3GPP TS 29.244 V16.1.0 (2019-09)

Technical Specification

3rd Generation Partnership Project;

Technical Specification Group Core Network and Terminals;

Interface between the Control Plane and the User Plane Nodes;

Stage 3

(Release 16)

.

 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP..  
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.  
This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

3GPP, EPC, PFCP

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

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

Internet

http://www.3gpp.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2019, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword 12

1 Scope 13

2 References 13

3 Definitions, symbols and abbreviations 15

3.1 Definitions 15

3.2 Abbreviations 15

4 Protocol Stack 16

4.1 Introduction 16

4.2 UDP Header and Port Numbers 17

4.2.1 General 17

4.2.2 Request Message 18

4.2.3 Response Message 18

4.3 IP Header and IP Addresses 18

4.3.1 General 18

4.3.2 Request Message 18

4.3.3 Response Message 18

4.4 Layer 2 18

4.5 Layer 1 18

5 General description 19

5.1 Introduction 19

5.2 Packet Forwarding Model 19

5.2.1 General 19

5.2.1A Packet Detection Rule Handling 21

5.2.1A.1 General 21

5.2.1A.2 PDI Optimization 22

5.2.1A.2A Provisioning of SDF filters 22

5.2.1A.3 Bidirectional SDF Filters 23

5.2.1A.4 Application detection with PFD 23

5.2.2 Usage Reporting Rule Handling 23

5.2.2.1 General 23

5.2.2.2 Provisioning of Usage Reporting Rule in the UP function 24

5.2.2.2.1 General 24

5.2.2.2.2 Credit pooling (for EPC) 27

5.2.2.3 Reporting of Usage Report to the CP function 28

5.2.2.3.1 General 28

5.2.2.3.2 Credit pooling 30

5.2.2.4 Reporting of Linked Usage Reports to the CP function 31

5.2.3 Forwarding Action Rule Handling 31

5.2.3.1 General 31

5.2.4 Buffering Action Rule Handling 32

5.2.4.1 General 32

5.2.4.2 Provisioning of Buffering Action Rule in the UP function 33

5.2.5 QoS Enforcement Rule Handling 33

5.2.5.1 General 33

5.2.5.2 Provisioning of QoS Enforcement Rule in the UP function 33

5.2.6 Combined SGW/PGW Architecture 34

5.2.7 Multi-Access Rule Handling (for 5GC) 34

5.2.7.1 General 34

5.3 Data Forwarding between the CP and UP Functions 35

5.3.1 General 35

5.3.2 Sending of End Marker Packets 36

5.3.3 Forwarding of Packets Subject to Buffering in the CP Function 36

5.3.3.1 General 36

5.3.3.2 Forwarding of Packets from the UP Function to the CP Function 36

5.3.3.3 Forwarding of Packets from the CP Function to the UP Function 37

5.3.4 Data Forwarding between the CP and UP Functions with one PFCP-u Tunnel per UP Function or PDN 37

5.3.4.1 General 37

5.3.4.2 Forwarding of Packets from the UP Function to the CP Function 38

5.3.4.3 Forwarding of Packets from the CP Function to the UP Function 38

5.3.5 Forwarding of user data using Control Plane CIoT 5GS Optimisation (for 5GC) 38

5.3.5.1 General 38

5.3.5.2 Forwarding of Packets from the UP Function to the CP Function 38

5.3.5.3 Forwarding of Packets from the CP Function to the UP Function 39

5.4 Policy and Charging Control 39

5.4.1 General 39

5.4.2 Service Detection and Bearer/QoS Flow Binding 39

5.4.3 Gating Control 40

5.4.4 QoS Control 40

5.4.5 DL Flow Level Marking for Application Detection 41

5.4.6 Usage Monitoring 41

5.4.7 Traffic Redirection 42

5.4.8 Traffic Steering 43

5.4.9 Provisioning of Predefined PCC/ADC Rules 43

5.4.10 Charging 44

5.4.11 (Un)solicited Application Reporting 45

5.4.12 Service Identification for Improved Radio Utilisation for GERAN 46

5.4.13 Transport Level Marking 46

5.4.14 Deferred PDR activation and deactivation 46

5.5 F-TEID Allocation and Release 47

5.5.1 General 47

5.5.2 F-TEID allocation in the CP function 47

5.5.3 F-TEID allocation in the UP function 47

5.6 PFCP Session Handling 48

5.6.1 General 48

5.6.2 Session Endpoint Identifier Handling 48

5.6.3 Modifying the Rules of an Existing PFCP Session 48

5.7 Support of Lawful Interception 49

5.7.1 General 49

5.7.2 Lawful Interception in EPC 49

5.7.3 Lawful Interception in 5GC 49

5.8 PFCP Association 49

5.8.1 General 49

5.8.2 Behaviour with an Established PFCP Association 50

5.8.3 Behaviour without an Established PFCP Association 50

5.9 Usage of Vendor-specific IE 51

5.10 Error Indication Handling 51

5.11 User plane inactivity detection and reporting 51

5.12 Suspend and Resume Notification procedures 52

5.13 Ethernet traffic (for 5GC) 52

5.13.1 General 52

5.13.2 Address Resolution Protocol or IPv6 Neighbour Solicitation Response by SMF 53

5.13.3 Address Resolution Protocol or IPv6 Neighbour Solicitation Response by UPF 53

5.13.3A Provisioning of MAC addresses and SDF filters in Ethernet Packet Filters 54

