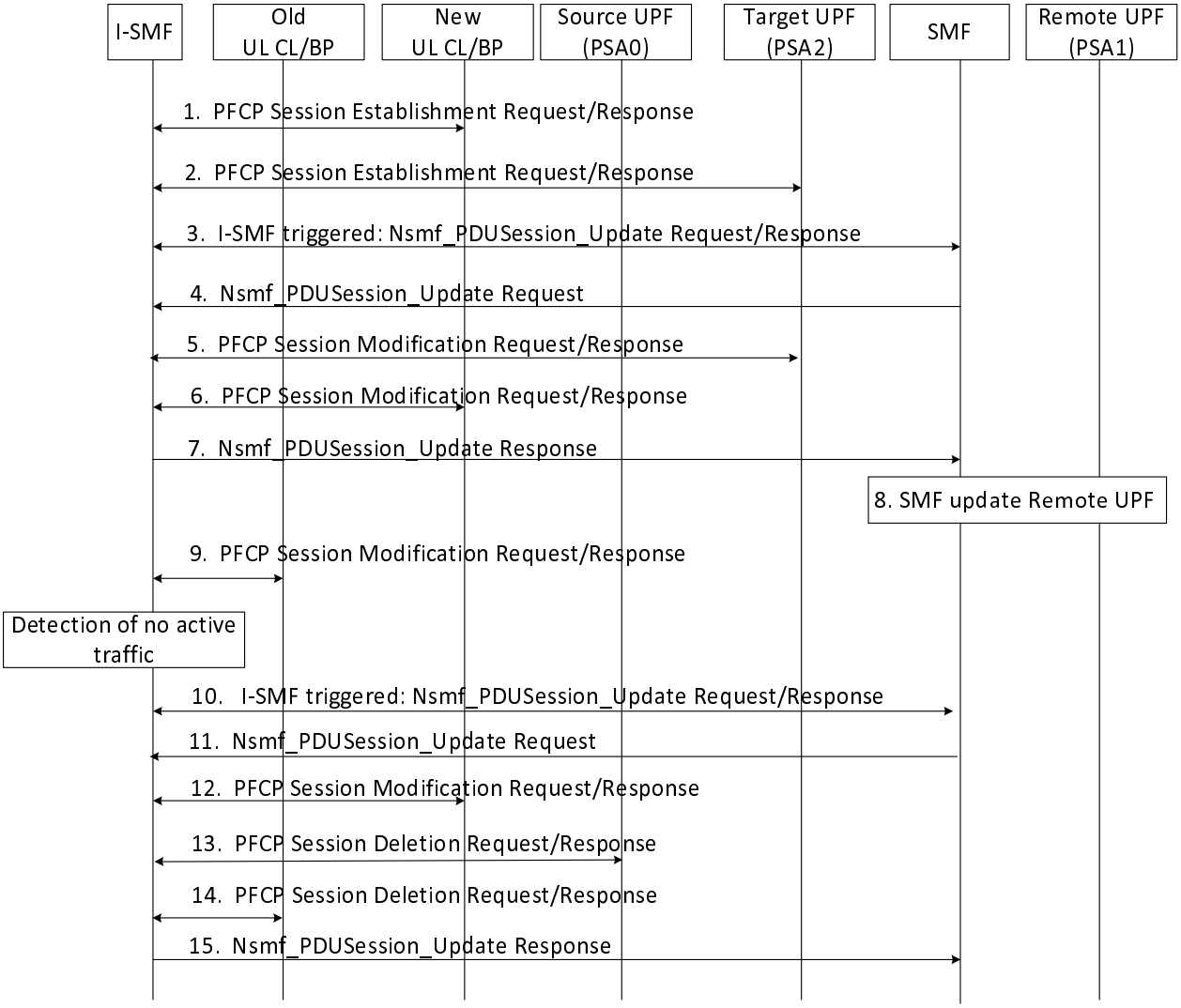



**Figure D.2.7-1 – Simultaneous change of UL CL/BP and PSA controlled by I-SMF**

1-2. These steps are the same as described in clause D.2.1 and correspond to steps 2 and 3 of Figure 4.23.9.4-1 of 3GPP TS 23.502 [29].

3. The I-SMF indicates to the SMF that it has inserted an UL CL/BP and PSA if both the I-SMF and the SMF support the "N9FSC" feature defined in clause 6.1.8 of 3GPP TS 29.502 [50], or the I-SMF indicates to the SMF a change of UL CL/BP and PSA if either the I-SMF or the SMF does no support the "N9FSC" feature.

4. When the I-SMF indicates to the SMF an insertion of UL CL/BP and PSA, and data forwarding between the new and old UL CL/BPs for EAS session continuity is required, the SMF shall send to the I-SMF a PFCP Session Establishment Request (for the new DNAI) and a PFCP Session Establishment Request for the new UL CL/BP.

When the I-SMF indicates to the SMF a change of UL CL/BP and PSA, or when the I-SMF indicates to the SMF an insertion of UL CL/BP and PSA and data forwarding between the new and old UL CL/BPs for EAS session continuity

is not required, the SMF shall send to the I-SMF a PFCP Session Establishment Request (for the new DNAI), a PFCP Session Deletion Request (for the old DNAI), a PFCP Session Deletion Request for the old UL CL/BP and a PFCP Session Establishment Request for the new UL CL/BP. The I-SMF shall behave as described in clauses D.2.1 and D.2.2 and return two PFCP Session Establishment Responses and two PFCP Session Deletion Responses.

The following signalling applies if both the I-SMF and the SMF support the "N9FSC" feature and data forwarding between the new and old UL CL/BPs for EAS session continuity is required.

Step 4 is same as described in clause D.2.1, in addition, the SMF shall send the following additional information to the I-SMF:

- in the PFCP Session Establishment Request for the new UL CL/BP:
  - Create PDR(s) IE for the UL traffic to forward to the old UL CL/BP with:
    - the Source Interface set to "Access";
    - the Traffic Endpoint IE referring to the UL traffic endpoint;
    - any additional Packet Detection Information to define the UL traffic to match for N9 forwarding (e.g. SDF Filter, Application ID, Ethernet Packet Filter);
    - any applicable PDR information, e.g. FAR ID, QER ID;
    - the UL PDR shall not contain the Outer Header Removal IE;
    - the Precedence value of the above UL PDR for N9 forwarding to the old UL CL/BP shall be set to a higher precedence than the UL PDR for the new UL CL/BP to support the UL traffic offloaded towards the PSA2, if the same Packet Detection Information applies.
  - one UL FAR, set to "forward" the UL traffic to the old UL CL/BP, with the Destination Interface set to "Core"; the UL FAR shall not contain the Outer Header Creation IE.
- the following additional information in the Update Request:
  - the indication that a N9 forwarding tunnel between UL CLs/BPs is required;
  - the list of Rule IDs pointing to the UL PDRs included in the PFCP Session Establishment Request for the new UL CL/BP to establish the UL N9 data forwarding in the new UL CL/BP;
  - the value of the timer to detect the end of activity on the N9 forwarding tunnel.

NOTE: The UL PDR(s) for UL traffic offloaded towards PSA2 will not be matched as long as the UL PDR(s) for UL traffic forwarding to the old UL CL/BP is installed in the target UL CL/BP if the same Packet Detection Information applies, since the latter PDR(s) has a higher precedence than the former.

5. The step is same as described in clause D.2.1, i.e. the SMF updates the remote PSA (PSA1) via N4 with the DL Tunnel Info of the Target UL CL/BP for the downlink traffic.
6. The I-SMF shall map the above rules received in the PFCP Session Establishment Request message to the new UL CL/BP. In particular:
   - the I-SMF shall add the Outer Header Removal IE to the UL PDR(s) of the UL CL/BP for the UL traffic to be forwarded to the old UL CL/BP;
   - the I-SMF shall add an Outer Header Creation IE to the UL FAR of the UL CL/BP to add a GTP-U header set to the old N3 UL F-TEID in the old UL CL/BP if it can be reused;
   - the I-SMF shall provision a DL PDR to receive DL traffic forwarded from the old UL CL/BP and a DL FAR to forward the received DL traffic towards the NG-RAN. The new UL CL/BP shall assign a new N9 DL F-TEID for the old UL CL/BP.
7. The I-SMF returns two PFCP Session Establishment Responses to the SMF.
8. The step is same as described in clause D.2.1.

9. The I-SMF shall send the following information to the old UL CL/BP in the PFCP Session Modification Request based on the additional information received in the Update Request from the SMF and the PFCP Session Establishment Response from the new UL CL/BP:

   - the I-SMF shall update the Outer Header Creation IE in the DL FAR of the old UL CL/BP to add a GTP-U header set to the F-TEID assigned by the new UL CL/BP for DL traffic forwarding;

   - the I-SMF shall update the UL PDR(s) to receive UL traffic forwarded from the new UL CL/BP, if the old UL CL/BP needs to assign a new N9 DL F-TEID for the new UL CL/BP;

   - instruct the old UL CL/BP to report user inactivity on the N9 forwarding tunnel by provisioning the received time in the User Plane Inactivity Timer IE (as specified in clause 5.11.2).

If the old UL CL/BP assigns a new N9 DL F-TEID to receive the UL traffic from the new UL CL/BP, the I-SMF shall send a PFCP Session Modification Request message to the new UL CL/BP to add an Outer Header Creation IE to the UL FAR of the UL CL/BP to add a GTP-U header set to the new N9 UL F-TEID assigned by the old UL CL/BP for UL traffic forwarding, and to add a Network Instance IE if needed.

10. If the User Plane Inactivity Report is received from the old UL CL/BP due to the User Plane Inactivity Timer expires, the I-SMF indicates to the SMF that it is removing the old UL CL/BP and PSA0.

11. The SMF shall send to the I-SMF a PFCP Session Deletion Request (for the old DNAI) and a PFCP Session Deletion Request for the old UL CL/BP.

12-14. The I-SMF shall remove the UL PDR(s) identified by the received Rule ID(s) in the target UL CL/BP and the PFCP sessions in old UL CL/BP/PSA0.

15. The I-SMF returns two PFCP Session Deletion Responses to the SMF.

## D.2.8 Simultaneous change of UL CL/BP and PSA controlled by different I-SMFs

The corresponding stage 2 call flow is specified in clause 4.23.9.5 of 3GPP TS 23.502 [29]. Figure D.2.8-1 specifies the details of the signalling between the SMF and the I-SMF, and between the I-SMFs and the UL CL/BPs and PSAs.

