



## **Ultra Cloud Core 5G Session Management Function, Release 2021.01 - Configuration and Administration Guide**

**First Published:** 2021-03-12

**Last Modified:** 2021-05-13

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



## CONTENTS

---

### PREFACE

<a href="#">About this Guide</a>	<a href="#">xlv</a>
<a href="#">Conventions Used</a>	<a href="#">xlv</a>

---

### CHAPTER 1

<a href="#">5G Architecture</a>	<a href="#">1</a>
<a href="#">Feature Summary and Revision History</a>	<a href="#">1</a>
<a href="#">Summary Data</a>	<a href="#">1</a>
<a href="#">Revision History</a>	<a href="#">1</a>
<a href="#">Overview</a>	<a href="#">2</a>
<a href="#">Control Plane Network Functions</a>	<a href="#">2</a>
<a href="#">User Plane Network Function</a>	<a href="#">2</a>
<a href="#">Subscriber Microservices Infrastructure Architecture</a>	<a href="#">3</a>
<a href="#">Control Plane Network Function Architecture</a>	<a href="#">4</a>

---

### CHAPTER 2

<a href="#">5G SMF Overview</a>	<a href="#">7</a>
<a href="#">Feature Summary and Revision History</a>	<a href="#">7</a>
<a href="#">Summary Data</a>	<a href="#">7</a>
<a href="#">Revision History</a>	<a href="#">7</a>
<a href="#">Product Description</a>	<a href="#">8</a>
<a href="#">Converged Core Overview</a>	<a href="#">9</a>
<a href="#">Use Cases and Features</a>	<a href="#">9</a>
<a href="#">Base SMF Configuration</a>	<a href="#">10</a>
<a href="#">4G Session Support</a>	<a href="#">10</a>
<a href="#">5G Session Support</a>	<a href="#">10</a>
<a href="#">Access and Mobility Support</a>	<a href="#">11</a>
<a href="#">Charging Integration</a>	<a href="#">12</a>
<a href="#">Cloud Native Infrastructure</a>	<a href="#">12</a>

Converged Core Network	12
IMS Support	13
IPAM Support	13
Lawful Intercept	13
MVNO Support	13
NF Management	14
OAM Support	14
Policy Integration	15
RADIUS Support	15
Roaming Support	15
SMF Inline Services	15
SMF Specification Compliance	16
Subscription Management	16
UPF Integration	16
WiFi Support	16
Deployment Architecture and Interfaces	17
SMF Architecture	17
SMF Deployment	17
Converged Core Architecture	18
Converged Core Deployment	18
Supported Interfaces	19
Life Cycle of Data Packet	20
License Information	24
Standards Compliance	24
Limitations	25
<hr/>	
<b>CHAPTER 3</b>	<b>Deploying and Configuring SMF through Ops Center</b> 27
	Feature Summary and Revision History 27
	Summary Data 27
	Revision History 27
	Feature Description 28
	SMF Ops Center 28
	Prerequisites 29
	Converged Core Refactoring Changes 29

Deploying and Accessing SMF	29
Deploying SMF	29
Accessing the SMF Ops Center	29
Day 0 Configuration	30
SMF Service Configuration	32
Configuring Pod-level Labels	32
Loading Day 1 Configuration	33
Day1 config.cli	34

---

**CHAPTER 4**
**Smart Licensing 35**

Feature Summary and Revision History	35
Summary Data	35
Revision History	35
Smart Software Licensing	35
Cisco Software Central	36
Smart Accounts/Virtual Accounts	36
Request a Cisco Smart Account	36
SMF Smart Licensing	37
Software Tags and Entitlement Tags	37
Configuring Smart Licensing	38
Users with Access to CSC	38
Users without Access to CSC	43
Monitoring and Troubleshooting Smart Licensing	48

---

**CHAPTER 5**
**SMF Rolling Software Update 49**

Feature Summary and Revision History	49
Summary Data	49
Revision History	49
Introduction	49
Updating SMF	51
Rolling Software Update Using SMI Cluster Manager	51
Prerequisites	52
Triggering the Rolling Software Upgrade	56
Monitoring the Upgrade	57

Viewing the Pod Details 58

---

**CHAPTER 6**

**Pods and Services Reference 61**

Feature Summary and Revision History 61

Summary Data 61

Revision History 61

Feature Description 62

Pods 63

Services 65

Open Ports and Services 68

Converged Core Refactoring Changes 69

Associating Pods to the Nodes 69

Viewing the Pod Details and Status 70

States 70

---

**CHAPTER 7**

**3GPP Specification Compliance for SMF Interfaces 73**

Feature Summary and Revision History 73

Summary Data 73

Revision History 73

Feature Description 74

Standards Compliance 74

Configuring Interfaces 75

Sample Configuration 76

---

**CHAPTER 8**

**4G to 5G Data Session Handover Support 79**

Feature Summary 79

Summary Data 79

Revision History 79

Feature Description 80

How it Works 80

Architecture 80

Call Flows 80

EPS to 5G Handover with N26 Interface – Preparation Call Flow 81

EPS to 5G Handover with N26 Interface – Execution Call Flow 83

UE Idle Mode Mobility from EPS to 5GS using N26 Interface	84
Standards Compliance	90
Limitations	90
Emergency SoS Support	91
Feature Description	91
How it Works	91
Configuring Emergency SoS Support	93
Configuring Local Authorization	94
Configuring Secondary Authentication	94
Configuring Charging Failure Handling	94

**CHAPTER 9****AN Modification Call Flow Support 97**

Feature Summary and Revision History	97
Summary Data	97
Revision History	97
Feature Description	98
How it Works	98

**CHAPTER 10****Application-based Alerts 105**

Feature Summary and Revision History	105
Summary Data	105
Revision History	105
Feature Description	106
Converged Core Refactoring Changes	106
How it Works	106
Configuring Alert Rules	106
Viewing Alert Logger	108
Call Flow Procedure Alerts	109
4G PDN Modify	109
4G PDN Release Success	109
4G PDN Setup Success	109
4G to 5G HO Success	110
4G To WiFi HO Success	110
5G N2 HO Success	111

5G PDU Idle Success	111
5G PDU Modify Success	111
5G PDU Release Success	111
5G PDU Setup Success	112
5G to 4G HO Success	112
5G To WiFi HO Success	112
5G Xn HO Success	113
PDN Session Create	113
PDU Session Create	113
PDU Session Modify	114
PDU Session Release	114
Interface Specific Alerts	115
GTPC Peer Down	115
N4 Message Success	115
N4 UPF Association Down	115
N4 UPF Association Up	116
N7 Interface Outbound	116
N7 Interface Inbound	116
N7 Message Timed Out	117
N10 Interface	117
N11 Interface Inbound	117
N11 Interface Outbound	118
N11 Message Timed Out	118
N40 Interface Inbound	118
N40 Interface Outbound	119
N40 Message Timed Out	119
NRF Discovery	119
SMF Service Start	120
IP Pool	120
IP Pool Used	120
Message Level Alerts	120
N11 SM Create	120
N11 SM Update	121
N11 SM Release	121



N1 N2 Message Transfer	121
N11 EBI Assignment	122
N11 SM Status Notify	122
N11 SM Context Retrieve	122
N7 SM Policy Create	123
N7 SM Policy Update	123
N7 SM Policy Delete	123
N7 SM Policy Notify Update	124
N7 SM Policy Notify Terminate	124
N10 UE Register	124
N10 UE DeRegister	125
N10 SM Subscription Fetch	125
N10 SM Subscribe for Notification	126
N10 Charging Data Request	126
N10 Charging Data Notify	126
Policy Rule Alerts	127
Addition of Dynamic PCC Rules	127
Modification of Dynamic PCC Rules	127
Removal of Dynamic PCC Rules	127
SMF Overload/Congestion	128
SMF Overload	128
SMF Sessions	128
Session Release Rate	128
Session Setup Failure	129
Session Setup Rate	129
Subscriber Limit	129

---

<b>CHAPTER 11</b>	<b>Bulk Statistics and Key Performance Indicators</b>	<b>131</b>
	Feature Summary and Revision History	131
	Summary Data	131
	Revision History	131
	Feature Description	131
	How it Works	132
	Supported KPIs	132

**CHAPTER 12**

**Cause Code Handling 143**

- Feature Summary and Revision History 143
  - Summary Data 143
  - Revision History 143
- Feature Description 143
- 5GSM Cause Code Handling 144
  - Feature Description 144
    - PDU Session Establishment Reject 144
    - PDU Session Modification Reject 145
    - PDU Session Release Reject 145
    - PDU Session Release Request 146
    - PDU Session Modification Command Reject 146
  - How it Works 147
    - Standards Compliance 147
  - Configuring the 5GSM Cause Handling Feature 147
  - 5GSM Cause Handling OAM Support 147
    - Statistics 147

**CHAPTER 13**

**Cisco Common Data Layer 151**

- Feature Summary and Revision History 151
  - Summary Data 151
  - Revision History 151
- Feature Description 152
  - Architecture 152
- How it Works 152
- Call Flows 153
  - CDL Endpoint Failure Call Flow 153
  - Limitations 154
- Configuring the CDL Through SMF Ops Center 154
  - Configuring the CDL Session Database and Defining the Base Configuration 154
  - Configuring the Zookeeper in CDL 155
    - Sample Configuration 156

---

<b>CHAPTER 14</b>	<b>CHF and PCF Integration for Access and Mobility Procedures</b>	<b>157</b>
	Feature Summary and Revision History	157
	Summary Data	157
	Revision History	157
	Feature Description	158
	How it Works	158
	Call Flows	159
	CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers Call Flow	159
	CHF and PCF Integration for N26 4G to 5G Handover Call Flow	161
	CHF and PCF Integration for N26 5G to 4G Handover Call Flow	163
	CHF and PCF Integration for Xn Handover Call Flow	165
	CHF and PCF Integration for Service Request Procedures	167
	Standards Compliance	168
<b>CHAPTER 15</b>	<b>Content Filtering, Event Detail Records, and X-Header Enrichment Support</b>	<b>169</b>
	Feature Summary and Revision History	169
	Summary Data	169
	Revision History	170
	Feature Description	170
	Converged Core Refactoring Changes	170
	Content Filtering Support	170
	Feature Description	170
	Configuring Content Filtering	171
	Configuring Content Filtering Support	171
	Event Data Record Logging Support	172
	Feature Description	172
	EDR Transaction File	173
	EDR Transaction Collision	188
	EDR Attributes	189
	Limitations	194
	Configuring EDRs	195
	Enable EDR Reporting	195
	Configure EDR Files for Generation	195

Configure EDR Parameters	196
Verifying EDR Transactions	196
OAM Support for EDR Logging	197
Bulk Statistics Support	197
Metadata Provided by SMF for EDR	198
X-Header Insertion Support	198
Supported X-Header Information	198
Bearer QCI Support	199
Feature Description	199

---

**CHAPTER 16**      **Customization of StarOS-based UPF on N4 Interface**    203

Feature Summary and Revision History	203
Summary Data	203
Revision History	203
Feature Description	204
Support for Prime PFD Message	204
Dynamic IP Pool Provisioning on UPF	205
Absence of NodeID Attribute from N4 Messages	205
Non Standard Attribute Type	205
Single QFI Support	205

---

**CHAPTER 17**      **Customized Configuration for Controlling Subscription Messages over N10**    207

Feature Summary and Revision History	207
Summary Data	207
Revision History	207
Feature Description	208
How it Works	208
Configuring Options for Controlling SDM Messages	208
Configuring RAT-type in DNN Profile	208

---

**CHAPTER 18**      **DNS Proxy Integration**    211

Feature Summary and Revision History	211
Summary Data	211
Revision History	211

Feature Description	212
Randomization of P-CSCF Addresses from DNS	212
How it Works	212
Call Flows	213
Configuring the DNS Proxy Feature	214
Configuring DNS Proxy Replica	214
Configuring DNS Proxy	215
Configuring P-CSCF Server Addresses	216
Configuring P-CSCF Server IPv4 Addresses	216
Configuring P-CSCF Server IPv6 Addresses	216
Configuring P-CSCF Server IPv4v6 Addresses	217
Verifying DNS Proxy Feature Configuration	217

**CHAPTER 19****DSCP Marking 219**

Feature Summary and Revision History	219
Summary Data	219
Revision History	219
Feature Description	219
DSCP Marking for User Plane Packets	220
Feature Description	220
How the DSCP Marking Works for Data Packets	220
Configuring 5QI-QoS Mapping	220
DSCP Marking for Control Plane Signaling	221
Feature Description	221
How the DSCP Marking Works for Control Signaling	222
Limitations	223
Configuring DSCP Marking for Control Plane Signaling	223
Configuring DSCP Marking per Endpoint	223
Configuring DSCP Marking per Interface	223

**CHAPTER 20****Emergency Services Support 225**

Summary Data	225
Revision History	225
Feature Description	225

How it Works	226
Configuring Emergency Service Support	228
Configuring Default Flow Only Timer in DNN Profile	228
Configuring Emergency DNN	228
Verifying Emergency DNN	229
OAM Support for SMF Emergency Services	230
Statistics	230
<hr/>	
<b>CHAPTER 21</b>	<b>EPS Interworking 231</b>
Feature Summary and Revision History	231
Summary Data	231
Revision History	232
Feature Description	232
Architecture	232
How it Works	233
Standards Compliance	234
Support for UE Initial Attach on E-UTRAN	234
Feature Description	234
How it Works	235
Converged Core Refactoring Changes	237
Configuring the UE Initial Attach Feature	237
Define FQDN in SMF Profile Configuration	237
Configure S5 Binding Address in SMF Service Configuration	237
Configuring GTP Endpoint Parameters	238
Verifying the UE Initial Attach Feature Configuration	238
Detach Procedure for EPS on SMF and P-GW	239
Feature Description	239
How it Works	239
Dedicated Bearer Activation and Deactivation	241
Feature Description	241
How it Works	241
EPS Fallback	247
Feature Description	247
How it Works	247

EPS Fallback Guard Timer Support	249
Feature Description	249
How It Works	249
Standards Compliance	251
Configuring the EPS Fallback Guard Timer	251
Indirect Data Forwarding Tunnel (IDFT) Timer Support	252
Feature Description	252
How it Works	252
Call Flows	252
Configuring the IDFT Timer	255
Bearer Modification for EPS Session on SMF	256
Feature Description	256
How it Works	256
Standards Compliance	263
Session Management Procedures for EPS and 5GC Interworking	263
Feature Description	263
How it Works	265
Call Flows	265
Standards Compliance	284
Limitations	285
Generating EPS PDN Connection Parameters from 5G PDU Session Parameters	285
5G to EPS Handover Using N26 Interface	286
Feature Description	286
How it Works	286
Standards Compliance	288
Create Dedicated Bearer Delay and Retry Support	288
Feature Description	288
How It Works	288
Call Flows	288
Configuring Create Dedicated Bearer Delay and Retry Support	290
Handling GTP-U Error Indication for 4G Sessions	291
Feature Description	291
Standards Compliance	291
How it Works	291

- GTP-U Error Handling Procedure 291
- GTP Path Failure Handling, Restoration, and Recovery 293
  - Feature Description 293
  - Call Flows 294
    - GTP-C Path Management 294
    - GTP-C Echo Request Handling 295
    - GTP-C Restoration on PGW-C/SMF 295
  - Memory and Performance Impact 296
  - Configuring Echo at GTP Endpoint 296
    - Sample Configuration 296
    - Show Command 297
  - Bulk Statistics 297
  - Limitations 297
- Configuration Support for Rejecting 4G-only Devices 298
- Dynamic Configuration Change Support 298
  - Feature Description 298
  - How it Works 298
    - Access Profile 298

---

**CHAPTER 22**      **Flow Failure Handling for Access and Mobility Procedures 301**

- Feature Summary and Revision History 301
  - Summary Data 301
  - Revision History 301
- Feature Description 302
  - How it Works 302
    - Call Flows 302
- Standards Compliance 321

---

**CHAPTER 23**      **Inter gNodeB Handover 323**

- Feature Summary and Revision History 323
  - Summary Data 323
  - Revision History 323
- Feature Description 324
  - How it Works 324



Call Flows	324
Xn-based Inter NG-RAN Handover	324
N2-based Inter NG-RAN Handover	327
Limitations	335
OAM Support	336
Statistics Support	336

**CHAPTER 24****IP Address Management 337**

Feature Summary and Revision History	337
Summary Data	337
Revision History	338
Feature Description	338
How it Works	338
IPAM Integration in SMF	339
Feature Description	339
Architecture	339
IPAM Integration in SMF	339
Components	340
How it Works	341
Call Flows	341
Configuring the IPAM Feature	342
Configuring IPv4 Address Ranges	343
Configuring IPv6 Address Ranges	343
Configuring IPv6 Prefix Ranges	344
Configuring SMF Tags	345
Configuring IPv4 Threshold	345
Configuring IPv6 Address Range Threshold	346
Configuring IPv6 Prefix-Range Threshold	346
Configuring IPv4 Address Range Spilt	347
Configuring IPv6 Address and Prefix Address-Range-Spilt	348
Configuring Global Threshold	349
Configuring IPAM Source	349
Verifying the IPAM Integration Configuration	350
Static IP Support	352

- Feature Description **352**
- How it Works **352**
  - Call Flows **355**
  - Limitations **356**
- Configuring Static IP Support **356**
- Dual-Stack Static IP Support Through IPAM **357**
  - Feature Description **357**
  - How it Works **357**
    - Limitations **358**
  - Configuring Dual-Stack Static IP Support Using IPAM Feature **358**
    - Configuring IPAM No-Split **358**
- IPAM Offline Mode Support **358**
  - Feature Description **358**
  - Configuring the IPAM Offline Mode **359**
    - Configuring Pool to Offline Mode **359**
    - Configuring IPv4 Address-Range to Offline Mode **359**
    - Configuring IPv6 Prefix-Ranges to Offline Mode **360**
- IPAM Redundancy Support Per UPF **360**
  - Feature Description **360**
  - How it Works **361**
- IPAM Static IP Pool Enhancements **361**
  - Feature Description **361**
  - How it Works **362**
    - Adding a DNN **362**
    - Adding a Static IP Address Range **362**
    - Adding a Static IP Pool **362**
    - Adding the UPF **363**
    - Deleting the UPF **363**
    - Deleting a Static IP Address Range **364**
    - Deleting a Static IP Pool **364**
    - Removing Sx Association with an Offline UPF **364**
    - Sx Path Failure on UPF **365**
    - Limitations **365**
- IPAM Quarantine Timer Support **365**

Feature Description	365
Configuring the IPAM Quarantine Timer Support Feature	365
Configuring IPAM Quarantine Timer	365
show ipam pool	366
show ipam pool <pool-name>	366
show ipam pool <pool-name> ipv4-addr	367
show ipam pool <pool-name> ipv6-addr	367
show ipam pool <pool-name> ipv6-prefix	367
show ipam dp	367
show ipam dp <dataplane-name>	368
show ipam dp <dataplane-name> ipv4-address	368
show ipam dp <dataplane-name> ipv6-addr	368
show ipam dp <dataplane-name> ipv6-prefix	369
show ipam	369
Configuring IPAM Quarantine Qsize Support Feature	369
Configuring IPAM Quarantine Queue Size	369
Overlapping IP Address Pools Support	370
Feature Description	370
Configuring Overlapping IP Address Pools	370
Virtual Routing and Forwarding Function	371
Feature Description	371
Configuring VRF	371
Configuring VRF Name	372

---

**CHAPTER 25**
**Local Breakout-based Roaming Support 373**

Feature Summary and Revision History	373
Summary Data	373
Revision History	373
Feature Description	373
Architecture	374

---

**CHAPTER 26**
**Monitoring Support 385**

Feature Summary and Revision History	385
Summary Data	385

- Revision History **385**
- Monitor Subscriber and Monitor Protocol **386**
  - Feature Description **386**
    - Converged Core Refactoring Changes **386**
  - Configuring the Monitor Subscriber and Monitor Protocol Feature **386**
    - Monitoring the Subscriber **386**
    - Enabling or Disabling the Transaction Messages **387**
    - Viewing the Sorted File on SMF Ops Center **387**
    - Monitoring the Interface Protocol **387**
    - Viewing Transaction History Logs **388**
    - Sample Transaction Log **388**
- RPC Remote Host Management **392**
  - Feature Description **392**
  - RPC Remote Host Management OAM Support **392**
    - show-rpc **393**

---

**CHAPTER 27**

- Multiple and Virtual DNN Support 395**
  - Feature Summary and Revision History **395**
    - Summary Data **395**
    - Revision History **396**
  - Feature Description **396**
  - How It Works **397**
  - Limitations **398**
  - Configuring the Virtual DNN Feature **398**
    - Configuring Subscriber Policy **398**
      - show full **399**
    - Configuring Operator Policy and Associating a DNN Policy **399**
      - Verifying the Configuration **399**
    - Configuring a DNN Policy **399**
      - Verifying the Configuration **400**
    - Configuring a Virtual DNN under a DNN Profile **400**
      - Verifying the Configuration **400**
  - Associating Subscriber Policy under the SMF Service **400**
    - Verifying the Configuration **401**

DNN Profile Offline Mode Support	401
Feature Description	401
How it Works	401
DNN Policy	401
DNN Profile	401
Limitations	402
Configuring the DNN Profile Offline Mode Support Feature	403
Configuring the DNN Profile to Offline Mode	403
Verifying the DNN Profile Offline Mode Configuration	403
DNN Profile Offline Mode OAM Support	403
Statistics	403
Dynamic Configuration Change Support	404
Feature Description	404
How it Works	404
Limitations	405
Configuring Dynamic Configuration Change Support	405
Configuring the DNN Profile to Offline Mode	405
Dynamic Configuration Change OAM Support	406
Statistics	406
IP Pool Allocation per DNN	406
Feature Description	406
How it Works	407
Configuring IP Pool Allocation	408
Allocating the IP Pool per DNN	408

---

**CHAPTER 28**

<b>Multiple PLMN Support</b>	<b>409</b>
Feature Summary and Revision History	409
Summary Data	409
Revision History	409
Feature Description	410
How it Works	410
Configuring Multiple PLMN	410
Configuring Peer Network Function	410
Configuring PLMN ID	411

- Configuring PLMN List 411
- Configuring Primary PLMN 411
- Configuring PLMN in NRF Discovery 412
- Configuring Serving PLMN MNC list 412
- Configuring Roamer in Operator Policy 412

---

**CHAPTER 29**

**Network-initiated Messages Support 413**

- Feature Summary and Revision History 413
  - Summary Data 413
  - Revision History 413
- Feature Description 413
- How it Works 414
- Call Flows 414
  - Downlink Data Notification User Plane Activation Call Flow for UE in CM-Connected State 414
  - Downlink Data Notification User Plane Activation Call Flow for UE in CM-Idle State 416
  - Network-Initiated Modification Call Flow for Active User Plane and UE in CM-Connected State 418
  - Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Connected State 419
  - Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Idle State 420
- Limitations 421
- Standards Compliance 421
- OAM Support 421
- Statistics Support 422

---

**CHAPTER 30**

**Network-Initiated Service Request 423**

- Feature Summary and Revision History 423
  - Summary Data 423
  - Revision History 423
- Feature Description 423
- How it Works 424
- Call Flows 424
  - UE-initiated Idle to Active Transition 424

Network-initiated Idle to Active Transition	425
Network Initiated Service Request	428
Limitations	432
Configuring N3 Tunnel Profile	432

---

**CHAPTER 31**
**NRF Discovery 433**

Feature Summary and Revision History	433
Summary Data	433
Revision History	434
Feature Description	434
Architecture	434
How it Works	435
Call Flows	435
Standards Compliance	437
Limitations	437
NF Heartbeat Support	437
Feature Description	437
How it Works	437
Call Flows	437
Standards Compliance	439
Caching Support for NF Discovery	440
Feature Description	440
Relationships	440
How it Works	440
Call Flows	440
Standards Compliance	442
Limitations	442
NRF Support for SMF Subscription and Notification	443
Feature Description	443
How it Works	444
Call Flows	444
Limitations	447
Configuring NRF Support for SMF Subscription and Notification	448
NRF Interface per Endpoint	449

Feature Description	449
Standards Compliance	450
Limitations	450
Configuring the NRF Interface Per Endpoint	450
Associating a Discovery Group with NF Type	450
Configuring Locality for NF Types	451
Associating NRF Management and SMF Locality to NRF Endpoint	451
Configuring the NRF Endpoints Profile Parameters	452
Configuring Locality for SMF	454
Configuring NF Profiles for a DNN	454
Configuring Network Element Profile Parameters for the NF	454
NRF Failure Handling Support	456
Feature Description	456
How it Works	457
Call Flow	458
Verifying the NRF Failure Handling	460
NF Management Failure Handling	460
NF Discovery Failure Handling	461
Local Configuration for NF Management	461
Feature Description	461
Relationships	462
Standards Compliance	462
Limitations	462
Configuring the NFs for NF Discovery	462
Configuring Locality for SMF	462
Configuring NF Profiles for a DNN	463
Configuring Network Element Profile Parameters for the NF	463
Configuring NF Client Profile	464
Defining Locality within NF Profile	465
Configuring NF Endpoint Profile Parameters	466
Verifying the Local Configuration for NF Discovery Feature	468
Fallback to Static IP Address Support	469
Feature Description	469
Relationships	469



How it Works	469
Standards Compliance	472
Limitations	472
Configuring the Fallback to Static IP Address Support Feature	472
Configuring the Failure Template	472
Sample Configurations	472
Configuring NF Service and Message Type	473
Configuring NF Failure Retry, Action, and Message Type	475
Configuring Invalidate (Purge) NF Discovery Cache	476
NF Profile Update	476
Feature Description	476
How it Works	477
Standards Compliance	479
Limitations	479
Configuration Support for List of Tracking Areas and Tracking Area Ranges	479
Feature Description	479
Configuring TAI Group	480
Configuring TAC List	480
Configuring TAC Range List	480
Verifying the TAI Group Configuration	480
Dynamic Configuration Change Support	481
Feature Description	481
NRF Show Command Enhancements	481
show nrf registration-info	481
show nrf subscription-info	482
show nrf discovery info	482
show nrf discovery-info AMF discovery-filter	482
show nrf discovery-info AMF discovery-filter dnn=intershat nf-discovery-profile	482
show nrf discovery-info AMF discovery-filter dnn=intershat nf-discovery-profile f9882966-a253-32d1-8b82-c785b34a7cc9 nf-service	483
<b>CHAPTER 32</b>	<b>PDU Session Establishment from 4G-Only and Option 3x Capable Devices</b>
	485
Feature Summary and Revision History	485
Summary Data	485

Revision History	486
Feature Description	486
How it Works	487
Limitations	488
Standards Compliance	488
Configuring Support for Packet Data Unit Sessions Establishment from 4G-Only and Option 3x Capable Devices	489
Configuring the NSSAI	489
Configuring the Sessions as Dual Connectivity New Radio	489
Verifying the Dual Connectivity New Radio Capability Configuration	490
Configuring DCNR based UPF	490
Configuring Secondary RAT Usage Report	491
Configuring Presence Reporting	491
Packet Data Unit Sessions Establishment from 4G-Only and Option 3x Capable Devices OA&M Support	492
Statistics Support	492
Bulk Statistics	493

---

**CHAPTER 33**

<b>Peer NF Failure Handling Support</b>	<b>495</b>
Feature Summary and Revision History	495
Summary Data	495
Revision History	495
Feature Description	496
Offline Failover Support for Charging	496
Feature Description	496
How it Works	496
Selecting a CHF Server	496
Failure Handling Profile	497
HTTP Cause Code Mapping with Failure Actions	498
SMF Behaviour for Failure Actions	499
Standards Compliance	500
Limitations	500
Configuring the Offline Failover Support for Charging	500
Configuring Failure Handling Profile in an NF Library	500

Configuring an Offline Server Client and an Offline Failure Handling Profile	501
SMF Failover to Secondary PCF	502
Feature Description	502
SMF PCF Failure Handling	502
Configuring SMF Failover to Secondary PCF Support	504
Configuring the PCF Failure Handling Profile	504
Configuring the Association of Failure Handling Profile	504
Configuring Secondary and Tertiary IP Addresses	505
SMF Failover to Secondary PCF OAM Support	505
Statistics Support	505
Unified Data Management Failure Handling	506
Feature Description	506
How it Works	507
Configuring UDM Failure Handling Support	509
Configuring UDM Failure Handling Profile	509
Configuring Association of FH profile	509
Configuring Secondary and Tertiary IP Addresses	510
Configuring Response Timeout Handling	510
Statistics	511
UDM Failure Handling OAM Support	511
Statistics Support	511
User Plane Function Failure Handling	512
Feature Description	512
Configuring the UPF Failure Handling on N4 Interface	513
Configuring the Failure Profile Association	514
Configuration Matrix	515
<b>CHAPTER 34</b>	
<b>PDU RAN Tunnel Endpoint Identifier Session</b>	<b>517</b>
Feature Summary and Revision History	517
Summary Data	517
Revision History	517
Feature Description	518
How it Works	518
Deactivation of the User Plane Connection of a PDU Session	518

Activation of the User Plane Connection of a PDU Session	520
Always-On PDU Session Support	521
Feature Description	521
How it Works	522
Call Flows	522
Configuring Always-On PDU Session Support	525
Verifying Always-On PDU Session Support	526
Always-On PDU Session OAM Support	527
Bulk Statistics Support	527

---

**CHAPTER 35**
**Policy and User Plane Management 529**

Feature Summary and Revision History	529
Summary Data	529
Revision History	530
Feature Description	530
QoS Management on SMF	531
Feature Description	531
Use Cases	531
Subscribed QoS	534
QoS Negotiation	534
QoS Flow Management	536
QoS Communication on 3GPP Interfaces	537
QoS Modification	538
Handling of Authorized QoS for Default Bearer	538
Feature Description	538
How it Works	539
Default-Bearer QoS Handling for 4G and WiFi Sessions	539
Default-Bearer QoS Handling for 5G Sessions	539
Default-Bearer QoS Handling During WiFi Handovers	540
Default-Bearer QoS Modification During Failure Handling	540
Limitations	541
Authorized QoS Handling OAM Support	541
Statistics Support	541
SMF Affinity	541

Dynamic Configuration Change Support	542
Feature Description	542
How it Works	542
Configuring Dynamic Configuration Change Support	543
Verifying Dynamic Configuration Change Support Configuration	544
Dynamic PCC Rules Enforcement	544
Feature Description	544
Supported Features Negotiation	544
Provisioning and Management of Session AMBR and Default QoS	545
Provisioning of Policy Revalidation Time	546
Provisioning and Management of Additional QoS Flows	546
QoS Enforcement	548
Policy Control Request Triggers	548
Gating Control	549
How it Works	550
Standards Compliance	551
Limitations	552
Configuring the Dynamic PCC Rules Enforcement Feature	552
Creating QoS Profile	552
Configuring QoS Parameters	552
Defining QoS Profile in DNN Profile Configuration	553
Verifying the Dynamic PCC Rules Enforcement Feature Configuration	553
Troubleshooting Information	554
Static PCC Rules Support	554
Feature Description	554
Relationships	554
Converged Core Refactoring Changes	555
How it Works	555
Pre-processing During Configuration	555
During PDU Session Creation	556
During PDU Session Modification	556
Limitations	557
Configuring the Static PCC Rules Support	557
Configuring ACS	558

Configuring Charging Action	558
Configuring Packet Filter	560
Configuring ACS Ruledef	561
Configuring ACS Group of Ruledefs	563
Configuring Rulebase and Predefined Rule Prefix	563
Configuring ACS Rulebase (APN Configuration Mode)	564
Configuring URR ID	564
Configuring GTPP Group	564
Configuring Access Point Name (APN)	565
Associating GTPP Group with APN	565
Configuring ACS Rulebase (ACS Configuration Mode)	565
Defining UPF APN Profile in DNN Profile Configuration	567
Configuring QoS Parameters	568
Verifying the Static PCC Rules Support Feature Configuration	569
Predefined PCC Rules	570
Feature Description	570
Predefined Rules vs Static Rules	570
Combined Application of Static, Predefined, and Dynamic Rules	571
Support for Configuring the Bandwidth ID	571
Feature Description	571
Limitations	571
Configuring Bandwidth ID	571
Verifying Bandwidth ID Configuration	572
Generating UE Camping Report for PCF	573
Feature Description	573
UPF Node Selection	573
UPF Selection Based on Query Parameters	574
Feature Description	574
How it Works	574
Configuring the UPF Selection Feature	576
UPF Selection OA&M Support	582
Co-located UPF Selection During Initial EPS Attach	583
Feature Description	583
How it Works	583

Configuring Node ID	583
Statistics Support	584
Support for UPF Node Reports and Proprietary Session Reports	585
Feature Description	585
Converged Core Refactoring Changes	585
How it Works	585
PCFP Node Report Handling	585
PCFP Session Report Handling	586
Collision Handling	586
Resiliency Handling	586
Standards Compliance	586
Limitations	586
OAM Support	587
Monitoring Support	587
Show Command Support	587
Statistics Support	588
Support for Session Report Rejection Procedure	590
Feature Description	590
Relationships	591
Configuring FH Action for Handling Session Report Errors	591
Verifying the Feature Configuration	592
OAM Support	592
Statistics Support	592
Outer Header Format	592

---

**CHAPTER 36**

<b>RADIUS Client for SMF</b>	<b>595</b>
Feature Summary and Revision History	595
Summary Data	595
Revision History	596
Feature Description	596
Architecture	597
RADIUS Integration in Mobile CNAT Architecture	597
RADIUS Client Integration in SMF	597
RADIUS Authentication	598

RADIUS Accounting	599
RADIUS Access Management	599
RADIUS NAS-IP Support	599
Handling RADIUS Disconnect and CoA Requests	600
How it Works	601
RADIUS Interaction for Authentication	601
RADIUS Authentication Attributes	604
Call Flows	606
RADIUS Interaction for Accounting	607
RADIUS Accounting Attributes	607
Call Flows	610
Processing of Usage Reporting Rules	611
Dynamic Configuration Update	612
RADIUS Attribute Definition	612
Standards Compliance	620
Limitations and Restrictions	620
Configuring the RADIUS Client	621
Configuring RADIUS Server	621
Verifying the RADIUS Configuration	622
Configuring RADIUS Server Selection Logic	623
Configuring RADIUS Attributes	623
Configuring RADIUS Detect Dead Server	624
Configuring RADIUS Dead Time	624
Configuring RADIUS Retries	625
Configuring RADIUS Timeout	625
Configuring RADIUS Pod	626
Configuring RADIUS NAS-IP	626
Configuring Secondary Authentication Method	627
Verifying the RADIUS Authentication Configuration	628
Configuring PAP, CHAP, or MSCHAP-based Authentication	628
Defining Priority for Authentication Algorithm	628
Configuring Host Password	629
Enabling RADIUS Accounting	629
Defining RADIUS Server Group in DNN Profile	630



Configuring RADIUS Accounting Options	631
Configuring RADIUS Accounting Server Group	632
Verifying the RADIUS Accounting Configuration	632
Configuring the Session Disconnect Feature	632
Configuring the Dynamic Authorization Service	632
Configuring the CoA-NAS Interface	633
RADIUS Test CLI support	634
Testing a RADIUS Accounting Server	634
Testing a RADIUS Authentication Server	635
RADIUS Client OA&M Support	636
Statistics Support	636

---

**CHAPTER 37****RPC Remote Host Management** 643

Feature Summary and Revision History	643
Feature Description	643
RPC Remote Host Management OAM Support	643
show-rpc	643

---

**CHAPTER 38****Resource Management** 645

Feature Summary and Revision History	645
Summary Data	645
Revision History	645
Feature Description	645
How it Works	646
Call Flows	646
IP and ID Allocation	646
IP and ID Deallocation	647

---

**CHAPTER 39****Router Solicit and Router Advertisement** 649

Feature Summary and Revision History	649
Summary Data	649
Revision History	649
Feature Description	649
Unsolicited Router Advertisement	650

Solicited Router Advertisement	650
ICMPv6 Profile Configuration	651

---

**CHAPTER 40**

<b>Session and Service Continuity Mode</b>	<b>653</b>
Feature Summary and Revision History	653
Summary Data	653
Revision History	653
Feature Description	653
SSC Mode Selection	654
Priority for Choosing SSC Mode	654
SSC Mode Selection Method	654
Configuring SSC Mode	655

---

**CHAPTER 41**

<b>SMF Charging</b>	<b>657</b>
Feature Summary and Revision History	657
Summary Data	657
Revision History	657
Overview	658
Converged Charging	659
Chargeable Events	659
Charging Identifier	659
Charging Information	659
How it Works	660
Charging Session	660
Offline Charging and Online Charging	660
CHF Selection	662
Charging Activities at SMF	663
Static and Predefined Rules for Charging	666
Modification Scenarios in Charging	666
URR Linking	667
Local Configuration	668
Zero Usage Report Suppression	668
Call Flows	669
Limitations	670

Standards Compliance	670
3GPP June 2019 Compliance for Charging Interface	670
Configuring SMF Charging	671
DNN Profile Configuration	671
Charging Characteristics Profile Configuration	671
Charging Profile Configuration	672
Configuring Zero Usage Report Suppression	674
Static PCC Rules Configuration	674
Mapping of Charging Scenario on Various Interfaces	675
Feature Description	675
How it Works	675
Limitations	681
Standards Compliance	681
Error Handling Scenarios	681
Application Error and Result Code Handling	682
Application Error Codes	682
RG-level Result Codes	683
CHF Server Reconciliation	684
Dynamic Configuration Change Support	685
Feature Description	685
How it Works	685
ACS Profile	685
Charging Profile	688

---

**CHAPTER 42**

<b>SMF Deregistration with NRF</b>	<b>693</b>
Feature Summary and Revision History	693
Summary Data	693
Revision History	693
Feature Description	693
How it Works	694
Call Flows	694
NF Deregistration Call Flow	694
NF Deregistration Trigger Events Call Flow	695
Standards Compliance	696

Limitations 696

---

**CHAPTER 43**

**SMF Overload Management 697**

Feature Summary and Revision History 697

Summary Data 697

Revision History 697

Feature Overview 698

SBA Interface Overload Control 698

Feature Description 698

How it Works 698

Message Priority 698

Overload Protection at Endpoint 699

Configuring Overload Protection 699

Configuring Overload Protection at Endpoint Level 699

Configuring Overload Protection at Client Level 700

Verifying the Overload Protection Configuration 701

Configuring the Message Priority 701

Monitoring and Troubleshooting 702

Statistics 702

---

**CHAPTER 44**

**Support for the Unsubscribe-To-Notifications Messages 705**

Feature Summary and Revision History 705

Summary Data 705

Revision History 705

Feature Description 706

How it Works 706

Standards Compliance 706

Call Flows 706

Unsubscribe-to-Notifications Call Flow 706

OAM Support for the Unsubscribe-To-Notifications Messages 707

Statistics Support 707

---

**CHAPTER 45**

**SMF Interface for Metrics 709**

Feature Summary and Revision History 709

Summary Data	709
Revision History	709
Feature Description	709
SMF Rest EP Microservice	710
Counters	710
Labels	710
SMF Service	711
Labels	711
SMF Protocol Microservice	712
Counters	712
Labels	713
Converged Core Refactoring Changes	714

---

**CHAPTER 46****System Logging Support Per SUPI 715**

Feature Summary and Revision History	715
Feature Description	715
Configuration Support for Persistent Transaction Logs	720
Configuring the Persistent Transaction Logs	720
Viewing the Transaction Logs	720

---

**CHAPTER 47****TAI Selection from AMF 723**

Feature Summary and Revision History	723
Summary Data	723
Revision History	723
Feature Description	723
How it Works	724
Architecture	724
Configuring TAI Selection from AMF	740
Configuring TAI Group List	740
Verifying TAI Group List	741
Configuring Priority in SMF Info	741
Verifying Priority in SMF Info	741

---

**CHAPTER 48****Timers Support 743**

- Feature Summary and Revision History **743**
  - Summary Data **743**
  - Revision History **743**
- Feature Description **743**
- 3GPP-compliant Timers **744**
  - GTP and N11 Timers Support **744**
    - Feature Description **744**
    - How it Works **744**
    - Configuring the GTP and N11 Timers **745**
- Custom-driven Timers **746**
  - Absolute Timer Support **746**
    - Feature Description **746**
    - Configuring Absolute Session Timeout **747**
  - Inactivity Timer Support **747**
    - Feature Description **747**
    - Configuring UP Inactivity Timer **747**
    - Configuring CP and UP Session Idle Timer **748**

---

**CHAPTER 49**

**UDP Proxy for SMF 749**

- Feature Summary and Revision History **749**
  - Summary Data **749**
  - Revision History **749**
- Feature Description **749**
  - Relationships **750**
  - Architecture **750**
  - How it Works **751**
    - Port and Sequence Number Selection **751**
    - Protocol POD Selection for Peer Initiated Messages **752**
    - High Availability for the UDP Proxy **752**
    - Call Flows **752**

---

**CHAPTER 50**

**UPF Path Management and Restoration 755**

- Feature Summary and Revision History **755**
  - Summary Data **755**

Revision History	755
Feature Description	756
Standards Compliance	756
Converged Core Refactoring Changes	756
How it Works	756
Configuration Support for UPF Path Management and Restoration	757
Configuring the Heartbeat Parameters for UPF	757
Verifying the Heartbeat Configuration for UPF	758
Configuring the Heartbeat Parameters for the UPF Profile	758
Verifying the Heartbeat Configuration for UPF Group	759
Associating UPF Group to Individual UPF Network Configuration	759
Verifying the Association of the UPF Group with the Individual UPF	759
OAM Support	760
Bulk Statistics	760

**CHAPTER 51****Voice over New Radio 761**

Feature Summary and Revision History	761
Summary Data	761
Revision History	761
Feature Description	762
Standards Compliance	762
VoNR P-CSCF Address Support	762
Feature Description	762
How it Works	762
Limitations	766
Configuring the VoNR P-CSCF Address Support	766
Creating P-CSCF Profile	766
Configuring P-CSCF Server Selection	766
Configuring P-CSCF IPv4 Server	767
Configuring P-CSCF IPv6 Server	767
Configuring P-CSCF IPv4v6 Server	768
Defining P-CSCF Profile in DNN Profile Configuration	769
Verifying the Feature Configuration	769
VoNR MO and MT Call Support	770

- Feature Description **770**
  - Call Flows **770**
- Paging Policy Differentiation Support **779**
  - Feature Description **779**
    - Call Flows **779**
  - Configuring the VoNR Paging Profile Differentiation **782**
    - Creating PPD Profile **782**
    - Configuring PPD Profile Parameters **782**
    - Enabling PPD in DNN Profile Configuration **782**
    - Verifying the Feature Configuration **783**
- P-CSCF FQDN **783**
  - Feature Description **783**
    - Relationships **783**
  - Configuring the P-CSCF FQDN **783**
    - Verifying the Feature Configuration **784**

---

**CHAPTER 52**

**VoLTE Support 785**

- Feature Summary and Revision History **785**
  - Summary Data **785**
  - Revision History **785**
- Feature Description **785**
  - How it Works **786**
    - Call Flows **786**
  - Standards Compliance **794**
  - Limitations **794**

---

**CHAPTER 53**

**VoWiFi Support 797**

- Feature Summary and Revision History **797**
  - Summary Data **797**
  - Revision History **797**
- Feature Description **797**
  - Architecture **798**
  - How it Works **798**
    - Call Flows **798**



Standards Compliance 804

Limitations 804

---

**CHAPTER 54**

**Wi-Fi Handovers 805**

Feature Summary and Revision History 805

Summary Data 805

Revision History 805

Feature Description 806

Architecture 806

ePDG and 5GS Interworking for Handover 806

EPS and ePDG Interworking for Handover 808

TFT Handling for WiFi Handovers 809

Standards Compliance 810

How it Works 810

EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow 810

Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow 813

Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow 816

5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow 819

Non 3GPP Untrusted LTE to WiFi Handover 823

Configuring the WiFi Handovers Feature 825

Configuring Compliance Profile 825

---

**CHAPTER 55**

**Wireless Priority Services 827**

Feature Summary and Revision History 827

Summary Data 827

Revision History 827

Feature Description 828

Use Cases 828

Multimedia Priority Services 828

Mission Critical Services 834

Expanded Prioritization for VoLTE/VoNR/Emergency Calls 834

DSCP Marking for N3/S5-U/S2-B over PFCP 835

WPS Profile Support 835

Converged Core Refactoring Changes 835

- How it Works 835
  - License Information 835
  - Standards Compliance 835
- Configuring Wireless Priority Services 836
  - Configuring the WPS Profile 836
  - Associating WPS Profile under DNN Profile 837
  - WPS OAM Support 837

---

CHAPTER 56

**SMF Serviceability Support 839**

- Feature Summary and Revision History 839
  - Summary Data 839
  - Revision History 839
- Feature Description 840
- show subscriber pei 840
- show subscriber gpsi 841
- show endpoint info 842

---

CHAPTER 57

**Troubleshooting Information 843**

- Feature Summary and Revision History 843
  - Summary Data 843
  - Revision History 843
- clear Commands 844
  - clear subscriber 844
  - clear subscriber supi imsi <imsi\_value> 844
  - clear subscriber supi imsi <imsi\_value> psid <psid\_value> 845
- show Commands 845
  - show helm 845
  - show peers all 845
  - show subscriber 846
  - show subscriber count 846
  - show subscriber count all 847
  - show subscriber count chf <chf\_address> 847
  - show subscriber count chf <chf\_address> dnn <dnn\_value> 848
  - show subscriber count supi <supi\_value> 848

show subscriber debug-info supi <supi_value>	848
show subscriber debug-info supi <supi_value> psid <psid_value>	848
show subscriber supi <supi_value> psid <psid_value> full	849
SMF Monitoring	849
SMF Data Collection Method	850
Application CLI	850
CEE Ops-Center CLI	850
SMF Data Collection - CLI Output	851
SMF Ops-Center CLI Commands	851
CEE Ops-Center CLI Commands	856
Grafana Charts	874
Error Logs	874

---

**CHAPTER 58****Sample SMF Configuration 881**

Feature Summary and Revision History	881
Summary Data	881
Revision History	881
Sample Configuration	881





## About this Guide

This preface describes the *5G Session Management Function Guide*, how it is organized and its document conventions.

This guide describes the Cisco Session Management Function (SMF) and includes infrastructure and interfaces, feature descriptions, specification compliance, session flows, configuration instructions, and CLI commands for monitoring and troubleshooting the system.

- [Conventions Used, on page xlv](#)

## Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	Description
Text represented as a screen display	This typeface represents displays that appear on your terminal screen, for example:  Login:
Text represented as <b>commands</b>	This typeface represents commands that you enter, for example:  <b>show ip access-list</b>  This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.

Typeface Conventions	Description
Text represented as a <b>command</b> <i>variable</i>	This typeface represents a variable that is part of a command, for example:  <b>show card</b> <i>slot_number</i>  <i>slot_number</i> is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example:  Click the <b>File</b> menu, then click <b>New</b>



# CHAPTER 1

## 5G Architecture

- [Feature Summary and Revision History, on page 1](#)
- [Overview, on page 2](#)
- [Subscriber Microservices Infrastructure Architecture, on page 3](#)
- [Control Plane Network Function Architecture, on page 4](#)

## Feature Summary and Revision History

### Summary Data

*Table 1: Summary Data*

Applicable Product(s) or FunctionalArea	<ul style="list-style-type: none"><li>• PCF</li><li>• SMF</li><li>• UPF</li></ul>
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 2: Revision History*

Revision Details	Release
First Introduced.	Pre-2020.02.0

# Overview

The Ultra Cloud Core is Cisco's solution supporting 3GPP's standards for 5G new radio (NR) standalone (SA) mode. These standards define various network functions (NFs) based on the separation of control plane (CP) and user plane (UP) (e.g. CUPS) functionality for increased network performance and capabilities.

## Control Plane Network Functions

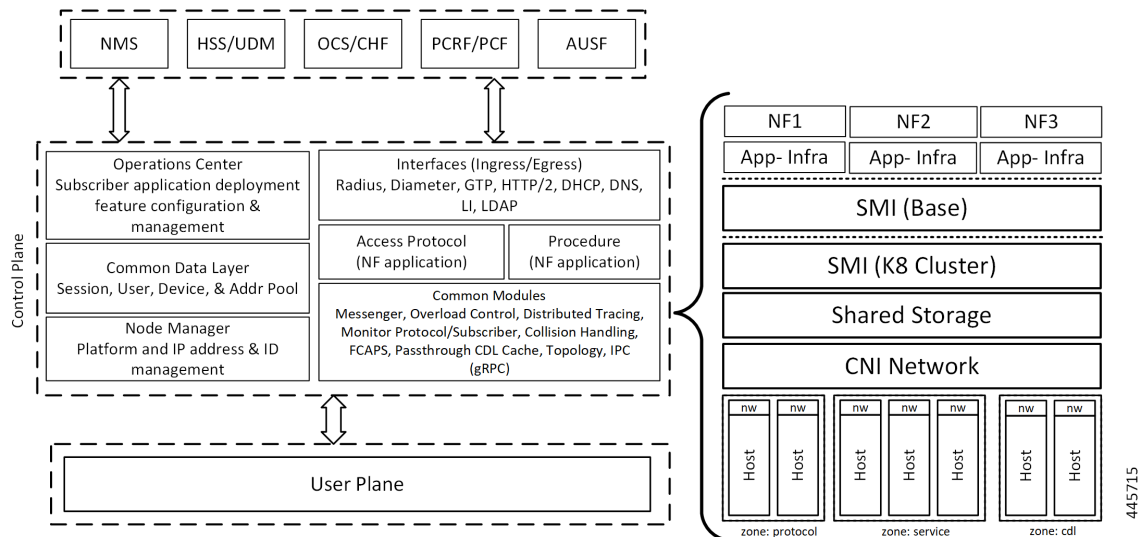
The CP-related NFs that comprise the Ultra Cloud Core are based on a common architecture designed around the following tenants:

- Cloud-scale — Fully virtualized for simplicity, speed, and flexibility
- Automation and orchestration — Optimized operations, service creation, and infrastructure
- Security — Multiple layers of security across the deployment stack from the infrastructure through the NF applications
- API exposure — Open and extensive for greater visibility, control, and service enablement
- Access agnostic — Support for heterogeneous network types (e.g. 5G, 4G, 3G, Wi-Fi, etc.)

These CP NFs are each designed as containerized applications (e.g. microservices) for deployment via the Subscriber Microservices Infrastructure (SMI).

The SMI defines the common application layers for functional aspects of the NF such as life cycle management (LCM), operations and management (OAM), and packaging.

**Figure 1: Ultra Cloud Core CP Architectural Components**



## User Plane Network Function

The 5G UP NF within the Ultra Cloud Core is the User Plane Function. Unlike the CP-related NFs, the 5G UPF leverages the same Vector Packet Processing (VPP) technology currently in use by the user plane



component within Cisco's 4G CUPS architecture. This commonality ensures the delivery of a consistent set of capabilities between 4G and 5G such as:

- Ultra-fast packet forwarding
- Extensive integrated IP services such as Subscriber Firewall, Tethering, Deep-Packet Inspection (DPI), Internet Content Adaption Protocol (ICAP), Application Detection and Control (ADC), and header enrichment (HE)
- Integrated third-party applications for traffic and TCP optimization

For more information on UPF, refer to *Ultra Cloud Core 5G UPF Configuration and Administration Guide*.

## Subscriber Microservices Infrastructure Architecture

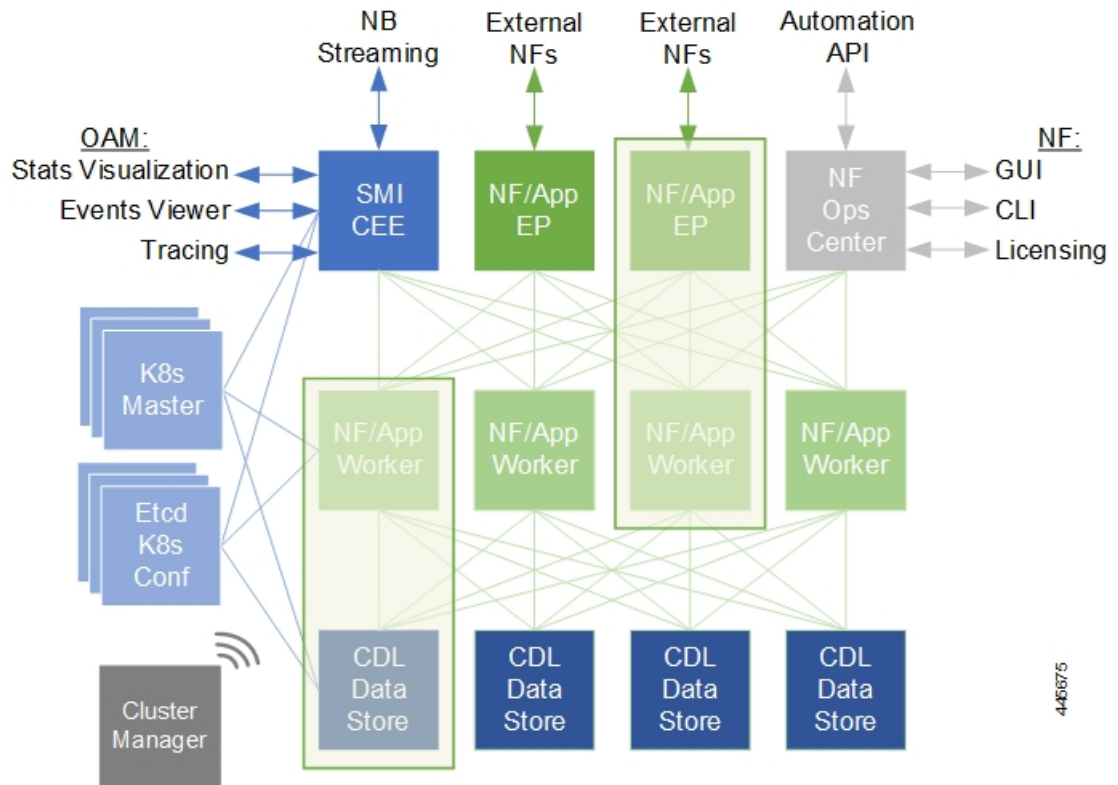
The Ultra Cloud Core Subscriber Microservices Infrastructure (SMI) is a layered stack of cloud technologies that enable the rapid deployment of, and seamless life-cycle operations for microservices-based applications.

The SMI stack consists of the following:

- SMI Cluster Manager—Creates the Kubernetes (K8s) cluster, creates the software repository, and provides ongoing LCM for the cluster including deployment, upgrades, and expansion.
- Kubernetes Management—Includes the K8s master and etcd functions, which provide LCM for the NF applications deployed in the cluster. This component also provides cluster health monitoring and resources scheduling.
- Common Execution Environment (CEE)—Provides common utilities and OAM functionalities for Cisco cloud native NFs and applications, including licensing and entitlement functions, configuration management, telemetry and alarm visualization, logging management, and troubleshooting utilities. Additionally, it provides consistent interaction and experience for all customer touch points and integration points in relation to these tools and deployed applications.
- Common Data Layer (CDL)—Provides a high performance, low latency, stateful data store, designed specifically for 5G and subscriber applications. This next generation data store offers HA in local or geo-redundant deployments.
- Service Mesh—Provides sophisticated message routing between application containers, enabling managed interconnectivity, additional security, and the ability to deploy new code and new configurations in low risk manner.
- NB Streaming—Provides Northbound Data Streaming service for billing and charging systems.
- NF/Application Worker nodes—The containers that comprise an NF application pod.
- NF/Application Endpoints (EPs)—The NF's/application's interfaces to other entities on the network.
- Application Programming Interfaces (APIs)—SMI provides various APIs for deployment, configuration, and management automation.

The following figure depicts how these components interconnect to comprise a microservice-based NF/application.

Figure 2: SMI Components



For more information on SMI components, refer to the [Ultra Cloud Core Subscriber Microservices Infrastructure documentation—Deployment Guide > Overview](#) chapter.

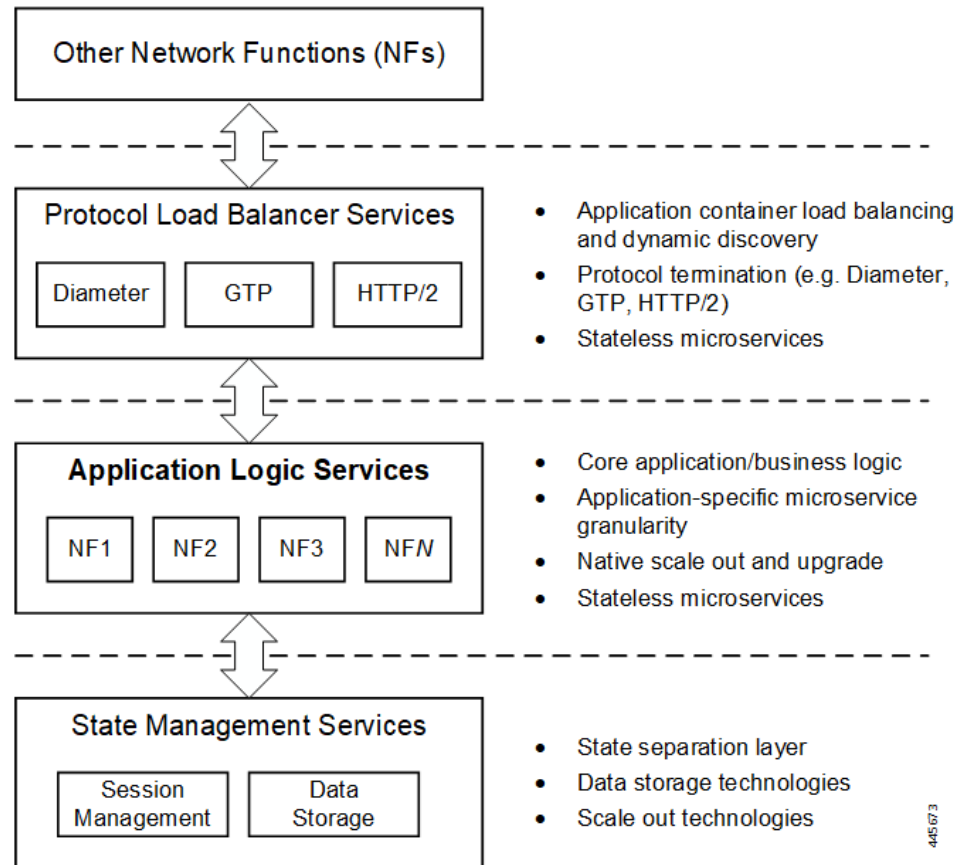
## Control Plane Network Function Architecture

CP NFs are designed around a three-tiered architecture that take advantage of the stateful/stateless capabilities afforded within cloud native environments.

The architectural tiers are as follows:

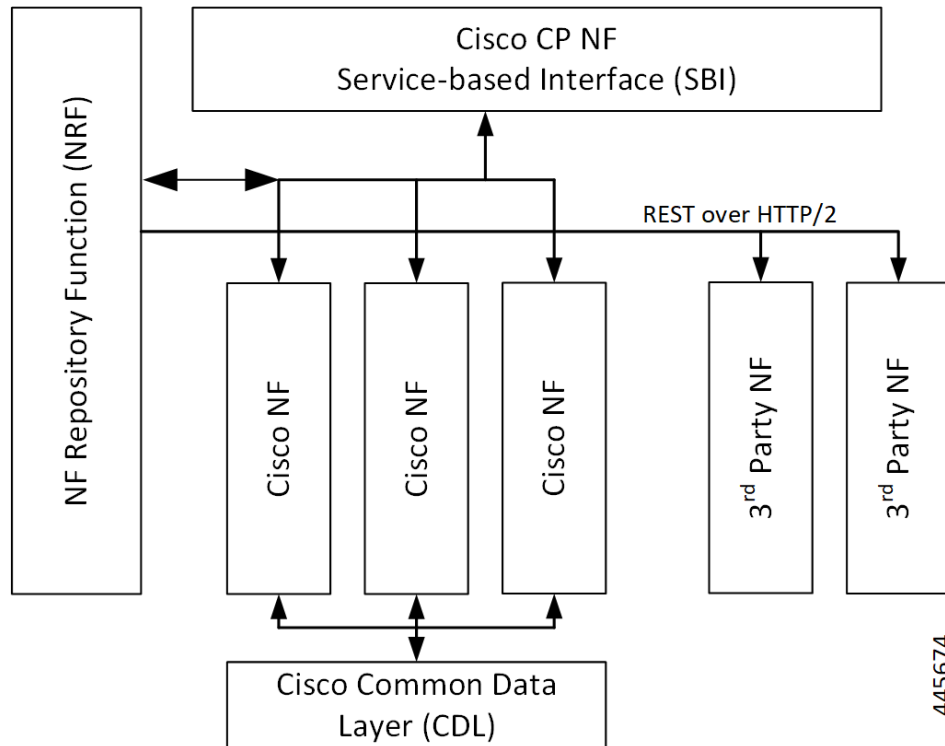
- **Protocol Load Balancer Services** — These are stateless microservices that are primarily responsible for dynamic discovery of application containers as well as for protocol proxy and/or termination. These include traditional 3GPP protocols and new protocols introduced with 5G.
- **Applications Services** — Responsible for implementing the core application/business logic, these are the stateless services that render the actual application based on the received information. This layer may contain varying degrees of microservice granularity. Application services are stateless.
- **State management services** — Enable stateless application services by providing a common data layer (CDL) to store/cache state information (e.g. session and subscriber data). This layer supports various data storage technologies from in-memory caches to full-fledge databases.

Figure 3: Control Plan Network Function Tiered Architecture



The three-tiered architecture on which Cisco's CP NFs are designed fully support the 5G core (5GC) Service-based Architecture (SBA) defined by 3GPP. These NFs communicate with each other and with third-party NFs over the Service-based Interface (SBI) using HTTP/2 over TCP as defined by 3GPP.

Figure 4: Cisco CP NF Service-based Architecture Support



For more information on the Cisco network functions, refer to the corresponding network function documentation.



## CHAPTER 2

# 5G SMF Overview

- [Feature Summary and Revision History, on page 7](#)
- [Product Description, on page 8](#)
- [Converged Core Overview, on page 9](#)
- [Use Cases and Features, on page 9](#)
- [Deployment Architecture and Interfaces, on page 17](#)
- [Life Cycle of Data Packet, on page 20](#)
- [License Information, on page 24](#)
- [Standards Compliance, on page 24](#)
- [Limitations, on page 25](#)

## Feature Summary and Revision History

### Summary Data

**Table 3: Summary Data**

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

**Table 4: Revision History**

Revision Details	Release
The converged core support for combined SMF + cnSGWc is added in this release.	2021.01.0

Revision Details	Release
First introduced.	Pre-2020.02.0

## Product Description

The Cisco Session Management Function (SMF) is one of the Control Plane Network Functions (NF) of the 5G core network (5GC). The SMF is responsible for the session management with the supported individual functions on a per-session basis.

A single instance of SMF can support some or all the functionality of the SMF. As specified in *3GPP TS 23.501*, the SMF supports the following functionality:

- Handles session management. For example, session establishment, modification and release, including the tunnel between the User Plane Function (UPF) and the access network (AN).
- Handles user element (UE) IP address allocation and management, which includes an optional authorization.
- Performs Dynamic Host Configuration Protocol for IPv4 (DHCPv4) and DHCPv6 functions, both as server and client.
- Performs Allocation and Retention Priority (ARP) proxying and IPv6 Neighbor Solicitation Proxying functionality for the Ethernet PDUs. The SMF communicates with the ARP and the IPv6 Neighbor Solicitation Request by providing the MAC address. This address corresponds to the IP address that exists in the request.
- Selects and controls the UPF for the Ethernet PDU sessions. The UP function includes controlling the UPF to proxy ARP or IPv6 Neighbor Discovery, and forwarding all ARP or IPv6 Neighbor Solicitation traffic to the SMF.
- Configures Traffic Steering at the UPF to route traffic to the corresponding Data Network (DN).
- Terminates interfaces toward the Policy Control Function (PCF).
- Handles the Lawful Intercept (LI) for Session Manager (SM) events and interface to the LI system.
- Controls and synchronizes the charging data collection at the UPF.
- Terminates the SM parts of Non-Access-Stratum (NAS) messages.
- Routes packets and ensures the delivery of information through the Downlink Data Notification (DDN).
- Initiates the AN-specific SM information that is sent through the Access and Mobility Management Function (AMF) to AN over the N2 interface.
- Determines the session and service continuity (SSC) mode of a session.
- Provides the following roaming functionality:
  - Manages the local enforcement to apply Quality of Service (QoS) SLAs (VPLMN).
  - Collects charging data and supports the charging interfaces.
  - Supports communication with the external DN. The communication is for the transport of signaling for the PDU session authorization or authentication by an external DN.

The SMF also provides support for an enterprise mobile virtual network operator (MVNO) model, which enables a mobile network operator (MNO) to perform secondary authentication for the leased MVNO subscribers. Additionally, the SMF supports other MVNO features, but is not limited to, RADIUS Client, vDNN, and so on.

## Converged Core Overview

The converged core solution provides an advanced, cloud native, converged control plane with the capability to support 4G and 5G devices, and use cases.



### Important

This release supports only the cloud-native integrated S-GW and SMF instance with S5C and cnSGWc functionalities.

The converged core solution removes the operational complexity by providing a unified core network to handle all types of subscribers and use cases.

The operator has the following benefits:

- Improves the overall network efficiency by reducing signaling between cnSGWc and SMF while handling a 4G subscriber or handoff from 5G to 4G coverage area.
- Reduces latency introduced due to the extra hop SGW-U for a subscriber in 4G coverage area by collapsing the data path in the Converged UPF, thus improving overall user experience.
- Ability to use a unified subscriber policy and billing infrastructure using SBA interfaces for 4G and 5G devices.

The solution supports the following converged control plane and user plane functions:

- Converged Control Plane Function:
  - Integrated S-GW and SMF network functions as a single deployment, under a single Kubernetes namespace, to support 4G and 5G devices from E-UTRAN/NR (converged core gateway)
  - Support for logical network functions (data only)
- Converged User Plane Function:
  - Integrated UPF and SGW-U functionalities as a single network function
  - Simultaneous support for N4 and Sxa interfaces
  - Terminate multiple control planes in a single deployment

## Use Cases and Features

This section describes the use cases that SMF supports in this release.

## Base SMF Configuration

The SMF base configuration provides a detailed view of the configurations that are required for making the SMF operational. This includes setting up the infrastructure to deploy the SMF, deploying the SMF through SMI, and configuring the Ops Center for exploiting the SMF capabilities over time.

For more information on SMI, see the *Ultra Cloud Core SMI Cluster Deployer Operations Guide*.