5.13.4 Bidirectional Ethernet Filters 54

5.13.5 Reporting of UE MAC addresses to the SMF 54

5.14 Support IPv6 Prefix Delegation 55

5.15 Signalling based Trace (De)Activation 55

5.16 Framed Routing 55

5.17 5G UPF (for 5GC) 55

5.17.1 Introduction 55

5.17.2 Uplink Classifier and Branching Point 55

5.17.3 Data Forwarding during handovers between 5GS and EPS 56

5.18 Enhanced PFCP Association Release 57

5.18.1 General 57

5.18.2 UP Function Initiated PFCP Session Release 57

5.19 Activation and Deactivation of Pre-defined PDRs 57

5.20 Support of Access Traffic Steering, Switching and Splitting for 5GC 58

5.20.1 General 58

5.20.2 MPTCP functionality 59

5.20.3 ATSSS-LL functionality 59

5.21 UE IP address/prefix Allocation and Release (for 5GC) 59

5.21.1 General 59

5.21.2 UE IP address/prefix allocation in the CP function 59

5.21.3 UE IP address/prefix allocation in the UP function 59

5.22 PFCP sessions successively controlled by different SMFs of an SMF set (for 5GC) 60

5.22.1 General 60

5.22.2 With one PFCP association per SMF Set and UPF 60

5.22.3 With one PFCP association per SMF and UPF 61

5.23 5G VN Group Communication (for 5GC) 62

5.24 Support of Ultra Reliable Low Latency Communication for 5GC 62

5.24.1 General 62

5.24.2 Redundant Transmission on N3/N9 interfaces 62

5.24.3 Redundant Transmission at transport layer 63

6 Procedures 63

6.1 Introduction 63

6.2 PFCP Node Related Procedures 63

6.2.1 General 63

6.2.2 Heartbeat Procedure 63

6.2.2.1 General 63

6.2.2.2 Heartbeat Request 63

6.2.2.3 Heartbeat Response 64

6.2.3 Load Control Procedure 64

6.2.3.1 General 64

6.2.3.2 Principles 64

6.2.3.3 Load Control Information 64

6.2.3.3.1 General Description 64

6.2.3.3.2 Parameters 65

6.2.3.3.2.1 Load Control Sequence Number 65

6.2.3.3.2.2 Load Metric 65

6.2.3.3.3 Frequency of Inclusion 66

6.2.4 Overload Control Procedure 66

6.2.4.1 General 66

6.2.4.2 Principles 66

6.2.4.3 Overload Control Information 67

6.2.4.3.1 General Description 67

6.2.4.3.2 Parameters 68

6.2.4.3.2.1 Overload Control Sequence Number 68

6.2.4.3.2.2 Period of Validity 68

6.2.4.3.2.3 Overload Reduction Metric 69

6.2.4.3.3 Frequency of Inclusion 69

6.2.4.4 Message Throttling 70

6.2.4.4.1 General 70

6.2.4.4.2 Throttling algorithm – "Loss" 70

6.2.4.4.2.1 Description 70

6.2.4.5 Message Prioritization 70

6.2.4.5.1 Description 70

6.2.4.5.2 Based on the Message Priority Signalled in the PFCP Message 71

6.2.5 PFCP PFD Management Procedure 71

6.2.5.1 General 71

6.2.5.2 CP Function Behaviour 71

6.2.5.3 UP Function Behaviour 72

6.2.6 PFCP Association Setup Procedure 72

6.2.6.1 General 72

6.2.6.2 PFCP Association Setup Initiated by the CP Function 72

6.2.6.2.1 CP Function Behaviour 72

6.2.6.2.2 UP Function behaviour 73

6.2.6.3 PFCP Association Setup Initiated by the UP Function 73

6.2.6.3.1 UP Function Behaviour 73

6.2.6.3.2 CP Function Behaviour 73

6.2.7 PFCP Association Update Procedure 74

6.2.7.1 General 74

6.2.7.2 PFCP Association Update Procedure Initiated by the CP Function 74

6.2.7.2.1 CP Function Behaviour 74

6.2.7.2.2 UP Function Behaviour 74

6.2.7.3 PFCP Association Update Procedure Initiated by UP Function 74

6.2.7.3.1 UP Function Behaviour 74

6.2.7.3.2 CP Function Behaviour 75

6.2.8 PFCP Association Release Procedure 75

6.2.8.1 General 75

6.2.8.2 CP Function Behaviour 75

6.2.8.3 UP Function behaviour 75

6.2.9 PFCP Node Report Procedure 76

6.2.9.1 General 76

6.2.9.2 UP Function Behaviour 76

6.2.9.3 CP Function behaviour 76

6.3 PFCP Session Related Procedures 76

6.3.1 General 76

6.3.2 PFCP Session Establishment Procedure 76

6.3.2.1 General 76

6.3.2.2 CP Function Behaviour 76

6.3.2.3 UP Function Behaviour 77

6.3.3 PFCP Session Modification Procedure 77

6.3.3.1 General 77

6.3.3.2 CP Function behaviour 77

6.3.3.3 UP Function Behaviour 77

6.3.4 PFCP Session Deletion Procedure 78

6.3.4.1 General 78

6.3.4.2 CP Function Behaviour 78

6.3.4.3 UP Function Behaviour 78

6.3.5 PFCP Session Report Procedure 78

6.3.5.1 General 78

6.3.5.2 UP Function Behaviour 78

6.3.5.3 CP Function Behaviour 78

6.4 Reliable Delivery of PFCP Messages 79

6.5 PFCP messages bundling 79

7 Messages and Message Formats 80

7.1 Transmission Order and Bit Definitions 80

7.2 Message Format 80

7.2.1 General 80

7.2.1A PFCP messages bundled in one UDP/IP packet 80

7.2.2 Message Header 81

7.2.2.1 General Format 81

7.2.2.2 PFCP Header for Node Related Messages 81

7.2.2.3 PFCP Header for Session Related Messages 82

7.2.2.4 Usage of the PFCP Header 82

7.2.2.4.1 General 82

7.2.2.4.2 Conditions for Sending SEID=0 in PFCP Header 83

7.2.3 Information Elements 83

7.2.3.1 General 83

7.2.3.2 Presence Requirements of Information Elements 83

7.2.3.3 Grouped Information Elements 84

7.2.3.4 Information Element Type 85

7.3 Message Types 85

7.4 PFCP Node Related Messages 86

7.4.1 General 86

7.4.2 Heartbeat Messages 86

7.4.2.1 Heartbeat Request 86

7.4.2.2 Heartbeat Response 87

7.4.3 PFCP PFD Management 87

7.4.3.1 PFCP PFD Management Request 87

7.4.3.2 PFCP PFD Management Response 88

7.4.4 PFCP Association messages 89

7.4.4.1 PFCP Association Setup Request 89

7.4.4.2 PFCP Association Setup Response 91

7.4.4.3 PFCP Association Update Request 92

7.4.4.4 PFCP Association Update Response 93

7.4.4.5 PFCP Association Release Request 93

7.4.4.6 PFCP Association Release Response 93

7.4.4.7 PFCP Version Not Supported Response 93

7.4.5 PFCP Node Report Procedure 93

7.4.5.1 PFCP Node Report Request 93

7.4.5.1.1 General 93

7.4.5.1.2 User Plane Path Failure Report IE within PFCP Node Report Request 94

7.4.5.2 PFCP Node Report Response 94

7.4.5.2.1 General 94

7.4.6 PFCP Session Set Deletion 94

7.4.6.1 PFCP Session Set Deletion Request 94

7.4.6.2 PFCP Session Set Deletion Response 95

7.5 PFCP Session Related Messages 95

7.5.1 General 95

7.5.2 PFCP Session Establishment Request 95

7.5.2.1 General 95

7.5.2.2 Create PDR IE within PFCP Session Establishment Request 98

7.5.2.3 Create FAR IE within PFCP Session Establishment Request 102

7.5.2.4 Create URR IE within PFCP Session Establishment Request 106

7.5.2.5 Create QER IE within PFCP Session Establishment Request 111

7.5.2.6 Create BAR IE within PFCP Session Establishment Request 114

7.5.2.7 Create Traffic Endpoint IE within Sx Session Establishment Request 115

7.5.2.8 Create MAR IE within PFCP Session Establishment Request 117

7.5.3 PFCP Session Establishment Response 118

7.5.3.1 General 118

7.5.3.2 Created PDR IE within PFCP Session Establishment Response 118

7.5.3.3 Load Control Information IE within PFCP Session Establishment Response 119

7.5.3.4 Overload Control Information IE within PFCP Session Establishment Response 119

7.5.3.5 Created Traffic Endpoint IE within Sx Session Establishment Response 119

7.5.4 PFCP Session Modification Request 120

7.5.4.1 General 120

7.5.4.2 Update PDR IE within PFCP Session Modification Request 124

7.5.4.3 Update FAR IE within PFCP Session Modification Request 125

7.5.4.4 Update URR IE within PFCP Session Modification Request 127

7.5.4.5 Update QER IE within PFCP Session Modification Request 131

7.5.4.6 Remove PDR IE within PFCP Session Modification Request 134

7.5.4.7 Remove FAR IE within PFCP Session Modification Request 134

7.5.4.8 Remove URR IE within PFCP Session Modification Request 134

7.5.4.9 Remove QER IE PFCP Session Modification Request 134

7.5.4.10 Query URR IE within PFCP Session Modification Request 135

7.5.4.11 Update BAR IE within PFCP Session Modification Request 135

7.5.4.12 Remove BAR IE within PFCP Session Modification Request 135

7.5.4.13 Update Traffic Endpoint IE within Sx Session Modification Request 136

7.5.4.14 Remove Traffic Endpoint IE within Sx Session Modification Request 137

7.5.4.15 Remove MAR IE within PFCP Session Modification Request 138

7.5.4.16 Update MAR IE within PFCP Session Modification Request 138

7.5.5 PFCP Session Modification Response 140

7.5.5.1 General 140

7.5.5.2 Usage Report IE within PFCP Session Modification Response 141

7.5.6 PFCP Session Deletion Request 142

7.5.7 PFCP Session Deletion Response 143

7.5.7.1 General 143

7.5.7.2 Usage Report IE within PFCP Session Deletion Response 143

7.5.8 PFCP Session Report Request 144

7.5.8.1 General 144

7.5.8.2 Downlink Data Report IE within PFCP Session Report Request 145

7.5.8.3 Usage Report IE within PFCP Session Report Request 146

7.5.8.4 Error Indication Report IE within PFCP Session Report Request 148

7.5.9 PFCP Session Report Response 149

7.5.9.1 General 149

7.5.9.2 Update BAR IE within PFCP Session Report Response 149

7.6 Error Handling 150

7.6.1 Protocol Errors 150

7.6.2 Different PFCP Versions 151

7.6.3 PFCP Message of Invalid Length 151

7.6.4 Unknown PFCP Message 151

7.6.5 Unexpected PFCP Message 151

7.6.6 Missing Information Elements 151

7.6.7 Invalid Length Information Element 152

7.6.8 Semantically incorrect Information Element 152

7.6.9 Unknown or unexpected Information Element 152

7.6.10 Repeated Information Elements 152

8 Information Elements 153

8.1 Information Elements Format 153

8.1.1 Information Element Format 153

8.1.2 Information Element Types 154

8.2 Information Elements 159

8.2.1 Cause 159

8.2.2 Source Interface 162

8.2.3 F-TEID 162

8.2.4 Network Instance 163

8.2.5 SDF Filter 163

8.2.6 Application ID 165

8.2.7 Gate Status 165

8.2.8 MBR 166

8.2.9 GBR 166

8.2.10 QER Correlation ID 166

8.2.11 Precedence 167

8.2.12 Transport Level Marking 167

8.2.13 Volume Threshold 167

8.2.14 Time Threshold 168

8.2.15 Monitoring Time 168

8.2.16 Subsequent Volume Threshold 169

8.2.17 Subsequent Time Threshold 169

8.2.18 Inactivity Detection Time 170

8.2.19 Reporting Triggers 170

8.2.20 Redirect Information 171

8.2.21 Report Type 172

8.2.22 Offending IE 172

8.2.23 Forwarding Policy 172

8.2.24 Destination Interface 173

8.2.25 UP Function Features 173

8.2.26 Apply Action 176

8.2.27 Downlink Data Service Information 176

8.2.28 Downlink Data Notification Delay 177

8.2.29 DL Buffering Duration 177

8.2.30 DL Buffering Suggested Packet Count 177

8.2.31 PFCPSMReq-Flags 178

8.2.32 PFCPSRRsp-Flags 178

8.2.33 Sequence Number 179

8.2.34 Metric 179

8.2.35 Timer 179

8.2.36 Packet Detection Rule ID (PDR ID) 180

8.2.37 F-SEID 180

8.2.38 Node ID 181

8.2.39 PFD Contents 181

8.2.40 Measurement Method 183

8.2.41 Usage Report Trigger 184

8.2.42 Measurement Period 185

8.2.43 Fully qualified PDN Connection Set Identifier (FQ-CSID) 185

8.2.44 Volume Measurement 186

8.2.45 Duration Measurement 187

8.2.46 Time of First Packet 187

8.2.47 Time of Last Packet 187

8.2.48 Quota Holding Time 188

8.2.49 Dropped DL Traffic Threshold 188

8.2.50 Volume Quota 189

8.2.51 Time Quota 189

8.2.52 Start Time 189

8.2.53 End Time 190

8.2.54 URR ID 190

8.2.55 Linked URR ID IE 190

8.2.56 Outer Header Creation 191

8.2.57 BAR ID 192

8.2.58 CP Function Features 192

8.2.59 Usage Information 193

8.2.60 Application Instance ID 193

8.2.61 Flow Information 194

8.2.62 UE IP Address 194

8.2.63 Packet Rate 195

8.2.64 Outer Header Removal 196

8.2.65 Recovery Time Stamp 197

8.2.66 DL Flow Level Marking 198

8.2.67 Header Enrichment 198

8.2.68 Measurement Information 199

8.2.69 Node Report Type 199

8.2.70 Remote GTP-U Peer 200

8.2.71 UR-SEQN 200

8.2.72 Activate Predefined Rules 201

8.2.73 Deactivate Predefined Rules 201

8.2.74 FAR ID 201

8.2.75 QER ID 202

8.2.76 OCI Flags 202

8.2.77 PFCP Association Release Request 202

8.2.78 Graceful Release Period 203

8.2.79 PDN Type 203

8.2.80 Failed Rule ID 204

8.2.81 Time Quota Mechanism 204

8.2.82 User Plane IP Resource Information 205

8.2.83 User Plane Inactivity Timer 206

8.2.84 Multiplier 206

8.2.85 Aggregated URR ID IE 206

8.2.86 Subsequent Volume Quota 207

8.2.87 Subsequent Time Quota 207

8.2.88 RQI 207

8.2.89 QFI 208

8.2.90 Query URR Reference 208

8.2.91 Additional Usage Reports Information 208

8.2.92 Traffic Endpoint ID 209

8.2.93 MAC address 209

8.2.94 C-TAG (Customer-VLAN tag) 210

8.2.95 S-TAG (Service-VLAN tag) 210

8.2.96 Ethertype 211

8.2.97 Proxying 211

8.2.98 Ethernet Filter ID 211

8.2.99 Ethernet Filter Properties 212

8.2.100 Suggested Buffering Packets Count 212

8.2.101 User ID 212

8.2.102 Ethernet PDU Session Information 213

8.2.103 MAC Addresses Detected 214

8.2.104 MAC Addresses Removed 214

8.2.105 Ethernet Inactivity Timer 214

8.2.106 Subsequent Event Quota 215

8.2.107 Subsequent Event Threshold 215

8.2.108 Trace Information 215

8.2.109 Framed-Route 216

8.2.110 Framed-Routing 216

8.2.111 Framed-IPv6-Route 217

8.2.112 Event Quota 217

8.2.113 Event Threshold 217

8.2.114 Event Time Stamp 217

8.2.115 Averaging Window 218

8.2.116 Paging Policy Indicator (PPI) 218

8.2.117 APN/DNN 218

8.2.118 3GPP Interface Type 219

8.2.119 PFCPSRReq-Flags 219

8.2.120 PFCPAUReq-Flags 220

8.2.121 Activation Time 220

8.2.122 Deactivation Time 221

8.2.123 MAR ID 221

8.2.124 Steering Functionality 221

8.2.125 Steering Mode 222

8.2.126 Weight 222

8.2.127 Priority 222

8.2.128 UE IP address Pool Identity 223

8.2.129 Alternative SMF IP Address 223

8.2.130 Packet Replication and Detection Carry-On Information 223

8.2.131 SMF Set ID 224

8.2.132 Quota Validity Time 224

Annex A (Informative): PFCP Load and Overload Control Mechanism 226

A.1 Throttling Aalgorithms 226

A.1.1 "Loss" Throttling Algorithm 226

A.1.1.1 Example of Possible Implementation 226

Annex B (Normative): CP and UP Selection Functions with Control and User Plane Separation 226

B.1 CP Selection Function 226

B.1.1 General 226

B.2 UP Selection Function 227

B.2.1 General 227

B.2.2 SGW-U Selection Function 227

B.2.3 PGW-U Selection Function 227

B.2.4 Combined SGW-U/PGW-U Selection Function 228

B.2.5 TDF-U selection function 228

B.2.6 UP Selection Function Based on DNS 228

B.2.6.1 General 228

B.2.6.2 SGW-U Selection Function Based on DNS 229

B.2.6.3 PGW-U Selection Function Based on DNS 229

B.2.6.4 Combined SGW-U/PGW-U Selection Function Based on DNS 229

Annex C (Informative): Examples scenarios 229

C.1 General 229

C.2 Charging Support 229

C.2.1 Online Charging 229

C.2.1.1 Online Charging Call Flow – Normal Scenario 229

C.2.1.2 Online Charging Call Flow with Credit Pooling 231

C.2.1.2.1 General 231

C.2.1.2.2 Example Call Flow 1 232

C.2.1.2.3 Example Call Flow 2 234

Annex D (Normative): Use of PFCP over N16a for the support of traffic offload by UPF controlled by I-SMF 236

D.1 General 236

D.2 Procedures 237

D.2.1 Addition of PSA and UL CL/BP controlled by I-SMF 237

D.2.2 Removal of PSA and UL CL/BP 239

D.2.3 Change of PSA 239

D.2.4 Traffic Usage Reporting 239

D.2.5 Updating N4 information towards I-SMF 240

Annex E (Informative): Change history 240

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

# 1 Scope

The present document specifies the Packet Forwarding Control Protocol (PFCP) used on the interface between the control plane and the user plane function.

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].

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

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

The prefix PFCP in message and procedure names is used to indicate that messages and procedures are common and used on Sx and N4 reference point. A PFCP session refers to both Sx and/or N4 sessions. PFCP association are describing procedures to establish associations between EPC nodes (SGW-C/PGW-C/TDF-C and SGW-U/PGW-U/TDF-U) and also between 5G nodes (SMF and UPF).

In the related stage 2 specifications the prefix Sx and N4 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".

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

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

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

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

**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.

**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.

**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.

## 3.2 Abbreviations

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

ADC Application Detection and Control

BAR Buffering Action Rule

BP Branching Point

CP Control Plane

DDoS Distributed Denial of Service

DEI Drop Eligible Indicator

DSCP Differentiated Services Code Point

eMPS enhanced Multimedia Priority Service

FAR Forwarding Action Rule

F-SEID Fully Qualified SEID

F-TEID Fully Qualified TEID

IP Internet Protocol

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

I-SMF Intermediate SMF

LMISF LI Mirror IMS State Function

NR New Radio

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

PSA PDU Session Anchor

QER QoS Enforcement Rule

S8HR S8 Home Routed

SDF Service Data Flow

SEID Session Endpoint Identifier

SGW Serving Gateway

SGW-C Serving Gateway Control plane function

SGW-U Serving Gateway User plane function

SMF Session Management Function

SX3LIF Split X3 LI Interworking Function

TDF Traffic Detection Function

TDF-C Traffic Detection Function Control plane function

TDF-U Traffic Detection Function User plane function

ToS Type of Service

TSSF Traffic Steering Support Function

UDP User Datagram Protocol

UL CL Uplink Classifier

UP User Plane

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 and combined Sxa/Sxb 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 and combined Sxa/Sxb and N4

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 an 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 an 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].

This clause specifies the high level principles of the PFCP protocol and describe how 3GPP functionalities are realised on the Sxa, Sxb, Sxc and N4 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 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 an 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 or a standalone PFCP session not tied to any PDU 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;

- 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.

- one MAR when the PDR is used for matching downlink traffic towards the UE, which contain instructions to apply ATSSS feature for a N4 session established for a MA PDU session. See clause 5.2.7.

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

A FAR, a QER, a URR and a 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:

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

NOTE 3: It is allowed for instance to provision in a PGW-U a same uplink PDR, matching any uplink traffic towards a particular application server's IP address, in two different PFCP sessions of two different UEs, as long as each PFCP session is also provisioned with another uplink PDR set with the respective UE IP address and/or uplink F-TEIDu, which allows the PGW-U to identify the PFCP session to which the packet corresponds.

- As an exception to the previous principle, the CP function may provision a PDR with all match fields wildcarded (i.e. all match fields omitted in the PDI) in a separate 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.

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

- 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 4: 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 an PFCP session, the UP function shall delete the PFCP session context and all the associated non-preconfigured rules.

NOTE 5: 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.

### 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, 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) and/or Ethernet PDU Session Information (see clause 5.13.1).

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 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

PDI Optimization is an optional feature which may be supported by the CP and UP Functions. 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 an 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.

If F-TEID allocation is performed in the UP function, 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 an 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 an 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 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, a Volume Quota, or both (and/or respectively a Time Threshold, a Time Quota, or both).

When both a Volume (or Time) Threshold and a Volume (or Time) Quota are provisioned, the UP function shall send a usage report only when reaching the Volume (or Time) Threshold; when subsequently reaching the Volume (or Time) Quota, the UP function shall stop forwarding packets (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.

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

NOTE 4: The Volume Quota or Time Quota can be armed in a PGW-U or TDF-U for online charging to enable the traffic to be forwarded up to an intermediate or final quotas granted by the OCS. The CP function can provision both a Volume (or Time) Threshold and a Volume (or Time) Threshold to request the UP function to:  
- send a usage report when the consumed resources reach the volume (or time) usage threshold provided by the OCS, and   
- to stop forwarding packets (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 5: 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 6: 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;

- 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 the first usage report after the Monitoring Time is reached;

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

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 redirect the traffic towards a redirect destination as specified in clause 5.4.7.

NOTE 7: 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 8: This can be used in a PGW-U for the PGW Pause of Charging procedure (see 3GPP TS 23.401 [14]).

##### 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.   
A 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 indepentently.

- 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 associatied 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 a URR towards the CP function, the UP function shall:

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

- re-apply 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; and

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

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

- 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.

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.

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.

NOTE 3: 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.

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

When being instructed to remove a URR or the last PDR associated to a URR, the UP function shall 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, and shall reset its ongoing measurements for the URR that is removed, or dissociated from the last PDR.

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;

NOTE 4: 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 5: 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.

The CP function may request the UP function, in an 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 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 by subtracting the time/volume reported in the usage report to determine when to generate the next report.

NOTE 6: 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 7: 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 8: 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 9: 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 PFCP Session Report Request messages need to be sent, the UP function shall indicate, either in the PFCP Session Modification Response or in one PFCP Session Report Request, how many usage reports will be sent in PFCP Session Report Request messages. If this is indicated in one PFCP Session Report Request, the PFCP Session Modification Response shall indicate that more reports will follow by setting the AURI flag of the Additional Usage Reports Information IE. 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 10: Events (e.g. application detection information) are reported individually and independently from the usage report sent for envelope closure.

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).

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.

#### 5.2.2.4 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".

### 5.2.3 Forwarding Action Rule Handling

#### 5.2.3.1 General

The CP function shall provision one and only one FAR for each PDR provisioned in an 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;

- buffer downlink packets by setting the BUFF flag and by optionally provisioning buffering parameters providing instructions on how to buffer the packets;

- notify the CP function about the arrival of a first DL packet being buffered, by setting the NOCP flag;

- duplicate the packets, by setting the DUPL flag and by provisioning the Duplicating Parameters providing instructions on how to forward the duplicated packets.