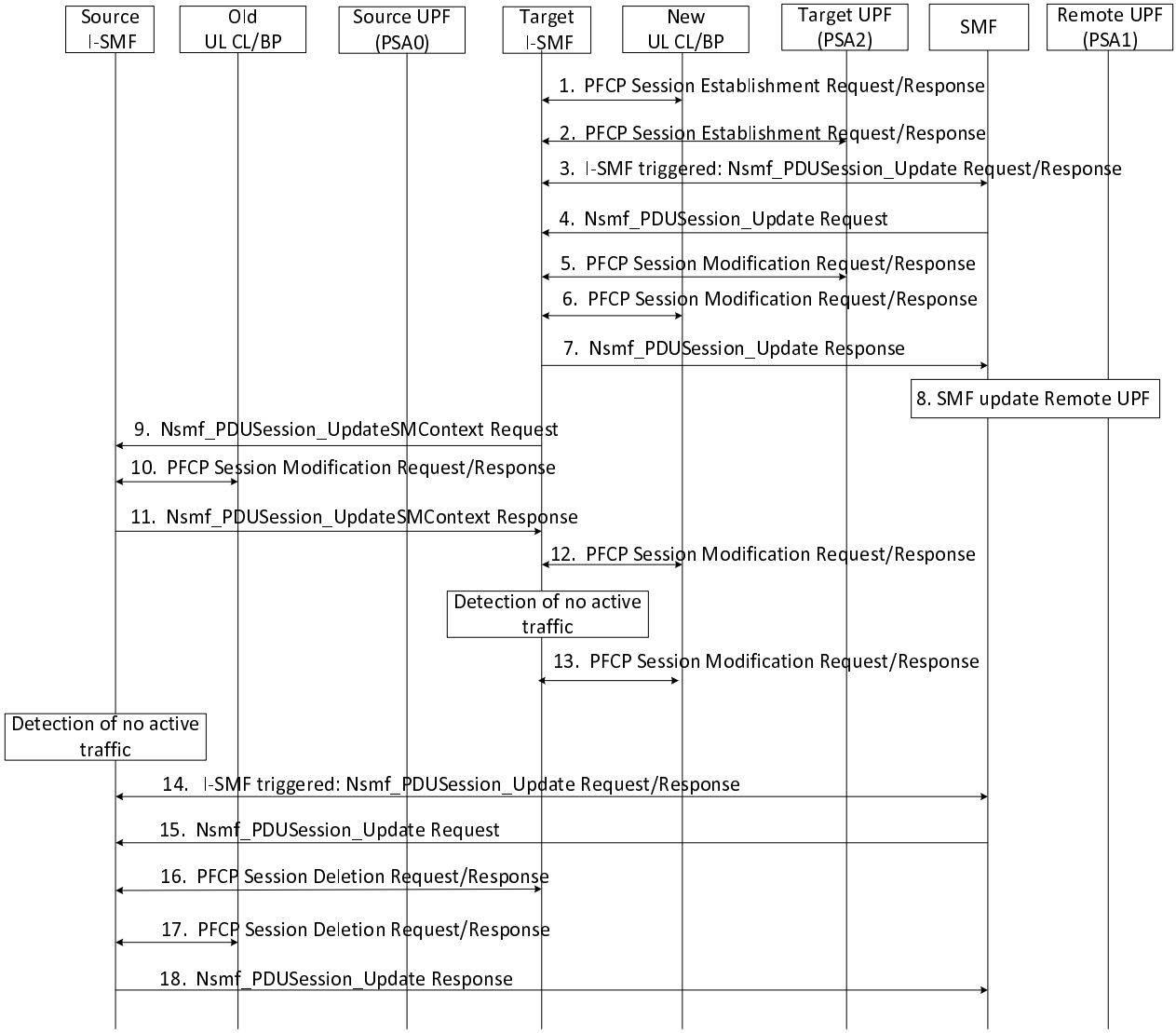



**Figure D.2.8-1 – Simultaneous change of UL CL/BP and PSA controlled by different I-SMFs**

1-2. These steps are the same as described in clause D.2.7.

3. The target I-SMF indicates to the SMF the insertion of UL CL/BP and PSA.

4. The SMF shall send to the target I-SMF a PFCP Session Establishment Request (for the new DNAI) and a PFCP Session Establishment Request for the new UL CL/BP.

In addition, to support the EAS session continuity, the SMF may send additional information to the target I-SMF as defined in step 4 of clause D.2.7.

5-6. The target I-SMF shall behave as described in step 5 and 6 of clause D.2.7. In addition, the target I-SMF shall provision a URR with a User Plane Inactivity Timer IE in the new UL CL/BP, based on the user plane inactivity time received from the SMF, and associate it to the UL PDR(s) used detecting the UL traffic to forward towards the old UL CL/BP and the DL PDR(s) used for detecting the DL traffic from the old UL CL/BP (as specified in clause 5.11.3).

7-8. These steps are the same as described in clause D.2.7.

9. The target I-SMF shall send an Nsmf_PDUSession_UpdateSMContext Request (N9 forwarding tunnel required, target UL CL N9 forwarding tunnel info, value of the timer to detect the end of activity on the N9 forwarding tunnel to support the EAS session continuity) to the source I-SMF, as specified in clause 5.2.2.3.x of 3GPP TS 29.502 [50].

10. The source I-SMF shall send the following information to the old UL CL/BP in the PFCP Session Modification Request based on the information received from the target I-SMF:

    - the source I-SMF shall update the Outer Header Creation IE in the DL FAR of the old UL CL/BP to add a GTP-U header set to the F-TEID assigned by the new UL CL/BP for DL traffic forwarding;

    - instruct the old UL CL/BP to report user inactivity on the N9 forwarding tunnel by provisioning the received time in the User Plane Inactivity Timer IE (as specified in clause 5.11.2).

11. The source I-SMF shall return information to the target I-SMF, e.g. F-TEID in old UL CL/BP on receiving the UL traffic from the new UL CL/BP, as specified in clause 5.2.2.3.x of 3GPP TS 29.502 [50]. The source I-SMF may return the old N3 UL F-TEID if it can be reused or a new N9 UL F-TEID assigned by the old UL CL/BP for UL traffic forwarding.

12. The target I-SMF shall update the UL FAR of the UL PDR(s) for UL data forwarding (to the old UL CL/BP) in new UL CL/BP with the F-TEID received.

13. Upon being notified about user plane inactivity of the N9 forwarding tunnel by the new UL CL/BP, the target I-SMF shall release the UL PDR(s) for UL data forwarding (to the old UL CL/BP) and the DL PDR(s) for DL data received (from the old UL CL/BP) in the new UL CL/BP.

14. Upon being notified about user plane inactivity of the N9 forwarding tunnel by the old UL CL/BP, the source I-SMF indicates to the SMF that it is removing the old UL CL/BP and PSA0.

15. The SMF shall send to the source I-SMF a PFCP Session Deletion Request (for the old DNAI) and a PFCP Session Deletion Request for the old UL CL/BP.

16-17. The source I-SMF shall remove the PFCP sessions in old UL CL/BP/PSA0.

18. The source I-SMF returns two PFCP Session Deletion Responses to the SMF.

# Annex E (Informative): Procedures Related to MPTCP Functionality

## E.1 General

This clause provides example MPTCP flows.

This Annex is informative and the normative descriptions in this specification and in 3GPP TS 23.501 [28], 3GPP TS 23.502 [29] and in 3GPP TS 24.193 [59], prevail over the descriptions in this Annex if there is any difference.

## E.2 Multipath TCP Connection Setup

### E.2.1 General

Multipath TCP Connection is setup between the MPTCP Client in the UE and the MPTCP Proxy in the UPF (PSA). The outgoing Multipath is initiated by the MPTCP Client in the UE towards the MPTCP Proxy in the UPF.

NOTE: The incoming Multipath which is assumed to be initiated by the MPTCP Proxy in the UPF towards the MPTCP Client in the UE is not supported in this release of the specification.

The RTT TCP Convert Protocol (specified in IETF RFC 8803 [60]) is used to setup Multipath TCP connection and used for data exchange. The MPTCP Proxy implements the Transport Converter functionality.

### E.2.2 Outgoing Multipath TCP Connection Setup

Figure E.2.2-1 describes the establishment of an outgoing multipath TCP connection through a Transport Converter.

The MPTCP Client initiates a Multipath TCP connection towards the Transport Converter, by sending a SYN with the MP_CAPABLE option (MPC in Figure E.2.2-1). The SYN includes the address and port number of the Server (i.e. remote host), that are extracted by the Transport Converter and used to initiate a Multipath TCP connection towards this Server. As the Server does not support Multipath TCP, it replies with a SYN+ACK that does not contain the MP_CAPABLE option. The Transport Converter notes that the connection with the Server does not support Multipath TCP and returns the extended TCP header received from the Server to the Client.

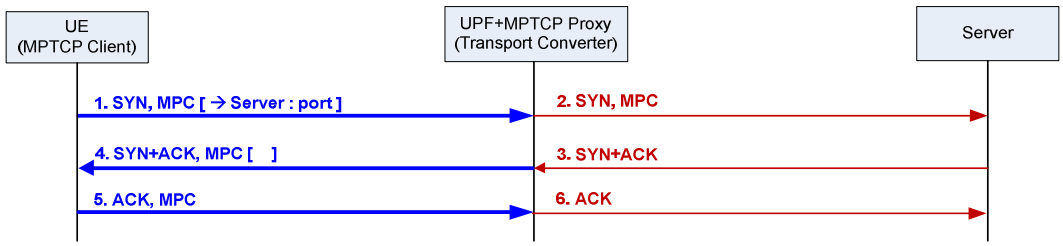



**Figure E.2.2-1 – Outgoing Converter-Assisted Multipath TCP Connection Setup**

### E.2.3 Incoming Multipath TCP Connection Setup

Incoming Multipath TCP Connection Setup as described in clause 5.2 of IETF RFC 8803 [60] is not supported in this release of the specification.

### E.2.4 MPTCP Session Entry Stored in MPTCP Proxy

Once Multipath TCP Connection is successfully setup between the MPTCP Client in the UE and the MPTCP Proxy in the UPF, the MPTCP Proxy stores the MPTCP session entry in its storage.

The MPTCP session entry includes the following information:

- UE link-specific multipath IP address and its TCP port;
- UE's MA-PDU session IP address and its TCP port, if the MA-PDU session IP address is used by MPTCP Proxy for IP translation;
- N6 routable IP address and its TCP port, if N6 routable IP address is used by the MPTCP Proxy for IP translation;
- the remote host IP address and its TCP port.

The stored MPTCP session entry is used by the MPTCP Proxy for IP translation when receiving uplink or downlink MPTCP traffic.

## E.3 IP Translation Procedure

### E.3.1 General

On receiving uplink or downlink MPTCP traffic, the UPF internally forwards the MPTCP traffic to the MPTCP Proxy. The MPTCP Proxy detects the MPTCP traffic is for data exchange, and performs IP translation before sending out the translated MPTCP traffic.