The following feature is related to this use case:

- [Deploying and Configuring SMF through Ops Center, on page 27](#)

## 4G Session Support

The SMF leverages the 3GPP provision for the UEs that can support both 5G and 4G NAS to connect to both 4G and 5G core networks. With this provision, the SMF includes the EPS interworking support and acts as a PGW-C+SMF. The interfaces, such as the Gx, Gy, or Gz, which are used for a 4G session creation are replaced with the corresponding 5G core SBI interfaces, such as the Npcf and Nchf.

The SMF supports interworking with EPS using the N26 interface (which is an inter-CN interface between the MME and the 5GS AMF) to enable interworking between the Evolved Packet Core (EPC) and the NG core networks. Support of the N26 interface in the network is optional for interworking. The N26 interface supports a subset of the functionalities over S10 interface to enable interworking. The UE uses the EPC NAS or 5GC NAS procedures that are based on the core network. The SMF supports QoS flow failures for access and mobility procedures.

The following features are related to this use case:

- [4G to 5G Data Session Handover Support, on page 79](#)
- [EPS Interworking, on page 231](#)
- [Flow Failure Handling for Access and Mobility Procedures, on page 301](#)
- [PDU Session Establishment from 4G-Only and Option 3x Capable Devices, on page 485](#)
- [Timers Support, on page 743](#)

## 5G Session Support

The Session and Service Continuity (SSC) support in 5G system architecture addresses the continuous requirements of different applications and services for a User Equipment (UE). The 5G system supports the SSC modes such that the network maintains the connectivity service to the UE. The SMF manages the UE IP address and ID allocation for establishing sessions. The SMF also maintains session connectivity on interfaces, such as N40, N4, N7, and N10, to facilitate charging.

The SMF uses the Xn interface to handover a UE from a source NG-RAN to the target NG-RAN when the AMF is unchanged, and without relocating the UPF. The SMF includes the N3 tunnel profile configuration to enable the notifications on the Control Plane (CP) and enable buffering on the UPF. The SMF supports activation and deactivation of the User Plane (UP) connection of a PDU session. The SMF also includes the DNS proxy feature to configure proxy servers for resolving the host names and their IP addresses.

The following features are related to this use case:

- [DNS Proxy Integration, on page 211](#)



- [Inter gNodeB Handover, on page 323](#)
- [IP Pool Allocation per DNN, on page 406](#)
- [Network-Initiated Service Request, on page 423](#)
- [PDU RAN Tunnel Endpoint Identifier Session, on page 517](#)
- [Resource Management, on page 645](#)
- [Session and Service Continuity Mode, on page 653](#)
- [Static IP Support, on page 352](#)
- [TAI Selection from AMF, on page 723](#)

## Access and Mobility Support

The SMF supports the access and mobility through session management procedures for PDU session establishment, modification, and release. The SMF supports N2-based handovers for intra-SMF or inter-AMF when a UE moves from one NG-RAN to another NG-RAN for Data Forwarding Tunnel (DFT) and Indirect Data Forwarding Tunnel (IDFT) cases. With the multi-DNN support, SMF has multiple PDN connections for providing various services including Internet and Voice over New Radio (VoNR) services. The SMF supports network-initiated messages when a UE is either in the CM-Idle state or in the CM-Connected state.

Access and mobility support includes the intra-5G handover use case, which has the following handover support:

- Xn Handover
- Intra-AMF N2 Handover
- Inter-AMF N2 Handover

The following features are related to this use case:

- [Cause Code Handling, on page 143](#)
- [AN Modification Call Flow Support, on page 97](#)
- [CHF and PCF Integration for Access and Mobility Procedures, on page 157](#)
- [Inter gNodeB Handover, on page 323](#)
- [Multiple and Virtual DNN Support, on page 395](#)
- [Network-initiated Messages Support, on page 413](#)
- [Policy and User Plane Management, on page 529](#)
- [Support for the Unsubscribe-To-Notifications Messages, on page 705](#)
- [Voice over New Radio, on page 761](#)

## Charging Integration

The SMF supports converged charging and uses the Nchf or N40 interface to generate charging events. The SMF supports offline failover for charging when a charging (CHF) server fails. Based on the charging data information that SMF receives, it provides reporting level support for online and offline charging.

The following feature is related to this use case:

- [SMF Charging, on page 657](#)

## Cloud Native Infrastructure

The SMF services includes the configuration to process PDU Session Management API calls. The IP Address Management (IPAM) technique is integrated with the SMF in the Application Services layer for tracking and managing the IP address space of a network. The SMF uses the Operations Center interface, which is a system-level infrastructure, to initiate the deployment of micro-services, to push application specific configuration to one or more micro-services, and to run application-specific commands to invoke APIs in application-specific pods.

The following features are related to this use case:

- [SMF Overload Management, on page 697](#)
- [UDP Proxy for SMF, on page 749](#)

## Converged Core Network

The SMF supports standalone deployment or an integrated deployment with cnSGWc for serving 4G and 5G subscribers. Converged Control Plane function comprises a combination of 4G and 5G control plane instances, that is, SMF and cnSGWc.

With converged core deployment, for the same PDN session, the S-GW and SMF select the same UPF instance so that the data path is optimized. The converged core architecture reduces the operational cost and the complexity of maintaining multiple different networks, leverages new interfaces and business avenues.

The converged core deployment involves changing some basic configurations of SMF, pod layout, and optimizing performance with call processing.

The following features are related to this use case:

- [Application-based Alerts, on page 105](#)
- [Content Filtering, Event Detail Records, and X-Header Enrichment Support, on page 169](#)
- [Deploying and Configuring SMF through Ops Center, on page 27](#)
- [EPS Interworking, on page 231](#)
  - [GTP Path Failure Handling, Restoration, and Recovery, on page 293](#)
  - [Support for UE Initial Attach on E-UTRAN, on page 234](#)
- [Monitoring Support, on page 385](#)
- [Pods and Services Reference, on page 61](#)

- [Policy and User Plane Management, on page 529](#)
  - [Support for UPF Node Reports and Proprietary Session Reports, on page 585](#)
  - [Static PCC Rules Support, on page 554](#)
- [SMF Interface for Metrics, on page 709](#)
- [UPF Path Management and Restoration, on page 755](#)
- [Wireless Priority Services, on page 827](#)

## IMS Support

The IP Multimedia Subsystem (IMS) connects to the LTE network and 5G core (through UPF node) for delivering voice services such as Voice over LTE (VoLTE) and Voice over New Radio (VoNR).

The following features are related to this use case:

- [Emergency SoS Support, on page 91](#)
- [VoLTE Support, on page 785](#)
- [Voice over New Radio, on page 761](#)

## IPAM Support

IP Address Management (IPAM) is a technique for tracking and managing IP addresses of a network. IPAM is one of the core components of the subscriber management system. The IPAM provides all the functionalities necessary for working with the cloud-native subscriber management system. Also, the IPAM acts as a generic IP address management system for the different network functions such as the Session Management Function (SMF), Policy Control Function (PCF), and so on.

The following feature is related to this use case:

- [IP Address Management, on page 337](#)

## Lawful Intercept

The Lawful Intercept (LI) feature enables law enforcement agencies (LEAs) to intercept subscriber communications. The LI functionality provides the network operator the capability to intercept and control data messages of targeted mobile users. The SMF that handles the Control Plane actions for the PDU sessions includes an IRI-POI that has the LI capability to generate the related xIRI.

For more details, contact your Cisco account representative.

## MVNO Support

The SMF provides support for an enterprise MVNO model. A mobile network operator can perform secondary authentication for the leased MVNO subscribers and also support any additional features related to the AAA server. The SMF uses the RADIUS protocol for such secondary authentication purposes.

The following features are related to this use case:

- [Multiple and Virtual DNN Support](#)
  - DNN Case Insensitive Support
- [Policy and User Plane Management](#)
  - Increase Max Groups Per Bandwidth Policy
- [RADIUS Client for SMF](#)
  - Handling RADIUS Disconnect and CoA Requests
  - RADIUS Access Management
  - RADIUS Accounting
  - RADIUS PAP/CHAP/MSCHAP Support
  - RADIUS NAS-IP Support

## NF Management

Based on the 3GPP-defined architecture model for 5G systems for data connectivity, SMF discovers the set of NF instances and their associate NF service instances. These instances, which are based on the NF profiles, are registered in the Network Repository Function (NRF) and meet the various input query parameters.

The following features are related to this use case:

- [NRF Discovery, on page 433](#)
- [Peer NF Failure Handling Support, on page 495](#)
- [SMF Deregistration with NRF, on page 693](#)

## OAM Support

This use case covers all the Operation, Administration, and Maintenance (OAM) functions of the SMF.

The following features are related to this use case:

- [Application-based Alerts, on page 105](#)
- [Bulk Statistics and Key Performance Indicators, on page 131](#)
- [Deploying and Configuring SMF through Ops Center, on page 27](#)
- [Monitoring Support, on page 385](#)
- [Pods and Services Reference, on page 61](#)
- [Smart Licensing, on page 35](#)
- [SMF Interface for Metrics, on page 709](#)
- [SMF Serviceability Support, on page 839](#)
- [System Logging Support Per SUPI, on page 715](#)

## Policy Integration

The SMF communicates with the Unified Data Management (UDM) and Policy Control Function (PCF) to perform the following:

- Procure the subscribed and authorized QoS parameters for the Guaranteed Bit Rate (GBR) and non-GBR flows
- Pass the relevant information to the UE (NAS), gNB (NGAP), and UPF (PFCP)

This ensures that all nodes on the network provide the desired QoS to the PDU session.

The SMF uses the service-based N7 interface with the PCF to retrieve the session management policy information corresponding to the PDU session of the UE. The SMF selects the PCF during the PDU Session Establishment procedure. It also acts as a consumer of the PCF-provided session management policy service.

The following features are related to this use case:

- [DSCP Marking, on page 219](#)
- [Policy and User Plane Management, on page 529](#)
- [Wireless Priority Services, on page 827](#)

## RADIUS Support

In the 5G architecture, the serving network authenticates the Subscription Permanent Identifier (SUPI) during authentication and the key agreement between the UE and the network. In addition, the serving network can perform a secondary authentication for data networks outside the mobile operator domain. For this purpose, various EAP-based authentication methods and associated credentials are used among which the RADIUS protocol is one of the widely used authentication protocols.

The following feature is related to this use case:

- [RADIUS Client for SMF, on page 595](#)

## Roaming Support

Mobile network operators make roaming partnerships to provide services to the subscribers seamlessly in geographies beyond their network reach. PLMNs define the operator network boundaries. HPLMN is the Subscriber's home network and VPLMN is the visited network from where the service is rendered.

The following features are related to this use case:

- [Local Breakout-based Roaming Support, on page 373](#)
- [Multiple PLMN Support, on page 409](#)

## SMF Inline Services

The SMF uses the Inline Services feature such as the Enhanced Charging Service (ECS) that enables operators to reduce billing-related costs and gives the ability to offer tiered, detailed, and itemized billing to their subscribers. Using shallow and deep packet inspection (DPI), the ECS [also known as Active Charging Service

(ACS)] allows operators to charge subscribers based on the actual usage, number of bytes, premium services, location, and so on. The ECS also generates charging records for postpaid and prepaid billing systems.

The following features are related to this use case:

- [Content Filtering, Event Detail Records, and X-Header Enrichment Support, on page 169](#)
- [Policy and User Plane Management, on page 529](#)

## SMF Specification Compliance

The SMF supports different 3GPP specification versions for the SMF interfaces. It processes the messages from the interfaces as per the compliance profile configured for the corresponding services.

The following feature is related to this use case:

- [3GPP Specification Compliance for SMF Interfaces, on page 73](#)

## Subscription Management

The SMF handles the user subscription management over the N10 interface.

The following feature is related to this use case:

- [Customized Configuration for Controlling Subscription Messages over N10, on page 207](#)

## UPF Integration

The SMF uses the available StarOS-based UPF node to meet the non-standard requirements on the UPF node to interwork with this UPF. To comply with the IPv6 Stateless Auto-configuration, the SMF supports ICMPv6 Router Solicit and Advertisement.

The following features are related to this use case:

- [Customization of StarOS-based UPF on N4 Interface, on page 203](#)
- [Policy and User Plane Management, on page 529](#)
- [Router Solicit and Router Advertisement, on page 649](#)
- [UPF Path Management and Restoration, on page 755](#)

## WiFi Support

The SMF supports Voice over Wi-Fi (VoWiFi). The VoWiFi technology provides the telephony services using Voice over IP (VoIP) from the mobile devices that are connected across a Wi-Fi network.

The following features are related to this use case:

- [VoWiFi Support, on page 797](#)
- [Wi-Fi Handovers, on page 805](#)

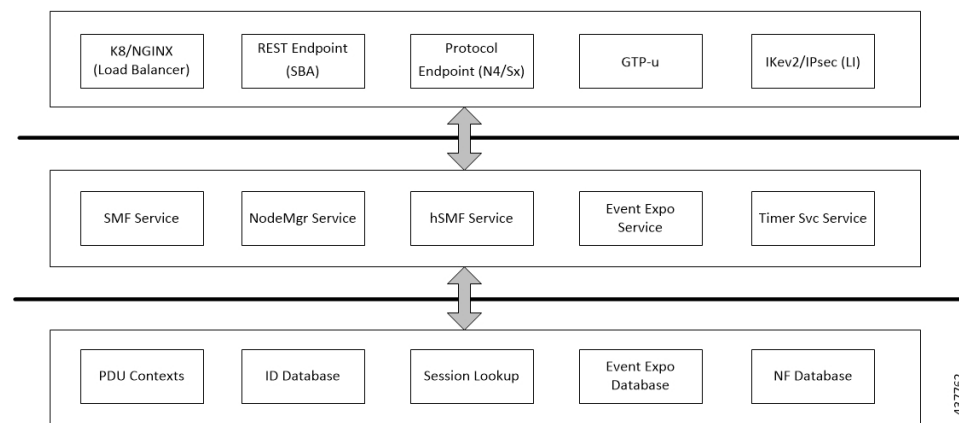
# Deployment Architecture and Interfaces

The Cisco SMF is a part of the 5G core network functions portfolio with a common mobile core platform architecture. The core network functions include Access and Mobility Management Function (AMF), Network Repository Function (NRF), Policy Control Function (PCF), Network Slice Selection Function (NSSF), and User Plane Function (UPF).

## SMF Architecture

The SMF network function consists of loosely coupled microservices together. The microservice decomposition is based on a three-layered architecture as illustrated in the following figure.

**Figure 5: SMF 3-Layered Micro Services Architecture**



Following are the three layers of the SMF architecture:

- Layer 1—Protocol and Load Balancer services (Stateless)
- Layer 2—Application services (Stateless)
- Layer 3—Database services (Stateful)

## SMF Deployment

The 5G Mobility NFs deployment supports the following modes:

- Standalone mode: In this mode, each NF together with the required microservices is deployed in a separate name space in Kubernetes.
- Converged mode: In this mode, several NFs are deployed together in a single name space and micro-service common to NFs render the service to all the deployed NFs.

## Converged Core Architecture

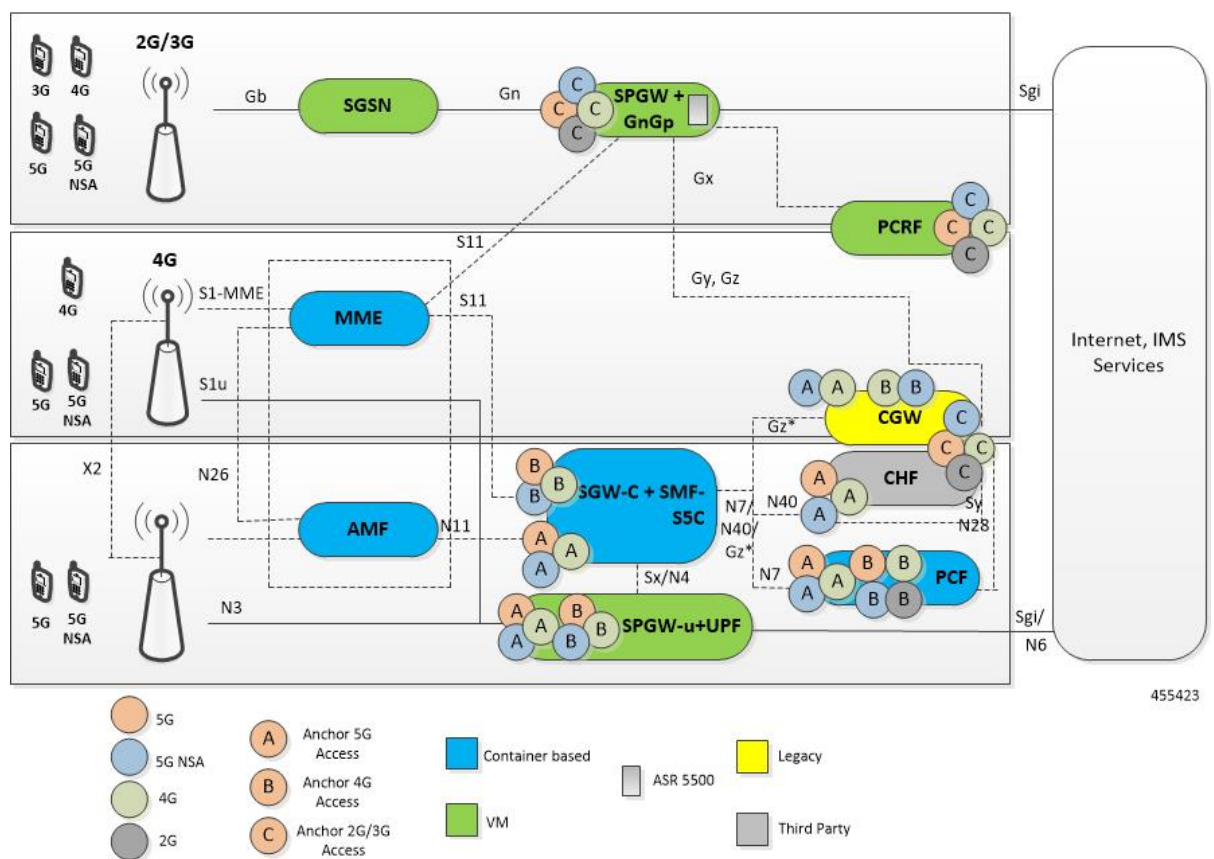
The converged core solution provides a single unified platform and architecture based on SMI. The supporting architecture integrates the cloud native S-GW and SMF deployment with S5-c and cnSGW-C functionalities. The solution uses 3GPP defined SBA interfaces for policy and charging functions.

In the converged core architecture, the 4G and 5G capable UEs are anchored on the same control plane instance. The control plane instance provides the SMF + S5-c and cnSGW-C functionalities.

The handoffs between 4G and 5G access types are seamless for 5G capable devices. The handoffs from LTE to UTRAN (4G/5G <-> 3G/2G) are not seamless for 4G capable devices.

The following figure illustrates the network architecture supported in this release.

**Figure 6: Converged Core Architecture**



The user plane function deployed as part of this solution is a VPC-SI VM. It supports SGW-U, PGW-U, and UPF functionalities in the same instance and exposes the Sxa/Sxb/Sxab/N4 interfaces towards the control plane. The UPF also supports multiple CP instances (up to 4) simultaneously. The UPF deployment is VM-based.

## Converged Core Deployment

The converged core deployment is based on the converged control plane and unified user plane infrastructure for all use cases.

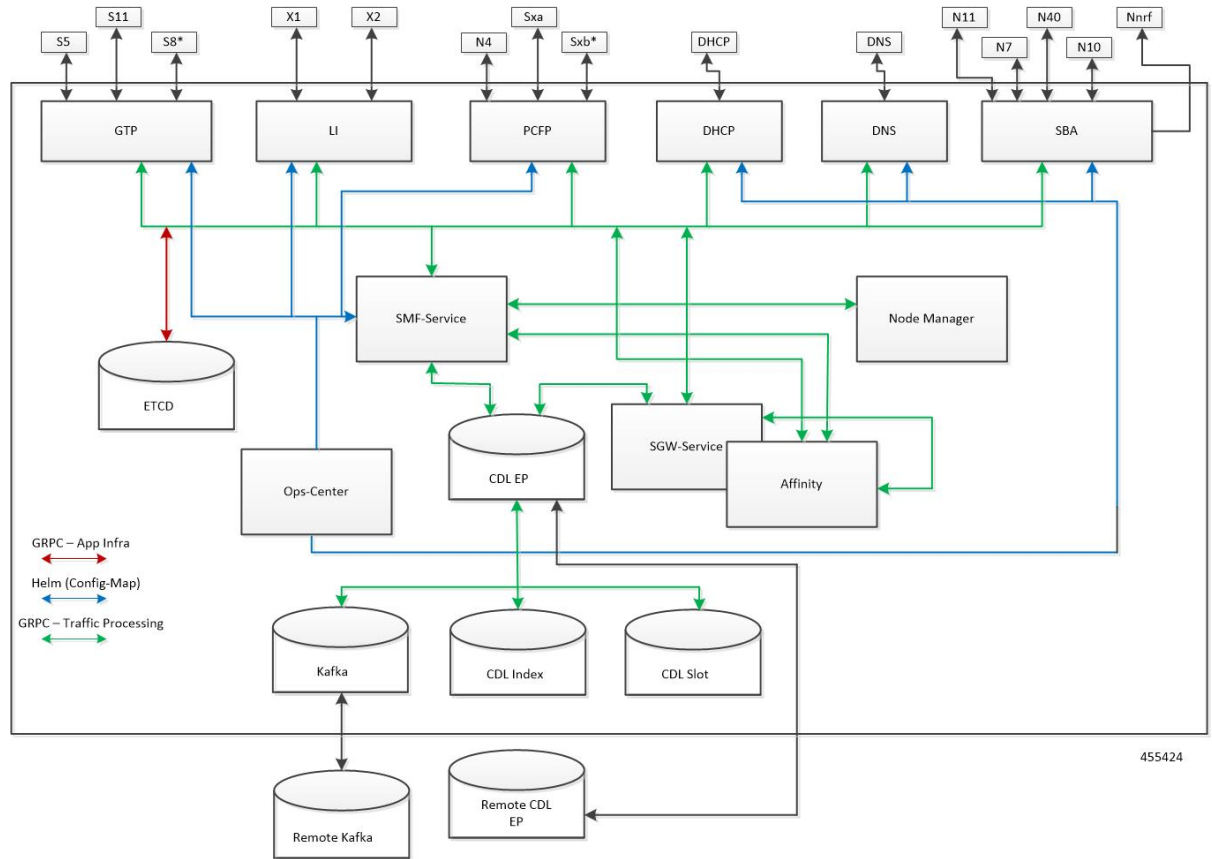


In the converged core deployment, all 4G and 5G capable UEs are anchored on the 5G core (SMF) with SBA interfaces towards policy and charging functions.

The converged core deployment has a Converged Ops Center. The Ops Center allows to configure the cnSGW and SMF services along with other microservices. A single product helm chart is used to install components.

The following figure illustrates the Kubernetes deployment for the converged S-GW and SMF network function.

**Figure 7: Kubernetes Deployment**



The protocol layer services are shared across SMF and S-GW. That is, the GTP end point terminates the S11 interface and S5/s8 interface. Similarly, the PCFP (protocol) end point terminates the N4 and Sxa interfaces.

The SMF and S-GW services are deployed as distinct pods and the session processing is segregated. Both the service pods use CDL for storing subscriber sessions.

## Supported Interfaces

This section describes the interfaces supported between the SMF and other network functions in the 5GC.

- N4—Reference point between the SMF and UPF.
- N7—Reference point between the SMF and PCF.
- N10—Reference point between the UDM and SMF.

- N11—Reference point between the AMF and SMF.
- N40—Reference point between the SMF and CHF.
- S5—Interface between the PGW-C and S-GW.
- S2b—Interface between the PGW-C and ePDG.

## Life Cycle of Data Packet

The following call flow depicts the life cycle of a data packet traversing through various pods of the SMF for a successful PDU session establishment.

The SMF application includes the following pods:

- REST-EP
- Cache
- Service
- Nodemgr
- Protocol
- UDP-Proxy
- CDL

Figure 8: End-to-End PDU Session Establishment Call Flow for Data Packets

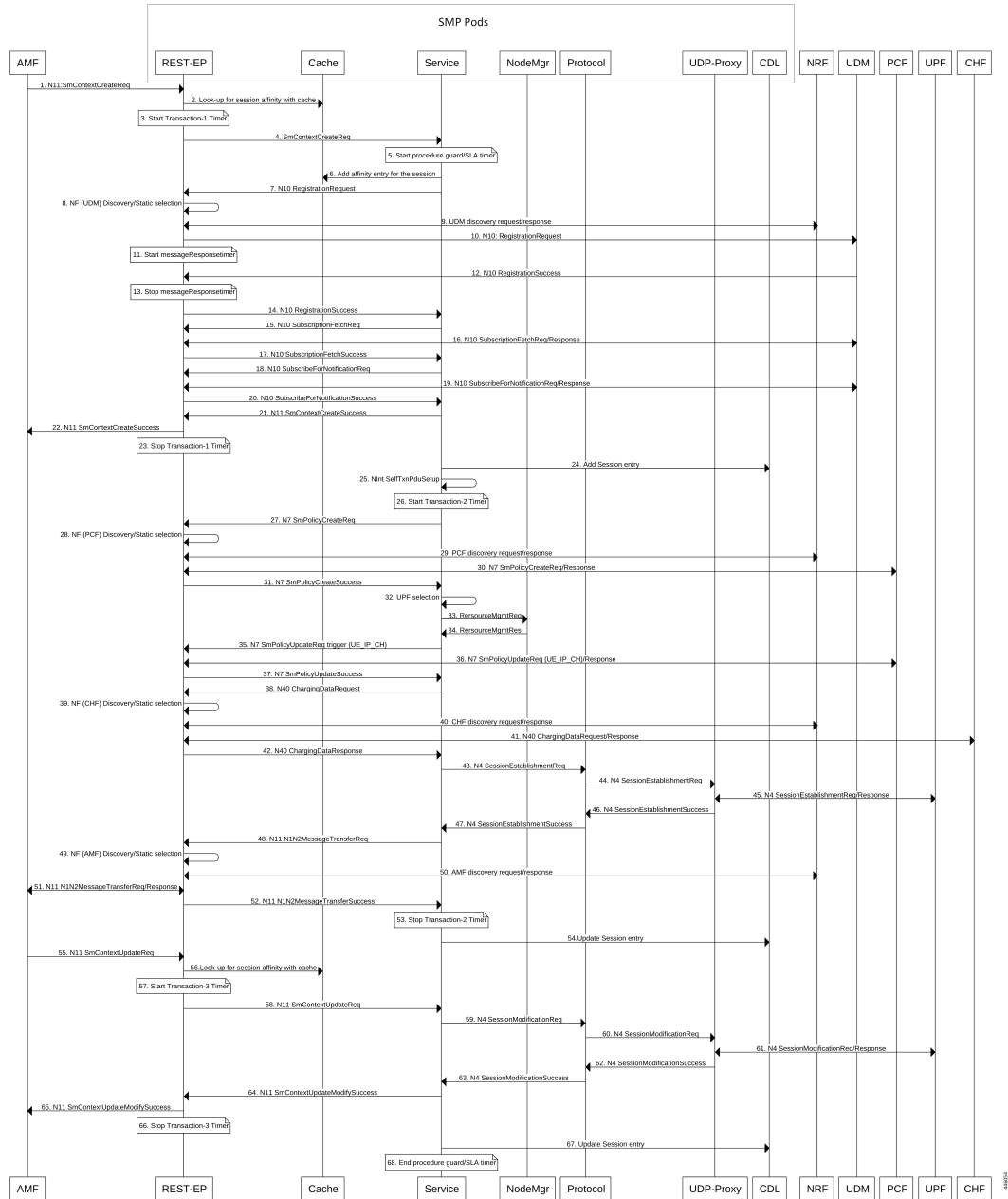


Table 5: End-to-End PDU Session Establishment Call Flow Description

Step	Description
1	The AMF sends N11:SmContextCreateRequest to the SMF, which terminates on the VIP-IP/external IP of REST-EP pod.

Step	Description
2	The REST-EP pod performs look-up for session affinity with cache pod. The SMF does not have the entry for the user session. The cache output does not result in any SMF-service affinity for the user session.  Kubernetes service/ISTIO load balancer selects one SMF-service pod from multiple SMF-service pods that are configured.
3	The REST-EP starts the timer associated with transaction-1. The PDU session establishment procedure involves using three transactions which are started at different stages of the call flow.  The default transaction timer on SMF is 10 seconds. The transaction timers are configurable through Service Level Agreement (SLA) feature.
4	The REST-EP forwards the N11:SMContextCreateRequest to the selected SMF-service.
5	The SMF-service starts procedure timer (guard timer/SLA timer). The SLA timers are configurable.
6	The SMF-service adds affinity entry with cache pod for the session. The SMF continues to use the same selected SMF-service in the subsequent stages of the call flow until the cache is expired.
7	The SMF-service instructs the REST-EP pod to trigger N10: Registration Request.
8	The REST-EP decides whether to perform NF discovery or static NF selection of UDM based on the configuration.
9	The REST-EP encodes and sends UDM discovery request to the NRF and receives a successful response with the list of UDMs.
10	The REST-EP encodes and sends N10:RegistrationRequest to the selected UDM.
11	The REST-EP starts messageResponseTimer. The default value of the configurable messageResponseTimeout is 2 seconds. The messageResponseTimer is applicable for all outbound HTTP2 messages initiated by SMF. They are not explicitly called out in the subsequent stages of the call flow.
12	The REST-EP receives successful N10:RegistrationResponse from the UDM.
13	The REST-EP stops messageResponseTimer.
14	The REST-EP forwards the N10:RegistrationResponse to the SMF-service.
15	The SMF-service instructs the REST-EP pod to trigger N10:SubscriptionFetchRequest.
16	The REST-EP encodes and sends N10: SubscriptionFetchRequest to the UDM. The REST-EP receives a response from the UDM.
17	The REST-EP forwards the N10:SubscriptionFetchResponse to the SMF-service.
18	The SMF-service instructs the REST-EP pod to trigger N10:SubscribeNotificationRequest.
19	The REST-EP encodes and sends N10:SubscribeNotificationRequest to UDM. The REST-EP receives a response from the UDM.
20	The REST-EP forwards the N10:SubscribeNotificationRequest to the SMF-service.
21	The SMF-service sends N11:SMContextCreateResponse to the REST-EP.
22	The REST-EP forwards the N11:SMContextCreateResponse to the AMF.

Step	Description
23	The REST-EP stops the transaction-1 timer started in step 3.
24	The SMF-service adds the session entry information in the CDL.
25	The SMF-service starts an internal transaction by sending NIntSelfTxnPduSetup message.
26	The SMF-service starts the timer associated with transaction-2.
27	The SMF-service instructs the REST-EP pod to trigger N7:SMPolicyCreateReq.
28	The REST-EP decides whether to perform NF discovery or static NF selection of PCF based on the configuration.
29	The REST-EP encodes and sends the PCF discovery request to the NRF and receives a successful response with the list of PCFs.
30	The REST-EP encodes and sends N7:SMPolicyCreateReq to the selected PCF. The REST-EP receives a response from the PCF.
31	The REST-EP forwards N7:SmPolicyCreateSuccess to the SMF-service.
32	The SMF-service performs the UPF selection.
33	The SMF-service sends ResourceMgmtReq to IPAM module of Nodemgr to request the IP address for the UE.
34	The SMF-service receives ResourceMgmtResp from the IPAM module of the Nodemgr with the IP address to the UE.
35	The SMF-service instructs the REST-EP pod to trigger N7:SMPolicyUpdateReq with trigger "UE_IP_CH".
36	The REST-EP encodes and sends N7:SMPolicyUpdateReq with UE_IP_CH trigger to the selected PCF. The REST-EP receives a response from the PCF.
37	The REST-EP sends N7:SMPolicyUpdateSuccess to the SMF-service.
38	The SMF-service instructs the REST-EP pod to trigger N40:ChargingDataRequest.
39	The REST-EP decides whether to perform the NF discovery or static NF selection of CHF based on the configuration.
40	The REST-EP encodes and sends the CHF discovery request to the NRF. The REST-EP receives a successful response with the list of CHFs.
41	The REST-EP encodes and sends N40:ChargingDataRequest to the selected CHF. The REST-EP receives a response from the CHF.
42	The REST-EP forwards N40:ChargingDataResponse to the SMF-service.
43	The SMF-service instructs the SMF-Protocol pod to trigger N4:SessionEstablishmentRequest.
44	The SMF-Protocol encodes and sends the N4:SessionEstablishmentRequest to the UDP-Proxy pod.
45	The UDP-Proxy pod sends the N4:SessionEstablishmentRequest to the UPF. The UDP-Proxy receives a response from the UPF.
46	The UDP-Proxy forwards the N4:SessionEstablishmentResponse to the SMF-Protocol pod.
47	The SMF-protocol forwards the N4:SessionEstablishmentResponse to the SMF-service.

Step	Description
48	The SMF-service instructs the REST-EP to trigger N11:N1N2MessageTransferReq.
49	The REST-EP decides whether to perform NF discovery or static NF selection of AMF based on the configuration.
50	The REST-EP encodes and sends the AMF discovery request to the NRF. The REST-EP receives a successful response with the list of AMFs.
51	The REST-EP encodes and sends N11:N1N2MessageTransferReq to the selected AMF. The REST-EP receives a successful response from the AMF.
52	The REST-EP forwards the N11:N1N2MessageTransferSuccess to the SMF-service.
53	The REST-EP stops the transaction-2 timer started in step 26.
54	The SMF-service updates the session entry in the CDL.
55	The REST-EP receives N11:SMContextUpdate from the AMF.
56	The REST-EP looks-up for session affinity in the cache pod and identifies the SMF-service handling the session.
57	The REST-EP starts the timer associated with transaction-3.
58	The REST-EP forwards the N11:SMContextUpdate to the SMF-service pod learnt in step 56.
59	The SMF-service instructs the SMF-Protocol pod to trigger N4:SessionModificationRequest.
60	The SMF-Protocol encodes and sends the N4:SessionModificationRequest to the UDP-Proxy pod.
61	The UDP-Proxy pod sends the N4:SessionModificationRequest to the UPF. The UDP-Proxy receives a response from the UPF.
62	The UDP-Proxy forwards the N4:SessionModificationResponse to the SMF-Protocol pod.
63	The SMF-protocol forwards the N4:SessionModificationResponse to the SMF-service.
64	The SMF-service forwards the N11:SMContextUpdateSuccess to the REST-EP.
65	The REST-EP forwards the N11:SMContextUpdateSuccess to the AMF.
66	The REST-EP stops the transaction-3 timer started in step 57.
67	The SMF-service updates the session entry in the CDL.
68	The SMF-service stops the procedure timer (guard timer/SLA timer).

## License Information

The SMF supports Cisco Smart Licensing. For more information, see the [Smart Licensing, on page 35](#) chapter in this document.

## Standards Compliance

Cisco SMF complies with the following 3GPP standards as per Release 15 Dec 2018:

- 3GPP TS 23.501
- 3GPP TS 23.502
- 3GPP TS 23.503
- 3GPP TS 23.510
- 3GPP TS 24.008
- 3GPP TS 24.501
- 3GPP TS 29.244
- 3GPP TS 29.501
- 3GPP TS 29.502
- 3GPP TS 29.503
- 3GPP TS 29.510
- 3GPP TS 29.512
- 3GPP TS 29.518
- 3GPP TS 32.255
- 3GPP TS 32.290
- 3GPP TS 32.291, Release 15 June 2019
- 3GPP TS 38.413

## Limitations

The SMF has the following limitation:

- QoS flow modifications and errors are not supported.







## CHAPTER 3

# Deploying and Configuring SMF through Ops Center

- [Feature Summary and Revision History, on page 27](#)
- [Feature Description, on page 28](#)
- [Deploying and Accessing SMF, on page 29](#)
- [SMF Service Configuration, on page 32](#)
- [Loading Day 1 Configuration, on page 33](#)

## Feature Summary and Revision History

### Summary Data

**Table 6: Summary Data**

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

**Table 7: Revision History**

Revision Details	Release
SMF deployment on bare metal server is supported and fully qualified in this release.	2021.01.0
First introduced.	Pre-2020.02.0

## Feature Description

The SMF deployment and configuration procedure involves deploying the SMF through the Subscriber Microservices Infrastructure (SMI) Cluster Deployer and configuring the settings or customizations through the SMF Operations (Ops) Center. The Ops Center is based on the ConfD CLI. The SMF configuration includes the NRF profile data configuration and the externally visible IP addresses and ports.

## SMF Ops Center

The Ops Center is a system-level infrastructure that provides the following functionality:

- A user interface to trigger a deployment of microservices with the flexibility of providing variable helm chart parameters to control the scale and properties of Kubernetes objects (deployment, pod, services, and so on) associated with the deployment.
- A user interface to push application-specific configuration to one or more microservices through Kubernetes configuration maps.
- A user interface to issue application-specific execution commands (such as show and clear commands). These commands:
  - Invoke some APIs in application-specific pods
  - Display the information returned on the user interface application

The following screenshot is a sample of the web-based command line interface presented to the user.

**Figure 9: Web-based CLI of Ops Center**

```

product smf#
product smf# show running-config
helm default-repository smf
helm repository smf
  url http://engci-maven-master.cisco.com/artifactory/mobile-cnaf-charts-dev/mobile-cnaf-smf/smf-products/master/
!
k8s namespace      smf
k8s registry        dockerhub.cisco.com/mobile-cnaf-docker-dev
k8s single-node     false
k8s use-volume-claims false
k8s ingress-host-name 10.86.73.232.nip.io
smf-services svc1
  smf-name          smf1
  smf-address       127.0.0.1
  http-endpoint base-url smf-service.com
  slices name slice1
  sst 88
  sdt 123456
!
smf-settings base-url-nrf http://10.142.40.191:8099
smf-settings base-url-pcf http://10.142.40.191:8099
smf-settings base-url-amf http://10.142.40.191:9000
smf-settings base-url-udm http://10.142.40.191:8099
smf-settings upf-ip-addr 10.142.40.191
smf-settings n4-peer-addr 10.142.40.191
smf-settings n4-peer-port 8809
smf-settings datastore-endpoint datastore-ep-smf:8980
smf-settings redis-endpoint redis-primary:6379
smf-settings rest-ep no-of-replicas 1
smf-settings rest-ep external-ip [ 10.86.74.150 ]
smf-settings service no-of-replicas 2
smf-settings upmgmt no-of-replicas 1
smf-settings protocol no-of-replicas 1
smf-settings protocol external-ip [ 10.86.74.150 ]

```

The SMF Ops Center allows you to configure the features such as licensing, SMF engine, REST Endpoint, and CDL.

## Prerequisites

Before deploying SMF on the SMI layer:

- Ensure that all the virtual network functions (VNFs) are deployed.
- Run the SMI synchronization operation for the SMF Ops Center and Cloud Native Common Execution Environment (CN-CEE)

## Converged Core Refactoring Changes

This section describes the changes related to converged core refactoring in this chapter.

The Day1 SMF configuration is updated to include the **s11** and **sxa** interfaces in the GTP endpoint and Protocol endpoint configuration respectively.

## Deploying and Accessing SMF

This section describes how to deploy SMF and access the SMF Ops Center.

### Deploying SMF

The Subscriber Microservices Infrastructure (SMI) platform is responsible for deploying and managing the Cloud Native 5G SMF application and other network functions.

For information on how to deploy SMF Ops Center on a vCenter environment, see *Deploying and Upgrading the Product* section in the *Ultra Cloud Core Subscriber Microservices Infrastructure — Operations Guide*.

For deploying SMF Ops Center on an OpenStack environment, see *UAME-based VNF Deployment* section in the *UAME-based 4G and 5G VNF Deployment Automation Guide*.

For information on how to deploy SMF Ops Center on bare metal servers (currently Cisco UCS-C servers) environment, see *Operating the SMI Cluster Manager on Bare Metal* section in *Ultra Cloud Core Subscriber Microservices Infrastructure — Operations Guide*.

### Accessing the SMF Ops Center

You can connect to the SMF Ops Center through SSH or the web-based CLI console.

- SSH:  

```
ssh admin@ops_center_pod_ip -p 2024
```
- Web-based console:
  1. Log in to the Kubernetes master node.
  2. Run the following command:  

```
kubectl get ingress <namespace>
```

The available ingress connections get listed.

3. Select the appropriate ingress and access the SMF Ops Center.
4. Access the following URL from your web browser:  
**cli.<namespace>-ops-center.<ip\_address>.nip.io**

By default, the Day 0 configuration is loaded into the SMF.

## Day 0 Configuration

To view the Day 0 configuration, run the following command.

### **show running-config**

The following is a sample Day 0 configuration:

```
# show running-config
helm default-repository base-repos
helm repository base-repos
  url https://charts.10.192.1.111.nip.io/ccg.2021.01.0.i60
exit
k8s name          2nd-a18-kub-cluster
k8s namespace     cn-cn3
k8s nf-name       smf
k8s registry      docker.10.192.1.111.nip.io/ccg.2021.01.0.i60
k8s single-node   false
k8s use-volume-claims false
k8s ingress-host-name 10.84.104.34.nip.io
k8s nodes 2nd-a18-kub-cluster-master-11
  node-type  master
  worker-type master
exit
k8s nodes 2nd-a18-kub-cluster-master-22
  node-type  master
  worker-type master
exit
k8s nodes 2nd-a18-kub-cluster-master-33
  node-type  master
  worker-type master
exit
aaa authentication users user admin
  uid          1117
  gid          1117
  password     $1$XNGJOr.C$iZZvQbNfmPN15qG4GpQa8/
  ssh_keydir   /tmp/admin/.ssh
  homedir      /tmp/admin
exit
aaa ios level 0
  prompt "\h> "
exit
aaa ios level 15
  prompt "\h# "
exit
aaa ios privilege exec
  level 0
  command action
  exit
  command autowizard
  exit
  command enable
  exit
```

```
command exit
exit
command help
exit
command startup
exit
exit
level 15
command configure
exit
exit
exit
nacm write-default deny
nacm groups group LI
  user-name [ liadmin ]
exit
nacm groups group admin
  user-name [ admin ]
exit
nacm rule-list admin
  group [ admin ]
  rule li-deny-tap
    module-name      lawful-intercept
    path              /lawful-intercept
    access-operations *
    action            deny
  exit
  rule li-deny-clear
    module-name      tailf-mobile-smf
    path              /clear/lawful-intercept
    access-operations *
    action            deny
  exit
  rule any-access
    action permit
  exit
exit
nacm rule-list confd-api-manager
  group [ confd-api-manager ]
  rule any-access
    action permit
  exit
exit
nacm rule-list ops-center-security
  group [ * ]
  rule change-self-password
    module-name      ops-center-security
    path              /smiuser/change-self-password
    access-operations exec
    action            permit
  exit
  rule smiuser
    module-name      ops-center-security
    path              /smiuser
    access-operations exec
    action            deny
  exit
exit
nacm rule-list lawful-intercept
  group [ LI ]
  rule li-accept-tap
    module-name      lawful-intercept
    path              /lawful-intercept
    access-operations *
```

```

        action          permit
    exit
    rule li-accept-clear
        module-name      tailf-mobile-smf
        path              /clear/lawful-intercept
        access-operations *
        action          permit
    exit
exit
nacm rule-list any-group
group [ * ]
rule li-deny-tap
    module-name      lawful-intercept
    path              /lawful-intercept
    access-operations *
    action          deny
exit
rule li-deny-clear
    module-name      tailf-mobile-smf
    path              /clear/lawful-intercept
    access-operations *
    action          deny
exit
exit

```

## SMF Service Configuration

The SMF service requires the basic configuration to process PDU Session Management API calls.

### Configuring Pod-level Labels



#### Important

The pod-level labelling configuration is applicable only when the SMF is deployed on a bare metal server.

Use the following sample configuration to configure the SMF pod layout when the virtual machine is short of CPU and memory resources.

#### config

```

    endpoint protocol
        labels key label_key value label_value
        cpu { max-process process_thread_count | request resource_request_number }

        memory { limit max_resource_limit | request resource_request_number }
    end

```

#### NOTES:

- **labels key *label\_key* value *label\_value***: Specify the K8 node affinity label key and value.

*label\_key* and *label\_value* accept alphanumeric characters. For example, the key can be `smi.cisco.com/protocol`.




---

**Important** The pod-level configuration takes precedence over the layered node-level configuration, that is, at the protocol, service, or session level configuration.

---

- **cpu** { **max-process** *process\_thread\_count* | **request** *resource\_request\_number* }: Enables the K8 pod CPU configuration.
  - **max-process** *process\_thread\_count*: Specify the maximum number of parallel OS threads to use. *process\_thread\_count* must be an integer in the range of 1-32.
  - **request** *resource\_request\_number*: Specify the CPU resource request in millicores. *resource\_request\_number* must be an integer in the range of 100-1000000.
- **memory** { **limit** *max\_resource\_limit* | **request** *resource\_request\_number* }: Enables the K8 pod memory configuration.
  - **limit** *max\_resource\_limit* : Specify the maximum number of used memory resources in megabytes. *max\_limit* must be an integer in the range of 100-200000.
  - **request** *resource\_request\_number*: Specify the memory resource request in megabytes. *request\_number* must be an integer in the range of 100-200000.

Use the following table for node-level labelling.

Node	OAM	Protocol	CDL	SMF
Node 1	Yes	Yes	Yes	No
Node 2	Yes	Yes	Yes	No
Node 3	Yes	No	No	Yes
Node 4	No	No	No	Yes

## Loading Day 1 Configuration

To load the Day 1 configuration for SMF, run the following command:

```
ssh admin@ops_center_pod_ip -p 2024 < Day1config.cli
```




---

**Note** The [Day1config.cli](#) file contains the necessary parameters required for the Day 1 configuration.

---

Alternatively, you can copy the configuration and paste it in the SMF Ops Center CLI to load the Day 1 configuration.

```
configure
<Paste the Day 1 configuration here>
commit
exit
```

A sample *Day1config.cli* file, which contains the Day 1 configuration for SMF is shown below.

## Day1config.cli

The following is a sample Day1config.cli file, which contains the Day 1 configuration for the SMF.





## CHAPTER 4

# Smart Licensing

- [Feature Summary and Revision History](#), on page 35
- [Smart Software Licensing](#), on page 35
- [Configuring Smart Licensing](#), on page 38
- [Monitoring and Troubleshooting Smart Licensing](#), on page 48

## Feature Summary and Revision History

### Summary Data

*Table 8: Summary Data*

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 9: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Smart Software Licensing

Smart Licensing is a cloud-based approach to licensing that simplifies the purchase, deployment, and management of Cisco software assets. Entitlements are purchased through your Cisco account via Cisco

Commerce Workspace (CCW) and immediately deposited into your Virtual Account for usage. This eliminates the need to install license files on every device. Products that are smart enabled communicate directly to Cisco to report consumption. A single location is available to customers to manage Cisco software licenses — the Cisco Software Central (CSC). License ownership and consumption are readily available to help make better purchase decision based on consumption or business need. See <https://www.cisco.com/c/en/us/buy/smart-accounts/software-licensing.html> for more information about Cisco Smart Licensing.

### Comparison Between Legacy Licensing and Smart Licensing

Cisco employs two types of license models - Legacy Licensing and Smart Software Licensing. Legacy Licensing consists of software activation by installing Product Activation Keys (PAK) on to the Cisco product. A Product Activation Key is a purchasable item, ordered in the same manner as other Cisco equipment and used to obtain license files for feature set on Cisco Products. Smart Software Licensing is a cloud-based licensing of the end-to-end platform through the use of a few tools that authorize and deliver license reporting. Smart Software Licensing functionality incorporated into the NFs complete the product registration and authorization.

## Cisco Software Central

Cisco Software Central (CSC) enables the management of software licenses and Smart Account from a single portal. The interface allows you to activate your product, manage entitlements, and renew and upgrade software. A functioning Smart Account is required to complete the registration process. To access the Cisco Software Central, see <https://software.cisco.com>.

## Smart Accounts/Virtual Accounts

A Smart Account provides a single location for all Smart-enabled products and entitlements. It helps speed procurement, deployment, and maintenance of Cisco Software. When creating a Smart Account, you must have the authority to represent the requesting organization. After submitting, the request goes through a brief approval process.

A Virtual Account exists as a sub-account within the Smart Account. Virtual Accounts are a customer-defined structure based on organizational layout, business function, geography or any defined hierarchy. They are created and maintained by the Smart Account administrator.

See <https://software.cisco.com> to learn about the set up or manage the Smart Accounts.

## Request a Cisco Smart Account

A Cisco Smart Account is an account where all products enabled for Smart Licensing are deposited. A Cisco Smart Account allows you to manage and activate your licenses to devices, monitor license use, and track Cisco license purchases. Through transparent access, you have a real-time view into your Smart Licensing products. IT administrators can manage licenses and account users within your organization's Smart Account through the Software Central.

---

**Step 1** In a browser window, enter the following URL:

`https://software.cisco.com`

- Step 2** Log in using your credentials, and then click **Request a Smart Account** in the **Administration** area. The **Smart Account Request** window is displayed.
- Step 3** Under **Create Account**, select one of the following options:
- **Yes, I have authority to represent my company and want to create the Smart Account** – If you select this option, you agree to authorization to create and manage product and service entitlements, users, and roles on behalf of your organization.
  - **No, the person specified below will create the account** – If you select this option, you must enter the email address of the person who will create the Smart Account.
- Step 4** Under **Account Information**:
- Click **Edit** beside **Account Domain Identifier**.
  - In the **Edit Account Identifier** dialog box, enter the domain, and click **OK**. By default, the domain is based on the email address of the person creating the account and must belong to the company that will own this account.
  - Enter the **Account Name** (typically, the company name).
- Step 5** Click **Continue**.  
The Smart Account request will be in pending status until it has been approved by the Account Domain Identifier. After approval, you will receive an email confirmation with instructions for completing the setup process.

## SMF Smart Licensing

At present, the Smart Licensing feature supports application entitlement for online and offline licensing for all 5G applications (PCF, SMF and NRF). The application usage is unrestricted during all stages of licensing including Out of Compliance (OOC) and expired stages.



**Note** A 90 day evaluation period is granted for all licenses in use. Currently, the functionality and operation of the 5G applications is unrestricted even after the end of the evaluation period.

## Software Tags and Entitlement Tags

Tags for the following software and entitlements have been created to identify, report, and enforce licenses.

### Software Tags

Software tags uniquely identify each licenseable software product or product suite on a device. The following software tags exist for the SMF.

Product Type / Description	Software Tag
Ultra Cloud Core - Session Management Function (SMF), Base Minimum	regid.2020-04.com.cisco.SMF,1.0_37ffdc21-3e95-4192-bcda-d3225b6590ce

### Entitlement Tags

The following entitlement tags identify licenses in use:

Product Type / Description	Entitlement Tag
Ultra Cloud Core - Session Management Function (SMF), Base Minimum	regid.2020-04.com.cisco.SMF_BASE,1.0_b49f5997-21aa-4d15-9606-0cff88729f69



**Note** The license information is retained during software upgrades and rollback.

## Configuring Smart Licensing

You can configure Smart Licensing after a new SMF deployment.

### Users with Access to CSC

This section describes how to configure Smart Licensing if you have access to CSC portal from your environment.

#### Setting Up the Product and Entitlement in CSC

Before you begin, you need to setup your product and entitlement in the CSC. To setup your product and entitlement:

1. Log in to your CSC account.
2. Click **Add Product** and enter the following details.
  - **Product name** – Specify the name of the deployed product. For example, SMF.
  - **Primary PM CEC ID** – Specify the primary Project Manager's CEC ID for the deployed product.
  - **Dev Manager CEC ID** – Specify the Development Manager's CEC ID for the deployed product.
  - **Description (Optional)** – Specify a brief description of the deployed product.
  - **Product Type** – Specify the product type.
  - **Software ID Tag** – Specify the software ID Tag provided by the Cisco Accounts team.
3. Click **Create**.
4. Select your product from the **Product/Entitlement Setup** grid.
5. Click **Entitlement** drop-down and select **Create New Entitlement**.
6. Select **New Entitlement** in **Add Entitlement** and enter the following details.

- **Entitlement Name** – Specify the license entitlement name. For example, SMF\_BASE.
  - **Description** (Optional) – Specify a brief description about the license entitlement.
  - **Entitlement Tag** – Specify the entitlement tag provided by the Cisco Accounts team.
  - **Entitlement Type** – Specify the type of license entitlement.
  - **Vendor String** – Specify the vendor name.
7. Click **Entitlement Allocation**.
  8. Click **Add Entitlement Allocation**.
  9. In **New License Allocation**, provide the following details:
    - **Product** – Select your product from the drop-down list.
    - **Entitlement** – Select your entitlement from the drop-down list.
  10. Click **Continue**.
  11. In **New License Allocation** window, provide the following details:
    - **Quantity** – Specify the number of licenses.
    - **License Type** – Specify the type of license.
    - **Expiring Date** – Specify the date of expiry for the license purchased.
  12. Click **Create**.
  13. Verify the status of Smart Licensing using the following command.

```
show license all
```

**Example:**

```
SMF# show license all

Smart Licensing Status
=====
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 83 days, 0 hr, 15 min, 8 sec
  Last Communication Attempt: NONE

License Conversion:
  Automatic Conversion Enabled: true
  Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME
```

```

Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 83 days, 0 hr, 15 min, 8 sec

License Usage
=====
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 83 days, 0 hr, 15 min, 8 sec

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: RESTRICTED_NOTALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
=====
UDI: PID:SMF,SN:6GKJ20A-NMUWA7Y

Agent Version
=====
Smart Agent for Licensing: 3.0.13

```

## Registering Smart Licensing

You must register the product entitled to the license with CSC. In order to register, you must generate an ID token from CSC.

1. Log in to your CSC account.
2. Click **General** > **New Token** and enter the following details:
  - **Description** – Specify a brief description about the ID token.
  - **Expires After** – Specify the number of days for the token to expire.
  - **Max. Number Users** – Specify the maximum number of users.
3. Click **Create Token**.
4. Select **new ID token** in **Product Instance Registration Token**.
5. Click **Actions** > **Copy**.
6. Log in to SMF Ops Center CLI and paste the **ID token** using the following command.

```
license smart register idtoken
```

### Example:

```

SMF# license smart register
Value for 'idtoken' (<string>): MTI2Y2F1NTAtOThkMi00YTaxLWE4M2QtOTNhNzNjNjY4ZmFiLTE2MTc4N
Tky%0AMTA5MDh8ck1jUHNwc3k1ZC9nWFFCSnVEcUp4QU1jTFoxOGxDTU5kQ3lpa25E%0Ab04wST0%3D%0A
SMF#

```

7. Verify the Smart Licensing status using the following command.

```
show license all
```

**Example:**

```

SMF# show license all

Smart Licensing Status
=====
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Cisco Systems, Inc.
  Virtual Account: SMF-SMF
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Apr 15 05:45:07 2020 GMT
  Last Renewal Attempt: SUCCEEDED on Apr 15 05:45:07 2020 GMT
  Next Renewal Attempt: Oct 12 05:45:07 2020 GMT
  Registration Expires: Apr 15 05:40:31 2021 GMT

License Authorization:
  Status: AUTHORIZED on Apr 15 05:45:12 2020 GMT
  Last Communication Attempt: SUCCEEDED on Apr 15 05:45:12 2020 GMT
  Next Communication Attempt: May 15 05:45:12 2020 GMT
  Communication Deadline: Jul 14 05:40:40 2020 GMT

License Conversion:
  Automatic Conversion Enabled: true
  Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec

License Usage
=====
License Authorization Status: AUTHORIZED as of Apr 15 05:45:12 2020 GMT

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: RESTRICTED_ALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
=====
UDI: PID:SMF,SN:6GKJ20A-NMUWA7Y

Agent Version
=====
Smart Agent for Licensing: 3.0.13

```

**NOTES:**

- **license smart register** – Registers Smart Licensing with CSC.
- *idtoken* – Specifies the ID token generated from CSC.

## Deregistering Smart Licensing

To deregister Smart Licensing:

1. Log in to SMF Ops Center CLI and use the following command.

```
license smart deregister
```

2. Verify the Smart Licensing status using the following command.

```
show license all
```

### Example:

```
SMF# show license all

Smart Licensing Status
=====
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec
  Last Communication Attempt: NONE

License Conversion:
  Automatic Conversion Enabled: true
  Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME

Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec

License Usage
=====
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 83 days, 0 hr, 10 min, 43 sec

UCC 5G SMF BASE (SMF_BASE)
  Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: RESTRICTED_NOTALLOWED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
=====
UDI: PID:SMF,SN:6GKJ20A-NMUWA7Y

Agent Version
=====
Smart Agent for Licensing: 3.0.13
```



SMF#

**NOTES:**

- **license smart deregister** – Deregisters Smart Licensing from CSC.

## Users without Access to CSC

The Smart License Reservation feature – Perpetual Reservation – is reserved for customers without access to CSC from their internal environments. With this feature, Cisco allows customers to reserve licenses from their virtual account and tie them to their devices Unique Device Identifier (UDI). Smart License Reservation enables customers to use their devices with reserved licenses in a disconnected mode.

The subsequent sections describe the procedure involved in reserving Smart License for users without access to CSC from their internal environment.

### Enabling Smart License Reservation

To enable Smart License reservation through SMF Ops Center CLI:

1. Log in to SMF Ops Center CLI and use the following configuration.

```
configure terminal
license smart reservation
commit
exit
```

**NOTES:**

- **license smart reservation** – Enables license reservation.

### Generating Smart License Reservation Request Code

To generate the Smart License reservation request code:

1. Log in to SMF Ops Center CLI.
2. To enable reservation, use the following configuration.

```
configure terminal
license smart reservation
commit
exit
```

3. To request for a reservation code, use the following command.

```
license smart reservation request
```

**Example:**

```
SMF# license smart reservation request
reservation-request-code CJ-ZSMF:6GKJ2OA-NMUWA7Y-Ai75GxtBs-3B
SMF#
Message from confd-api-manager at 2020-04-15 05:51:37...
Global license change NotifyReservationInProgress reason code Success - Successful.
SMF#
```

**NOTES:**

- **license smart reservation** – Enables license reservation request code.
- **license smart reservation request** – Generates the license reservation request code.




---

**Important** You must copy the generated license request code from the SMF Ops Center CLI.

---

**Generating an Authorization Code from CSC**

To generate an authorization code from CSC using the license reservation request code:

1. Log in to your CSC account.
2. Click **License Reservation**.
3. Enter the Request Code: Paste the license reservation request code copied from the SMF Ops Center CLI in the **Reservation Request Code** text-box.
4. Select the Licenses: Click **Reserve a Specific License** radio-button and select *UCC 5G SMF BASE*.




---

**Note** In the **Reserve** text-box enter the value *1*.

---

5. Review your selection.
6. Click **Generate Authorization Code**.
7. Download the response file: The authorization code is generated and displayed on-screen. Click **Download as File** to download the authorization code.
8. Click **Close**.

**Reserving Smart Licensing**

To reserve Smart License for the deployed product using the authorization code generated in CSC:

1. Log in to SMF Ops Center CLI and use the following command.

```
license smart reservation install authorization_code
```

**Example:**

```
SMF# license smart reservation install
Value for 'key' (<string>):
<specificPLR><authorizationCode><flag>A</flag><version>C</version>
<piiid>35757dc6-2bdf-4fal-ba7e-4190f5b6ea22</piiid><timestamp>1586929992297</timestamp>
<entitlements><entitlement><tag>regid.2020-04.com.cisco.SMF_BASE,1.0_60b1da6f-3832-4687-90c9-8879dc815a27</tag>
<count>1</count><startDate>2020-Apr-08 UTC</startDate><endDate>2020-Oct-05 UTC</endDate>
<licenseType>TERM</licenseType><displayName>UCC 5G SMF BASE</displayName>
<tagDescription>Ultra Cloud Core - Session Management Function (SMF), Base
Minimum</tagDescription>
<subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode>
<signature>MEYCIQC/9v5LpgFoEk2l4omIgjkk83g5WXjzs09kQnsO8D0jRgIhAMh+
```

```
D6DRuYmqh1TlfJoZxNte0fPKw6fHEY5CEF3+kPQj</signature>
<udi>P:SMF,S:6GKJ2OA-NMUWA7Y</udi></specificPLR>
SMF#
```

2. Verify the smart licensing status using the following command.

```
show license all
```

**Example:**

```
SMF# show license all
```

```
Smart Licensing Status
=====
Smart Licensing is ENABLED
License Reservation is ENABLED
```

**Registration:**

```
Status: REGISTERED - SPECIFIC LICENSE RESERVATION
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Wed Apr 15 05:53:31 GMT 2020
Last Renewal Attempt: None
```

**License Authorization:**

```
Status: AUTHORIZED - RESERVED on Wed Apr 15 05:53:31 GMT 2020
```

```
Utility:
  Status: DISABLED
```

```
Transport:
  Type: CALLHOME
```

```
Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec
```

```
License Usage
=====
```

**License Authorization Status:**

```
Status: AUTHORIZED - RESERVED on Wed Apr 15 05:53:31 GMT 2020
Last Communication Attempt: SUCCEEDED on Apr 15 05:53:31 2020 GMT
Next Communication Attempt: NONE
Communication Deadline: NONE
```

**UCC 5G SMF BASE (SMF\_BASE)**

```
Description: Ultra Cloud Core - Session Management Function (SMF),
Base Minimum
```

```
Count: 1
```

```
Version: 1.0
```

```
Status: AUTHORIZED
```

```
Export status: NOT RESTRICTED
```

```
Feature Name: <empty>
```

```
Feature Description: <empty>
```

```
Reservation:
```

```
  Reservation Status: SPECIFIC INSTALLED
```

```
  Total Reserved Count: 1
```

```
  Term expiration: 2020-Oct-05 GMT
```

```
Product Information
=====
```

```
UDI: PID:SMF,SN:6GKJ2OA-NMUWA7Y
```

```
Agent Version
=====
Smart Agent for Licensing: 3.0.13
```

**NOTES:**

- **license smart reservation install** *authorization\_code* – Installs a Smart License Authorization code.

**Returning the Reserved License**

You can return the reserved license to CSC if required. Use the following procedure to return the reserved license:

1. When the license reservation authorization code is installed in the SMF Ops Center.
  - a. Log in to the SMF Ops Center CLI and use the following command.

```
license smart reservation return
```

**Example:**

```
SMF# license smart reservation return
reservation-return-code CJ6m3k-RAvu6b-hMNmwf-mrdcko-NoSwKL-tF7orz-9aNtEu-yVjGAm-D6j
SMF#
```

- b. Copy the license reservation return code generated in SMF Ops Center CLI.
- c. Log in to your CSC account.
- d. Select your product instance from the list.
- e. Click **Actions > Remove**.
- f. Paste the license reservation return code in **Return Code** text-box.

**NOTES:**

- **license smart reservation return** – Returns a reserved Smart License.
2. When the license reservation authorization code is not installed in the SMF Ops Center.
    - a. Log in to the SMF Ops Center CLI and use the following command to generate the return code.

```
license smart reservation return
authorization_code
```

**Important**


---

Paste the license reservation authorization code generated in CSC to generate the return code.

---

- b. Log in to your CSC account.
  - c. Select your product instance from the list.
  - d. Click **Actions > Remove**.
  - e. Paste the license reservation return code in **Return Code** text-box.
3. Verify the smart licensing status using the following command.

**show license all****Example:**

```
SMF# show license all
```

```
Smart Licensing Status
=====
```

```
Smart Licensing is ENABLED
License Reservation is ENABLED
```

## Registration:

```
Status: UNREGISTERED
Export-Controlled Functionality: Not Allowed
```

## License Authorization:

```
Status: EVAL MODE
Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec
Last Communication Attempt: SUCCEEDED on Apr 15 05:53:31 2020 GMT
Next Communication Attempt: NONE
Communication Deadline: NONE
```

## License Conversion:

```
Automatic Conversion Enabled: true
Status: NOT STARTED
```

## Utility:

```
Status: DISABLED
```

## Transport:

```
Type: CALLHOME
```

## Evaluation Period:

```
Evaluation Mode: In Use
Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec
```

## License Usage

```
=====
```

```
License Authorization Status: EVALUATION MODE
Evaluation Period Remaining: 83 days, 0 hr, 5 min, 15 sec
```

## UCC 5G SMF BASE (SMF\_BASE)

```
Description: Ultra Cloud Core - Session Management Function (SMF), Base Minimum
Count: 1
Version: 1.0
Status: EVAL MODE
Export status: RESTRICTED_NOTALLOWED
Feature Name: <empty>
Feature Description: <empty>
```

## Product Information

```
=====
```

```
UDI: PID:SMF,SN:6GKJ20A-NMUWA7Y
```

## Agent Version

```
=====
```

```
Smart Agent for Licensing: 3.0.13
```

```
SMF#
```

# Monitoring and Troubleshooting Smart Licensing

You can use the following show commands to view Smart Licensing related information in the SMF Ops Center.

```
show license [ all | UDI | displaylevel | reservation | smart | status |  
summary | tech-support | usage ]
```

## NOTES:

- **all** – Displays an overview of Smart Licensing information that includes license status, usage, product information and Smart Agent version.
- **UDI** – Displays Unique Device Identifiers (UDI) details.
- **displaylevel** – Depth to display information.
- **reservation** – Displays Smart Licensing reservation information.
- **smart** – Displays Smart Licensing information.
- **status** – Displays the overall status of Smart Licensing.
- **summary** – Displays a summary of Smart Licensing.
- **tech-support** – Displays Smart Licensing debugging information.
- **usage** – Displays the license usage information for all the entitlements that are currently in use.



## CHAPTER 5

# SMF Rolling Software Update

- [Feature Summary and Revision History, on page 49](#)
- [Introduction, on page 49](#)
- [Updating SMF, on page 51](#)

## Feature Summary and Revision History

### Summary Data

*Table 10: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 11: Revision History*

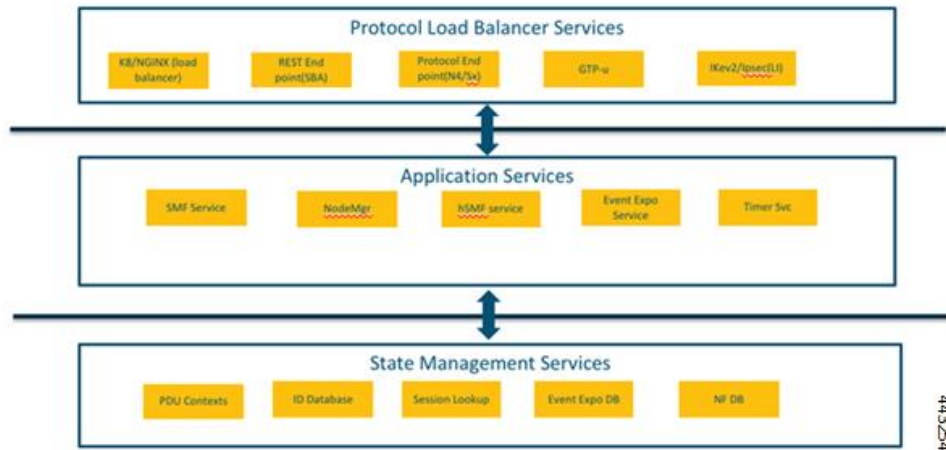
Revision Details	Release
First introduced.	Pre-2020.02.0

## Introduction

The Cisco SMF has a three-tier architecture consisting of Protocol, Service, and Session tiers. Each tier includes a set of microservices (pods) for a specific functionality. Within these tiers, there exists a Kubernetes Cluster comprising of Kubernetes (K8s) master, and worker nodes (including Operation and Management nodes).