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

The CP function may provision one or more FAR(s) per 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, by sending an 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.

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 3: It is not defined how to support SGi PtP tunnelling mechanisms other than based on UDP/IP encapsulation (such as PMIPv6/GRE, L2TP, GTP-C/U, see 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 4: 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 an 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 5: 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 an PFCP session and associate it to the FAR(s) of the PFCP session in an PFCP Session Establishment Request or an 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 an 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 an 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 an 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.

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 an 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 an PFCP session in an PFCP Session Establishment Request or an 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.

### 5.2.6 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.

The CP function (i.e. the SMF) shall provision one and only one MAR for every downlink PDR when the PDR is provisioned in a PFCP session if the PFCP session is established for a Multi-Access PDU session and if the UPF supports the ATSSS feature.

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 a 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;

- 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;

- 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.

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 together with a different steering mode, while different MARs of a same PFCP session may be associated with the same FAR(s).

## 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  CP to UP function | PGW | UPF to SMF  SMF to UPF |
| 2 | Forwarding of packets between the CP function and the external PDN (over SGi) / DN (over N6). | UP to CP function  CP to UP function | PGW | UPF to SMF  SMF to UPF |
| 3 | Forwarding of packets subject to buffering in the CP function. | UP to CP function  CP to UP function | SGW | UPF to SMF  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  CP to UP function | - | UPF to SMF  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.

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

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

- establish (once) one standalone 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";

- a 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";

- a 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].

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.

### 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, the traffic redirection may be enforced in the CP function or in the UP function. For 5GC, the traffic redirection may be enforced in the UP function only. 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 CP function, the CP function shall instruct the UP function to forward the applicable user traffic to the CP function, as specified in clause 5.3.1.

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

- create the necessary PDR(s) to represent the traffic to be redirected, if not already existing;

- create a FAR with:

- the Redirect Information IE including the redirect destination, if the traffic needs to be redirected towards a redirect destination provided by the CP function; a redirect destination provided by the CP function shall prevail over a redirect destination preconfigured in the UP function;

- 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 within:

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

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

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

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

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

- associating the URR to the PDR.

For unsolicited application reporting, an 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: 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 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.

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 fucntion 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, or update the PDR without providing Activation Time and Deactivation Time, or create the corresponding PDR rule if the PDR is not provisioned yet.

## 5.5 F-TEID Allocation and Release

### 5.5.1 General

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

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

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

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

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

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

The CP function may request the UP function to allocate the same F-TEID to several PDRs to be created within one single 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 an 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.

## 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 an 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. A 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.

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 an 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 clauses 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

An 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.

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 an IP address (see clause 8.2.38).

Prior to establishing an 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 1: 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 2: 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 clause 4.3.2 and 4.3.3.

### 5.8.2 Behaviour with an Established PFCP Association

When an 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 an 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;

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

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

- shall accept 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.

### 5.8.3 Behaviour without an Established PFCP Association

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

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

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

## 5.10 Error Indication Handling

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

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

- shall initiate an 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

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

Clause 4.3.7 and 4.3.2.2.2 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 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].

The CP function may request the UP function to detect and report when no user plane packets are received for an 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 an 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.

## 5.12 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 used as source address of frames sent UL by the UE, as specified in clause 5.13.5.

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 clause 7.5.2.2-x), 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 an 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 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 that are detected subsequently;

- report UE MAC addresses 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.

## 5.14 Support IPv6 Prefix Delegation

Clause 5.3.1.2.6 of 3GPP TS 23.401 [14] specifies the requirements for IPv6 Prefix Delegation via DHCPv6, that allow assigning a single network prefix shorter than the default /64 prefix to a PDN connection.

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 UP function with the IPv6D flag set to "1" and IPv6 Prefix Delegation Bits field to indicating the length of IPv6 Prefix for delegation.

## 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 DL PDRs to describe framed routes associated to the PDU session.

## 5.17 5G UPF (for 5GC)

### 5.17.1 Introduction

The following clauses describe the 5GS specific functionalites 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

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.

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 funciton 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 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 the Enhanced PFCP Association Release as described in 5.18.1 or when it detects an error, the UP function shall:

- send one or more PFCP Session Report Request messages for this PFCP session;

- 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.

## 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, a 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 can not 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 a multi-access PDU Connectivity Service, which can exchange PDUs between the UE and a data network by simultaneously using one 3GPP access network and one non-3GPP access network. The multi-access PDU Connectivity Service is realized by establishing a Multi-Access PDU (MA PDU) Session, i.e. a PDU Session that may have user-plane resources on two access networks.

Support of the ATSSS feature is an optional for the SMF and UPF, for 5GC. See 3GPP TS 23.501 [28].

When establishing a N4 session for a MA PDU session, the (h)SMF shall select a (h)UPF supporting the MA PDU Session Capability, i.e. ATSSS-LL capability, MPTCP capability, or both, and the h(SMF) shall provision a Multi-Access Rule for every downlink PDR which is used to match traffic sent towards the UE in the N4 session. (See also clause 5.2.7)

### 5.20.2 MPTCP functionality

Editor's Note: This clause will document any impact on N4 to support MPTCP functionality in UPF.

### 5.20.3 ATSSS-LL functionality

Editor's Note: This clause will document any impact on N4 to support ATSSS-LL functionality in UPF, including support of Access Network Performance Measurement function, i.e. PMF.

## 5.21 UE IP address/prefix Allocation and Release (for 5GC)

### 5.21.1 General

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 or the UPF 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].

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.

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

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).

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

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 flag 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); and

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

The CP function may request the UP function to allocate the same UE IP address/prefix 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 UE IP Address IE of each PDR to be created with a new UE IP address/prefix;

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

- including the UE IP Address IE only in the Create Traffic Endpoint IE and by setting the CHOOSE flag in the UE IP Address IE of this IE; and

- including the Traffic Endpoint ID in all the PDRs to be created with the same UE IP address.

If the PDR(s) is created successfully, the UP function shall return the UE IP address/prefix 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, 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.

## 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, or with each SMF of the SMF set establishing its own PFCP association with the UPF as described in clause 5.22.3, per SMF implementation choice.

### 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 in the PFCP Association Setup Request.

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.

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.

4) The UPF shall initiate PFCP session related requests (e.g. PFCP Session Report Request) towards any 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 use the IP addresses of alternative SMFs received during the PFCP association setup or update procedures, if any. 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 the new SMF, the UPF shall set a null SEID in the header of the PFCP request and include the CP F-SEID assigned by the previous SMF in the request.

5) An SMF may redirect a UPF initiated PFCP session related request to a different SMF in the SMF set by rejecting the request with the cause "Redirection Requested" and with the the IP address of the new SMF to contact. When sending the redirected request to the new SMF, the UPF shall set a null SEID 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 SMF in the SMF set; the new SMF answers to the UPF, including the CP F-SEID IE with the IPv4 or IPv6 address of the new SMF 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 SMF.

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) 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 3: 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.

### 5.22.3 With one PFCP association per SMF and UPF

Editor's note: The principle to enable the establishment of one PFCP association per SMF was agreed by CT4. However the technical details of the solution are subject to further discussion and possible changes.

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.  
  
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 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.

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) An SMF may redirect a UPF initiated PFCP session related request 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 SMF to contact. When sending the redirected request to the new SMF, the UPF shall set a null SEID 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 SMF in the SMF set; the new SMF answers to the UPF, including the CP F-SEID IE with the IPv4 or IPv6 address of the new SMF 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 SMF.

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 any 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. When sending the request to the new SMF, the UPF shall set a null SEID in the 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.

## 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 brocadcast 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).

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

Editor's Note: This clause will document the function on N4 to support URLLC in UPF in general.

### 5.24.2 Redundant Transmission on N3/N9 interfaces

Stage 2 requirements for support of Redundant Transmission on N3/N9 interfaces for high reliability communication are specified in clause 5.33.2.2 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).

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 as follows:

Editor's note: how to request the UPF to duplicate downlink packets is FFS.

If redundant transmission is required for a QoS flow, the SMF shall instruct the PSA UPF to eliminate the duplicated uplink packets of the QoS Flow, based on their sequence numbers, as follows:

Editor's note: how to request the UPF eliminate the duplicate uplink packets is FFS.

Editor's note: how to realize the sequence number for support of redundant transmission is FFS.

### 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 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, the CP function may request the UP function to perform the redundant transmission at transport layer during a PFCP session establishment or a PFCP session modification procedure.

Editor's Note: How the CP function request the UP function to perform the redundant transmission is FFS.

# 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 the node related 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

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

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

A CP function or UP function shall be prepared to receive an Heartbeat Request at any time (even from unknown peers) and it shall reply with an Heartbeat Response.

#### 6.2.2.3 Heartbeat Response

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

### 6.2.3 Load Control Procedure

#### 6.2.3.1 General

Load Control is an optional feature defined over the Sxa, Sxb, 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 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 occuring, unless the Overload Reduction Metric is set to 0, which signals that the overload condition has ceased. Conversely, the absence of the OCI IE in a message does not mean that the overload has abated.

##### 6.2.4.3.3 Frequency of Inclusion

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

- the sender may include OCI IE towards a receiver only when the new/changed value has not already been provided to the given receiver;

- the sender may include the OCI IE in a subset of the messages towards the receiver;

- the sender may include the OCI IE periodically, i.e. include the information during a first period then cease to do so during a second period.

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

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

#### 6.2.4.4 Message Throttling

##### 6.2.4.4.1 General

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

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

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

##### 6.2.4.4.2 Throttling algorithm – "Loss"

###### 6.2.4.4.2.1 Description

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

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 an 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

The PFCP Association Setup procedure shall be used to setup an 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 an 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 initiates the PFCP Association Setup procedure to request to setup an 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;

- shall send the PFCP Association Setup Request with the Node ID of the CP function;

- shall include the list of optional features the CP function supports which may affect the UP function behaviour, if any.

The CP function shall only initiate 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 an 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 an PFCP Association Setup Response with a successful cause, its Node ID, and information of all supported optional features in the UP function and optionally the available user plane resources, e.g. IP address(es) or F-TEID range;

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

#### 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 an PFCP association towards a CP function. The UP function is configured with a set of CP functions to which it shall establish an 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 and information of all supported optional features in the UP function and optionally the available user plane resources, e.g. IP address(es) or F-TEID range.

##### 6.2.6.3.2 CP Function Behaviour

When receiving an 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 an 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 an 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 an 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

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 an PFCP Association Update Request, the UP function:

- shall update the list of optional features of the CP function, when received;

- shall send an PFCP Association Update Response with an appropriate error cause if the Node ID is not known by the UP Function;

- shall return an 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 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, change of the available user plane resources, an indication to request to release the PFCP association.

The UP function may send an 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 an PFCP Association Release Request.

##### 6.2.7.3.2 CP Function Behaviour

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

- shall update the list of optional features of the UP function, when received;

- shall send an PFCP Association Update Response with an appropriate error cause if the Node ID is not known by the CP Function;

- shall return an 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 an 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 immediately initiate the PFCP Association Release Procedure, as specified in clause 5.18.

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

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

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 an 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 an PFCP Association Release Response with a successful cause.

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

### 6.2.9 PFCP Node Report Procedure

#### 6.2.9.1 General

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 an 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 an PFCP Node Report Request message, it shall:

- process the information being reported as appropriate and send an 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 and Sxc reference points. The behaviour of the CP function and UP function when sending and receiving session related messages is described.

### 6.3.2 PFCP Session Establishment Procedure

#### 6.3.2.1 General

The PFCP Session Establishment procedure shall be used to setup an 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 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 assign a local F-TEID for the access side and/or core side and provide it in the PDI, if F-TEID allocation is performed in the CP function.

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

#### 6.3.2.3 UP Function Behaviour

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

- store and apply the rules received in the request and send an 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, 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.

### 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 an modification of PDN connection, IP CAN session or TDF session.

The CP function shall:

- include a complete PDI if the PDI in the existing PDR is to be updated;

- remove locally the reference to a rule in the PDRs when the related Rule is deleted;

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

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 an PFCP Session Modification Response with the cause "success" it shall continue with the procedure which has initiated the PFCP Session Modification procedure.

#### 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 an 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 an acceptance cause value if all the requested modifications are accepted and performed successfully.

### 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 an PFCP Session Deletion procedure towards the UP function to delete an existing PFCP session e.g. when the corresponding PDN is deleted.

The CP shall:

- send an 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 an 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 an 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 an 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 an 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 bunding 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 bunding (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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | |
| Octets |  | 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 message 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;

- If a node receives a message for which it has no session, i.e. if SEID in the PFCP header is not known, it shall respond with "Session context not found" cause in the corresponding response message to the sender, the SEID used in the PFCP header in the response message shall be then set to "0";

- If a node receives a request message containing protocol error, e.g. Mandatory IE missing, which requires the receiver to reject the message as specified in clause 7.6, it shall reject the request message. For the response message, the node should look up the remote peer's SEID and accordingly set SEID in the PFCP header and the message cause code. As an implementation option, the node may not look up the remote peer's SEID and set the PFCP header SEID to "0" in the response message. However in this case, the cause value shall not be set to "Session not found".

### 7.2.3 Information Elements

#### 7.2.3.1 General

The format of PFCP Information Elements are defined in 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 an 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 with a message, these IEs shall have different IE types.

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

#### 7.2.3.4 Information Element Type

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

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

An IE Type value uniquely identifies a specific IE.

One IE type value is specified for Vendor Specific IEs.

## 7.3 Message Types

The PFCP message types to be used over the Sxa, Sxb, Sxc and N4 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 |
| 0 | Reserved |  |  |  |  |
|  | **PFCP Node related messages** |  |  |  |  |
| 1 | PFCP Heartbeat Request | X | X | X | X |
| 2 | PFCP Heartbeat Response | 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 |
| 6 | PFCP Association Setup Response | X | X | X | X |
| 7 | PFCP Association Update Request | X | X | X | X |
| 8 | PFCP Association Update Response | X | X | X | X |
| 9 | PFCP Association Release Request | X | X | X | X |
| 10 | PFCP Association Release Response | X | X | X | X |
| 11 | PFCP Version Not Supported Response | X | X | X | X |
| 12 | PFCP Node Report Request | X | X | X | X |
| 13 | PFCP Node Report Response | X | X | X | X |
| 14 | PFCP Session Set Deletion Request | X | X | - |  |
| 15 | PFCP Session Set Deletion Response | X | X | - |  |
| 16 to 49 | For future use |  |  |  |  |
|  | **PFCP Session related messages** |  |  |  |  |
| 50 | PFCP Session Establishment Request | X | X | X | X |
| 51 | PFCP Session Establishment Response | X | X | X | X |
| 52 | PFCP Session Modification Request | X | X | X | X |
| 53 | PFCP Session Modification Response | X | X | X | X |
| 54 | PFCP Session Deletion Request | X | X | X | X |
| 55 | PFCP Session Deletion Response | X | X | X | X |
| 56 | PFCP Session Report Request | X | X | X | X |
| 57 | PFCP Session Report Response | 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 the node related messages used over the Sxa, Sxb, Sxc and N4 reference points.