Figure E.3.1-1 illustrates the IP translation model for uplink and downlink MPTCP traffics, both on the UE side and the UPF side.

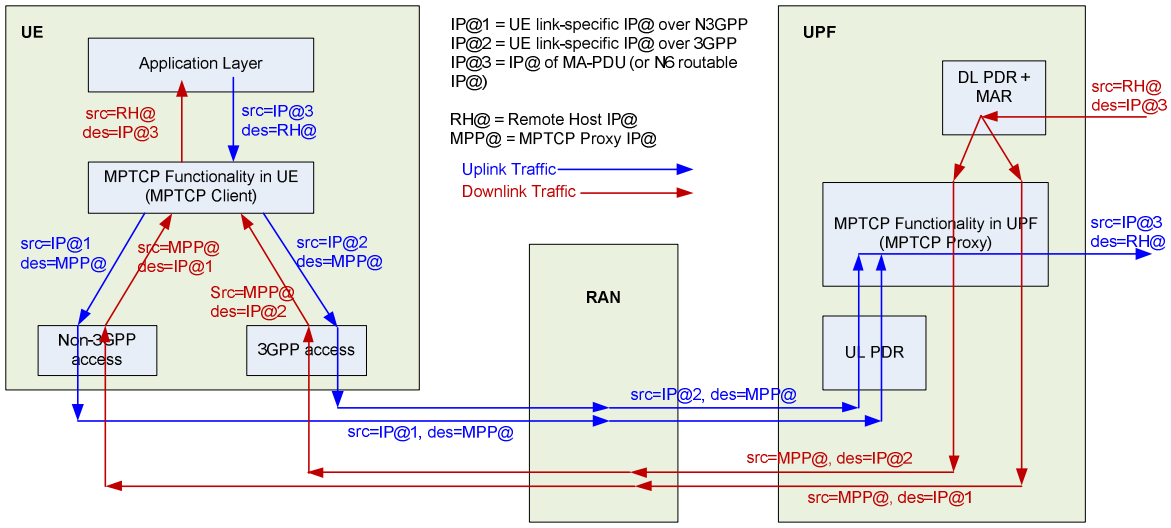



**Figure E.3.1-1 IP Translation Model**

When UE's MA-PDU session IP address is used by MPTCP Proxy for IP translation, port collision and port exhaustion can potentially occur because the UE also uses the MA-PDU session IP address for non-MPTCP traffic. To avoid this, an N6 routable IP address can be used by the MPTCP Proxy for IP translation, based on the UPF implementation.

## E.3.2 IP Translation on Uplink IP Packets

Once uplink MPTCP traffic is detected by the UPF, the UPF internally forwards the uplink IP packets to the MPTCP Proxy.

The MPTCP Proxy performs IP translation to the uplink IP packets, based on the stored MPTCP session entry:

- replace the source IP address and port, from the UE link-specific multipath IP@ and its port, to the UE's MA-PDU session IP@ and its port (or N6 routable IP@ and its port);
- replace the destination IP address and port, from the MPTCP Proxy IP@ and its port, to the remote host IP@ and its port.

After performing IP translation, the MPTCP Proxy forwards the translated uplink IP packets to N6 interface.

## E.3.3 IP Translation on Downlink IP Packets

Once downlink MPTCP traffic is detected by the UPF, the UPF internally forwards the downlink IP packets to the MPTCP Proxy.

The MPTCP Proxy performs IP translation to the downlink IP packets, based on the stored MPTCP session entry:

- replace the source IP address and port, from the remote host IP@ and its port, to the MPTCP Proxy IP@ and its port;
- replace the destination IP address and port, from the UE's MA-PDU session IP@ and its port (or N6 routable IP@ and its port), to the UE link-specific multipath IP@ and its port.

After performing IP translation, the MPTCP Proxy forwards the translated downlink IP packets to N3 or N9 interface.