For high availability and fault tolerance, a minimum of two K8s worker nodes are required for each tier. You can have multiple replicas for each worker node. Kubernetes orchestrates the pods using the StatefulSets controller. The pods require a minimum of two replicas for fault tolerance.

Figure 10: SMF Architecture



The following figure depicts an SMF K8s Cluster with 12 nodes – three Master nodes, three Operations and Management (OAM) worker nodes, two Protocol worker nodes, two Service worker nodes, and two Session (data store) worker nodes.

Figure 11: SMF Kubernetes Cluster

SMF Kubernetes Cluster											
O	O	O	M	M	M	P	P	S	S	S	S
A	A	A	A	A	A	R	R	E	E	E	E
M	M	M	S	S	S	O	O	R	R	S	S
			T	T	T	T	T	I	I	I	I
			E	E	E	O	O	V	V	V	V
			R	R	R			C	C	C	C
								E	E	N	N



**Note**

- OAM worker nodes: These nodes host the Ops Center pods for configuration management and metrics pods for statistics and Key Performance Indicators (KPIs).
- Protocol worker nodes: These nodes host the SMF protocol-related pods for service-based interfaces (N11, N7, N10, N40, NRF) and UDP-based protocol interfaces (N4, S5/S8).
- Service worker nodes: These nodes host the SMF application-related pods that perform session management processing.
- Session worker nodes: These nodes host the database-related pods that store subscriber session data.



# Updating SMF

The following section describes the procedure involved in updating the SMF software.

## Rolling Software Update Using SMI Cluster Manager

The SMF software update or in-service update procedure utilizes the K8s rolling strategy to update the pod images. In K8s rolling update strategy, the pods of a StatefulSet are updated sequentially to ensure that the ongoing process remains unaffected. Initially, a rolling update on a StatefulSet causes a single pod instance to terminate. A pod with an updated image replaces the terminated pod. This process continues until all the replicas of the StatefulSet are updated. The terminating pods exit gracefully after completing all the ongoing processes. Other in-service pods continue to receive and process the traffic to provide a seamless software update. You can control the software update process through the Ops Center CLI.



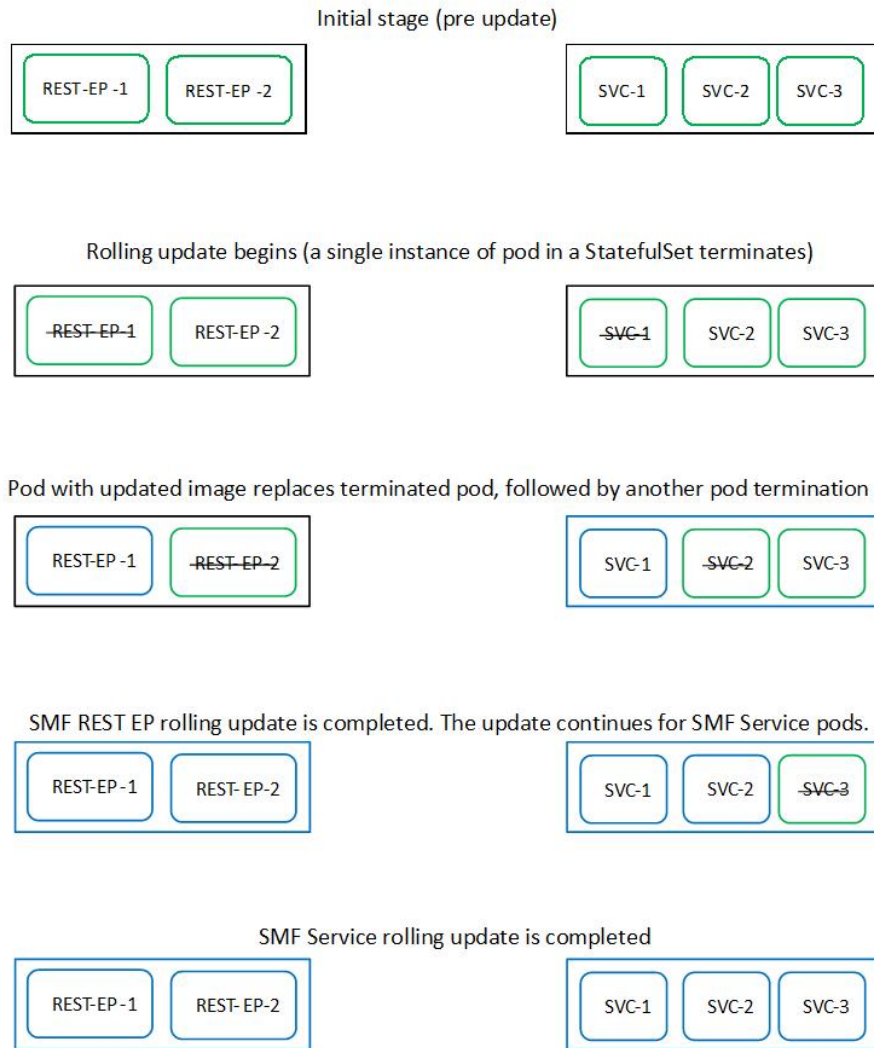
---

**Note** Each pod needs a minimum of two pods for high availability. In a worst-case scenario, the processing capacity of the pod may briefly reduce to 50% while the software update is in-progress.

---

The following figure illustrates an SMF rolling update for SMF REST Endpoint pods (two replicas) on Protocol worker nodes along with SMF Service pods (three replicas) on Service worker nodes.

Figure 12: SMF Rolling Update



442797

## Prerequisites

The prerequisites for upgrading SMF are:

- All the nodes – including all the pods in the node – are up and running.
- A patch version of the SMF software.



**Note** Currently, major versions does not support rolling upgrade.




---

**Important** Trigger rolling upgrade only when the CPU usage of the nodes is less than 50%.

---

## SMF Health Check

You need to perform an health check to ensure that all the services are running and nodes are in ready state. To perform an health check:

1. Log in to master node and use the following configuration

```
kubectl get pods -n smi
kubectl get nodes
kubectl get pod --all-namespaces -o wide
kubectl get pods -n smf-wsp -o wide
kubectl get pods -n cee-wsp -o wide
kubectl get pods -n smi-vips -o wide
helm list
kubectl get pods -A | wc -l
```




---

**Important** Ensure that all the services are running and nodes are in ready state before you proceed further.

---

## Preparing the Upgrade

This section describes the procedure involved creating a backup configuration, logs and deployment files. To backup the files:

1. Log in to the SMI Cluster Manager Node as an **ubuntu** user.
2. Create a new directory for deployment.

**Example:**

```
test@smismf-cm01:~$ mkdir -p "temp_$(date +%m%d%Y_T%H%M)" && cd "$_"
```

3. Move all the working files into the newly created deployment directory.
4. Untar the *smf* deployment file.

**Example:**

```
test@smi1smf01-cm01:~/temp_08072019_T1651$ tar -xzvf smf.2020.01.0-1.SPA.tgz
./
./smf_REL_KEY-CCO_RELEASE.cer
./cisco_x509_verify_release.py
./smf.2020.01.0-1.tar
./smf.2020.01.0-1.tar.signature.SPA
./smf.2020.01.0-1.tar.SPA.README
```

5. Verify the downloaded image.

**Example:**

```
test@smi1smf01-cm01:~/temp_08072019_T1651$ cat smf.2020.01.0-1.tar.SPA.README
```



**Important** Follow the procedure mentioned in the *SPA.README* file to verify the build before proceeding to the next step.

## Back Up Ops Center Configuration

This section describes the procedure involved in creating a backup of the Ops Center configurations.

To perform a backup of the Ops Center configurations:

1. Log in to SMI Cluster Manager node as an **ubuntu** user.
2. Run the following command to backup the SMI Ops Center configuration to `/home/ubuntu/smiops.backup` file.

```
ssh -p <port_number> admin@$(kubectl get svc -n smi | grep
'.*netconf.*<port_number>' | awk '{ print $4 }') "show run | nomore"
> smiops.backup_$(date +%m%d%Y_T%H%M')
```

3. Run the following command to backup the CEE Ops Center configuration to `/home/ubuntu/ceeops.backup` file.

```
ssh admin@<cee-vip> "show run | nomore" > ceeops.backup_$(date
+%m%d%Y_T%H%M')
```

4. Run the following command to backup the SMF Ops Center configuration to `/home/ubuntu/smfops.backup` file.

```
ssh admin@<smf-vip> "show run | nomore" > smfops.backup_$(date
+%m%d%Y_T%H%M')
```

## Back Up CEE and SMF Ops Center Configuration

This section describes the procedure involved in creating a backup of CEE and Ops Center configuration from the master node. To perform a backup of CEE and Ops Center configuration:

1. Log in to the master node as an **ubuntu** user.
2. Create a directory to backup the configuration files.

```
mkdir backups_$(date +%m%d%Y_T%H%M') && cd "$_"
```

3. Backup the SMF Ops Center configuration and verify the line count of the backup files.

```
ssh -p <port_number> admin@$(kubectl get svc -n $(kubectl get namespaces
| grep -oP 'smf-(\d+|\w+)') | grep <port_number> | awk '{ print $3
}') "show run | nomore" > smfops.backup_$(date +%m%d%Y_T%H%M') && wc
-l smfops.backup_$(date +%m%d%Y_T%H%M')
```

### Example:

```
ubuntu@posmf-mas01:~/backups_09182019_T2141$ ssh -p 2024 admin@$(kubectl get svc -n
$(kubectl get namespaces | grep -oP 'smf-(\d+|\w+)') | grep <port_number> | awk '{ print
$3 }') "show run | nomore" > smfops.backup_$(date +%m%d%Y_T%H%M') && wc -l
smfops.backup_$(date +%m%d%Y_T%H%M')
admin@<ipv4address>'s password: smf-OPS-PASSWORD
334 smfops.backup
```

- Backup the CEE Ops Center configuration and verify the line count of the backup files.

```
ssh -p <port_number> admin@$(kubectl get svc -n $(kubectl get namespaces
| grep -oP 'cee-(\d+|\w+)') | grep <port_number> | awk '{ print $3
}') "show run | nomore" > ceeops.backup_$(date +%m%d%Y_T%H%M') && wc
-l ceeops.backup_$(date +%m%d%Y_T%H%M')
```

**Example:**

```
ubuntu@posmf-mas01:~/backups_09182019_T2141$ ssh -p <port_number> admin@$(kubectl get
svc -n $(kubectl get namespaces | grep -oP 'cee-(\d+|\w+)') | grep <port_number> | awk
'{ print $3 }') "show run | nomore" > ceeops.backup_$(date +%m%d%Y_T%H%M') && wc -l
ceeops.backup_$(date +%m%d%Y_T%H%M')
admin@<ipv4address>'s password: CEE-OPS-PASSWORD
233 ceeops.backup
```

- Move the SMI Ops Center backup file (from the SMI Cluster Manager) to the backup directory.

```
scp $(grep cm01 /etc/hosts | awk '{ print $1
}'):/home/ubuntu/smiops.backup_$(date +%m%d%Y_T%H%M') .
```

**Example:**

```
ubuntu@posmf-mas01:~/backups_09182019_T2141$ scp $(grep cm01 /etc/hosts | awk '{ print
$1 }'):/home/ubuntu/smiops.backup_$(date +%m%d%Y_T%H%M') .
ubuntu@<ipv4address>'s password: SMI-CM-PASSWORD
smiops.backup                                100% 9346      22.3MB/s
00:00
```

- Verify the line count of the backup files.

**Example:**

```
ubuntu@posmf-mas01:~/backups_09182019_T2141$ wc -l *
233 ceeops.backup
334 smfops.backup
361 smiops.backup
928 total
```

## Staging a New SMF Image

This section describes the procedure involved in staging a new SMF image before initiating the upgrade.

To stage the new SMF image:

- Download and verify the new SMF image.
- Log in to the SMI Cluster Manager node as an **ubuntu** user.
- Copy the images to **Uploads** directory.

```
sudo mv <smf_new_image.tar> /data/software/uploads
```




---

**Note** The SMI uses the new image present in the **Uploads** directory to upgrade.

---

- Verify whether the image is picked up by the SMI for processing from the **Uploads** directory.

```
sleep 30; ls /data/software/uploads
```

**Example:**

```
ubuntu@posmf-cm01:~/temp_08072019_T1651$ sleep 30; ls /data/software/uploads
ubuntu@posmf-cm01:~/temp_08072019_T1651$
```

5. Verify whether the images were successfully picked up and processed.

**Example:**

```
auser@unknown:$ sudo du -sh /data/software/packages/*
1.6G /data/software/packages/cee.2019.07
5.3G /data/software/packages/smf.2019.08-04
16K /data/software/packages/sample
```




---

**Note** The SMI must unpack the images into the **packages** directory successfully to complete the staging.

---

## Triggering the Rolling Software Upgrade

The SMF utilizes the SMI Cluster Manager to perform a rolling software update. To update SMF using SMI Cluster Manager, use the following configurations:




---

**Important** Before you begin, ensure that SMF is up and running with the current version of the software.

---

1. Log in to SMI Cluster Manager Ops Center.
2. Download the latest TAR ball from the URL.

```
software-packages download url
```

**Example:**

```
SMI Cluster Manager# software-packages download <url>
```

3. Verify whether the TAR balls are loaded.

```
software-packages list
```

**Example:**

```
SMI Cluster Manager# software-packages list
[ smf-2019-08-21 ]
[ sample ]
```

4. Update the product repository URL with the latest version of the product chart.




---

**Note** If the repository URL contains multiple versions, the Ops Center automatically selects the latest version.

---

```
configure
cluster cluster_name
ops-centers app_name smf_instance_name
repository url
exit
exit
```

**Example:**

```
SMI Cluster Manager# config
SMI Cluster Manager(config)# clusters test2
SMI Cluster Manager(config-clusters-test2)# ops-centers smf data
SMI Cluster Manager(config-ops-centers-smf/data)# repository <url>
SMI Cluster Manager(config-ops-centers-smf/data)# exit
SMI Cluster Manager(config-clusters-test2)# exit
```

5. Run the **cluster sync** command to update to the latest version of the product chart.

```
clusters cluster_name actions sync run
```

**Example:**

```
SMI Cluster Manager# clusters test2 actions sync run
```



**Important**

- The cluster synchronization updates the SMF Ops Center, which in turn updates the application pods (through **helm sync** command) one at a time automatically.
- When you trigger rolling upgrade on a specific pod, the SMF avoids routing new calls to that pod.
- The SMF honors in-progress call by waiting for 30 seconds before restarting the pod where rolling upgrade is initiated. Also, the SMF establishes all the in-progress calls completely within 30 seconds during the upgrade period (maximum call-setup time is 10 seconds).



**Note**

- **software-packages download url** – Specifies the software packages to be downloaded through HTTP/HTTPS.
- **software-packages list** – Specifies the list of available software packages.
- **cluster** – Specifies the K8s cluster.
- *cluster\_name* – Specifies the name of the cluster.
- **ops-centers app\_name instance\_name** – Specifies the product Ops Center and instance. *app\_name* is the application name. *instance\_name* is the name of the instance.
- **repository url** – Specifies the local registry URL for downloading the charts.
- **actions** – Specifies the actions performed on the cluster.
- **sync run** – Triggers the cluster synchronization.

## Monitoring the Upgrade

You can monitor the status of the upgrade through SMI Cluster Manager Ops Center. To monitor the upgrade status, use the following configurations:

**configure**

```
clusters cluster_name actions sync run debug true
clusters cluster_name actions sync logs
monitor sync-logs cluster_name
```

```
clusters cluster_name actions sync status
exit
```

**Example:**

```
SMI Cluster Manager# clusters test1 actions sync run
SMI Cluster Manager# clusters test1 actions sync run debug true
SMI Cluster Manager# clusters test1 actions sync logs
SMI Cluster Manager# monitor sync-logs test1
SMI Cluster Manager# clusters test1 actions sync status
```

**Important**

- **clusters** *cluster\_name* – Specifies the information about the nodes to be deployed. *cluster\_name* is the name of the cluster.
- **actions** – Specifies the actions performed on the cluster.
- **sync run** – Triggers the cluster synchronization.
- **sync logs** – Shows the current cluster synchronization logs.
- **sync status** – Shows the current status of the cluster synchronization. **debug true** – Enters the debug mode.
- **monitor sync logs** – Monitors the cluster synchronization process.

**Important**

You can view the pod details after the upgrade through CEE Ops Center. For more information on pod details, see [Viewing the Pod Details](#) section.

## Viewing the Pod Details

You can view the details of the current pods through CEE Ops Center. To view the pod details, use the following command (in CEE Ops Center CLI):

```
cluster pods instance_name pod_name detail
```

**Note**

- **cluster pods** – Specifies the current pods in the cluster.
- *instance\_name* – Specifies the name of the instance.
- *pod\_name* – Specifies the name of the pod.
- **detail** – Displays the details of the specified pod.

The following example displays the details of the pod named *alertmanager-0* in the *smf-data* instance.

**Example:**

```
cee# cluster pods smf-data alertmanager-0 detail
details apiVersion: "v1"
kind: "Pod"
metadata:
  annotations:
```



```

    alertmanager.io/scrape: "true"
    cni.projectcalico.org/podIP: "<ipv4address/subnet>"
    config-hash: "5532425ef5fd02add051cb759730047390b1bce51da862d13597dbb38dfbde86"
    creationTimestamp: "2020-02-26T06:09:13Z"
    generateName: "alertmanager-"
    labels:
      component: "alertmanager"
      controller-revision-hash: "alertmanager-67cdb95f8b"
      statefulset.kubernetes.io/pod-name: "alertmanager-0"
    name: "alertmanager-0"
    namespace: "smf"
    ownerReferences:
      - apiVersion: "apps/v1"
        kind: "StatefulSet"
        blockOwnerDeletion: true
        controller: true
        name: "alertmanager"
        uid: "82a11da4-585e-11ea-bc06-0050569ca70e"
    resourceVersion: "1654031"
    selfLink: "/api/v1/namespaces/smf/pods/alertmanager-0"
    uid: "82aee5d0-585e-11ea-bc06-0050569ca70e"
  spec:
    containers:
      - args:
          - "/alertmanager/alertmanager"
          - "--config.file=/etc/alertmanager/alertmanager.yml"
          - "--storage.path=/alertmanager/data"
          - "--cluster.advertise-address=$(POD_IP):6783"
        env:
          - name: "POD_IP"
            valueFrom:
              fieldRef:
                apiVersion: "v1"
                fieldPath: "status.podIP"
        image: "<path_to_docker_image>"
        imagePullPolicy: "IfNotPresent"
        name: "alertmanager"
        ports:
          - containerPort: 9093
            name: "web"
            protocol: "TCP"
        resources: {}
        terminationMessagePath: "/dev/termination-log"
        terminationMessagePolicy: "File"
        volumeMounts:
          - mountPath: "/etc/alertmanager/"
            name: "alertmanager-config"
          - mountPath: "/alertmanager/data/"
            name: "alertmanager-store"
          - mountPath: "/var/run/secrets/kubernetes.io/serviceaccount"
            name: "default-token-kbjnx"
            readOnly: true
        dnsPolicy: "ClusterFirst"
        enableServiceLinks: true
        hostname: "alertmanager-0"
        nodeName: "for-smi-cdl-1b-worker94d84de255"
        priority: 0
        restartPolicy: "Always"
        schedulerName: "default-scheduler"
        securityContext:
          fsGroup: 0
          runAsUser: 0
        serviceAccount: "default"
        serviceAccountName: "default"

```

```

subdomain: "alertmanager-service"
terminationGracePeriodSeconds: 30
tolerations:
- effect: "NoExecute"
  key: "node-role.kubernetes.io/oam"
  operator: "Equal"
  value: "true"
- effect: "NoExecute"
  key: "node.kubernetes.io/not-ready"
  operator: "Exists"
  tolerationSeconds: 300
- effect: "NoExecute"
  key: "node.kubernetes.io/unreachable"
  operator: "Exists"
  tolerationSeconds: 300
volumes:
- configMap:
  defaultMode: 420
  name: "alertmanager"
  name: "alertmanager-config"
- emptyDir: {}
  name: "alertmanager-store"
- name: "default-token-kbjnx"
  secret:
  defaultMode: 420
  secretName: "default-token-kbjnx"
status:
  conditions:
  - lastTransitionTime: "2020-02-26T06:09:02Z"
    status: "True"
    type: "Initialized"
  - lastTransitionTime: "2020-02-26T06:09:06Z"
    status: "True"
    type: "Ready"
  - lastTransitionTime: "2020-02-26T06:09:06Z"
    status: "True"
    type: "ContainersReady"
  - lastTransitionTime: "2020-02-26T06:09:13Z"
    status: "True"
    type: "PodScheduled"
  containerStatuses:
  - containerID: "docker://821ed1a272d37e3b4c4c9c1ec69b671a3c3fe6eb4b42108edf44709b9c698ccd"

    image: "<path_to_docker_image>"
    imageID: "docker-pullable://<path_to_docker_image>"
    lastState: {}
    name: "alertmanager"
    ready: true
    restartCount: 0
    state:
      running:
        startedAt: "2020-02-26T06:09:05Z"
    hostIP: "<host_ipv4address>"
    phase: "Running"
    podIP: "<pod_ipv4address>"
    qosClass: "BestEffort"
    startTime: "2020-02-26T06:09:02Z"
cee#

```



## CHAPTER 6

# Pods and Services Reference

- [Feature Summary and Revision History, on page 61](#)
- [Feature Description, on page 62](#)
- [Associating Pods to the Nodes, on page 69](#)
- [Viewing the Pod Details and Status, on page 70](#)

## Feature Summary and Revision History

### Summary Data

*Table 12: Summary Data*

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 13: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

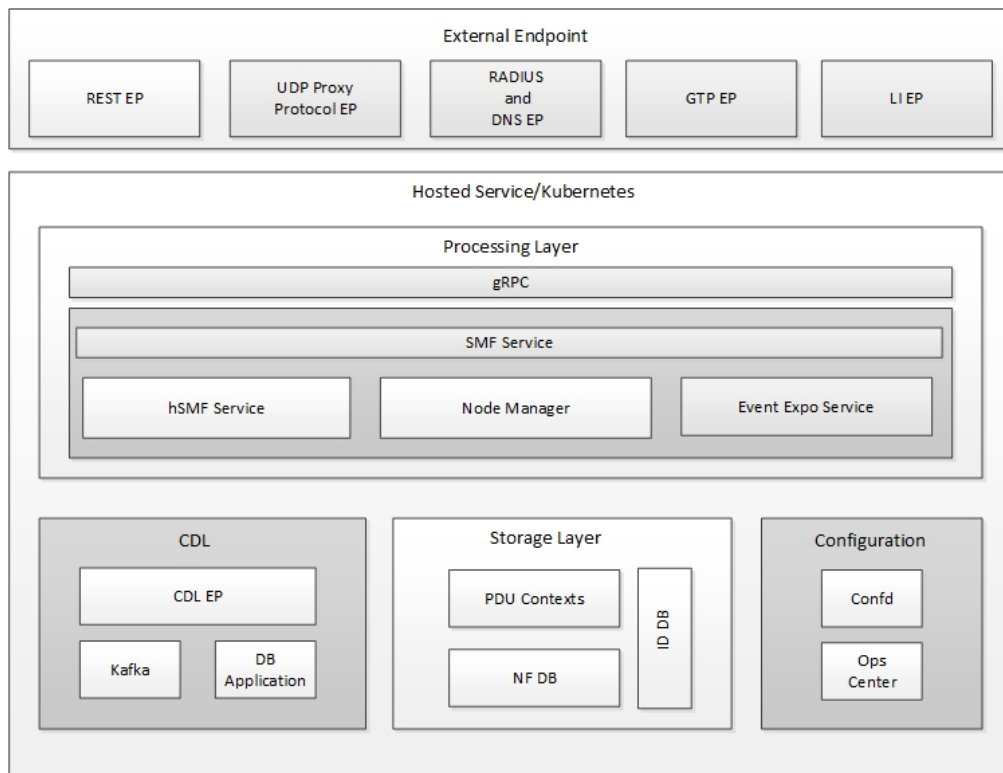
## Feature Description

The SMF is built on the Kubernetes cluster strategy, which implies that it has adopted the native concepts of containerization, high availability, scalability, modularity, and ease of deployment. To achieve the benefits offered by Kubernetes, SMF uses the construct that includes the components such as pods and services.

Depending on your deployment environment, the SMF deploys the pods on the virtual machines that you have configured. Pods operate through the services that are responsible for the intrapod communications. If the machine hosting the pods fail or experiences network disruption, the pods are terminated or deleted. However, this situation is transient and SMF spins new pods to replace the invalid pods.

The following workflow provides a high-level visibility into the host machines, and the associated pods and services. It also represents how the pods interact with each other. The representation might defer based on your deployment infrastructure.

**Figure 13: Communication Workflow of Pods**



Kubernetes deployment includes the kubectl command-line tool to manage the Kubernetes resources in the cluster. You can manage the pods, nodes, and services.

For generic information on the Kubernetes concepts, see the Kubernetes documentation.

For more information on the Kubernetes components in SMF, see the following:

- Pods
- Services

## Pods

A pod is a process that runs on your Kubernetes cluster. Pod encapsulates a granular unit known as a container. A pod contains one or multiple containers.

Kubernetes deploys one or multiple pods on a single node which can be a physical or virtual machine. Each pod has a discrete identity with an internal IP address and port space. However, the containers within a pod can share the storage and network resources.

The following tables list the SMF and Common Execution Environment (CEE) pod names and the hosts on which they are deployed depending on the labels that you assign. For information on how to assign the labels, see [Associating Pods to the Nodes](#).

**Table 14: SMF Pods**

Pod Name	Description	Host Name
api-smf-ops-center	Functions as the <i>confD</i> API pod for the SMF Ops Center.	OAM
base-entitlement-smf	Supports Smart Licensing feature.	OAM
cache-pod	Operates as the pod to cache any sort of system information that will be used by other pods as applicable.	Protocol
cdl-ep-session-c1	Provides an interface to the CDL.	Session
cdl-index-session-c1	Preserves the mapping of keys to the session pods.	Session
cdl-slot-session-c1	Operates as the CDL Session pod to store the session data.	Session
documentation	Contains the documentation.	OAM
etcd-smf-etcd-cluster	Hosts the etcd for the SMF application to store information such as pod instances, leader information, NF-UUID, endpoints, and so on.	OAM
grafana-dashboard-app-infra	Contains the default dashboard of app-infra metrics in Grafana.	OAM
grafana-dashboard-cdl	Contains the default dashboard of CDL metrics in Grafana.	OAM
grafana-dashboard-smf	Contains the default dashboard of SMF-service metrics in Grafana.	OAM
gtpc-ep-n0	Operates as GTPC endpoint of SMF.	Protocol
kafka	Hosts the Kafka details for the CDL replication.	Protocol
li-ep-n0	Operates as Lawful Intercept endpoint of SMF.	Protocol
oam-pod	Operates as the pod to facilitate Ops Center actions like show commands, configuration commands, monitor protocol monitor subscriber, and so on.	OAM
ops-center-smf-ops-center	Acts as the SMF Ops Center.	OAM
smart-agent-smf-ops-center	Operates as the utility pod for the SMF Ops Center.	OAM

Pod Name	Description	Host Name
nodemgr-n0	Performs node level interactions such as N4 link establishment, management (heart-beat), and so on. Also, generates unique identifiers such as UE IP address, SEID, CHF-ID, Resource URI, and so on.	Service
protocol-n0	Operates as encoder and decoder of application protocols (PCF, GTP, RADIUS, and so on) whose underlying transport protocol is UDP.	Protocol
smf-radius-dns-n0	Operates as RADIUS and DNS endpoint of SMF.	Protocol
rest-ep-n0	Operates as REST endpoint of SMF for HTTP2 communication.	Protocol
service-n0	Contains main business logic of SMF.	Service
udp-proxy	Operates as proxy for all UDP messages. Owns UDP client and server functionalities.	Protocol
swift-smf-ops-center	Operates as the utility pod for the SMF Ops Center.	OAM
zookeeper	Assists Kafka for topology management.	OAM

Table 15: CEE Pods

Pod Name	Description	Host Name
alert-logger	Stores the history of active and resolved alerts.	OAM
alertmanager	Duplicates alerts and sends out resolution of alerts when they are resolved in Prometheus.	OAM
api-cee-global-ops-center	Functions as the confD API pod for the CEE Ops Center.	OAM
bulk-stats	Assists to retrieve bulkstats saved by Prometheus containers.	OAM
cee-global-product-documentation	Contains the product documentation (API, CLI, and so on).	OAM
core-retriever	Assists in retrieving the core dumps.	All the nodes except ETCD nodes.
documentation	Contains the documentation (metrics and usage).	OAM
grafana-dashboard-metrics	Assists in collating Grafana metrics on the dashboard.	OAM
grafana	Contains the Grafana metrics for CEE.	OAM
kube-state-metrics	Assists in generating metrics about the state of Kubernetes objects: node status, node capacity (CPU and memory), and so on.	OAM

Pod Name	Description	Host Name
logs-retriever	Assists in retrieving Kernel, Kubelet, and Container level logs through output to JournalD driver.	All the nodes except ETCD nodes.
node-exporter	Exports the node metrics.	All the nodes.
ops-center-cee-global-ops-center	Provides NETCONF and CLI interface to the application.	OAM
path-provisioner	Provisions the local storage volume.	All the nodes except ETCD nodes.
pgpool	<i>Pgpool</i> is a middleware that works between <i>PostgreSQL</i> servers and a <i>PostgreSQL</i> database.	OAM
postgres	Storage of alerts and Grafana dashboards.	OAM
prometheus-hi-res	Stores all metrics and generates alerts by alerting rules.	OAM
prometheus-rules	Contains the default alerting rules and recording rules for Prometheus.	OAM
prometheus-scrapeconfigs-synch	Synchronizes the Prometheus scrape configuration.	OAM
pv-manager	Provisions the local storage volume.	OAM
pv-provisioner	Provisions the local storage volume.	OAM
show-tac-manager	Assists in creating and deleting debug package.	OAM
smart-agent-cee-global-ops-center	Operates as the utility pod for the CEE Ops Center.	OAM
snmp-trapper	Sends the SNMP traps based on triggered alerts.	OAM
swift-cee-global-ops-center	Operates as the utility pod for the CEE Ops Center	OAM
thanos-query-hi-res	Implements the Thanos query for Prometheus HA.	OAM
fluentbit	Assists in log forwarding to the external logs collector.	All the nodes except ETCD nodes.

## Services

The SMF configuration is composed of several microservices that run on a set of discrete pods. Microservices are deployed during the SMF deployment. SMF uses these services to enable communication between the pods. When interacting with another pod, the service identifies the pod's IP address to initiate the transaction and acts as an endpoint for the pod.

The following table describes the SMF services and the pod on which they run.

Table 16: SMF Services and Pods

Service Name	Pod Name	Description
base-entitlement-smf	base-entitlement-smf	Supports Smart Licensing feature.
datastore-ep-session	cdl-ep-session-c1	Responsible for the CDL session.
datastore-notification-ep	smf-rest-ep	Responsible for sending the notifications from the CDL to the <i>smf-service</i> through <i>smf-rest-ep</i> .
datastore-tls-ep-session	cdl-ep-session-c1	Responsible for the secure CDL connection.
documentation	documentation	Responsible for the SMF documents.
etcd	etcd-smf-etcd-cluster-0, etcd-smf-etcd-cluster-1, etcd-smf-etcd-cluster-2	Responsible for pod discovery within the namespace.
etcd-smf-etcd-cluster-0	etcd-smf-etcd-cluster-0	Responsible for synchronization of data among the <i>etcd</i> cluster.
etcd-smf-etcd-cluster-1	etcd-smf-etcd-cluster-1	Responsible for synchronization of data among the <i>etcd</i> cluster.
etcd-smf-etcd-cluster-2	etcd-smf-etcd-cluster-2	Responsible for synchronization of data among the <i>etcd</i> cluster.
grafana-dashboard-app-infra	grafana-dashboard-app-infra	Responsible for the default dashboard of app-infra metrics in Grafana.
grafana-dashboard-cdl	grafana-dashboard-cdl	Responsible for the default dashboard of CDL metrics in Grafana.
grafana-dashboard-smf	grafana-dashboard-smf	Responsible for the default dashboard of SMF-service metrics in Grafana.
gtpc-ep	gtpc-ep-n0	Responsible for inter-pod communication with GTP-C pod.
helm-api-smf-ops-center	api-smf-ops-center	Manages the Ops Center API.
kafka	kafka	Processes the Kafka messages.
li-ep	li-ep-n0	Responsible for lawful-intercept interactions.
local-ldap-proxy-smf-ops-center	ops-center-smf-ops-center	Responsible for leveraging Ops Center credentials by other applications like Grafana.
oam-pod	oam-pod	Responsible to facilitate Exec commands on the Ops Center.



Service Name	Pod Name	Description
ops-center-smf-ops-center	ops-center-smf-ops-center	Manages the SMF Ops Center.
ops-center-smf-ops-center-expose-cli	ops-center-smf-ops-center	To access SMF Ops Center with external IP address.
smart-agent-smf-ops-center	smart-agent-smf-ops-center	Responsible for the SMF Ops Center API.
smf-sbi-service	smf-rest-ep	Responsible for routing incoming HTTP2 messages to REST-EP pods.
smf-n10-service	smf-rest-ep	Responsible for routing incoming N10 messages to REST-EP pods.
smf-n11-service	smf-rest-ep	Responsible for routing incoming N11 messages to REST-EP pods.
smf-n40-service	smf-rest-ep	Responsible for routing incoming N40 messages to REST-EP pods.
smf-n7-service	smf-rest-ep	Responsible for routing incoming N7 messages to REST-EP pods.
smf-nrf-service	smf-rest-ep	Responsible for routing incoming NRF messages to REST-EP pod.
smf-nodemgr	smf-nodemgr	Responsible for inter-pod communication with <i>smf-nodemgr</i> pod.
smf-protocol	smf-protocol	Responsible for inter-pod communication with <i>smf-protocol</i> pod
smf-radius-dns	smf-radius-dns	Responsible for inter-pod communication with <i>smf-radius-dns</i> pod
smf-rest-ep	smf-rest-ep	Responsible for inter-pod communication with <i>smf-rest-ep</i> pod
smf-service	smf-service	Responsible for inter-pod communication with <i>smf-service</i> pod
swift-smf-ops-center	swift	Operates as the utility pod for the SMF Ops Center
zookeeper	zookeeper	Assists Kafka for topology management
zookeeper-service	zookeeper	Assists Kafka for topology management

## Open Ports and Services

The SMF uses different ports for communication purposes. The following table describes the default open ports and the associated services.

**Table 17: Open Ports and Services**

Port	Service	Usage
22	SSH	SMI uses this TCP port to communicate with the virtual machines.
80	HTTP	SMI uses this TCP port for providing Web access to CLI, Documentation, and TAC.
443	SSL/HTTP	SMI uses this TCP port for providing Web access to CLI, Documentation, and TAC.
1434	ms-sql-m	SMI uses this UDP port to communicate with BIRD. BIRD is an open source BGP client that is used to exchange routing information between hosts.
6443	HTTP	SMI uses this port to communicate with the Kubernetes API server.
9100	jetdirect	SMI uses this TCP port to communicate with the Node exporter.  Node Exporter is a Prometheus exporter for hardware and OS metrics with pluggable metric collectors. It allows you to measure various machine resources such as memory, disk, and CPU utilization.
10250	SSL/HTTP	SMI uses this TCP port to communicate with Kubelet.  Kubelet is the lowest level component in Kubernetes. It is responsible for what is running on an individual machine. You can think of it as a process watcher like supervisor but focused on running containers. It has one job: given a set of containers to run, make sure they are all running.
10251		SMI uses this TCP port to interact with the Kube scheduler.  Kube scheduler is the default scheduler for Kubernetes and runs as part of the control plane. A scheduler watches for newly created Pods that have no node assigned. For every Pod that the scheduler discovers, the scheduler becomes responsible for finding the best Node for that Pod to run on
10252	apollo-relay	SMI uses this TCP port to interact with the Kube controller.  The Kubernetes controller manager is a daemon that embeds the core control loops shipped with Kubernetes. The controller is a control loop that watches the shared state of the cluster through the apiserver and makes changes attempting to move the current state towards the desired state.
10256	HTTP	SMI uses this TCP port to interact with the Kube proxy.  Kube proxy is a network proxy that runs on each node in your cluster, implementing part of the Kubernetes Service concept. Kube proxy maintains network rules on nodes. These network rules allow network communication to your Pods from network sessions inside or outside of your cluster.

## Converged Core Refactoring Changes

This section describes the changes related to converged core refactoring in this chapter.

### SMF Pods

In the converged core architecture, the pod names mentioned in the following table are renamed.

**Table 18: Pod Names**

Non-converged Core	Converged Core
smf-nodemgr-n0	nodemgr-n0
smf-protocol-n0	protocol-n0
smf-rest-ep-n0	rest-ep-n0
smf-service-n0	service-n0
smf-udp-proxy	udp-proxy

## Associating Pods to the Nodes

This section describes how to associate a pod to the node based on their labels.

After you have configured a cluster, you can associate pods to the nodes through labels. This association enables the pods to get deployed on the appropriate node based on the key-value pair.

Labels are required for the pods to identify the nodes where they must get deployed and to run the services. For example, when you configure the protocol-layer label with the required key-value pair, the pods are deployed on the nodes that match the key-value pair.

1. To associate pods to the nodes through the labels, use the following configuration:

```

configure
  label
    cdl-layer
      key key_value
      value value
    oam-layer
      key key_value
      value value
    protocol-layer
      key key_value
      value value
    service-layer
      key key_value
      value value
  end

```

**NOTES:**

- If you opt not to configure the labels, then SMF assumes the labels with the default key-value pair.
  - **label** { **cdl-layer** { **key** *key\_value* | **value** *value* } }: Configures the key value pair for CDL.
  - **oam-layer** { **key** *key\_value* | **value** *value* } }: Configures the key value pair for OAM layer.
  - **protocol-layer** { **key** *key\_value* | **value** *value* } }: Configures the key value pair for protocol layer.
  - **service-layer** { **key** *key\_value* | **value** *value* } }: Configures the key value pair for the service layer.

## Viewing the Pod Details and Status

If the service requires additional pods, SMF creates and deploys the pods. You can view the list of pods that are participating in your deployment through the SMF Ops Center.

You can run the `kubectl` command from the master node to manage the Kubernetes resources.

1. To view the comprehensive pod details, use the following command.

```
kubectl get pods -n smf pod_name -o yaml
```

The pod details are available in YAML format. The output of this command results in the following information:

- The IP address of the host where the pod is deployed.
- The service and application that is running on the pod.
- The ID and name of the container within the pod.
- The IP address of the pod.
- The current state and phase in which the pod is.
- The start time from which pod is in the current state.

Use the following command to view the summary of the pod details.

```
kp get pods -n smf_namespace -o wide
```

## States

Understanding the pod's state lets you determine the current health and prevent the potential risks. The following table describes the pod's states.

**Table 19: Pod States**

State	Description
Running	The pod is healthy and deployed on a node. It contains one or more containers.
Pending	The application is in the process of creating the container images for the pod.
Succeeded	Indicates that all the containers in the pod are successfully terminated. These pods cannot be restarted.

State	Description
Failed	One or more containers in the pod have failed the termination process. The failure occurred as the container either exited with non zero status or the system terminated the container.
Unknown	The state of the pod could not be determined. Typically, this could be observed because the node where the pod resides was not reachable.





## CHAPTER 7

# 3GPP Specification Compliance for SMF Interfaces

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 73](#)
- [Feature Description, on page 74](#)
- [Configuring Interfaces, on page 75](#)
- [Sample Configuration, on page 76](#)

## Feature Summary and Revision History

### Summary Data

*Table 20: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 21: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

The SMF currently supports either the December 2018 compliance version of 3GPP specification or the June 2019 compliance version of 3GPP specification for the SMF interfaces such as N1, N2, N4, N7, N10, N11, N40, and Nnrf. The SMF processes the messages from these interfaces as per the compliance profile configured for the corresponding services. For information on the compliance profile configurations, see the [Configuring Interfaces, on page 75](#) section.

Currently, only IE encoding and decoding is supported. The existing features work with the June 2019 specification versions. No additional features in the June 2019 version are supported.



### Note

The SMF continues to support the older versions of 3GPP specifications and the compliance profile configuration controls the same for the SMF interfaces.

## Standards Compliance

The SMF is one of the control plane (CP) NFs of the 5G core network. The SMF uses different interfaces to communicate with the other NFs or nodes. For example, the N4 interface exists between the SMF and User Plane Function (UPF). Each of the SMF interfaces comply to a specific version of the 3GPP specification depending on the compliance version supported.

Use the following table to determine the compliance mapping of each SMF interface and the 3GPP Standards specification versions.

Interface	Relationship	3GPP Specification	Version
N11	Between AMF and SMF	29.518 29.502	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0
N7	Between PCF and SMF	29.512	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0
N4	Between UPF and SMF	29.244	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0
Nnrf	Between NRF and SMF	29.510	For December 2018 Compliance Support: 15.0.0 For June 2019 Compliance Support: 15.4.0
N10	Between UDM and SMF	29.503	For December 2018 Compliance Support: 15.2.1 For June 2019 Compliance Support: 15.4.0



Interface	Relationship	3GPP Specification	Version
N40	Between SMF and CHF	32.291	For December 2018 Compliance Support: 15.1.0 For June 2019 Compliance Support: 15.3.0
N1	Between UE and AMF	24.501	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0
N2/NGAP	Between RAN and AMF	38.413	For December 2018 Compliance Support: 15.2.0 For June 2019 Compliance Support: 15.4.0

## Configuring Interfaces

Use the following commands to configure the SMF interfaces in compliance with the 3GPP specifications.

```

configure
  profile compliance profile_name
    service
      n1 version full version_format spec spec_version
      uri_version uri_version
      n2 version full version_format spec spec_version
      uri_version uri_version
      namf-comm version full version_format spec spec_version
      uri_version uri_version
      nchf-convergedcharging version full version_format
      spec spec_version
      uri_version uri_version
      nnrf-disc version full version_format spec spec_version
      uri_version uri_version
      nnrf-nfm version full version_format spec spec_version
      uri_version uri_version
      npcfc-smpolicycontrol version full version_format spec spec_version
      uri_version uri_version
      nsmf-pdusession version full version_format spec spec_version
      uri_version uri_version
      nudm-sdm version full version_format spec spec_version
      uri_version uri_version
      nudm-uecm version full version_format spec spec_version
      uri_version uri_version
    range
  !
  !

```




---

**Important** Service selection is based only on the specification version. In future releases, the full API version will be used.

---

**NOTES:**

- **version full:** Specifies the API full version for each service in the following format:  
 <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>]  
 The format is specified in *3GPP TS 29.501 V15.2.0, section 4.3.1.1*.
- **version spec:** Specifies the 3GPP specification version number. It can be one of the following values:
  - 15.0.0
  - 15.1.0
  - 15.2.0
  - 15.2.1
  - 15.4.0




---

**Important** Configuring the 3GPP specification version value depends on the SMF interface. Not all the preceding versions are options for the SMF interfaces. Only a combination of the preceding versions exist as options for the 3GPP version compliance configuration. For details on the compliance version, see the [Standards Compliance, on page 74](#) section.

---

For example, to support 3GPP June 2019 specification compliance for the N7 (PCF) interface, configure the specification version as *15.4.0*.

The default version number depends on the SMF interface. For example, the default version is *15.2.0* for the N7 interface. Similarly, for the N10 interface, the default version is *15.2.1*.

- **version uri:** Specifies the API version URI for each service in the following format:  
 "v" concatenated with a number  
 It can be both v1 and v2, or either v1 or v2.  
 For example, for the compliance version 15.4.0 in the NRF configuration for the service type nudm-sdm/nudm-uecm, mandate the configuration of the uri-version in the version to 'v2'. For compliance version 15.2.1, this configuration is optional.  
 For example, version v1: (- url: '{apiRoot}/nsmf-pdusession/v1')
- **service:** Specifies the service names as cited in *3GPP TS 29.510 V15.2.0, section 6.1.6.3.11*.

## Sample Configuration

The following is a sample output of the interface configuration:

```
product smf(config-compliance-comp1)# show full
profile compliance comp1
  service nsmf-pduseession
    version uri v1
    version full 1.0.0
    version spec 15.2.0
product smf(config-service-nsmf-pdu)# compliance-profile comp1
product smf(config)# show full-configuration profile smf
profile smf smf1
  service name nsmf-pdu
  -----
  compliance-profile comp1
  -----
!
!
```





## CHAPTER 8

# 4G to 5G Data Session Handover Support

- [Feature Summary](#) , on page 79
- [Feature Description](#), on page 80
- [How it Works](#), on page 80
- [Emergency SoS Support](#), on page 91

## Feature Summary

### Summary Data

*Table 22: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 23: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

The SMF leverages the 3GPP provision for the UEs that can support both 5G and 4G NAS to connect to E-UTRAN and 5G core network. With this provision, the SMF includes the EPS interworking support and acts as PGW-C+SMF. The SMF uses the S5 or S8 interface to receive the 4G Session Creation Request. The interfaces, such as the Gx, Gy, or Gz, that are used for a 4G session creation are replaced with the corresponding 5G core SBI interfaces, such as the NPCF and NCHF.

After a PDU session is created on PGW-C+SMF through E-UTRAN, MME, and S-GW, the SMF can perform the 4G to 5G data session handover.

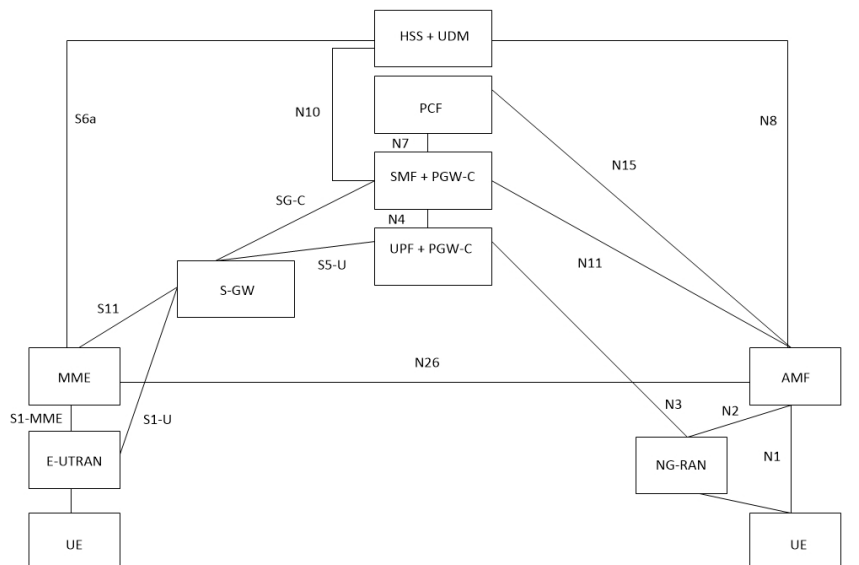
## How it Works

To interwork with EPS, a UE that supports both 5GC and EPS NAS works in one of the following modes:

- **Single-registration Mode**—In this mode, the UE has only one active MM state, which is either the RM state in 5GC or EMM state in EPS. In addition, this state is either in 5GC NAS mode or in EPS NAS mode when connected to 5GC or EPS, respectively.
- **Dual-registration Mode**—In this mode, the UE handles independent registrations for 5GC and EPS using separate RRC connections. The UE may be registered to 5GC only, EPS only, or to both 5GC and EPS.

## Architecture

This section describes the network architecture for the EPS-5G Core interworking.



## Call Flows

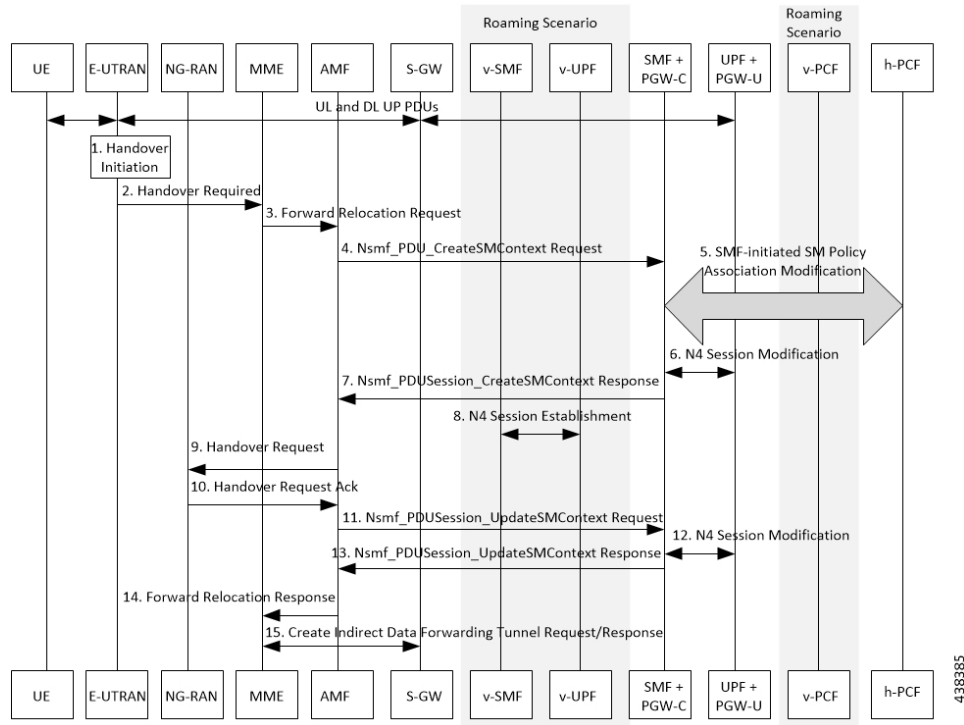
This section describes the following call flows.

- EPS to 5G Handover with N26 Interface – Preparation Call Flow
- EPS to 5G Handover with N26 Interface – Execution Call Flow
- UE Idle Mode Mobility from EPS to 5GS using N26 Interface – PDU is in Inactive State
- UE Idle Mode Mobility from EPS to 5GS using N26 interface – User Plane Connection Reactivation Request

## EPS to 5G Handover with N26 Interface – Preparation Call Flow

This section describes the call flow of the preparation of the EPS to 5G Handover with the N26 interface.

**Figure 14: Preparation Call Flow for the EPS to 5G Handover with the N26 Interface**



**Table 24: Preparation Call Flow Description for the EPS to 5G Handover with the N26 Interface**

Step	Description
1	Call handover initiation starts from UE and E-UTRAN toward each other, proceeds from E-UTRAN to the S-GW. Then for roaming calls, call handover initiation proceeds from S-GW to the UPF+P-GW-U.
2	The E-UTRAN sends the Handover Call Request to the MME.
3	The MME forwards the Relocation Request to the AMF.

Step	Description
4	The AMF invokes the NsmfPDUSessionCreateSMContext service operation on SMF. The PGW-C+SMF address identifies this service operation. The service operations can be UE EPS PDN Connection, AMF ID, or Direct Forwarding Flag. The AMF then indicates the handover preparation to avoid switching the UP path. The SMF searches for the corresponding PDU session that is based on EPS Bearer Contexts. The AMF includes Direct Forwarding Flag to inform the SMF of the applicability of indirect data forwarding.
5	If you have deployed the dynamic PCC, the SMF+PGW-C initiates the SMF-initiated SM Policy Modification toward the PCF. <b>Important</b> Cisco SMF does not support this step in this release.
6	The PGW-C+SMF sends the N4 Session Modification to PGW-U+UPF to establish the CN tunnel for a PDU Session. The PGW-U+UPF receives the uplink packets from NG-RAN. This step involves creating uplink PDRs and FARs for the 5G session along with the QFIs that are mapped from the existing 4G bearers.
7	The PGW-C+SMF sends a NsmfPDUSessionCreateSMContext Response to the AMF. This response includes PDU Session ID, S-NSSAI, and N2 SM Information.  The N2 SM Information includes PDU Session ID, S-NSSAI, QFIs, QoS Profiles, EPS Bearer Setup List, mapping between EBIs and QFIs, CN Tunnel information, and cause code details.  The SMF includes mapping between EBIs and QFIs as the N2 SM Information container. If the P-GW-C+SMF determines that session continuity from EPS to 5GS is not supported for the PDU session, then the P-GW-C+SMF does not provide the Session Manager information for the corresponding PDU session. However, the P-GW-C+SMF includes the cause code details for rejecting the PDU session transfer in the N2 SM information.
8	The V-SMF and V-UPF establish an N4 session with each other.
9	The AMF sends the Handover Request to NG-RAN.
10	The NG-RAN sends an acknowledgment for the received Handover Request to the AMF.
11	The AMF sends a NsmfPDUSessionUpdateSMContext Request, T-RAN SM N3 forwarding information list message to the SMF for updating the N3 tunnel information.  The NsmfPDUSessionUpdateSMContext request includes a PDU Session ID, S-NSSAI, and N2 SM Information. The tunnel information exists in the NGAP IE DL Forwarding UP TNL Information of the Handoff Request Acknowledgment that is received from NG-RAN.
12	The SMF+PGW-C performs the N4 session modification toward UPF+PGW-U to create the indirect tunnel to forward the DL data from eNodeB to NG-RAN. This step includes creating UL PDRs for the redirected DL data and associating FARs with them to forward the FARs to NG-RAN. The mapping of these PDRs and FARs is based on QFI and the corresponding bearer ID.
13	The PGW-C+SMF sends the NsmfPDUSessionUpdateSMContext Response to the AMF. This response includes PDU Session ID, EPS Bearer Setup List, and CN tunnel information for data forwarding. At this point, the indirect tunnels are established for DL data forwarding.
14	The AMF sends the Forward Relocation Response to the MME.
15	The MME sends the creation request for the indirect data forwarding tunnel to the S-GW. The S-GW sends the response for the indirect data forwarding tunnel to the MME.



## EPS to 5G Handover with N26 Interface – Execution Call Flow

This section describes the call flow of the execution of the EPS to 5G Handover with the N26 interface.

Figure 15: Execution Call Flow for the EPS to 5G Handover with the N26 Interface

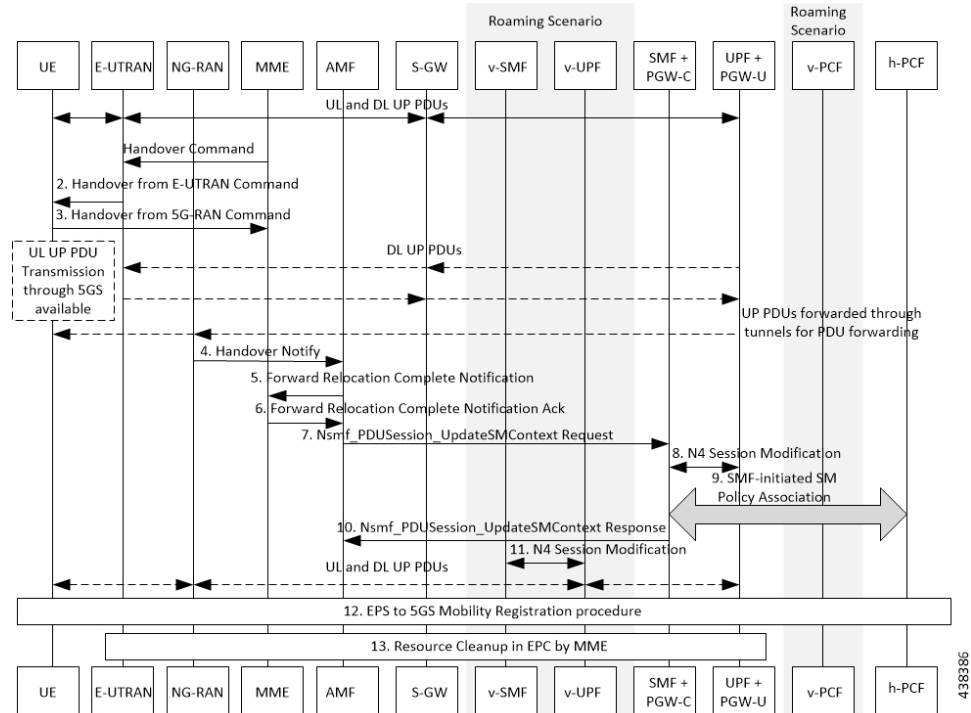


Table 25: Execution Call Flow Description for the EPS to 5G Handover with the N26 Interface

Step	Description
1	Call handover initiation starts from the UE and E-UTRAN toward each other, proceeds from E-UTRAN to S-GW. Then for roaming calls, call handover initiation proceeds from S-GW to the UPF+P-GW-U. The MME sends the handover command to E-UTRAN.
2	The E-UTRAN sends the handover command to the UE.
3	The UE sends the confirmation message to NG-RAN for the received handover to 5G-RAN.
4	The NG-RAN sends the Handover Notification message to the AMF.
5	The AMF sends the Forward Relocation Complete Notification to the MME.
6	The MME sends the Acknowledgment Response for the received Forward Relocation Complete Notification.
7	The AMF sends NsmfPDUSessionUpdateSMContext Request to SMF+PGW-C. This request includes Handover Complete Indication for PDU Session ID details. For indirect forwarding, a timer in SMF+PGW-C starts to check when resources in UPF are to be released.

Step	Description
8	The SMF performs N4 Modification Request with UPF+PGW-U to update the DL tunnel information for the FARs that are associated with DL PDRs of the 5G session. The DL data path is activated. At this point, the indirect tunnel also exists.
9	The SMF informs PCF of the RAT type change. <b>Important</b> Cisco SMF does not support this step in this release.
10	The SMF sends NsmfPDUSessionUpdateSMContext Response, with PDU Session ID, to AMF. The SMF confirms the reception of Handover Complete.
11	After the timer that started in Step 7 expires, the SMF sends N4 Modification Request to UPF. This request is to remove the PDRs and FARs that are associated with the indirect data tunnel.
12	The UE starts the EPS to 5GS mobility registration procedure and sends it to H-PCF.
13	The E-UTRAN performs the resource cleanup in EPC by MME.

## UE Idle Mode Mobility from EPS to 5GS using N26 Interface

The SMF and PGW-C support EPS to 5GS Idle Mode Mobility procedure. For Idle Mode Mobility from EPS to 5GS, the UE performs Mobility Registration Update Procedure with AMF. The AMF and SMF retrieve MM and SM contexts from EPS and move UE context from EPS to 5GS by interacting with other core NFs.

This feature enables the EPS and 5GS core network elements to support the following use cases during EPS to 5GS Idle Mode Mobility procedure.

- UE idle mode mobility from EPS to 5GS using N26 interface - PDU session in inactive state
- UE idle mode mobility from EPS to 5GS using N26 interface - User Plane connection reactivation request

### PDU Session is in Inactive State

The following call flows captures information on UE Idle Mode Mobility from EPS to 5GS using N26 Interface when PDU session is in inactive state.

Figure 16: PDU Session in Inactive State

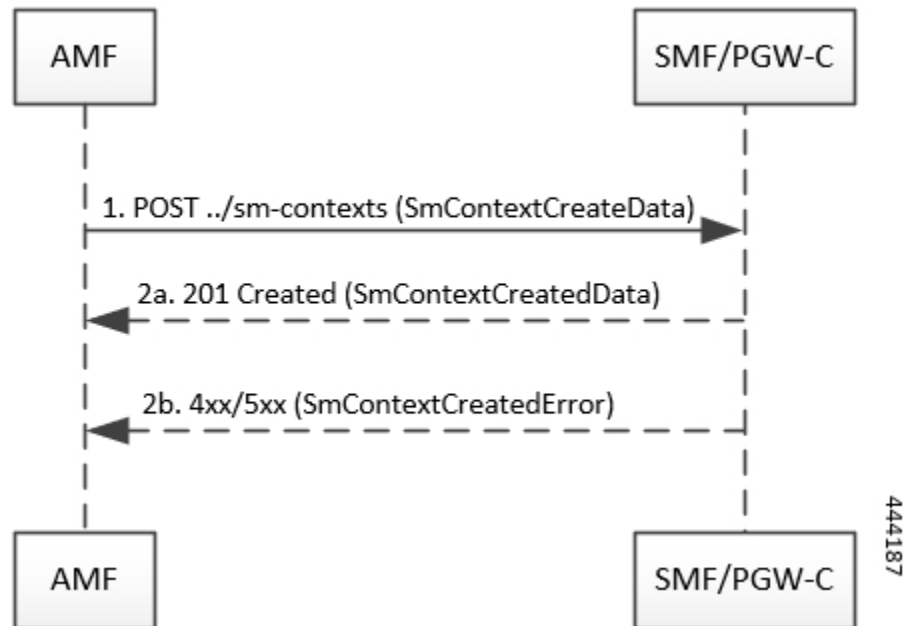


Table 26: PDU Session in Inactive State

Step	Description
1	<p>AMF sends a POST request towards SMF/PGW-C of each UE EPS PDN connection with following information:</p> <ul style="list-style-type: none"> <li>• UE EPS PDN connection, including the EPS bearer contexts, received from the MME, representing the individual SM context to be created.</li> <li>• EPS Bearer Context Status attribute, indicating the status of all the EPS bearer contexts in the UE, if corresponding information is received in the Registration Request from the UE.</li> </ul>
2	<p>Upon receipt of such a request, if:</p> <ul style="list-style-type: none"> <li>• a corresponding PDU session is found based on the EPS bearer contexts.</li> <li>• the default EPS bearer context of the corresponding PDU session is not reported as inactive by the UE in the EPS Bearer Connection Status attribute, if received; and</li> <li>• it is possible to proceed with moving the PDN connection to 5GS.</li> </ul>

Step	Description
2a	<p>SMF returns a 201 Created response including the following information:</p> <ul style="list-style-type: none"> <li>• PDU Session ID corresponding to the default EPS bearer ID of the EPS PDN connection.</li> <li>• Allocated EBI List, containing the EBI(s) allocated to the PDU session.</li> </ul> <p>The Location header present in the POST response contains the URI of the created SM context resource.</p> <p>AMF stores the association of the PDU Session ID and the SMF ID, and allocated EBI(s) associated to the PDU Session ID.</p> <p>If the EPS Bearer Context Status attribute is received in the request, the SMF checks whether some EPS bearer(s) of the corresponding PDU session have been deleted by the UE but not notified to the EPS. If so, SMF releases these EPS bearers, corresponding QoS rules and QoS flow level parameters locally.</p>
2b	<p>SMF returns 4xx/5xx failure response if:</p> <ul style="list-style-type: none"> <li>• SMF determines that seamless session continuity from EPS to 5GS is not supported for the PDU session. SMF sets the cause attribute in the Problem Details structure to NO_EPS_5GS_CONTINUITY.</li> <li>• The default EPS Bearer Context of the PDU session is reported as inactive by the UE in the EPS Bearer Context Status attribute. SMF sets the cause attribute in the Problem Details structure to DEFAULT_EPS_BEARER_INACTIVE.</li> </ul>

### User Plane Connection Reactivation Request

The following call flows captures information on UE idle mode mobility from EPS to 5GS with UP (User Plane) connection reactivation using N26 interface.