### 7.4.2 Heartbeat Messages

#### 7.4.2.1 Heartbeat Request

Table 7.4.2.1-1: Information Elements in Heartbeat Request

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

#### 7.4.2.2 Heartbeat Response

Table 7.4.2.2-1: Information Elements in Heartbeat Response

|  |  |  |  |
| --- | --- | --- | --- |
| **Information elements** | **P** | **Condition / Comment** | **IE Type** |
| Recovery Time Stamp | M | This IE shall contain the time stamp when the PFCP entity was started see clause 19A of 3GPP TS 23.007 [24]. | 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 |
| Sxa | Sxb | Sxc | N4 |  |
| Application ID's PFDs | C | This IE shall contain an Application Identifier and the associated PFDs to be provisioned in the UP function.  Several IEs with the same IE type may be present to provision PFDs for multiple Application IDs.  The UP function shall delete all the PFDs received and stored earlier for all the Application IDs if this IE is absent in the message. | - | X | X | X | Application ID's PFDs |

Table 7.4.3.1-2: Application ID's PFDs

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Octet 1 and 2 |  | Application ID's PFDs IE Type = 58 (decimal) | | | | | |
| Octets 3 and 4 |  | Length = n | | | | | |
| Information elements | P | Condition / Comment | Appl. | | | | IE Type |
| Sxa | Sxb | Sxc | N4 |  |
| 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.  When present, it shall describe the PFD to be provisioned in the UP function.  Several IEs with the same IE type may be present to provision multiple PFDs for this Application ID.  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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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 |

### 7.4.4 PFCP Association messages

#### 7.4.4.1 PFCP Association Setup Request

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

|  |  |  |  |
| --- | --- | --- | --- |
| Information elements | P | Condition / Comment | IE Type |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | Node ID |
| Recovery Time Stamp | M | This IE shall contain the time stamp when the CP or UP function was started, see clause 19A of 3GPP TS 23.007 [24]. (NOTE) | 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.  When present, this IE shall indicate the features the UP function supports. | UP Function Features |
| CP Function Features | C | This IE shall be present if the CP function sends this message and the CP function supports at least one CP feature defined in this IE.  When present, this IE shall indicate the features the CP function supports. | CP Function Features |
| User Plane IP Resource Information | O | This IE may be present if the UP function sends this message.  When present, this IE shall contain an IPv4 and/or an IPv6 address, together with a TEID range that the CP function shall use to allocate GTP-U F-TEID in the UP function.  Several IEs with the same IE type may be present to represent multiple User Plane IP Resources. | User Plane IP Resource Information |
| UE IP address Pool Identity | O | This IE may be present if the UP function sends this message.  When present, this IE shall contain an UE IP address Pool Identity  Several IEs with the same IE type may be present to represent multiple UE IP address Pool Identities. | UE IP address Pool Identity |
| Alternative SMF IP Address | O | This IE may be present if the SMF advertises the support of the SSET feature in the CP Function Features IE (see clause 8.2.58).  When present, this IE shall contain an IPv4 and/or IPv6 address of an alternative SMF.  Several IEs with the same IE type may be present to represent multiple alternative SMF IP addresses. | Alternative SMF IP Address |
| SMF Set ID | C | This IE shall be present if the SMF advertises the support of the MPAS feature in the CP Function Features IE (see clause 5.22.3).  When present, this IE shall contain an FQDN representing the SMF set to which the SMF belongs. | SMF Set ID |
| NOTE: A PFCP function that receives a PFCP Association Setup Request shall proceed with:  - establishing the PFCP association; and  - deleting the existing PFCP association and associated PFCP sessions, if a PFCP association was already established for the Node ID received in the request, regardless of the Recovery Timestamp received in the request. | | | |

#### 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 | IE Type |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | Node ID |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | Cause |
| Recovery Time Stamp | M | This IE shall contain the time stamp when the CP or UP function was started, see clause 19A of 3GPP TS 23.007 [24]. (NOTE) | 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.  When present, this IE shall indicate the features the UP function supports. | UP Function Features |
| CP Function Features | C | This IE shall be present if the CP function sends this message and the CP function supports at least one CP feature defined in this IE.  When present, this IE indicates the features the CP function supports. | CP Function Features |
| User Plane IP Resource Information | O | This IE may be present if the UP function sends this message.  When present, this IE shall contain an IPv4 and/or an IPv6 address, together with a TEID range that the CP function shall use to allocate GTP-U F-TEID in the UP function.  Several IEs with the same IE type may be present to represent multiple User Plane IP Resources. | User Plane IP Resource Information |
| Alternative SMF IP Address | O | This IE may be present if the SMF advertises the support of the SSET feature in the CP Function Features IE (see clause 8.2.58).  When present, this IE shall contain an IPv4 and/or IPv6 address of an alternative SMF.  Several IEs with the same IE type may be present to represent multiple alternative SMF IP addresses. | Alternative SMF IP Address |
| 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 | IE Type |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | Node ID |
| UP Function Features | O | If present, this IE shall indicate the supported Features when the sending node is the UP function. | UP Function Features |
| CP Function Features | O | If present, this IE shall indicate the supported Features when the sending node is the CP function. | CP Function Features |
| PFCP Association Release Request | C | This IE shall be present if the UP function requests the CP function to release the PFCP association. | 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. | Graceful Release Period |
| User Plane IP Resource Information | O | This IE may be present if the UP function sends this message.  When present, this IE shall contain an IPv4 and/or an IPv6 address, together with a TEID range that the CP function shall use to allocate GTP-U F-TEID in the UP function.  Several IEs with the same IE type may be present to represent multiple User Plane IP Resources. | User Plane IP Resource Information |
| PFCPAUReq-Flags | O | This IE shall be included if at least one of the flags is set to 1.  - 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. | PFCPAUReq-Flags |
| Alternative SMF IP Address | O | This IE may be present if the SMF advertises the support of the SSET feature in the CP Function Features IE (see clause 8.2.58).  When present, this IE shall contain an IPv4 and/or IPv6 address of an alternative SMF.  Several IEs with the same IE type may be present to represent multiple alternative SMF IP addresses. | Alternative SMF IP Address |

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

#### 7.4.4.5 PFCP Association Release Request

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

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

#### 7.4.4.6 PFCP Association Release Response

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

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

#### 7.4.4.7 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 and N4 interface by the UP function to report information to the CP function that is not specific to an PFCP session.

Table 7.4.5.1.1-1: Information Elements in PFCP Node Report Request

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
| Sxa | Sxb | Sxc | N4 |  | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | X | X | X | X | Node ID | |
| Node Report Type | M | This IE shall indicate the type of the report. | X | X | X | X | Node Report Type | |
| User Plane Path Failure Report | C | This IE shall be present if the Node Report Type indicates a User Plane Path Failure Report. | X | X | - | X | User Plane Path Failure 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 |
| Sxa | Sxb | Sxc | N4 |  | |
| 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.  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 | 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 and N4 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 |
| Sxa | Sxb | Sxc | N4 |  | |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | 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 | 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 | 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 and Sxb 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 and Sxb 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 |
| Sxa | Sxb | Sxc | N4 |  |
| Node ID | M | This IE shall contain the node identity of the originating node of the message. | X | X | - |  | Node ID |
| SGW-C FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - |  | FQ-CSID |
| PGW-C FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - |  | FQ-CSID |
| SGW-U FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | - | - |  | FQ-CSID |
| PGW-U FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - |  | FQ-CSID |
| TWAN FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - |  | FQ-CSID |
| ePDG FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - |  | FQ-CSID |
| MME FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - |  | FQ-CSID |

#### 7.4.6.2 PFCP Session Set Deletion Response

The PFCP Session Set Deletion Response shall be sent over the Sxa and Sxb interface by the UP function or the CP function as a reply to the 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 |
| Sxa | Sxb | Sxc | N4 |  |
| Node ID | M | This IE shall contain the unique identifier of the sending node. | X | X | - |  | Node ID |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | X | - |  | Cause |
| Offending IE | C | This IE shall be included if the rejection is due to an conditional or mandatory IE missing or faulty. | X | X | - |  | Offending IE |

## 7.5 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 and N4 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 an PFCP Session Establishment Request

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Information elements | P | Condition / Comment | Appl. | | | | IE Type |
| Sxa | Sxb | Sxc | N4 |  |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | 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 | F-SEID |
| Create PDR | M | This IE shall be present for at least one PDR to be associated to the PFCP session.  Several IEs with the same IE type may be present to represent multiple PDRs.  See Table 7.5.2.2-1. | 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.  Several IEs with the same IE type may be present to represent multiple FARs.  See Table 7.5.2.3-1. | 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.  Several IEs within the same IE type may be present to represent multiple URRs.  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.  Several IEs within the same IE type may be present to represent multiple QERs.  See Table 7.5.2.5-1. | - | 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.  Several IEs within the same IE type may be present to represent multiple Traffic Endpoints.  See Table 7.5.2.7-1. | 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).  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 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 | 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 | 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.  See NOTE. | 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 | APN/DNN |
| Create MAR | C | This IE shall be present for a N4 session established for a MA PDU session.  Several IEs with the same IE type may be present to represent multiple MARs.  See Table 7.5.2.8-1. | - | - | - | X | Create MAR |
| 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) 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, etc.  NOTE 3: The SGW-C may set PDN type as Non-IP for an Ethernet PDN to allow interworking with a legacy SGW-U. | | | | | | | |

#### 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 |  |
| PDR ID | M | This IE shall uniquely identify the PDR among all the PDRs configured for that PFCP session. | 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 | Precedence |
| PDI | M | This IE shall contain the PDI against which incoming packets will be matched.  See Table 7.5.2.2-2. | 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 | 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.  When present this IE shall contain the FAR ID to be associated to the PDR. | 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.  When present, this IE shall contain the URR IDs to be associated to the PDR.  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.  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 | 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.  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 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 |
| NOTE 1: When the Activation Time and Deactivation Time are not present, the PDR shall be activated immediately at receiving the message. | | | | | | | |

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 |  | |
| Source Interface | M | This IE shall identify the source interface of the incoming packet. | X | X | X | X | Source Interface | |
| Local F-TEID | O | This IE shall not be present if Traffic Endpoint ID is present.  If present, this IE shall identify the local F-TEID to match for an incoming packet.  The CP function shall set the CHOOSE (CH) bit to 1 if the UP function supports the allocation of F-TEID and the CP function requests the UP function to assign a local F-TEID to the PDR. | X | X | - | X | F-TEID | |
| 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.  If present, this IE shall identify the Network instance to match for the incoming packet. See NOTE 1, NOTE2. | X | X | X | X | Network Instance | |
| UE IP address | O | This IE shall not be present if Traffic Endpoint ID is present.  If present, this IE shall identify the source or destination IP address to match for the incoming packet. (NOTE 5)  The CP function shall set the CHOOSE (CH) bit 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. | - | 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.  If present, this IE shall uniquely identify the Traffic Endpoint for that PFCP session.  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 | 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.  See NOTE 3. | - | 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 | 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.  Several IEs with the same IE type may be present to represent a list of Ethernet Packet Filters.  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.  If present, this IE shall identify the QoS Flow Identifier to match for the incoming packet.  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 DL PDR if the UPF indicated support of Framed Routing (see clause 8.2.25). If present, this IE shall describe a framed route.  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 clause 8.2.25). If present, this IE shall describe a framed route. | - | X | - | X | Framed-Routing | |
| Framed-IPv6-Route | O | This IE may be present for a DL PDR if the UPF indicated support of Framed Routing (see clause 8.2.25). If present, this IE shall describe a framed IPv6 route.  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 | 3GPP Interface 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.  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 2 Traffic Endpoint ID containing different Local TEIDs per PDI can be provisioned over N4 interface for a PFCP session which is established for a PDU session subject for 5G to EPS mobility with N26 supported. | | | | | | | | |

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 |
| Sxa | Sxb | Sxc | N4 |  | |
| 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.  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.  Several IEs with the same IE type may be present to represent a list of SDF filters. | - | - | - | X | SDF Filter | |

#### 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 |  |
| FAR ID | M | This IE shall uniquely identify the FAR among all the FARs configured for that PFCP session. | 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 | 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.  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.  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.  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.  Several IEs with the same IE type may be present to represent to duplicate the packets to different destinations. See NOTE 1.  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 |
| 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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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.  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.  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 |
| 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.  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. | | | | | | | |

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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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. | | | | | | | |

#### 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 |
| Sxa | Sxb | Sxc | N4 |  | |
| 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. | 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)  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)  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)  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.  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.  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.  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 | 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).  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).  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.  Applicable flags are:  - 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.  - 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.  - 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.  - 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. .  - 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. | -  -  -  -  X | X  X  X  X  X | X  -  -  X  X | X  X  X  X  X | 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.  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.  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. | - | 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.  When present, it shall contain the duration of the Ethernet inactivity period. | - | - | - | X | Ethernet Inactivity Timer | |
| 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.  Several IEs with the same IE type may be present to provide multiple Monitoring Times. | X | X | X | X | Additional Monitoring Time | |
| 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. | | | | | | | | |

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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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 |
| Sxa | Sxb | Sxc | N4 |  | |
| 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 |
| Sxa | Sxb | Sxc | N4 |  |
| QER ID | M | This IE shall uniquely identify the QER among all the QER configured for that PFCP session | - | 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 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 | 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.  For EPC, this IE may be set to the value of:  - the APN-AMBR, for a QER that is referenced by all the PDRs of the non-GBR bearers of a PDN connection;  - the TDF session MBR, for a QER that is referenced by all the PDRs of a TDF session;  - the bearer MBR, for a QER that is referenced by all the PDRs of a bearer;  - the SDF MBR, for a QER that is referenced by all the PDRs of a SDF.  For 5GC, this IE may be set to the value of:  - the Session-AMBR, for a QER that is referenced by all the PDRs of the non-GBR QoS flows of a PDU session;  - the QoS Flow MBR, for a QER that is referenced by all the PDRs of a QoS Flow;  - the SDF MBR, for a QER that is referenced by all the PDRs of a SDF. | - | 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.  This IE may be set to the value of:  - the aggregate GBR, for a QER that is referenced by all the PDRs of a GBR bearer;  - the QoS Flow GBR, for a QER that is referenced by all the PDRs of a QoS Flow (for 5GC);  - the SDF GBR, for a QER that is referenced by all the PDRs of a SDF. | - | 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.  When present, this IE shall indicate the uplink and/or downlink maximum packet rate to be enforced for packets matching the PDR.  This IE may be set to the value of:  - downlink packet rate for Serving PLMN Rate Control, for a QER that is referenced by all PDRs of the UE belonging to the PDN connection using CIoT EPS Optimizations as described in 3GPP TS 23.401 [2]);  - uplink and/or downlink packet rate for APN Rate Control, for a QER that is referenced by all the PDRs of the UE belonging to PDN connections to the same APN using CIoT EPS Optimizations as described in 3GPP TS 23.401 [2]). | - | X | - | - | Packet Rate |
| DL Flow Level Marking | C | This IE shall be set if the UP function is required to mark the packets for QoS purposes:  - by the TDF-C, for DL flow level marking for application indication (see clause 5.4.5);  - 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 by the UPF. | - | - | - | X | QFI |
| Reflective QoS | C | This IE shall be present if the UP function is required to insert a Reflective QoS Identifier 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]).  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) | - | - | - | X | Averaging Window |
| NOTE: As 5QI is not signalled over N4, one default averaging window shall be pre-configured in the UPF. | | | | | | | |