# Annex F (Informative): Change history

| Date | TSG # | TSG Doc. | CR | Rev | Cat | Subject/Comment | New |
|---|---|---|---|---|---|---|---|
| 2016-07 | CT4#74 | C4-164286 | | | | First version after CT4#74 | 0.1.0 |
| 2016-10 | CT4#74 bis | C4-165318 | | | | Version after CT4#74bis | 0.2.0 |
| 2016-11 | CT4#75 | C4-166347 | | | | Version after CT4#75 | 0.3.0 |
| 2017-01 | CT4#75 bis | C4-170124 | | | | Version after CT4#75bis | 0.4.0 |
| 2017-02 | CT4#76 | C4-171423 | | | | Version after CT4#76 | 0.5.0 |
| 2017-03 | CT#75 | CP-170016 | | | | This version was sent for information | 1.0.0 |
| 2017-04 | C4#77 | C4-172285 | | | | Version after CT4#77 | 1.1.0 |
| 2017-05 | C4#78 | C4-173360 | | | | Version after CT4#78 | 1.2.0 |
| 2017-06 | CT#76 | CP-171047 | | | | This version was sent for approval | 2.0.0 |
| 2017-06 | CT#76 | CP-171183 | | | | Editorial correction | 2.0.1 |
| 2017-06 | CT#76 | CP-171183 | | | | Approved in CT#76 | 14.0.0 |
| 2017-09 | CT#77 | CP-172020 | 0001 | - | | PDN Instance over Sx | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0002 | 1 | | Transport Level Marking & DL Flow Level Marking | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0003 | 2 | | Clarifications and corrections to Usage Reporting | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0004 | - | | PDN Type over Sx | 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 | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0006 | 1 | | Message with a rejection cause | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0007 | - | | Corrections to the number of Fixed Octets | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0008 | 1 | | QER correlation ID | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0009 | 3 | | Sx Protocol extension to support Envelope Reporting | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0010 | 1 | | OCI Flags | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0011 | 2 | | IP Address(es) and TEIDs of a UP function | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0012 | 1 | | Clarification on bearer of a PDN connection and description on UP fucntion feature | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0013 | 2 | | Clarification on Rule IDs | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0014 | 1 | | Clarification on creating rules | 14.1.0 |
| 2017-09 | CT#77 | CP-172020 | 0018 | 2 | | URR and QER handling | 14.1.0 |
| 2017-12 | CT#78 | CP-173023 | 0026 | 4 | | Reporting User Plane Inactivity | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0027 | - | | Reporting of Usage Reports to the CP function | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0028 | - | | Suspend and Resume Notification procedures | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0029 | - | | Network Instance parameter | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0030 | 1 | | User Plane traffic handling upon reaching quotas based on operator policies | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0031 | - | | Reduced Application Detection Information for Envelope Reporting | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0034 | 3 | | Sx protocol extension to support Credit Pool | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0035 | - | | Clarification on the Setting of Precedence | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0036 | 1 | | Presence of UP F-SEID in Sx Session Establishment Response | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0042 | 1 | | Change the Title of the TS | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0043 | 1 | | Clarification on Create PDR and Create FAR IEs in Sx Session Establishment Request | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0047 | 1 | | Outer Header Creation | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0048 | 1 | | Clarification on presence of Activate Predefined Rule Name | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0056 | - | | Correction on Load Control Information IE Type value | 14.2.0 |
| 2017-12 | CT#78 | CP-173023 | 0058 | 2 | | Provisioning of Subsequent Time Quota and Subsequent Volume Quota | 14.2.0 |
| 2017-12 | CT#78 | CP-173027 | 0032 | | | Quota Action to apply upon reaching quotas | 15.0.0 |
| 2017-12 | CT#78 | CP-173036 | 0033 | 2 | | SGW/PGW selection for NR | 15.0.0 |
| 2017-12 | CT#78 | CP-173034 | 0037 | 2 | | Update of the TS to prepare it for 5GC/N4 | 15.0.0 |
| 2017-12 | CT#78 | CP-173034 | 0038 | 1 | | Update introdcution clause to 5GC | 15.0.0 |
| 2017-12 | CT#78 | CP-173034 | 0039 | 2 | | Update on general procedures for N4 | 15.0.0 |
| 2017-12 | CT#78 | CP-173034 | 0040 | 1 | | Node related Messages supported on N4 interface | 15.0.0 |
| 2017-12 | CT#78 | CP-173034 | 0041 | 1 | | User plane reporting | 15.0.0 |
| 2017-12 | CT#78 | CP-173034 | 0049 | 2 | | Session establishment on N4 | 15.0.0 |
| 2017-12 | CT#78 | CP-173034 | 0050 | 2 | | Session Modification on N4 | 15.0.0 |
| 2017-12 | CT#78 | CP-173034 | 0051 | 1 | | Session deletion on N4 | 15.0.0 |
| 2017-12 | CT#78 | CP-173034 | 0052 | 2 | | Session Reporting on N4 | 15.0.0 |
| 2017-12 | CT#78 | CP-173034 | 0053 | 2 | | Load-overload control on N4 | 15.0.0 |
| 2017-12 | CT#78 | CP-173034 | 0054 | 2 | | QOS enhancements on N4 for 5G | 15.0.0 |
| 2018-03 | CT#79 | CP-180018 | 0062 | 1 | | PDR with multiple SDFs | 15.1.0 |
| 2018-03 | CT#79 | CP-180018 | 0064 | 1 | | Bidirectional SDF Filters | 15.1.0 |
| 2018-03 | CT#79 | CP-180018 | 0066 | - | | Source and Destination Interface setting for Indirect Data Forwarding | 15.1.0 |
| 2018-03 | CT#79 | CP-180018 | 0068 | 2 | | Correlating additional usage reports with the query URR request | 15.1.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2018-03 | CT#79 | CP-180019 | 0071 | 5 | | PDI optimisation | 15.1.0 |
| 2018-03 | CT#79 | CP-180018 | 0078 | | | Corrections to the Association Setup, Update and Release Procedures | 15.1.0 |
| 2018-03 | CT#79 | CP-180018 | 0087 | 1 | | Error correction for Cause IE and Online-Charing Call Flow Alternative 2 example | 15.1.0 |
| 2018-03 | CT#79 | CP-180019 | 0075 | 1 | | Missing Feature Description on Transport Level Marking | 15.1.0 |
| 2018-03 | CT#79 | CP-180026 | 0055 | 6 | | Support of Ethernet frames on N4 | 15.1.0 |
| 2018-03 | CT#79 | CP-180026 | 0059 | 4 | | N4 alignment | 15.1.0 |
| 2018-03 | CT#79 | CP-180026 | 0060 | - | | Reporting User Plane Inactivity on N4 | 15.1.0 |
| 2018-03 | CT#79 | CP-180026 | 0079 | 1 | | Adding QFIs to the Packet Detection Information | 15.1.0 |
| 2018-03 | CT#79 | CP-180020 | 0069 | 1 | | Condition correction for SGW-U/PGW-U selection based on DCNR | 15.1.0 |
| 2018-03 | CT#79 | CP-180020 | 0076 | 2 | | Selection of SGW-C/PGW-C for Dual Connectivity with NR | 15.1.0 |
| 2018-06 | CT#80 | CP-181119 | 0093 | 2 | | Clarification of volume-based measurement report from UP to CP | 15.2.0 |
| 2018-06 | CT#80 | CP-181119 | 0095 | - | | Usage reports queried by the CP function | 15.2.0 |
| 2018-06 | CT#80 | CP-181119 | 0103 | 1 | | Linked URR | 15.2.0 |
| 2018-06 | CT#80 | CP-181119 | 0106 | 1 | | Duplicating the user plane packets to multiple destinations | 15.2.0 |
| 2018-06 | CT#80 | CP-181119 | 0108 | 2 | | The Source Interface in the User Plane IP Resource Information | 15.2.0 |
| 2018-06 | CT#80 | CP-181125 | 0097 | 2 | | Quota Action Buffering | 15.2.0 |
| 2018-06 | CT#80 | CP-181125 | 0100 | 1 | | Quota Action to apply upon reaching quotas | 15.2.0 |
| 2018-06 | CT#80 | CP-181125 | 0104 | 1 | | The report and update of a URR | 15.2.0 |
| 2018-06 | CT#80 | CP-181132 | 0089 | 1 | | User ID | 15.2.0 |
| 2018-06 | CT#80 | CP-181132 | 0090 | 1 | | PDN Type of ethernet | 15.2.0 |
| 2018-06 | CT#80 | CP-181132 | 0091 | 1 | | Update attributes in QER | 15.2.0 |
| 2018-06 | CT#80 | CP-181132 | 0101 | - | | Ethernet traffic | 15.2.0 |
| 2018-06 | CT#80 | CP-181132 | 0111 | 1 | | Resolve editor's notes | 15.2.0 |
| 2018-06 | CT#80 | CP-181132 | 0112 | 1 | | PDR for Ethernet PDU session | 15.2.0 |
| 2018-06 | CT#80 | CP-181132 | 0113 | 1 | | Reporting of UE MAC addresses to the SMF | 15.2.0 |
| 2018-09 | CT#81 | CP-182079 | 0118 | 2 | | Essential correction on UE IP address | 15.3.0 |
| 2018-09 | CT#81 | CP-182079 | 0120 | 1 | | Essential correction on Monitoring Time | 15.3.0 |
| 2018-09 | CT#81 | CP-182079 | 0122 | 1 | | Essential clarification on the CHOOSE bit in F-TEID IE | 15.3.0 |
| 2018-09 | CT#81 | CP-182079 | 0124 | 2 | | Essential correction on the Forward Policy | 15.3.0 |
| 2018-09 | CT#81 | CP-182079 | 0128 | 2 | | Usage Report Trigger IMMER | 15.3.0 |
| 2018-09 | CT#81 | CP-182079 | 0132 | 1 | | Essential clarification on the zero quota | 15.3.0 |
| 2018-09 | CT#81 | CP-182079 | 0134 | 1 | | Essential clarification on the provision of several SDF filters in a PDI | 15.3.0 |
| 2018-09 | CT#81 | CP-182079 | 0142 | 3 | | Event reporting | 15.3.0 |
| 2018-09 | CT#81 | CP-182079 | 0154 | 2 | | Application detection report when the PFDs are removed | 15.3.0 |
| 2018-09 | CT#81 | CP-182079 | 0158 | 1 | | Essential correction on reporting the usage | 15.3.0 |
| 2018-09 | CT#81 | CP-182079 | 0160 | 1 | | Essential clarification on the provision of SDF filter | 15.3.0 |