Figure 17: User Plane Connection Reactivation Request

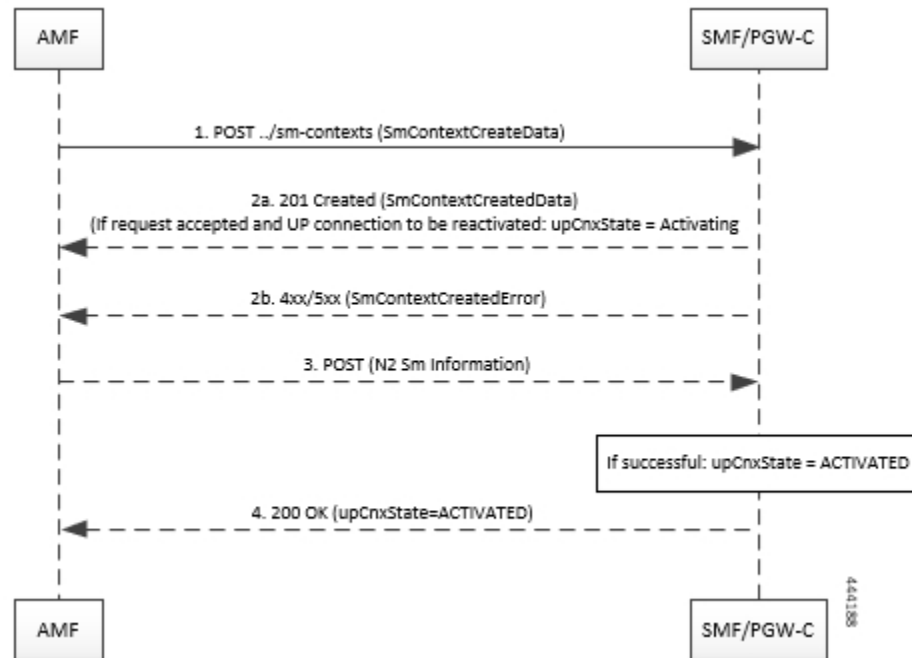


Table 27: User Plane Connection Reactivation Request

Step	Description
1	<p>AMF sends a POST request towards SMF/PGW-C of each UE EPS PDN connection with following information:</p> <ul style="list-style-type: none"> <li>• UE EPS PDN connection, including the EPS bearer contexts, received from the MME, representing the individual SM context to be created.</li> <li>• the PDU Sessions Activate List attribute, including the PDU Session ID of all the PDU session(s) to be re-activated.</li> <li>• EPS Bearer Context Status attribute, indicating the status of all the EPS bearer contexts in the UE, if corresponding information is received in the Registration Request from the UE.</li> </ul>
2	<p>Upon receipt of such a request, if:</p> <ul style="list-style-type: none"> <li>• a corresponding PDU session is found based on the EPS bearer contexts.</li> <li>• the default EPS bearer context of the corresponding PDU session is not reported as inactive by the UE in the EPS Bearer Context attribute, if received; and</li> <li>• it is possible to proceed with moving the PDN connection to 5GS.</li> </ul>

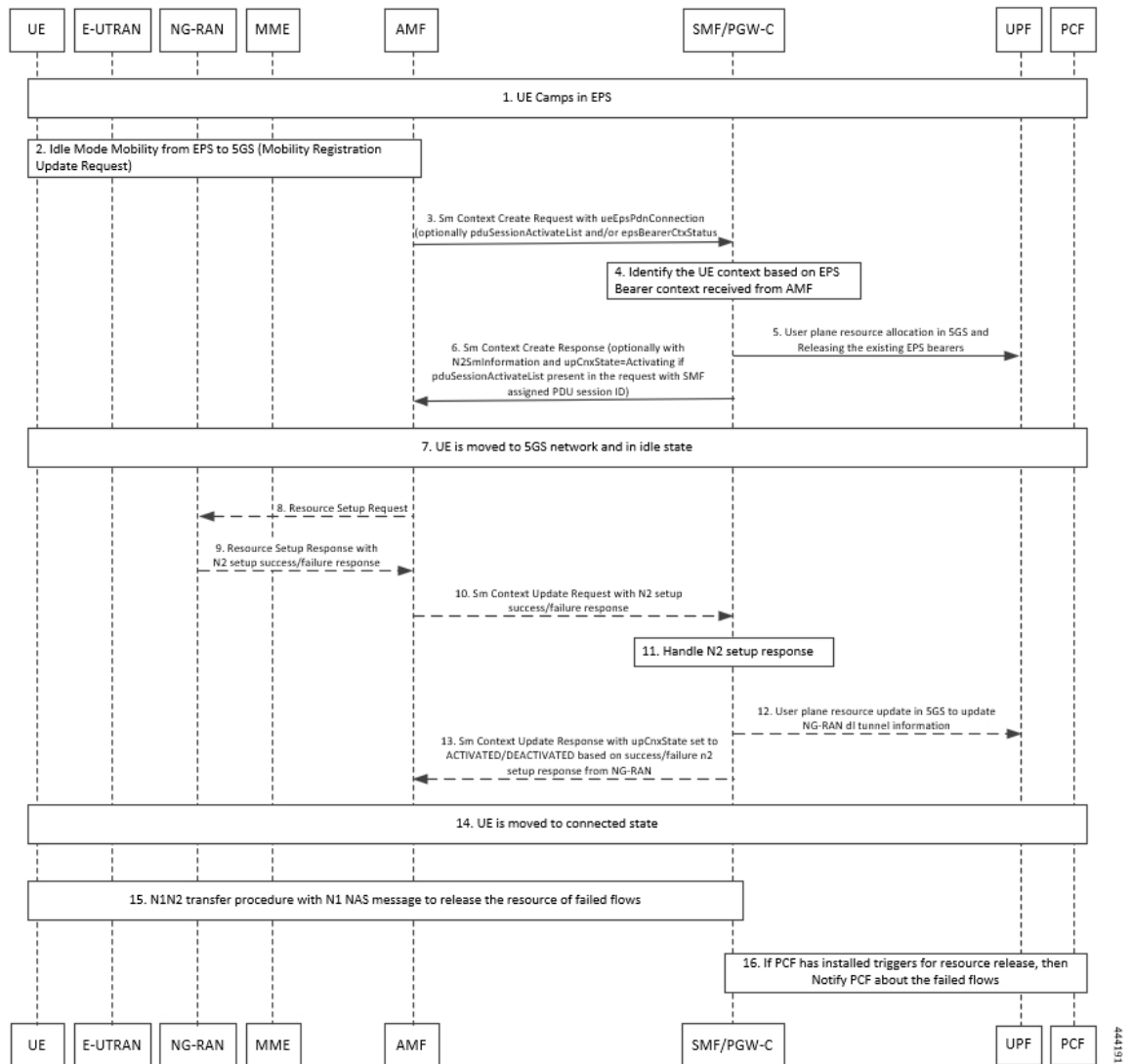
Step	Description
2a	<p>SMF returns a 201 Created response including the following information:</p> <ul style="list-style-type: none"> <li>• PDU Session ID corresponding to the default EPS bearer ID of the EPS PDN connection.</li> <li>• Allocated EBI List, containing the EBI(s) allocated to the PDU session.</li> </ul> <p>and, if the PDU session that is derived by the SMF based on the EPS bearer contexts was requested to be re-activated, i.e. if the PDU Session ID was present in the PDU Sessions Activate List,</p> <ul style="list-style-type: none"> <li>• the User Plane Connection State attribute is set to ACTIVATING.</li> <li>• N2 SM information to request the 5G-AN to assign resources to the PDU session (PDU Session Resource Setup Request Transfer), including the transport layer address and tunnel endpoint of the uplink termination point for the user plane data for this PDU session (i.e. UPF's GTP-U F-TEID for uplink traffic).</li> </ul> <p>The Location header present in the POST response contains the URI of the created SM context resource.</p> <p>AMF stores the association of the PDU Session ID and the SMF ID, and allocated EBI(s) associated to the PDU Session ID.</p> <p>If the EPS Bearer Context Status attribute is received in the request, the SMF checks whether some EPS bearer(s) of the corresponding PDU session have been deleted by the UE but not notified to the EPS. If so, SMF releases these EPS bearers, corresponding QoS rules and QoS flow level parameters locally.</p>
2b	<p>SMF returns 4xx/5xx failure response if:</p> <ul style="list-style-type: none"> <li>• SMF determines that seamless session continuity from EPS to 5GS is not supported for the PDU session. SMF sets the cause attribute in the Problem Details structure to NO_EPS_5GS_CONTINUITY.</li> <li>• The default EPS Bearer Context of the PDU session is reported as inactive by the UE in the EPS Bearer Context Status attribute. SMF sets the cause attribute in the Problem Details structure to DEFAULT_EPS_BEARER_INACTIVE.</li> </ul>

Step	Description
3	<p>If the SMF returns a 200 OK response, the AMF subsequently updates the SM context in the SMF by sending POST request with the following information:</p> <ul style="list-style-type: none"> <li>• N2 SM information received from the 5G-AN (PDU Session Resource Setup Response Transfer IE), including the transport layer address and tunnel endpoint of one or two downlink termination point(s). It also includes the associated list of QoS flows for this PDU session (i.e. 5G-AN's GTP-U F-TEID(s) for downlink traffic), if the 5G-AN succeeded in establishing resources for the PDU sessions; or</li> <li>• N2 SM information received from the 5G-AN (PDU Session Resource Setup Unsuccessful Transfer IE), including the Cause of the failure, if resources failed to be established for the PDU session.</li> </ul> <p>Upon receipt of this request, the SMF:</p> <ul style="list-style-type: none"> <li>• Updates the UPF with the 5G-AN's F-TEID(s) and sets the User Plane Connection State attribute to ACTIVATED, if the 5G-AN succeeds in establishing resources for the PDU sessions; or</li> <li>• Considers that the activation of the User Plane connection has failed and sets the User Plane Connection State attribute to DEACTIVATED.</li> </ul>
4	<p>SMF returns a 200 OK response including the User Plane Connection State attribute representing the final state of the user plane connection.</p>

## Message Flows

The following message flow describes the different scenarios of idle mode mobility procedure across 5GS network elements and subscriber.

Figure 18: Message Flow across 5GS NEs and Subscriber



## Standards Compliance

The SMF Support for 4G to 5G Data Session Handover feature complies with the following standard:

- 3GPP TS 23.502 V15.2.0 (2018-09)

## Limitations

The 4G to 5G Data Session Handover feature has the following limitations:

- SMF supports N26 4G to 5G handoff with single UPF, which implies that UPF selection and UPF modification are not supported.
- SMF does not support PCF trigger.



- SMF does not support charging and PCF integration.
- SMF does not support the roaming scenario.

# Emergency SoS Support

## Feature Description

The Emergency SoS Support feature enables the co-located cloud-native SMF and PGW-C to support SoS emergency over LTE for subscribers camped on the 4G network and SoS emergency service fallback to LTE for subscribers camped on the 5G network.

The Emergency SoS Support feature supports the following functionalities:

- Provides a new configuration to skip UDM interaction.
- Enables an emergency PDN connection creation in 4G (LTE) for PGW-C.
- Supports emergency service fallback to LTE requirement for SMF serving subscriber in NR.
- Supports interworking with an existing charging interface failure handling to 'continue' emergency call creation upon failure.
- Supports interworking with an existing secondary authentication using radius to skip radius authentication for emergency calls when not configured.
- Provides inter-RAT handover support (4G to 5G and 5G to 4G) for EPS interworking capable subscribers.

## How it Works

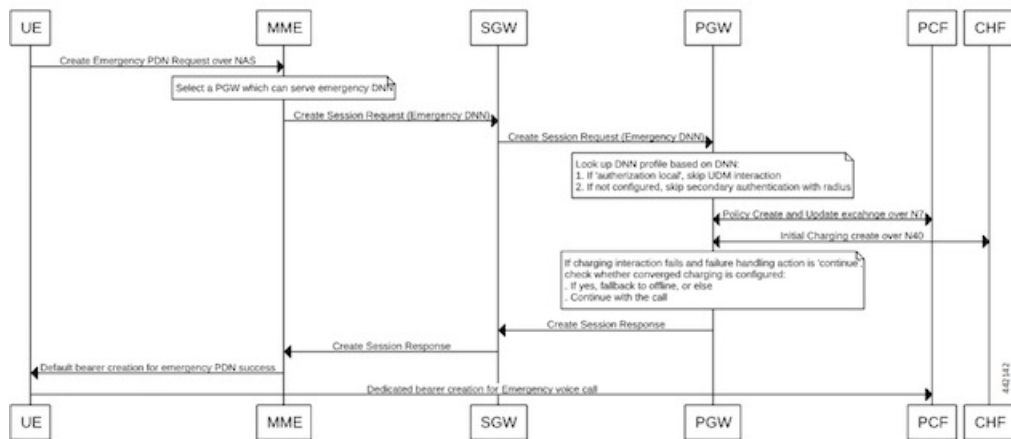
This section provides a brief of how the Emergency SoS Support feature works.

## Call Flows

This section includes the following call flows.

## Emergency Session Creation in LTE Call Flow

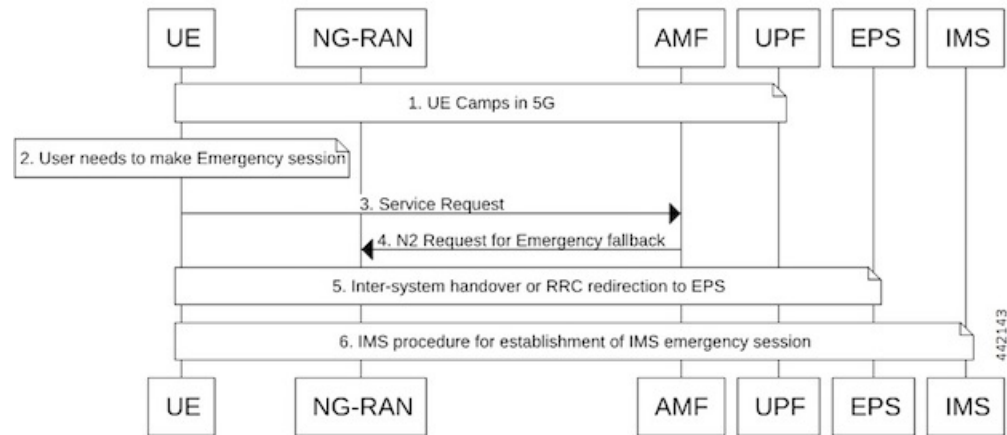
Figure 19: Emergency Session Creation in LTE



Step	Description
1	When an emergency service is required and an emergency PDU session is not already established, the UE initiates the UE-requested PDU session establishment procedure with a request type indicating, "Emergency Request" in LTE.
2	The MME selects an APN or DNN for the emergency PDN creation, and sends a 'Create Session Request' to the P-GW via the S-GW.
3	The DNN profile lookup at P-GW is based on the subscriber policy or DNN policy. These policies are associated in the SMF profile. The subscriber policy has higher precedence over DNN policy when both the configurations are present.
4	The DNN policy can have the DNN profile configuration for each of the UE-requested APN or DNN received in the "Create Session Request" from the MME or S-GW.
5	When a new configuration 'authorization local' under the selected DNN profile is present: <ul style="list-style-type: none"> <li>• P-GW skips the UDM interaction for fetch subscription and uses the values received in the 'Create Session Request' message from the MME.</li> <li>• P-GW skips the UDM interaction to 'Subscribe-for-Notification' from the UDM.</li> </ul>
6	When the 'Secondary Authentication Radius' under the selected DNN profile is not present, the PGW-C rejects the RADIUS-based secondary authentication.
7	When 'failure handling' for charging interaction is set as 'action continue': <ul style="list-style-type: none"> <li>• P-GW continues the call if converged charging is not configured.</li> <li>• P-GW falls back to offline charging and continues the call.</li> </ul>
8	During handover from 4G to 5G using N26, if the emergency PDN gets handed over, the SMF checks the DNN profile and if 'authorization local' is present, it skips the UDM interactions for registration and deregistration.

## Emergency Services Fallback to LTE Call Flow

Figure 20: Emergency Services Fallback to LTE



Step	Description
1	UE camps on E-UTRA or NR cell in the 5GS (in either CM_IDLE or CM_CONNECTED state).
2	UE has a pending IMS emergency session request (example, voice) from the upper layers.
3	If the AMF has indicated support for emergency services using fallback via the “Registration Accept” message for the current RAT, the UE sends a “Service Request” message indicating that it requires an emergency services fallback.
4	The 5GC executes an NG-AP procedure in which it indicates to the NG-RAN that this is a fallback for emergency services. This procedure triggers the “Emergency Services Fallback” request. Currently the Cisco SMF and PGW-C supports Emergency Services in the EPC core Network (LTE). The AMF includes the EPC as a target CN to trigger inter-RAT fallback. When the AMF initiates the redirection for UEs that are successfully authenticated, AMF includes the security context in the request to trigger fallback towards the NG-RAN.
5	The NG-RAN initiates the handover or redirection to the E-UTRAN connected to the EPS (N26 interface based handover or redirection procedure). The NG-RAN uses the security context that the AMF to secure the redirection procedure.  If the redirection procedure is used, the target CN is also conveyed to the UE to enable it to perform the S1 mode NAS procedures. The UE uses the emergency indication in the RRC message and E-UTRAN provides the emergency indication to the MME during the “Tracking Area Update”.
6	After handover to the target cell, the UE establishes a PDU session or PDN connection for IMS emergency services and performs the IMS procedures for establishment of an IMS emergency session (example, voice).

## Configuring Emergency SoS Support

This section describes how to configure the Emergency SoS Support feature.

Configuring the Emergency SoS Support involves the following steps:

1. Local authorization configuration under DNN profile
2. Secondary authentication configuration under DNN profile
3. Charging failure handling configuration under Charging profile

## Configuring Local Authorization

To configure the local authorization under the DNN profile, use the following commands:

```
configure
  profile dnn pool_name
    [ no ] authorization local
  end
```

### NOTES:

**no:** Disables the local authorization under the DNN profile.

## Configuring Secondary Authentication

To configure secondary authentication under the DNN profile, use the following commands:

```
configure
  profile dnn pool_name
    [ no ] secondary authentication radius
  end
```

### NOTES:

- **no:** Disables the secondary authentication under the DNN profile.
- **radius:** Specifies RADIUS for secondary authentication.

## Configuring Charging Failure Handling

To configure failure handling action for both converged charging and offline charging failure cases under the charging profile, use the following commands:

```
configure
  profile network-element chf charging_profile_name
    nf-client-profile offline_charging_profile_name
    failure-handling-profile failure_handling_profile_name
  exit
exit
```

### NOTES:

- **profile network-element chf** *charging\_profile\_name*: Specifies the charging function (CHF) as the network element profile. *charging\_profile\_name* must be an alphanumeric string representing the corresponding network element profile name.
- **nf-client-profile** *offline\_charging\_profile\_name*: Specifies the local NF client profile. *offline\_charging\_profile\_name* must be an alphanumeric string representing the corresponding NF client profile name.

- **failure-handling-profile** *failure\_handling\_profile\_name*: Specifies the NRF failure handling network profile for the configured NF type. *failure\_handling\_profile-name* must be an alphanumeric string representing the corresponding NRF failure handling network profile name.

### Sample Configuration

The following is a sample configuration of the failure handling action for converged charging:

```
profile nf-client-failure nf-type chf
profile failure-handling [failure_handling_profile_name]
service name type nchf-convergedcharging
message type ChfConvergedchargingCreate
status-code httpv2 0
action continue
exit
```





## CHAPTER 9

# AN Modification Call Flow Support

- [Feature Summary and Revision History, on page 97](#)
- [Feature Description, on page 98](#)
- [How it Works, on page 98](#)

## Feature Summary and Revision History

### Summary Data

*Table 28: Summary Data*

Applicable Product(s) or FunctionalArea	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 29: Revision History*

Revision Details	Release
First introduced.	2020.02.0

## Feature Description

This procedure releases the logical NG-AP signalling connection for the UE between the (R)AN and the AMF and the associated N3 User Plane connections, and (R)AN signalling connection between the UE and the (R)AN and the associated (R)AN resources.

## How it Works

When the NG-AP signalling connection is lost due to (R)AN or AMF failure, the AN release is performed locally by the AMF or the (R)AN as described in the following procedure without using or relying on any of the signalling shown between (R)AN and AMF. The AN release causes all UP connections of the UE to be deactivated.

The initiation of AN release may be due to:

- (R)AN-initiated with cause, for example, O&M Intervention, Unspecified Failure, (R)AN (for example, Radio) Link Failure, User Inactivity, Inter-System Redirection, request for establishment of QoS Flow for IMS voice, Release due to UE-generated signalling connection release, mobility restriction, Release Assistance Information (RAI) from the UE, and so on, or
- AMF-initiated with cause like Unspecified Failure, and so on

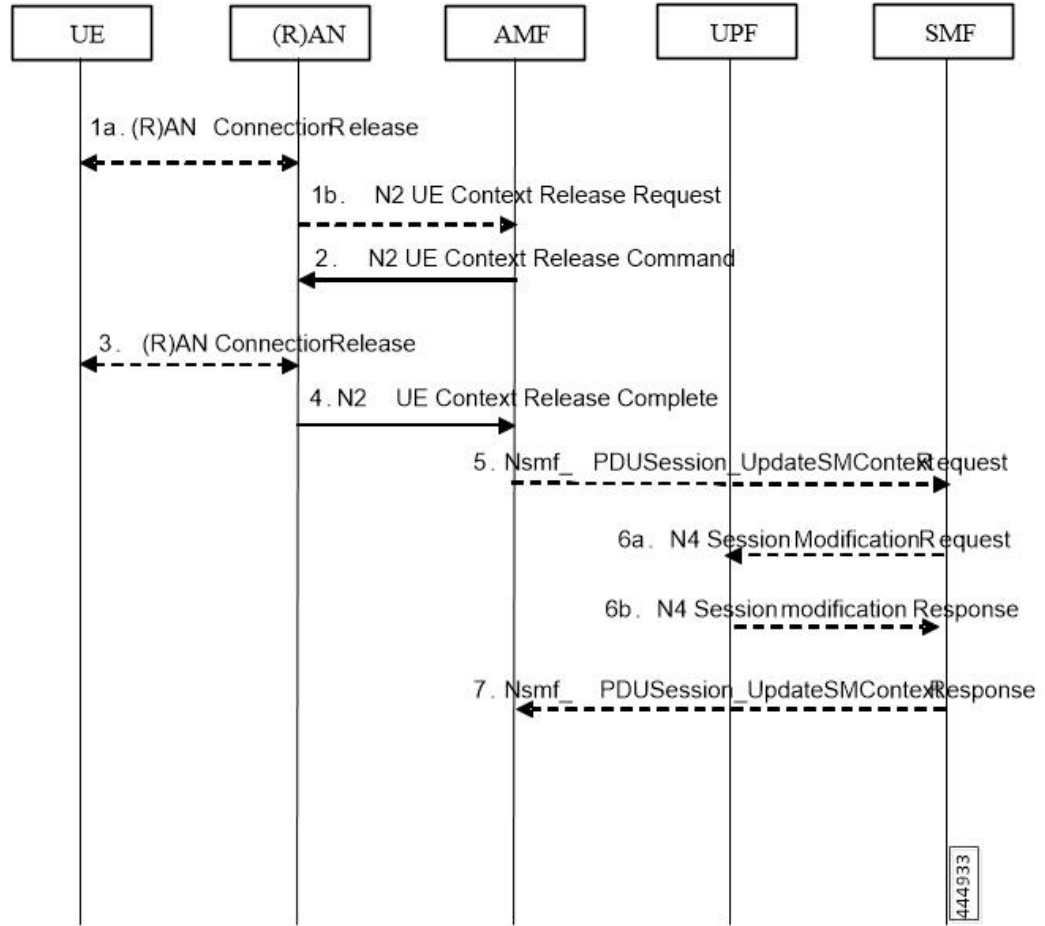
Both (R)AN-initiated and AMF-initiated AN Release procedures are shown in the following figure.

If Service Gap Control is applied for the UE and the Service Gap timer is not already running, the Service Gap timer is started in AMF and UE when entering CM-IDLE, unless the connection was initiated after a paging of an MT event, or after a Registration procedure without Uplink data status.

For this procedure, the impacted SMF and UPF are all under control of the PLMN serving the UE, for example, in Home Routed roaming case the SMF and UPF in HPLMN are not involved.



Figure 21: AN Release Procedure



Step	Description
1.	<p>If there is some confirmed (R)AN conditions like Radio Link Failure or for other (R)AN internal reason, the (R)AN may decide to initiate the UE context release in the (R)AN. In this case, the (R)AN sends an N2 UE Context Release Request (Cause, List of PDU Session ID(s) with active N3 user plane) message to the AMF. Cause indicates the reason for the release (for example, AN Link Failure, O&amp;M intervention, unspecified failure, and so on). The List of PDU Session ID(s) indicates that the PDU Sessions served by (R)AN of the UE. If the (R)AN is NG-RAN "UE Context Release Request (NG-RAN node initiated)".</p> <p>If the reason for the release is the NG-RAN received an AS Release Assistance Indicator, NG-RAN does not release the RRC connection but sends an N2 UE Context Release Request message to the AMF. If the AS RAI indicates that only a single downlink transmission is expected, then NG-RAN sends only the N2 UE Context Release Request after a single downlink NAS PDU or N3 data PDU has been transferred.</p> <p>If N2 Context Release Request cause indicates the release, then release is requested due to user inactivity or AS RAI. Then, the AMF continues with the AN Release procedure unless the AMF is aware of pending MT traffic or signalling.</p>
2.	<p>If the AMF receives the N2 UE Context Release Request message or due to an internal AMF event, including the reception of Service Request or Registration Request to establish another NAS signalling connection still via (R)AN, the AMF sends an N2 UE Context Release Command (Cause) to the (R)AN. The Cause indicates either the Cause from (R)AN in step 1 or the Cause due to an AMF event. In case the (R)AN is an NG-RAN this step, "UE Context Release (AMF initiated)". In case the (R)AN is an N3IWF/TNGF/W-AGF this step.</p> <p>If the AMF receives Service Request or Registration Request to establish another NAS signalling connection still via (R)AN, after successfully authenticating the UE, the AMF releases the old NAS signalling connection, and then continues the Service Request or Registration Request procedure.</p>
3.	<p>If the (R)AN connection (for example, RRC connection or NWu connection) with the UE is not already released (step 1), either:</p> <ol style="list-style-type: none"> <li data-bbox="441 1234 1484 1289">1. The (R)AN requests the UE to release the (R)AN connection. Upon receiving (R)AN connection release confirmation from the UE, the (R)AN deletes the UE's context, or</li> <li data-bbox="441 1318 1484 1373">2. If the Cause in the N2 UE Context Release Command indicates that the UE has already locally released the RRC connection, the (R)AN locally releases the RRC connection.</li> </ol>

Step	Description
4.	<p>The (R)AN confirms the N2 Release by returning an N2 UE Context Release Complete (List of PDU Session ID(s) with active N3 user plane, User Location Information, Age of Location Information) message to the AMF. The List of PDU Session ID(s) indicates that the PDU Sessions served by (R)AN of the UE. The AMF always stores the latest UE Radio Capability information or NB-IoT specific UE Radio Access Capability Information received from the NG-RAN node received. The N2 signalling connection between the AMF and the (R)AN for that UE is released. The (R)AN provides the list of recommended cells / TAs / NG-RAN node identifiers for paging to the AMF.</p> <p>If the PLMN has configured secondary RAT usage reporting, the NG-RAN node provides RAN usage data Report.</p> <p>This step is performed immediately after step 2, for example, in a situation where the UE does not acknowledge the RRC Connection Release.</p> <p>The NG-RAN includes Paging Assistance Data for CE capable UE, if available, in the N2 UE Context Release Complete message. The AMF stores the received Paging Assistance Data for CE capable UE in the UE context for subsequent Paging procedure.</p>
5.	<p>For each of the PDU Sessions in the N2 UE Context Release Complete, the AMF invokes Nsmf_PDUSession_UpdateSMContext Request (PDU Session ID, PDU Session Deactivation, Cause, Operation Type, User Location Information, Age of Location Information, N2 SM Information (Secondary RAT usage data)). The Cause in step 5 is the same Cause in step 2. If List of PDU Session ID(s) with active N3 user plane is included in step 1b, the step 5 through step 7 are performed before step 2. The Operation Type is set to "UP deactivate" to indicate deactivation of user plane resources for the PDU Session.</p> <p>For PDU Sessions using Control Plane CIoT 5GS Optimization and if the UE has negotiated the use of extended Idle mode DRX, the AMF informs the SMF immediately that the UE is not reachable for downlink data. For PDU Sessions using Control Plane CIoT 5GS Optimization and if the UE has negotiated the use of MICO mode with Active Time, the AMF informs the SMF that the UE is not reachable for downlink data once the Active Time has expired.</p>

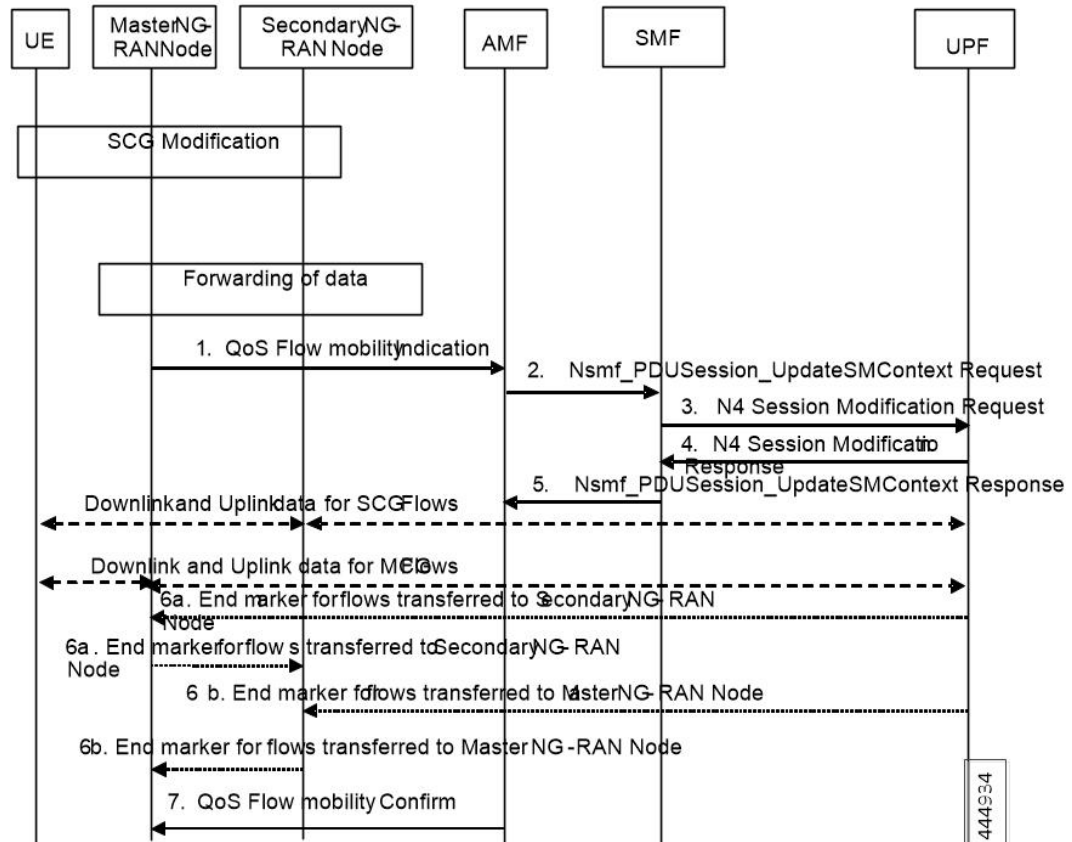
Step	Description
6.	<p>The SMF sends N4 Session Modification Request (AN or N3 UPF Tunnel Info to be removed, Buffering on/off) to the UPF.</p> <p>For PDU Sessions not using Control Plane CIoT 5GS Optimization, the SMF initiates an N4 Session Modification procedure indicating the need to remove Tunnel Info of AN or UPF terminating N3. Buffering on/off indicates whether the UPF has to buffer incoming DL PDU or not.</p> <p>If the SMF has received an indication from the AMF that the UE is not reachable for downlink data for PDU Sessions using Control Plane CIoT 5GS Optimization, the SMF initiates an N4 Session Modification procedure to activate buffering in the UPF.</p> <p>If multiple UPFs are used in the PDU Session and the SMF determines to release the UPF terminating N3, step 6a is performed towards the UPF (for example, PSA) terminating N9 towards the current N3 UPF. The SMF then releases the N4 session towards the N3 UPF (the N4 release is not shown in the call flow).</p> <p>If the cause of AN Release is because of User Inactivity, or UE Redirection, the SMF preserves the GBR QoS Flows. Otherwise, the SMF triggers the PDU Session Modification procedure for the GBR QoS Flows of the UE after the AN Release procedure is completed.</p> <p>If the redundant I-UPFs are used for URLLC, the N4 Session Modification Request procedure is done for each I-UPF. In this case, the SMF selects both the redundant I-UPFs to buffer the DL packets for this PDU Session or drop the DL packets for this PDU session or forward the DL packets for this PDU session to the SMF, based on buffering instruction provided by the SMF.</p> <p>If the redundant N3 tunnels are used for URLLC, the N4 Session Modification Request procedure to the UPF of N3 terminating point is to remove the dual AN Tunnel Info for N3 tunnel of the corresponding PDU Session.</p>
6b.	The UPF sends N4 Session Modification Response acknowledging the SMF request to the SMF.
7.	The SMF sends Nsmf_PDUSession_UpdateSMContext Response for step 5 to the AMF. Once the procedure is completed, the AMF considers the N2 and N3 as released and enters CM-IDLE state. After completion of the procedure, the AMF reports towards the NF consumers.

### Dual Connectivity Support

This procedure is used to transfer QoS Flows to and from Secondary RAN Node. During this procedure, the SMF, and UPF are never re-allocated. The presence of IP connectivity between the UPF and the Master RAN node, as well as between the UPF and the Secondary RAN node is assumed.

If QoS Flows for multiple PDU Sessions need to be transferred to or from Secondary RAN Node, the procedure shown in the below figure below is repeated for each PDU Session.

Figure 22: NG-RAN initiated QoS Flow mobility procedure



Step	Description
1.	The Master RAN node sends a N2 QoS Flow mobility Indication (PDU Session ID, QFI(s), AN Tunnel Info) message to the AMF. AN Tunnel Info includes the new RAN tunnel endpoint for the QFI(s) for which the AN Tunnel Info shall be modified.
2.	AMF to SMF, Nsmf_PDUSession_UpdateSMContext request (N2 QoS Flow mobility Indication message PDU Session ID).
3.	The SMF sends an N4 Session Modification Request (PDU Session ID(s), QFI(s), AN Tunnel Info for downlink user plane) message to the UPF.
4.	The UPF returns an N4 Session Modification Response (CN Tunnel Info for uplink traffic) message to the SMF after requested QFIs are switched. <b>Important</b> Step 7 can occur anytime after receipt of N4 Session Modification Response at the SMF.
5.	SMF to AMF, Nsmf_PDUSession_UpdateSMContext response (N2 SM information (CN Tunnel Info for uplink traffic)) for QFIs of the PDU Session which have been switched successfully. If none of the requested QFIs are switched successfully, the SMF sends an N2 QoS Flow mobility Failure message.

Step	Description
6.	In order to assist the reordering function in the Master RAN node and/or Secondary RAN node, for each affected N3 tunnel the UPF sends one or more "end marker" packets on the old tunnel immediately after switching the tunnel for the QFI. The UPF starts sending downlink packets to the Target NG-RAN.
7.	The AMF relays message 5 to the Master RAN node.



# CHAPTER 10

## Application-based Alerts

- [Feature Summary and Revision History, on page 105](#)
- [Feature Description, on page 106](#)
- [How it Works, on page 106](#)
- [Configuring Alert Rules, on page 106](#)

## Feature Summary and Revision History

### Summary Data

*Table 30: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 31: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

When the system detects an anomaly, it generates an alert notification. The system statistics are the cause for these alert notifications. You can set an expression to trigger an alert when the expression becomes true.

## Converged Core Refactoring Changes

This section describes the changes related to converged core refactoring in this chapter.

For the following interface-specific alerts, the **n4** and **smf** prefixes in the procedure type names and statistic names respectively are removed.

- N4 Message Success
- N4 UPF Association Down
- N4 UPF Association Up

## How it Works

The Common Execution Environment (CEE) uses the Prometheus Alert Manager for alerting operations. The CEE YANG model - either through CLI or API - allows users to view the active alerts, silenced alerts, and alert history. Also, the applications can call the alert API directly to add or clear alerts. The Prometheus Alert Manager API (v2) is the standard API used.

The Prometheus Alerts Manager includes the following options:

- **Defining Alert Rules:** This option defines the types of alerts that the Alert Manager should trigger. Use the Prometheus Query Language (PromQL) to define the alerts.
- **Defining Alert Routing:** This option defines the action the Alert Manager should take after receiving the alerts. At present, the SNMP Trapper is supported as the outbound alerting. Also, the CEE provides an Alert Logger for storing the generated alerts.

## Configuring Alert Rules

To configure the alert rules, use the following configuration:

```
configure
  alerts rules group alert_group_name
  interval-seconds seconds
  rule rule_name
    expression promql_expression
    duration duration
    severity severity_level
    type alert-type
    annotation annotation_name
    value annotation_value
```



```

    exit
  exit

```

**NOTES:**

- **alerts rules:** Specifies the Prometheus alerting rules.
- **group** *alert\_group\_name*: Specifies the Prometheus alerting rule group. One alert group can have multiple lists of rules. *alert-group-name* is the name of the alert group. The alert-group-name must be a string in the range of 0–64 characters.
- **interval-seconds** *seconds*: Specifies the evaluation interval of the rule group in seconds.
- **rule** *rule\_name*: Specifies the alerting rule definition. *rule\_name* is the name of the rule.
- **expression** *promql\_expression*: Specifies the PromQL alerting rule expression. *promql\_expression* is the alert rule query expressed in PromQL syntax.
- **duration** *duration*: Specifies the duration of a true condition before it is considered true. *duration* is the time interval before the alert is triggered.
- **severity** *severity\_level*: Specifies the severity of the alert. *severity-level* is the severity level of the alert. The severity levels are critical, major, minor, and warning.
- **type** *alert\_type*: Specifies the type of the alert. *alert\_type* is the user-defined alert type. For example, Communications Alarm, Environmental Alarm, Equipment Alarm, Indeterminate Integrity Violation Alarm, Operational Violation Alarm, Physical Violation Alarm, Processing Error Alarm, Quality of Service Alarm, Security Service Alarm, Mechanism Violation Alarm, or Time Domain Violation Alarm.
- **annotation** *annotation\_name*: Specifies the annotation to attach to the alerts. *annotation\_name* is the name of the annotation.
- **value** *annotation\_value*: Specifies the annotation value. *annotation\_value* is the value of the annotation.

The following example configures an alert, which is triggered when the percentage of Unified Data Management (UDM) responses is less than the specified threshold limit.

**Example:**

```

configure terminal
  alerts rules group SMFUDMchk_incr
    interval-seconds 300
    rule SMFUDMchk_incr
      expression "sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\", response_status=~\"2..\"}[3m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"udm\", message_direction=\"outbound\"}[3m]))
< 0.95"
      severity major
      type "Communications Alarm"
      annotation summary
      value "This alert is fired when the percentage of UDM responses is less than threshold"
    exit
  exit
exit

```

You can view the configured alert using the **show running-config alerts** command.

**Example:**

The following example displays the alerts configured in the running configuration:

```

show running-config alerts
  interval-seconds 300
  rule SMFUDMchk_incr
    expression "sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\", response_status=~\"2..\"}[3m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"udm\", message_direction=\"outbound\"}[3m]))
< 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of UDM responses is less than threshold"

  exit
exit
exit

```

## Viewing Alert Logger

The Alert Logger stores all the generated alerts by default. You can view the stored alerts using the following **show** command.

### **show alert history [ filtering ]**

You can narrow down the result using the following filtering options:

- **annotations**: Specifies the annotations of the alert.
- **endsAt**: Specifies the end time of the alert.
- **labels**: Specifies the additional labels of the alert.
- **severity**: Specifies the severity of the alert.
- **source**: Specifies the source of the alert.
- **startsAt**: Specifies the start time of the alert.
- **type**: Specifies the type of the alert.

The following example displays the history of the alerts configured in the system:

### **Example:**

```

show alerts history
alerts active SMFUDMchk_incr ac2a970ab621
state active
severity major
type "Communications Alarm"
startsAt 2019-11-15T08:26:48.283Z
source System
annotations [ "summary:This alert is fired when the percentage of UDM responses is less
than threshold." ]

```

You can view the active and silenced alerts with the **show alerts active** and **show alerts active** commands.

The following example displays the active alerts. The alerts remain active as long as the evaluated expression is true.

### **Example:**

```

show alerts active
alerts active SMFUDMchk_incr ac2a970ab621
state active

```

```
severity major
type "Communications Alarm"
startsAt 2019-11-15T08:26:48.283Z
source System
annotations [ "summary:This alert is fired when the percentage of UDM responses is less
than threshold." ]
```

## Call Flow Procedure Alerts

This section provides detail of commands that are required to configure alerts related to various call flow procedures.

### 4G PDN Modify

Use the following commands to configure alerts related to the 4G PDN Modify procedure.

```
alerts rules group SMFPDN
  interval-seconds 300
  rule SMFPDNModify
    expression "sum(smf_service_stats{procedure_type=~\"pdn_ho_location_changed|
pdn_ho_rat_type_changed|pdn_inter_sgw_handover|pdn_mbr\" ,
status=\"success\"})/sum(smf_service_stats{procedure_type=~
\"pdn_ho_location_changed|pdn_ho_rat_type_changed |pdn_inter_sgw_handover|pdn_mbr\" ,
status=\"attempted\"}) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage successful 4G PDN Modify is below
threshold"
    exit
  exit
```

### 4G PDN Release Success

Use the following commands to configure alerts related to the 4G PDN Release Success procedure.

```
alerts rules group SMFPDN
  interval-seconds 300
  rule SMFPDNRelease
    expression "sum(smf_service_stats{procedure_type=~\".*pdn_sess_rel\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=~\".*pdn_sess_rel\" ,
status=\"attempted\"}) < 0.95 "
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage successful 4G PDN Release is below
threshold."
    exit
  exit
```

### 4G PDN Setup Success

Use the following commands to configure alerts related to the 4G PDN Setup Success procedure.

```

alerts rules group SMFPDN
  interval-seconds 300
  rule SMFPDNSetup
    expression "sum(smf_service_stats{procedure_type=\"pdn_sess_create\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=\"pdn_sess_create\" ,
status=\"attempted\"}) < 0.95 "
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage successful 4G PDN Setup is below
threshold."
    exit
  exit

```

## 4G to 5G HO Success

Use the following commands to configure alerts related to the 4G to 5G HO Success procedure.

```

alerts rules group Handover
  interval-seconds 300
  rule 4gTo5gHOSuccess
    expression
"sum(smf_service_stats{procedure_type=~\"n26_4g_to_5g_handover|n26_4g_to_5g_im_mobility\"
, status=\"success\"}) /
sum(smf_service_stats{procedure_type=~\"n26_4g_to_5g_handover|n26_4g_to_5g_im_mobility\" ,
status=\"attempted\"}) < 0.95 "
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage successful 4G to 5G HO is below
threshold."
    exit
  exit

```

## 4G To WiFi HO Success

Use the following commands to configure alerts related to the 4G to WiFi HO Success procedure.

```

alerts rules group Handover
  interval-seconds 300
  rule 4GtoWifiHOSuccess
    expression "sum(smf_service_stats{procedure_type=\"enb_to_untrusted_wifi_handover\"
, status=\"success\"}) /
sum(smf_service_stats{procedure_type=\"enb_to_untrusted_wifi_handover\" ,
status=\"attempted\"}) < 0.95 "
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of N4 responses sent is lesser than 95
%."
    exit
  exit

```

## 5G N2 HO Success

Use the following commands to configure alerts related to the 5G N2 HO Success procedure.

```

alerts rules group Handover
  interval-seconds 300
  rule N2HOSuccess
  expression "sum(smf_service_stats{procedure_type=\"n2_handover\" , status=\"success\"})
  / sum(smf_service_stats{procedure_type=\"n2_handover\" , status=\"attempted\"}) < 0.95 "
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage successful 5G N2 HO is below threshold."

  exit
exit

```

## 5G PDU Idle Success

Use the following commands to configure alerts related to the 5G PDU Idle Success procedure.

```

alerts rules group SMFPDU
  interval-seconds 300
  rule SMFPDUIdleSuccess
  expression "sum(smf_service_stats{procedure_type=~\".*idle\" , status=\"success\"})
  / sum(smf_service_stats{procedure_type=~\".*idle\" , status=\"attempted\"}) < 0.95 "
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage successful 5G PDU Idle is below threshold"

  exit
exit

```

## 5G PDU Modify Success

Use the following commands to configure alerts related to the 5G PDU Modify Success procedure.

```

alerts rules group SMFPDU
  interval-seconds 300
  rule SMFSessionModifySuccess
  expression "sum(smf_service_stats{procedure_type=~\".*pdu_sess_mod\" ,
  status=\"success\"}) / sum(smf_service_stats{procedure_type=~\".*pdu_sess_mod\" ,
  status=\"attempted\"}) < 0.95 "
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage successful 5G PDU Modify is below
  threshold"
  exit
exit

```

## 5G PDU Release Success

Use the following commands to configure alerts related to the 5G PDU Release Success procedure.

```

alerts rules group SMFPDU
  interval-seconds 300
  rule SMFSessionReleaseFailure
  expression "sum(smf_service_stats{procedure_type=~\".*pdu_sess_rel\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=~\".*pdu_sess_rel\" ,
status=\"attempted\"}) < 0.95 "
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage successful 5G PDU Setup is below
threshold"
  exit
exit

```

## 5G PDU Setup Success

Use the following commands to configure alerts related to the 5G PDU Setup Success procedure.

```

alerts rules group SMFPDU
  interval-seconds 300
  rule SMFSessionSetupFailure
  expression "sum(smf_service_stats{procedure_type=\"pdu_sess_create\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=\"pdu_sess_create\" ,
status=\"attempted\"}) < 0.95 "
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when failed to setup sessions is more than 5%"
  exit
exit

```

## 5G to 4G HO Success

Use the following commands to configure alerts related to the 5G to 4G HO Success procedure.

```

alerts rules group Handover
  interval-seconds 300
  rule 5gTo4gHOSuccess
  expression "sum(smf_service_stats{procedure_type=~\"pdn_5g_4g_handover
|pdn_5g_4g_handover_dft|eps_fb_5g_4g_handover_dft|eps_fb_5g_4g_handover_idft
|pdn_5g_4g_handover_idft\" , status=\"success\"}) /
sum(smf_service_stats{procedure_type=~\"pdn_5g_4g_handover
|pdn_5g_4g_handover_dft|eps_fb_5g_4g_handover_dft|
eps_fb_5g_4g_handover_idft|pdn_5g_4g_handover_idft\" , status=\"attempted\"}) < 0.95 "
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage successful 5G to 4G HO is below
threshold."
  exit
exit

```

## 5G To WiFi HO Success

Use the following commands to configure alerts related to the 5G to WiFi HO Success procedure.

```

alerts rules group Handover
  interval-seconds 300
  rule 5GtoWifiHOSuccess
    expression "sum(smf_service_stats{procedure_type=\"nr_to_untrusted_wifi_handover\" ,
status=\"success\"}) / sum(smf_service_stats{procedure_type=\"nr_to_untrusted_wifi_handover\"
, status=\"attempted\"}) < 0.95 "
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of N4 responses sent is lesser than 95
%."
    exit
exit

```

## 5G Xn HO Success

Use the following commands to configure alerts related to the 5G Xn HO Success procedure.

```

alerts rules group Handover
  interval-seconds 300
  rule XnHOSuccess
    expression "sum(smf_service_stats{procedure_type=\"xn_handover\" , status=\"success\"})
/ sum(smf_service_stats{procedure_type=\"xn_handover\" , status=\"attempted\"}) < 0.95 "
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage successful 5G Xn HO is below threshold."

    exit
exit

```

## PDN Session Create

Use the following commands to configure alerts related to the PDN Session Create procedure.

```

alerts rules group SMFProcStatus
  interval-seconds 300
  rule PDNSessCreate
    expression "sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=
/\ "pdn_sess_create\",status=\"success\"}[5m])) /
sum(increase(smf_service_stats{app_name=\"SMF\
/\",procedure_type=\"pdn_sess_create\",status=\" /attempted\"}[5m])) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the success percentage of pdn_sess_create procedure is
lesser threshold."
    exit
exit

```

## PDU Session Create

Use the following commands to configure alerts related to the PDU Session Create procedure.

```

alerts rules group SMFProcStatus
  interval-seconds 300
  rule PDUssCreate
    expression "sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=
/\pdu_sess_create\",status=\"success\"}[5m]))sum
/(increase(smf_service_stats{app_name=\"SMF\", /procedure_type=\"pdu_sess_create\",status=
/attempted\"}[5m])) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the success percentage of pdu_sess_create procedure is
lesser threshold."
    exit
exit

```

## PDU Session Modify

Use the following commands to configure alerts related to the PDU Session Modify procedure.

```

alerts rules group SMFProcStatus
  interval-seconds 300
  rule PDUssModify
    expression "sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=~\".
/*req_pdu_sess_mod\",status=\"success\"}[5m]))sum(increase
/(smf_service_stats{app_name=\"SMF\",procedure_type=~
/\\".*req_pdu_sess_mod\",status=\"attempted\"}[5m])) / < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the success percentage of req_pdu_sess_mod procedure
is lesser threshold."
    exit
exit

```

## PDU Session Release

Use the following commands to configure alerts related to the PDU Session Release procedure.

```

alerts rules group SMFProcStatus
  interval-seconds 300
  rule PDUssRelease
    expression
"sum(increase(smf_service_stats{app_name=\"SMF\",procedure_type=~\".*req_pdu_sess_rel\",status=
/\"success\"}[5m]))sum(increase(smf_service_stats{app_name=\"SMF
/\",procedure_type=~\".*req_pdu_sess_rel\",status= /\"attempted\"}[5m])) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the success percentage of req_pdu_sess_rel procedure
is lesser threshold."
    exit
exit

```



## Interface Specific Alerts

This section provides detail of commands that are required to configure alerts related to various interfaces.

### GTPC Peer Down

Use the following commands to configure alerts related to the GTPC Peer Down procedure.

```

alerts rules group GTPCPeerDown
  interval-seconds 300
  rule GTPCPeerDown
  expression nodemgr_gtpc_peer_status{gtpc_peer_status="gtpc_peer_path_down"}
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the GTPC Path failure detected for peer crosses
  threshold"
  exit
exit

```

### N4 Message Success

Use the following commands to configure alerts related to the N4 Message Success procedure.

```

alerts rules group SMFSvcStatus
  interval-seconds 300
  rule SMFN4MessageSuccess
  expression "sum(protocol_udp_res_msg_total{message_direction="inbound",
  status="accepted"}) / sum(protocol_udp_res_msg_total{message_direction="inbound",
  status=~"accepted|denied"}) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of N4 responses sent is lesser than 95
  %."
  exit
exit

```

### N4 UPF Association Down

Use the following commands to configure alerts related to the N4 UPF Association Down query by N4 address.

```

alerts rules group N4Association
  interval-seconds 300
  rule SMFAssociationRelease
  expression "proto_udp_res_msg_total{procedure_type="n4_association_release_res",
  message_direction="inbound", status="accepted"} "
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the N4 Association with UPF is released"
  exit
exit

```

## N4 UPF Association Up

Use the following commands to configure alerts related to the N4 UPF Association Up query by N4 address.

```

alerts rules group N4Association
  interval-seconds 300
  rule N4AssociationUP
    expression "proto_udp_res_msg_total{procedure_type=\"n4_association_setup_res\",
message_direction= \"inbound\", status=\"accepted\"}"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the N4 Association with UPF is established"
  exit
exit

```

## N7 Interface Outbound

Use the following commands to configure alerts related to an outbound N7 interface.

```

alerts rules group SMFsvcStatus
  interval-seconds 300
  rule SMFN7Outbound
    expression "sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\", message_direction=\"outbound\"}[5m]))
< 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of N7 responses received is lesser
threshold."
  exit
exit

```

## N7 Interface Inbound

Use the following commands to configure alerts related to an inbound N7 interface.

```

alerts rules group SMFsvcStatus
  interval-seconds 300
  rule SMFN7Inbound
    expression "sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"inbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"pcf\", message_direction=\"inbound\"}[5m]))
< 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of N7 responses sent is lesser threshold."

  exit
exit

```

## N7 Message Timed Out

Use the following commands to configure alerts related to the N7 Message Timed Out procedure.

```

alerts rules group MessageTimeout
  interval-seconds 300
  rule SMFN7Timeout
    expression "sum(irate(smf_restep_http_msg_total{nf_type=\"pcf\",
message_direction=\"inbound\", response_status=\"504\"}[5m])) > 5"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the increase in timeout for N7 messages toward PCF
crosses threshold"
    exit
  exit

```

## N10 Interface

Use the following commands to configure alerts related to the N10 interface.

```

alerts rules group SMFSvcStatus
  interval-seconds 300
  rule SMFN10
    expression "sum(increase(smf_restep_http_msg_total{nf_type=\"udm\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"udm\", message_direction=\"outbound\"}[5m]))
< 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of N10 responses received is lesser
threshold."
    exit
  exit

```

## N11 Interface Inbound

Use the following commands to configure alerts related to an inbound N11 interface.

```

alerts rules group SMFSvcStatus
  interval-seconds 300
  rule SMFN11Inbound
    expression "sum(increase(smf_restep_http_msg_total{nf_type=\"amf\",
message_direction=\"inbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"amf\", message_direction=\"inbound\"}[5m]))
< 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of N11 responses sent is lesser
threshold."
    exit
  exit

```

## N11 Interface Outbound

Use the following commands to configure alerts related to an outbound N11 interface.

```

alerts rules group SMFsvcStatus
  interval-seconds 60
  rule SMFN11Outbound
    expression "sum(increase(smfc_restep_http_msg_total{nf_type=\"amf\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smfc_restep_http_msg_total{nf_type=\"amf\", message_direction=\"outbound\"}[5m]))
< 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of N11 responses received is lesser
threshold."
    exit
  exit

```

## N11 Message Timed Out

Use the following commands to configure alerts related to the N11 Message Timed Out procedure.

```

alerts rules group MessageTimeout
  interval-seconds 300
  rule SMFN40Timeout
    expression "sum(irate(smfc_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"inbound\", response_status=\"504\"}[5m])) > 5"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the increase in timeout for N11 messages toward AMF
crosses threshold"
    exit
  exit

```

## N40 Interface Inbound

Use the following commands to configure alerts related to an inbound N40 interface.

```

alerts rules group SMFsvcStatus
  interval-seconds 300
  rule SMFN40Inbound
    expression "sum(increase(smfc_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"inbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smfc_restep_http_msg_total{nf_type=\"chf\", message_direction=\"inbound\"}[5m]))
< 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of N40 responses sent is lesser
threshold."
    exit
  exit

```

## N40 Interface Outbound

Use the following commands to configure alerts related to an outbound N40 interface.

```

alerts rules group SMFSvcStatus
  interval-seconds 300
  rule SMFN40Outbound
    expression "sum(increase(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"outbound\", response_status=~\"2..\"}[5m])) /
sum(increase(smf_restep_http_msg_total{nf_type=\"chf\", message_direction=\"outbound\"}[5m]))
< 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of N40 responses received is lesser
threshold."
    exit
  exit

```

## N40 Message Timed Out

Use the following commands to configure alerts related to the N40 Message Timed Out procedure.

```

alerts rules group MessageTimeout
  interval-seconds 300
  rule SMFN11Timeout
    expression "sum(irate(smf_restep_http_msg_total{nf_type=\"chf\",
message_direction=\"inbound\", response_status=\"504\"}[5m])) > 5"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired the increase in timeout for N40 messages toward CHF crosses
threshold"
    exit
  exit

```

## NRF Discovery

Use the following commands to configure alerts related to the NRF Discovery procedure.

```

alerts rules group NRF
  interval-seconds 300
  rule NRFDISCOVERY
    expression
"sum(nf_discover_messages_total{result=~\"success|failure\",svc_name=\"nnrf-disc\",
service_name=\"smf-rest-ep\"}) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of N4 responses sent is lesser than 95
%."
    exit
  exit

```

## SMF Service Start

Use the following commands to configure alerts related to the SMF Service Start procedure.

```

alerts rules group SMFService
  interval-seconds 300
  rule SMFServiceStart
  expression "irate(outgoing_response_msg_total{msg_type=\"NrfNfmRegistration\"}[5m])"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when SMF-Service starts upon registration with NRF"
  exit
exit

```

## IP Pool

This section provides detail of commands that are required to configure alerts related to IP Pool.

### IP Pool Used

Use the following commands to configure alerts related to the IP Pool used procedure.

```

alerts rules group IPPool
  interval-seconds 300
  rule IPPool
  expression "sum(IPAM_address_allocations_current) > THRESHOLD"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage IP pool addresses used is above the
threshold"
  exit
exit

```

## Message Level Alerts

This section provides detail of commands that are required to configure alerts related to various messages.

### N11 SM Create

Use the following commands to configure alerts related to N11 SM Create.

```

alerts rules group SMFSvcStatus
  interval-seconds 300
  rule SMFN11Success
  expression "sum(increase(smfc_restep_http_msg_total{api_name=\"amf_create_sm_context\",
message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smfc_restep_http_msg_total{api_name=\"amf_create_sm_context\",
message_direction=\"inbound\"}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary

```

```

    value "This alert is fired when the percentage of amf_create_sm_context responses sent
    is lesser threshold."
    exit
exit

```

## N11 SM Update

Use the following commands to configure alerts related to N11 SM Update.

```

alerts rules group SMFSvcStatus
    interval-seconds 300
    rule SMFN11Update
        expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_update_sm_context\",
        message_direction=\"inbound\", response_status=\"200\"}[5m])) /
        sum(increase(smf_restep_http_msg_total{api_name=\"amf_update_sm_context\",
        message_direction=\"inbound\"}[5m])) < 0.95"
        severity major
        type "Communications Alarm"
        annotation summary
        value "This alert is fired when the percentage of amf_update_sm_context responses sent
        is lesser threshold."
        exit
exit

```

## N11 SM Release

Use the following commands to configure alerts related to N11 SM Release.

```

alerts rules group SMFSvcStatus
    interval-seconds 300
    rule SMFN11Release
        expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_release_sm_context\",
        message_direction=\"inbound\", response_status=\"204\"}[5m])) /
        sum(increase(smf_restep_http_msg_total{api_name=\"amf_release_sm_context\",
        message_direction=\"inbound\"}[5m])) < 0.95"
        severity major
        type "Communications Alarm"
        annotation summary
        value "This alert is fired when the percentage of amf_release_sm_context responses sent
        is lesser threshold."
        exit
exit

```

## N1 N2 Message Transfer

Use the following commands to configure alerts related to N1 N2 Message Transfer.

```

alerts rules group SMFSvcStatus
    interval-seconds 300
    rule SMFN1N2Transfer
        expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_n1_n2_transfer\",
        message_direction=\"outbound\", response_status=\"200\"}[5m])) /
        sum(increase(smf_restep_http_msg_total{api_name=\"amf_n1_n2_transfer\",
        message_direction=\"outbound\"}[5m])) < 0.95"
        severity major
        type "Communications Alarm"

```

```

    annotation summary
    value "This alert is fired when the percentage of amf_n1_n2_transfer responses received
    is lesser threshold."
    exit
exit

```

## N11 EBI Assignment

Use the following commands to configure alerts related to N11 EBI Assignment.

```

alerts rules group SMFSvcStatus
    interval-seconds 300
    rule SMFN11EBI
        expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_assign_ebi\",
        message_direction=\"outbound\", response_status=\"200\"}[5m])) /
        sum(increase(smf_restep_http_msg_total{api_name=\"amf_assign_ebi\",
        message_direction=\"outbound\"}[5m])) < 0.95"
        severity major
        type "Communications Alarm"
        annotation summary
        value "This alert is fired when the percentage of amf_assign_ebi responses received is
        lesser threshold."
        exit
exit

```

## N11 SM Status Notify

Use the following commands to configure alerts related to N11 SM Status Notify.

```

alerts rules group SMFSvcStatus
    interval-seconds 300
    rule SMFN11StatusNotify
        expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_status_notify\",
        message_direction=\"outbound\", response_status=\"201\"}[5m])) /
        sum(increase(smf_restep_http_msg_total{api_name=\"amf_status_notify\",
        message_direction=\"outbound\"}[5m])) < 0.95"
        severity major
        type "Communications Alarm"
        annotation summary
        value "This alert is fired when the percentage of amf_status_notify responses received
        is lesser threshold."
        exit
exit

```

## N11 SM Context Retrieve

Use the following commands to configure alerts related to N11 SM Context Retrieve.

```

alerts rules group SMFSvcStatus
    interval-seconds 300
    rule SMFN11ContextRetrieve
        expression "sum(increase(smf_restep_http_msg_total{api_name=\"amf_retrieve_sm_context\",
        message_direction=\"inbound\", response_status=\"201\"}[5m])) /
        sum(increase(smf_restep_http_msg_total{api_name=\"amf_retrieve_sm_context\",
        message_direction=\"inbound\"}[5m])) < 0.95"
        severity major

```



```

    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of amf_retrieve_sm_context responses
sent is lesser threshold."
    exit
exit

```

## N7 SM Policy Create

Use the following commands to configure alerts related to N7 SM Policy Create.

```

alerts rules group SMFSvcStatus
    interval-seconds 300
    rule SMFN7PolicyCreate
    expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_create\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_create\",
message_direction=\"outbound\"}[5m])) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of pcf_sm_policy_control_create responses
received is lesser threshold."
    exit
exit

```

## N7 SM Policy Update

Use the following commands to configure alerts related to N7 SM Policy Update.

```

alerts rules group SMFSvcStatus
    interval-seconds 300
    rule SMFN7PolicyUpdate
    expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update\",
message_direction=\"outbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_update\",
message_direction=\"outbound\"}[5m])) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of pcf_sm_policy_control_update responses
received is lesser threshold."
    exit
exit

```

## N7 SM Policy Delete

Use the following commands to configure alerts related to N7 SM Policy Delete.

```

alerts rules group SMFSvcStatus
    interval-seconds 300
    rule SMFN7PolicyDelete
    expression
"sum(increase(smf_restep_http_msg_total{api_name=\"pcf_sm_policy_control_delete\",

```

```

message_direction="outbound", response_status="204"[5m])) /
sum(increase(smf_restep_http_msg_total{api_name="pcf_sm_policy_control_delete",
message_direction="outbound"}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of pcf_sm_policy_control_delete responses
received is lesser threshold."
  exit
exit

```

## N7 SM Policy Notify Update

Use the following commands to configure alerts related to N7 SM Policy Notify Update.

```

alerts rules group SMFsvcStatus
  interval-seconds 300
  rule SMFN7PolicyUpdateNotify
  expression
    "sum(increase(smf_restep_http_msg_total{api_name="pcf_sm_policy_control_update_notify",
message_direction="inbound", response_status="201"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name="pcf_sm_policy_control_update_notify",
message_direction="inbound"}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of pcf_sm_policy_control_update_notify
responses sent is lesser threshold."
  exit
exit

```

## N7 SM Policy Notify Terminate

Use the following commands to configure alerts related to N7 SM Policy Terminate.

```

alerts rules group SMFsvcStatus
  interval-seconds 300
  rule SMFN7PolicyTerminateNotify
  expression
    "sum(increase(smf_restep_http_msg_total{api_name="pcf_sm_policy_control_terminate_notify",
message_direction="inbound", response_status="201"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name="pcf_sm_policy_control_terminate_notify",
message_direction="inbound"}[5m])) < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of pcf_sm_policy_control_terminate_notify
responses sent is lesser threshold."
  exit
exit

```

## N10 UE Register

Use the following commands to configure alerts related to N10 UE Register.

```

alerts rules group SMFSvcStatus
  interval-seconds 300
  rule SMFN10UERegister
    expression "sum(increase(smf_restep_http_msg_total{api_name=\"register_ue\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"register_ue\",
message_direction=\"outbound\"}[5m])) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of register_ue responses received is
lesser threshold."
    exit
  exit

```

## N10 UE DeRegister

Use the following commands to configure alerts related to N10 UE DeRegister.

```

alerts rules group SMFSvcStatus
  interval-seconds 300
  rule SMFN10UEDeRegister
    expression "sum(increase(smf_restep_http_msg_total{api_name=\"deregister_ue\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"deregister_ue\",
message_direction=\"outbound\"}[5m])) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of deregister_ue responses received is
lesser threshold."
    exit
  exit

```

## N10 SM Subscription Fetch

Use the following commands to configure alerts related to N10 Subscription Fetch.

```

alerts rules group SMFSvcStatus
  interval-seconds 300
  rule SMFN10SubscriptionFetch
    expression "sum(increase(smf_restep_http_msg_total{api_name=\"subscription_req\",
message_direction=\"outbound\", response_status=\"200\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"subscription_req\",
message_direction=\"outbound\"}[5m])) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of subscription_req responses received
is lesser threshold."
    exit
  exit

```

## N10 SM Subscribe for Notification

Use the following commands to configure alerts related to N10 Subscribe for Notification.

```

alerts rules group SMFsvcStatus
  interval-seconds 300
  rule SMFN10SubscriptionNotification
    expression "sum(increase(smf_restep_http_msg_total{api_name=\"sdm_subscription_req\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"sdm_subscription_req\",
message_direction=\"outbound\"}[5m])) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of sdm_subscription_req responses received
is lesser threshold."
    exit
exit

```

## N10 Charging Data Request

Use the following commands to configure alerts related to N10 Charging Data Request.

```

alerts rules group SMFsvcStatus
  interval-seconds 300
  rule SMFN10ChargingRequest
    expression
"sum(increase(smf_restep_http_msg_total{api_name=\"chf_charging_data_request\",
message_direction=\"outbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"chf_charging_data_request\",
message_direction=\"outbound\"}[5m])) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of chf_charging_data_request responses
received is lesser threshold."
    exit
exit

```

## N10 Charging Data Notify

Use the following commands to configure alerts related to N10 Charging Data Notify.

```

alerts rules group SMFsvcStatus
  interval-seconds 300
  rule SMFN10ChargingDataNotify
    expression "sum(increase(smf_restep_http_msg_total{api_name=\"chf_abort_notify\",
message_direction=\"inbound\", response_status=\"201\"}[5m])) /
sum(increase(smf_restep_http_msg_total{api_name=\"chf_abort_notify\",
message_direction=\"inbound\"}[5m])) < 0.95"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of chf_abort_notify responses sent is
lesser threshold."

```

```

    exit
exit

```

## Policy Rule Alerts

This section provides detail of commands that are required to configure alerts related to various policy rules.

### Addition of Dynamic PCC Rules

Use the following commands to configure alerts related to addition of dynamic PCC rules.

```

alerts rules group SMFPolicyStatus
  interval-seconds 300
  rule AddPCCRule
  expression
    "sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"success\",operation=\"install\"}[5m]))
    /
    sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"attempted\",operation=\"install\"}[5m]))
    < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of successful addition of dynamic pcc
  rules is lesser threshold."
  exit
exit

```

### Modification of Dynamic PCC Rules

Use the following commands to configure alerts related to modification of dynamic PCC rules.

```

alerts rules group SMFPolicyStatus
  interval-seconds 300
  rule ModifyPCCRule
  expression
    "sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"success\",operation=\"modify\"}[5m]))
    /
    sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"attempted\",operation=\"modify\"}[5m]))
    < 0.95"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of successful modification of dynamic
  pcc rules is lesser threshold."
  exit
exit

```

### Removal of Dynamic PCC Rules

Use the following commands to configure alerts related to removal of dynamic PCC rules.

```

alerts rules group SMFPolicyStatus
  interval-seconds 300
  rule RemovePCCRule
  expression

```

```

"sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"success\",operation=\"remove\"}[5m]))
/
sum(increase(policy_dynamic_pcc_rules_total{app_name=\"SMF\",event=\"attempted\",operation=\"remove\"}[5m]))
< 0.95"
severity major
type "Communications Alarm"
annotation summary
value "This alert is fired when the percentage of successful removal of dynamic pcc
rules is lesser threshold."
exit
exit

```

## SMF Overload/Congestion

This section provides detail of commands that are required to configure alerts related to various SMF Overload/Congestion.

### SMF Overload

Use the following commands to configure alerts related to the SMF Overload procedure.

```

alerts rules group SMFSvcStatus
interval-seconds 300
rule SMFOverload
expression "sum by (component) (system_overload_status) == true"
severity major
type "Communications Alarm"
annotation summary
value "This alert is fired when increase in events not processed due to system overload"

exit
exit

```

## SMF Sessions

This section provides detail of commands that are required to configure alerts related to various SMF sessions.