#### 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 |
| Sxa | Sxb | Sxc | N4 |  | |
| 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.  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 the feature UDBC.  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 | |

#### 7.5.2.7 Create Traffic Endpoint IE within Sx 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 |  | |
| Traffic Endpoint ID | M | This IE shall uniquely identify the Traffic Endpoint for that Sx session. | 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.  The CP function shall set the CHOOSE (CH) bit to 1 if the UP function supports the allocation of F-TEID and the CP function requests the UP function to assign a local F-TEID to the 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.  If present, this IE shall identify the Network instance to match for the incoming packet. See NOTE 1, NOTE2. | X | X | X | X | Network Instance | |
| UE IP address | O | If present, this IE shall identify the source or destination IP address to match for the incoming packet. (NOTE 3)  The CP function shall set the CHOOSE (CH) bit 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. | - | 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 DL PDR if the UPF indicated support of Framed Routing (see clause 8.2.25). If present, this IE shall describe a framed route.  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 clause 8.2.25). If present, this IE shall describe the framed routing associated to a framed route. | - | X | - | X | Framed-Routing | |
| Framed-IPv6-Route | O | This IE may be present for a DL PDR if the UPF indicated support of Framed Routing (see clause 8.2.25). If present, this IE shall describe a framed IPv6 route.  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.  If present, this IE shall identify the QoS Flow Identifier to match for the incoming packet received from the traffic endpoint.  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 | |
| 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.  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. | | | | | | | | |

#### 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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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 |
| Access Forwarding Action Information 1 | M | This IE shall be present to provision access specific (non-3gpp or 3gpp) forwarding action information. | - | - | - | X | Access Forwarding Action Information 1 |
| Access Forwarding Action Information 2 | C | This IE shall be present to provision access specific (non-3gpp or 3gpp) forwarding action information if the UE is registered for both non-3GPP and 3GPP accesses. | - | - | - | X | Access Forwarding Action Information 2 |

Table 7.5.2.8-2: Access Forwarding Action Information 1 IE in the Create MAR IE

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Octet 1 and 2 |  | Access Forwarding Action Information 1 IE Type = 166 (decimal) | | | | | |
| Octets 3 and 4 |  | Length = n | | | | | |
| Information elements | P | Condition / Comment | Appl. | | | | IE Type |
| Sxa | Sxb | Sxc | N4 |  |
| 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)  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 |
| NOTE 1: The weights for all FARs included in both Access Forwarding Action Information 1 and Access Forwarding Action Information 2 need to sum up to be 100.  NOTE 2: The Priority value shall be set to "Active" or "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 Access Forwarding Action Information 1 and Access Forwarding Action Information 2 shall set different values.  NOTE 3: One or more URRs may still be provisioned in the Create PDR IE when a 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: Access Forwarding Action Information 2 IE in the Create MAR IE

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Octet 1 and 2 |  | Access Forwarding Action Information 2 IE Type = 167 (decimal) | | | | | |
| Octets 3 and 4 |  | Length = n | | | | | |
| Information elements | P | Condition / Comment | Appl. | | | | IE Type |
| Sxa | Sxb | Sxc | N4 |  |
| Same IEs and requirements as defined in Table 7.5.2.8-2 | | | | | | | |

### 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 |  |
| Node ID | M | This IE shall contain the unique identifier of the sending Node. | 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 | 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 | 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 identifing the session. | 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.  When present, this IE shall contain the PDR information associated to the PFCP session. There may be several instances of this IE.  See table 7.5.3.2-1. | 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.  See Table 7.5.3.3-1. | 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 | Overload Control Information |
| SGW-U FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | - | - | - | FQ-CSID |
| PGW-U FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - | - | FQ-CSID |
| Failed Rule ID | C | This IE shall be included if the Cause IE indicates a rejection due to a rule creation or modification failure. | X | X | X | 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.  There may be several instances of this IE. | X | X | - | X | Created Traffic Endpoint |

#### 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 |  |
| PDR ID | M |  | 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 |
| 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. | - | - | - | X | UE IP Address |

#### 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 |
| Sxa | Sxb | Sxc | N4 |  |
| Load Control Sequence Number | M | See clause 6.2.3.3.2 for the description and use of this parameter. | 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 | 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 |
| Sxa | Sxb | Sxc | N4 |  |
| Overload Control Sequence Number | M | See clause 6.2.4.3.2 for the description and use of this parameter. | 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 | Metric |
| Period of Validity | M | See clause 6.2.4.3.2 for the description and use of this parameter. | 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 | OCI Flags |

#### 7.5.3.5 Created Traffic Endpoint IE within Sx 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 Sx 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 |  |
| Traffic Endpoint ID | M | This IE shall uniquely identify the Traffic Endpoint for that Sx session. | 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 |
| 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. | - | - | - | X | UE IP Address |

### 7.5.4 PFCP Session Modification Request

#### 7.5.4.1 General

The PFCP Session Modification Request is used over the Sxa, Sxb, Sxc and N4 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 |
| Sxa | Sxb | Sxc | N4 |  | |
| 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 | 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 | 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 | 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 | 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. | 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 | 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 | 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 | 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. | 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 | 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 | Update FAR | |
| Update URR | C | This IE shall be present if URR(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 URRs. Previously URRs that are not modified shall not be included. 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.  Several IEs within the same IE type may be present to represent a list of modified QERs.  Previously created QERs that are not modified shall not be included.  See Table 7.5.4.5-1. | - | 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.  A previously created BAR that is not modified shall not be included.  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.  All the PDRs that refer to the Traffic Endpoint shall use the updated Traffic Endpoint information.  See Table 7.5.4.13-1. | 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.  - 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).  - 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). | X  X | -  X | -  X | X  X | PFCPSMReq-Flags | |
| Query URR | C | This IE shall be present if the CP function requests immediate usage report(s) to the UP function.  Several IEs within the same IE type may be present to represent a list of URRs for which an immediate report is requested.  See Table 7.5.4.10-1.  See NOTE 3. | X | X | X | X | Query URR | |
| PGW-C FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - | - | FQ-CSID | |
| SGW-C FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - | - | FQ-CSID | |
| MME FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | X | X | - | - | FQ-CSID | |
| ePDG FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - | - | FQ-CSID | |
| TWAN FQ-CSID | C | This IE shall be included according to the requirements in clause 23 of 3GPP TS 23.007 [24]. | - | X | - | - | FQ-CSID | |
| User Plane Inactivity Timer | C | This IE shall be present if it needs to be changed. | - | 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 a MAR previously created for the PFCP session needs to be modified. See Table 7.5.4.16-1.  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.  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 | Node ID | |
| 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 an 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. | | | | | | | | |

#### 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 |
| Sxa | Sxb | Sxc | N4 |  |
| PDR ID | M | This IE shall uniquely identify the PDR among all the PDRs configured for that PFCP session. | X | X | X | X | PDR ID |
| Outer Header Removal | C | This IE shall be present if it needs to be changed. | 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 | 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 | PDI |
| FAR ID | C | This IE shall be present if it needs to be changed | 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.  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.  When present, this IE shall contain the list of all the QER IDs to be associated to the PDR. | - | 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.  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.  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 |
| 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.  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 |  |
| FAR ID | M | This IE shall identify the FAR to be updated. | X | X | X | X | FAR ID |
| Apply Action | C | This IE shall be present if it is changed. | 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.  Several IEs with the same IE type may be present to request to duplicate the packets to different destinations. | X | X | - | - | Update Duplicating Parameters |
| BAR ID | C | This IE shall be present if the BAR ID associated to the FAR needs to be modified. | X | - | - | X | BAR ID |

Table 7.5.4.3-2: Update Forwarding Parameters IE in FAR

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octet 1 and 2 |  | Update Forwarding Parameters IE Type = 11 (decimal) | | | | | | |
| Octets 3 and 4 |  | Length = n | | | | | | |
| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
| Sxa | Sxb | Sxc | N4 |  | |
| Destination Interface | C | This IE shall only be provided if it is changed.  When present, it shall indicate the destination interface of the outgoing packet. | X | X | 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. 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. 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.  - 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 | |
| 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 FAR

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octet 1 and 2 |  | Update Duplicating Parameters IE Type = 105 (decimal) | | | | | | |
| Octets 3 and 4 |  | Length = n | | | | | | |
| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
| Sxa | Sxb | Sxc | N4 |  | |
| Destination Interface | C | This IE shall only be provided if it is changed.  When present, it shall indicate the destination interface of the outgoing packet. | X | X | - | - | Destination Interface | |
| Outer Header Creation | C | This IE shall only be provided if it is changed. 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. 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. | | | | | | | | |

#### 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 |
| Sxa | Sxb | Sxc | N4 |  | |
| 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.  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.  When present, this IE shall indicate the trigger(s) for reporting network resources usage to the CP function, e.g. periodic reporting or reporting upon reaching a threshold, or envelope closure. | X | X | X | X | Reporting Triggers | |
| Measurement Period | C | This IE shall be present if the Measurement Period needs to be modified.  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.  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.  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.  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.  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.  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.  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.  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.  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.  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.  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.  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.  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).  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.  Applicable flags are:  - 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.  - 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.  - 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. | -  -  - | X  X  X | -  -  X | X  X  X | Measurement Information | |
| Time Quota Mechanism | C | This IE shall be present if time-based measurement based on CTP or DTP needs to be modified. | - | X | - | - | Time Quota Mechanism | |
| Aggregated URRs | C | This IE shall be included if the Aggregated URRs IE needs to be modified. See Table 7.5.2.4-2.  Several IEs with the same IE type may be present to provision multiple aggregated URRs.  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.  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. | - | 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.  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 | |
| 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. | | | | | | | | |

#### 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 |
| Sxa | Sxb | Sxc | N4 |  |
| QER ID | M | This IE shall uniquely identify the QER among all the QRs configured for that PFCP session | - | 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.  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.  See NOTE 1. | - | 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.  When present, this IE shall indicate the uplink and/or downlink maximum bit rate to be enforced for packets matching the PDR.  For EPC, this IE may be set to the value of:  - the APN-AMBR, for a QER that is referenced by all the PDRs of the non-GBR bearers of a PDN connection;  - the TDF session MBR, for a QER that is referenced by all the PDRs of a TDF session;  - the bearer MBR, for a QER that is referenced by all the PDRs of a bearer;  - the SDF MBR, for a QER that is referenced by all the PDRs of a SDF.  For 5GC, this IE may be set to the value of:  - the Session-AMBR, for a QER that is referenced by all the PDRs of the non-GBR QoS flows of a PDU session;  - the QoS Flow MBR, for a QER that is referenced by all the PDRs of a QoS Flow;  - the SDF MBR, for a QER that is referenced by all the PDRs of a SDF.  See NOTE 1. | - | 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.  This IE may be set to the value of:  - the aggregate GBR, for a QER that is referenced by all the PDRs of a GBR bearer;  - the QoS Flow GBR, for a QER that is referenced by all the PDRs of a QoS Flow (for 5GC);  - the SDF GBR, for a QER that is referenced by all the PDRs of a SDF.  See NOTE 1. | - | 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 | - | - | Packet Rate |
| DL Flow Level Marking | C | This IE shall be set if the DL Flow Level Marking IE needs to be modified.  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 | QFI |
| Reflective QoS | C | This IE shall be present if it needs to be modified. | - | - | - | 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 |
| 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.  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.

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 |
| Sxa | Sxb | Sxc | N4 |  |
| PDR ID | M | This IE shall identify the PDR to be deleted. | 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 |
| Sxa | Sxb | Sxc | N4 |  |
| FAR ID | M | This IE shall identify the FAR to be deleted. | 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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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.

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 |
| Sxa | Sxb | Sxc | N4 |  |
| QER ID | M | This IE shall identify the QER to be deleted. | - | 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 |
| Sxa | Sxb | Sxc | 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 |
| Sxa | Sxb | Sxc | N4 |  | |
| 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.  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 the feature UDBC.  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 | |

#### 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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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 Sx 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 Sx 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 |
| Sxa | Sxb | Sxc | N4 |  | |
| Traffic Endpoint ID | M | This IE shall uniquely identify the Traffic Endpoint to be modified for that Sx session. | X | X | X | X | Traffic Endpoint ID | |
| Local F-TEID | C | This IE shall be present if it needs to be changed.  The CP function shall set the CHOOSE (CH) bit to 1 if the UP function supports the allocation of F-TEID and the CP function requests the UP function to assign a local F-TEID to the PDR.  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 | Network Instance | |
| UE IP address | C | This IE shall be present if it needs to be changed.  See NOTE. | - | X | X | X | UE IP address | |
| Framed-Route | C | This IE shall be present for a DL PDR if the UPF indicated support of Framed Routing (see clause 8.2.25) and it needs to be changed. If present, this IE shall describe a framed route.  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 clause 8.2.25) and it needs to be changed. If present, this IE shall describe the framed routing associated to a framed route. | - | X | - | X | Framed-Routing | |
| Framed-IPv6-Route | C | This IE shall be present for a DL PDR if the UPF indicated support of Framed Routing (see clause 8.2.25) and it needs to be changed. If present, this IE shall describe a framed IPv6 route.  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.  If present, this IE shall identify the QoS Flow Identifier to match for the incoming packet.  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 | |
| NOTE: 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). | | | | | | | | |

#### 7.5.4.14 Remove Traffic Endpoint IE within Sx 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 Sx 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 |
| Sxa | Sxb | Sxc | N4 |  |
| Traffic Endpoint ID | M | This IE shall identify the Traffic Endpoint to be deleted. | 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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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.z-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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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 Access Forwarding Action Information 1 | C | This IE shall be present if the Access Forwarding Action Information 1 was provisioned previously and if any of IEs is to be changed.  This IE shall also be present to remove Access Forwarding Action Information 1 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 Access Forwarding Action Information 1 |
| Update Access Forwarding Action Information 2 | C | This IE shall be present if the Access Forwarding Action Information 2 was provisioned previously and if any of IEs is to be changed.  This IE shall also be present to remove Access Forwarding Action Information 2 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 Access Forwarding Action Information 2 |
| Access Forwarding Action Information 1 | C | This IE shall be present to provision access specific (non-3gpp or 3gpp) forwarding action information when another access is added, i.e. when the UE is registered in both non-3GPP and 3GPP accesses.  See Table 7.5.2.8-2. | - | - | - | X | Access Forwarding Action Information 1 |
| Access Forwarding Action Information 2 | C | This IE shall be present to provision access specific (non-3gpp or 3gpp) forwarding action information when another access is added, i.e. when the UE is registered in both non-3GPP and 3GPP accesses.  See Table 7.5.2.8-3. | - | - | - | X | Access Forwarding Action Information 2 |