| 2018-09 | CT#81 | CP-182079 | 0162 | 2 | | Essential correction on the Dropped DL Traffic Threshold | 15.3.0 |
| 2018-09 | CT#81 | CP-182068 | 0136 | 1 | | Add support for 5G Trace | 15.3.0 |
| 2018-09 | CT#81 | CP-182084 | 0137 | - | | QFI in Downlink Data Report | 15.3.0 |
| 2018-09 | CT#81 | CP-182084 | 0138 | 1 | | User ID extensions | 15.3.0 |
| 2018-09 | CT#81 | CP-182084 | 0139 | 2 | | Framed Routing | 15.3.0 |
| 2018-09 | CT#81 | CP-182084 | 0143 | - | | 5GS restoration procedures | 15.3.0 |
| 2018-09 | CT#81 | CP-182084 | 0144 | 1 | | Uplink Classifier and Branching Point functionalities | 15.3.0 |
| 2018-09 | CT#81 | CP-182084 | 0145 | 1 | | Pause of charging. | 15.3.0 |
| 2018-09 | CT#81 | CP-182084 | 0146 | 2 | | Data forwarding | 15.3.0 |
| 2018-09 | CT#81 | CP-182084 | 0147 | 1 | | Sending of endmarker packets in 5GC | 15.3.0 |
| 2018-09 | CT#81 | CP-182084 | 0148 | 1 | | Predefined Rules PCC/ADC Rules | 15.3.0 |
| 2018-09 | CT#81 | CP-182084 | 0149 | 1 | | Downlink Data Notification Delay | 15.3.0 |
| 2018-09 | CT#81 | CP-182084 | 0150 | 1 | | Clarification on Editor's notes and cleanup of the specification. | 15.3.0 |
| 2018-09 | CT#81 | CP-182076 | 0152 | 3 | | Linked usage report | 15.3.0 |
| 2018-12 | CT#82 | CP-183103 | 0166 | 1 | | Clarification on UL/DL MBR | 15.4.0 |
| 2018-12 | CT#82 | CP-183103 | 0171 | 2 | | Forwarding End Marker | 15.4.0 |
| 2018-12 | CT#82 | CP-183103 | 0173 | 1 | | Reapplying Thresholds | 15.4.0 |
| 2018-12 | CT#82 | CP-183103 | 0175 | 1 | | Support of event based reporting for charging | 15.4.0 |
| 2018-12 | CT#82 | CP-183103 | 0177 | 1 | | Usage Report Sequence Number Starting Value | 15.4.0 |
| 2018-12 | CT#82 | CP-183103 | 0179 | 1 | | Transport Level Marking | 15.4.0 |
| 2018-12 | CT#82 | CP-183103 | 0181 | 2 | | Correction on the support of PGW Pause of Charging | 15.4.0 |
| 2018-12 | CT#82 | CP-183103 | 0183 | 1 | | Network Instance in relation to IP Address | 15.4.0 |
| 2018-12 | CT#82 | CP-183103 | 0185 | - | | Time of First (Last) Packet | 15.4.0 |
| 2018-12 | CT#82 | CP-183103 | 0187 | 1 | | Outer Header Removal for IPv4v6 GTP-U tunnel | 15.4.0 |
| 2018-12 | CT#82 | CP-183103 | 0203 | 1 | | Essential correction on the start point of time based measurement | 15.4.0 |
| 2018-12 | CT#82 | CP-183103 | 0205 | 2 | | FAR for HTTP Redirection | 15.4.0 |
| 2018-12 | CT#82 | CP-183092 | 0163 | 1 | | Cleanup and Alignment | 15.4.0 |
| 2018-12 | CT#82 | CP-183092 | 0169 | 6 | | VLAN Tag support in outer header creation | 15.4.0 |
| 2018-12 | CT#82 | CP-183092 | 0191 | 1 | | The VIDs handling in N4 aligned with 23.501 | 15.4.0 |
| 2018-12 | CT#82 | CP-183092 | 0193 | - | | QFI Correction | 15.4.0 |
| 2018-12 | CT#82 | CP-183092 | 0194 | 1 | | Clarification to ARP / IPv6 ND Proxying | 15.4.0 |
| 2018-12 | CT#82 | CP-183092 | 0195 | 6 | | Adding Averaging Window parameter on N4 | 15.4.0 |
| 2018-12 | CT#82 | CP-183092 | 0196 | 4 | | Adding 5G Session-AMBR | 15.4.0 |
| 2018-12 | CT#82 | CP-183092 | 0197 | 1 | | Paging Policy Differentiation in 5GC | 15.4.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2018-12 | CT#82 | CP-183092 | 0198 | 3 | | Clarification on forwarding user plane data via a shared Sx-u tunnel | 15.4.0 |
| 2018-12 | CT#82 | CP-183092 | 0199 | 1 | | 5G UPF Introduction | 15.4.0 |
| 2018-12 | CT#82 | CP-183092 | 0206 | 2 | | PFD Procedure | 15.4.0 |
| 2018-12 | CT#82 | CP-183092 | 0209 | 1 | | Traffic steering control with AF provided N6 traffic routing information | 15.4.0 |
| 2018-12 | CT#82 | CP-183092 | 0210 | 2 | | Data forwarding between 5GS and EPS | 15.4.0 |
| 2018-12 | CT#82 | CP-183099 | 0188 | - | | Corrections for wrong references | 15.4.0 |
| 2018-12 | CT#82 | CP-183099 | 0200 | 2 | | Interpretation of predefined Rules | 15.4.0 |
| 2019-03 | CT#83 | CP-190040 | 0215 | 1 | | Clarifications to CP/UP function, Node, PFCP entity and PFCP Association concepts | 15.5.0 |
| 2019-03 | CT#83 | CP-190032 | 0211 | 1 | | (Un)solicited Application Reporting | 15.5.0 |
| 2019-03 | CT#83 | CP-190032 | 0212 | 2 | | Policy and Charging Control | 15.5.0 |
| 2019-03 | CT#83 | CP-190032 | 0213 | 1 | | Legal Interception support for 5GC SMF/UPF | 15.5.0 |
| 2019-03 | CT#83 | CP-190032 | 0216 | 1 | | PFD Contents and Management | 15.5.0 |
| 2019-03 | CT#83 | CP-190032 | 222 | 1 | | Clarification on ARP Proxy | 15.5.0 |
| 2019-03 | CT#83 | CP-190032 | 0230 | 1 | | Inactivity timer for Always-on PDU session | 15.5.0 |
| 2019-03 | CT#83 | CP-190032 | 0231 | 1 | | SMF Derivation of DSCP on N4 | 15.5.0 |
| 2019-03 | CT#83 | CP-190039 | 0217 | 2 | | Clarification on the use of Graceful Release Period | 15.5.0 |
| 2019-03 | CT#83 | CP-190039 | 0219 | 2 | | PFCP Association Release Procedure | 15.5.0 |
| 2019-03 | CT#83 | CP-190039 | 0221 | 3 | | URR triggered packets dropping or redirection | 15.5.0 |
| 2019-03 | CT#83 | CP-190039 | 0232 | 1 | | IE Name Corrections | 15.5.0 |
| 2019-06 | CT#84 | CP-191021 | 0248 | 1 | | Correct the length of redirection server address | 15.6.0 |
| 2019-06 | CT#84 | CP-191021 | 0257 | - | | Correct the length of Multiplier | 15.6.0 |
| 2019-06 | CT#84 | CP-191024 | 0235 | 1 | | Release of F-TEID by the UP Function upon removal of PDR | 15.6.0 |
| 2019-06 | CT#84 | CP-191024 | 0242 | 1 | | Essential correction on report of user plane path failure | 15.6.0 |
| 2019-06 | CT#84 | CP-191024 | 0244 | 2 | | Parameters for Performance Measurement | 15.6.0 |
| 2019-06 | CT#84 | CP-191024 | 0243 | 3 | | Accurate Interface Type for Supporting Performance Measurement | 15.6.0 |
| 2019-06 | CT#84 | CP-191024 | 0245 | 3 | | Update the redirection server address to support dual stack UE | 15.6.0 |
| 2019-06 | CT#84 | CP-191024 | 0262 | 1 | | Framed-Route and Framed-IPv6-Route in a PDR | 15.6.0 |
| 2019-06 | CT#84 | CP-191024 | 0258 | 1 | | Corrections to the Recovery Time Stamp | 15.6.0 |
| 2019-06 | CT#84 | CP-191024 | 0251 | 1 | | Matching a PFD | 15.6.0 |
| 2019-06 | CT#84 | CP-191058 | 0233 | - | | Correction to Framed Routing | 15.6.0 |
| 2019-06 | CT#84 | CP-191058 | 0260 | - | | Reverting N4 requirements for Lawful Interception support in 5GC | 15.6.0 |
| 2019-06 | CT#84 | CP-191047 | 0240 | 1 | | Enhancement to the PFCP Association Release Procedure | 16.0.0 |
| 2019-06 | CT#84 | CP-191047 | 0241 | 2 | | Deferred PDR Activation and Deactivation | 16.0.0 |
| 2019-06 | CT#84 | CP-191047 | 0263 | 1 | | Activation and Deactivation of Pre-defined PDRs | 16.0.0 |
| 2019-06 | CT#84 | CP-191050 | 0247 | 1 | | User Plane Forwarding with Control Plane CIoT 5GS Optimisation | 16.0.0 |
| 2019-06 | CT#84 | CP-191051 | 0237 | 1 | | Support for ATSSS | 16.0.0 |
| 2019-06 | CT#84 | CP-191051 | 0236 | 1 | | Update on the Packet Forwarding Model | 16.0.0 |
| 2019-06 | CT#84 | CP-191051 | 0238 | 2 | | Multi-Access Action Rule | 16.0.0 |
| 2019-06 | CT#84 | CP-191054 | 0259 | 1 | | UE IP addresses/prefixes allocation by UPF | 16.0.0 |
| 2019-06 | CT#84 | CP-191054 | 0252 | 3 | | Update the PFCP association setup to support UE IP address Allocation by AAA/DHCP | 16.0.0 |
| 2019-06 | CT#84 | CP-191055 | 0261 | 1 | | PFCP sessions successively controlled by different SMFs of a same SMF set | 16.0.0 |
| 2019-06 | CT#84 | CP-191056 | 0253 | 2 | | Update description of 5G UPF with redundant transmission | 16.0.0 |
| 2019-09 | CT#85 | CP-192129 | 0293 | 1 | | Editorial and style corrections | 16.1.0 |
| 2019-09 | CT#85 | CP-192129 | 0267 | - | | Application report when the PFDs are removed or modified | 16.1.0 |
| 2019-09 | CT#85 | CP-192129 | 0273 | 1 | | Measurement Before QoS Enforcement Clarification | 16.1.0 |
| 2019-09 | CT#85 | CP-192129 | 0274 | 1 | | Number of packets | 16.1.0 |
| 2019-09 | CT#85 | CP-192129 | 0278 | 1 | | F-TEID in a PDR | 16.1.0 |
| 2019-09 | CT#85 | CP-192129 | 0282 | - | | Clarification to C-Tag and S-Tag encoding | 16.1.0 |
| 2019-09 | CT#85 | CP-192129 | 0285 | 1 | | PFCP messages bundling | 16.1.0 |
| 2019-09 | CT#85 | CP-192096 | 0280 | - | | Essential Correction on Heartbeat procedure | 16.1.0 |
| 2019-09 | CT#85 | CP-192133 | 0271 | 1 | | Support 5G VN Group Communication – unicast traffic | 16.1.0 |
| 2019-09 | CT#85 | CP-192133 | 0272 | 1 | | Support 5G VN Group Communication – broadcast traffic | 16.1.0 |
| 2019-09 | CT#85 | CP-192133 | 0283 | 1 | | 3GPP Interface Type values | 16.1.0 |
| 2019-09 | CT#85 | CP-192194 | 0270 | 3 | | PFCP sessions controlled by different SMFs in a set | 16.1.0 |
| 2019-09 | CT#85 | CP-192194 | 0294 | - | | Support of SMF set and association establishement between SMF and UPF initiated by the UPF. | 16.1.0 |
| 2019-09 | CT#85 | CP-192193 | 0265 | 3 | | Enhancing UE IP address Pool Identity IE type | 16.1.0 |
| 2019-09 | CT#85 | CP-192193 | 0266 | 2 | | PFCP usage over N16a for the support of traffic offload by UPF controlled by I-SMF | 16.1.0 |
| 2019-09 | CT#85 | CP-192126 | 0281 | 1 | | Protocol support for Ethernet PDN in EPS | 16.1.0 |
| 2019-09 | CT#85 | CP-192187 | 0287 | 2 | | Supporting redundant transmission at transport layer Negotiation | 16.1.0 |
| 2019-09 | CT#85 | CP-192187 | 0269 | 3 | | Validity time in Create URR IE | 16.1.0 |
| 2019-12 | CT#86 | CP-193023 | 0398 | 1 | | Correct Terminology of Sx Session to PFCP Session | 16.2.0 |