### Session Release Rate

Use the following commands to configure alerts related to the Session Release Rate procedure.

```

alerts rules group SMFSession
interval-seconds 300
rule SMFSessionReleaseRate
expression "sum(rate(smf_service_stats{procedure_type=~\".*pdu_sess_rel|.pdn_sess_rel\"
, status=\"attempted\"}[5m])) > THRESHOLD "
severity major
type "Communications Alarm"
annotation summary
value "This alert is fired when the session release rate exceeds the threshold"
exit
exit

```

## Session Setup Failure

Use the following commands to configure alerts related to the Session Setup Failure procedure.

```

alerts rules group SMFSession
interval-seconds 300
rule SMFSessionSetupFailure
expression "sum(smf_service_stats{procedure_type=~\"pdu_sess_create|pdn_sess_create\"
, status=\"failures\"}) /
sum(smf_service_stats{procedure_type=\"pdu_sess_create|pdn_sess_create\" ,
status=\"attempted\"}) > 0.05 "
severity major
type "Communications Alarm"
annotation summary
value "This alert is fired when failed to setup sessions is more than 5%"
exit
exit

```

## Session Setup Rate

Use the following commands to configure alerts related to the Session Setup Rate procedure.

```

alerts rules group SMFSession
interval-seconds 300
rule SMFSessionSetupRate
expression
"sum(rate(smf_service_stats{procedure_type=~\"pdu_sess_create|pdn_sess_create\" ,
status=\"attempted\"}[5m]))> THRESHOLD "
severity major
type "Communications Alarm"
annotation summary
value "This alert is fired when the session setup rate exceeds the threshold"
exit
exit

```

## Subscriber Limit

Use the following commands to configure alerts related to the Subscriber Limit procedure.

```

alerts rules group SMFSession
interval-seconds 300
rule SMFSubscriberLimit
expression "sum(smf_session_counters{pdu_type=~\"ipv4v6|ipv4|ipv6\"}) > THRESHOLD"
severity major
type "Communications Alarm"
annotation summary
value "This alert is fired when the max number of subscribers is more
than the threshold"
exit
exit

```







# CHAPTER 11

## Bulk Statistics and Key Performance Indicators

- [Feature Summary and Revision History, on page 131](#)
- [Feature Description, on page 131](#)
- [How it Works, on page 132](#)

### Feature Summary and Revision History

#### Summary Data

*Table 32: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 33: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

### Feature Description

This chapter provides details of bulk statistics, and Key Performance Indicators (KPIs) used for performance analysis on SMF.

There are two types of bulk statistics:

- Gauge - A snapshot value that shows the statistic at that reporting moment (for example, the number of current PDP contexts, simultaneous Active EPS Bearers). Gauge statistics can increment or decrement continuously.
- Counter - A historic value that shows the statistic that accumulated over time (for example, the total number of CSR requests received). Counter values can only increment except in two cases: rollover, where a counter exceeds its maximum value and rolls over to zero, and reset, where a counter is manually reset to zero.

## How it Works

The following bulk statistics are supported in SMF for Attempted, Success, and Failures:

- 4G and WiFi message-level statistics (CREATE, DELETE, UPDATE)
- PCF and CHF message-level statistics
- Handover:
  - 4G to 5G
  - 5G to 4G
  - Voice over New Radio (VoNR)
  - WiFi to NR
  - NR to WiFi
  - WiFi to eNB
  - eNB to WiFi

## Supported KPIs

### Common Statistics

The following table provides details of KPIs related to common statistics.

KPI Name	Type	Description/Formula	Label
Total PCF Policy Create Attempted	Counter	Total number of PCF Create attempted (%smPolicyCreate%)	status="attempted",dnn,rat_type
Total PCF Policy Create Success	Counter	(%smPolicyCreate%) Total PCF Policy Create Attempted - Total PCF Policy Create Failure	dnn,rat_type

KPI Name	Type	Description/Formula	Label
Total PCF Policy Create Failure	Counter	(%smPolicyCreate%)	status="failed",dnn, rat_type
Total PCF Policy Update Attempted	Counter	(%smPolicyUpdate%)	status="attempted", dnn, rat_type
Total PCF Policy Update Success	Counter	(%smPolicyUpdate%) Total PCF Policy Update Attempted - Total PCF Policy Update Failure	dnn, rat_type
Total PCF Policy Update Failure	Counter	(%smPolicyUpdate%)	status="failed", dnn, rat_type
Total PCF Update Notify Received	Counter	(%smPolicyUpdateNotify%)	status="accepted",dnn, rat_type
Total PCF Update Notify success	Counter	Total PCF Update Notify Received - Total PCF Update Notify failure	dnn, rat_type
Total PCF Update Notify Failure	Counter	(%smPolicyUpdateNotify%)	status="rejected"/status="failed",dnn, rat_type
Total PCF Terminate Attempted	Counter	(%smPolicyTerminate%)	status="attempted", dnn, rat_type
Total PCF Terminate Success	Counter	(%smPolicyTerminate %)	status="success",dnn, rat_type
Total PCF Terminate Failures	Counter	(%smPolicyTerminate%)	status="failure", dnn, rat_type
Total CHF Update Attempted	Counter	(%charging_update%)	status="attempted", dnn, rat_type
Total CHF Update Success	Counter	(%charging_update%)	status="success", dnn, rat_type
Total CHF Update Failure/Timeout	Counter	(%charging_update%)	status="failure", dnn, rat_type
Total CHF terminate Attempted	Counter	(%charging_terminate%)	status="attempted", dnn, rat_type

KPI Name	Type	Description/Formula	Label
Total CHF terminate Success	Counter	(%charging_terminate%)	status="success", dnn, rat_type
Total CHF terminate Failure	Counter	(%charging_terminate%)	status="failure", dnn, rat_type
Total 5gto4g Handover Attempted	Counter	pdn_5g_4g_handover pdn_5g_4g_handover_dft pdn_5g_4g_handover_idft	status="attempted"
Total 5gto4g Handover Success	Counter	pdn_5g_4g_handover pdn_5g_4g_handover_dft pdn_5g_4g_handover_idft	status="success"
Total 5gto4g Handover Failure	Counter	pdn_5g_4g_handover pdn_5g_4g_handover_dft pdn_5g_4g_handover_idft	status="failure", reason="idft_setup_failure" reason="mbr_setup_failure" reason="upf_failure"
Total 4gto5g Handover Attempted	Counter	n26_4g_to_5g_handover n26ho_4g_5g_dft n26ho_4g_5g_idft n26_4g_to_5g_im_mobility	status="attempted"
Total 4gto5g Handover Success	Counter	n26_4g_to_5g_handover n26ho_4g_5g_dft n26ho_4g_5g_idft n26_4g_to_5g_im_mobility	status="success"
Total 4gto5g Handover Failure	Counter	n26_4g_to_5g_handover n26ho_4g_5g_dft n26ho_4g_5g_idft n26_4g_to_5g_im_mobility	status="failure" reason="n26ho_4g_5g_n1n2_transfer_failure" reason="disc_n26_4g_5g_ho_udm_reg_failed" reason="disc_n26_4g_5g_ho_n4_modify_failed"
Total EPSFB Attempted	Counter	eps_fb_5g_4g_handover_dft eps_fb_5g_4g_handover_idft eps_fb_ded_brr	status="attempted",

KPI Name	Type	Description/Formula	Label
Total EPSFB Success	Counter	eps_fb_5g_4g_handover_dft eps_fb_5g_4g_handover_idft eps_fb_ded_brr	status="success",
Total EPSFB Failure	Counter	eps_fb_5g_4g_handover_dft eps_fb_5g_4g_handover_idft eps_fb_ded_brr	status="failure", reason="idft_setup_failure" reason="mbr_setup_failure" reason="upf_failure" reason="sgw_failure"
Total NRtoWifi Attempted	Counter	nr_to_untrusted_wifi_handover pdn_5g_4g_handover pdn_5g_4g_handover_dft pdn_5g_4g_handover_idft	status="attempted"
Total NRtoWifi Success	Counter	nr_to_untrusted_wifi_handover pdn_5g_4g_handover pdn_5g_4g_handover_dft pdn_5g_4g_handover_idft	status="success"
Total NRtoWifi Failure	Counter	nr_to_untrusted_wifi_handover pdn_5g_4g_handover pdn_5g_4g_handover_dft pdn_5g_4g_handover_idft	status="failure", reason="nr_to_untrusted_wifi_invalid_json" reason="nr_to_untrusted_wifi_invalid_paa" reason="nr_to_untrusted_wifi_invalid_msg" reason="nr_to_untrusted_wifi_pcf_failed" reason="nr_to_untrusted_wifi_n40_failed" reason="nr_to_untrusted_wifi_n4_failed" reason="nr_to_untrusted_wifi_pcf_failed_post_cb" reason="nr_to_untrusted_wifi_n40_failed_post_cb" reason="nr_to_untrusted_wifi_n4_failed_post_cb" reason="nr_to_untrusted_wifi_cbr_failed" reason="nr_to_untrusted_wifi_n1n2_release_failed" reason="nr_to_untrusted_wifi_n4_failed_post_ho" reason="nr_to_untrusted_wifi_pcf_update_failed_post_ho" reason="nr_to_untrusted_wifi_chf_update_failed_post_ho"

KPI Name	Type	Description/Formula	Label
Total WifitoNR Attempted	Counter	n26_4g_to_5g_handover n26ho_4g_5g_dft n26ho_4g_5g_idft	status="attempted"
Total WifitoNR Success	Counter	n26_4g_to_5g_handover n26ho_4g_5g_dft n26ho_4g_5g_idft	status="success"
Total WifitoNR Failure	Counter	n26_4g_to_5g_handover n26ho_4g_5g_dft n26ho_4g_5g_idft	status="failure"
Total eNBtoWifi Attempted	Counter	enb_to_untrusted_wifi_handover	status="attempted"
Total eNBtoWifi Success	Counter	enb_to_untrusted_wifi_handover	status="success"

KPI Name	Type	Description/Formula	Label
Total eNBtoWifi Failure	Counter	enb_to_untrusted_wifi_handover	status="failure", reason="enb_to_untrusted_wifi_to_enb_ho_reject" reason="enb_to_untrusted_wifi_to_enb_invalid_sess_state" reason="enb_to_untrusted_wifi_to_enb_invalid_json" reason="enb_to_untrusted_wifi_to_enb_invalid_paa" reason="enb_to_untrusted_wifi_to_enb_invalid_msg" reason="enb_to_untrusted_wifi_to_enb_udm_failed" reason="enb_to_untrusted_wifi_to_enb_n40_failed" reason="enb_to_untrusted_wifi_to_enb_n4_failed" reason="enb_to_untrusted_wifi_to_enb_pcf_failed_post_cb" reason="enb_to_untrusted_wifi_to_enb_mbr_failed" reason="enb_to_untrusted_wifi_to_enb_n4_failed_post_mbr" reason="enb_to_untrusted_wifi_to_enb_n40_failed_post_cb" reason="enb_to_untrusted_wifi_to_enb_n4_failed_post_cb" reason="enb_to_untrusted_wifi_to_enb_n40_failed_post_db" reason="enb_to_untrusted_wifi_to_enb_pcf_failed_post_db" reason="enb_to_untrusted_wifi_to_enb_cbr_failed" reason="enb_to_untrusted_wifi_to_enb_dbr_failed"
Total WifitoeNB Attempted	Counter	untrusted_wifi_to_enb_handover	status="attempted"
Total WifitoeNB Success	Counter	untrusted_wifi_to_enb_handover	status="success",

KPI Name	Type	Description/Formula	Label
Total WifitoeNB Failure	Counter	untrusted_wifi_to_enb_handover	status="failure", reason="enb_to_untrusted_wifi_to_enb_ho_reject" reason="enb_to_untrusted_wifi_to_enb_invalid_sess_state" reason="enb_to_untrusted_wifi_to_enb_invalid_json" reason="enb_to_untrusted_wifi_to_enb_invalid_paa" reason="enb_to_untrusted_wifi_to_enb_invalid_msg" reason="enb_to_untrusted_wifi_to_enb_udm_failed" reason="enb_to_untrusted_wifi_to_enb_n40_failed" reason="enb_to_untrusted_wifi_to_enb_n4_failed" reason="enb_to_untrusted_wifi_to_enb_pcf_failed_post_cb" reason="enb_to_untrusted_wifi_to_enb_mbr_failed" reason="enb_to_untrusted_wifi_to_enb_n4_failed_post_mbr" reason="enb_to_untrusted_wifi_to_enb_n40_failed_post_cb" reason="enb_to_untrusted_wifi_to_enb_n4_failed_post_cb" reason="enb_to_untrusted_wifi_to_enb_n40_failed_post_db" reason="enb_to_untrusted_wifi_to_enb_pcf_failed_post_db" reason="enb_to_untrusted_wifi_to_enb_cbr_failed" reason="enb_to_untrusted_wifi_to_enb_dbr_failed"

#### 4G Subscriber

The following table provides details of KPIs related to 4G subscriber statistics.



**Note** Labels dnn, qci and rat\_type are used to filter the counters. Here, rat\_type is eutra.



KPI Name	Type	Description/Formula	Label
Total Active sessions	Gauge	Total number of PDN Contexts (%smf_session_counters%)	dnn, rat_type="eutra"
Total Active Bearers	Gauge	Total number of active Bearers (%total_bearer%)	dnn
Total Active Default Bearers	Gauge	(%total_bearer-dedicated_bearer%)	dnn
Total Active Dedicated Bearers	Gauge	Total number of active Dedicated Bearers (%dedicated_bearer%)	dnn
Total Bearer Creation Attempted	Counter	(%pdn_sess_create+pcf_req_ded_brr_create+eps_fb_ded_brr)	status="attempted",dnn
Total Bearers Creation Success	Counter	(%pdn_sess_create+pcf_req_ded_brr_create+eps_fb_ded_brr)	status="success",dnn
Total Bearers Creation Failure	Counter	(%pdn_sess_create+pcf_req_ded_brr_create+eps_fb_ded_brr)	status="failure",dnn
Total Dedicated Bearers Attempted	Counter	(%pcf_req_ded_brr_create+eps_fb_ded_brr %)	status="attempted",dnn
Total Dedicated Bearers Failure/Rejected	Counter	(%pcf_req_ded_brr_create+eps_fb_ded_brr %)	status="failure",dnn
Total Dedicated Bearers Success	Counter	(%pcf_req_ded_brr_create+eps_fb_ded_brr %)	status="success", dnn, rat_type="eutra"
Total CSR Attempted	Counter	(%pdn_sess_create%)	status="attempted",dnn
Total CSR Failure/Rejected	Counter	(%pdn_sess_create%)	status="failure",dnn,
Total CSR Success	Counter	(%pdn_sess_create%)	status="success",dnn
Total CBR Attempted	Counter	(%create_bearer_request%)	status="attempted",dnn, fiveqi, rat_type="eutra"
Total CBR failure	Counter	(%create_bearer_request%)	status="failure", fiveqi, dnn, rat_type="eutra"
Total CBR success	Counter	(%create_bearer_request%)	status="success",dnn, fiveqi, rat_type="eutra"
Total CBR retransmission rx	Counter	(%create_bearer_request%)	status="retransmit",dnn, fiveqi, rat_type="eutra"

KPI Name	Type	Description/Formula	Label
Total DBR Attempted	Counter	(%delete_bearer_request%)	status="attempted",dnn, fiveqi, rat_type="eutra"
Total DBR failure/Rejected	Counter	(%delete_bearer_request%)	status="failure", fiveqi, dnn, rat_type="eutra"
Total DBR success	Counter	(%delete_bearer_request%)	status="success", fiveqi, dnn, fiveqi, rat_type="eutra"
Total DBR retransmission tx	Counter	(%delete_bearer_request%)	status="retransmit", dnn, fiveqi, rat_type="eutra"
Total UBR Attempted	Counter	(%update_bearer_request%)	status="attempted",dnn, fiveqi, rat_type="eutra"
Total UBR failure/Rejected	Counter	(%update_bearer_request%)	status="failure", fiveqi, dnn, rat_type="eutra"
Total UBR Success	Counter	(%update_bearer_request%)	status="success", fiveqi, dnn, rat_type="eutra"
Total UBR retransmission	Counter	(%update_bearer_request%)	status="retransmit",dnn , rat_type="eutra"
Total EPSFB Dedicated Bearers	Counter	(%eps_fb_ded_brr%)	dnn

### 5G Subscriber

The following table provides details of KPIs related to 5G subscriber statistics.

KPI Name	Type	Description/Formula	Label
Total Active sessions	Gauge	Total number of PDU Contexts (%smf_session_counters%)	dnn, rat_type="nr"
Total Active Flows	Gauge	(%policy_pdu_flows_curent%)	dnn, fiveqi, rat_type="nr"
Total Flow Creation Attempted	Counter	(%policy_pdu_flows_total%)	status="attempted",dnn, fiveqi, rat_type="nr"
Total Flow Creation Success	Counter	(%policy_pdu_flows_total%)	status="success",dnn, fiveqi, rat_type="nr"
Total Flow Creation Failure	Counter	(%policy_pdu_flows_total%)	status="failure",dnn, fiveqi, rat_type="nr"

### WiFi Subscriber

The following table provides details of KPIs related to WiFi subscriber statistics.

KPI Name	Type	Description/Formula	Label
Total CSR Attempted	Counter	(%untrusted_wifi_to_enb_handover%)	status="attempted",dnn, rat_type="wlan"
Total CSR failure/Rejected	Counter	(%untrusted_wifi_to_enb_handover%)	status="failure",dnn, rat_type="wlan"
Total CSR success	Counter	(%untrusted_wifi_to_enb_handover%)	status="success",dnn , rat_type="wlan"
Total CBR Attempted	Counter	(%create_bearer_request%)	status="attempted", rat_type="wlan"
Total CBR failure	Counter	(%create_bearer_request%)	status="failure", rat_type="wlan"
Total CBR success	Counter	(%create_bearer_request%)	status="success", rat_type="wlan"
Total DBR Attempted	Counter	(%delete_bearer_request%)	status="attempted", rat_type="wlan"
Total DBR failure/Rejected	Counter	(%delete_bearer_request%)	status="failure", rat_type="wlan"
Total DBR success	Counter	(%delete_bearer_request%)	status="success", rat_type="wlan"





# CHAPTER 12

## Cause Code Handling

- [Feature Summary and Revision History](#), on page 143
- [Feature Description](#), on page 143
- [5GSM Cause Code Handling](#), on page 144

### Feature Summary and Revision History

#### Summary Data

*Table 34: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 35: Revision History*

Revision Details	Release
Added support for 5GSM cause code handling.	2020.02.0

### Feature Description

This chapter describes the GPRS Tunneling Protocol, Version 2 (GTPv2) IEs and cause codes for 4G and 5G procedures.

# 5GSM Cause Code Handling

## Feature Description

The SMF supports 5GSM cause handling for the UE and Network initiated procedures.

The supported procedures are:

- PDU-Session-Establishment
- PDU-Session-Modification
- PDU-Session-Release

## PDU Session Establishment Reject

If the connectivity with the requested DN is rejected by the network, SMF sets the 5GSM cause IE of the PDU Session Establishment Reject message to indicate the reason for rejecting the PDU Session Establishment procedure.

The SMF supports the following causes in the PDU Session Establishment Reject message.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #26 – insufficient resources	The SMF includes this cause when it receives N2SmInfoType with "PDU_RES_SETUP_FAIL" along with any of the following N2 causes: <ul style="list-style-type: none"> <li>• RadioNetwork/Radio_resources_not_available</li> <li>• RadioNetwork/Failure_in_the_radio_interface_procedure</li> <li>• Misc/Not_enough_user_plane_processing_resources</li> </ul>
Cause #27 – missing or unknown DNN	The SMF includes this cause when DNN is not present in SmContextCreateData even though it is required and not configured in SMF.
Cause #28 – unknown PDU session type	The SMF includes this cause when the PDU Session Establishment Request message includes a PDU session type that is not supported by SMF.
Cause #29 – user authentication or authorization failed	The SMF includes this cause when DN authentication of the UE was performed and completed unsuccessfully (Radius Authentication Timeout).
Cause #32 – service option not supported	The SMF supports this cause when the validation of received S-NSSAI fails against the allowed list of S-NSSAI.
Cause #33 – requested service option not subscribed	The SMF supports this cause when the UE requests a service option for which it has no subscription.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #38 – network failure	The SMF supports this cause when the requested service was rejected due to an error in the network. This includes any internal failures or no response from any external NF during the PDN-setup procedure.
Cause #54 – PDU session does not exist	The SMF supports this cause when it does not have any information about the PDU session which is requested by the UE to transfer between 3GPP access and non-3GPP access or from the EPS to the 5GS.
Cause #70 – missing or unknown DNN in a slice	The SMF supports this cause when the slice configuration is present but the requested DNN is not configured under the slice in the SMF.
Protocol errors	
Cause #95 – Semantically incorrect message	This 5GSM cause reports receipt of a message with semantically incorrect content.  <b>Important</b> For mandatory parameters (PDU Session Identity and Procedure Transaction Identity) with non-semantical error also, the SMF sends this cause.

## PDU Session Modification Reject

If the SMF does not accept the request to modify the PDU session, it sets the 5GSM cause IE of the PDU Session Modification Reject message to indicate the reason for rejecting the PDU session modification procedure.

The SMF supports the following causes in the PDU Session Modification Reject message.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #43 – Invalid PDU session identity	The SMF sends this cause when SMF does not have the session.
Protocol errors	
Cause #95 – Semantically incorrect message	This 5GSM cause reports receipt of a message with semantically incorrect content.  <b>Important</b> For mandatory parameters (PDU Session Identity and Procedure Transaction Identity) with non-semantical error also, the SMF sends this cause.

## PDU Session Release Reject

If the SMF does not accept the request to release the PDU session, SMF sets the 5GSM Cause IE of the PDU Session Release Reject message to indicate the reason for rejecting the PDU session release.

The SMF supports the following causes in the PDU Session Release Reject message.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #43 – Invalid PDU session identity	The SMF supports this cause when SMF does not have the session.
Protocol errors	
Cause #95 – Semantically incorrect message	This 5GSM cause reports receipt of a message with semantically incorrect content.  <b>Important</b> For mandatory parameters (PDU Session Identity and Procedure Transaction Identity) with non-semantical error also, the SMF sends this cause.

## PDU Session Release Request

To initiate the UE-requested PDU Session Release procedure, UE sends the PDU Session Release Request message with the 5GSM Cause IE to indicate the reason for releasing the PDU session.

The SMF supports the following causes in the PDU Session Release Request message.

Reject Cause / 5GSM Cause	SMF Behavior
Cause #36 – regular deactivation	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #41 – Semantic error in the TFT operation	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #42 – Syntactical error in the TFT operation	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #44 – Semantic errors in packet filter(s)	The SMF retains the statistics based on the cause and continues with the Release procedure.
Cause #45 – Syntactical errors in packet filter(s)	The SMF retains the statistics based on the cause and continues with the Release procedure.

## PDU Session Modification Command Reject

If the UE rejects the PDU-Session-Modification-Command, it sets the 5GSM cause IE of the PDU Session Modification Reject message to indicate the reason for rejecting the PDU session modification.

The SMF supports the following 5GSM causes.

5GSM Cause	SMF Behavior
Cause #26 – insufficient resources	The SMF retains the statistics based on the cause.
Cause #43 – Invalid PDU session identity	The SMF retains the statistics based on the cause and releases the existing PDU session.
Cause #44 – Semantic error in packet filter(s)	The SMF retains the statistics based on the cause.



5GSM Cause	SMF Behavior
Cause #45 – Syntactical error in packet filter(s)	The SMF retains the statistics based on the cause.
Cause #83 – Semantic error in the QoS operation	The SMF retains the statistics based on the cause.
Cause #85 – Syntactical error in the QoS operation	The SMF retains the statistics based on the cause.

## How it Works

The SMF supports 5GSM cause handling for the PDU-Session-Establishment, PDU-Session-Modification and PDU-Session-Release procedures. An appropriate SM cause will be sent over the N1 message to the UE.

## Standards Compliance

The 5GSM Cause Handling feature complies with the *3GPP TS 24.501, version 15.4.0, Release 15* (Non-Access-Stratum (NAS) protocol for 5G System (5GS)).

## Configuring the 5GSM Cause Handling Feature

### 5GSM Cause Handling OAM Support

This section describes operations, administration, and maintenance information for this feature.

### Statistics

The 5GSM Cause Handling feature supports the following statistics to track the number of failures based on the 5GSM cause.

#### SMF N1 Message Stats

##### PDU-Session-Establishment-Reject:

- **NETWORK\_FAILURE:** The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "NETWORK\_FAILURE".
- **UNKNOWN\_PDU\_SESSION\_TYPE:** The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "UNKNOWN\_PDU\_SESSION\_TYPE".
- **USER\_AUTHENTICATION\_OR\_AUTHORIZATION\_FAILED:** The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "USER\_AUTHENTICATION\_OR\_AUTHORIZATION\_FAILED".
- **REQUESTED\_SERVICE\_OPTION\_NOT\_SUBSCRIBED:** The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "REQUESTED\_SERVICE\_OPTION\_NOT\_SUBSCRIBED".
- **MISSING\_OR\_UNKNOWN\_DNN:** The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "MISSING\_OR\_UNKNOWN\_DNN".
- **SERVICE\_OPTION\_NOT\_SUPPORTED:** The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "SERVICE\_OPTION\_NOT\_SUPPORTED".

- **INSUFFICIENT\_RESOURCES**: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "INSUFFICIENT\_RESOURCES".
- **MISSING\_OR\_UNKNOWN\_DNN\_IN\_A\_SLICE**: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "MISSING\_OR\_UNKNOWN\_DNN\_IN\_A\_SLICE".
- **PDU\_SESSION\_DOES\_NOT\_EXIST**: The number of PDU-Session-Establishment-Reject messages sent from SMF with N1 Cause "PDU\_SESSION\_DOES\_NOT\_EXIST".

#### **PDU-Session-Modification-Reject:**

- **INVALID\_PDU\_SESSION\_IDENTITY**: The number of PDU-Session-Modification-Reject messages sent from SMF with N1 Cause "INVALID\_PDU\_SESSION\_IDENTITY".

#### **PDU-Session-Release-Reject:**

- **INVALID\_PDU\_SESSION\_IDENTITY**: The number of PDU-Session-Release-Reject messages sent from SMF with N1 Cause "INVALID\_PDU\_SESSION\_IDENTITY".

#### **PDU-Session-Release-Request:**

- **REGULAR\_DEACTIVATION**: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "REGULAR\_DEACTIVATION".
- **SEMANTIC\_ERRORS\_IN\_PACKET\_FILTER**: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SEMANTIC\_ERRORS\_IN\_PACKET\_FILTER".
- **SYNTACTICAL\_ERROR\_IN\_PACKET\_FILTER**: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SYNTACTICAL\_ERROR\_IN\_PACKET\_FILTER".
- **SEMANTIC\_ERROR\_IN\_THE\_TFT\_OPERATION**: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SEMANTIC\_ERROR\_IN\_THE\_TFT\_OPERATION".
- **SYNTACTICAL\_ERROR\_IN\_THE\_TFT\_OPERATION**: The number of PDU-Session-Release-Request messages received in SMF with N1 Cause "SYNTACTICAL\_ERROR\_IN\_THE\_TFT\_OPERATION".

#### **PDU-Session-Modification-Command-Reject:**

- **INSUFFICIENT\_RESOURCES**: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "INSUFFICIENT\_RESOURCES".
- **INVALID\_PDU\_SESSION\_IDENTITY**: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "INVALID\_PDU\_SESSION\_IDENTITY".
- **SEMANTIC\_ERRORS\_IN\_PACKET\_FILTER**: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SEMANTIC\_ERRORS\_IN\_PACKET\_FILTER".
- **SYNTACTICAL\_ERROR\_IN\_PACKET\_FILTER**: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SYNTACTICAL\_ERROR\_IN\_PACKET\_FILTER".
- **SEMANTIC\_ERROR\_IN\_THE\_QOS\_OPERATION**: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SEMANTIC\_ERROR\_IN\_THE\_QOS\_OPERATION".

- SYNTACTICAL\_ERROR\_IN\_THE\_TFT\_OPERATION: The number of PDU-Session-Modification-Command-Reject messages received in SMF with N1 Cause "SYNTACTICAL\_ERROR\_IN\_THE\_TFT\_OPERATION".





# CHAPTER 13

## Cisco Common Data Layer

- [Feature Summary and Revision History, on page 151](#)
- [Feature Description, on page 152](#)
- [How it Works, on page 152](#)
- [Call Flows, on page 153](#)
- [Configuring the CDL Through SMF Ops Center, on page 154](#)

### Feature Summary and Revision History

#### Summary Data

*Table 36: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 37: Revision History*

Revision Details	Release
Added the procedures for configuration and verification of the event trace data in the CDL database record.	2021.02.0
First introduced.	Pre-2020.02.0

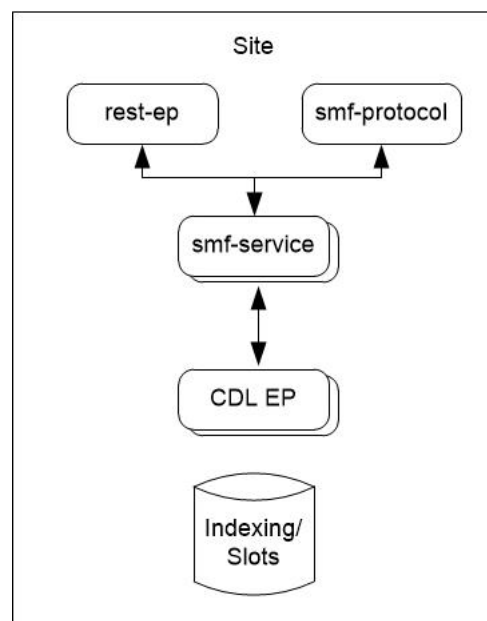
## Feature Description

The SMF extends support to the Geo Redundant (GR) version of the Cisco Common Data Layer (CDL). When the primary CDL endpoint fails, the SMF attempts the same operation on the next highly rated secondary endpoint thus providing a non-disrupted N7 or Diameter message handling. If the next rated endpoint is unavailable, then the SMF reattempts the operation on the subsequent endpoint that has the highest rating and so on.

## Architecture

The following figure depicts the failover that happens when the SMF service is unable to access the CDL datastore endpoint.

**Figure 23: CDL Datastore Architecture**



With relevance to this architecture, you can configure CDL through SMF Ops Center. When the SMF connects to the CDL, it uses the local endpoints.

## How it Works

When you configure the CDL in SMF through the SMF Ops Center, SMF gets enabled to support multiple CDL datastore endpoints. You can configure the endpoints by specifying the IP addresses, ports, and assigning ratings to each endpoint. By default, SMF considers the local endpoint as the primary endpoint, which has the highest rating. SMF performs CDL API operations on the primary endpoint. If this endpoint is unavailable, then SMF routes the operations to the next highest rated endpoint. SMF keeps failing over to the accessible secondary endpoint or until all the configured secondaries are exhausted. It does not reattempt a query on the next rated endpoint if the endpoint is reachable but responds with error or timeout.

If SMF is unable to access any of the endpoints in the cluster, then CDL operation fails with the "Datastore Unavailable" error.

## Call Flows

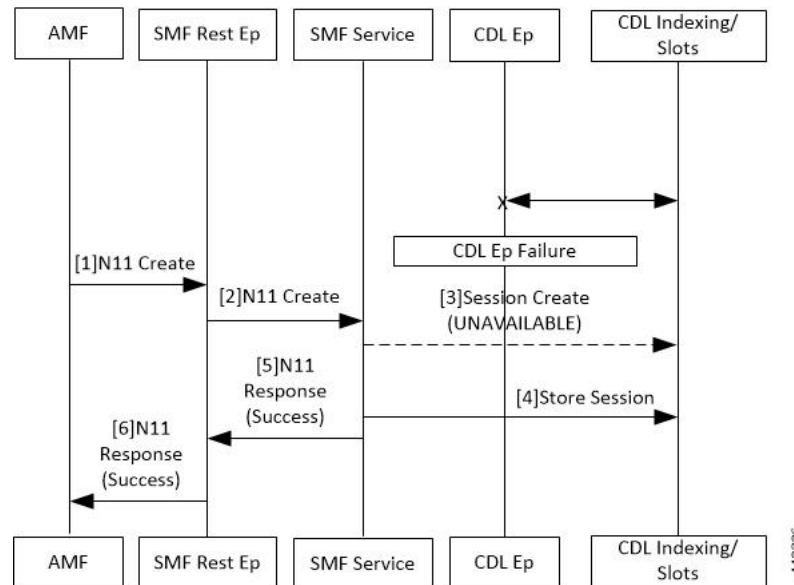
This section describes the call flow that is associated with this feature.

- [CDL Endpoint Failure Call Flow, on page 153](#)

### CDL Endpoint Failure Call Flow

This section describes the SMF local data store endpoint failure call flow.

**Figure 24: CDL Endpoint Failure Call Flow**



**Table 38: CDL Endpoint Failure Call Flow Description**

Step	Description
1	The AMF sends a Create Request to SMF REST endpoint over the N11 interface.
2	After receiving the request, the SMF REST endpoint forwards the Create Request to the SMF service.
3	The SMF service attempts to reach the CDL endpoint to send the session creation request. However, the CDL endpoint is unreachable.
4	The Create Request is evaluated in the stored session and the SMF service forwards the request to the CDL endpoint.
5	After the call request is successful, the SMF service notifies the Success Message to the SMF REST endpoint.

Step	Description
6	The SMF REST endpoint forwards the Success Message to the AMF.

## Limitations

The CDL configuration in SMF has the following limitations:

- The SMF service attempts to reroute the calls only when it encounters gRPC errors such as UNAVAILABLE. It does not acknowledge errors that the datastore endpoint returns and actual gRPC timeouts such as DEADLINE\_EXCEEDED gRPC status code.
- The SMF service does not resolve failures occurring with the datastore such as indexing and slot failures. The CDL layer must resolve these failures and if necessary, send an API call on the remote.

## Configuring the CDL Through SMF Ops Center

The configuration of the CDL using SMF Ops Center involves the following steps:

1. [Configuring the CDL Session Database and Defining the Base Configuration, on page 154](#)
2. [Configuring the Zookeeper in CDL, on page 155](#)

## Configuring the CDL Session Database and Defining the Base Configuration

This section describes how to configure the CDL session database and define the base configuration in SMF.

1. From the SMF Ops Center, run the following command to configure the CDL session database and base configuration.

```

config
  cdl system-id system_id
  cdl node-type node_type
  cdl zookeeper replica zookeeper_replica_id
  exit
  cdl logging default-log-level debug_level
  cdl datastore session
    cluster-id cluster_id
    endpoint replica 1
    endpoint replica num_replica
    index map map_value
    slot replica num_replica
    slot map num_map/shards
    slot write-factor write_factor
    slot notification host host
    slot notification port port
    slot notification limit tps
    index replica num_replica
    index map num_map/shards
    index write-factor write_factor

```



**end**

#### NOTES:

- **cdl system-id** *system\_id*: This is an optional command. Specifies the system or Kubernetes cluster identity. The default value is 1.
- **cdl node-type** *node\_type*: This is an optional command. Specifies the Kubernetes node label to configure the node affinity. The default value is “session.” Accepted length of the value is 0–64 alphabets.
- **cdl zookeeper replica** *zookeeper\_replica\_id*: Specifies the zookeeper replica server's ID.
- **endpoint replica** *num\_replica*: This is an optional command. Specifies the number of replicas to be created. The default value is 1. Must be an integer in the range of 1–16.
- **slot replica** *num\_replica*: This is an optional command. Specifies the number of replicas to be created. The default value is 1. *num\_replica* must be an integer in the range of 1–16.
- **slot map** *num\_map/shards*: This is an optional command. Specifies the number of partitions in a slot. The default value is 1. *num\_map/shards* must be an integer in the range of 1–1024.
- **slot write-factor** *write\_factor*: This is an optional command. Specifies the number of copies to be written before successful response. The default value is 1. *write\_factor* must be an integer in the range of 0–16. Make sure that the value is lower than or equal to the number of replicas.
- **slot notification host** *host*: This is an optional command. Specifies the notification server hostname or IP address. The default value is `datastore-notification-ep`.
- **slot notification port** *port*: This is an optional command. Specifies the notification server Port number. The default value is 8890.
- **slot notification limit** *tps*: This is an optional command. Specifies the notification limit per second. The default value is 2000.
- **index replica** *num\_replica*: This is an optional command. Specifies the number of replicas to be created. The default value is 2. *num\_replica* must be an integer in the range of 1–16.
- **index map** *num\_map/shards*: This is an optional command. Specifies the number of partitions in a slot. The default value is 1. *num\_map/shards* must be an integer in the range of 1–1024. Avoid modifying this value after deploying the CDL.
- **index write-factor** *write\_factor*: This is an optional command. Specifies the number of copies to be written before successful response. The default value is 1. *write\_factor* must be an integer in the range of 0–16.

## Configuring the Zookeeper in CDL

This section describes how to configure the Zookeeper in CDL.

1. Open the Policy Ops Center console and navigate to the datastore CLI.
2. Run the following command to define the parameters.

```
configure
  cdl zookeeper data-storage-size data_storage_size_in_gb
```

```

log-storage-size log_storage_size_in_gb
replica number_of_replicas
enable-JMX-metrics boolean_value
enable-persistence boolean_value
end

```

**NOTES:**

All the following parameters are optional.

- **cdl zookeeper data-storage-size** *data\_storage\_size\_in\_gb*: Specifies the size of the Zookeeper data storage in gigabyte. The default value is 20 GB. Accepted value is an integer in the range of 1-64.
- **log-storage-size** *log\_storage\_size\_in\_gb*: Specifies the size of the Zookeeper data log's storage in gigabyte. The default value is 20 GB. Accepted value is an integer in the range of 1-64.
- **replica** *num\_replicas*: Specifies the number of replicas that must be created. The default value is 3. Accepted value is an integer in the range of one to 16.
- **enable-JMX-metrics** *boolean\_value*: Specifies the status of the JMX metrics. The default value is true.
- **enable-persistence** *boolean\_value*: Specifies the status of the persistent storage for Zookeeper data. The default value is *false*.

**Sample Configuration**

This section shows a sample configuration of CDL in a HA environment.

```

config
cdl system-id system_id
cdl zookeeper replica num_zk_replica
cdl datastore session
  endpoint replica ep_replica
  index map index_shard_count
  slot replica slot_replica
  slot map slot_shard_count

exit

```



# CHAPTER 14

## CHF and PCF Integration for Access and Mobility Procedures

- [Feature Summary and Revision History, on page 157](#)
- [Feature Description, on page 158](#)
- [How it Works, on page 158](#)

### Feature Summary and Revision History

#### Summary Data

*Table 39: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled - Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 40: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

The SMF leverages the 3GPP provision for the access and mobility procedures. With this provision, the SMF integrates the Charging Function (CHF) and Policy Control Function (PCF). SMF supports the following integration functions:

- CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers—SMF supports this function when a UE moves from one NG-RAN to another NG-RAN for Data Forwarding Tunnel (DFT) and Indirect Data Forwarding Tunnel (IDFT) cases.
- CHF and PCF Integration for N26 4G to 5G Handover—SMF supports the EPS to 5GS procedures with the N26 interface. SMF establishes Uplink (UL) Packet Detection Rule (PDR) or Downlink (DL) PDR toward with the qualified EPS Bearer Identity (EBI) list in 5GS and replicate EBIs to the respective flows. SMF also creates IDFT to support the Downlink forwarding traffic between SGW-U to NR over UPF.
- CHF and PCF Integration for N26 5G to 4G Handover—SMF supports 5GS to EPS procedures with the N26 interface. PGW-C establishes UL PDRs or DL PDRs toward SGW-U with qualified flows in 5GS and replicate EBIs to respective flows. PGW-C also creates an IDFT tunnel to support Downlink forwarding traffic between NR to SGW-U over UPF. Session-Level or Rating-Group level Charging Triggers are received during PDU Session establishment or in response to SMF-initiated Charging Update Request or CHF-initiated Charging Update Notify response in EPS procedures.
- CHF and PCF Integration for Xn Handover—SMF supports the Xn-based inter NG-RAN handover with and without UPF reallocation. The SMF supports Xn handovers for intra-AMF mobility only. SMF processes the received SM context update request that includes the path switch request N2-based message and the access-ide parameters. These parameters identify the CHF and PCF triggers that are received during PDU session establishment.
- CHF and PCF Integration for Service Request Procedures—SMF supports the service requests from both the UE and network-initiated procedures. Either a UE in CM-Idle state or the 5GC uses the Service Request procedure to request the establishment of a secure connection to an AMF. The UE in both the CM-Idle and in CM-Connected state use the Service Request procedure to activate a User Plane connection for an established PDU Session. The UE does not initiate a Service Request procedure if an ongoing Service Request procedure exists.

SMF saves the CHF and PCF triggers that SMF receives from CHF and PCF as part of session creation or PCF or UE-initiated modifications. When a UE triggers access and mobility procedures for the preceding functions, SMF identifies the triggers from CHF and PCF against the received access parameters. Then, SMF sends an update toward CHF and PCF.

## How it Works

The SMF integrates the CHF and PCF functions based on the following information:

- Policy control request triggers—received in the SM policy decision during
  - PDU session establishment or
  - PCF or UE initial modification

- Session-level or rating-group-level charging triggers—received during
  - PDU session establishment or
  - in response to
    - SMF-initiated Charging Update Request
    - CHF-initiated Charging Update Notify Request

The SMF supports the following access-side information to detect the PCF and CHF triggers. The SMF sends the trigger information to the CHF and PCF during the N2-based handover.

**Table 41: Access-Side Information for PCF and CHF Triggers**

Access-Side	CHF-Triggers	PCF-Triggers
UserLocation	USER_LOCATION_CHANGE	SAREA_CH
UeTimeZone	UE_TIMEZONE_CHANGE	SAREA_CH
ServingNetwork	PLMN_CHANGE	PLMN_CH
TargetServingNfId	SERVING_NODE_CHANGE	

## Call Flows

This section describes the following call flows:

- CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers Call Flow
- CHF and PCF Integration for N26 4G to 5G Handover Call Flow
- CHF and PCF Integration for N26 5G to 4G Handover Call Flow
- CHF and PCF Integration for Xn Handover Call Flow
- CHF and PCF Integration for Service Request Procedures

### CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers Call Flow

This section describes the call flow for the CHF and PCF Integration for Intra-AMF and Inter-AMF N2-based handovers.

Figure 25: CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers Call Flow

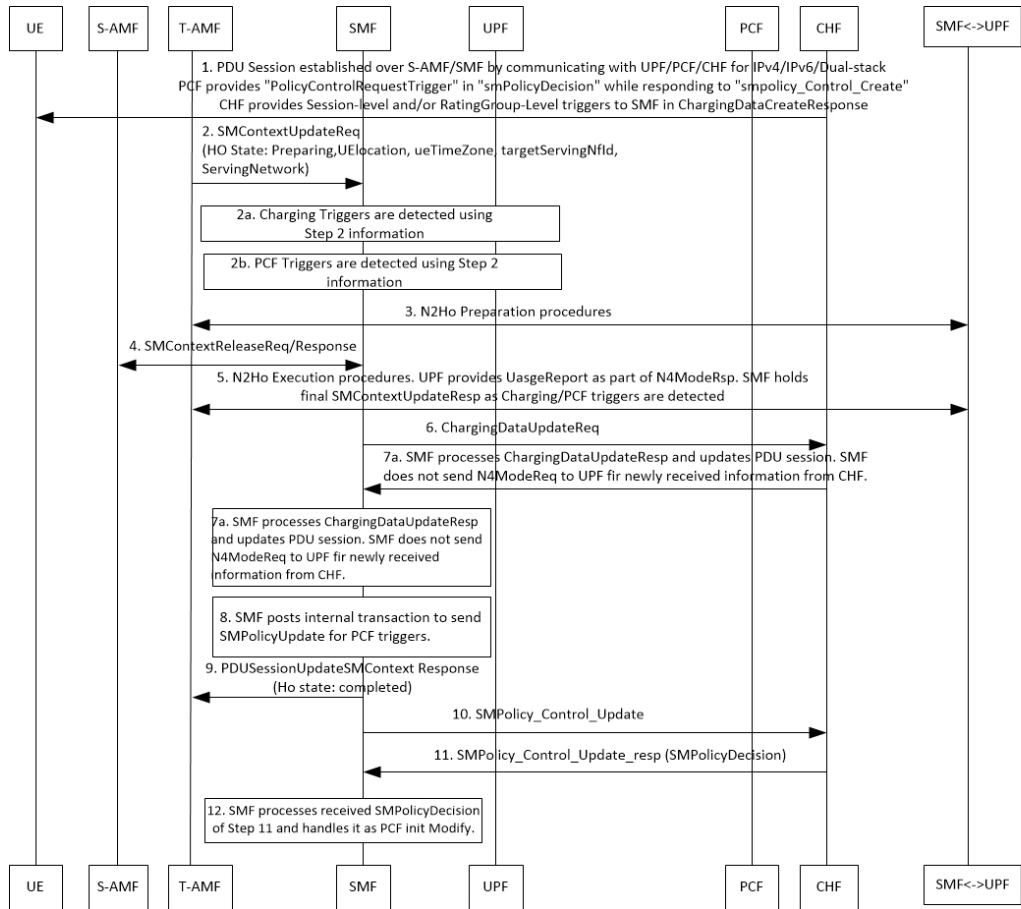


Table 42: CHF and PCF Integration for Intra-AMF and Inter-AMF N2-Based Handovers Call Flow Description

Step	Description
1	<p>The PDU session is established over S-AMF and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack.</p> <p>The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control.</p> <p>The CHF provides session-level and rating-group-level triggers to SMF as the Charging Data Create Response.</p>
2	<p>The T-AMF sends SM Context Update Request by including handover state to the SMF. The handover state includes the information on preparation, UE location, UE time zone, target serving NFID, and serving network. The AMF includes target serving NFID information for inter-AMF handoff.</p>
2a	<p>The SMF detects access-side changes that are received in the SM Context Update Request and the charging triggers with the information that is available in Step 2.</p>
2b	<p>The SMF detects the PCF triggers with the information that is available in Step 2.</p>

Step	Description
3	The N2-based Handover Preparation procedure starts from T-AMF towards the SMF and CHF and vice-versa.
4	In the N2-based Handover Execution procedure, in case of inter-AMF handoff, the SMF receives SM Context Release Request from S-AMF and responds with the SM Context Release Response to the S-AMF.
5	In N2-based Handover Execution procedure, the UPF provides the usage report as part of N4 modification response. The SMF holds the final SM Context Release Response when the SMF detects the CHF or PCF triggers.
6	The SMF sends the Charging Data Update Request to the CHF. This request includes the information on session-level triggers, multi-unit-Information (with rating-group-level triggers with usage report), customer identification, and PDU session charging information.
7	The CHF sends the Charging Data Update Response with optional multi-unit-information. The CHF also sends the new session or rating-group-level triggers to the SMF.
7a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 modification request to the UPF for the newly received information from the CHF.
8	The SMF posts the internal transaction to send the SM policy update information for PCF triggers.
9	The SMF sends the SM Context Update Response, for which the handover state is complete, to the T-AMF.
10	The SMF sends the SM Policy Control Update information to the PCF. The SM Policy Control Update information includes details, such as the user location information, UE time zone, and serving network.
11	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
12	The SMF processes the SM policy decision that is received as response and handles the response as PCF Initiation Modify procedure.

## CHF and PCF Integration for N26 4G to 5G Handover Call Flow

This section describes the call flow for the CHF and PCF Integration for N26 4G to 5G handovers.

Figure 26: CHF and PCF Integration for N26 4G to 5G Handover Call Flow

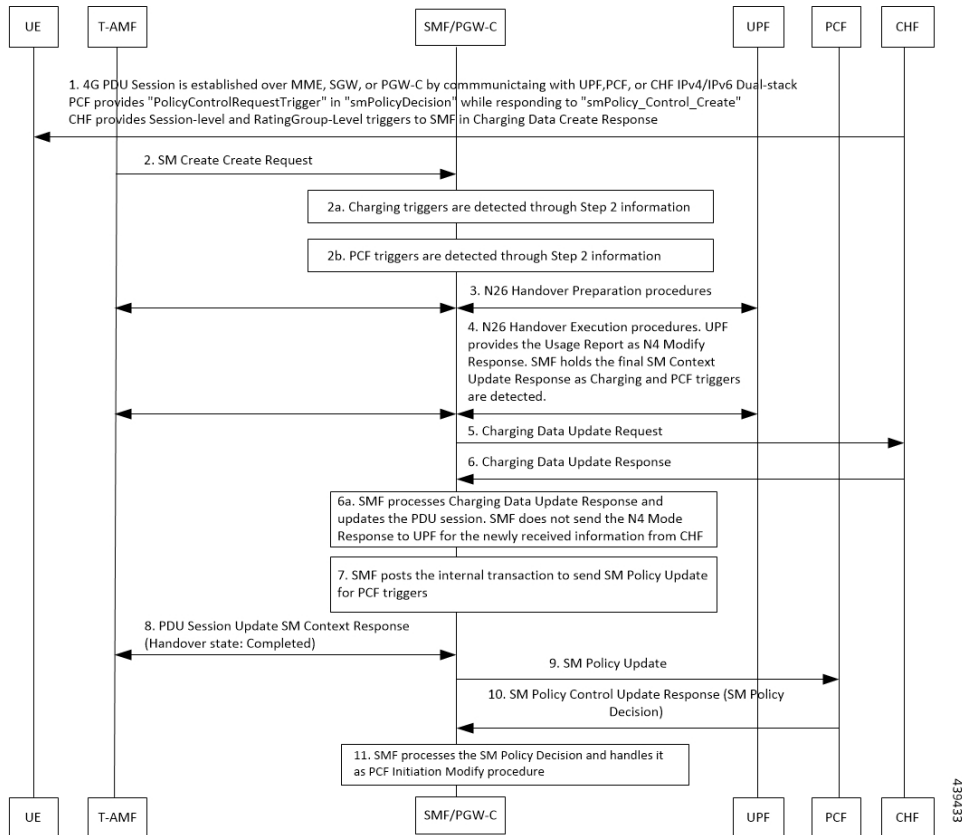


Table 43: CHF and PCF Integration for N26 4G to 5G Handover Call Flow Description

Step	Description
1	<p>The PDU session is established over MME, SGW, and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack.</p> <p>The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control.</p> <p>The CHF provides session-level and rating-group-level triggers to SMF as the Charging Data Create Response.</p>
2	The T-AMF sends SM Context Create Request to the SMF. This request includes information on handover state as preparing, UE location, UE time zone, serving NFID, serving network, and RAT type.
2a	The SMF detects access-side changes that are received in the SM Context Create Request and the charging triggers with the information that is available in Step 2.
2b	The SMF detects the PCF triggers with the information that is available in Step 2.
3	The N26-based Handover Preparation procedure starts from T-AMF toward the SMF or PGW-C and UHF and vice versa, as defined in 3GPP TS 23.502, section 4.1.9.3.



Step	Description
4	In the N26 Handover Execution procedure, the UPF sends the usage report as part of N4 modification response to SMF. The SMF holds the final SM Context Update Response when the SMF detects the CHF or PCF triggers.
5	The SMF sends the Charging Data Update Request to the CHF. This request includes the information on session-level triggers, multi-unit-Information (with rating-group-level triggers and usage report), customer identification, and PDU session charging information.
6	The CHF sends the Charging Data Update Response with optional multi-unit-information. The CHF also sends the new session or rating-group-level triggers to the SMF.
6a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 modification request to the UPF for the newly received information from the CHF.
7	The SMF posts the internal transaction to send the SM policy update information for PCF triggers.
8	The SMF sends the SM Context Update Response, for which the handover state is complete, to the AMF.
9	The SMF sends the SM Policy Control Update information to the PCF. The SM Policy Control Update includes details, such as the user location information, UE time zone, and serving network.
10	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
11	The SMF processes the SM policy decision that is received as response and handles the response as PCF Initiation Modify procedure, as defined in <i>3GPP TS 23.502, section 4.3.3.2</i> .

## CHF and PCF Integration for N26 5G to 4G Handover Call Flow

This section describes the call flow for the CHF and PCF Integration for N26 5G to 4G handovers.

Figure 27: CHF and PCF Integration for N26 5G to 4G Handover Call Flow

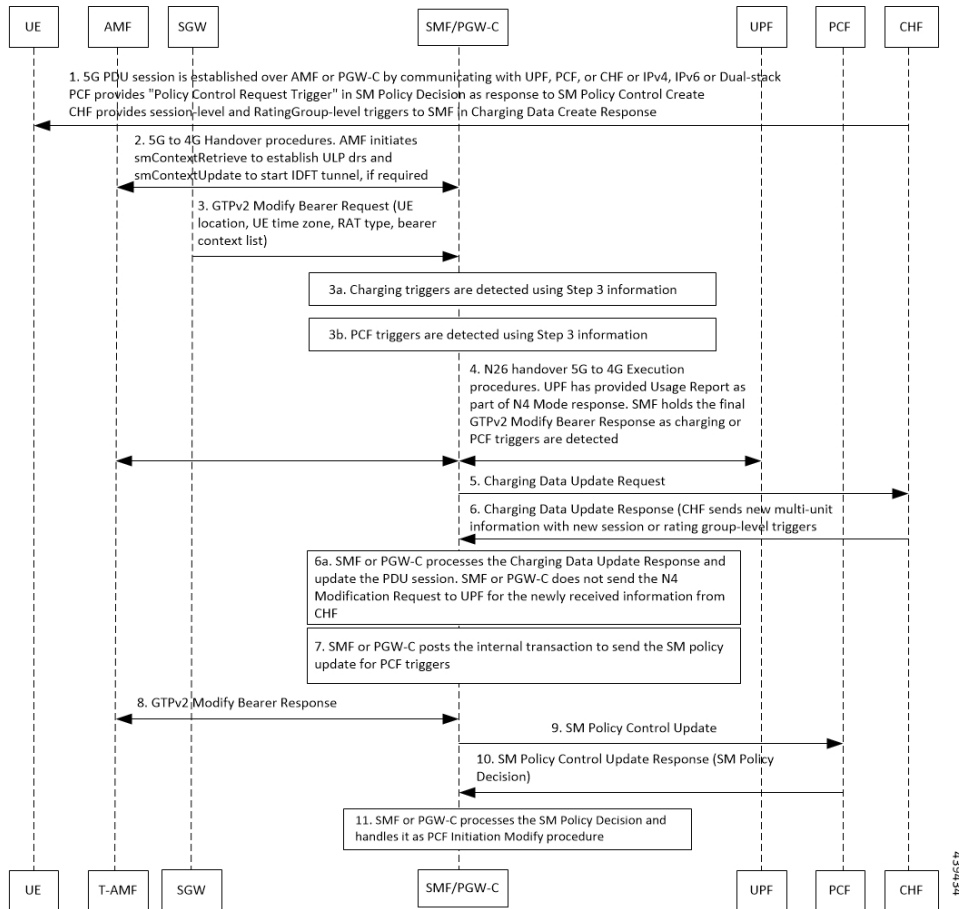


Table 44: CHF and PCF Integration for N26 5G to 4G Handover Call Flow Description

Step	Description
1	<p>The PDU session is established over S-AMF or SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack.</p> <p>The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control.</p> <p>The CHF provides session-level and rating-group-level triggers to SMF as the Charging Data Create Response.</p>
2	<p>The 5G to 4G Handover procedure starts from AMF toward the SMF or PGW-C and vice versa. AMF initiates the SM Context Retrieve Request to establish the UL PDRs and send SM Context Update Response to start the IDFT tunnel, if necessary.</p>
3	<p>In the N26 5G to 4G Handover Execution procedure, the SGW sends the GTPv2 Modify Bearer Request to PGW-C. This request includes the information on UE location, UE time zone, RAT type, and Bearer Context List.</p>
3a	<p>The SMF detects access-side changes that are received in the SM Context Update Request and the charging triggers with the information that is available in Step 3.</p>

Step	Description
3b	The SMF detects the PCF triggers with the information that is available in Step 3.
4	In the N26 Handover 5G to 4G Execution procedure, the PGW-C requests UPF to create a GTP-U tunnel for each flow. This tunnel is for the EBIs received in the Bearer Context List of GTPv2 Modify Bearer Request. After the DL PDRs are established, UPF sends the usage report as part of N4 modification response to SMF. The SMF holds the final GTPv2 Modify Bearer Response when the SMF detects the CHF or PCF triggers.
5	The SMF sends the Charging Data Update Request to the CHF. This request includes the information on session-level triggers, multi-unit-Information (with rating-group-level triggers and usage report), customer identification, and PDU session charging information.
6	The CHF sends the Charging Data Update Response with optional multi-unit-information. The CHF also sends the new session or rating-group-level triggers to the SMF.
6a	The SMF or PGW-C processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 modification request to the UPF for the newly received information from the CHF.
7	The SMF or PGW-C posts the internal transaction to send the SM policy update information for PCF triggers.
8	The SMF or PGW-C sends the SM Context Update Response, for which the handover state is complete, to the AMF.
9	The SMF or PGW-C sends the SM Policy Control Update information to the PCF. The SM Policy Control Update includes details, such as the user location information, UE time zone, and serving network.
10	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
11	The SMF processes the SM policy decision that is received as response and handles the response as PCF Initiation Modify procedure, as defined in <i>3GPP TS 23.502, section 4.3.3.2</i> .

## CHF and PCF Integration for Xn Handover Call Flow

This section describes the call flow for the CHF and PCF Integration for the Xn handover.

Figure 28: CHF and PCF Integration for Xn Handover Call Flow

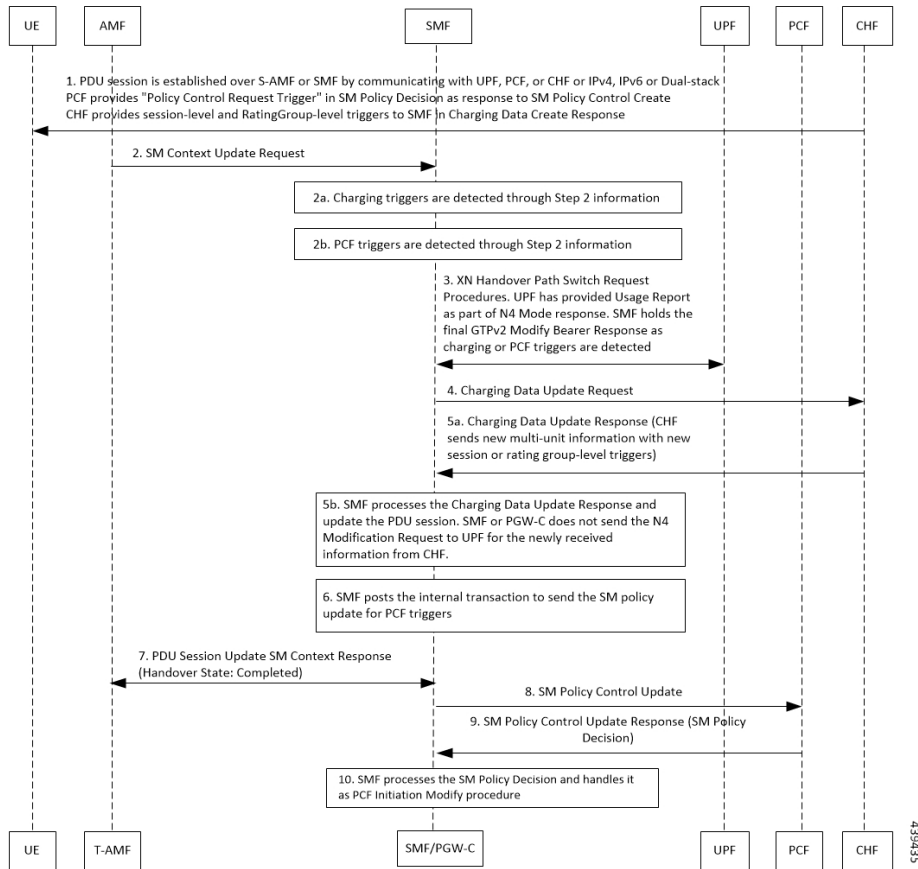


Table 45: CHF and PCF Integration for Xn Handover Call Flow Description

Step	Description
1	The PDU session is established over MME, SGW, and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack.  The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control.  The CHF provides session-level and rating-group-level triggers to SMF as the Charging Data Create Response.
2	The AMF sends SM Context Update Request to the SMF. The SM Context Update Request includes the information on UE location, UE time zone, and path switch request N2 message.
2a	The SMF detects access-side changes that are received in the SM Context Update Request and the charging triggers with the information that is available in Step 2.
2b	The SMF detects the PCF triggers with the information that is available in Step 2.

Step	Description
3	The Xn Handover Preparation procedure starts from SMF toward UPF and vice versa, as defined in <i>3GPP TS 23.502, section 4.9.1.2</i> .  SMF sends the N4 Modification Request to UPF and updates the received DL tunnel information of T-gNB. After the tunnel information is updated, UPF provides the usage report as part of N4 modification response. The SMF holds the final SM Context Update Response when the SMF detects the CHF or PCF triggers.
4	The SMF sends the Charging Data Update Request to the CHF. This request includes the information on session-level triggers, multi-unit-Information (with rating-group-level triggers and usage report), customer identification, and PDU session charging information.
5	The CHF sends the Charging Data Update Response with optional multi-unit-information. The CHF also sends the new session or rating-group-level triggers to the SMF.
5a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 modification request to the UPF for the newly received information from the CHF.
6	The SMF posts the internal transaction to send the SM policy update information for PCF triggers.
7	The SMF sends the SM Context Update Response to the AMF. This response includes the path switch request acknowledgment N2 message.
8	The SMF sends the SM Policy Control Update information to the PCF. The SM Policy Control Update includes details, such as the user location information and UE time zone.
9	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
10	The SMF processes the SM policy decision that is received as response and handles the response as PCF Initiation Modify procedure, as defined in <i>3GPP TS 23.502, section 4.3.3.2</i> .

## CHF and PCF Integration for Service Request Procedures

This section describes the CHF and PCF integration for service request procedures.

SMF processes the received SM Context Update Request to update N3 tunnel path state from Idle to Active or Active to Idle. SMF performs the following steps:

1. When UE is in CM-Idle state at AMF, which is Active to Idle mode—Based on the configuration, SMF updates UPF for N3 tunnel state to drop or buffer by sending the N4 session mode request. Based on charging configuration, SMF receives a usage report. Based on the Charging Triggers that qualify during session creation, SMF sends the N40 Charging Update request.
2. When UE is in CM-Connected state at AMF, which implies SMF receives UE-requested Procedures to change the subscriber N3 Tunnel Path from Idle to Active State—SMF receives the updated user location and UE time zone in the SM Context Update Request. SMF sends the N4 Session Modification Request to UPF to update the DL tunnel details of gNB. Based on charging configuration, SMF receives a usage report. Based on the Charging Triggers that qualify during session creation, SMF sends the N40 Charging Update request.
3. When the N3 Tunnel is unavailable for the Network Service Request Triggers, which implies that UE is in CM-Idle state at AMF—SMF initiates the Network Service Request Procedures for AMF to initiate

Paging toward the end user. Then, AMF begins the UE Service Request Procedures to configure the N3 Tunnel as specified in Step 2.

## Standards Compliance

The CHF and PCF integration for Intra-AMF and Inter-AMF N2-based handover feature complies with the *3GPP TS 23.502 V15.2.0 (2018-09)*.



## CHAPTER 15

# Content Filtering, Event Detail Records, and X-Header Enrichment Support

---

- [Feature Summary and Revision History, on page 169](#)
- [Feature Description, on page 170](#)
- [Content Filtering Support, on page 170](#)
- [Event Data Record Logging Support, on page 172](#)
- [Metadata Provided by SMF for EDR, on page 198](#)
- [X-Header Insertion Support, on page 198](#)
- [Supported X-Header Information, on page 198](#)
- [Bearer QCI Support, on page 199](#)

## Feature Summary and Revision History

### Summary Data

*Table 46: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

## Revision History

Table 47: Revision History

Revision Details	Release
Custom EDR Generation	2021.01.0
First introduced.	Pre-2020.02.0

## Feature Description

The SMF supports the following functionality:

- Content Filtering
- Event Detail Record (EDR)
- X-header Enrichment

## Converged Core Refactoring Changes

This section describes the changes related to converged core refactoring in this chapter.

The **edr-format** *edr\_format\_name* CLI command in the Active Charging Service configuration mode is deprecated in 2021.01 and later releases.

## Content Filtering Support

### Feature Description

The Content Filtering (CF) service prevents subscribers from inadvertently getting exposed to universally unacceptable content, or content that is inappropriate as per subscriber preferences. Based on the URLs in the subscriber requests, the CF service filters HTTP and WAP requests from mobile subscribers. Operators can filter and control the content for an individual subscriber to access.

The CF service provides the following solutions:

- URL Blacklisting—In this solution, all HTTP or WAP URLs in subscriber requests must match against a database of "blacklisted" URLs. If there is a match, it discards the flow, redirects, or terminates as per the configuration. In case of no match, subscribers view the content as usual.

URL Blacklisting may not be a subscriber opt-in service. Operators can enable URL Blacklisting either for all subscribers or for a subset of subscribers. Typical cases include applying a blacklisted database of child porn URLs to all subscribers so that they are inadvertently not exposed to the universally unacceptable content.



- Category-based Static Content Filtering—In this solution, all HTTP or WAP URLs in subscriber requests must match against a static URL categorization database. Action initiates based on the URL's category and as per the configuration in the subscriber CF policy. Possible actions include:
  - Permitting
  - Blocking
  - Redirecting
  - Inserting content

## Configuring Content Filtering

This section describes how to configure the following:

- Content Filtering

## Configuring Content Filtering Support

This section describes how to configure CF support.



### Note

Apart from the following configurations, all other configurations are used only in the UPF, and are only sent from the SMF to the UPF via RCM. The SMF does not use these configurations.

### Configuring Content Filtering under Active Charging Service

To configure CF support under the active charging service, use the following configuration:

```

configure
  active-charging service service_name
    content-filtering category policy-id cf_policy_id
      analyze priority priority { all | category category
        | x-category xcategory } action { allow |
        content-insert content_string | discard | redirect-url url |
        terminate-flow | www-reply-code-and-terminate-flow reply_code
      } [ edr edr_format] failure-action { allow |
        content-insert content_string | discard | redirect-url url
        | terminate-flow | www-reply-code-and-terminate-flow reply_code}
      [ edr edr_format]
    end
  
```

### Configuring Content Filtering under Rulebase

To configure CF under the rulebase, use the following configuration:

```

configure
  active-charging service service_name
    content-filtering category policy-id cf_policy_id
  
```

```
content-filtering mode category static-only
end
```

## Configuring Content Filtering under APN

To configure CF under the APN, use the following configuration:

```
configure
context context_name
  apn apn_name
    content-filtering category policy-id cf_policy_id
  end
```

## Content Filtering Policy ID on N7 Interface

The CF categories are configured under the active charging service under specific policy IDs. The rulebase and APN also have an associated policy ID. For any session, one policy ID can be associated with the session at anytime. The categories configured under that CF policy ID are applicable for the session on the UPF.