Table 7.5.4.16-2: Update Access Forwarding Action Information 1 IE in Update MAR IE

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octet 1 and 2 |  | Update Access Forwarding Action Information 1 IE Type = 175 (decimal) | | | | | | |
| Octets 3 and 4 |  | Length = n | | | | | | |
| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
| Sxa | Sxb | Sxc | N4 |  | |
| 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.  When present, this IE shall contain the list of all the URR IDs to be associated to this access. | - | - | - | X | URR ID | |

Table 7.5.4.z-3: Update Access Forwarding Action Information 2 IE in Update MAR IE

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octet 1 and 2 |  | Update Access Forwarding Action Information 2 IE Type = 176 (decimal) | | | | | | |
| Octets 3 and 4 |  | Length = n | | | | | | |
| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
| Sxa | Sxb | Sxc | N4 |  | |
| Same IEs and requirements as defined in Table 7.5.4.16-2 | | | | | | | | |

### 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 |  |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | 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 | Offending IE |
| Created PDR | C | This IE shall be present if the cause is set to "success", new PDR(s) were requested to be created and the UP function was requested to allocate the local F-TEID for the PDR(s).  When present, this IE shall contain the PDR information associated to the PFCP session.  See Table 7.5.3.2-1. | 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.  See Table 7.5.3.3-1. | 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 | Overload Control Information |
| Usage Report | C | This IE shall be present if:  - the Query URR IE was present or the QAURR flag was set to "1" in the PFCP Session Modification Request,  - traffic usage measurements for that URR are available at the UP function, and  - the UP function decides to return some or all of the requested usage reports in the PFCP Session Modification Response.  This IE shall be also present if:  - a URR or the last PDR associated to a URR has been removed,  - non-null traffic usage measurements for that URR are available in the UP function, and  - 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).  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 | 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).  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 for the Traffic Endpoint(s).  When present, this IE shall contain the Traffic Endpoint information associated to the PFCP session.  See Table 7.5.3.5-1. | X | X | - | X | Created Traffic Endpoint |

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

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

Table 7.5.5.2-1: Usage Report IE within 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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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'.  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'.  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 an PFCP Session Modification Request and the Query URR Reference IE was present in the PFCP Session Modification Request.  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 |

### 7.5.6 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.

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Information elements | P | Condition / Comment | Appl. | | | | IE Type |
| Sxa | Sxb | Sxc | N4 |  |
|  |  |  |  |  |  |  |  |

### 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 |
| Sxa | Sxb | Sxc | N4 |  |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | X | 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 | 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 | 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 | 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 |

#### 7.5.7.2 Usage Report IE within PFCP Session Deletion Response

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

Table 7.5.7.2-1: Usage Report IE within 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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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'.  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'.  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 and N4 interface by the UP function to report information related to an PFCP session to the CP function.

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Information elements | P | Condition / Comment | Appl. | | | | IE Type |
| Sxa | Sxb | Sxc | N4 |  |
| Report Type | M | This IE shall indicate the type of the report. | 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 | Downlink Data Report |
| Usage Report | C | This IE shall be present if the Report Type indicates a Usage Report.  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 | 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.  See Table 7.5.3.3-1. | 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 | Overload Control Information |
| Additional Usage Reports Information | C | This IE shall be included in one additional PFCP Session Report Request message, if the PFCP Session Modification Response indicated that more reports would follow (i.e. if the AURI flag was set to 1) (see clause 5.2.2.3.1).  When present, this IE shall 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 |
| PFCPSRReq-Flags | C | This IE shall be included if at least one of the flags is set to 1.  - PSDBU (PFCP Session Deleted By the UP function): 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. | 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.  When present, it shall indicate the CP F-SEID assigned by the previous SMF to the PFCP session. | - | - | - | X | F-SEID |

#### 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 Figure 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 |
| Sxa | Sxb | Sxc | N4 |  |
| PDR ID | M | This IE shall identify the PDR for which downlink data packets have been received at the UP function.  More than one IE with this type may be included to represent multiple PDRs having received downlink data packets. | X | - | - | X | PDR ID |
| Downlink Data Service Information | C | This IE shall be included for an 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]).  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]).  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.  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 |

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

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

Table 7.5.8.3-1: Usage Report IE within 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 |
| Sxa | Sxb | Sxc | N4 |  | |
| 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'.  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'.  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 | |
| 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 an PFCP Session Modification Request and the Query URR Reference IE was present in the PFCP Session Modification Request.  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.  When present, it shall be set to the time when the event occurs.  Several IEs with the same IE type may be present to report multiple occurrences for an event for this URR ID. | - | X | X | X | Event 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 | |
| NOTE 1: This is the case for unsolicited application reporting by the TDF. The Network instance is required when the UE IP address cannot be used to determine the corresponding PDN connection. | | | | | | | | |

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Octet 1 and 2 |  | Application Detection Information IE Type = 68 (decimal) | | | | | | |
| Octets 3 and 4 |  | Length = n | | | | | | |
| Information elements | P | Condition / Comment | Appl. | | | | | IE Type |
| Sxa | Sxb | Sxc | N4 |  | |
| 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 | |

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 |
| Sxa | Sxb | Sxc | N4 |  | |
| MAC Addresses Detected | C | This IE shall be present if one or more new MAC addresses have been detected.  When present, it shall identify the MAC (Ethernet) addresses newly detected as source address of frames sent UL by the UE. | - | - | - | X | MAC Addresses Detected | |
| MAC Addresses Removed | C | This IE shall be present if one or more new MAC addresses have been removed.  When present, it shall identify the MAC (Ethernet) addresses that have been inactive for a duration exceeding the Ethernet inactivity Timer. | - | - | - | X | MAC Addresses Removed | |

#### 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 Figure 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 |
| Sxa | Sxb | Sxc | N4 |  |
| 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.  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 | F-TEID |

### 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 and N4 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 |
| Sxa | Sxb | Sxc | N4 |  |
| Cause | M | This IE shall indicate the acceptance or the rejection of the corresponding request message. | 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 | Offending IE |
| Update BAR | C | This IE shall be present if a BAR previously created for the PFCP session needs to be modified.  A previously created BAR that is not modified shall not be included.  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.  - 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).  When present, it shall be set to the new F-SEID that the UPF shall use for sending subsequent PFCP session related messages. | - | - | - | 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)".  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).  When present, it shall be set to the IP address of the new SMF to contact. | - | - | - | X | Alternative SMF IP Address |
| 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 an 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 Figure 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 |
| Sxa | Sxb | Sxc | N4 |  | |
| 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.  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.  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.  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.  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 an 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 Echo Request message, if one or more mandatory information elements are missing in the received Request message, the PFCP entity should log the error and shall send a Response message with Cause IE value set to "Mandatory IE missing" with the type of the missing mandatory IE.

If a PFCP entity receives a Response message with Cause IE value set to "Mandatory IE missing", it shall notify its upper layer.

A PFCP entity shall check if all mandatory IEs are present in the received Response message without a rejection Cause value. If one or more mandatory information elements are missing, the PFCP entity shall notify the upper layer and should log the error.

A PFCP entity shall check if conditional information elements are present in the received Request message, if possible (i.e. if the receiving entity has sufficient information available to check if the respective conditions were met). If one or more conditional information elements are missing, a PFCP entity should log the error and shall send a Response message with Cause IE value set to "Conditional IE missing" together with the type of the missing conditional IE.

A PFCP entity shall check if conditional information elements are present in the received Response message without a rejection Cause value, if possible (i.e. if the receiving entity has sufficient information available to check if the respective conditions were met). If one or more conditional information elements are missing, a PFCP entity shall notify the upper layer and should log the error.

For Response messages containing a rejection Cause value, see 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = xxx (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 to (n+4) | IE specific data or content of a grouped IE | | | | | | | | |  |

Figure 8.1.1-2: 3GPP defined Information Element Format

NOTE 2: Bit 8 of Octet 1 is not set. This indicates that the Information Element type value has been allocated by 3GPP.

For illustration, Figure 8.1.1-3 depicts the format of a vendor-specific Information Element, which content is not specified and the IE type value shall be within the range of 32768 to 65535.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = xxx (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 to 6 | Enterprise ID | | | | | | | | |  |
|  | 7 to (n+4) | IE specific data or content of a grouped IE | | | | | | | | |  |

Figure 8.1.1-3: Vendor-Specific Information Element Format

NOTE 3: Bit 8 of Octet 1 is set. This indicates that the IE type value has been allocated by the vendor identified by the Enterprise ID. The content of this IE is vendor specific and therefore out of scope of this specification.

### 8.1.2 Information Element Types

A PFCP message may contain several IEs. In order to have forward compatible type definitions for the PFCP IEs, all of them shall be TLV (Type, Length, Value) coded. PFCP IE type values are specified in the Table 8.1.2-1. The last column of this table indicates whether the IE is:

- Fixed Length: the IE has a fixed set of fields, and a fixed number of octets;

- Variable Length: the IE has a fixed set of fields, and has a variable number of octets.  
For example, the last octets may be numbered similar to "5 to (n+4)". In this example, if the value of the length field, n, is 0, then the last field is not present;

- Extendable: the IE has a variable number of fields, and has a variable number of octets.  
The last fields are typically specified with the statement: "These octet(s) is/are present only if explicitly specified". The legacy receiving entity shall ignore the unknown octets.

An IE of any of the above types may have a null length as specified in 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 | q-4 |
| 22 | Network Instance | Variable Length / Clause 8.2.4 | Not Applicable |
| 23 | SDF Filter | Extendable / Clause 8.2.5 | v+2-4 |
| 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 | q+7-4 |
| 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 | q+7-4 |
| 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 | (8+a-1)-4 |
| 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 | k-4 |
| 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 | p+15-4 |
| 58 | Application ID's PFDs | Extendable / Table 7.4.3.1-2 | Not Applicable |
| 59 | PFD context | Extendable / Table 7.4.3.1-3 | Not Applicable |
| 60 | Node ID | Extendable / Clause 8.2.38 | o-4 |
| 61 | PFD contents | Extendable / Clause 8.2.39 | v-4 |
| 62 | Measurement Method | Extendable / Clause 8.2.40 | 1 |
| 63 | Usage Report Trigger | Extendable / Clause 8.2.41 | 1 |
| 64 | Measurement Period | Extendable / Clause 8.2.42 | 4 |
| 65 | FQ-CSID | Extendable / Clause 8.2.43 | (q+1)-4 |
| 66 | Volume Measurement | Extendable / Clause 8.2.44 | q+7-4 |
| 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 | m+7-4 |
| 73 | Volume Quota | Extendable / Clause 8.2.50 | q+7-4 |
| 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 | r+1-4 |
| 85 | Create BAR | Extendable / Table 7.5.2.6-1 | Not Applicable |
| 86 | Update BAR (Session Modification Request) | Extendable / Table 7.5.4.11-1 | Not Applicable |
| 87 | Remove BAR | Extendable / Table 7.5.4.12-1 | Not Applicable |
| 88 | BAR ID | Extendable / 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 | m-4 |
| 93 | UE IP Address | Extendable / Clause 8.2.62 | p+15-1 |
| 94 | Packet Rate | Extendable / Clause 8.2.63 | p+2-4 |
| 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 | p+1-4 |
| 98 | Header Enrichment | Extendable / Clause 8.2.67 | q-4 |
| 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 | p+15-4 |
| 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 | p-4 |
| 115 | Time Quota Mechanism | Extendable / Clause 8.2.81 | 5 |
| 116 | User Plane IP Resource Information | Extendable / Clause 8.2.82 | l+1-4 |
| 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 | q+7-4 |
| 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 | m-4 |
| 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 | s-1-4 |
| 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 |  |
| 141 | User ID | Extendable / Clause 8.2.101 | h-1-4 |
| 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 | q-4 |
| 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 | Event 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 | Access Forwarding Action Information 1 | Extendable / Table 7.5.2.8-2 | Not Applicable |
| 167 | Access Forwarding Action Information 2 | 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 Access Forwarding Action Information 1 | Extendable / Table 7.5.4.16-2 | Not Applicable |
| 176 | Update Access Forwarding Action Information 2 | Extendable / Table 7.5.4.16-3 | Not Applicable |
| 177 | UE IP address Pool Identity | Extendable / Clause 8.2.128 | 6 |
| 178 | Alternative SMF IP Address | Extendable / Clause 8.2.129 | m-1-4 |
| 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 to 65535 | Spare. For future use. |  |  |

## 8.2 Information Elements

### 8.2.1 Cause

Cause IE is coded as depicted in Figure 8.2.1-1.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| . |  | Bits | | | | | | | | |  |
|  | Octets | 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. |
| 2-63 | 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). |
| 72 | No established PFCP Association | This cause shall be used by the CP function or the UP function if they receive a PFCP Session related 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. |
| 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 to 255 | Spare for future use in a response message. See NOTE 2. | This value range shall be used by Cause values in a rejection response message. See NOTE 2. |
| NOTE 1: This value is or may be used in future version of the specification. If the receiver cannot comprehend the value, it shall be interpreted as an unspecified acceptance cause. Unspecified/unrecognized acceptance cause shall be treated in the same ways as the cause value 1 " Request accepted (success)".  NOTE 2: This value is or may be used in a future version of the specification. If the receiver cannot comprehend the value, it shall be interpreted as an unspecified rejection cause. Unspecified/unrecognized rejection cause shall be treated in the same ways as the cause value 32 "Request rejected (reason not specified)". | | | |

### 8.2.2 Source Interface

The Source Interface IE type shall be encoded as shown in Figure 8.2.2-1. It indicates the type of the interface from which an incoming packet is received.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | |  |
|  | Octets | 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 allocating 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 28 (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 to 8 | QER Correlation ID value | | | | | | | | |  |
|  | 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | |  |

Figure 8.2.10-1: QER Correlation ID

The QER Correlation ID value shall be encoded as an Unsigned32 binary integer value.

### 8.2.11 Precedence

The Precedence IE type shall be encoded as shown in Figure 8.2.11-1. It defines the relative precedence of a PDR among all the PDRs provisioned within an PFCP session, when looking for a PDR matching an incoming packet.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 37 (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 | LIUSA | DROTH | STOPT | START | QUHTI | TIMTH | VOLTH | PERIO |  | |
|  | 6 | Spare | Spare | EVEQU | EVETH | MACAR | ENVCL | TIMQU | VOLQU |  | |
|  | 7 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | |  |

Figure 8.2.19-1: Reporting Triggers

Octet 5 shall be encoded as follows:

- Bit 1 – PERIO (Periodic Reporting): when set to 1, this indicates a request for periodic reporting.