| 2019-12 | CT#86 | CP-193041 | 0318 | 3 | | Correction to number of fixed octets in table 8.1.2 | 16.2.0 |
| 2019-12 | CT#86 | CP-193045 | 0277 | 3 | | Controlling of number of reports | 16.2.0 |
| 2019-12 | CT#86 | CP-193045 | 0295 | 1 | | Clarification to Create PDR/FAR/URR/QER/BAR/MAR IEs in a modification message | 16.2.0 |
| 2019-12 | CT#86 | CP-193045 | 0302 | 1 | | PFCP Association Setup Request with same Node ID | 16.2.0 |
| 2019-12 | CT#86 | CP-193045 | 0315 | 2 | | Null Usage Report | 16.2.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2019-12 | CT#86 | CP-193045 | 0317 | 3 | | Clarifications to Vendor-specific IE handling | 16.2.0 |
| 2019-12 | CT#86 | CP-193045 | 0329 | 2 | | Reestablishment of PFCP sessions after a UP function restart | 16.2.0 |
| 2019-12 | CT#86 | CP-193045 | 0335 | 1 | | Cause No established PFCP Association | 16.2.0 |
| 2019-12 | CT#86 | CP-193045 | 0340 | 1 | | User Plane Path Recovery Report | 16.2.0 |
| 2019-12 | CT#86 | CP-193045 | 0341 | 1 | | UE IP address allocation | 16.2.0 |
| 2019-12 | CT#86 | CP-193045 | 0342 | 4 | | Additional PFCP Session Report Request | 16.2.0 |
| 2019-12 | CT#86 | CP-193045 | 0349 | 1 | | Reporting PDR ID in a Usage Report | 16.2.0 |
| 2019-12 | CT#86 | CP-193046 | 0310 | 2 | | Support of IPTV service | 16.2.0 |
| 2019-12 | CT#86 | CP-193046 | 0327 | 1 | | IPv6 address allocation and IPv6 prefix delegation for RG connecting to 5GC | 16.2.0 |
| 2019-12 | CT#86 | CP-193049 | 0288 | 7 | | Small Data Rate Control Parameters | 16.2.0 |
| 2019-12 | CT#86 | CP-193050 | 0309 | 2 | | 5GS Bridge information reporting for Time Sensitive Communication | 16.2.0 |
| 2019-12 | CT#86 | CP-193050 | 0314 | 1 | | Network Instance representing the 5G VN group | 16.2.0 |
| 2019-12 | CT#86 | CP-193050 | 0316 | 1 | | Transfer of TSN bridge port management information | 16.2.0 |
| 2019-12 | CT#86 | CP-193050 | 0347 | 2 | | Reporting the clock drift between TSN and 5GS times | 16.2.0 |
| 2019-12 | CT#86 | CP-193051 | 0298 | 1 | | General description of ATSSS and Multi-Access Rule | 16.2.0 |
| 2019-12 | CT#86 | CP-193051 | 0300 | 4 | | Handling of GBR traffic of a MA PDU session | 16.2.0 |
| 2019-12 | CT#86 | CP-193051 | 0322 | 2 | | Session Reporting Rule | 16.2.0 |
| 2019-12 | CT#86 | CP-193051 | 0301 | 1 | | Access type of a MA PDU session becoming (un)available | 16.2.0 |
| 2019-12 | CT#86 | CP-193051 | 0304 | 4 | | ATSSS Funtionality Required and ATSSS Control Parameters Returned | 16.2.0 |
| 2019-12 | CT#86 | CP-193051 | 0325 | 3 | | Clarifications to ATSSS feature | 16.2.0 |
| 2019-12 | CT#86 | CP-193056 | 0297 | 1 | | UL FAR in UL CL or BP towards Local PSA | 16.2.0 |
| 2019-12 | CT#86 | CP-193056 | 0306 | 2 | | Clarification on N4 Rules Exchanged via N16a Interface | 16.2.0 |
| 2019-12 | CT#86 | CP-193056 | 0330 | 1 | | UE IP Address Pool ID in PFCP Association Procedure | 16.2.0 |
| 2019-12 | CT#86 | CP-193056 | 0331 | 1 | | UE IP address Pool Identity | 16.2.0 |
| 2019-12 | CT#86 | CP-193057 | 0296 | 2 | | PFCP sessions successively controlled by different SMFs of an SMF set | 16.2.0 |
| 2019-12 | CT#86 | CP-193060 | 0312 | 4 | | Function description for URLLC | 16.2.0 |
| 2019-12 | CT#86 | CP-193060 | 0326 | 1 | | GTP-U Path QoS Monitoring | 16.2.0 |
| 2019-12 | CT#86 | CP-193060 | 0346 | 2 | | Per QoS Flow per UE QoS Monitoring | 16.2.0 |
| 2020-03 | CT#87e | CP-200035 | 0350 | 2 | | IETF reference update for IPv6 multicast | 16.3.0 |
| 2020-03 | CT#87e | CP-200033 | 0352 | 1 | | Support of MT-EDT | 16.3.0 |
| 2020-03 | CT#87e | CP-200033 | 0385 | 2 | | MO Exception Data Indication | 16.3.0 |
| 2020-03 | CT#87e | CP-200033 | 0386 | 2 | | Packet Rate Status Reporting and Control | 16.3.0 |
| 2020-03 | CT#87e | CP-200016 | 0354 | 1 | | Provision alternative SMF IP addresses of PFCP entities pertaining to the same SMF | 16.3.0 |
| 2020-03 | CT#87e | CP-200017 | 0355 | 1 | | Transferring N4 messages over N16a | 16.3.0 |
| 2020-03 | CT#87e | CP-200017 | 0388 | - | | Clarification to N4 information | 16.3.0 |
| 2020-03 | CT#87e | CP-200038 | 0357 | 4 | | Removing a URR | 16.3.0 |
| 2020-03 | CT#87e | CP-200038 | 0358 | 2 | | UPF ID | 16.3.0 |
| 2020-03 | CT#87e | CP-200038 | 0359 | 1 | | 3GPP Interface Type | 16.3.0 |
| 2020-03 | CT#87e | CP-200038 | 0360 | 2 | | Miscellaneous small corrections | 16.3.0 |
| 2020-03 | CT#87e | CP-200038 | 0361 | 1 | | The Source IP Address in Heartbeat Request message | 16.3.0 |
| 2020-03 | CT#87e | CP-200038 | 0362 | 2 | | UP function Initiated PFCP Association Release at timeout | 16.3.0 |
| 2020-03 | CT#87e | CP-200038 | 0363 | 1 | | UP function initiated PFCP session release | 16.3.0 |
| 2020-03 | CT#87e | CP-200038 | 0366 | 1 | | The Recovery Time Stamp in PFCP Session Establishment Request message | 16.3.0 |
| 2020-03 | CT#87e | CP-200038 | 0374 | 2 | | F-TEID allocation | 16.3.0 |
| 2020-03 | CT#87e | CP-200038 | 0376 | 2 | | Reflective QoS | 16.3.0 |
| 2020-03 | CT#87e | CP-200038 | 0384 | 1 | | SDF Handling when waiting for credit | 16.3.0 |
| 2020-03 | CT#87e | CP-200023 | 0364 | - | | Ethernet PDU Session Anchor Relocation | 16.3.0 |
| 2020-03 | CT#87e | CP-200023 | 0375 | 2 | | Support of Redundant Transmission | 16.3.0 |
| 2020-03 | CT#87e | CP-200031 | 0367 | 2 | | Steering Mode Value | 16.3.0 |
| 2020-03 | CT#87e | CP-200031 | 0368 | - | | Port Type of MPTCP Proxy and PMF | 16.3.0 |
| 2020-03 | CT#87e | CP-200031 | 0369 | 1 | | Apply ATSSS-LL together with MPTCP | 16.3.0 |
| 2020-03 | CT#87e | CP-200031 | 0370 | 2 | | More Description for MPTCP Functionality | 16.3.0 |
| 2020-03 | CT#87e | CP-200031 | 0381 | 1 | | Signalling to the UPF that an access of a MA PDU session is unavailable | 16.3.0 |
| 2020-03 | CT#87e | CP-200032 | 0379 | 1 | | Update of 5G VN Group Communication | 16.3.0 |
| 2020-03 | CT#87e | CP-200032 | 0380 | 1 | | TSN Domain and Time Domain | 16.3.0 |
| 2020-03 | CT#87e | CP-200032 | 0382 | 1 | | 5GS Bridge information reporting cleanup for Time Sensitive Communication | 16.3.0 |
| 2020-04 | CT#87e | | | | | Clause 5.24.3 was deleted by mistake during implementation after CT#87e | 16.3.1 |
| 2020-06 | CT#88e | CP-201029 | 0415 | 1 | | Restoring deleted statement | 16.4.0 |
| 2020-06 | CT#88e | CP-201029 | 0441 | 1 | | DL Data Notification for the subsequent DL data pertaining to a different QoS flow | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0356 | 1 | | Activating a predefined FAR/URR/QER | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0390 | - | | Miscellaneous small correction on Figures | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0395 | 1 | | New S-NSSAI IE | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0396 | - | | Inconsistent description for the use of Activation/Deactivation time | 16.4.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2020-06 | CT#88e | CP-201051 | 0397 | - | | F-TEID allocation cleanup | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0398 | - | | Encoding of the Remote GTP-U Peer IE | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0403 | - | | UE IP address allocation | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0404 | 1 | | UE IP address pool based on S-NSSAI | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0406 | 1 | | Report Trigger for Quota Validity Time Expiry | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0411 | 1 | | Clarification on Partial Failure of UP Function | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0413 | 2 | | Node level vs PFCP entity level procedures | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0417 | 2 | | Heartbeat procedure clarification | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0418 | 2 | | Alternative IP Address in SSET | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0419 | 2 | | Clarification when Node ID is set to an IP address | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0420 | 2 | | Association Update Response for EPFAR | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0422 | 1 | | UP function features description update | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0427 | 3 | | Downlink data reordering - new feature definition | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0438 | 2 | | UE IP address pool based on IP version | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0444 | 1 | | Remaining Quota in the UP function | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0445 | 1 | | Adjust Threshold/Quota after a usage report in the UP function | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0446 | 2 | | Quota Reporting Trigger Clarification | 16.4.0 |
| 2020-06 | CT#88e | CP-201051 | 0449 | 1 | | Editorial corrections | 16.4.0 |
| 2020-06 | CT#88e | CP-201050 | 0389 | 1 | | Support of IPUPS Functionality | 16.4.0 |
| 2020-06 | CT#88e | CP-201046 | 0391 | 3 | | First discarded downlink packet notification | 16.4.0 |
| 2020-06 | CT#88e | CP-201046 | 0392 | 2 | | Add RDS configuration information | 16.4.0 |
| 2020-06 | CT#88e | CP-201046 | 0394 | 2 | | Data rate control during mobility between 5GS and EPS | 16.4.0 |
| 2020-06 | CT#88e | CP-201046 | 0414 | 1 | | Aligning "MO Exception data" handling with stage 2 - UPF | 16.4.0 |
| 2020-06 | CT#88e | CP-201044 | 0393 | 1 | | MPTCP Indication for a Uplink PDR for traffic applicable for MPTCP | 16.4.0 |