The PCF can override the CF policy ID by sending this value on the N7 interface. For this purpose, a proprietary IE is available in the YAML definition for the N7 interface. The hierarchy for the CF policy ID is as follows:

```
smPolicyDecision
  ciscoAvpSet:
    cfPolicyId: uint32 value
```

When the PCF does not send a CF policy ID, the existing CF policy ID in the rulebase configuration or the policy ID configured in the APN configuration is selected, in the order of precedence. This CF policy ID value is sent to the UPF in PFCP Session Establishment Request message in the "Subscriber Parameters" attribute. During PDU Session Modification, if the PCF changes the CF policy ID, the ID is sent to the UPF in PFCP Session Modification Request message.

# Event Data Record Logging Support

## Feature Description

Event Data Records (EDRs) collect information that you can use to charge subscribers for specific events that they consume. The EDRs catch whatever bytes get transmitted over the flow.

When a flow ends, the SMF generates EDRs with detail information of the terminated flow. The SMF supports logging of EDRs for both 4G and 5G subscriber sessions.

The SMF uses the event reports to generate EDR files comprised of logged information in comma-separated value (CSV) format. The SMF sends one CSV record per line. The CSV records are stored in a file and are optionally compressed before sending to an external server.

These CSV files can be downloaded and used offline to—

- Debug or understand the application behaviour.
- Diagnose the call flow for the specific subscribers.

The SMF supports EDR file generation for transaction and transaction-collision level details for subscriber sessions. By default, the EDR generation is disabled.

### EDR Format

In addition to the existing Transaction EDR fields, the application appends procedure-id and event-id along with their field values. Application registers the procedure-id, event-id, and field-id along with their corresponding names. This mapping is used to format the CSV event entry. Each event entry consists of comma-separated procedure-id, event-id, and field-value. These registered mappings can also be used in CLI commands to disable EDRs at procedure, event, or field level. You can enable or disable the EDRs dynamically during runtime. The existing EDR records remain the same and the runtime changes get reflected only in the newly generated EDR records.

### Transaction EDR Format

Transaction-EDR-Fields, list of Event-Entries []

### Event Entries

Procedure-id1, Event-id1, list of field-id1-values[]

The following is a sample transaction entry along with a list of events in the CSV format.

```
Transaction-id-value, Start-Time, Elapsed-Time, .....,
Procedure-id1, event-id1, field-id1-value, field-id2-value.....,
Procedure-id1, event-id2, field-id1-value, field-id2-value.....,
    Procedure-id1, event-id1, field-id1-value, field-id2-value.....
```



**Note** There might be different set of fields for a combination of procedure-id and event-id. You can enable or disable the EDRs dynamically during runtime by using a CLI command. For configuration details, see the [Configure EDR Files for Generation, on page 195](#) section in this guide.

The CSV file is generated in each SMF service pod where the subscriber sessions and events are processed. The location of the EDR files inside pod is as follows:

```
/tmp/edr/smf-service/<pod-instance>/transactions.csv
/tmp/edr/smf-service/<pod-instance>/transaction_collisions.csv
```

### Example:

```
/tmp/edr/smf-service/1/transactions.csv
/tmp/edr/smf-service/1/transaction_collisions.csv
```

## EDR Transaction File

The EDR transaction file dumps the transaction information at the end of the transaction. By default, the file generation is disabled.

The following table provides the information that is stored in the file.

**Table 48: EDR Transaction File Fields**

Field Number	Field Name	Field Description
1	Transaction ID	Transaction ID

Field Number	Field Name	Field Description
2	Start Time	The transaction start time in yyyy/MM/dd HH:mm:ss.SSS format.
3	Elapsed Ms	The time taken for transaction to end in milliseconds.
4	Subscriber ID	The subscriber ID. For example, imsi-123456789012345
5	Transaction Type	The transaction type (integer) which is defined internally in the application.
6	Transaction Description	The transaction description in string format.
7	Session Primary Key	The primary key of the session.
8	Session Unique Keys	The unique keys for the session separated by  .
9	Session Non Unique Keys	The non-unique keys for the session separated by  .
10	Status	The transaction status (success or error).
11	Status Code	The transaction status code to indicate the failure reason.
12	Procedure Name	The procedure name for which the transaction was submitted.
13	Sub Procedure Name	The sub procedure name for which the transaction was submitted.

Field Number	Field Name	Field Description
14	State	The transaction state. It can be: <ul style="list-style-type: none"> <li>• Started</li> <li>• New</li> <li>• Ready</li> <li>• Active</li> <li>• Pending</li> <li>• Suspend</li> <li>• SuspendWaitingForResponse</li> <li>• SuspendWaitingForLock</li> <li>• Abort</li> <li>• Finished</li> <li>• Timeout</li> <li>• Unknown</li> </ul>
15	Execution stages	The list of stages the transaction went through its lifecycle separated by

**NOTES:**

- Each field is separated by comma (,).
- Fields session\_uks, session\_nuks, execution\_stages are a list. These fields are separated by pipe (|). For example, session\_uks can be denoted as uk1|uk2|uk3.

**CSV Format Examples:**

```
1,2020/10/06 16:56:09.276,161,imsi-123456789012345,7,N11SmContextCreateReq,
imsi-123456789012345:5,,supi:imsi-123456789012345|gpsi:msisdn-9999988888|pei:
imei-123456786666660|udm:10.1.5.52|dnn:intershat|rat:nr|access:3gpp access|
connectivity:5g|policy:1,success,success,PDU Session Establishment,N11SmContextCreateReq,
Active,init_done|SETUP: Idle|SETUP: Await UDM Registration|SETUP: Await UDM Subscription
Fetch|
SETUP: Await UDM Subscribe for Notification|finished

2,2020/10/06 16:56:09.432,659,imsi-123456789012345,106,NIntSelfTxnPduSetup,
imsi-123456789012345:5,33554442,supi:imsi-123456789012345|gpsi:msisdn-9999988888|pei:
imei-123456786666660|udm:10.1.5.52|dnn:intershat|rat:nr|access:3gpp access|connectivity:
5g|pcfGroupId:PCF-dnn=intershat;|pcf:10.1.5.52|policy:2|upf:10.1.5.52|upfEpKey:10.1.5.52:
10.1.5.54|ipv4-addr:poolv4/12.0.0.1|ipv4-pool:poolv4|ipv4-range:poolv4/12.0.0.1|ipv4-startrange:
poolv4/12.0.0.1|amf:10.1.5.52,success,success,unknown,unknown,Active,init_done|SETUP:
Await PCF Internal|SETUP: Await PCF Create|SETUP: Await Address Allocation|SETUP:
Await PCF Update|SETUP: Await Charging Create|SETUP: Await UPF Setup|SETUP:
Await Assign Ebi Response|SETUP: Await N1 N2|finished

3,2020/10/06 16:56:10.151,167,imsi-123456789012345,10,N11SmContextUpdateReq,
imsi-123456789012345:5,33554442,supi:imsi-123456789012345|gpsi:msisdn-9999988888|pei:
imei-123456786666660|udm:10.1.5.52|dnn:intershat|rat:nr|access:3gpp access|connectivity:
5g|pcfGroupId:PCF-dnn=intershat;|pcf:10.1.5.52|policy:2|upf:10.1.5.52|
```

```

upfEpKey:10.1.5.52:10.1.5.54|ipv4-addr:poolv4/12.0.0.1|ipv4-pool:poolv4|
ipv4-range:poolv4/12.0.0.1|ipv4-startrange:poolv4/12.0.0.1|amf:10.1.5.52,success,success,
PDU Session Establishment,N11SmContextUpdateReq,Active,init_done|SETUP: Await AMF Update|
SETUP: Await UPF Modify|finished

4,2020/10/06 16:56:12.404,159,imsi-123456789012345,24,N11SmContextReleaseReq,
imsi-123456789012345:5,33554442,supi:imsi-123456789012345|gpsi:msisdn-9999988888|pei:
imei-123456786666660|udm:10.1.5.52|dnn:intershat|rat:nr|access:3gpp access|connectivity:
5g|pcfGroupId:PCF-dnn=intershat;|pcf:10.1.5.52|policy:2|upf:10.1.5.52|upfEpKey:10.1.5.52:
10.1.5.54|amf:10.1.5.52,success,success,unknown,unknown,Active,init_done|RELEASE: Idle|
RELEASE: Await UPF Release|RELEASE: Await Resource Release|finished

5,2020/10/06 16:56:12.563,158,imsi-123456789012345,123,NIntPduReleaseComplete,
imsi-123456789012345:5,,,success,success,PDU Session Release - AMF initiated,
NIntPduReleaseComplete,Active,init_done|RELEASE: Await Internal Charging Terminate|
RELEASE: Await Charging Terminate|RELEASE: Await PCF Delete|finished|finished

```

## Procedure-level EDR Generation

The Event Logging feature captures procedure-level information per subscriber. Upon completing a procedure, either successfully or unsuccessfully, the SMF generates a procedure summary or event report logging the event.

The EDR generation per procedure is configurable. For configuration details, see the [Configure EDR Files for Generation, on page 195](#) section in this guide.

The following table lists the supported procedures and the corresponding IDs.

**Table 49: Procedure List**

Procedure	Procedure-ID
PDN-SESSION-CREATE or PDU-SESSION-CREATE	3
PDN-SESSION-DELETE or PDU-SESSION-DELETE	4

Further, the SMF captures event-level information per procedure. The following table provides details on the subscriber events and the respective event IDs.

The events captured per procedure are configurable. For configuration details, see the [Configure EDR Files for Generation, on page 195](#) section in this guide.

**Table 50: Event ID**

EVENT	EVENT-ID
N11SmContextCreateReq	1287
N11SmContextUpdateReq	1290
N11N1N2MessageTransferReq	1299
N11SmContextUpdateModifyReq	1293
N11EbiAssignmentReq	1302
N11SmContextReleaseReq	1304
N11SmContextStatusNotifyReq	1310
N11N1N2MessageTransferFailNotificationReq	1339
N4SessionModificationReq	527

EVENT	EVENT-ID
N4SessionReleaseReq	530
N4SessionEstablishmentReq	524
N7SmPolicyCreateReq	3329
N7SmPolicyDeleteReq	3335
N7SmPolicyUpdateReq	3332
N7SmPolicyTerminateNotifyReq	3341
N10UnsubscribeForNotificationReq	1432
N10SubscribeForNotificationReq	1319
N10RegistrationRequest	1313
N10SubscriptionFetchReq	1316
N10DeregistrationRequest	1325
N10UnsubscribeForNotificationReq	1432
N10UpdateNotifyReq	1322
N40ChargingDataReq	3585
N40ChargingDataReq	3585
N40ChargingNotificationReq	3588
SecondaryAuthenReq	2307
S5S8CreateSessReq	2051
S5S8DeleteBearerReq	2057
S5S8DeleteSessReq	2055
metadata	1000

The following tables list the detailed event record for the PDU Session Create and Delete procedures.

**Table 51: PDU Session Create Procedure**

Attributes	Event ID	Field Name	Presence	Type	Description
TXN EDR fields			M		
PROCEDURE ID	EVENT-ID	VERSION	M	String	N11SmContext CreateReq
		SUPI	M	String	
		IMEI/PEI	M	String	
		IMSI	M	String	
		MSISDN	M	String	
		GPSI	M	String	

Attributes	Event ID	Field Name	Presence	Type	Description
		STATUS	M	String	
		STATUS-CODE	O	Number	
		PDU(PDN)- SESSION-TYPE	O	Number	
		SSC-MODE	O	Number	
		CAUSE	O	String	
		PCO	O	PCO	
		N1MSGREQ TYPE	O	N1N2MSGREQ CONTENT	PDU-SESSION -ESTB-REQUEST
		N2MSGREQ TYPE	O	N1N2MSGREQ CONTENT	
		N1MSGRESP TYPE	O	N1N2MSGRSP CONTENT	PDU-SESSION- ESTB-REJECT
		N2MSGRESP TYPE	O	N1N2MSGRSP CONTENT	
		MAX-SUPP- FILTERS	O	Number	
		ALWAYS-ON	O	Boolean	
		BACKOFF-TIME	O	NA	NA
		RAT-TYPE	M	String	
PROCEDURE ID	EVENT-ID2	VERSION	M	String	N11SmContext UpdateReq
		STATUS	M	String	
		STATUS-CODE	O	Number	
		PCO	O	PCO	
		N1MSGREQ TYPE	O	N1N2MSGREQ CONTENT	
		N2MSGREQ TYPE	O	N1N2MSGREQ CONTENT	
		N1MSGRESP TYPE	O	N1N2MSGRSP CONTENT	
		N2MSGRESP TYPE	O	N1N2MSGRSP CONTENT	
		CAUSE	O		
		BACKOFF-TIME	O	NA	NA



Attributes	Event ID	Field Name	Presence	Type	Description		
PROCEDURE ID	EVENT-ID3	VERSION	M	String	N11N1N2Message TransferReq		
		STATUS	M	String			
		STATUS-CODE	O	Number			
		N1MSGREQ TYPE	O	N1N2MSGREQ CONTENT	PDU-SESSION -ESTB-ACCEPT, PDU-SESSION -ESTB-REJECT, and so on		
		N2MSGREQ TYPE	O	N1N2MSGREQ CONTENT			
		N1MSGRESP TYPE	O	N1N2MSGRESP CONTENT			
		N2MSGRESP TYPE	O	N1N2MSGRESP CONTENT			
		PCO	O	PCO			
		PDU-SESSION- TYPE	O	Number			
		SSC-MODE	O	Number			
		DNN	O	String			
		QOS-RULE	O	QOS-RULE			
		QOS-DESC	O	QOS-DESC			
		SESSION-AMBR	O	SESS-AMBR			
		CAUSE	O	String			
		PAA	O	PAA			
		S-NSSAI	O	NSSAI			
		ALWAYS-ON	O	Boolean			
		PROCEDURE ID	EVENT-ID	VERSION	M	String	N7SmPolicy CreateReq
				SUPI	M	String	
IMEI/PEI	M			String			
GPSI	M			String			
STATUS	M			String			
STATUS-CODE	O			Number			

Attributes	Event ID	Field Name	Presence	Type	Description
		PDU(PDN)-SESSION-TYPE	O	Number	
		QOS-DESC	O	QOS-DESC	
		SESSION-AMBR	O	SESS-AMBR	
		CAUSE	O	String	
PROCEDURE-ID=3	EVENT-ID=<event_id>	VERSION	M	String	EVENT= N4Session ModificationReq, N10Deregistration Request N7SmPolicy UpdateReq, N10Subscription FetchReq, N10Unsubscribe ForNotification Req, SecondaryAuthen Req, N10SubscribeFor NotificationReq N40Charging DataReq, N7SmPolicy DeleteReq, N11Ebi AssignmentReq, N4Session EstablishmentReq, N4Session ReleaseReq, N10Registration Request
		STATUS	M	String	
		STATUS-CODE	O	Number	
		PDU-SESSION-TYPE	M	Number	
		CAUSE	O	String	

Attributes	Event ID	Field Name	Presence	Type	Description
PROCEDURE ID	EVENT-ID	VERSION	M	String	S5S8Create SessReq
		SUPI	M	String	
		IMEI/PEI	M	String	
		IMSI	M	String	
		MSISDN	M	String	
		GPSI	M	String	
		STATUS	M	String	
		STATUS-CODE	O	Number	
		PCO	O	PCO	
		PDU-SESSION-TYPE	O	Number	
		SSC-MODE	O	Number	
		DNN/APN	O	String	
		QOS-RULE	O	QOS-RULE	
		QOS-DESC	O	QOS-DESC	
		SESSION-AMBR	O	SESS-AMBR	
		CAUSE	O	String	
		PAA	O	PAA	
		S-NSSAI	O	NSSAI	
		RAT-TYPE	M	String	
	EVENT-ID1=1000	VERSION	M	Number	META DATA
		SUPI	M		
		IMEI/PEI	M		
		IMSI	M		
		MSISDN	M		
		GPSI			
		SERVING-PLMN	M		
		UE-LOCATION	M	UE-LOCATION	
		START-TIME	M	String	
		END-TIME	M	String	
		TRIGGER-NF	M		

Attributes	Event ID	Field Name	Presence	Type	Description
		TRIGGER-EVENT	M		
		USERPLANE-STATUS	M		
		CAUSE	M		
		SGW-ID	O		
		DISCONNECT-REASON	O		
		STATUS	M		
		STATUS-CODE	O		
		DNN	M		
		RAT-TYPE	M		
		UE-TIMEZONE	M		
		PDU-SESSION-TYPE	M		
		UE-PLMN	M		
		SUBSCRIBED-SESS-AMBR-UPLINK	M		
		SUBSCRIBED-SESS-AMBR-DOWNLINK	M		
		SUBSCRIBED-5QI	M		
		SUBSCRIBED-ARP	M		
		PAA	M		
		LOCAL-SEID	M		
		REMOTE-SEID	M		
		ROAMING-STATUS	M		
		CONNECTION-TIME	M	NA	NA
		PDU-SESSION-ID	O		
		ALWAYS-ON	O		
		EPS-IWK	O		

Attributes	Event ID	Field Name	Presence	Type	Description
		S-NSSAI	O		
		MAX-SUPP-FILTERS	O		
		SSC-MODE	O		
		UE-TYPE	O		
		LOCAL-CFTEID-TEID	O		
		LOCAL-CFTEID-IP	O		
		REMOTE-CFTEID-TEID	O		
		REMOTE-CFTEID-IP	O		
		VIRTUAL-DNN/APN	O		

For details on the listed attributes, see the table in the [EDR Transaction File](#), on page 173 section.

**Table 52: PDN Delete Event**

Attributes	Event ID	Name	Presence	Description
TXN EDR fields			M	

Attributes	Event ID	Name	Presence	Description
PROCEDURE-ID=3	EVENT-ID= <event_id>	VERSION	M	EVENT= N11SmContext ReleaseReq, N40Charging DataReq, N7SmPolicy DeleteReq, N10UnsubscribeFor NotificationReq, N10Deregistration Request, N7SmPolicy TerminateNotifyReq, N40Charging NotificationReq, RadiusCoa DisconnectReq, N7SmPolicy TerminateNotifyReq, N40Charging NotificationReq, N10Update NotifyReq, N11SmContext StatusNotifyReq, N11N1N2Message TransferFail NotificationReq
		STATUS	M	
		STATUS-CODE	M	
		CAUSE	O	
	EVENT-ID= <event_id>	VERSION	M	N1N2Message TransferReq, N11SmContext UpdateReq
		STATUS	M	
		STATUS-CODE	O	

Attributes	Event ID	Name	Presence	Description
		N1MSGREQTYPE	O	PduSessionReleaseCommand, PduSessionReleaseRequest, PduSessionReleaseComplete
		N2MSGREQTYPE	O	PduSessionResourceReleaseCommand
		N1MSGRESPTYPE	O	PduSessionReleaseReject
		N2MSGRESPTYPE	O	
		BACKOFF-TIME	O	NA
		PCO	O	
		CAUSE	O	
	EVENT-ID1=1000	VERSION	M	META-DATA
		SUPI	M	
		IMSI	M	
		IMEI	M	
		MSISDN	M	
		GPSI		
		SERVING-PLMN	M	
		UE-LOCATION	M	
		START-TIME	M	
		END-TIME	M	
		TRIGGER-NF	M	
		TRIGGER-EVENT	M	
		USERPLANE-STATUS	M	
		CAUSE	M	
		SGW-ID	O	
		DISCONNECT-REASON	O	
		STATUS	M	
		UPDATE-TIME	M	NA

**NOTES:**

- Userplane-status is of type number. The number can be one of the following:
  - UpStateNone = 0
  - UpStateEstablishing = 1 // UPF Session is being established or setup
  - UpStateActivating = 2 // UPF Session is being modified to Activate Access Tunnel
  - UpStateActivated = 3 // UPF Session Active for Access & Core Tunnel
  - UpStateDeactivating = 4 // UPF Session is being modified to Deactivate Access Tunnel
  - UpStateDeactivated = 5 // UPF Session Deactivated for Access, valid Core Tunnel Only
  - UpStateModifying = 6 // UPF Session is being modified for QoS/flow parameters
  - UpStateDeleting = 7 // UPF Session is being Released
  - UpStateDeleted = 8 // UPF Session is Released
- PduSessionType is of type number. The number can be one of the following:
  - UnknownSessionType = 0
  - Ipv4PduSession = 1
  - Ipv6PduSession = 2
  - Ipv4V6PduSession = 3
  - Unstructured = 4
  - Ethernet = 5
  - FutureUsePduSessionType = 7
- SSC mode is of type number. The number can be one of the following:
  - UnknownSscMode = 0
  - SscMode1 = 1
  - SscMode2 = 2
  - SscMode3 = 3
  - DupSscMode1 = 4
  - DupSscMode2 = 5
  - DupSscMode3 = 6
  - FutureUseSscMode = 7
- Eps Iwk (Type: Number)
  - EpsInterworkingIndication\_DummyEnum = 0
  - EpsInterworkingIndication\_NONE = 1



- EpsInterworkingIndication\_WITH\_N26 = 2
- EpsInterworkingIndication\_WITHOUT\_N26 = 3
- Roaming status (Type: Number)
  - ROAMING\_STATUS\_NONE = 0
  - ROAMING\_STATUS\_HOMER = 1 //HOMER
  - ROAMING\_STATUS\_VISITOR\_LBO = 2 //LBO
  - ROAMING\_STATUS\_VISITOR\_HR = 3 //IN-HR
  - ROAMING\_STATUS\_ROMER = 4 //OUT-HR
- PreemptionCapability (type: Number)

**5G:**

- 0: "PreemptionCapability\_DummyEnum",
- 1: "NOT\_PREEMPT",
- 2: "MAY\_PREEMPT",

**Others:**

- 0: Disabled
- 1: Enabled

- PreemptionVulnerability (type: Number)

**5G:**

- 0: "PreemptionVulnerability\_DummyEnum",
- 1: "NOT\_PREEMPTABLE",
- 2: "PREEMPTABLE",

- Disconnect-Reason (type: String)

Disconnect-Reason contains a self-explanatory string. If it holds a number, then the string interpretation is as follows:

- PduRelReason\_Error = 1
- PduRelReason\_SessIdleTimeout = 2
- PduRelReason\_SessCpIdleTimeout = 3
- PduRelReason\_SessAbsoluteTimeout = 4

**Procedure EDR Example:**

```
1,2021/03/18 13:43:40.892,1448,imsi-123456789012345,1287,N11SmContextCreateReq,
.
```

```
.
3,1313,V1,Success,201,1,,3,1316,V1,Success,200,1,,3,1319,V1,Success,201,1,,3,1287,V1,
imsi-123456789012345,imei-123456786666660,123456789012345,9999988888,msisdn-9999988888,
Success,,1,0,,193|,,,,,NR,3,3329,V1,imsi-123456789012345,imei-123456786666660,msisdn-9999988888,
Success,201,1,3|1;2;7|3000 mbps|4000 mbps|1000 mbps|2000 mbps,20 kbps|20
kbps,,3,3332,V1,Success,
204,1,,3,3585,V1,Success,201,1,,3,524,V1,Success,,1,Request_Accepted,3,1299,V1,Success,200,194|,
77|,,,,1,1,intershat,2|1|0|2|128|1|filters:0;3;1;;|3|1|0|2|192|1|filters:0;3;1;;|1|1|1|1|255|1|
filters:0;3;1;;,5|0 kbps|0 kbps|0 kbps|0 kbps|3|6000 mbps|8000 mbps|2000 mbps|4000 mbps,20
kbps|
20 kbps,N1_N2_TRANSFER_INITIATED,12.0.4.0|,2|Abf123||,0
```

In the preceding example, the initial entries represent the transaction EDRs and last part provided here represents the procedure-level EDRs.

## EDR Transaction Collision

This EDR file dumps the transaction collision information whenever the collision occurs. It is useful to debug collision scenarios.

**Table 53: EDR Transaction Collision File Fields**

Field No.	Field Name	Field Description
1	Subscriber ID	The subscriber ID. For example, imsi-123456789012345
2	Collision Time	Collision time in yyyy/MM/dd HH:mm:ss.SSS format.
3	Force Resolution	Indicates whether the resolution is forced (true/false).
4	Collision Cause	The cause of collision.
5	New Transactions Before Collision	Transactions in the new state before collision handling separated by  .
6	Pending Transactions Before Collision	Transactions in the pending state before collision handling separated by  .
7	Active Transactions Before Collision	Transactions in the active state before collision handling separated by  .
8	New Transactions After Collision	Transactions in the new state after collision handling separated by  .
9	Pending Transactions After Collision	Transactions in the pending state after collision handling separated by  .
10	Active Transactions After Collision	Transactions in the active state after collision handling separated by  .
11	Suspended Transactions After Collision	Transactions in the suspended state after collision handling separated by  .

Field No.	Field Name	Field Description
12	Aborted Transactions After Collision	Transactions in the aborted state after collision handling separated by  .

**CSV Format Examples:**

```

supi:imsi-123456789012345,2020/10/06 16:15:11.801,true,SessionLockSamePriority,17,,,,,|17,,
supi:imsi-123456789012345,2020/10/06 16:15:11.824,true,SessionLockSamePriority,18,,,,,|18,,
supi:imsi-123456789012345,2020/10/06 16:15:11.857,true,SessionLockSamePriority,19,,,,,|19,,
supi:imsi-123456789012345,2020/10/06 16:15:11.883,true,SessionLockSamePriority,20,,,,,|20,,
supi:imsi-123456789012345,2020/10/06 16:15:11.888,true,SessionLockRelease,,,,,,,,,x

```

## EDR Attributes

This section provides details of the EDR attributes and its sub attributes.

**Table 54: QOS-RULE**

QOS-RULE-LIST	qr-id qr-opcode qr-dqr qr-qfi qr-precedence num-filters filters:flter-id;flter-dir;fltr-cmp-type;ip;port			
	Field	Sub field	Sub-sub field	Presence
	QOS-RULE			
		QOS-RULE-ID		M
		QOS-RULE-OPCODE		M
		QOS-RULE-DQR		M
		QOS-RULE-QFI		M
		QOS-RULE-PRECEDENCE		M
		NO-PKT-FILTERS		
		PKT-FILTER-LIST		M
			PKT-FILTER-ID	M
			PKT-FILTER-DIRECTION	M
			PKT-FILTER-CMP-TYPE	M
			PKT-FILTER-IP-ADDRESS	O
			PKT-FILTER-PORT	O



**Note** Delimiters subject to change based on the position of QOS-RULE in the attribute.

Table 55: QOS-DESC

<b>QOS-DESC</b>	[5qi preEmpCap;preEmpVul;Prior  mbr-ul mbr-dl gbr-ul gbr-dl]	
<b>Sub field</b>	<b>Type</b>	<b>Presence</b>
5QI		M
ARP	ARP	M
MBR-UPLINK		O
MBR-DOWNLINK		O
GBR-UPLINK		O
GBR-DOWNLINK		O



**Note** Delimiters subject to change based on the position of QOS-DESC in the attribute.

Table 56: PCO

<b>PCO</b>	[TYPE PCSCF-ADDR-LIST DNS-ADDR-LIST  PDU-SESSION-ID  QOS-RULE-LIST SESSION-AMBR  QOS-DESC S-NSSAI  MS-SUPPORT-NW_ADDR-TFT  NW-SUPPORT-NW_ADDR-TFT  PCSCF-ADDR-REQ DNS-ADDR-REQ MTU-REQ  MTU-SIZE]		
<b>Sub field</b>	<b>Type</b>	<b>Presence</b>	
TYPE	String	M	EPCO or PCO or APCO
PCSCF-ADDR-LIST	PCSCF-ADDR	O	CSR Response sent from SMF
DNS-ADDR-LIST	DNS-ADDR	O	CSR Response sent from SMF
PDU-SESSION-ID		O	CSR Response sent from SMF
QOS-RULE-LIST	QOS-RULE	O	CSR Response sent from SMF
SESSION-AMBR	SESS-AMBR	O	CSR Response sent from SMF
QOS-DESC	QOS-DESC	O	CSR Response sent from SMF
S-NSSAI	NSSAI	O	CSR Response sent from SMF
MS-SUPPORT-NW_ADDR-TFT	Boolean	O	CSR Response sent from SMF
NW-SUPPORT-NW_ADDR-TFT	Boolean	O	CSR Response sent from SMF

PCSCF-ADDR-REQ	PCSCF-ADDR-REQ	O	CSR Response sent from SMF
DNS-ADDR-REQ	DNS-ADDR-REQ	O	CSR Response sent from SMF
IPV4-MTU-REQUEST	Boolean	O	CSR Response sent from SMF
IPV4-MTU-SIZE	String	O	CSR Response sent from SMF



**Note** In the preceding table, CSR Request and CSR Response messages refer to 4G and Wi-Fi call flows. N11 SM Context Create Request and Response messages refer to 5G call flows.

**Table 57: PCSCF-ADDR-REQ**

<b>PCSCF-ADDR-REQ</b>	[PCO-PCSF-ADDR-IPV4-REQ; PCO-PCSF-ADDR-IPV6-REQ]	
<b>Sub field</b>	<b>Presence</b>	<b>Type</b>
PCO-PCSF-ADDR-IPV4-REQ	M	Boolean
PCO-PCSF-ADDR-IPV6-REQ	M	Boolean

**Table 58: PCSCF-ADDR**

<b>PCSCF-ADDR</b>	[ipv4-Primary; ipv4-secondary; ipv4-tertiary; ipv6-Primary; ipv6-secondary; ipv6-tertiary]	
<b>Sub field</b>	<b>Presence</b>	<b>Type</b>
PCSF-ADDR-IPV4-LIST	O	List
PCSF-ADDR-IPV6-LIST	O	List

**Table 59: DNS-ADDR**

<b>DNS-ADDR</b>	[ipv4-Primary; ipv4-secondary; ipv4-tertiary; ipv6-Primary; ipv6-secondary; ipv6-tertiary]	
<b>Sub field</b>	<b>Presence</b>	<b>Type</b>
DNS-ADDR-IPV4-LIST	O	List
DNS-ADDR-IPV6-LIST	O	List

**Table 60: DNS-ADDR-REQ**

<b>DNS-ADDR-REQ</b>	[PCO-PCSF-ADDR-IPV4-REQ; PCO-PCSF-ADDR-IPV6-REQ]	
<b>Sub field</b>	<b>Presence</b>	<b>Type</b>
PCO-PCSF-ADDR-IPV4-REQ	M	Boolean

PCO-PCSF-ADDR-IPV6-REQ	M	Boolean
------------------------	---	---------

**Table 61: NSSAI**

<b>NSSAI</b>	[sst sd hplmnsst hplmnsd]	
<b>Sub field</b>	<b>Presence</b>	<b>Type</b>
SST	M	Number
SD	O	String
HPLMN-SST	O	Number
HPLMN-SD	O	String



**Note** Delimiters subject to change based on the position of S-NSSAI in the attribute.

**Table 62: PAA**

<b>PAA</b>	[ipv4-addr ipv6-addr]	
<b>Sub field</b>	<b>Presence</b>	<b>Type</b>
ADDR-IPV4	O	String
ADDR-IPV6	O	String

**Table 63: N1N2MSGREQCONTENT**

N1-Msg-Req-Content	[msg-type cause]	
<b>Sub field</b>	<b>Presence</b>	<b>Type</b>
MSG-TYPE	M	SMF N1N2MsgType
Cause	O	String

**Table 64: PLMN-ID**

<b>PLMN-ID</b>	mcc mnc	
<b>Sub field</b>	<b>Presence</b>	
MCC	M	
MNC	M	



**Note** Delimiters subject to change based on the position of PLMN-ID in the parent attribute.

Table 65: GUAMI

<b>GUAMI</b>	amf-id plmn-id
<b>Sub field</b>	<b>Presence</b>
AMF-ID	M
PLMN-ID	M

Table 66: SESS-AMBR

<b>SESS-AMBR</b>	[ambr-dl  ambr-ul]	
<b>Sub field</b>	<b>Presence</b>	<b>Type</b>
mbr-dl	O	Number
ambr-ul	O	Number

Table 67: UE-LOCATION

<b>UE-LOCATION</b>	[locationType  <b>Ecgi</b> : ECGI  <b>Tai</b> :TAI] or [locationType  <b>Ncgi</b> : NCGI  <b>Tai</b> :TAI]		
<b>Sub field</b>	<b>Presence</b>	<b>Type</b>	
locationType	M	String	“Eutra” or “NR”
ECGI or NCGI	O	ECGI/NCGI	
Tai	O	TAI	

Table 68: ECGI or NCGI

<b>ECGI /NCGI</b>	[plmn-id;cellId]	
<b>Sub field</b>	<b>Presence</b>	<b>Type</b>
Plmn-id	M	PLMN-ID
Cell-id	M	String

Table 69: TAI

<b>TAI</b>	[plmn-id;tac]	
<b>Sub field</b>	<b>Presence</b>	<b>Type</b>
Plmn-id	M	PLMN-ID
tac	M	String

The SMF generates detailed records with field-level details per event. The following table lists the different N1 N2 messages and the associated IDs.

Table 70: N1 N2 Message Types

Message	Message ID
PDU-SESSION-ESTB-REQUEST	193
PDU-SESSION-ESTB-ACCEPT	194
PDU-SESSION-ESTB-REJECT	195
PDU-SESSION-MOD-REQ	201
PDU-SESSION-MOD-CMD	203
PDU-SESSION-MOD-CMD-REJ	202
PDU-SESSION-MOD-CMD-COMP	204
PDU-SESSION-REL-REQ	209
PDU-SESSION-REL-CMD	211
PDU-SESSION-REL-REJ	210
PDU-SESSION-REL-COMP	212
N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND	85
N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE	130
N2_PDU_SESSION_RESOURCE_SETUP_REQUEST	77
SM-CONTEXT-CREATE	2500
SM-CONTEXT-CREATE-RESP	2501
SM-CONTEXT-UPDATE	2502
SM-CONTEXT-UPDATE-RESP	2503
PDU-RES-SETUP-REQ	3000

## Limitations

The EDR Logging feature has the following limitations:

- Event record generation does not work for the following procedures:
  - PDU Session Modify
  - Handover
  - Idle-Active transition
  - Active-Idle transition
- The SMF supports only IMSI (SUPI)-based EDR reporting.
- The SMF currently supports EDR generation in CSV format. The EDR file storage format is not configurable.
- This feature is not applicable to a procedure that does not send a response explicitly to an incoming request.



## Configuring EDRs

This section describes how to configure the EDR Logging feature.

### Enable EDR Reporting



**Note** Currently, the EDR file generation works for only specific subscribers. EDR generation occurs after configuring the subscriber ID.

Use the following sample configuration to enable or disable the EDR generation for particular subscribers.

```
config
  edr reporting enable
  edr subscribers subscriber_id
end
```

#### NOTES:

- **edr reporting enable:** Specify this keyword to enable the EDR reporting on SMF. Use the **edr reporting disable** command to disable the EDR reporting functionality. By default, the EDR reporting is disabled.
- **edr subscribers subscriber\_id :** Specify the ID of subscribers for which the EDR reporting must be enabled. *subscriber\_id* must be an alphanumeric string. The default value is empty.



**Note** Be sure to specify the exact subscriber key in this command. The SMF supports only IMSI (SUPI)-based EDR reporting.

- Configure a minimum of one subscriber upon enabling the EDR reporting.
- You can configure up to a maximum of 10 subscribers for EDR generation.

### Configure EDR Files for Generation

Use the following sample configuration to generate the EDR events at transaction level.

```
config
  edr file { transaction | transaction-collision }
  disable procedure-id procedure_id_value
  procedure-id procedure_id_value
  disable event-id event_id_value
  event-id event_id_value
  disable field-id field_id_value
end
```

- **edr file { transaction | transaction-collision }:** Specify to generate EDR files with transaction or transaction-collision level details for subscriber sessions.
- **procedure-id procedure\_id\_value:** Specify the procedure ID or procedure name for which the event reporting must be enabled.

- **event-id** *event\_id\_value*: Specify the event ID or event name for which the event reporting must be enabled.
- **field-id** *field\_id\_value*: Specify the field ID or field name for which the event reporting must be enabled.
- All procedure IDs, event IDs, and field IDs registered by application, are enabled by default.
- If a procedure-id is disabled, no event start, add field, or event-end will be honored for the procedure-id.
- If an event-id is disabled within a procedure id, then event-start, event-end, or add field will not be honored for the procedure-id and event-id combination.
- If a field-id is disabled for an event-id, then add-field will not be honored, and a blank entry will be present instead of value in CSV entry.

**Example configuration:**

```
edr file transaction
  disable procedure-id 24 32
  procedure-id 25
    disable event-id 5 7 8
    event-id 5
    disable field-id 10 12 14
```

In the preceding example, **disable event-id 5 7 8** means disable the event-id 5, 7, and 8 for procedure-id 25. The **disable field-id 10 12 14** means disable the field-id 10, 12, and 14 for procedure-id 25 and event-id 5.

## Configure EDR Parameters

Use the following sample configuration to configure the EDR parameters.

```
config
  edr file transaction
    limit size file_size count file_count
    flush interval file_flush_interval
  end
```

**NOTES:**

- **limit size** *file\_size* **count** *file\_count*: Specify the maximum size of one EDR file, after which the EDR file is compressed and new CSV file is created. The default file size is 100 MB.
- **count** *file\_count*: Specify the maximum number of EDR files to be preserved. The default file count is 10.
- **flush interval** *file\_flush\_interval*: Specify the time interval, in milliseconds, to flush the EDR files. The default value is 1000 ms.

## Verifying EDR Transactions

Use the following show commands to display the currently registered procedures, events, and fields for the application along with their respective IDs.

```
show edr transaction-procedure procedure_id event event_id
show edr event event_id
```

You can provide all the procedures and events. Otherwise, you can provide a particular procedure name and event name or procedure-id and event-id.



**Note** The show command output is based on the mapping registered by the application.

The following is an example of the show command output.

```

Procedure-id 20, Procedure-Name: xyz
  Event-id 1, Event-Name: abc
    1 - Field1-Name
    2 - Field2-Name
    ...
    ...
    ...
  Event-id 2, Event-Name: efgh
    1 - Field1-Name
    2 - Field2-Name
    ...
    ...
    ...
...
...
...
Procedure-id 21, Procedure-Name: bbbb
  Event-id 1, Event-Name: cccc
    1 - Field1-Name
    2 - Field2-Name
    ...
    ...
    ...
  Event-id 2, Event-Name: dddd
    1 - Field1-Name
    2 - Field2-Name
    ...
    ...
    ...

```

This output helps the operator to know current CSV format of a particular procedure-id and event-id pair.

## OAM Support for EDR Logging

This section describes operations, administration, and maintenance information for this feature.

### Bulk Statistics Support

The SMF maintains the following bulk statistics as part of this feature.

- `edr_error_total`

**Labels:**

- `error_code` – The EDR writing error code

This metric is pegged whenever an error occurs during EDR writing. This metric displays "EdrQueueFull" as the `error_code` when the writing queue is full and the EDR is dropped.

## Metadata Provided by SMF for EDR

The SMF provides the following metadata to the User Plane Function (UPF), which includes the data in the generated EDRs:

- Called-Station-ID: Specifies the DNN for the session
- Calling-Station-ID: Specifies the MSISDN of the UE
- RAT Type: RAT type for the current session (NR or EUTRAN)
- ULI: User location for the current session

The UPF receives the above data in the "Subscriber Parameters" IE in the PFCP Session Establishment Request message. The RAT type and ULI can change during the lifetime of session (for events, such as 5G to 4G handover). The UPF receives the changed values of these parameters in the PFCP Session Modification Request message.



### Note

- All the parameters are always sent from the SMF to the UPF irrespective of EDR configuration being available. These parameters ensure that any change in configuration after the session creation is immediately applied on the UPF.
- The SMF supports EDR-related configurations. However, the SMF does not require these configurations for its functionality. These configurations are sent to the UPF through RCM.

## X-Header Insertion Support

With the X-Header Insertion and X-Header Encryption features, collectively known as Header Enrichment, you can append headers to HTTP or WSP GET and POST request packets, and HTTP response packets for use by end applications. For example, mobile advertisement insertion (MSISDN, IMSI, IP address, user-customizable, and so on).

## Supported X-Header Information

Out of all the configurable X-header information, some information requires control plane (SMF) to send the corresponding values to the user plane (UPF). The following table lists the information that is sent from the SMF to the UPF for X-header Insertion support.

Xheader Field	Description	Present in Session Establishment	Modified in Session Modification
String Constant	Inserts the configured string in xheader	N/A	N/A
Charging ID	Per Flow/Bearer Charging Id	Yes	N/A
IMEI	IMEI for the call	Yes	N/A
IMSI	IMSI for the call	Yes	N/A

Xheader Field	Description	Present in Session Establishment	Modified in Session Modification
Rat-Type	RAT type for the UE session	Yes	Yes
s-mcc-mnc	MCC/MNC of the SGW/AMF	Yes	N/A
Sgsn-address	AMF/SGW address	Yes	Yes
ULI	User Location Info	Yes	Yes
GGSN-Address	N4/S5 endpoint of SMF	Yes	Yes
Radius-station-ID	MSISDN of the UE	N/A	N/A
Sn-rulebase	Rulebase for a call	Yes	Yes
Subscriber-ip-address	IP address allocated to UE	N/A	N/A
Msisdn-no-cc	Obtained from MSISDN	Yes	No

The subscriber-specific fields—IMSI, MSIDN, and IMEI—are encoded in the "User ID" standard IE. See, 3GPP 29.244, Section 8.2.101 for more information.

Rest of the fields are sent in the "Subscriber Parameters" proprietary AVP. Some fields, such as the "Rulebase" and "UE IP address", are sent as a part of the created PDRs.



#### Note

- All the parameters are always sent from the SMF to the UPF irrespective of whether X-header configuration is available. These parameters ensure that any change in configuration after session creation is immediately applied on the UPF.
- The SMF supports X-header Insertion-related configurations. The SMF does not require these configurations for its functionality. These configurations are sent to the UPF through the RCM.

## Bearer QCI Support

### Feature Description

The User Plane function (UPF) requires the Bearer level information (BLI) for each QoS flow like QFI for 5G and Bearer Id for 4G, 5G QoS Identifier (5QI) allocation and retention priority (ARP), and Charging ID, to support inline services. The Bearer QCI Support feature facilitates this requirement with the SMF.



#### Note

The Bearer QCI Support feature also includes support for Bli\_ID and QFI values in the "Create PDR" message.

The SMF sends the Bearer QoS Class Identifier (QCI) Information Element (IE), which is cisco proprietary IE, in the PFCP session establishment request and PFCP session modification request. The UPF implicitly derives the deletion indication. If a BLI ID is no longer associated with any PDR, the UPF removes it from the PFCP session context. The UPF adds the 5QI or QCI value in the EDR. Currently, the Bearer QCI field is used for 5G to add the 5QI.

The BLI is reported to the UPF as shown in the following table. The formats and encoding and decoding of these IEs are the same as other 3GPP IEs as described in *TS 29.244*.

Information Elements	Mandatory /Optional	Data Type	Description
valid		guint8	Validity of the Bearer level information IE
bli_id	Mandatory	PfcpBliId	QoS flow identifier (QFI) of 5G or Bearer ID (4G)
qci	Optional	PfcpQci	Used by PGW-C, not relevant for SMF
_5qi	Optional	Pfcp5qi	5QI associated with the QoS flow
arp	Mandatory	PfcpArp	ARP comprises of pre-emption capability, Pre-emption vulnerability, and priority level.
charging_id	Optional	PfcpChargingId	Charging ID associated with the QoS flow or Bearer (or both).

### Bearer Level Information ID

The unique ID for each Bearer level information sent from SMF. The recommended value of this IE is QFI (in 5G) or Bearer-id (in 4G). The format of IE is as below:

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 232 (decimal)							
3 to 4	Length = 1							
5	BLI_ID value							
6 to n+4	These octets are present only if explicitly specified							

**QCI** : This is not applicable for 5G. It is used in CUPS, if required.

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 233 (decimal)							
3 to 4	Length = 1							

5	QCI value
6 to n+4	These octets are present only if explicitly specified

**5QI:** The SMF uses this this IE to send the 5QI value.

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 234 (decimal)							
3 to 4	Length = 1							
5	5QI value							
6 to n+4	These octets are present only if explicitly specified							

**ARP:** The ARP value is sent with this IE.



**Note** From SMF, the ARP value is encoded as arp->pci)<<4) | arp->pl)<<2)| arp->pvi)

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 235 (decimal)							
3 to 4	Length = 1							
5	ARP value							
6 to n+4	These octets are present only if explicitly specified							

**Charging ID:** The Charging IE is sent with this IE.

	Bits							
Octets	8	7	6	5	4	3	2	1
1 to 2	Type = 236 (decimal)							
3 to 4	Length = 1							
5	Charging Id value							
6 to n+4	These octets are present only if explicitly specified							

### Triggers for Bearer Level Information IE

The following are the triggers for sending the BLI IE in PFCP messages:

#### PFCP Session Establishment Message

The Bearer level information IE is sent for each new QoS flow with the unique QFI ID. This IE is added in the policy decision in the N7 Policy Control Create Response message from the PCF. Therefore, SMF sends multiple instances of this IE, in a single PFCP message.

**PFCP Session Modification Message:**

Any new QoS flow addition or new PCC rule referring to an existing QoS flow that results in a new QER or PDR IE that has a new Bearer level information IE for each unique QFI ID.

The BLI IE is not included in the PFCP Session Modification Message if the modification is for IDFT tunnels.





## CHAPTER 16

# Customization of StarOS-based UPF on N4 Interface

- [Feature Summary and Revision History, on page 203](#)
- [Feature Description, on page 204](#)

## Feature Summary and Revision History

### Summary Data

*Table 71: Feature Summary*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 72: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

The SMF interacts with the already available StarOS-based UPF node for initial trials. The SMF must meet some non-standard requirements on the UPF node to interwork with this UPF.

### Support for Prime PFD Message

The StarOS-based UPF node needs basic ECS rules configuration pushed from SMF. These default rules need to be provisioned in UPF dynamically even for dynamic PCC policy.

- The StarOS UPF expects SMF to send the configuration in a new custom message. This message is called `SX_PRIME_PFD_MANAGEMENT_REQUEST`. The custom message ID of this message is 0x2F.
- The response sent by UPF for this message is `SX_PRIME_PFD_MANAGEMENT_RESPONSE` with message ID 0x30.

The following snapshot shows the contents of this message:

```
[U-PLANE]PFCP Rx PDU, from 192.60.181.6:40259 to 192.60.181.2:8805 (81)
SEID: NA, Message type: SX_MSG_PRIME_PFD_MANAGEMENT_REQUEST (0x2F)
Sequence Number: 0x000001 (1)
PFCP HEADER
  Version number: 1
  SEID flag: Not present
  Message Length: 0x004D (77)
INFORMATION ELEMENTS
  CONFIG ACTION:
    Type: 202 Length: 1
    Value: ADD
    Hex: 00CA 0001 01
  CORRELATION ID:
    Type: 203 Length: 2
    Value: 4
    Hex: 00CB 0002 0004
  SUB PART NUMBER:
    Type: 204 Length: 1
    Value: 245
    Hex: 00CC 0001 F5
  CONTENT TLV:
    Type: 206 Length: 53
    Value:
      Content Type: ACS_LEVEL_INFO
      Content Length: 50
      Hex: 00CE 0035 0B00 325C 00F1 015F 5F64 657F
          6661 756C 745F 5F10 0113 2C01 0111 C801
          132C 0101 132C 0101 532C 0101 0155 01FF
          01FF 0101 1001 032C 01
Tuesday August 21 2018
<<<<OUTBOUND 09:43:39:380 Eventid:221302(3)
[U-PLANE]PFCP Tx PDU, from 192.60.181.2:8805 to 192.60.181.6:40259 (19)
SEID: NA, Message type: SX_MSG_PRIME_PFD_MANAGEMENT_RESPONSE (0x30)
Sequence Number: 0x000001 (1)
PFCP HEADER
  Version number: 1
  SEID flag: Not present
  Message Length: 0x000F (15)
INFORMATION ELEMENTS
  CAUSE:
```

```

Type: 19 Length: 1
Value:
Cause: PFCP_CAUSE_REQUEST_ACCEPTED (0x01)
Hex: 0013 0001 01
CORRELATION ID:
Type: 203 Length: 2
Value: 4
Hex: 00CB 0002 0004

```

## Dynamic IP Pool Provisioning on UPF

The StarOS UPF expects SMF to send the configured IP pool range for assigning the IP address to UE during PDU session creation. The UPF uses this information to install static routes for the entire range of IP addresses and advertises the same. The IP pool range information consists of:

- Start and end IP address of the pool range
- VPN context ID in which the pool must be dynamically configured in the UPF.

The SMF does not have any VPN ID supported in this release. It sends a configured value that also must be configured on the UPF.

- IP pool chunk ID

The SMF currently does not break the pool into smaller chunks. Hence, it always sends 1 as the chunk ID.

- IP pool information

The pool information is sent to the UPF in an N4 Association Update Request message after the N4 Association Setup Request or Response has been successfully exchanged with UPF and also after the SX Prime PFD Management Request or Response has been exchanged. The Content TLV IE (IE type 206) is used to send this pool information in the N4 Association Update Request.

## Absence of NodeID Attribute from N4 Messages

As per the 3GPP specifications, the NodeID attribute uniquely identifies the SMF to the UPF. This IE is a mandatory attribute in the N4 Session Establishment Request or Response message. The UPF currently does not support this IE in any of the Session Management related messages. As a customization, the SMF does not send this IE and does not expect this IE in the response messages.

## Non Standard Attribute Type

As per 3GPP specifications, the FAR ID attribute has an ID type 108. The StarOS UPF assumes this IE type as 200. As a customization, the SMF sets 200 as the FAR ID IE type.

## Single QFI Support

As per 3GPP specifications, the PDR sent to UPF may have a list of QFIs associated to all the QERs. The StarOS UPF currently supports only one QFI. As a customization, the SMF includes only one QFI.





# CHAPTER 17

## Customized Configuration for Controlling Subscription Messages over N10

- [Feature Summary and Revision History, on page 207](#)
- [Feature Description, on page 208](#)
- [How it Works, on page 208](#)
- [Configuring Options for Controlling SDM Messages, on page 208](#)

### Feature Summary and Revision History

#### Summary Data

*Table 73: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 74: Revision History*

Revision Details	Release
First introduced.	2020.03.0

## Feature Description

The SMF introduces new RAT type configuration options with the existing configuration **authorization local** in the DNN profile. With this optional configuration, the SMF stops the Subscription Data Management (SDM) messages from sending over N10 interface towards Unified Data Management (UDM).

## How it Works

This feature works with the customized RAT-type configuration in the DNN profile configuration.

When the SMF skips UDM subscription, then it stops sending Fetch-Subscription and Subscribe-for-Notification during session establishment.

When the SMF skips the UDM subscription, then it stops sending Unsubscribe-to-Notification during session release. The SMF sends Unsubscribe-to-Notification only when the UDM receives the UECM messages.

The SMF supports dynamic change for UDM subscription skip configuration. That is, new configuration is applicable for the new session getting established. The existing sessions continue as per the old behavior of configuration.

For information on the complete configuration commands, see the following section.

## Configuring Options for Controlling SDM Messages

This section describes how to configure this feature for controlling SDM messages over the N10 interface.

### Configuring RAT-type in DNN Profile

To configure the RAT-type with the local authorization under the DNN profile, use the following commands:

```
configure
  profile dnn dnnprofile
    authorization local rat-type [ nr | eutra | wlan ]
  end
```

#### NOTES:

- **authorization local**: This command skips the SDM messages for EPS sessions only. Upon configuring this command under the selected DNN profile, the SMF skips the UDM interaction for fetch subscription. The SMF uses the values received in the ‘Create Session Request’ message. The SMF skips the UDM interaction to receive ‘Subscribe-for-Notification’ from the UDM.
- **rat-type [ nr | eutra | wlan ]**: This keyword skips the following SDM messages based on the specified RAT-type.
  - udm subscription-fetch
  - subscribe-to-notification
  - unsubscribe-to-notifications

Upon configuring the RAT-type with **authorization local** command in the selected dnn-profile, then for sessions on that RAT-type, the SMF skips the following interactions:

- the UDM interaction for ‘UDM fetch subscription’ during session establishment
  - the UDM interaction to ‘subscriber-for-notification’ during session establishment
  - the UDM interaction to ‘unsubscribe-for-notification’ during session release
- **no authorization local rat-type [ nr | eutra | wlan ]**: Disables the local authorization under the DNN profile.







# CHAPTER 18

## DNS Proxy Integration

- [Feature Summary and Revision History, on page 211](#)
- [Feature Description, on page 212](#)
- [Configuring the DNS Proxy Feature, on page 214](#)

### Feature Summary and Revision History

#### Summary Data

*Table 75: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 76: Revision History*

Revision Details	Release
Added support for randomization of P-CSCF addresses from DNS.	2021.01.0
First introduced.	Pre-2020.02.0

## Feature Description

The Domain Name System (DNS) is a network of servers that translates numeric IP addresses into readable, hierarchical Internet addresses, and vice-versa. The DNS Proxy allows you to configure one or more proxy servers for resolving the host names. The DNS queries are sent to the configured DNS servers through the DNS proxy servers for resolving host names to their IP addresses.

The DNS proxy feature is integrated in the SMF network function.

## Randomization of P-CSCF Addresses from DNS

The SMF service supports random selection of resolved hosts. If a DNS resolution yielded a set of IP addresses for a host and if the **randomize-answers** CLI is enabled in the DNS Proxy profile configuration, the DNS lookup selects IP addresses randomly. The selection of addresses is based on pseudo-random permutation of integers that ensure randomization.

Every DNS query for a particular host gives different sets of IP addresses when the **randomize-answers** CLI is enabled. This is applicable for both IPv4 and IPv6 addresses.

The selection method is either round-robin or randomized for the DNS Proxy profile.

### Example:

For a DNS lookup to get a subset of five IP addresses with **randomize-answers** enabled.

Host1 = { "1.1.1.1", "2.2.2.2", "3.3.3.3", "4.4.4.4", "5.5.5.5", "6.6.6.6", "7.7.7.7", "8.8.8.8", "9.9.9.9", "10.10.10.10" }

First lookup: [5.5.5.5 1.1.1.1 9.9.9.9 2.2.2.2 7.7.7.7]

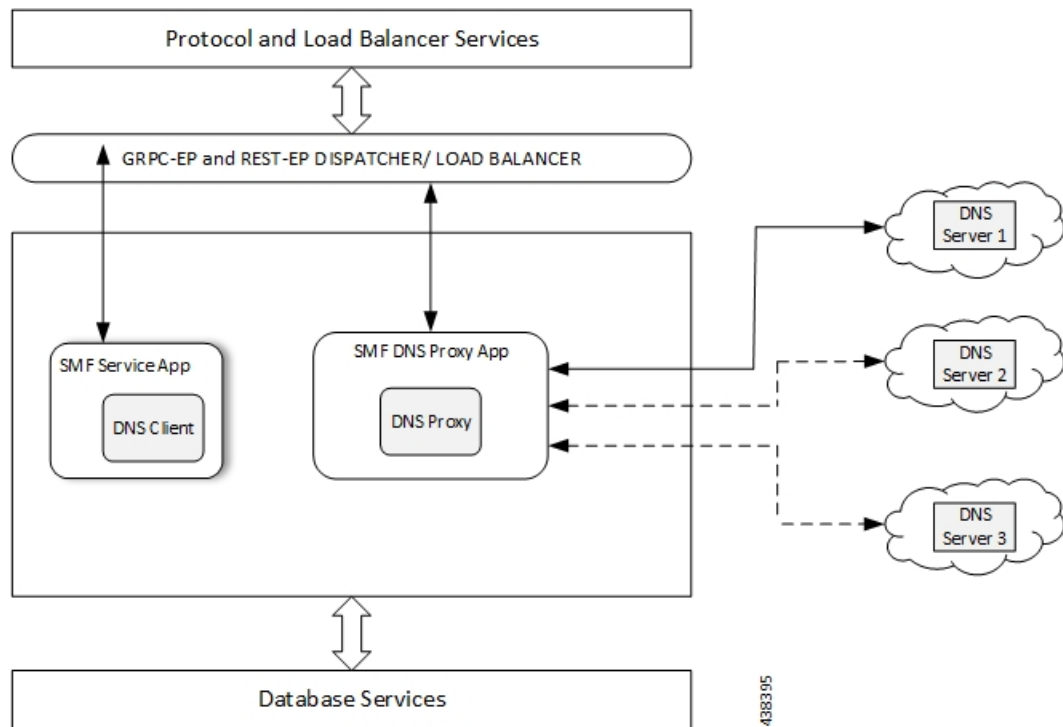
Second lookup: [8.8.8.8 6.6.6.6 2.2.2.2 3.3.3.3 9.9.9.9]

Third lookup: [7.7.7.7 5.5.5.5 2.2.2.2 4.4.4.4 9.9.9.9]

## How it Works

The DNS Proxy feature is integrated in the SMF cluster. For sending the list of host names to resolve the DNS Proxy server, the SMF Client Library calls the `smfdnsclnt.DNSLookupRequest()` Request. The DNS Proxy server forwards the request to the Open source DNS package for host name to IP address resolution.

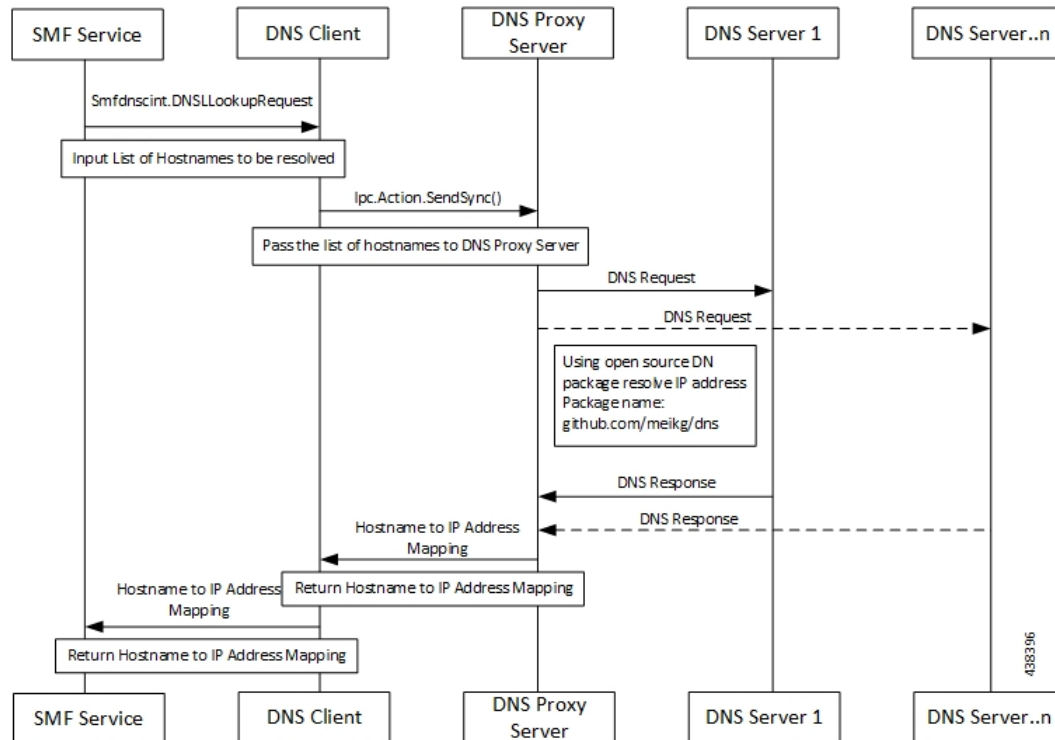
Figure 29: DNS Proxy Integration in SMF



## Call Flows

The following call flow illustrates the communication between the DNS client and the Proxy server.

Figure 30: DNS Client and Proxy Server Communication Call Flow



## Configuring the DNS Proxy Feature

This section describes how to configure the DNS Proxy feature.

Configuring the DNS Proxy feature involves the following steps:

1. [Configuring DNS Proxy Replica](#)
2. [Configuring DNS Proxy](#)
3. [Configuring P-CSCF Server Addresses](#)

## Configuring DNS Proxy Replica

Use the following sample configuration to configure the DNS proxy replica.

```

config
  instance instance-id gr_instance_id
  endpoint dns-proxy replicas replica_value
  commit
  
```

### NOTES:

- **endpoint dns-proxy replicas replica\_value**: Specify the number of replicas of the DNS proxy pod per node.

*replica\_value* must be an integer.

- **commit**: Saves the configuration.

## Configuring DNS Proxy

Use the following sample configuration to configure the DNS Proxy feature for SMF.

```
config
  profile dns-proxy
    cache-ttl dns_response_ttl_value
    query-type { ipv4v6 | ipv4 | ipv6 }
    randomize-answers
    round-robin-answers
    servers dns_server_name
      ip server_ip_address
      port server_port
      priority server_priority
      protocol { tcp | udp }
    timeout dns_timeout_value
  commit
```

### NOTES:

- **profile dns-proxy**: Enter the DNS Proxy Configuration mode.
- **cache-ttl** *dns\_response\_ttl\_value*: Specify the TTL value of DNS responses in cache, in seconds. *dns\_response\_ttl\_value* must be an integer in the range of 60-86400.
- **query-type**: Specify the DNS query type.
- **randomize-answers**: Enable DNS for fetching addresses by the randomized selection method.
- **round-robin-answers**: Enable DNS for fetching addresses by the round-robin selection method.
- **servers** *dns\_server\_name*: Specify the name of the DNS server. For example, serv1.
  - **ip** *server\_ip\_address*: Specify the IP address of the DNS server.
  - **port** *server\_port*: Specify the port of the DNS server. *server\_port* must be an integer in the range of 1-65535.
  - **priority** *server\_priority*: Specify the priority of the DNS server. *server\_priority* must be an integer in the range of 1-100.
  - **protocol**: Specify the protocol type for the DNS server as TCP or UDP.
- **timeout** *dns\_timeout\_value*: Specify the DNS timeout value, in milliseconds. *dns\_timeout\_value* must be an integer.
- **commit**: Saves the configuration.

## Configuring P-CSCF Server Addresses

This section describes how to configure IPv4, IPv6, and IPv4v6 addresses for primary, secondary, and tertiary P-CSCF servers.

### Configuring P-CSCF Server IPv4 Addresses

Use the following sample configuration to configure the IPv4 address of the primary, secondary, and tertiary P-CSCF servers.

```
config
  profile pscsf pscsf_profile_name
    v4-list
      precedence precedence_value
      primary server_ipv4_address
      secondary server_ipv4_address
      tertiary server_ipv4_address
    end
```

#### NOTES:

- **precedence** *precedence\_value*: Specify the precedence value. *precedence\_value* must be an integer in the range of 1-64. This precedence value is used for the round-robin selection of P-CSCF server. The lower the precedence, the higher the priority.
- **primary** *server\_ipv4\_address*: Specify the IPv4 address of the primary P-CSCF server in dotted-decimal notation.
- **secondary** *server\_ipv4\_address*: Specify the IPv4 address of the secondary P-CSCF server in dotted-decimal notation.
- **tertiary** *server\_ipv4\_address*: Specify the IPv4 address of the tertiary P-CSCF server in dotted-decimal notation.

### Configuring P-CSCF Server IPv6 Addresses

Use the following sample configuration to configure the IPv6 address of the primary, secondary, and tertiary P-CSCF servers.

```
config
  profile pscsf pscsf_profile_name
    v6-list
      precedence precedence_value
      primary server_ipv6_address
      secondary server_ipv6_address
      tertiary server_ipv6_address
    end
```

#### NOTES:

- **precedence** *precedence\_value*: Specify the precedence value. *precedence\_value* must be an integer in the range of 1-64. This precedence value is used for the round-robin selection of P-CSCF server. The lower the precedence, the higher the priority.

- **primary server\_ipv6\_address**: Specify the IPv6 address of the primary P-CSCF server in colon-separated hexadecimal notation.
- **secondary server\_ipv6\_address**: Specify the IPv6 address of the secondary P-CSCF server in colon-separated hexadecimal notation.
- **tertiary server\_ipv6\_address**: Specify the IPv6 address of the tertiary P-CSCF server in colon-separated hexadecimal notation.

## Configuring P-CSCF Server IPv4v6 Addresses

Use the following sample configuration to configure the IPv4v6 address of the primary, secondary, and tertiary P-CSCF servers.

```

config
  profile pcscf pcscf_profile_name
    v4v6-list
      precedence precedence_value
      primary ipv4 server_ipv4_address ipv6 server_ipv6_address
      secondary { [ ipv4 server_ipv4_address ] [ ipv6 server_ipv6_address ]
    }
      tertiary { [ ipv4 server_ipv4_address ] [ ipv6 server_ipv6_address ] }
    end

```

### NOTES:

- **precedence precedence\_value**: Specify the precedence value. *precedence\_value* must be an integer in the range of 1-64. This precedence value is used for the round-robin selection of P-CSCF server. The lower the precedence, the higher the priority.
- **primary ipv4 server\_ipv4\_address ipv6 server\_ipv6\_address**: Specify the IPv4 and IPv6 address of the primary P-CSCF server in dotted-decimal notation and colon-separated hexadecimal notation respectively.
- **secondary { [ ipv4 server\_ipv4\_address ] [ ipv6 server\_ipv6\_address ] }**: Specify the IPv4 and IPv6 address of the secondary P-CSCF server in dotted-decimal notation and colon-separated hexadecimal notation respectively.
- **tertiary { [ ipv4 server\_ipv4\_address ] [ ipv6 server\_ipv6\_address ] }**: Specify the IPv4 and IPv6 address of the tertiary P-CSCF server in dotted-decimal notation and colon-separated hexadecimal notation respectively.

## Verifying DNS Proxy Feature Configuration

This section describes how to verify the DNS Proxy feature configuration.

Use the **show running-config profile dns-proxy** command to confirm the configuration of DNS Proxy feature.

The following is an example output of **show running-config profile dns-proxy** command with configuration for two DNS servers, serv1 and serv2.

```

show running-config profile dns-proxy profile1
  query-type ipv4
  timeout 5
  servers serv1

```

```
round-robin-answers
servers serv1
ip 10.105.227.227
port 53
protocol tcp
priority 1
exit
servers serv2
ip 10.105.227.228
port 20
protocol udp
priority 2
randomise-answers
exit
exit
```





# CHAPTER 19

## DSCP Marking

- [Feature Summary and Revision History, on page 219](#)
- [Feature Description, on page 219](#)
- [DSCP Marking for User Plane Packets, on page 220](#)
- [DSCP Marking for Control Plane Signaling, on page 221](#)

## Feature Summary and Revision History

### Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

Revision Details	Release
Provided support for DSCP marking of control plane signaling messages	2021.01.0
First introduced.	Pre-2020.02.0

## Feature Description

The SMF supports a mechanism for differentiated services code point (DSCP) marking of user plane data packets and control plane signaling messages.