- Bit 2 – VOLTH (Volume Threshold): when set to 1, this indicates a request for reporting when the data volume usage reaches a volume threshold

- Bit 3 – TIMTH (Time Threshold): when set to 1, this indicates a request for reporting when the time usage reaches a time threshold.

- Bit 4 – QUHTI (Quota Holding Time): when set to 1, this indicates a request for reporting when no packets have been received for a period exceeding the Quota Holding Time.

- Bit 5 – START (Start of Traffic): when set to 1, this indicates a request for reporting when detecting the start of an SDF or Application traffic.

- Bit 6 – STOPT (Stop of Traffic): when set to 1, this indicates a request for reporting when detecting the stop of an SDF or Application Traffic.

- Bit 7 - DROTH (Dropped DL Traffic Threshold): when set to 1, this indicates a request for reporting when the DL traffic being dropped reaches a threshold.

- Bit 8: - LIUSA (Linked Usage Reporting): when set to 1, this indicates a request for linked usage reporting, i.e. a request for reporting a usage report for a URR when a usage report is reported for a linked URR (see 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.

- Bits 7 to 8: Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

### 8.2.20 Redirect Information

Redirect Information is coded as depicted in Figure 8.2.20-1.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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 | | | | | | | | | |  |
|  | 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 |
| Spare, for future use. | 5 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.

### 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | | 3 | | 2 | 1 |  | |
|  | 1 to 2 | Type = 39 (decimal) | | | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | | | |  |
|  | 5 | Spare | | | | | 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 to 8 – Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

### 8.2.22 Offending IE

Offending IE IE is coded as depicted in Figure 8.2.22-1.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| . |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 43 (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 to 6 | Supported-Features | | | | | | | | |  |
|  | 7 to 8 | Additional Supported-Features 1 | | | | | | | | |  |
|  | 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | |  |

Figure 8.2.25-1: UP Function Features

The UP Function Features IE takes the form of a bitmask where each bit set indicates that the corresponding feature is supported. Spare bits shall be ignored by the receiver. The same bitmask is defined for all PFCP interfaces.

The following table specifies the features defined on PFCP interfaces and the interfaces on which they apply.

Table 8.2.25-1: UP Function Features

|  |  |  |  |
| --- | --- | --- | --- |
| Feature Octet / Bit | Feature | Interface | Description |
| 5/1 | BUCP | Sxa, N4 | Downlink Data Buffering in CP function is supported by the UP function. |
| 5/2 | DDND | Sxa, N4 | The buffering parameter 'Downlink Data Notification Delay' is supported by the UP function. |
| 5/3 | DLBD | Sxa, N4 | The buffering parameter 'DL Buffering Duration' is supported by the UP function. |
| 5/4 | TRST | Sxb, Sxc, N4 | Traffic Steering is supported by the UP function. |
| 5/5 | FTUP | Sxa, Sxb, N4 | F-TEID allocation / release in the UP function is supported by the UP function. |
| 5/6 | PFDM | Sxb, Sxc, N4 | The PFD Management procedure is supported by the UP function. |
| 5/7 | HEEU | Sxb, Sxc, N4 | Header Enrichment of Uplink traffic is supported by the UP function. |
| 5/8 | TREU | Sxb, Sxc, N4 | Traffic Redirection Enforcement in the UP function is supported by the UP function. |
| 6/1 | EMPU | Sxa, Sxb, N4 | Sending of End Marker packets supported by the UP function. |
| 6/2 | PDIU | Sxa, Sxb, Sxc, N4 | Support of PDI optimised signalling in UP function (see clause 5.2.1A.2). |
| 6/3 | UDBC | Sxb, Sxc, N4 | Support of UL/DL Buffering Control |
| 6/4 | QUOAC | Sxb, Sxc, N4 | The UP function supports being provisioned with the Quota Action to apply when reaching quotas. |
| 6/5 | TRACE | Sxa, Sxb, Sxc, N4 | The UP function supports Trace (see clause 5.15). |
| 6/6 | FRRT | Sxb, N4 | The UP function supports Framed Routing (see IETF RFC 2865 [37] and IETF RFC 3162 [38]). |
| 6/7 | PFDE | Sxb, N4 | The UP function supports a PFD Contents including a property with multiple values. |
| 6/8 | EPFAR | Sxa, Sxb, Sxc, N4 | The UP function supports the Enhanced PFCP Association Release feature (see clause 5.18). |
| 7/1 | DPDRA | Sxb, Sxc, N4 | The UP function supports Deferred PDR Activation or Deactivation. |
| 7/2 | ADPDP | Sxa, Sxb, Sxc, N4 | The UP function supports the Activation and Deactivation of Pre-defined PDRs (see clause 5.19). |
| 7/3 | UEIP | N4 | The UPF supports allocating UE IP addresses or prefixes (see clause 5.21). |
| 7/4 | SSET | N4 | UPF support of PFCP sessions successively controlled by different SMFs of a same SMF Set (see clause 5.22). |
| 7/5 | MNOP | Sxa, Sxb, Sxc, N4 | UPF supports measurement of number of packets which is instructed with the flag 'Measurement of Number of Packets' in a URR. See also 5.2.2.2.1. |
| 7/6 | MTE | N4 | UPF supports multiple instances of Traffic Endpoint IDs in a PDI. |
| 7/7 | BUNDL | Sxa, Sxb, Sxc, N4 | PFCP messages bunding (see clause 6.5) is supported by the UP function. |
| 7/8 | GCOM | N4 | UPF support of 5G VN Group Communication. (See clause 5.23) |
| 8/1 | MPAS | N4 | UPF support for multiple PFCP associations to the SMFs in an SMF set (see clause 5.22.3). |
| 8/2 | RTTL | N4 | The UP function supports redundant transmission at transport layer. |
| 8/3 | VTIME | Sxb,N4 | UPF support of quota validity time feature. |
| 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.  Description: A clear textual description of the feature. | | | |

### 8.2.26 Apply Action

The Apply Action IE indicates the action(s) the UP function is required to apply to packets. It is coded as shown in Figure 8.2.26-1.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 44 (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 | Spare | Spare | Spare | DUPL | NOCP | BUFF | FORW | DROP |  | |
|  | 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | |  |

Figure 8.2.26-1: Apply Action

The octet 5 shall be encoded as follows:

- Bit 1 – DROP (Drop): when set to 1, this indicates a request to drop the packets.

- Bit 2 – FORW (Forward): when set to 1, this indicates a request to forward the packets.

- Bit 3 – BUFF (Buffer): when set to 1, this indicates a request to buffer the packets.

- Bit 4 – NOCP (Notify the CP function): when set to 1, this indicates a request to notify the CP function about the arrival of a first downlink packet being buffered.

- Bit 5 – DUPL (Duplicate): when set to 1, this indicates a request to duplicate the packets.

- Bit 6 to 8 – Spare, for future use and set to 0.

One and only one of the DROP, FORW and BUFF flags shall be set to 1.

The NOCP flag may only be set if the BUFF flag is set.

The DUPL flag may be set with any of the DROP, FORW, BUFF and NOCP flags.

### 8.2.27 Downlink Data Service Information

The Downlink Data Service Information IE is used to carry downlink data service information. It is coded as shown in Figure 8.2.27-1.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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  Bits 5 to 1 represent the binary coded timer value.  Timer unit  Bits 6 to 8 defines the timer value unit as follows:  Bits  **8 7 6**  0 0 0 value is incremented in multiples of 2 seconds  0 0 1 value is incremented in multiples of 1 minute  0 1 0 value is incremented in multiples of 10 minutes  0 1 1 value is incremented in multiples of 1 hour  1 0 0 value is incremented in multiples of 10 hours  1 1 1 value indicates that the timer is infinite  Other values shall be interpreted as multiples of 1 minute in this version of the protocol.  Timer unit and Timer value both set to all "zeros" shall be interpreted as an indication that the timer is stopped. |

### 8.2.30 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 49 (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 | Spare | Spare | Spare | Spare | Spare | QAURR | SNDEM | DROBU |  | |
|  | 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | |  |

Figure 8.2.31-1: 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 to 8 – Spare, for future use, shall be set to 0 by the sender and discarded by the receiver.

### 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 Figure 8.2.32-1.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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: Timerinformation element

|  |
| --- |
| Timer value  Bits 5 to 1 represent the binary coded timer value.  Timer unit  Bits 6 to 8 defines the timer value unit for the timer as follows:  Bits  **8 7 6**  0 0 0 value is incremented in multiples of 2 seconds  0 0 1 value is incremented in multiples of 1 minute  0 1 0 value is incremented in multiples of 10 minutes  0 1 1 value is incremented in multiples of 1 hour  1 0 0 value is incremented in multiples of 10 hours  1 1 1 value indicates that the timer is infinite  Other values shall be interpreted as multiples of 1 minute in this version of the protocol.  Timer unit and Timer value both set to all "zeros" shall be interpreted as an indication that the timer is stopped. |

### 8.2.36 Packet Detection Rule ID (PDR ID)

The PDR ID IE is coded as depicted in Figure 8.2.36-1.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 60 (decimal) | | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | | |  |
|  | 5 | Spare | | | | | Node ID Type | | | | |  |
|  | 6 to o | Node ID value | | | | | | | | | |  |
|  | m to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | | |  |

Figure 8.2.38-1: Node ID

Node ID Type indicates the type of the Node ID value. It shall be encoded as a 4 bits binary integer as specified in Table 8.2.38-2.

Table 8.2.38-2: Node ID Type

|  |  |
| --- | --- |
| Node ID Type Value (Decimal) | Node ID Type |
| 0 | IPv4 address |
| 1 | IPv6 address |
| 2 | FQDN |
| 3 to 15 | Spare, for future use. |

If the Node ID is an IPv4 address, the Node ID value length shall be 4 Octet.

If the Node ID is an IPv6 address, the Node ID value length shall be 16 Octet.

If the Node ID is an FQDN, the Node ID value encoding shall be identical to the encoding of a FQDN within a DNS message of 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.x 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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 8.2.39-3. The encoding of URL 2, 3 up to m fields are the same as the URL field.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | |  |
|  | Octets | 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 | | | | | | | 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.

- 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 to 8: Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

### 8.2.42 Measurement Period

The Measurement Period IE contains the period, in seconds, for generating periodic usage reports. It shall be encoded as shown in Figure 8.2.42-1.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 64 (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 to 8 | Measurement Period | | | | | | | | |  |
|  | 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | |  |

Figure 8.2.42-1: Measurement Period

The Measurement Period field shall be encoded as an Unsigned32 binary integer value.

### 8.2.43 Fully qualified PDN Connection Set Identifier (FQ-CSID)

A fully qualified PDN Connection Set Identifier (FQ-CSID) identifies a set of PDN connections belonging to an arbitrary number of UEs on a SGW-C, PGW-C, SGW-U and PGW-U. The FQ-CSID is used on Sxa and Sxb interfaces.

The size of CSID is two octets. The FQ-CSID is coded as follows:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 65 (decimal) | | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | | |  |
|  | 5 | FQ-CSID Node-ID Type | | | | | Number of CSIDs= m | | | | |  |
|  | 6 to p | Node-Address | | | | | | | | | |  |
|  | (p+1) to (p+2) | First PDN Connection Set Identifier (CSID) | | | | | | | | | |  |
|  | (p+3) to (p+4) | Second PDN Connection Set Identifier (CSID) | | | | | | | | | |  |
|  | ... | ... | | | | | | | | | |  |
|  | q to q+1 | m-th PDN Connection Set Identifier (CSID) | | | | | | | | | |  |
|  | (q+2) to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | | |  |

Figure 8.2.43-1: FQ-CSID

Where FQ-CSID Node-ID Type values are:

0 indicates that Node-Address is a global unicast IPv4 address and p = 9.

1 indicates that Node-Address is a global unicast IPv6 address and p = 21.

2 indicates that Node-Address is a 4 octets long field with a 32 bit value stored in network order, and p= 9. The coding of the field is specified below:

- Most significant 20 bits are the binary encoded value of (MCC \* 1000 + MNC).

- Least significant 12 bits is a 12 bit integer assigned by an operator to an MME, SGW-C, SGW-U, PGW-C or PGW-U. Other values of Node-Address Type are reserved.

Values of Number of CSID other than 1 are only employed in the PFCP Session Deletion Request.

The node that creates the FQ-CSID (i.e. SGW-C for SGW-C FQ-CSID, SGW-U for SGW-U FQ-CSID, PGW-C for PGW-C FQ‑CSID and PGW-U for PGW-U FQ‑CSID) needs to ensure that the Node-ID is globally unique and the CSID value is unique within that node.

### 8.2.44 Volume Measurement

The Volume Measurement IE contains the measured traffic volumes. It shall be encoded as shown in Figure 8.2.44-1.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 71 (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 to 8 | Quota Holding Time value | | | | | | | | |  |
|  | 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | |  |

Figure 8.2.48-1: Quota Holding Time

The Quota Holding Time value shall be encoded as an Unsigned32 binary integer value.

### 8.2.49 Dropped DL Traffic Threshold

The Dropped DL Traffic Threshold IE type shall be encoded as shown in Figure 8.2.49-1. It contains the dropped DL traffic volume thresholds to be monitored by the UP function.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | | 1 | |  | | |
|  | 1 to 2 | Type = 72 (decimal) | | | | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | | | | |  |
|  | 5 | Spare | | | | | | | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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) |
| 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]).  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). | |

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. 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. 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. Otherwise it shall not be present. When present, it shall contain the destination IPv6 address to set in the IPv6 header of the outgoing packet.

The Port Number field shall be present if the Outer Header Creation Description requests the creation of a UDP/IP header (i.e. it is set to the value 4). Otherwise it shall not be present. When present, it shall contain the destination Port Number to set in the UDP header of the outgoing packet.

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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 89 (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 | Supported-Features | | | | | | | | |  |
|  | 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | |  |

Figure 8.2.58-1: CP Function Features

The CP Function Features IE takes the form of a bitmask where each bit set indicates that the corresponding feature is supported. Spare bits shall be ignored by the receiver. The same bitmask is defined for all PFCP interfaces.

The following table specifies the features defined on PFCP interfaces and the interfaces on which they apply.