| 2020-06 | CT#88e | CP-201044 | 0408 | 1 | | Packet Forwarding Model for MPTCP | 16.4.0 |
| 2020-06 | CT#88e | CP-201044 | 0423 | 1 | | Update IETF References for MPTCP | 16.4.0 |
| 2020-06 | CT#88e | CP-201044 | 0425 | 1 | | PMFP Message Handling | 16.4.0 |
| 2020-06 | CT#88e | CP-201044 | 0426 | 1 | | N6 Routable IP address | 16.4.0 |
| 2020-06 | CT#88e | CP-201044 | 0434 | 1 | | DL PDRs of a MA PDU session | 16.4.0 |
| 2020-06 | CT#88e | CP-201044 | 0435 | 1 | | PMF control information to enable/disable PMF RTT measurements | 16.4.0 |
| 2020-06 | CT#88e | CP-201037 | 0400 | 1 | | Redundant Transmission on transport layer | 16.4.0 |
| 2020-06 | CT#88e | CP-201045 | 0401 | 1 | | Clarification for TSN NW-TT port number | 16.4.0 |
| 2020-06 | CT#88e | CP-201045 | 0402 | 2 | | Support of QoS differentiation for NPN | 16.4.0 |
| 2020-06 | CT#88e | CP-201045 | 0436 | 1 | | 5GS Bridge ID clarification | 16.4.0 |
| 2020-06 | CT#88e | CP-201045 | 0437 | 1 | | 5GS Bridge and port information separation for Time Sensitive Communication | 16.4.0 |
| 2020-06 | CT#88e | CP-201031 | 0433 | 1 | | N4 information exchanged over N16a during PDU session release | 16.4.0 |
| 2020-06 | CT#88e | CP-201068 | 0412 | 1 | | Inter-system handover with direct data forwarding | 16.4.0 |
| 2020-06 | CT#88e | CP-201070 | 0447 | 1 | | Data Forwarding Info | 16.4.0 |
| 2020-09 | CT#89e | CP-202114 | 0466 | 2 | | Interworking between ETSUN and URLLC/TSC | 16.5.0 |
| 2020-09 | CT#89e | CP-202114 | 0475 | 1 | | End marker handling in service request procedure | 16.5.0 |
| 2020-09 | CT#89e | CP-202114 | 0482 | - | | Correcting the example of addition of PSA2 and UL CL controlled by I-SMF | 16.5.0 |
| 2020-09 | CT#89e | CP-202102 | 0471 | 3 | | Reporting UE IP Address Usage | 16.5.0 |
| 2020-09 | CT#89e | CP-202102 | 0479 | - | | Interface Type of Traffic Endpoint | 16.5.0 |
| 2020-09 | CT#89e | CP-202102 | 0484 | 2 | | SMF-Set ID in PFCP Association Messages | 16.5.0 |
| 2020-09 | CT#89e | CP-202107 | 0472 | 2 | | Correct IE Type of Redundant Transmission Parameters | 16.5.0 |
| 2020-09 | CT#89e | CP-202107 | 0473 | 1 | | Time Stamp in QoS Monitoring Report IE | 16.5.0 |
| 2020-09 | CT#89e | CP-202105 | 0474 | 1 | | Small data rate control and Serving PLMN rate control | 16.5.0 |
| 2020-09 | CT#89e | CP-202106 | 0477 | 1 | | Editor's Note on TSN Bridge Name | 16.5.0 |
| 2020-09 | CT#89e | CP-202106 | 0478 | 1 | | Editor's Note on TSN NW-TT Port relation to PDU session | 16.5.0 |
| 2020-09 | CT#89e | CP-202103 | 0480 | 1 | | IPv6 Prefix Delegation via DHCPv6 | 16.5.0 |
| 2020-12 | CT#90e | CP-203038 | 0492 | - | | Message Priority encoding | 16.6.0 |
| 2020-12 | CT#90e | CP-203038 | 0494 | 1 | | Essential clarification on the Additional Usage Reports | 16.6.0 |
| 2020-12 | CT#90e | CP-203038 | 0496 | 2 | | Essential clarification on the Framed-Route | 16.6.0 |
| 2020-12 | CT#90e | CP-203038 | 0497 | 1 | | IPv6 Prefix delegation when the UP function allocating UE IP Address | 16.6.0 |
| 2020-12 | CT#90e | CP-203038 | 0499 | 1 | | Implicitly allowing packets be forwarded via provisioning a non-zero quota | 16.6.0 |
| 2020-12 | CT#90e | CP-203038 | 0500 | 1 | | Miscellaneous corrections | 16.6.0 |
| 2020-12 | CT#90e | CP-203041 | 0501 | 2 | | Notify the discarded downlink packet | 16.6.0 |
| 2020-12 | CT#90e | CP-203042 | 0490 | - | | PFCP session used to send PMIC and BMIC | 16.6.0 |
| 2020-12 | CT#90e | CP-203042 | 0491 | | | Removing NW-TT Port Number from Created Bridge Info for TSC IE | 16.6.0 |
| 2020-12 | CT#90e | CP-203043 | 0485 | 1 | | Replace reference draft-ietf-tcpm-converters-19 by reference to RFC 8803 | 16.6.0 |
| 2020-12 | CT#90e | CP-203043 | 0489 | 1 | | Incorrect IE type values | 16.6.0 |
| 2020-12 | CT#90e | CP-203043 | 0498 | 1 | | Procedures Related to MPTCP Functionality | 16.6.0 |
| 2020-12 | CT#90e | CP-203046 | 0487 | - | | GTP-U path interface type IE in GTP-U Path QoS Report | 16.6.0 |
| 2020-12 | CT#90e | CP-203046 | 0488 | 3 | | QoS monitoring of a PDU session based on GTP-U path monitoring | 16.6.0 |
| 2020-12 | CT#90e | CP-203051 | 0495 | 1 | | End Marker Reception Reporting Corrections | 16.6.0 |
| 2021-03 | CT#91e | CP-210045 | 0504 | 3 | | Stop of QoS Monitoring | 16.7.0 |
| 2021-03 | CT#91e | CP-210045 | 0508 | 2 | | Usage Reporting when using Redundant Transmission on N3/N9 interfaces | 16.7.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2021-03 | CT#91e | CP-210051 | 0509 | 1 | | Distinguishing FQ-CSIDs in PFCP messages | 16.7.0 |
| 2021-03 | CT#91e | CP-210051 | 0511 | 2 | | Essential correction on the use of the Updated PDR | 16.7.0 |
| 2021-03 | CT#91e | CP-210051 | 0512 | 1 | | Clarification on the deletion of several IEs with the same IE Type | 16.7.0 |
| 2021-03 | CT#91e | CP-210051 | 0514 | 1 | | Clarification on the FAR ID for Quota Action | 16.7.0 |
| 2021-03 | CT#91e | CP-210051 | 0515 | 1 | | Adding MAR and SRR in Failed Rule ID | 16.7.0 |
| 2021-03 | CT#91e | CP-210051 | 0518 | 2 | | Clarification on the update for a bitmap style IE | 16.7.0 |
| 2021-03 | CT#91e | CP-210051 | 0525 | 1 | | N9 forwarding tunnel removal | 16.7.0 |
| 2021-03 | CT#91e | CP-210051 | 0526 | 1 | | UE IP address / prefix Allocation | 16.7.0 |
| 2021-03 | CT#91e | CP-210051 | 0527 | 2 | | Interface Type | 16.7.0 |
| 2021-03 | CT#91e | CP-210037 | 0517 | 1 | | Essential correction on the use of null SEID | 16.7.0 |
| 2021-03 | CT#91e | CP-210049 | 0520 | 1 | | SNSSAI Update in PFCP Session Modification | 16.7.0 |
| 2021-03 | CT#91e | CP-210022 | 0506 | 1 | | Implementation of conclusions agreed for KI#3 of TR 29.820 | 17.0.0 |
| 2021-03 | CT#91e | CP-210032 | 0507 | - | | Rule activation failure | 17.0.0 |
| 2021-03 | CT#91e | CP-210032 | 0513 | 1 | | Editorial Correction | 17.0.0 |
| 2021-03 | CT#91e | CP-210032 | 0516 | 1 | | Filter ID | 17.0.0 |
| 2021-03 | CT#91e | CP-210032 | 0519 | 2 | | Addition of RAT Type IE on PFCP Interface | 17.0.0 |
| 2021-03 | CT#91e | CP-210032 | 0528 | 1 | | Support of Radius, Diameter or DHCP communication via UPF | 17.0.0 |
| 2021-03 | CT#91e | CP-210033 | 0510 | 2 | | Enhancement on the support of Pause of Charging | 17.0.0 |
| 2021-03 | CT#91e | CP-210030 | 0521 | 1 | | Partial failure handling support over N4 | 17.0.0 |
| 2021-06 | CT#92e | CP-211070 | 0543 | 1 | | Essential Clarification on PDR Provisioning and 2-Steps Packet Matching | 17.1.0 |
| 2021-06 | CT#92e | CP-211025 | 0545 | 3 | | Control of Start and Stop Usage Measurement for a PFCP session | 17.1.0 |
| 2021-06 | CT#92e | CP-211029 | 0554 | 2 | | Support of L2TP | 17.1.0 |
| 2021-06 | CT#92e | CP-211031 | 0535 | 2 | | UL packet buffering during EAS relocation | 17.1.0 |
| 2021-06 | CT#92e | CP-211033 | 0536 | 4 | | Support of thresholds in ATSSS | 17.1.0 |
| 2021-06 | CT#92e | CP-211033 | 0537 | 4 | | Steering Mode Indicator | 17.1.0 |
| 2021-06 | CT#92e | CP-211033 | 0540 | 1 | | Support of MA PDU with 3GPP access connected to EPC and Non-3GPP access connected to 5GC | 17.1.0 |
| 2021-06 | CT#92e | CP-211033 | 0551 | 1 | | Per QoS Flow Performance Measurement | 17.1.0 |
| 2021-06 | CT#92e | CP-211035 | 0529 | - | | Generalization Time Sensitive Communication to other than IEEE TSN | 17.1.0 |
| 2021-06 | CT#92e | CP-211035 | 0530 | - | | External time and Time domain terms | 17.1.0 |
| 2021-06 | CT#92e | CP-211035 | 0548 | 1 | | Terminology of the Time Sensitive Communication MIC and Bridge ID | 17.1.0 |
| 2021-06 | CT#92e | CP-211035 | 0549 | 1 | | UE-UE communication for TSC | 17.1.0 |
| 2021-06 | CT#92e | CP-211042 | 0546 | - | | Editorial Corrections | 17.1.0 |
| 2021-06 | CT#92e | CP-211042 | 0547 | - | | Correction to interface type value | 17.1.0 |
| 2021-06 | CT#92e | CP-211043 | 0544 | 2 | | PFCP Session Set Modification to restore PFCP Sessions | 17.1.0 |
| 2021-06 | CT#92e | CP-211046 | 0539 | 1 | | Simultaneous change of Branching Point or UL CL and additional PSA | 17.1.0 |
| 2021-06 | CT#92e | CP-211059 | 0532 | 1 | | SMF and UPF behaviour in SSET / MAPS cases | 17.1.0 |
| 2021-09 | CT#93e | CP-212068 | 0575 | 1 | A | IEEE 802.1AS-2020 reference update | 17.2.0 |
| 2021-09 | CT#93e | CP-212027 | 0556 | 1 | F | Correction on references | 17.2.0 |
| 2021-09 | CT#93e | CP-212027 | 0561 | 1 | B | L2TP Corrections | 17.2.0 |
| 2021-09 | CT#93e | CP-212027 | 0562 | 1 | B | LNS Address | 17.2.0 |
| 2021-09 | CT#93e | CP-212038 | 0557 | 1 | B | PMF address information per QoS flow | 17.2.0 |
| 2021-09 | CT#93e | CP-212038 | 0563 | 2 | B | Handling of PMF Message with UE Assistance Data | 17.2.0 |
| 2021-09 | CT#93e | CP-212031 | 0564 | - | B | Edge Relocation using EAS IP address Replacement | 17.2.0 |
| 2021-09 | CT#93e | CP-212031 | 0565 | 1 | B | EAS Discovery procedure with Local DNS Server/Resolver | 17.2.0 |
| 2021-09 | CT#93e | CP-212031 | 0566 | - | B | Direct Reporting of QoS monitoring events to Local NEF or AF | 17.2.0 |
| 2021-09 | CT#93e | CP-212044 | 0558 | - | F | 5GS User Plane Node | 17.2.0 |
| 2021-09 | CT#93e | CP-212044 | 0569 | 1 | B | SNSSAI Update after EPS to 5GS Handover | 17.2.0 |
| 2021-09 | CT#93e | CP-212044 | 0570 | 1 | F | Partial Failure Information | 17.2.0 |