The DSCP Marking feature enables the SMF to perform traffic classification and prioritisation to provide the appropriate quality of service (QoS) treatment. DSCP is the six most significant bit of the DiffServ field.

Implementation of this feature requires the use of certain CLIs commands to configure DSCP parameters for both signaling messages and data packets.

## DSCP Marking for User Plane Packets

### Feature Description

DSCP Marking supports granular configuration. For Interactive Traffic Class (ITC), the SMF supports per-APN configurable DSCP marking for Uplink and Downlink direction that is based on 5QI and ARP-Priority level. This support allows the users to assign different DSCP values for flows with the same 5QI but different ARP priority values. For example, the ability to assign DSCP values that are based on 5QI+ARP can be used to meet compliance on priority and emergency calling via VoLTE.

DSCP Marking is a CLI-controlled feature, which enables to create and map 5QI and ARP values to enforceable QoS parameters.

### How the DSCP Marking Works for Data Packets

Allocation of different DSCP values for flows with the same 5QI, but different ARP values, works as follows:

- Allows DSCP marking of packets that is based on 5QI+ARP combination.
- 5QI+ARP configuration overrides any pre-entry of DSCP marking of packets that was based on 5QI+ARP combination.
- 5QI-only DSCP entry overrides all existing 5QI+ARP configuration.
- Allows implementation of associated DSCP marking for 5QI+ARP for Uplink and Downlink functionality.

### Configuring 5QI-QoS Mapping

Use the following CLI commands to create and map 5QI values to enforceable QoS parameters.

```
configure
  profile qos qos_name
    dscp-map qi5 qi5_value [ arp-priority-level arp_value ] uplink
  user-datagram dscp-marking dscp_marking_value
    dscp-map qi5 5qi_value [ arp-priority-level arp_value ] downlink {
  encaps-header { copy-inner | dscp-marking dscp_marking_value } | user-datagram
    dscp-marking dscp_marking_value encaps-header { copy-inner | dscp-marking
dscp_marking_value } }
  commit
```

#### NOTES:

- **dscp-map**: Configures 5QI (referred as qi5 in the code) to DSCP-Marking mapping.

- **qi5** *5qi\_value*: Identifier for the authorized QoS parameters. The *5qi\_value* must be within the range of 0 through 255.
- **arp-priority-level** *arp\_value*: Configures the ARP Priority Level. The *arp\_value* must be an integer from 1 through 15.
- **downlink**: Configures the downlink traffic.
- **uplink**: Configures the uplink traffic.
- **user-datagram**: Specifies the DSCP value to be applied to user datagram. Use this keyword to set the DSCP in the inner IP header in uplink or downlink direction.
- **dscp-marking**: Specifies the DSCP value to be applied to packets with this 5QI. The value of **dscp-marking** must be a hexadecimal number from 0x00 through 0x3F.
- **encaps-header**: Configures the DSCP value to be applied to encaps header. Use this keyword to set the DSCP in the outer-ip header in downlink direction.
- **copy-inner**: Copies the DSCP value from inner IP header to the outer IP header.

The following is a sample configuration.

```
profile qos test
dscp-map qi5 1 downlink encaps-header copy-inner
dscp-map qi5 1 downlink encaps-header dscp-marking 0x3b
dscp-map qi5 2 downlink user-datagram dscp-marking 0x3b
dscp-map qi5 3 downlink user-datagram dscp-marking 0x3b encaps-header copy-inner
dscp-map qi5 4 downlink user-datagram dscp-marking 0x3b encaps-header dscp-marking 0x3f
dscp-map qi5 2 uplink user-datagram dscp-marking 0x3b

dscp-map qi5 1 arp-priority-level 1 downlink encaps-header copy-inner
dscp-map qi5 2 arp-priority-level 2 downlink encaps-header dscp-marking 0x3b
dscp-map qi5 4 arp-priority-level 3 downlink user-datagram dscp-marking 0x3b
dscp-map qi5 2 arp-priority-level 4 downlink user-datagram dscp-marking 0x3b encaps-header
copy-inner
dscp-map qi5 4 arp-priority-level 5 downlink user-datagram dscp-marking 0x3b encaps-header
dscp-marking 0x3f
dscp-map qi5 4 arp-priority-level 5 uplink user-datagram dscp-marking 0x3b
```

# DSCP Marking for Control Plane Signaling

## Feature Description

The SMF supports per-interface configurable DSCP marking for control plane signaling messages.



**Note** The current implementation of DSCP marking supports only per RPC and Endpoint. Also, the customers should be aware of the DSCP code value range and its denoted priority.

## How the DSCP Marking Works for Control Signaling

The SMF marks the ingress and egress packets after the QoS classification. The protocol endpoints provide the DSCP values at the time of registering the Endpoint and RPC host.

The SMF uses the **dscp** command in the endpoint and interface configuration to define the DSCP values.

The following table lists the commonly used DSCP values as described in RFC 2475.

**Table 77: Commonly Used DSCP Values**

DSCP Value	Decimal Value	Meaning	Drop Probability	Equivalent IP Precedence Value
101 110	46	High Priority Expedited Forwarding (EF)	N/A	101 - Critical
000 000	0	Best Effort	N/A	000 - Routine
001 010	10	AF11	Low	001 - Priority
001 100	12	AF12	Medium	001 - Priority
001 110	14	AF13	High	001 - Priority
010 010	18	AF21	Low	010 - Immediate
010 100	20	AF22	Medium	010 - Immediate
010 110	22	AF23	High	010 - Immediate
011 010	26	AF31	Low	011 - Flash
011 100	28	AF32	Medium	011 - Flash
011 110	30	AF33	High	011 - Flash
100 010	34	AF41	Low	100 - Flash Override
100 100	36	AF42	Medium	100 - Flash Override
100 110	38	AF43	High	100 - Flash Override
001 000	8	CS1		1
010 000	16	CS2		2
011 000	24	CS3		3
100 000	32	CS4		4
101 000	40	CS5		5
110 000	48	CS6		6
111 000	56	CS7		7

DSCP Value	Decimal Value	Meaning	Drop Probability	Equivalent IP Precedence Value
000 000	0	Default		
101 110	46	EF		

## Limitations

The DSCP Marking is per interface basis and not per peer or session.

## Configuring DSCP Marking for Control Plane Signaling

The following sections provide the configurations required for the DSCP marking of signaling messages.

### Configuring DSCP Marking per Endpoint

Use the following sample configuration to configure the DSCP values at the endpoint level.

```

config

    endpoint { gtp | li | protocol | radius | sbi }
        dscp dscp_value
    commit
  
```

#### NOTES:

- The DSCP Marking configuration is applicable only to the following endpoints:
  - protocol
  - sbi
  - gtp
  - radius
  - li
- **dscp** *dscp\_value*: Specify the DSCP value for the control plane signaling messages. *dscp\_value* must be a hexadecimal number from 0x00 through 0x3F or a decimal value ranging from 0 through 63.
- The DSCP Marking feature supports dynamic change of the configuration.

### Configuring DSCP Marking per Interface

Use the following sample configuration to configure the DSCP values at the interface level.

```

configure

    endpoint { gtp | li | protocol | radius | sbi }
        interface { coa-nas | gtpu | n4 | n7 | n10 | n11 | n16 | n40 |
nrf | radius-client | s2b | s5 | s8 | upf-rcm-conn | upf-rcm-reg }
  
```

```
dscp dscp_value  
commit
```

**NOTES:**

- The DSCP marking configuration is applicable to all the interfaces defined within the configured endpoints.
- **dscp** *dscp\_value*: Configures the DSCP value for the control plane signaling messages. *dscp\_value* must be a hexadecimal number from 0x00 through 0x3F or a decimal value ranging from 0 through 63.
- The DSCP Marking feature supports dynamic change of the configuration.
- The Service-based Interface (SBI) configuration applies to all the interfaces. If a specific interface configuration is present, it overrides the DSCP values.
- For the interfaces to work properly, it is mandatory to configure vip-ip, vip-port, and loopbackPort at each interface level.



## CHAPTER 20

# Emergency Services Support

- [Summary Data, on page 225](#)
- [Revision History, on page 225](#)
- [Feature Description, on page 225](#)
- [How it Works, on page 226](#)
- [Configuring Emergency Service Support, on page 228](#)
- [OAM Support for SMF Emergency Services, on page 230](#)

## Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

## Revision History

*Table 78: Revision History*

Revision Details	Release
First introduced.	2020.02.5.t1

## Feature Description

"Emergency Services" refers to functionalities provided by the serving network when the network is configured to support Emergency Services. Emergency Services are provided to support IMS emergency sessions.

To implement IMS emergency services in 4G and 5G, the SMF performs the following functions:.

- Identifies 5G emergency session based on Request Type in SmContextCreate message or emergency configuration in DNN.
- Identifies 4G emergency session based on emergency configuration in DNN.
- Interacts with UDM if SUPI/IMSI is authenticated and “authorize local” is not set. Else, skips the interaction with UDM.
- Enables PDU session establishment for Emergency Services with PEI or IMEI.
- A new configuration to classify DNN as an Emergency DNN.
- Configures P-CSCF profile for Emergency Services
- Configures UPF for Emergency Services
- Configures default QoS profile for Emergency Services and flow only timer used during tear down of dedicated bearer from PCF.

## How it Works

### Identification of Emergency Service Sessions

#### 5G

SMF identifies the Emergency Session based on request type “Initial Emergency Request” or “Existing Emergency PDU Session” received in SmContextCreate Message from AMF or if the DNN is configured as an Emergency DNN.

#### 4G

SMF identifies the emergency session based on the authentication status of IMSI. If the IMSI is unauthenticated (UIMSI is set to 1), the session is considered as an emergency session.

If IMSI is authenticated (UIMSI is set to 0), and DNN is configured as an emergency DNN (using new CLI) in SMF, the session is identified as an emergency session.

- For non-emergency session, SUPI/IMSI is mandatory.
- For emergency session:
  - For an authenticated SUPI/IMSI, SUPI or IMSI is used as the session-key as per the current implementation.
  - For an unauthenticated SUPI or IMSI, PEI or IMEI is always used as the session-key, If PEI or IMEI is not present, then the call is rejected.

### UDM Interaction for Emergency Sessions

1. SMF skips UDM interaction if SUPI or IMSI is unauthenticated.
2. SMF skips UDM interaction if SUPI/IMSI is authenticated and if “authorization” in DNN configuration is set to “local”.



3. SMF interacts with UDM if SUPI or IMSI is authenticated and if “authorization” in DNN configuration is not set to local.
  - If UDM rejects, then the call will be rejected.
  - If UDM exchanges fail, further handling is done as per UDM FH template provisioning.




---

**Important**

SMF does not consider whether “authorization local” is configured in DNN profile or not.

---

### Configuring Emergency Sessions

1. Existing DNN, P-CSCF, UPF, and QoS Profile configuration works for emergency sessions.
2. Use CLI classify a DNN as Emergency DNN.
3. If "**authorization**" is set (using CLI) to local under DNN, UDM interaction is not required.
4. Use default Flow Only timer configuration to retain the default bearer to enable PSAP Callback session.

### Support for Emergency Services if Request Type is “Existing Emergency PDU Session”

1. If the request type indicates "Existing Emergency PDU Session", the SMF determines that the request is HO from EPS (4G and WiFi). Current implementation supports emergency sessions mobility in WIFI to 5G HO using request type as “Existing Emergency PDU Session” and in 4G to 5G HO using N26 interface.
2. The SMF identifies the existing PDU session based on the PDU Session ID.
3. SMF updates the existing SM context to provide the representation of the updated SM context to the AMF in the response instead of creating new SM, which is equivalent to handling of “Existing PDU Session”.

### Default Flow Only Timer for an Emergency Service (Dedicated Bearer)

At reception of an HTTP POST message that removes one or several PCC Rules from a PDU Session restricted to emergency services:

- When all PCC Rules bound to a QoS flow are removed, SMF initiates a QoS flow termination procedure.
- When not all PCC Rules bound to a QoS flow are removed, SMF initiates an QoS flow modification procedure.

In addition, the SMF initiates a default flow only timer if all PCC Rules with a 5QI other than the 5QI of the default QoS flow or the 5QI used for IMS signalling are removed from the PDU session restricted to Emergency Services (e.g., to enable PSAP Callback session). When the default flow only timer expires, the SMF initiates a PDU session termination procedure.

1. Default flow only timer is started when a PCF initiated modify procedure removes a dedicated bearer(voice/video). The main intension of this timer is to hold the emergency session for some more time to facilitate a PSAP callback.
2. When default flow only timer expires, the PCEF initiates a PDU session termination of the IMS Emergency session.
3. Default flow only timer is stopped on getting a PCF initiated modify for creating a new bearer.

**EPS FB**

If gNB rejects the QFI and EPS FB is armed. SMf performs the EPS fallback as it is done for a normal non-emergency session.

**Use of PEI as Session Key**

SMF uses PEI as session key if SUPI is not present or is not authenticated. Following conditions must be met for PduContext on SMF:

1. REST-EP, when the message is received, checks affinity based on SUPI and PEI. First lookup will be done with SUPI. If it fails, checks with the PEI.  
Or  
Both keys SUPI and PEI can be looked up.
2. When Smf-Service chooses PEI as key, it sets affinity in cache-pod using PEI.
3. When Smf-Service inserts CDL record using PEI as key, PEI will be added as Primary Key type. Either Primary key is SUPI+PduSessionid or PEI+PduSessionID.
4. After first transaction, CDL lookup will happen both with SUPI or PEI as per the availability.
5. SEID is generated using PEI hashing.

## Configuring Emergency Service Support

This section describes how to configure Emergency Service Support.

### Configuring Default Flow Only Timer in DNN Profile

Use the following configuration to configure Default Flow Only Timer.

```
configure
timeout default-flow-only flow_only_timer
end
```

**NOTES:**

- **timeout default-flow-only *flow\_only\_timer*** : Maximum allowed idle duration for a PDU/PDN session before system automatically terminates it. *flow\_only\_timer* Must be an integer between and 0 and 2147483647 seconds. Default is 0, which indicates the function is disabled.

### Configuring Emergency DNN

Use the following configuration to configure Default Flow Only Timer.

```
configure
emergency { false | true }
end
```

**NOTES:**

- **emergency** { *false* / *true* }: Enables for emergency session only. *false* / *true* is followed by emergency indicating default flow only timer as emergency or not.

## Verifying Emergency DNN

Use the following show command to verify Emergency DNN configuration:

**show subscriber all**

```
subscriber-details
{
  "subResponses": [
    [
      "supi:imsi-123456789012345",
      "gpsi:msisdn-9999988888",
      "pei:imei-123456786666660",
      "psid:5",
      "dnn:intershat",
      "emergency:false",
      "rat:nr",
      "access:3gpp access",
      "connectivity:5g",
      "udm-uecm:10.84.17.161",
      "udm-sdm:10.84.17.161",
      "pcfGroupId:PCF-dnn=",
      "pcf:10.84.17.161",
      "policy:2",
      "upf:10.84.17.161",
      "upfEpKey:10.84.17.161:10.84.17.160",
      "ipv4-addr:poolv4/12.0.0.1",
      "ipv4-pool:poolv4",
      "ipv4-range:poolv4/12.0.0.1",
      "ipv4-startrange:poolv4/12.0.0.1",
      "amf:10.84.17.161",
      "peerGtpuEpKey:10.84.17.161:10.106.183.198"
    ],
    [
      "gpsi:msisdn-9999988888",
      "pei:imei-352099001761480",
      "psid:6",
      "dnn:intershat",
      "emergency:true",
      "rat:nr",
      "access:3gpp access",
      "connectivity:5g",
      "pcfGroupId:PCF-dnn=",
      "pcf:10.84.17.161",
      "policy:2",
      "upf:10.84.17.161",
      "upfEpKey:10.84.17.161:10.84.17.160",
      "ipv4-addr:poolv4/12.0.4.0",
      "ipv4-pool:poolv4",
      "ipv4-range:poolv4/12.0.0.1",
      "ipv4-startrange:poolv4/12.0.4.0",
      "amf:10.84.17.161",
      "peerGtpuEpKey:10.84.17.161:10.106.183.198"
    ]
  ]
}
```

# OAM Support for SMF Emergency Services

This section describes operations, administration, and maintenance information for this feature.

## Statistics

The following are the enhanced statistics for the SMF Emergency Services Support:

**Table 79: Bulk statistics for SMF Emergency Services Support**

<b>Bulk Statistics</b>	<b>Description</b>
smf_session_counters	Indicates that the gauge updated to show the number of active always-on pdu sessions.
smf_service_stats	This counter increments with every query made to the smf-service.
resource_mgmt_stats	This counter increments for every IP address dynamic/static allocation/release queries made to the node-mngr in smf-service.



# CHAPTER 21

## EPS Interworking

- [Feature Summary and Revision History, on page 231](#)
- [Feature Description, on page 232](#)
- [Support for UE Initial Attach on E-UTRAN, on page 234](#)
- [Detach Procedure for EPS on SMF and P-GW, on page 239](#)
- [Dedicated Bearer Activation and Deactivation, on page 241](#)
- [EPS Fallback, on page 247](#)
- [EPS Fallback Guard Timer Support, on page 249](#)
- [Indirect Data Forwarding Tunnel \(IDFT\) Timer Support, on page 252](#)
- [Bearer Modification for EPS Session on SMF, on page 256](#)
- [Session Management Procedures for EPS and 5GC Interworking, on page 263](#)
- [5G to EPS Handover Using N26 Interface, on page 286](#)
- [Create Dedicated Bearer Delay and Retry Support, on page 288](#)
- [Handling GTP-U Error Indication for 4G Sessions, on page 291](#)
- [GTP Path Failure Handling, Restoration, and Recovery, on page 293](#)
- [Configuration Support for Rejecting 4G-only Devices, on page 298](#)
- [Dynamic Configuration Change Support, on page 298](#)

## Feature Summary and Revision History

### Summary Data

*Table 80: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

## Revision History

*Table 81: Revision History*

Revision Details	Release
Introduced procedure to support dynamic configuration of the Access Profile configuration.	2020.03.0
New CLI command in the DNN profile configuration to reject calls from 4G-only UE devices.	2020.02.1
First introduced.	Pre-2020.02.0

## Feature Description

The SMF implements the 3GPP recommendations for interworking of Evolved Packet System (EPS) and 5G Core Network (5GC).

The UEs capable of supporting both 4G and 5G NAS connect to the Evolved Terrestrial Radio Access Network (E-UTRAN) and the 5GC network. The SMF with the EPS interworking capability acts as a PGW-C+SMF and uses the S5 or S8 interface with S-GW to receive the 4G Session Creation Request. All the other interfaces involved in the 4G Session Creation (for example, Gx, Gy, Gz, and so on) are replaced by the corresponding 5GC Service Based Interfaces (for example, Npcf and Nchf).

After a PDU session is created on the PGW-C+SMF with E-UTRAN, Mobility Management Entity (MME) and Serving Gateway (S-GW), the UE can hand over E-UTRAN to 5G New Radio (NR) and vice-versa.

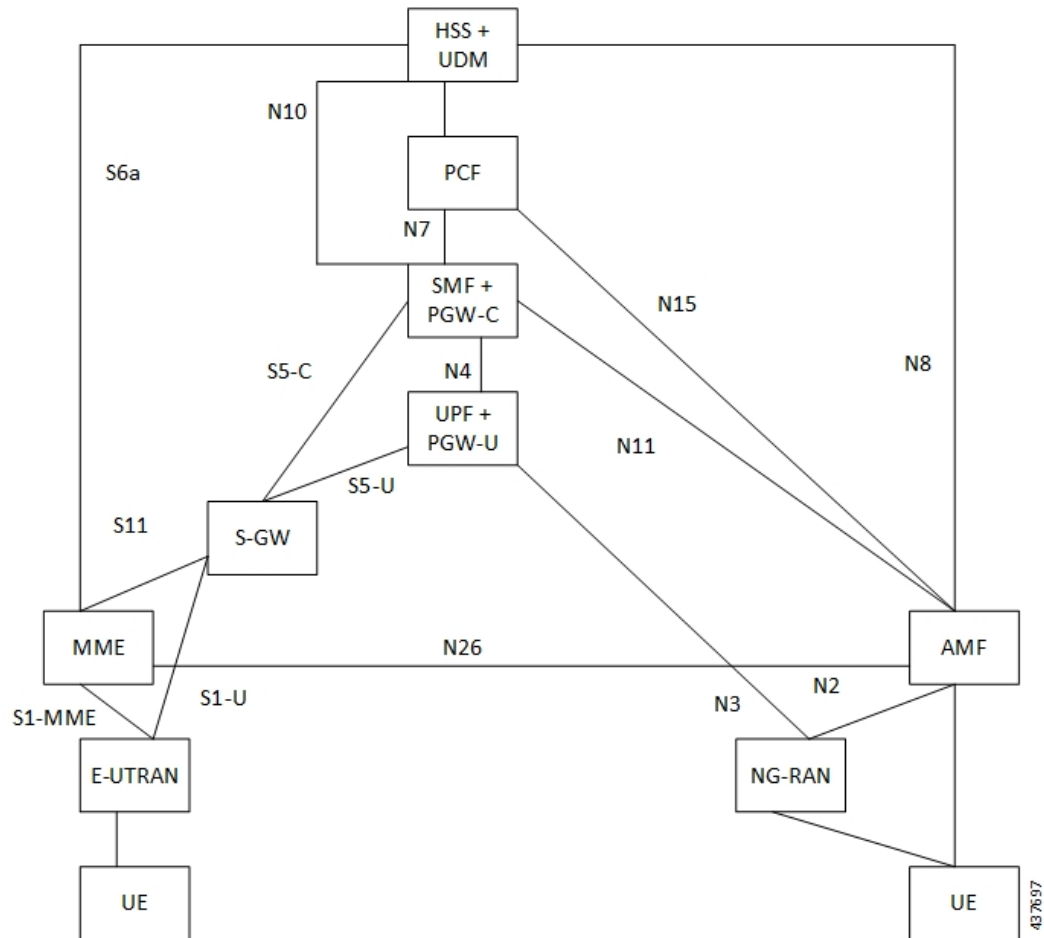
The SMF currently supports interworking with EPS using the N26 interface. This interface is an inter-CN interface between the MME and 5GS AMF to enable interworking between Evolved Packet Core (EPC) and the NG core networks. Support of N26 interface in the network is optional for interworking. N26 supports a subset of the functionalities over S10 interface to enable interworking.

The UE uses EPC NAS or 5GC NAS procedures depending on the core network by which it is served.

## Architecture

The following figure shows the network architecture for the EPS-5G Core interworking.

Figure 31: 3GPP Non-Roaming Architecture for EPS-5GC Interworking



## How it Works

A UE that supports only EPS based Dual Connectivity with secondary RAT NR:

- Always performs initial access through E-UTRA (LTE-Uu) but never through NR.
- Performs EPS NAS procedures over E-UTRA (that is, Mobility Management, Session Management and so on) as defined in 3GPP TS 24.301.

A UE that supports camping on 5G Systems with 5GC NAS:

- Performs initial access either through E-UTRAN that connects to 5GC or through NR towards 5GC.
- Performs initial access through E-UTRAN towards EPS, if supported and needed.
- Performs EPS NAS or 5GC NAS procedures over E-UTRAN or NR respectively (that is, Mobility Management, Session Management, and so on) depending on whether the UE requests 5GC access or EPS access, if the UE also supports EPS NAS.

For interworking with EPS, the UE that supports both 5GC and EPS NAS can operate in one of the following modes:

- Single-registration mode: UE has only one active MM state (either RM state in 5GC or EMM state in EPS) and it is either in 5GC NAS mode or in EPS NAS mode (when connected to 5GC or EPS, respectively).
- Dual-registration mode: UE handles independent registrations for 5GC and EPS using separate RRC connections. In this mode, the UE may be registered to 5GC only, EPS only, or to both 5GC and EPS.

Networks that support interworking with EPS, may support interworking procedures that use the N26 interface or interworking procedures that do not use the N26 interface.

- Interworking procedures with N26 support provide IP address continuity on inter-system mobility to UEs that support 5GC NAS and EPS NAS and that operate in single registration mode. Interworking procedures using the N26 interface, enables the exchange of MM and SM states between the source and target network.
- Networks that support interworking procedures without N26 support procedures to provide IP address continuity on inter-system mobility to UEs operating in both single-registration mode and dual-registration mode. For interworking without the N26 interface, IP address preservation is provided to the UEs on inter-system mobility by storing and fetching PGW-C+SMF and corresponding APN or DNN information via the HSS+UDM.




---

**Important**

Interworking of SMF and EPS currently works only with the N26 interface.

---

## Standards Compliance

The 5GC and EPS Interworking feature complies with the following standards:

- *3GPP TS 23.401, Version 15.6.0*
- *3GPP TS 23.501, Version 15.4.0*
- *3GPP TS 23.502, Version 15.4.0*
- *3GPP TS 29.502, Version 15.2.1*
- *3GPP TS 29.512, Version 15.2.0*

## Support for UE Initial Attach on E-UTRAN

### Feature Description

The SMF supports the UE performing initial attach on E-UTRAN via MME and S-GW to create the default bearer.

Initial attach on E-UTRAN or EPS follows the procedure defined in 3GPP specification 23.401, Section 5.3.2.1. There are few deviations from the defined procedure to enable connectivity through the 5G core. The deviations are as follows:

- The Packet Data Network Gateway (P-GW) in the procedure is replaced by SMF+PGW.



- The IP-CAN Session establishment and modification is replaced by SM Policy Association Establishment procedure.
- The online and offline charging functionality using Gy and Gz interfaces is replaced by integrated charging over Nchf interface with Charging Function (CHF).
- The interface with the user-plane node is through N4 interface instead of Sxb interface.

## How it Works

### Call Flows

#### Initial Attach on E-UTRAN or EPS Procedure

The following figure shows the call flow derived from 3GPP reference for initial attach on E-UTRAN or EPS.

**Figure 32: Call Flow for Initial Attach on E-UTRAN via 5G Core**

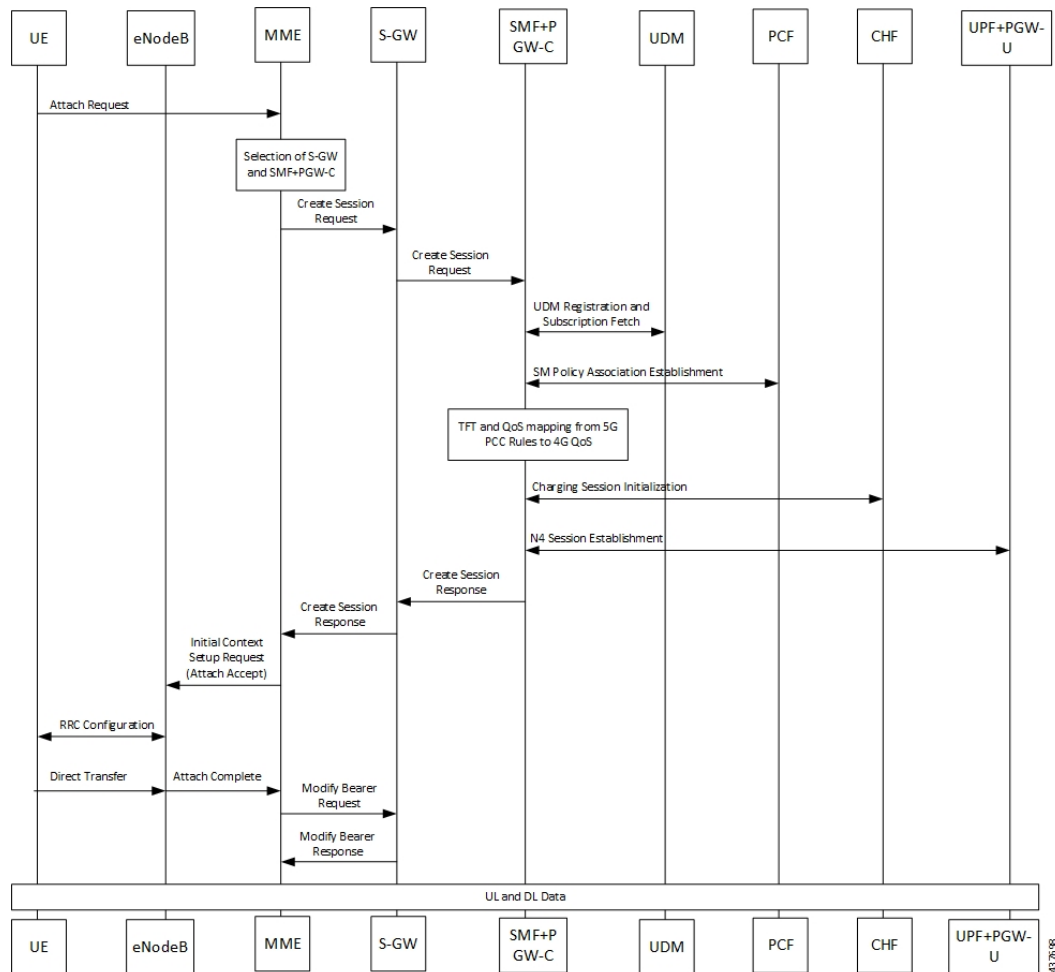


Table 82: Call Flow Description for Initial Attach on E-UTRAN via 5G Core

Step	Description
1	UE sends Attach Request to the MME through eNodeB.
2	The MME determines that the UE is capable and subscribed for handoff to NR. It selects an SMF node as the P-GW for this PDU session.
3	The MME sends Create Session Request to the selected S-GW and includes the selected SMF address in it.
4	The S-GW initiates Create Session Request towards the SMF.
5	The SMF extracts the PDU Session ID sent by the UE in the Protocol Configuration Option (PCO) 001AH (PDU session ID) and saves it. It then performs a Unified Data Management (UDM) registration and sends P-GW Fully Qualified Domain Name (FQDN) to the UDM. After registration, the SMF initiates subscription fetch from the UDM.
6	<p>The SMF sends Npcf_SMPolicyControl_Create to the PCF to initiate SM policy Association Establishment.</p> <p>The SMF includes the information elements received in Create Session Request message into the Npcf_SMPolicyControl_Create Service as follows:</p> <ul style="list-style-type: none"> <li>• The SUPI contains the IMSI.</li> <li>• The DNN contains the APN.</li> <li>• The PEI contains the IMEI-SV.</li> <li>• The Session AMBR contains the APN-AMBR.</li> <li>• The default QoS information contains the default EPS bearer QoS. The QCI values are mapped into 5QI values.</li> </ul>
7	The SMF receives Policy Charging and Control (PCC) Rules and PDU Session Policy Information, 5G QoS information in PCC Rule and in PDU Session Policy Information which are mapped into EPS QoS information. The SMF creates Traffic Flow Template (TFT) from the Service Data Filters (SDFs) received in PCC rules and associates them with the corresponding default and dedicated bearers.
8	Based on the charging policies received from PCF, the SMF initiates Nchf_ConvergedCharging_Create operation towards the CHF. This procedure is similar to a 5G session and is based on the charging rules received from the PCF.
9	The SMF performs UPF+PGW-U selection and N4 Session Establishment. Since this is a 4G session connecting the SMF, a separate CN tunnel is created for each bearer and QoS Flow ID (QFI) is not sent in the QoS Enforcement Rule (QER) and Packet Detection Rule (PDR).
10	The SMF sends Create Session Response to S-GW and includes the bearer information and Tunnel Endpoint Identifier (TEID) for the default bearer. The SMF also includes the 5G QoS parameters in PCO options 001CH (QoS rules), 001DH (Session-AMBR), 001EH (PDU session address lifetime) and 001FH (QoS flow descriptions) to the UE.
11	The S-GW sends Create Session Response to the MME.
12	The MME sends Initial Context Setup Request to the eNodeB with N1 Attach Accept message.

Step	Description
13	The eNodeB and UE perform Radio Resource Control (RRC) configuration.
14	The UE sends Direct transfer message to the eNodeB.
15	The eNodeB sends Attach Complete message in Initial Context Setup Response to the MME along with the TEID of eNodeB.
16	The MME sends a Modify Bearer Request to the S-GW with eNodeB TEID.
17	The SMF sends the Modify Bearer Response to the S-GW.
18	The S-GW sends Modify Bearer Response to the MME.

## Converged Core Refactoring Changes

This section describes the changes related to converged core refactoring in this chapter.

The `k8 smf local tracing enable true` CLI command is deprecated in 2021.01 and later releases.

## Configuring the UE Initial Attach Feature

This section describes how to configure the UE Initial Attach feature.

Configuring the UE Initial Attach feature involves the following steps:

1. Define FQDN in SMF Profile Configuration
2. Configure S5 Binding Address in SMF Service Configuration
3. Enable Kubernetes Configuration for SMF GTP Endpoint PODs

### Define FQDN in SMF Profile Configuration

Use the following configuration to specify the FQDN of SMF+PGW-C. The configured FQDN is sent to the UDM during registration.

```

config
  profile smf smf_profile_name
fqdn fqdn_name
end

```

NOTES:

- `fqdn fqdn_name`: Configures the PGW-C FQDN. *fqdn\_name* must be an alphanumeric string.

### Configure S5 Binding Address in SMF Service Configuration

Use the following configuration to define the S5 binding address at which the SMF listens for GTP messages from S-GW (S5 interface).

```

configure
  profile smf smf_profile_name
  service name smf_service_name

```

```
s5 bind-address { ipv4 ipv4_address | ipv6 ipv6_address }
end
```

**NOTES:**

- **s5 bind-address { ipv4 ipv4\_address | ipv6 ipv6\_address }**: Enter the IP address at which SMF listens for GTP messages from S-GW via S5 interface. Enter the address in either standard IPv4 dotted decimal format or in standard IPv6 colon notation format.

## Configuring GTP Endpoint Parameters

Use the following sample configuration to define the GTP endpoint parameters.

**config**

```
endpoint gtp
  replicas replica_count
  vip-ip ipv4_address
  vip-ipv6 ipv6_address
end
```

**NOTES:**

- **endpoint gtp**: Enter the GTP endpoint configuration.
- **replicas replica\_count**: Enter the number of replicas to be created per node. The default value is 1.
- **vip-ip**: Specify the IPv4 address for the GTP endpoint.
- **vip-ipv6**: Specify the IPv6 address for the GTP endpoint.

## Verifying the UE Initial Attach Feature Configuration

This section describes how to verify the UE Initial Attach feature configuration.

The following configuration is a sample output of the **show running-config** command:

```
show running-config
.
.
.
profile smf smf1
  node-id          ABC123
  bind-address ipv4 127.0.0.1
  bind-port        8008
  allowed-nssai   [ slice1 ]
  plmn-id mcc 123
  plmn-id mnc 456
  fqdn ciscosmf1
  service name nsmf-pdu
  type            pdu-session
.
.
.
n4 bind-address ipv4 10.81.70.229
s5 bind-address ipv4 10.81.70.229
http-endpoint base-url http://smf-service
.
.
```

```

.
k8 smf local redis-endpoint redis-primary:6379
k8 smf local service no-of-replicas 1
k8 smf local nodemgr no-of-replicas 1
.
.
.
    
```

# Detach Procedure for EPS on SMF and P-GW

## Feature Description

The SMF supports the default bearer deletion procedures for a UE attached through E-UTRAN, MME, and S-GW.

## How it Works

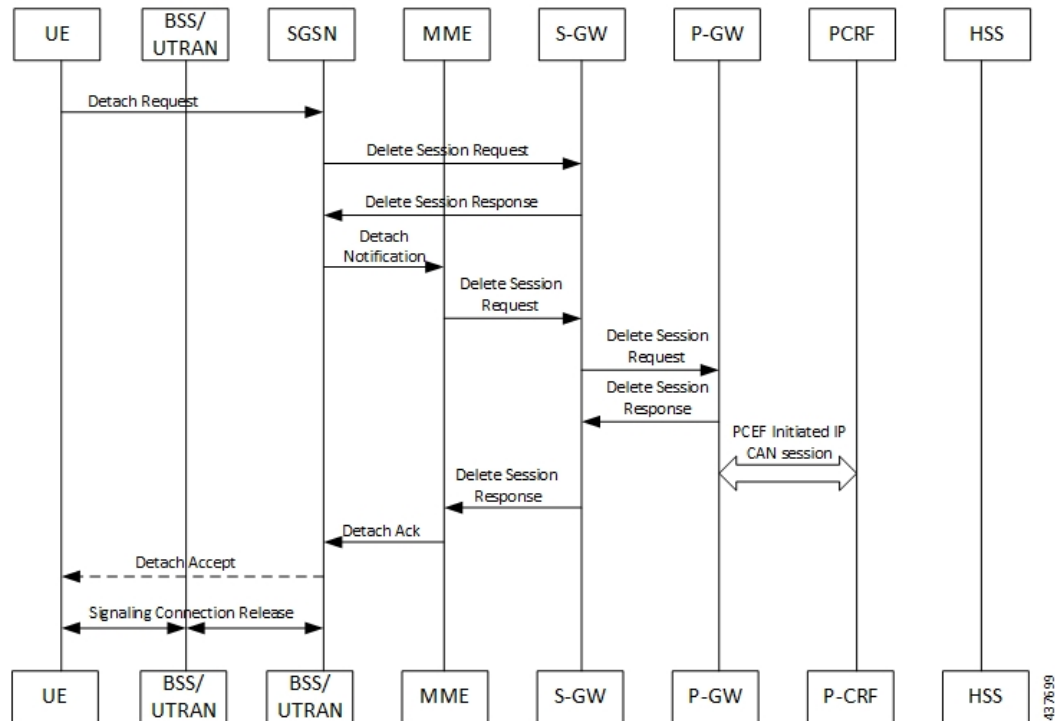
### Call Flows

This section describes the call flows associated with this feature.

#### UE-initiated EPS Call Release Procedure

The following figure shows the call flow for UE-initiated release of EPS call.

**Figure 33: UE-initiated EPS Call Release Flow**



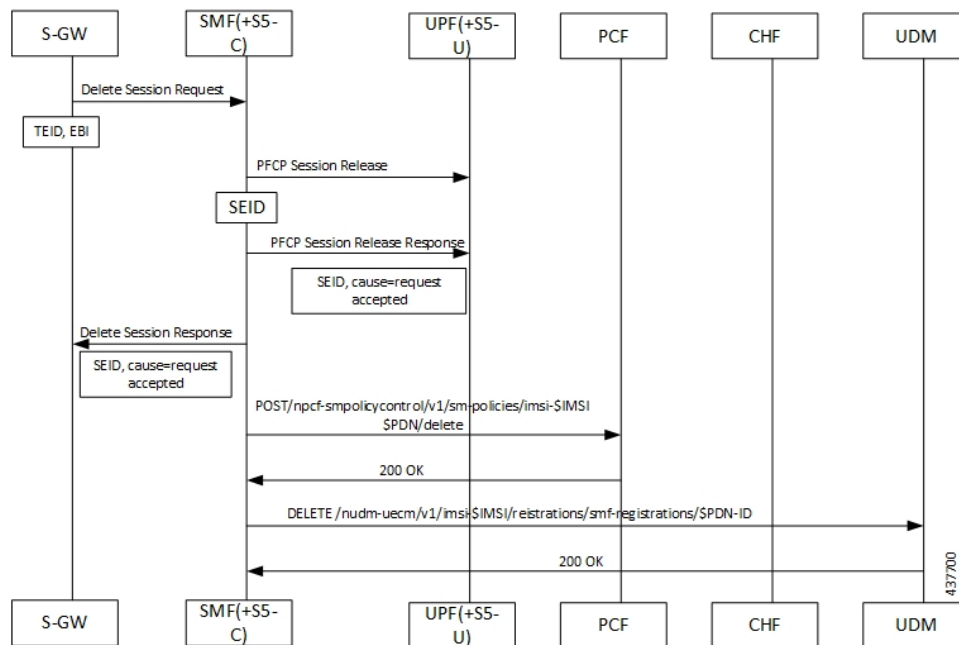
The detach procedures for the EPS are defined in 3GPP 23.401, Section 5.3.8. When the UE is attached to E-UTRAN, the detach procedure remains the same as mentioned in the specified 3GPP section except for the following changes:

- Any interaction towards PCRF (CCR-T), that is PCEF-initiated IP-CAN session between P-GW and PCRF, is replaced by Npcf\_SMPolicyControl\_Update Request from the SMF to the PCF. The parameters sent in this message follow a mapping from Delete Session Request contents in a way similar to the Create Session Request message for initial attach.
- All Gy and Gz interface messages are replaced by Nchf\_ConvergedCharging\_Release service operations.
- The user plane resources are removed using the N4 Session Release procedure towards the UPF.

*UE-initiated Call Release Detail Procedure*

The following figure shows the detailed procedure of UE-initiated release of EPS call.

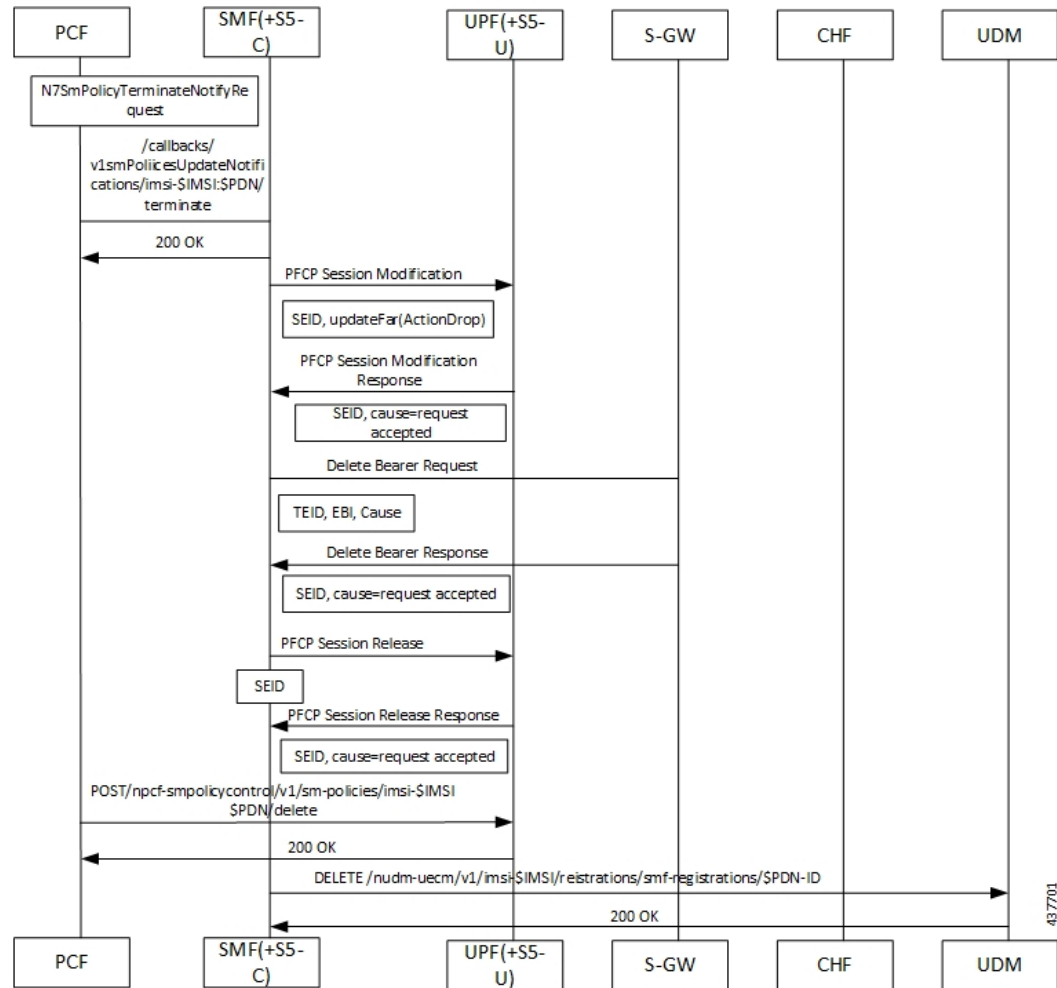
**Figure 34: Detailed Call Flow of UE-initiated EPS Call Release**



*PCF-initiated Call Release Detail Procedure*

The following figure shows the detailed procedure of PCF-initiated release of EPS call.

Figure 35: Detailed Call Flow of PCF-initiated EPS Call Release



437701

# Dedicated Bearer Activation and Deactivation

## Feature Description

SMF supports the PCF-initiated dedicated bearer creation and dedicated bearer deletion procedures for a UE attached via E-UTRAN, MME, and S-GW.

## How it Works

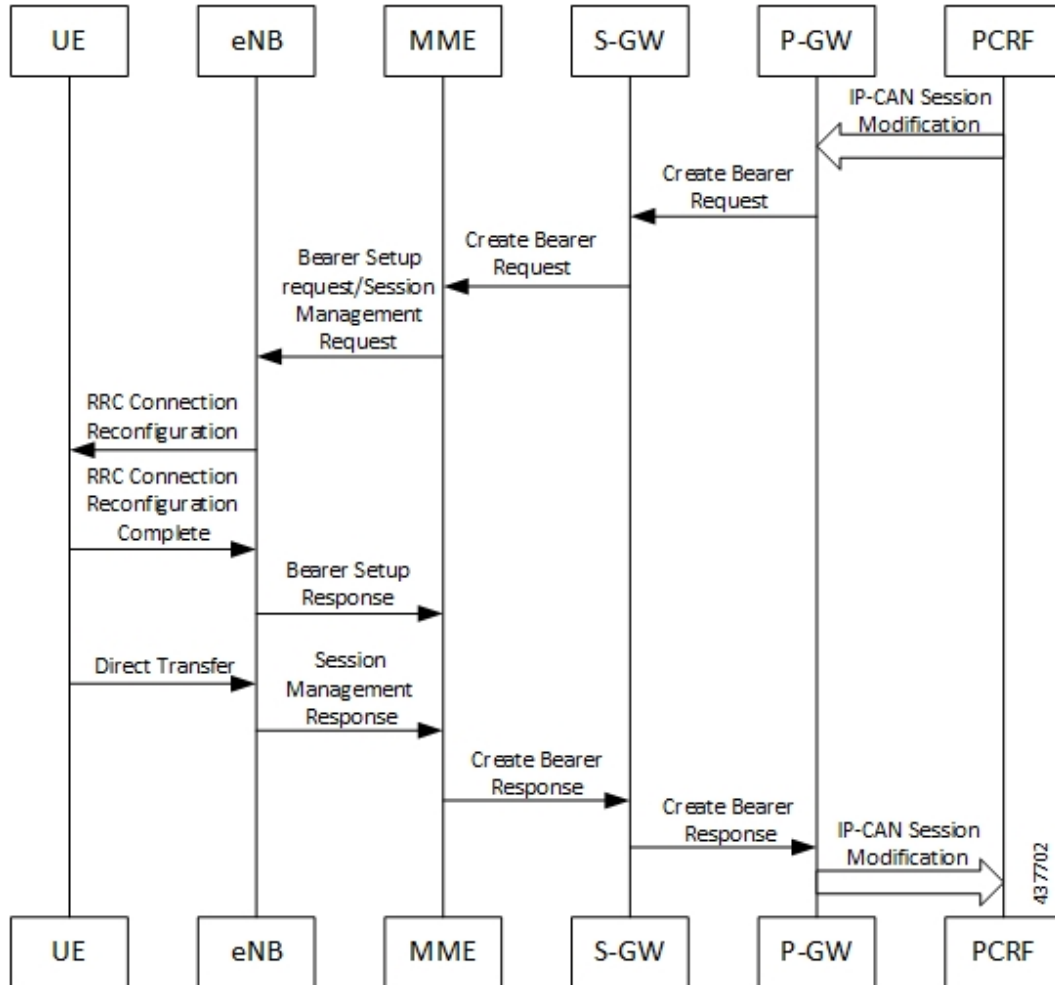
### Call Flows

This section describes the call flows associated with this feature.

Dedicated Bearer Creation Call Flow

The following figure describes the Dedicated Bearer Creation procedure.

Figure 36: Dedicated Bearer Creation Call Flow



The dedicated bearer creation or activation procedure for the EPS session is defined in 3GPP 23.401, Section 5.4.1. When the UE is attached to E-UTRAN, the dedicated bearer procedure remains the same as mentioned in the specified 3GPP section except for the following changes:

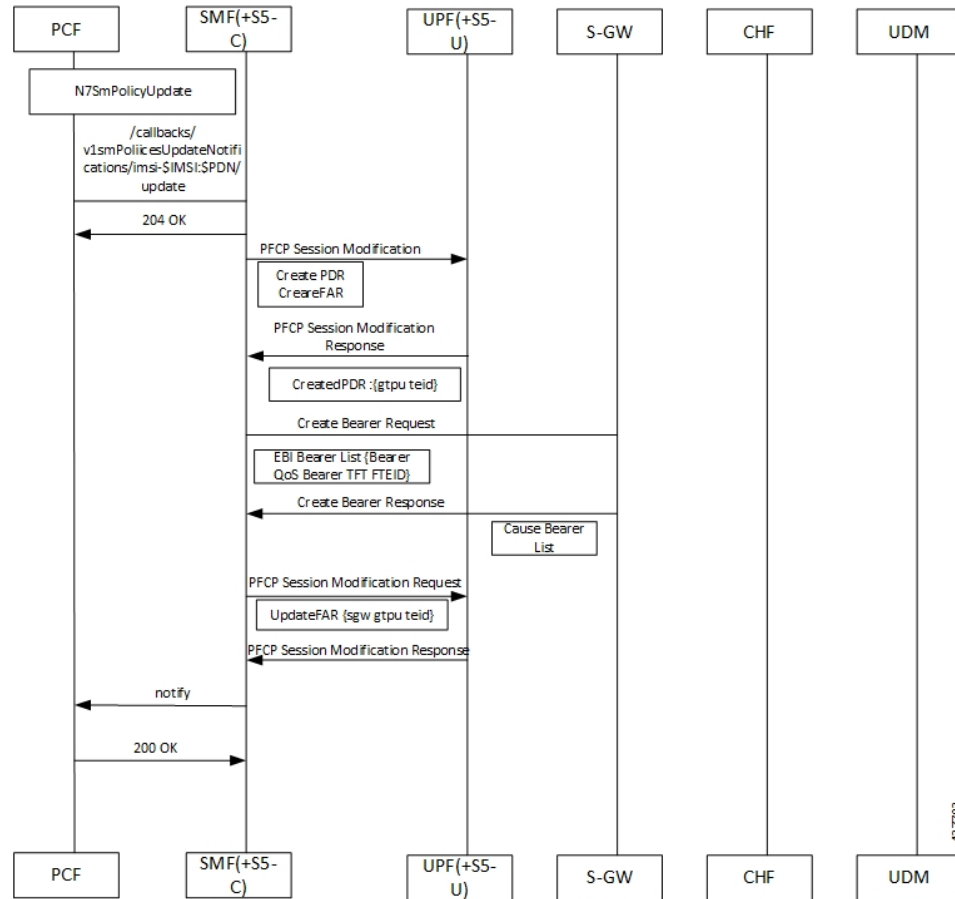
- Any interaction towards the PCRF (RAR from the PCRF or CCR-U to the PCRF) are replaced by Npcf\_SMPolicyControl\_UpdateNotify request from the PCF to the SMF and Npcf\_SMPolicyControl\_Update Request from the SMF to the PCF respectively.
- The PCC rules provided by PCF are mapped to TFTs for the new dedicated bearer and the associated QoS is mapped to 4G QoS as defined in the [Generating EPS PDN Connection Parameters from 5G PDU Session Parameters, on page 285](#).
- All Gy and Gz interface messages are replaced by Nchf\_ConvergedCharging\_Update service operations.
- The user plane resources for dedicated bearers are added using the N4 Session Modification procedure towards UPF where PDRs, QERs and FARs are added for the SDF filters for the new dedicated bearer.



- The SMF+PGW-C saves the EBI for the dedicated bearer as received in Create Bearer response.

The following figure describes the PCF-initiated Dedicated Bearer Activation procedure.

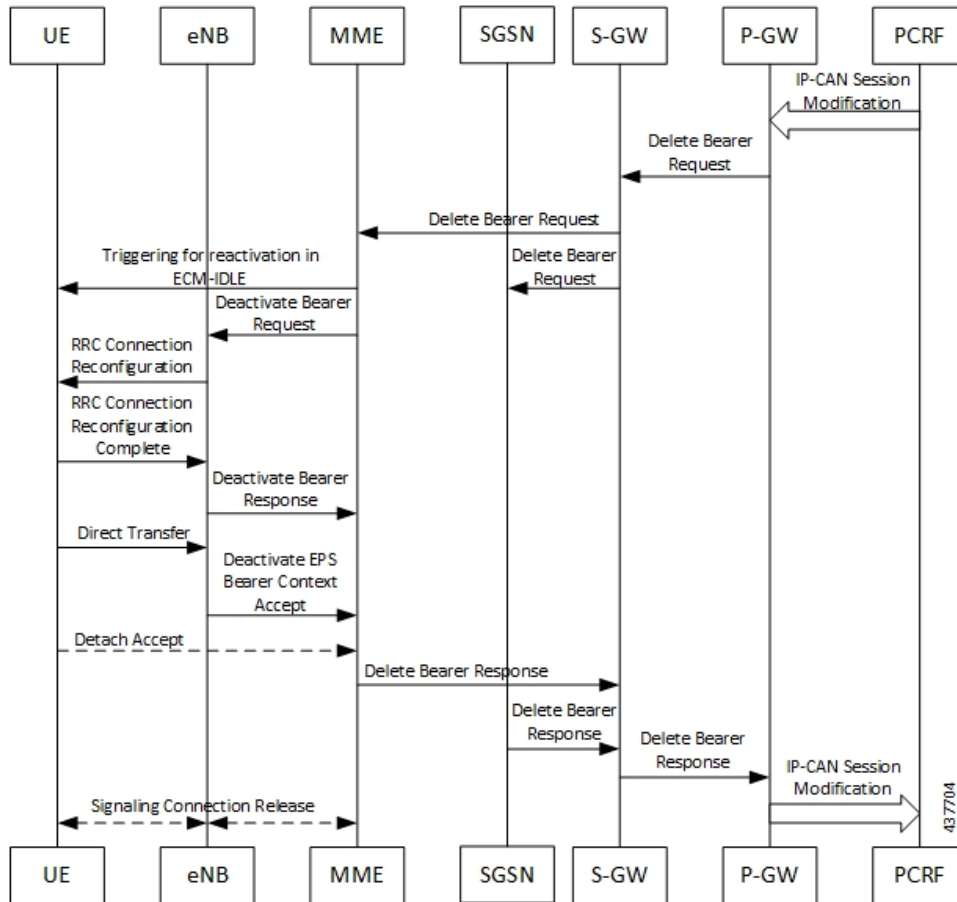
**Figure 37: PCF-initiated Dedicated Bearer Activation**



**Dedicated Bearer Deactivation Call Flow**

The following figure describes the Dedicated Bearer Deactivation procedure.

Figure 38: Dedicated Bearer Deactivation Call Flow



The dedicated bearer deactivation procedure for the EPS session is defined in 3GPP 23.401, Section 5.4.4. When the UE is attached to E-UTRAN, the dedicated bearer procedure remains the same as mentioned in the specified 3GPP section except for the following changes:

- Any interaction towards PCRF (RAR from the PCRF/CCR-U to the PCRF) are replaced by Npcf\_SMPolicyControl\_UpdateNotify request from PCF to the SMF and Npcf\_SMPolicyControl\_Update Request from the SMF to the PCF respectively.
- The PCC rules removed by PCF are mapped to the corresponding dedicated bearers and the bearer deactivation is triggered for these bearers.
- All Gy and Gz interface messages are replaced by Nchf\_ConvergedCharging\_Update service operations.
- The user plane resources for dedicated bearers are removed using the N4 Session Modification procedure towards UPF where PDRs, QERs and Forward Action Rule (FARs) are removed for the SDF filters for the deleted dedicated bearer.

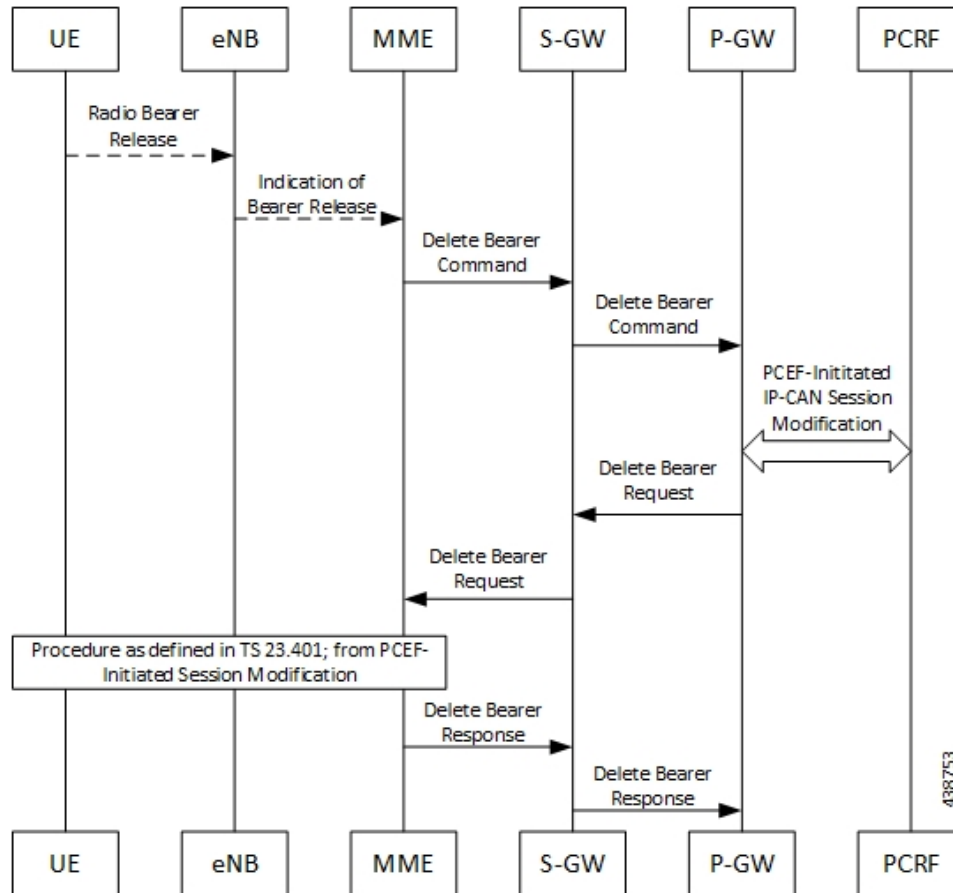
**MME-initiated Dedicated Bearer Deactivation**

The MME uses the UE or MME-requested PDN Disconnection procedure to initiate the release of PDN connections. The following call flow illustrates the procedure in which the dedicated bearers are deactivated.



**Note** The default bearers are not affected during the disconnection process.

**Figure 39: MME-initiated Dedicated Bearer Deactivation**



Step	Description
1	The release of Radio bearers for the UE in the ECM-CONNECTED state occurs due to local reasons such as abnormal resource limitation. The UE deletes the bearer contexts related to the released radio bearers.
2	When the eNodeB releases radio bearers, it sends an indication of bearer release to the MME. This indication could either be the Bearer Release Request (EPS Bearer Identity) message to the MME, or Initial Context Setup Complete, Handover Request Ack and UE Context Response. Path Switch Request can also indicate the release of a bearer. The eNodeB includes the ECGI and TAI in the indication sent to the MME.
3	The MME sends the Delete Bearer Command (EPS Bearer Identity, User Location Information, UE Time Zone, RAN or NAS Release Cause, if available) message per PDN connection to the S-GW to deactivate the selected dedicated bearer. RAN or NAS Release Cause indicates the RAN release cause or the NAS release cause. RAN or NAS Release Cause is only sent by the MME to the P-GW, if permitted according to the MME operator policy.

Step	Description
4	The S-GW sends the Delete Bearer Command (EPS Bearer Identity, User Location Information, UE Time Zone, RAN/NAS Release Cause) message per PDN connection to the P-GW.
5	If the PCC infrastructure is deployed, the P-GW informs the PCRF about the loss of resources by means of a PCEF-initiated IP-CAN Session Modification procedure as defined in 3GPP TS 23.203 and provides the User Location Information, UE Time Zone and RAN or NAS Release cause, if available, received in the Delete Bearer Command from the S-GW if requested by the PCRF as defined in 3GPP TS 23.203. The PCRF sends an updated PCC decision to the P-GW.  <b>Note</b> User Location Information and UE Time Zone may be unavailable if the MME or the S-GW are of a previous release and did not provide this information.
6	The P-GW sends a Delete Bearer Request (EPS Bearer Identity) message to the S-GW.
7	The S-GW sends the Delete Bearer Request (EPS Bearer Identity) message to the MME.
8	This step involves invoking Step 5 through Step 8. Note that these steps are omitted if the bearer deactivation was triggered by the eNodeB in Step 1 and Step 2.  Also, these steps are omitted if the MME initiated bearer release due to failed bearer set up during handover, the UE and the MME deactivate the failed contexts locally without peer-to-peer ESM signaling.
9	The MME deletes the bearer contexts related to the deactivated EPS bearer and acknowledges the bearer deactivation to the S-GW by sending a Delete Bearer Response (EPS Bearer Identity, User Location Information (ECGI)) message.
10	The S-GW deletes the bearer context related to the deactivated EPS bearer and acknowledges the bearer deactivation to the P-GW by sending a Delete Bearer Response (EPS Bearer Identity) message.

### SMF-initiated Dedicated Bearer Deactivation

The following procedure describes the SMF-initiated dedicated bearer deactivation process as defined in 3GPP TS 23.203.

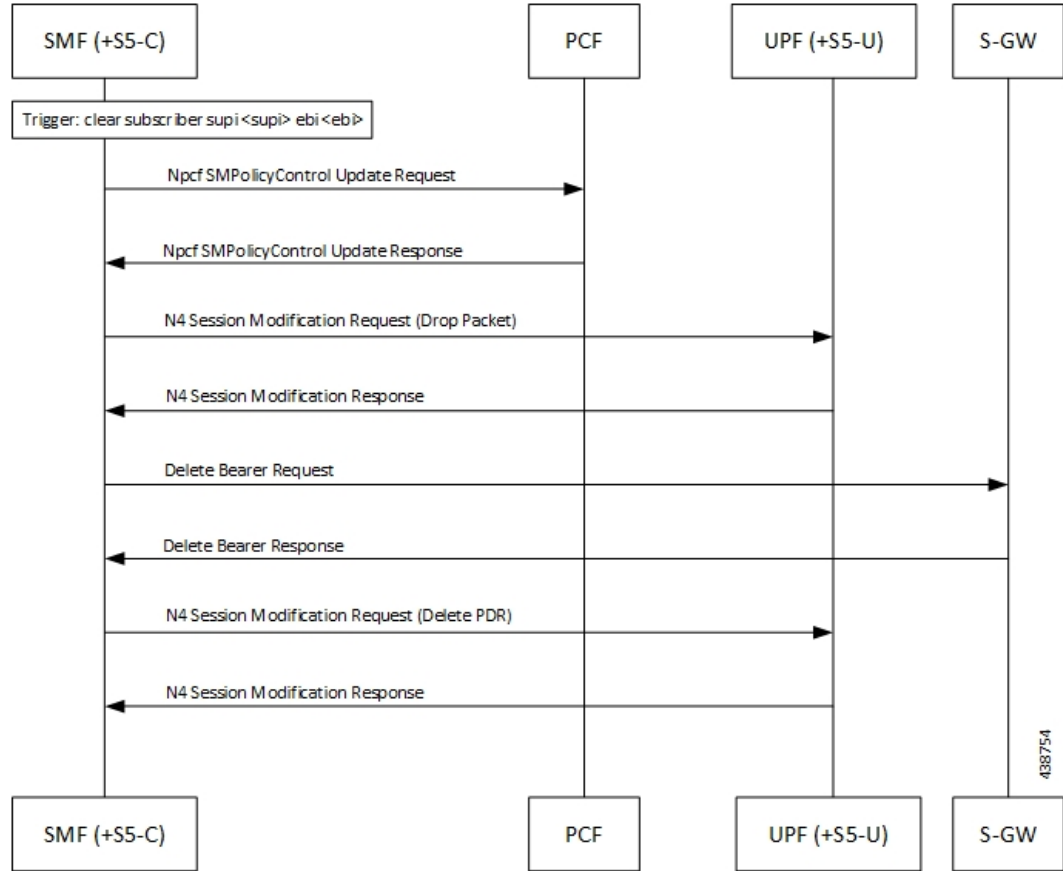


**Note** Default bearers are not affected during the dedicated bearer deactivation process.

- The SMF-initiated delete bearer is triggered using the **clear subscriber** command.
- If the PCC infrastructure is deployed, the P-GW informs the PCRF about the loss of resources by means of a PCEF-initiated IP-CAN Session Modification procedure and provides the User Location Information, UE Time Zone and RAN or NAS Release cause, if available, received in the **clear subscriber** command if requested by the PCRF. The PCRF sends an updated PCC decision to the P-GW.
- The P-GW sends a Delete Bearer Request (EPS Bearer Identity) message to the S-GW.
- The S-GW deletes the bearer context related to the deactivated EPS bearer and acknowledges the bearer deactivation to the P-GW by sending a Delete Bearer Response (EPS Bearer Identity) message.

The following call flow illustrates the SMF-initiated dedicated bearer deactivation.

Figure 40: SMF-initiated Dedicated Bearer Deactivation



# EPS Fallback

## Feature Description

SMF supports fallback to EPS from 5GC for IMS sessions if gNB rejects the dedicated bearer creation with ims-voice-eps-fallback or rat-fallback triggered.

For the UE devices not supporting VoNR, the SMF performs a fallback to EPS for voice calls. This includes 5G to EPS handover and dedicated bearer creation in 4G for voice call.

## How it Works

### Call Flows

The following call flow depicts the EPS Fallback procedure.