Table 8.2.58-1: CP Function Features

|  |  |  |  |
| --- | --- | --- | --- |
| Feature Octet / Bit | Feature | Interface | Description |
| 5/1 | LOAD | Sxa, Sxb, Sxc, N4 | Load Control is supported by the CP function. |
| 5/2 | OVRL | Sxa, Sxb, Sxc, N4 | Overload Control is supported by the CP function. |
| 5/3 | EPFAR | Sxa, Sxb, Sxc, N4 | The CP function supports the Enhanced PFCP Association Release feature (see clause 5.18). |
| 5/4 | SSET | N4 | SMF support of PFCP sessions successively controlled by different SMFs of a same SMF Set (see clause 5.22). |
| 5/5 | BUNDL | Sxa, Sxb, Sxc, N4 | PFCP messages bunding (see clause 6.5) is supported by the CP function. |
| 5/6 | MPAS | N4 | SMF support for multiple PFCP associations from an SMF set to a single UPF (see clause 5.22.3). |
| 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.  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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | | 4 | | 3 | | 2 | | 1 | |  | |
|  | 1 to 2 | Type = 93 (decimal) | | | | | | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | | | | | | |  |
|  | 5 | Spare | | | | CH | | IPv6D | | S/D | | V4 | | V6 | |  |
|  | m to (m+3) | IPv4 address | | | | | | | | | | | | | |  |
|  | p to (p+15) | IPv6 address | | | | | | | | | | | | | |  |
|  | r | IPv6 Prefix Delegation Bits | | | | | | | | | | | | | |  |
|  | 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" and the CH bit is not set, then the IPv6 address field shall be present in the UE IP Address, otherwise the IPv6 address field shall not be present.

- Bit 2 – V4: If this bit is set to "1" and the CH bit is not set, then the IPv4 address field shall be present in the UE IP Address, otherwise the IPv4 address field shall not be present.

- Bit 3 – S/D: This bit is only applicable to the UE IP Address IE in the PDI IE. It shall be set to "0" and ignored by the receiver in IEs other than PDI IE. In the PDI IE, if this bit is set to "0", this indicates a Source IP address; if this bit is set to "1", this indicates a Destination IP address.

- Bit 4 – IPv6D: This bit is only applicable to the UE IP address IE in the PDI IE and when V6 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 – CH (CHOOSE): If this bit is set to "1", then the IPv4 address and IPv6 address fields shall not be present and the UP function shall assign 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 6 to 8 Spare, for future use and set to 0.

Octets "m to (m+3)" or "p to (p+15)" (IPv4 address / IPv6 address fields), if present, shall contain the address value.

Octet r, if present, shall contain the number of bits allocated for IPv6 prefix delegation, e.g. if /60 prefix is used, the value is set to "4". When using UE IP address IE in a PDI to match the packets, the UP function shall only use the IPv6 prefix part and ignore the interface identifier part.

### 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | | 1 | |  | | | |
|  | 1 to 2 | Type = 94 (decimal) | | | | | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | | | | | |  |
|  | 5 | Spare | | | | | | | DLPR | | ULPR | | |  | |
|  | m | Spare | | | | | Uplink Time Unit | | | | | |  | | |
|  | (m+1) to (m+2) | Maximum Uplink Packet Rate | | | | | | | | | | | | |  |
|  | p | Spare | | | | | Downlink Time Unit | | | | | |  | | |
|  | (p+1) to (p+2) | Maximum Downlink Packet Rate | | | | | | | | | | | | |  |
|  | q to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | | | | | |  |

Figure 8.2.63-1: Packet Rate

The following flags are coded within Octet 5:

- Bit 1 – ULPR (Uplink Packet Rate): If this bit is set to "1", then octets m to (m+2) shall be present, otherwise these octets shall not be present.

- Bit 2 – DLPR (Downlink Packet Rate): If this bit is set to "1", then octets p to (p+2) shall be present, otherwise these octets shall not be present.

- Bit 3 to 8: Spare, for future use and set to 0.

At least one bit in Octet 5 shall be set to 1. Several bits may be set to 1.

When present, octets m to (m+2) indicate the maximum number of uplink packets allowed to be sent within the uplink time unit.

When present, octets p to (p+2) indicate the maximum number of downlink packets allowed to be sent within the downlink time unit.

Table 8.2.63.1: Uplink/Downlink Time Unit

|  |
| --- |
| Uplink/Downlink Time unit  Bits 1 to 3 define the time unit as follows:  Bits  **3 2 1**  0 0 0 minute  0 0 1 6 minutes  0 1 0 hour  0 1 1 day  1 0 0 week  Other values shall be interpreted as 000 in this version of the protocol. |

The Maximum Uplink/Downlink Packet Rate shall be encoded as an Unsigned16 binary integer value. They shall indicate the maximum number of uplink/downlink packets allowed to be sent in the indicated uplink/downlink time unit respectively.

### 8.2.64 Outer Header Removal

The Outer Header Removal IE type shall be encoded as shown in Figure 8.2.64-1. It contains the instructions to remove an Outer Header.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 95 (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 | Outer Header Removal Description | | | | | | | | |  |
|  | 6 | 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) | 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 S-TAG (See NOTE 5) | 7 |
| S-TAG and C-TAG (See NOTE 5) | 8 |
| For future use. Shall not be sent. If received, shall be interpreted as the value "1". | 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.  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.  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]).  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.  NOTE 5: This value may apply to DL packets received by a UPF over N6 for Ethernet PDU sessions over (see clause 5.8.2.11.3 of 3GPP TS 23.501 [28]).  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]). | |

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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | | 4 | | 3 | | 2 | | 1 |  | |
|  | 1 to 2 | Type = 100 (decimal) | | | | | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | | | | | |  |
|  | 5 | Spare | | | | 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.

- Bits 6 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, 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | |  | |
|  | 1 to 2 | Type = 101 (decimal) | | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | | |  |
|  | 5 | Spare | | | | | | | | UPFR | |  |
|  | 6 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | | |  |

Figure 8.2.69-1: Node Report Type

Octet 5 shall be encoded as follows:

- Bit 1 – UPFR (User Plane Path Failure Report): when set to 1, this indicates a User Plane Path Failure Report.

- Bit 2 to 8 – Spare, for future use and set to 0.

At least one bit shall be set to 1. Several bits may be set to 1.

### 8.2.70 Remote GTP-U Peer

The Remote GTP-U Peer IE shall be encoded as depicted in Figure 8.2.70-1.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | |  |
|  | Octets | 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 specified in clause 8.2.24.

The Network Instance field, when present, shall be encoded as the same as Network Instance IE 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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 Periodinformation element

|  |
| --- |
| Timer value  Bits 5 to 1 represent the binary coded timer value.  Timer unit  Bits 6 to 8 defines the timer value unit for the timer as follows:  Bits  **8 7 6**  0 0 0 value is incremented in multiples of 2 seconds  0 0 1 value is incremented in multiples of 1 minute  0 1 0 value is incremented in multiples of 10 minutes  0 1 1 value is incremented in multiples of 1 hour  1 0 0 value is incremented in multiples of 10 hours  1 1 1 value indicates that the timer is infinite  Other values shall be interpreted as multiples of 1 minute in this version of the protocol.  Timer unit and Timer value both set to all "zeros" shall be interpreted as an indication that the timer is stopped. |

### 8.2.79 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 114 (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 | Spare | | | Rule ID Type | | | | | |  |
|  | 6 to p | Rule ID value | | | | | | | | |  |
|  | (p+1) to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | |  |

Figure 8.2.80-1: Failed Rule ID

The Rule ID Type shall be encoded as a 5 bits binary integer value as specified in Table 8.2.80-1.

Table 8.2.80-1: Rule ID Type

|  |  |
| --- | --- |
| Rule ID Type | Value (Decimal) |
| PDR | 0 |
| FAR | 1 |
| QER | 2 |
| URR | 3 |
| BAR | 4 |
| For future use. Shall not be sent. If received, shall be interpreted as the value "1". | 5 to 31 |

The length and the value of the Rule ID value field shall be set as specified for the PDR ID, FAR ID, QER ID, URR ID and BAR ID IE types respectively.

### 8.2.81 Time Quota Mechanism

The Time Quota Mechanism type shall be encoded as shown in Figure 8.2.81-1.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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 User Plane IP Resource Information

The User Plane IP Resource Information IE type shall be encoded as shown in Figure 8.2.82-1.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 116 (decimal) | | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | | |  |
|  | 5 | Spare | ASSOSI | ASSONI | TEIDRI | | | | V6 | V4 |  | |
|  | 6 | TEID Range | | | | | | | | | |  |
|  | m to (m+3) | IPv4 address | | | | | | | | | |  |
|  | p to (p+15) | IPv6 address | | | | | | | | | |  |
|  | k to l | Network Instance | | | | | | | | | |  |
|  | r | Spare | | | | | Source Interface | | | | |  |
|  | s to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | | |  |

Figure 8.2.82-1: User Plane IP Resource Information

The following flags are coded within Octet 5:

- Bit 1 – V4: If this bit is set to "1", then the IPv4 address field shall be present, otherwise the IPv4 address field shall not be present.

- Bit 2 – V6: If this bit is set to "1", then the IPv6 address field shall be present, otherwise the IPv6 address field shall not be present.

- Bit 3-5 – TEID Range Indication (TEIDRI): the value of this field indicates the number of bits in the most significant octet of a TEID that are used to partition the TEID range, e.g. if this field is set to "4", then the first 4 bits in the TEID are used to partition the TEID range.

- Bit 6 – Associated Network Instance (ASSONI): if this bit is set to "1", then the Network Instance field shall be present, otherwise the Network Instance field shall not be present.

- Bit 7 – Associated Source Interface (ASSOSI): if this bit is set to "1", then the Source Interface field shall be present, otherwise the Source Interface field shall not be present.

- Bit 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".

If both the ASSONI and ASSOSI flags are set to "0", this shall indicate that the User Plane IP Resource Information provided can be used by CP function for any Network Instance and any Source Interface of GTP-U user plane in the UP function.

Octet 6 (TEID Range) shall be present if the TEID Range Indication is not set to zero and shall contain a value of the bits which are used to partition the TEID range. E.g. if the TEID Range Indication is set to "4", then Octet 6 shall be one of values between 0 and 15. When TEID Range Indication is set to zero, the Octet 6 shall not be present, the TEID is not partitioned, i.e. all TEID values are available for use by the CP function.

Octets "m to (m+3)" and/or "p to (p+15)" (IPv4 address / IPv6 address fields), if present, shall contain the respective IP address values.

Octets "k to l", if present, shall contain a Network Instance value as encoded in octet "5 to n+4" of the Figure 8.2.4-1 in clause 8.2.4, identifying a Network Instance with which the IP address or TEID Range is associated.

Octet r, if present, shall contain a Source Interface value as encoded in octet 5 of the Figure 8.2.2-1 in clause 8.2.2, identifying the Source Interface with which the IP address or TEID Range is associated.

### 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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 RQI IE shall be encoded as shown in Figure 8.2.88-1. It indicates if Reflective QoS applies for the UL.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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 specified in 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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).

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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 Number of Additional Usage Reports 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 number of usage reports which need to be sent in additional PFCP Session Report Request messages, in response to a PFCP Session Modification Request querying URR(s).

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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 a MAC address value.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | | |  |
|  | Octets | 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 a MAC address value (12-digit [hexadecimal numbers](https://www.lifewire.com/working-with-binary-and-hexadecimal-numbers-816247)).

### 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].

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | | | |  |
|  | Octets | 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]

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | | | |  |
|  | Octets | 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 V-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].

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | | 3 | | 2 | | 1 | |  | |
|  | 1 to 2 | Type = 141 (decimal) | | | | | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | | | | | |  |
|  | 5 | Spare | | | | | 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 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 to 8: Spare, for future use and set to 0.

One or more flags may be set to 1.

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 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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 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](https://www.lifewire.com/working-with-binary-and-hexadecimal-numbers-816247).

### 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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 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](https://www.lifewire.com/working-with-binary-and-hexadecimal-numbers-816247).

### 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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 | | | | | | | | |  |
|  | 13 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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 | | | | | | | | |  |
|  | 13 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  | |
|  | Octets | 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.z-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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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 | | | | | | | | |  |
|  | 13 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 149 (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 to 8 | Event Threshold | | | | | | | | |  |
|  | 13 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 Event Time Stamp

The Event Time Stamp IE indicates the time stamp when the event occurs in a given usage report. It shall be encoded as shown in Figure 8.2.114-1.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  | |
|  | 1 to 2 | Type = 156 (decimal) | | | | | | | | |  |
|  | 3 to 4 | Length = n | | | | | | | | |  |
|  | 5 to 8 | Event Time Stamp | | | | | | | | |  |
|  | 9 to (n+4) | These octet(s) is/are present only if explicitly specified | | | | | | | | |  |

Figure 8.2.114-1: Event Time Stamp

The Event 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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 | 1 |
| S4-U | 2 |
| S11-U | 3 |
| S12-U | 4 |
| Gn/Gp-U | 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 | 15 |
| SGi | 16 |
| N6 | 17 |
| N19 | 18 |
| Spare | 19 to 64 |

### 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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 to be used in a MAR.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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 Functionality

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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | |  |
|  | Octets | 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 |
| High | 2 |
| Low | 3 |
| Spare | 4 to 15 |

### 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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]).

### 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.x-1.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | |  |
|  | Octets | 8 | 7 | 6 | 5 | 4 | 3 | 2 | | 1 | |  | | |
|  | 1 to 2 | Type = 178 (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 8.2.129-1: 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 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.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | |  |
|  | Octets | 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.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Bits | | | | | | | | |  |
|  | Octets | 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.

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 a IPv6 prefix is received in the PDN Address Allocation (PAA) IE in the Create Session Request, e.g. static address assignment in the user subscription, the PGW-C shall select a PGW-U which can support the requested UE's IP address and/or IPv6 prefix.

Otherwise, the PGW-C shall determine the list of candidate PGW-Us taking into account the requested APN.

The PGW-C shall select, among the candidate PGW-U functions, a PGW-U function which supports all the capabilities required for the particular UE session, considering the information received during the 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 an 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 an 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 an 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 an 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 an 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 an 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 an Sx 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 an Sx Session Report Request to the CP function with a Usage Report IE including the Usage Report Trigger set to "Volume Quota" and the Volume Measurement set to 50 Mbytes.

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 an 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 the CP function due to reaching the Quota 100. So the UP function sends an 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 an 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 an 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 an 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 an 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 an 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 an 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 information 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 include the rules related to the UL and DL traffic to offload via PSA2. The I-SMF shall generate on its own N4 information towards the UL CL/BP for UL and DL traffic exchanged between the AN and PSA1.

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 [x]. 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, and in the latter case, the DNAI to which the PFCP session related message relates to.

## 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 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".

Editor's Note: It is FFS how to let the I-SMF know the identity of the Local PSA towards which the UL traffic is to be forwarded, when more than one Local PSA is inserted by the I-SMF for the PDU session.

- 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: 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 "Core";

- 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 "Core"; the DL FAR shall not contain the Outer Header Creation IE.

NOTE: 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.

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/BO 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;

- 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 Responses to the SMF.

### 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 X.2.1 and X.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.

Annex E (Informative):  
Change history

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **New** |
| 2016-07 | CT4#74 | C4-164286 |  |  | First version after CT4#74 | 0.1.0 |
| 2016-10 | CT4#74bis | 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#75bis | 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 |  | 269 | 3 | Validity time in Create URR IE | 16.1.0 |