| 2021-09 | CT#93e | CP-212044 | 0571 | 1 | B | Add SUPI, GPSI, and PEI to User ID | 17.2.0 |
| 2021-09 | CT#93e | CP-212044 | 0572 | 1 | F | Predefined Rule Name | 17.2.0 |
| 2021-09 | CT#93e | CP-212035 | 0559 | 1 | B | Protocol impact on N4mb for 5G MBS | 17.2.0 |
| 2021-09 | CT#93e | CP-212040 | 0573 | 1 | B | Introduction of TSCTSF and other stage2 and 3 alignments | 17.2.0 |
| 2021-09 | CT#93e | | | | | Editorial corrections | 17.2.1 |
| 2021-12 | CT#94e | CP-213097 | 0560 | 2 | B | Protocol impact on N4 for 5G MBS | 17.3.0 |
| 2021-12 | CT#94e | CP-213097 | 0587 | 1 | F | 5MBS corrections | 17.3.0 |
| 2021-12 | CT#94e | CP-213093 | 0578 | 1 | F | Reference to UPF service specification | 17.3.0 |
| 2021-12 | CT#94e | CP-213099 | 0579 | 2 | B | Enabling and disabling the adjustment of DL traffic steering rules | 17.3.0 |
| 2021-12 | CT#94e | CP-213099 | 0580 | 1 | B | UPF behaviour of setting source and destination addresses of PMF message | 17.3.0 |
| 2021-12 | CT#94e | CP-213099 | 0581 | 1 | B | Condition of Inclusion of Threshold Values IE and Steering Mode Indicator IE | 17.3.0 |
| 2021-12 | CT#94e | CP-213090 | 0582 | 2 | B | Per Slice UP Resource Allocatoin and Usage Report | 17.3.0 |
| 2021-12 | CT#94e | CP-213090 | 0583 | 2 | B | Per Slice UE IP Address Usage Report | 17.3.0 |
| 2021-12 | CT#94e | CP-213090 | 0584 | 2 | B | Adding S-NSSAI as a factor in managing UPF resources | 17.3.0 |
| 2021-12 | CT#94e | CP-213101 | 0585 | - | F | Updates for Bridge/User plane Node ID configuration | 17.3.0 |
| 2021-12 | CT#94e | CP-213089 | 0589 | 1 | F | Outer Header Removal | 17.3.0 |
| 2021-12 | CT#94e | CP-213129 | 0590 | 1 | F | Usage Reporting for Monitoring Time | 17.3.0 |
| 2021-12 | CT#94e | CP-213125 | 0591 | - | F | Traffic usage reporting on Redundant Transmission at transport layer | 17.3.0 |
| 2022-03 | CT#95e | CP-220027 | 0599 | 1 | B | UE IP allocation in CP function with SSET and MPAS | 17.4.0 |
| 2022-03 | CT#95e | CP-220027 | 0602 | 2 | F | Missing Definition for Tunnel Password IE | 17.4.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2022-03 | CT#95e | CP-220031 | 0610 | - | B | IP Address and Port number Replacement IE in EAS Discovery procedure with Local DNS Server/Resolver | 17.4.0 |
| 2022-03 | CT#95e | CP-220035 | 0592 | 1 | F | Clarification to the MBS Session N4 Information | 17.4.0 |
| 2022-03 | CT#95e | CP-220035 | 0595 | 1 | F | Associated QoS Flow | 17.4.0 |
| 2022-03 | CT#95e | CP-220035 | 0597 | - | B | Location dependent MBS service | 17.4.0 |
| 2022-03 | CT#95e | CP-220035 | 0603 | - | F | Incorrect IE Type Value - MBS Session N4 Information IE | 17.4.0 |
| 2022-03 | CT#95e | CP-220035 | 0606 | - | B | PFCP Node related messages supported over N4mb | 17.4.0 |
| 2022-03 | CT#95e | CP-220035 | 0607 | 1 | B | Mapping MBS QoS Flows to Associated QoS Flows | 17.4.0 |
| 2022-03 | CT#95e | CP-220035 | 0608 | 1 | B | User Plane (In)Activity Detection and Reporting over N4mb | 17.4.0 |
| 2022-03 | CT#95e | CP-220037 | 0600 | 1 | B | Reporting of the restart of a GTP-U entity | 17.4.0 |
| 2022-03 | CT#95e | CP-220046 | 0600 | 1 | B | Clarification on Allocation of Access Specific UDP Ports or MAC Addresses | 17.4.0 |
| 2022-03 | CT#95e | CP-220086 | 0593 | - | D | Editorial corrections | 17.4.0 |
| 2022-03 | CT#95e | CP-220086 | 0596 | 1 | F | Correcting PFCP Associations setup description | 17.4.0 |
| 2022-03 | CT#95e | CP-220086 | 0598 | - | F | CVLAN tag removal from DL traffic received on N6 | 17.4.0 |
| 2022-03 | CT#95e | CP-220086 | 0604 | - | F | Corrections to IE Definitions | 17.4.0 |
| 2022-03 | CT#95e | CP-220086 | 0605 | 1 | F | Return Node ID in PFCP Session Report Response | 17.4.0 |
| 2022-03 | CT#95e | CP-220086 | 0609 | 1 | F | PFCP session related procedures apply to 5GC | 17.4.0 |
| 2022-03 | CT#95e | CP-220086 | 0611 | 2 | B | Paging Policy Differentiation | 17.4.0 |
| 2022-03 | CT#95e | CP-220086 | 0612 | 1 | F | Additional Usage Reports Information | 17.4.0 |
| 2022-03 | CT#95e | CP-220086 | 0613 | 1 | B | Redirect Port Information | 17.4.0 |
| 2022-06 | CT#96 | CP-221023 | 0622 | 1 | B | Transport Level Marking information for PFCP sessions over N4mb | 17.5.0 |
| 2022-06 | CT#96 | CP-221023 | 0621 | 1 | B | MBS Session Identifier | 17.5.0 |
| 2022-06 | CT#96 | CP-221023 | 0617 | 1 | B | Restoration procedure for MB-UPF restart | 17.5.0 |
| 2022-06 | CT#96 | CP-221023 | 0616 | - | F | Incorrect references to N19mb and Nmb9 reference points | 17.5.0 |
| 2022-06 | CT#96 | CP-221023 | 0615 | - | B | DL MBS QFI Sequence Number in PDU Session Container | 17.5.0 |
| 2022-06 | CT#96 | CP-221024 | 0644 | 1 | B | Outer Header Removal for PSA UPF | 17.5.0 |
| 2022-06 | CT#96 | CP-221024 | 0637 | - | F | MB-UPF failure without restart | 17.5.0 |
| 2022-06 | CT#96 | CP-221024 | 0636 | - | F | 3GPP Interface Type extensions for MBS | 17.5.0 |
| 2022-06 | CT#96 | CP-221024 | 0635 | - | F | CP and UP function features supported over N4mb | 17.5.0 |
| 2022-06 | CT#96 | CP-221024 | 0634 | - | F | N4mb requirements for PFCP Node Related messages | 17.5.0 |
| 2022-06 | CT#96 | CP-221024 | 0633 | - | F | N4mb requirements for PFCP Session Related messages | 17.5.0 |
| 2022-06 | CT#96 | CP-221034 | 0642 | 1 | B | DNS Query Filter Encoding | 17.5.0 |
| 2022-06 | CT#96 | CP-221035 | 0630 | 1 | F | Two N3 UL CN tunnels information | 17.5.0 |
| 2022-06 | CT#96 | CP-221045 | 0619 | 1 | F | PFCP Node ID | 17.5.0 |
| 2022-06 | CT#96 | CP-221045 | 0618 | 1 | F | Failure to restore a PFCP session at UPF restart | 17.5.0 |
| 2022-06 | CT#96 | CP-221045 | 0614 | 3 | F | Node Report Type value for PFCP node reports not defined by 3GPP | 17.5.0 |
| 2022-06 | CT#96 | CP-221046 | 0646 | - | F | UE IP address | 17.5.0 |
| 2022-06 | CT#96 | CP-221046 | 0645 | 1 | F | Corrections on QoS Monitoring per QoS flow | 17.5.0 |
| 2022-06 | CT#96 | CP-221046 | 0643 | - | F | Corrections on PFCP Session Deletion Response with Additional Usage Report Info | 17.5.0 |
| 2022-06 | CT#96 | CP-221046 | 0641 | - | F | Incomplete CR implementation on Partial failure handling support over N4 | 17.5.0 |
| 2022-06 | CT#96 | CP-221046 | 0632 | 1 | F | Format of Tunnel Password | 17.5.0 |
| 2022-06 | CT#96 | CP-221046 | 0629 | 1 | F | Clarfication on the Threshold and Quota | 17.5.0 |
| 2022-06 | CT#96 | CP-221046 | 0628 | 1 | F | Number of Reports and Monitoring Time/Measurement Before QoS Enforcement | 17.5.0 |
| 2022-06 | CT#96 | CP-221046 | 0627 | - | F | Resolving editor's note for IPUPS | 17.5.0 |
| 2022-06 | CT#96 | CP-221046 | 0626 | 1 | F | Clarification on reactivation of an inactive URR | 17.5.0 |
| 2022-06 | CT#96 | CP-221046 | 0625 | - | F | Usage Report at expiry of the Quota Validity Timer | 17.5.0 |
| 2022-06 | CT#96 | CP-221046 | 0624 | - | F | Packet Rate for N4 | 17.5.0 |
| 2022-06 | CT#96 | CP-221046 | 0623 | 1 | F | Essential Correction on the support of the SMF Set | 17.5.0 |
| 2022-06 | CT#96 | CP-221050 | 0631 | 1 | F | N9 forwarding tunnel between ULCLs controlled by I-SMF | 17.5.0 |
| 2022-06 | CT#96 | CP-221065 | 0620 | 2 | A | Time domain identification in the clock drift reporting | 17.5.0 |
| 2022-06 | CT#96 | CP-221067 | 0640 | - | A | PDRs and Traffic Endpoints in PFCP Session Modification Request and Response | 17.5.0 |
| 2022-09 | CT#97e | CP-222031 | 0649 | 2 | F | Outer header creation | 17.6.0 |
| 2022-09 | CT#97e | CP-222031 | 0650 | 2 | F | Clarifications to Add MBS Unicast Parameters | 17.6.0 |
| 2022-09 | CT#97e | CP-222031 | 0651 | 4 | F | PLLSSM and FSSM flags | 17.6.0 |
| 2022-09 | CT#97e | CP-222031 | 0653 | - | F | Ingress address over N6mb or Nmb9 | 17.6.0 |
| 2022-09 | CT#97e | CP-222031 | 0655 | 1 | F | No URR support over N4mb | 17.6.0 |
| 2022-09 | CT#97e | CP-222031 | 0656 | - | F | FSSM Flag | 17.6.0 |
| 2022-09 | CT#97e | CP-222031 | 0658 | - | F | Unicast transport is used over Nmb9 | 17.6.0 |
| 2022-09 | CT#97e | CP-222041 | 0652 | 1 | F | Corrections on applicability of Flags | 17.6.0 |
| 2022-09 | CT#97e | CP-222041 | 0654 | 1 | F | Corrections to FQ-CSID node types | 17.6.0 |
| 2022-09 | CT#97e | CP-222041 | 0660 | - | D | Remove duplicate tables | 17.6.0 |
| 2022-09 | CT#97e | CP-222042 | 0647 | 1 | F | Uplink packets buffering during EAS relocation | 17.6.0 |
| 2022-12 | CT#98e | CP-223036 | 0665 | 1 | F | MBS Session Deactivation and (Re)activation | 17.7.0 |
| 2022-12 | CT#98e | CP-223036 | 0667 | - | F | Incorrect implementation of CR 29.244 #0650 | 17.7.0 |
| 2022-12 | CT#98e | CP-223036 | 0668 | - | F | Incomplete implementation of CR 29.244 #0658 | 17.7.0 |
| 2022-12 | CT#98e | CP-223036 | 0669 | - | F | N4 requirements for MBS session deactivation and reactivation | 17.7.0 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2022-12 | CT#98e | CP-223059 | 0663 | 3 | F | Clarifications and corrections on Time Sensitive Communication | 17.7.0 |
| 2022-12 | CT#98e | CP-223059 | 0666 | 1 | F | Essential clarification on Gate Status | 17.7.0 |
| 2022-12 | CT#98e | | | | | A style of header 7.5.4.10 corrected as H4. | 17.7.1 |

# History

| Document history | | |
|---|---|---|
| V17.4.0 | May 2022 | Publication |
| V17.5.0 | July 2022 | Publication |
| V17.6.0 | October 2022 | Publication |
| V17.7.1 | January 2023 | Publication |
| | | |