Figure 41: EPS Fallback Call Flow

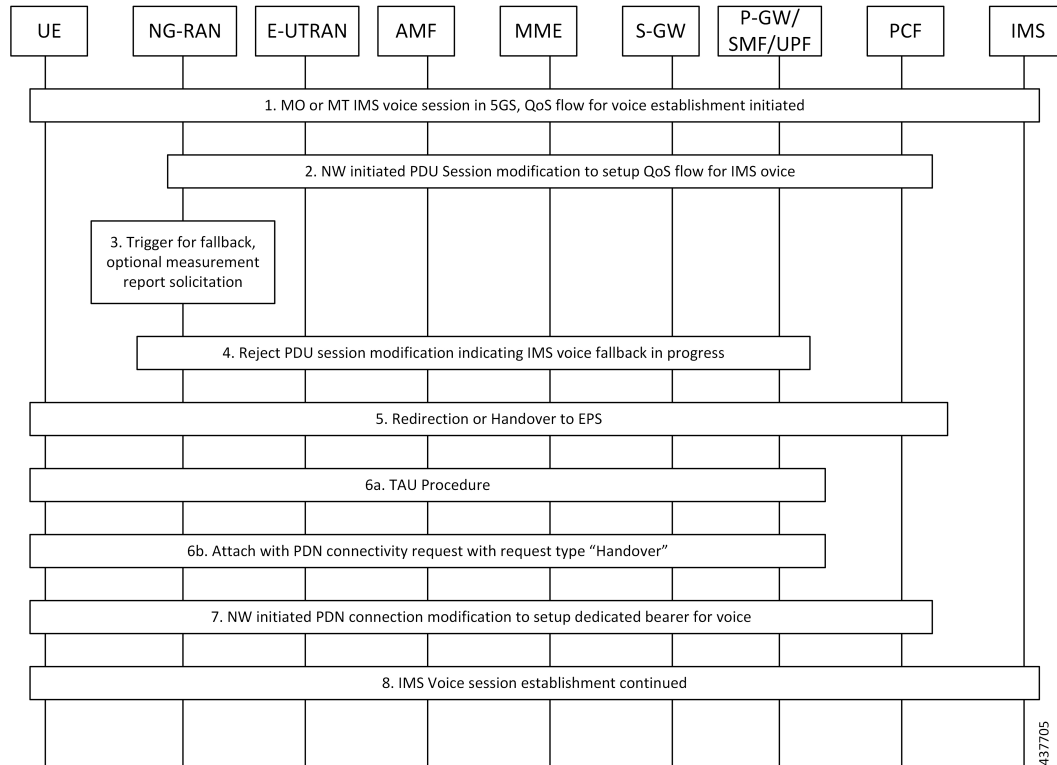


Table 83: EPS Fallback Call Flow Description

Step	Description
1	The UE initiates Mobile-Originated (MO) or a Mobile-Terminated (MT) IMS voice establishment procedure with NG-RAN in 5GS.
2	The Network-initiated PDU Session modification request to setup QoS flow for voice reaches the NG-RAN.
3	The NG-RAN is configured to support the EPS fallback for IMS voice. Based on the UE functionalities, indication from the AMF to redirect EPS fallback for voice, network configuration, and radio conditions, the NG-RAN triggers fallback to EPS. If the NG-RAN determines to not trigger the fallback to EPS, then the procedure stops, and the following steps are not performed.  The NG-RAN initiates measurement report solicitation from the UE including E-UTRAN as target.

Step	Description
4	<p>The NG-RAN rejects the PDU Session modification request received in Step 2 with an indication that mobility due to fallback for IMS voice is ongoing.</p> <p>The NG-RAN indicates the rejection of the PDU session modification to configure QoS flow for IMS voice that is received in Step 2 as PDU Session Response message toward the SMF through the AMF. This message includes the details on the ongoing mobility due to fallback for IMS voice. The SMF maintains the PCC rules that are associated with the QoS flows.</p> <p>For a roaming scenario, the PDU Session Response message is sent toward H-SMF through V-SMF.</p>
5	<p>Based on the UE functionalities, the NG-RAN initiates handover to the EPS. The SMF reports change of the RAT type, if the PCF is subscribed for it.</p> <p>A timer starts to track failure in the EPS fallback. After the timer expires, the SMF notifies the PCF about the dedicated bearer creation failure and new statistics, with the “smf_eps_fb” and “timeout” labels, is incremented.</p>
6a	For 5GS to EPS handover, the UE initiates TAU procedure.
6b	The UE attaches the PDN connectivity request with the “handover” request type.
7	After the completion of the 5GS to EPS handover procedure, the SMF or P-GW re-initiates the configuration of the dedicated bearer for IMS voice and mapping the 5G QoS to EPC QoS parameters. The SMF notifies about the Successful Resource Allocation and Access Network Information, if the PCF is subscribed for it.
8	The IMS voice session establishment continues.

## EPS Fallback Guard Timer Support

### Feature Description

SMF supports the guard timer to track failure in the EPS fallback. After the timer starts, it waits for the EPS fallback to happen before the bearer creation failure information is communicated to PCF.

### How It Works

The EPS fallback timer starts after receiving the notification for dedicated bearer creation failure with the EPS fallback cause from gNB through AMF. In this case, SMF does not send the failure notification to PCF and waits for 5G to 4G handover to complete. Then, SMF triggers the bearer creation in 4G. The EPS fallback timer stops on the completion of the 5G to 4G handover.

In case the timer expires before the completion of the 5G to 4G handover, SMF sends a notification for dedicated bearer creation failure to PCF. Then, the new statistics counter, with the “smf\_eps\_fb” and “timeout” labels, is incremented. However, the 5G to 4G handover procedure continues.

### Call Flows

This section includes the following call flow.

EPS Fallback Guard Timer Call Flow

This section describes the 5G to EPS fallback guard timer call flow.

Figure 42: EPS Fallback Guard Timer Call Flow

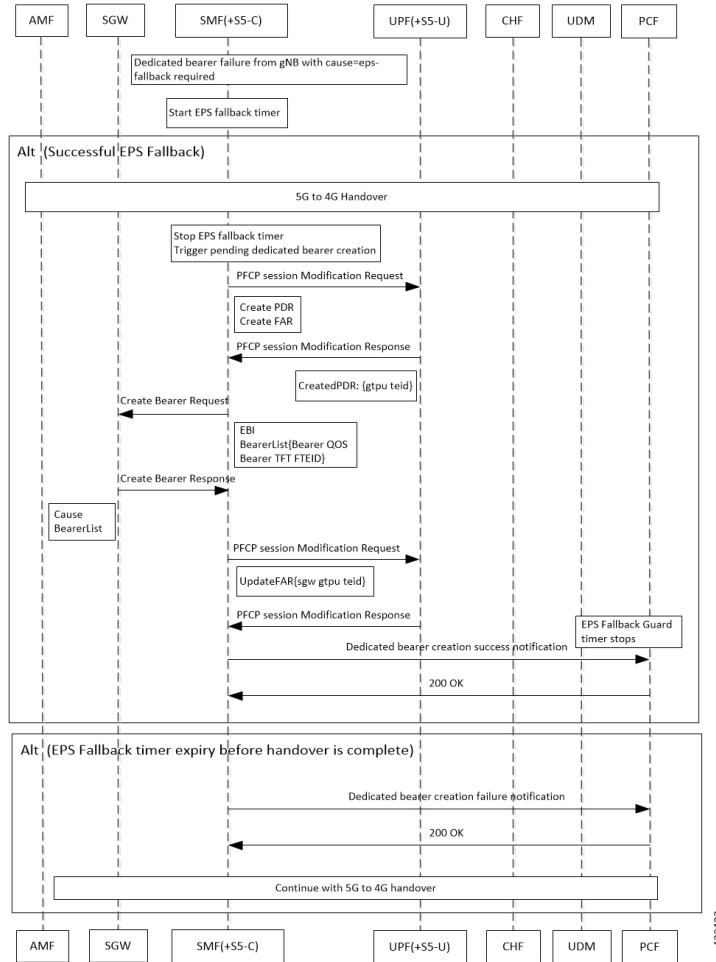


Table 84: EPS Fallback Guard Timer Call Flow Description

Step	Description
1	gNB sends the dedicated bearer creation failure information with the fallback cause through AMF.
2	EPS fallback timer starts.
In the successful EPS fallback with 5G to 4G handover scenario, Steps 3 –12 happen.	
3	EPS fallback timer stops and triggers pending dedicated bearer creation.
4	SMF(+S5-C) sends the PCFP session modification request to UPF(+S5-U).
5	PDR and FAR are created.
6	UPF(+S5-U) sends the PCFP session modification response to SMF(+S5-C).
7	The information on the created PDR with the GTP-U TEID is available.



Step	Description
8	SMF(+S5-C) sends the Create Bearer Request to SGW.
9	SGW sends the Create Bearer Response to SMF(+S5-C).
10	SMF(+S5-C) sends the PFCP Session Modification Request to UPF(+S5-U).
11	UPF(+S5-U) sends the notification of the successful dedicated bearer creation to PCF.
12	EPS fallback guard timer stops.
13	PCF sends the “200 OK” acknowledgment to SMF(+S5-C)
In the EPS fallback timer expiry before handover completion scenario, Steps 14–16 happen.	
14	SMF(+S5-C) sends the failure notification of the dedicated bearer creation to PCF.
15	PCF sends the “200 OK” acknowledgment to SMF(+S5-C).
16	The 5G to 4G handover procedure continues.

## Standards Compliance

The EPS fallback guard timer support feature complies with the following standards:

- *3GPP TS 23.502 V16.1.1 (2019-06)*

## Configuring the EPS Fallback Guard Timer

This section describes how to configure the EPS Fallback Guard Timer feature.

### configure

```
profile access test [ eps-fallback | n2 | n26 ]
  eps-fallback guard timeout timeout_value
  n26 idft enable timeout n26_timeout_value
  n2 idft enable timeout n2_timeout_value
end
```

### NOTES:

- **profile access:** Accesses the profile configuration.
- **test:** Accesses the profile instance.
- **eps-fallback:** Enters the EPS fallback configuration.
- **eps-fallback guard timeout:** Enters the value for the EPS fallback timer from the range of 500 to 15000 milliseconds.
- **n26:** Enters the N26 interface, which is the E-UTRAN and NG-RAN configuration.
- **n2:** Enters the N2 interface, which is the NG-RAN configuration.
- **idft enable timeout:** Enters the value from 15 to 60 for the IDFT timer to expire.

# Indirect Data Forwarding Tunnel (IDFT) Timer Support

## Feature Description

SMF supports the Indirect Data Forwarding Tunnel (IDFT) timer during the IDFT procedures for 5G to 4G handover. During the handover, the IDFT tunnels of 5G are released. SMF receives the NSMF PDU Session Update SM Context Request to release the forwarding tunnels from AMF. When SMF does not receive this request, the IDFT timer ensures the release of unused tunnels.

## How it Works

### Call Flows

This section includes the following call flow.

#### 5G to EPS Handover with IDFT Timer Call Flow

This section describes the 5G to EPS handover with IDFT timer call flow.

Figure 43: 5G to EPS Handover with IDFT Timer Call Flow

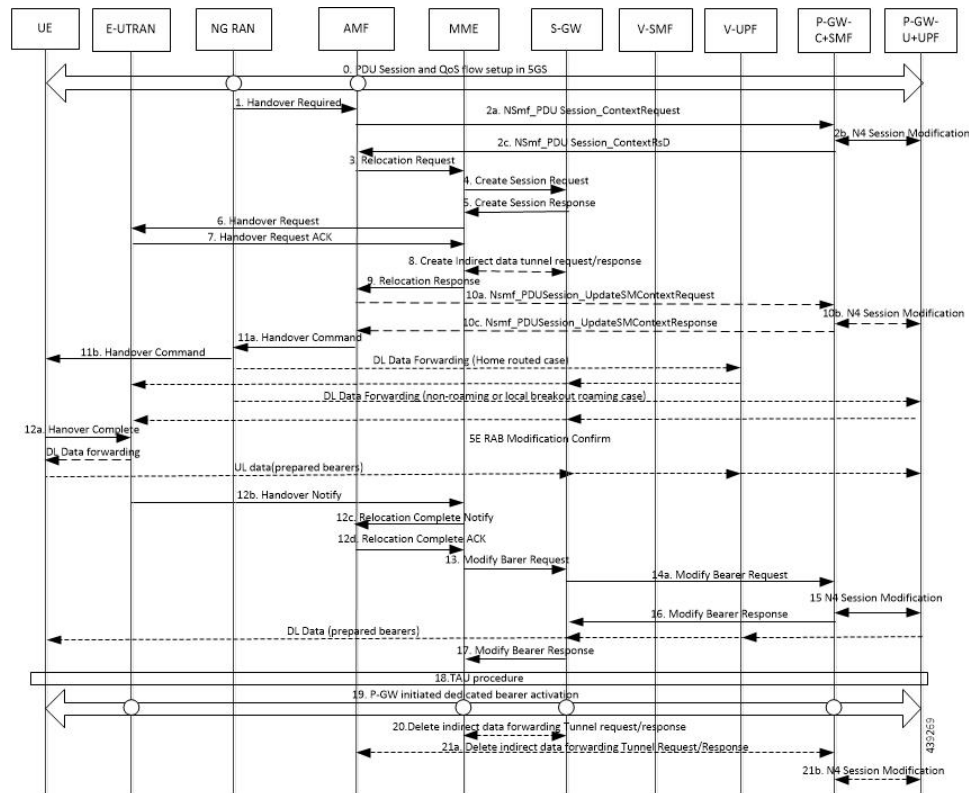


Table 85: 5G to EPS Handover with IDFT Timer Call Flow Description

Step	Description
1	NG-RAN determines to handover UE to E-UTRAN. If NG-RAN is configured to perform inter-RAT mobility due to the IMS voice fallback that is triggered by QoS flow setup and request to set up QoS flow for IMS voice is received, then NG-RAN indicates the rejection of the QoS flow establishment. This indication is because of mobility due to fallback for the IMS voice through N2 SM information and triggers the handover to E-UTRAN. The NG-RAN sends a Handover Required message to the AMF. This message includes the details on target eNB ID, direct forwarding path availability, source to target transparent container, and inter-system handover indication. NG-RAN uses the source to target transparent container to indicate bearers for the corresponding 5G QoS flows for data forwarding.
2a	AMF sends the NSMF PDU Session Context Request to the SMF+PGW-C to provide SM Context.
2b	<p>SMF+PGW-C sends the N4 session modification to PGW-U+UPF to establish the CN tunnel for each EPS bearer. The bearer mapping to the 5G QoS and PCC rules, which PCC sends, are available in the SMF. The SMF also has the bearer IDs that are received from the bearer ID allocation procedure. The SMF+PGW-C creates new PDRs for the N4 session and gets the TEID allocated for each bearer as required by the 4G system.</p> <p>The timer in SMF+PGW-C starts in this step. This timer monitors the resources for indirect data forwarding in UPF that are to be released.</p> <p>Following are the cases for the IDFT timer expiry:</p> <ul style="list-style-type: none"> <li>• Step 21a does not happen and the timer expires—The PDRs and FARs that are not required for the indirect tunnels, are removed before Step 21a.</li> <li>• The timer expires before or during the Steps 14a and 16—The PDRs and FARs that are not required for the indirect tunnels, are removed and the call flow continues independently.</li> <li>• Step 21a happens after the timer expiry—The SMF does not send the N4 Modification Request to UPF+PGW-U as the resources are released on the timer expiry.</li> </ul>
2c	<p>SMF+PGW-C sends the EPS bearer contexts to AMF. The bearer context is a string with the byte format, which is the base64-encoded characters, encoding the UE EPS PDN Connection IE.</p> <p>The SMF+PGW-C also provides the CN tunnel information to AMF for all the bearers for the uplink traffic from E-UTRAN.</p>
3	AMF sends a Forward Relocation Request to MME. The AMF includes the mapped SM EPS UE Contexts for the PDU Sessions with and without active UP connections.
4	MME sends the Create Session Request to SGW. See S1-based handover in the normal case section in <i>3GPP TS 23.401, clause 5.5.1.2.2</i> for details.
5	SGW sends the Create Session Response to MME. See S1-based handover in the normal case section in <i>3GPP TS 23.401, clause 5.5.1.2.2</i> for details.
6	MME sends the handover request to E-UTRAN.
7	E-UTRAN sends the handover request acknowledgment to MME.
8	MME and SGW send and receive the indirect data forwarding request and response to each other.
9	MME sends the Relocation Response to AMF.

Step	Description
10a	In case of indirect data forwarding, AMF sends the NSMF PDU Session Update SM Context Request to PGW-C+SMF. This request is for SGW addresses and SGW DL TEIDs for data forwarding and for creating the indirect data forwarding tunnel.
10b	PGW-C+SMF sends the N4 Modification Request to UPF+PGW-U to create more PDRs and FARS. The PDRs and FARS are created to receive the redirected DL data over the indirect tunnel from NG RAN and to forward them to eNodeB. The UL PDRs have the QFI to match the forwarded DL data from NG RAN. The associated QER has the QFI to forward the data to eNodeB. Also, the FAR redirects the received data to eNodeB over the appropriate tunnel based on the QFI.
10c	PGW-C+SMF sends the NSMF PDU Session Update SM Context Response to AMF. This response includes details on cause, CN tunnel information for data forwarding, and QoS flows for data forwarding. PGW-C+SMF sends this response to create indirect data forwarding. Based on the correlation between QFIs and SGW addresses and TEIDs for data forwarding, the PGW-U+UPF maps the QoS flows into the data forwarding tunnels in EPC.
11a	AMF sends the Handover Command to the source NG-RAN.
11b	The source NG-RAN sends the Handover Command to UE to handover to the target access network. The UE correlates the ongoing QoS Flows with the indicated EPS Bearer IDs (EBI) that are to be set up in the handover command. If the QoS Flow associated with the default QoS rule in the PDU Session has an unassigned EBI, the UE deletes the PDU Session locally. If the QoS Flow that is associated that is with the default QoS rule has an assigned EBI, the UE retains the PDU session. For the QoS Flow with unassigned EBIs, the UE deletes the QoS rules and the QoS Flow level QoS parameters locally if any associated with those QoS Flows. Then, the UE notifies the impacted applications that the dedicated QoS resource has been released. The UE deletes any UE-derived QoS rules. The EBI that was assigned for the QoS Flow of the default QoS rule in the PDU Session becomes the EBI of the default bearer in the corresponding PDN connection.
12a	UE sends the notification of handover completion to E-UTRAN.
12b	E-UTRAN sends the Handover Notify request to MME.
12c	MME sends the Relocation Complete Notification to AMF.
12d	AMF sends the Relocation Complete Notification acknowledgment to MME.
13	MME sends the Modify Bearer Request to SGW.
14a	SGW sends the Modify Bearer Request to SMF+PGW-C. This request includes the information on DL TEIDs on SMF for the bearers.
15	PGW-C+SMF initiates a N4 Session Modification procedure toward the UPF+PGW-U to update the User Plane path, which implies that DL User Plane for the indicated PDU Session is switched to E-UTRAN. The PGW-C+SMF releases the resource of the CN tunnel for PDU Session in UPF+PGW-U.

Step	Description
16	<p>PGW-C+SMF sends Modify Bearer Response to SGW. At this stage, the User Plane path is established for the default bearer and the dedicated EPS bearers between the UE, target eNodeB, SGW, and the PGW-U+UPF. The PGW-C+SMF uses the EPS QoS parameters as assigned for the dedicated EPS bearers during the QoS Flow establishment. PGW-C+SMF maps all the other IP flows to the default EPS bearer.</p> <p>If indirect forwarding tunnels are established, the PGW-C+SMF starts a timer to release the resources that are used for indirect data forwarding.</p>
17	SGW sends Modify Bearer Response to MME.
18	<p>UE initiates a Tracking Area Update procedure. See the S1-based handover in the normal case section in <i>3GPP TS 23.401, clause 5.5.1.2.2</i> for details.</p> <p>This procedure deregisters the old AMF for 3GPP access from HSS+UDM. Any registration that is associated with the non-3GPP access in the old AMF is not removed. It implies that an AMF that is serving the UE over both the 3GPP and non-3GPP accesses does not consider the UE as deregistered over non-3GPP access and remains registered and subscribed to subscription data updates in UDM.</p>
19	If PCC is deployed, then PCF determines to provide the earlier removed PCC rules to the PGW-C+SMF again. With these PCC rules, the PGW-C+SMF initiates the dedicated bearer activation procedure.
20	SGW sends the Delete Indirect Data Forwarding Tunnel Request to MME. The MME sends the Delete Indirect Data Forwarding Tunnel Response to SGW.
21a	AMF initiates NSMF PDU Session Update SM Context Request service operation with an indication to release the forwarding tunnels.
21b	SMF sends the N4 Modification Request to UPF+PGW-U to delete the PDRs and FARs for the indirect tunnels. The PDRs and FARs for the 5G session which are not required are also removed. The IDFT timer that started in Step 2b stops.

## Standards Compliance

The IDFT timer support feature complies with the following standards:

- *3GPP TS 23.502 V16.1.1 (2019-06)*
- *3GPP TS 23.401 version 12.6.0 Release 12*

## Configuring the IDFT Timer

This section describes how to configure the IDFT timer.

### configure

```

profile access test [ eps-fallback | n2 | n26 ]
eps-fallback guard enable timeout timeout_value
n26 idft enable timeout n26_timeout_value
n2 idft enable timeout n2_timeout_value

```

```

    end
exit

```

**NOTES:**

- **profile access:** Accesses the profile configuration.
- **test:** Accesses the profile instance.
- **eps-fallback:** Enters the EPS fallback configuration.
- **n26:** Enters the N26 interface, which is the E-UTRAN and NG-RAN configuration
- **n2:** Enters the N2 interface, which is the NG-RAN configuration.
- **idft enable timeout:** Enters the value from 15 to 60 for the IDFT timer to expire.

# Bearer Modification for EPS Session on SMF

## Feature Description

SMF supports modification of EPS bearer that a PCF or an MME initiates. The SMF+PGW handles the following triggers for this feature:

- QoS modifications.
- RAT, ULI, and SGW modifications.
- UE time zone modifications.

## How it Works

The bearer modification for an EPS session on SMF works with the following modifications:

- **PCF and MME-Initiated Bearer Modifications for EPS session on SMF**—These procedures are used either when one or multiple EPS Bearer QoS parameters QCI, GBR, MBR, or ARP are modified or to modify the APN-AMBR. The PCF-initiated or the MME-initiated bearer modification procedures do not support the modification from a QCI of non-GBR resource type to a GBR resource type QCI and vice versa.
- **X2 and S1 Based Handover for EPS Session Connected to SMF**—The X2-based handover procedure is used to hand over a UE from a source eNodeB to a target eNodeB using X2. In this procedure, the MME is unchanged and the MME determines to relocate the SGW.

The S1-based handover procedure is used when the X2-based handover cannot be used. The source eNodeB initiates a handover by sending the Handover Required message over the S1-MME reference point. This procedure may relocate the MME or the SGW.

## Call Flows

This section includes the following call flows:

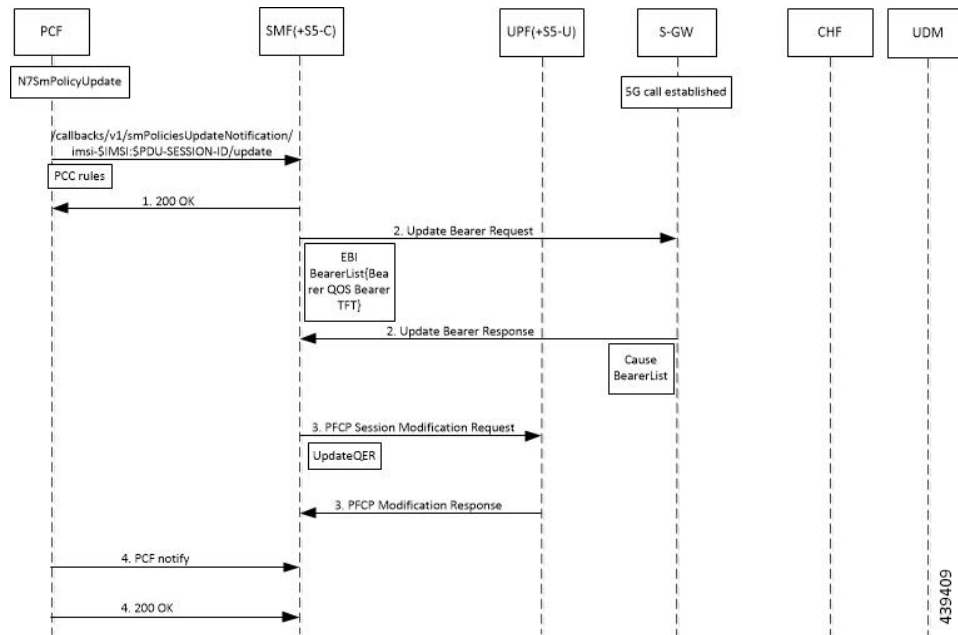
- PCF-Initiated Bearer Modification for EPS session on SMF call flow

- MME-Initiated Bearer Modification for EPS session on SMF call flow
- X2 and S1 Based Handover for EPS Session Connected to SMF call flow

*PCF-initiated Bearer Modification for EPS session on SMF Call Flow*

This section describes the PCF-Initiated Bearer Modification for EPS session on SMF call flow.

**Figure 44: PCF-Initiated Bearer Modification for EPS session on SMF Call Flow**



**Table 86: PCF-Initiated Bearer Modification for EPS session on SMF Call Flow Description**

Step	Description
1	PCF initiates the N7 Policy Update Notify with the updated parameters of QoS or TFT toward SMF.
2	SMF sends the “200 OK” acknowledgment to PCF. The PCC rules that the PCF provides are mapped to TFTs for the modified dedicated bearer. The associated QoS is mapped to 4G QoS.
3	SMF sends the Update Bearer Request to SGW.
4	SGW sends the Update Bearer Response to SMF with EPS Bearer ID and the modified QoS or TFT for the associated bearer.
5	SMF initiates the PFCP Modification request toward UPF.
6	UPF sends the PFCP Modification Response to SMF with updated QER.
7	SMF sends the PCF Notify message to PCF.
8	PCF sends the “200 OK” acknowledgment to SMF.

*MME-initiated Bearer Modification for EPS session on SMF Call Flow*

This section describes the MME-Initiated Dedicated Bearer Modification for EPS session on SMF call flow.

Figure 45: MME-Initiated Bearer Modification for EPS session on SMF Call Flow

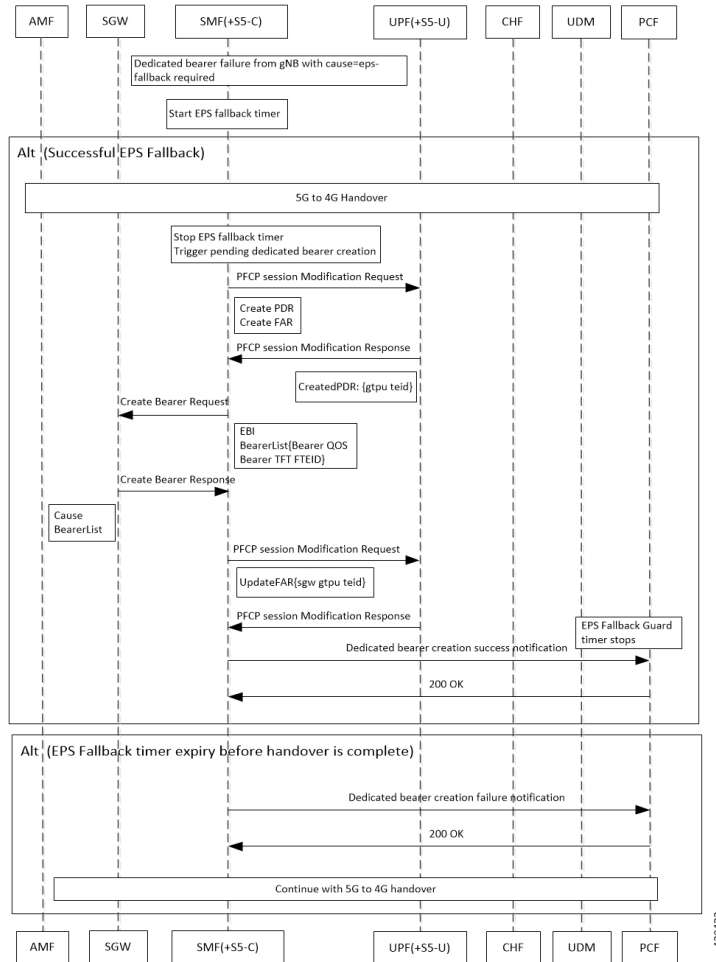


Table 87: MME-Initiated Bearer Modification for EPS session on SMF Call Flow Description

Step	Description
1	HSS sends an Insert Subscriber Data message to the MME. The subscription data includes the details on IMSI, EPS subscribed QoS (QCI and ARP), and the subscribed UE-AMBR and APN-AMBR.
2	If the subscribed UE-AMBR is modified, the MME calculates a new UE-AMBR value and sends the Modify Bearer Command to SGW.
3	SGW sends the Modify Bearer Command message to the SMF or PDN GW. This message includes the details on EPS Bearer Identity, EPS Bearer QoS, and APN-AMBR.
4	SMF or PDN GW sends the updated APN-AMBR to PCF.
5	PCF sends the updated PCC decision to the SMF or PDN GW. The PCF modifies the APN-AMBR that is associated with the default bearer in response to the SMF or PDN GW.
6	SMF sends the Update Bearer Request to SGW.

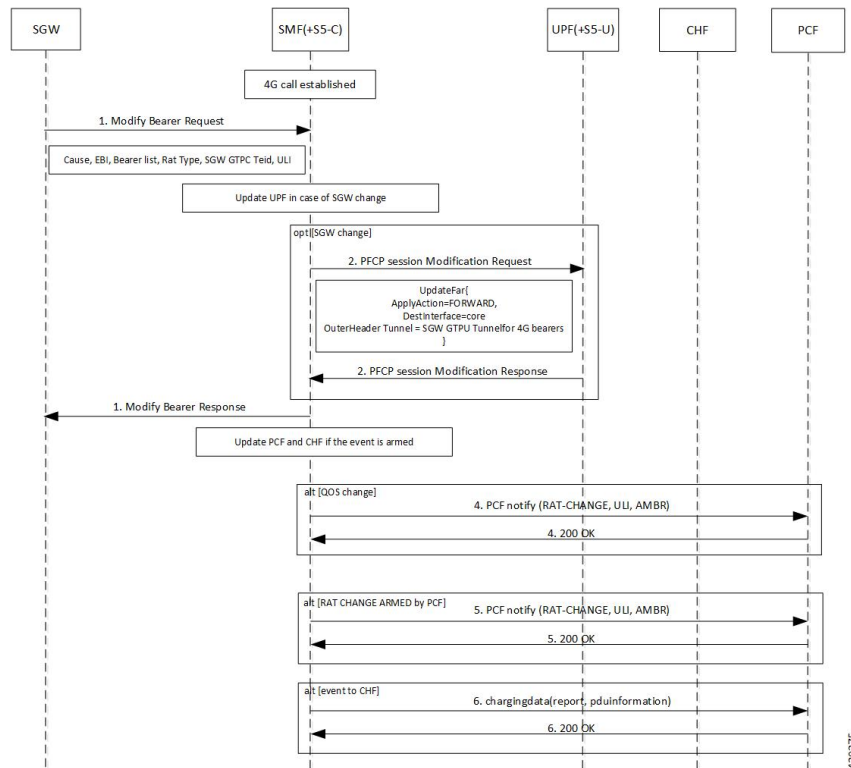


Step	Description
7	SGW sends the Update Bearer Request to MME. This request message includes the details on EBI, EPS Bearer QoS, TFT, and APN-AMBR.
8	MME sends the Update Bearer Response to SGW.
9	SGW sends the Update Bearer Response as acknowledgment for the bearer modification to the SMF or PDN GW. The response message includes the details on EBI and user location information.
10	UPF sends the PFCP Session Modification Response to SMF. Based on the PCC decision provision message (QoS policy) that is received from the PCF, the SMF or PDN GW initiates the dedicated bearer modification procedure. SMF or PDN GW uses the QoS policy to determine if a service data flow is to be added or removed from an active bearer or if the authorized QoS of a service data flow is changed.
11	UPF updates the PFCP parameters and sends a PFCP Session Modification Response to the SMF or PDN GW. UPF confirms the successful modification of the PFCP session.
12	SMF or PDN GW notifies PCF on the requested PCC decision whether it was enforced or not.
13	PCF sends the “200 OK” acknowledgment to SMF or PDN GW.

*X2 and S1 based Handover for EPS Session Connected to SMF*

This section describes the X2 and S1-Based Handover for EPS Session Connected to SMF.

**Figure 46: X2 and S1 based Handover for EPS Session Connected to SMF**

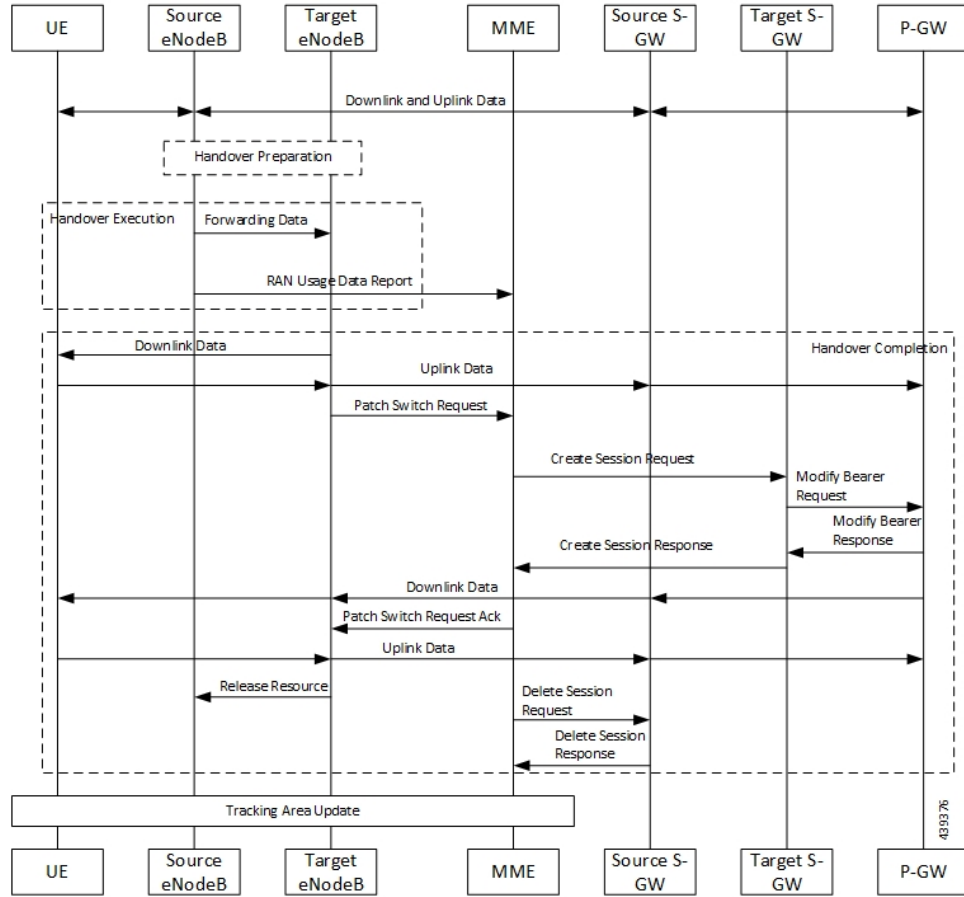


**Table 88: X2 and S1 based Handover Call Flow Description**

Step	Description
1	The SGW sends the Modify Bearer Request to the SMF. This request includes the user location information IE, UE time zone IE, and the serving network IE per PDN connection to the associated PDN GWs information that is received from the MME.
2	In case of change in S-GW, SMF or P-GW sends the PFCP Session Modification Request to the UPF.
3	If Step 2 occurs, the UPF sends the PFCP Session Modification Response to SMF or PDN GW.
4	After receiving the response from the UPF, the SMF or P-GW sends the Modify Bearer Response to S-GW.
5	If PCF has armed notification for QoS modification, the SMF or P-GW sends a notification to the PCF.
6	If Step 5 occurs, the PCF sends the “200 OK” acknowledgment to the SMF or P-GW.
7	If PCF has armed notification for ULI or RAT modifications, SMF or PDN GW sends a notification to PCF.
8	If Step 7 occurs, PCF sends the “200 OK” acknowledgment to SMF or PDN GW.
9	If CHF has armed notification for QoS, ULI, or RAT modifications, SMF or PDN GW sends a notification to PCF.
10	If Step 9 occurs, PCF sends the “200 OK” acknowledgment to SMF or PDN GW.

The following call flow shows the X2-based handover with S-GW relocation:

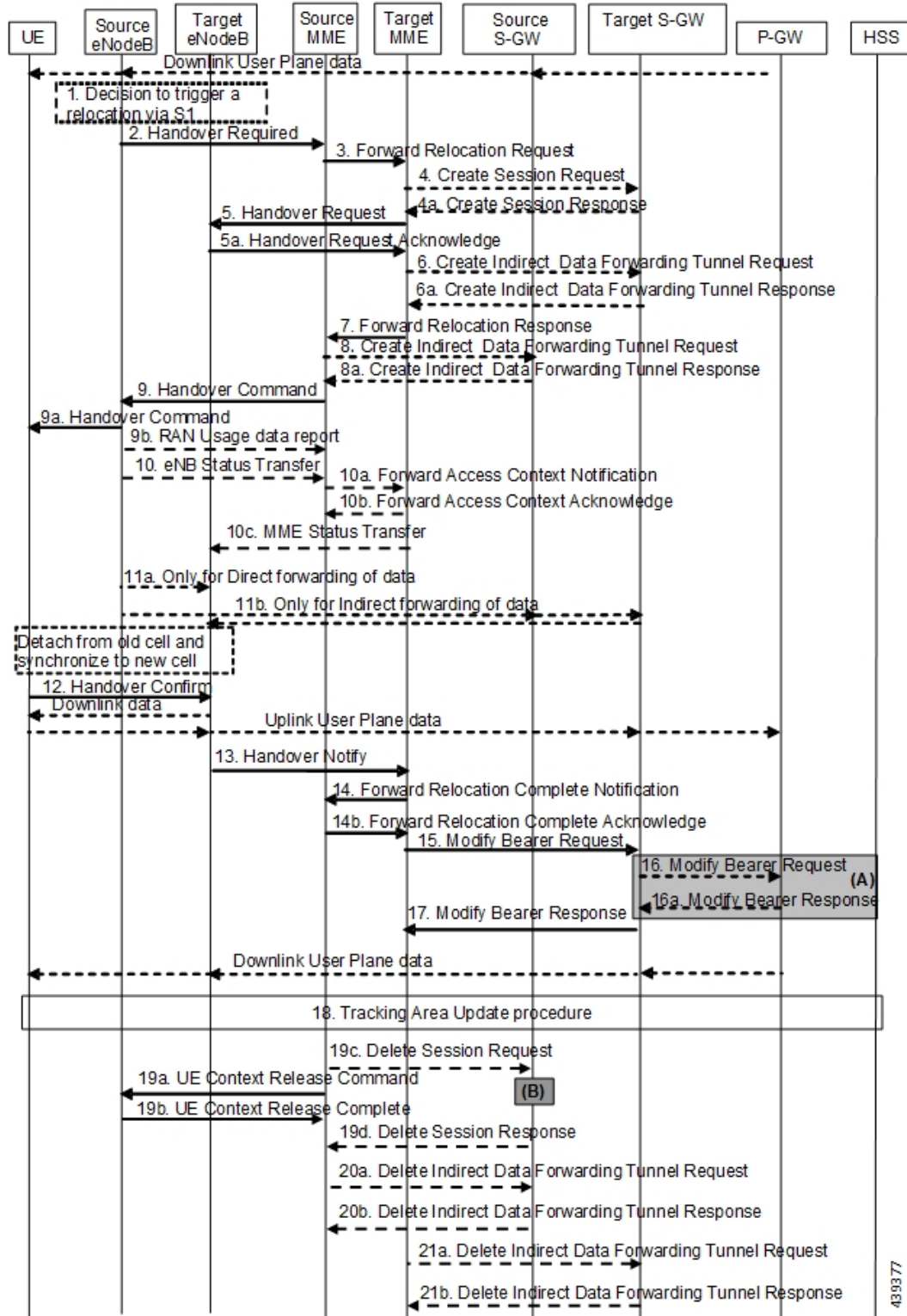
Figure 47: X2-Based Handover with SGW Relocation Call Flow



For call flow description, see the section 5.5.1.1.3 "X2-based handover with Serving GW relocation" from 3GPP TS 23.401.

The following call flow shows the S1-based handover:

Figure 48: S1-based Handover Call Flow



For call flow description, see section 5.5.1.2.2 "S1-based handover, normal" from 3GPP TS 23.401.

## Standards Compliance

The Bearer Modification for EPS Session on SMF feature complies with the following standards:

- *3GPP TS 23.401*
- *3GPP TS 23.502 V16.1.1 (2019-06)*

# Session Management Procedures for EPS and 5GC Interworking

## Feature Description

The 5G Session Management procedures defined in *3GPP TS 23.502* ensure that the EPS interworking is successful when the UE moves to an LTE 4G radio after performing the initial attach to a 5G NR radio.

### Support for Number of Packet Filters in NAS Message

The UE sends the Number of packet filter IE to the SMF in PDU Establishment and Modification request messages. By default, the UE sends a maximum of 16 packet filters.

The UE supports more than 16 packet filters in the following scenarios:

- When the UE is attaching to the SMF in N1 mode.
- When the initial attach to the SMF in S1 mode is complete and the 4G to 5G handover is ongoing.

The SMF sends the maximum filters to the PCF in PolicyCreateControl in "NumOfPackFilter" field. If the Number of packet filter IE is received from the UE in N1 mode, then the SMF uses the "Maximum number of supported filters" field in PDU establishment request. If this IE is not received from the UE in N1 mode or if the received value is lesser than 16, the SMF sends the max filters as 16. If the UE attaches to the SMF in S1 mode and the 4G to 5G or 5G to 4G handover is ongoing, the SMF sends the default value, that is, 16 packet filters.

If there is any change in the packet filter value, then the SMF sends the new value to the PCF through PolicyUpdate message along with NUM\_OF\_PACKET\_FILTER trigger.

The SMF controls the maximum filters allowed per PDU session based on the numOfPackFilter IE. If the number of packet filters crosses the maximum allowed by the UE, the SMF caps the packet filters. This means that the SMF drops the PCC rules when the limit crosses and sends the rule report with INCOR\_FLOW\_INFO failure code.



**Note** INCOR\_FLOW\_INFO is not the correct failure code for this kind of deletion. Use the appropriate failure code when available in the 3GPP specification.

Maximum supported filters are only valid for dynamic rules and not for static and predefined rules.

The "pcc\_rule\_report\_max\_supported\_filter" statistics is introduced under the policy\_pcc\_rule\_report category. This statistics is incremented if the PCC rule report is generated upon reaching the maximum supported filters.

### Support for PCF ID in SmContextCreate

The AMF includes the PCF ID in the Nsmf\_PDUSession\_CreateSMContext Request. The PCF ID identifies the Home Policy Control Function (H-PCF) in the non-roaming case and the Visited Policy Control Function (V-PCF) in the local breakout roaming case. See the 3GPP specification 23.501, section 6.3.7.1 for more details on when the AMF forwards the PCF ID to the SMF.

When the SMF receives the PCF ID, use the following CLI configuration in the PCF network profile to control the SMF behaviour in using the PCF ID.

#### UseAmfProvidedPCF [True/False]

The default behaviour is to use the PCF ID provided by AMF in SmContextCreate.

If the PCF ID provided by AMF is not reachable, the SMF behaves as per the configured failure handling template. In this case, it uses the static configuration.

### Support for DNN Selection Mode in SmContextCreate

The SMF uses the DNN Selection Mode for deciding whether to accept or reject the UE request.

The SMF uses the DNN Selection Mode for deciding whether to retrieve the Session Management Subscription data. In case the DNN, S-NSSAI of the HPLMN is not explicitly subscribed, the SMF uses the local configuration instead of the Session Management Subscription data.



**Note** The preceding use case is not supported.

The SMF validates the IE present in SmContextCreate data. If there is a DnnSelectionMode failure due to the mismatch between DnnSelectionMode and the configured CLI, the SMF does not proceed with the registration. When the DnnSelectionMode failure is observed, the “disc\_pdusetup\_sm\_cxt\_unsupported\_ie” is incremented as part of the disconnect reasons.

DnnSelectionMode Type	Description
Not Present	The SMF sends the subscription request to fetch the subscription data.
Verified	The SMF sends the subscription request to fetch the subscription data.
UE_DNN_NOT_VERIFIED	If the <b>dnn-selection-mode verified ue-provided</b> CLI command is configured as shown in the following configuration, the SMF sends the subscription request to fetch the subscription data. Otherwise, the SMF rejects the Context Request with "Invalid DNN selection Mode" cause.
NW_DNN_NOT_VERIFIED	If the <b>dnn-selection-mode verified network-provided</b> CLI is configured, the SMF sends the subscription request to fetch the subscription data. Otherwise, the SMF rejects the Context Request with "Invalid DNN selection Mode" cause.

The SMF uses the following configuration to configure the DnnSelectionMode.

```
configure
  profile smf profile_name
    dnn-selection-mode [ verified ue-provided | network-provided ]
  end
```

One or more DnnSelectionMode types can be configured. By default, the DnnSelectionMode is verified. Post the subscription request, if no subscription data is fetched from UDM, the SMF falls back to the local DNN profile for subscription data. Neither the subscription data is fetched from the UDM nor the local configuration is present, the SMF sends the SmContextCreateError with subscription failure.

## How it Works

### Call Flows

This section describes the 5G Session Management procedures to support EPS and 5GC interworking.

#### PDU Session Creation Call Flow

This section describes the PDU Session Creation procedure as specified in *3GPP TS 23.502, section 4.3.2.2.1*.

Figure 49: PDU Session Creation Call Flow

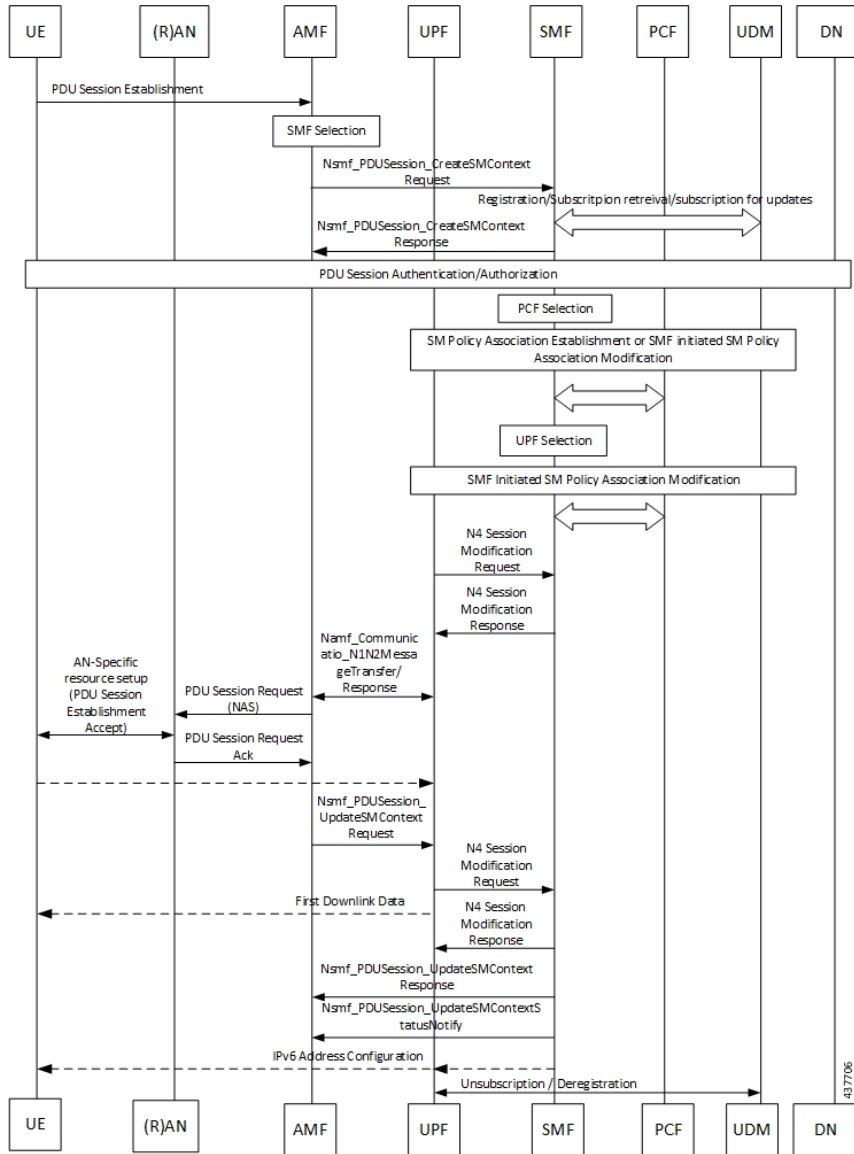


Table 89: PDU Session Creation Call Flow Description

Step	Description
1	The UE initiates the UE Requested PDU Session Establishment procedure by transmitting a NAS message containing a PDU Session Establishment Request within the N1 SM container. The PDU Session Establishment Request includes a PDU session ID, Requested PDU Session Type, a Requested SSC mode, 5GSM Capability PCO, SM PDU DN Request Container, Number of Packet Filters, and optionally Always-on PDU Session Requested.
2	The AMF performs SMF selection as described in 3GPP specification.



Step	Description
3	The AMF includes EPS Interworking Indication in the Nsmf_PDUSession_CreateSMContext Request message sent to the SMF. This parameter indicates whether the UE can perform 4G to 5G handover (and vice versa) and if it is allowed with or without the presence of the N26 interface between the AMF and MME.
4	If the EPS Interworking Indication received from the AMF indicates that the UE supports EPS interworking and the SMF determines (for example, if EPS interworking is allowed for this DNN and S-NSSAI based on UE subscription data) that the PDU session supports EPS interworking, the PGW-C+SMF FQDN for the S5/S8 interface is included in the Nudm_UECM_Registration Request message.
5	The SMF sends either Nsmf_PDUSession_CreateSMContext Response (Cause, SM Context ID or N1 SM container (PDU Session Reject (Cause))) or an Nsmf_PDUSession_UpdateSMContext Response depending on the Request received in Step 3.  If the SMF received Nsmf_PDUSession_CreateSMContext Request in Step 3 and the SMF can process the PDU Session Establishment Request, the SMF creates an SM context and responds to the AMF by providing an SM Context Identifier.
6	(Optional). If the Request Type in Step 3 indicates "Existing PDU Session", the SMF does not perform secondary authorization and authentication.  If the Request Type received in Step 3 indicates "Emergency Request" or "Existing Emergency PDU Session", the SMF does not perform secondary authorization and authentication.  If the SMF needs to perform secondary authorization and authentication during the establishment of the PDU Session by a DN-AAA server as described in <i>3GPP TS 23.501, section 5.6.6</i> , the SMF triggers the PDU session establishment authentication and authorization as described in <i>3GPP TS 23.501, section 4.3.2.3</i> .
7a	If dynamic PCC is to be used for the PDU Session, the SMF performs PCF selection as described in <i>3GPP TS 23.501, section 6.3.7.1</i> . If the Request Type indicates "Existing PDU Session" or "Existing Emergency PDU Session", the SMF uses the PCF already selected for the PDU Session. Otherwise, the SMF may apply local policy.
7b	The SMF performs the mapping of PCC rules and 5G QoS parameters to 4G TFTs and 4G QoS as described in the Generating EPS PDN Connection Parameters from 5G PDU Session Parameters section in this document. Based on the QoS flows, the SMF+PGW-C also determines the number of dedicated bearers required for the session when it hands off to EPS and the required flows (all non-GBR flows) in the default bearer. The SMF+PGW-C saves the mapping of 5G flows to 4G bearers.
8	If the Request Type in Step 3 indicates "Initial request", the SMF selects an SSC mode for the PDU Session as described in <i>3GPP TS 23.501, section 5.6.9.3</i> . The SMF also selects one or more UPFs as needed as described in <i>3GPP TS 23.501, section 6.3.3</i> .
9	The SMF performs an SMF-initiated SM Policy Association Modification procedure as defined in <i>3GPP TS 23.502, section 4.16.5.1</i> to provide information on the Policy Control Request Trigger conditions that have been met. If Request Type is "initial request" and dynamic PCC is deployed and PDU Session Type is IPv4 or IPv6 or IPv4v6, the SMF notifies the PCF (if the Policy Control Request Trigger condition is met) with the allocated UE IP address/prefix(es).  SMF+PGW-C initiates the EBI allocation procedure as defined in <i>3GPP TS 23.502, section 4.11.1.4</i> .

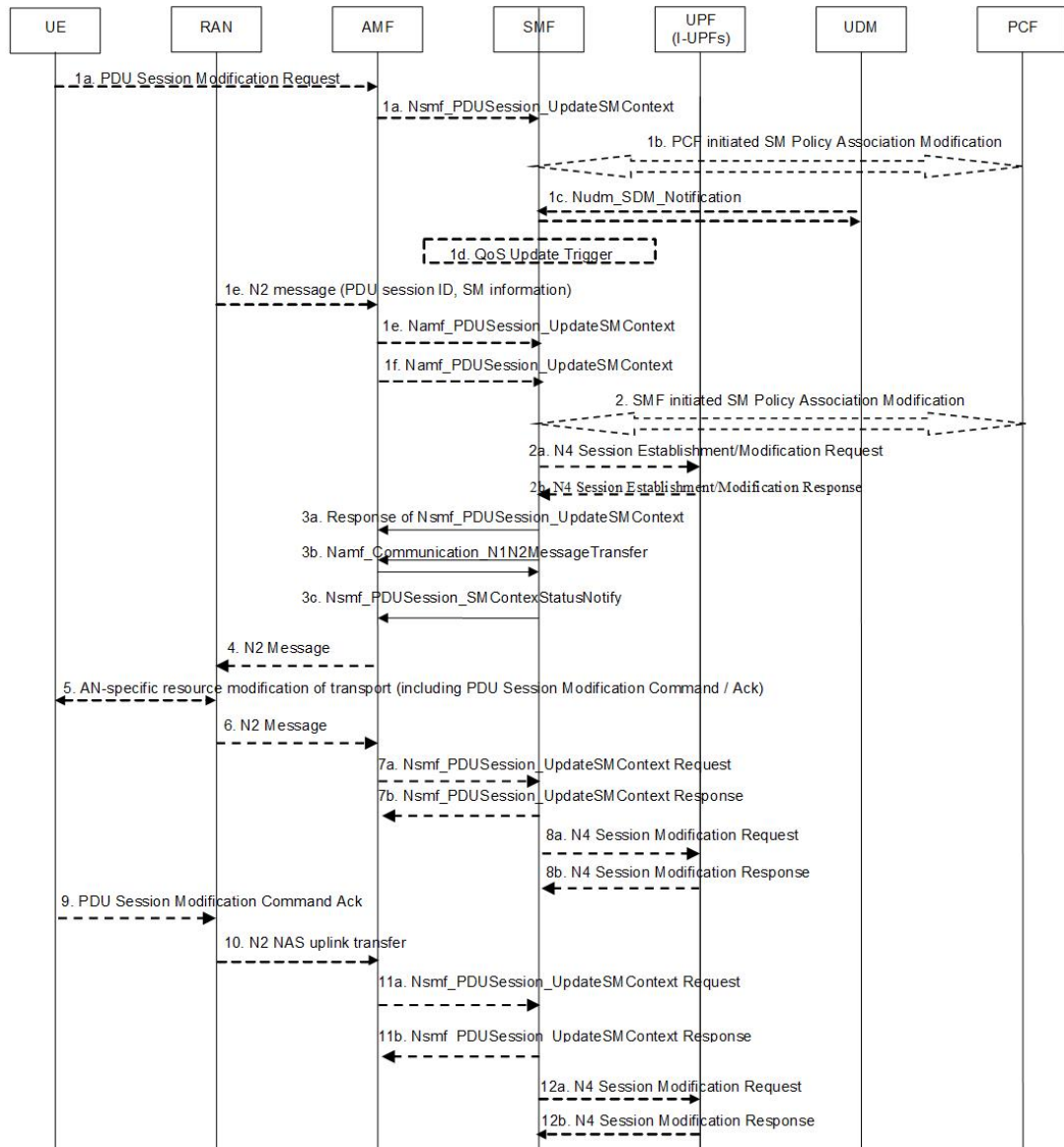
Step	Description
10	<p>If the Request Type indicates "initial request", the SMF initiates an N4 Session Establishment procedure with the selected UPF. Otherwise, it initiates an N4 Session Modification procedure with the selected UPF.</p> <p>If multiple UPFs are selected for the PDU Session, the SMF initiates N4 Session Establishment/Modification procedure with each UPF of the PDU Session in this step.</p>
11	<p>In the non-roaming or LBO scenario, the PGW-C+SMF includes the mapped EPS bearer context(s) and the corresponding QoS flow(s) to be sent to the UE in the N1 SM container. The PGW-C+SMF also indicates the mapping between the QoS flow(s) and mapped EPS bearer context(s) in the N1 SM container. The PGW-C+SMF also includes the mapping between the received EBI(s) and QFI(s) in the N2 SM information to be sent to the NG-RAN. The PGW-C+SMF sends the N1 SM container and N2 SM information to the AMF through the Namf_Communication_N1N2MessageTransfer message.</p>
12	<p>The AMF sends N2 PDU Session Request (N2 SM information, NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept))) to the (R)AN.</p> <p>The AMF sends the NAS message containing PDU Session ID and PDU Session Establishment Accept targeted to the UE and the N2 SM information received from the SMF within the N2 PDU Session Request to the (R)AN.</p>
13	<p>The (R)AN may issue AN-specific signaling exchange with the UE that is related with the information received from the SMF. For example, in case of an NG-RAN, an RRC Connection Reconfiguration may take place with the UE establishing the necessary NG-RAN resources related to the QoS rules for the PDU Session Request received in Step 12.</p>
14	<p>(R)AN issues N2 PDU Session Response (PDU Session ID, Cause, N2 SM information (PDU Session ID, AN Tunnel Info, List of accepted/rejected QFI(s), User Plane Enforcement Policy Notification)) to the AMF.</p>
15	<p>The AMF sends Nsmf_PDUSession_UpdateSMContext Request (N2 SM information, Request Type) to the SMF.</p> <p>The AMF forwards the N2 SM information received from (R)AN to the SMF.</p>
16a	<p>The SMF initiates an N4 Session Modification procedure with the UPF. The SMF provides AN Tunnel Information and the corresponding forwarding rules to the UPF.</p>
16b	<p>The UPF provides an N4 Session Modification Response to the SMF.</p> <p>If multiple UPFs are used in the PDU session, the UPF in Step 16a refers to the UPF terminating N3.</p> <p>After this step, the UPF delivers any downlink packets to the UE that may have been buffered for this PDU session.</p>
17	<p>The SMF sends Nsmf_PDUSession_UpdateSMContext Response (Cause) to the AMF.</p>
18	<p>(Conditional) The SMF sends Nsmf_PDUSession_SMContextStatusNotify (Release) to the AMF.</p> <p>If during the procedure, any time after Step 5, the PDU Session establishment is not successful, the SMF informs the AMF by invoking Nsmf_PDUSession_SMContextStatusNotify (Release). The SMF also releases any N4 session(s) created, any PDU session address if allocated (for example, IP address) and releases the association with PCF, if any.</p>

Step	Description
19	If the PDU Session Type is IPv6 or IPv4v6, the SMF generates an IPv6 Router Advertisement and sends it to the UE via N4 and the UPF.
20	<p>If the PDU Session Establishment failed after Step 4, the SMF performs the following:</p> <ul style="list-style-type: none"> <li>• The SMF unsubscribes to the modifications of Session Management Subscription data for the corresponding (SUPI, DNN, S-NSSAI), using Nudm_SDM_Unsubscribe (SUPI, Session Management Subscription data, DNN, S-NSSAI), if the SMF is no more handling a PDU session of the UE for this (DNN, S-NSSAI). The UDM may unsubscribe to the modification notification from UDR by Nudr_DM_Unsubscribe (SUPI, Subscription Data, Session Management Subscription data, S-NSSAI, DNN).</li> <li>• The SMF deregisters for the given PDU session using Nudm_UECM_Deregistration (SUPI, DNN, PDU Session ID). The UDM may update corresponding UE context by Nudr_DM_Update (SUPI, Subscription Data, UE context in SMF data).</li> </ul>

### PDU Session Modification Call Flow

This section describes the PDU session modification procedure as specified in *3GPP TS 23.502, section 4.3.3.2*.

Figure 50: PDU Session Modification Call Flow



444599

Table 90: PDU Session Modification Call Flow Description

Step	Description
1a	The UE initiates the UE Requested PDU Session Modification procedure by transmitting a NAS message containing a PDU Session Modification Request within the N1 SM container. The PDU Session Modification Request includes a PDU session ID, Packet Filters, Operation, Requested QoS, Segregation, and 5GSM Core Network Capability.
1b	(SMF-requested modification) The PCF performs a PCF-initiated SM Policy Association Modification procedure to notify the SMF about the modification of policies. The policy decision or upon AF requests, for example, Application Function influence on traffic routing, triggers this procedure.

Step	Description
1c	(SMF-requested modification) The UDM updates the subscription data of SMF by Nudm_SDM_Notification (SUPI, Session Management Subscription Data). The SMF updates the Session Management Subscription Data and acknowledges the UDM by returning an Ack with (SUPI).
1d	(SMF-requested modification) The SMF decides to modify PDU session. This procedure is also triggered based on locally configured policy or triggered from the (R)AN.  If the SMF receives one of the triggers in step 1b to 1d, the SMF starts SMF-requested PDU Session Modification procedure.
1e	(AN-initiated modification) (R)AN indicates to the SMF when the AN resources onto which a QoS Flow is mapped are released irrespective of whether notification control is configured.  (R)AN sends the N2 message (PDU Session ID, N2 SM information) to the AMF. The N2 SM information in the smf_PDU_Session_UpdateContext includes the following information: <ul style="list-style-type: none"> <li>• QoS Flow Identifier (QFI)</li> <li>• User location Information</li> <li>• QoS Flow Release List IE - list of QoS flows which are released by NG-RAN node</li> <li>• QoS Flow Notify List IE and Notification Cause IE - list of GBR QoS flows that fulfilled a specific criteria, and the flows that missed fulfilling the criteria</li> </ul> The SMF supports AN-initiated modification to release the QFI from RAN. For details on this support, see the following section.
2	The SMF reports the subscribed event to the PCF by performing an SMF-initiated SM Policy Association Modification procedure. The SMF skips this step if the PDU Session Modification procedure is triggered by step 1b or 1d. If the dynamic PCC is not deployed, the SMF may apply local policy to decide whether to change the QoS profile. The SMF does not invoke the steps 3 to 7 when the PDU Session Modification requires only action at a UPF (for example, gating).
3a	For UE or AN-initiated modification, the SMF responds to the AMF through Nsmf_PDUSession_UpdateSMContext including N2 SM information and N1 SM container.  The N2 SM information carries information that the AMF provides to the (R)AN. It includes the QoS profiles and the corresponding QFIs to notify the (R)AN that one or more QoS flows were added, or modified. It includes only QFI(s) to notify the (R)AN that one or more QoS flows were removed.  The N1 SM container carries the PDU Session Modification Command that the AMF provides to the UE. It includes the QoS rule(s), QoS rule operation, QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with the QoS rule(s), and Session-AMBR.
3b	For SMF-requested modification, the SMF invokes Namf_Communication_N1N2MessageTransfer including N2 SM information and N1 SM container.  If the UE is in CM-IDLE state and an Asynchronous type communication (ATC) is activated, the AMF updates and stores the UE context based on the Namf_Communication_N1N2MessageTransfer, and skips the steps 4, 5, 6 and 7. When the UE is reachable, that is, when the UE enters CM-CONNECTED state, the AMF forwards the N1 message to synchronize the UE context with the UE.

Step	Description
4	The AMF sends N2 PDU Session Request (N2 SM information received from the SMF, NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command))) Message to the (R)AN.
5	The (R)AN issues AN-specific signalling exchange with the UE that is related with the information received from the SMF. For example, in an NG-RAN, an RRC Connection Reconfiguration takes place with the UE modifying the necessary (R)AN resources related to the PDU session.
6	The (R)AN acknowledges N2 PDU Session Request by sending a N2 PDU Session Ack Message to the AMF.
7	The AMF forwards the N2 SM information and the User location Information from the AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation. The SMF sends Nsmf_PDUSession_UpdateSMContext Response.  If the (R)AN rejects QFI(s), the SMF updates the QoS rules and QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with the QoS rule(s) in the UE accordingly.
8	The SMF updates N4 session of the UPF(s) that are involved by the PDU Session Modification by sending N4 Session Modification Request message to the UPF.
9	The UE acknowledges the PDU Session Modification Command by sending a NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command Ack)).
10	The (R)AN forwards the NAS message to the AMF.
11	The AMF forwards the N1 SM container (PDU Session Modification Command Ack) and User Location Information from the AN to the SMF through Nsmf_PDUSession_UpdateSMContext service operation. The SMF sends Nsmf_PDUSession_UpdateSMContext Response.
12	The SMF updates N4 session of the UPF(s) that are involved by the PDU Session Modification by sending N4 Session Modification Request (N4 Session ID) message to the UPF.  For a PDU Session of Ethernet PDU Session Type, the SMF notifies the UPF to add or remove Ethernet Packet Filter Set(s) and forwarding rule(s).
13	If the SMF interacts with the PCF in step 1b or 2, the SMF notifies the PCF whether the PCC decision is enforced or not by performing an SMF-initiated SM Policy Association Modification procedure.  The SMF notifies any entity that has subscribed to User Location Information related with PDU Session change.  If the step 1b is triggered to perform Application Function influence on traffic routing, the SMF reconfigures the User Plane of the PDU session.

### Releasing QFI During AN-initiated Modification Procedure

For the SMF to support AN-initiated modification to release the QFIs, perform the following steps:

1. If the EPS Interworking Indication is enabled for a given PDU session, the SMF initiates the EBI release towards the AMF.

2. The SMF sends N4 Modification to the UPF to delete the Packet Detection Rule (PDR), QoS Enforcement Rule (QER), and Usage Reporting Rule (URR) related to the flows being released.
3. The SMF initiates N1N2TransferMessage containing N1 PDU Session Modification command. This message includes information about the deleted flows, Mapped EPS Bearer Context.
4. Then, the SMF interacts with the PCF to report the flows released for the rules if “RES\_RELEASE” trigger is set.




---

**Note** The "policy\_pdu\_flows\_total" statistics is available to check the released flows.

---

### EPS Interworking Indication in PDU Session Modification

The EpsInterworkingIndication field denotes the possibility of handover between EPS and 5GC. This field holds the following values:

- NONE: The PDU session cannot be moved to EPS.
- WITH\_N26: The PDU session is moved to EPS, with N26 interface supported during EPS interworking procedures.
- WITHOUT\_N26: The PDU session is moved to EPS, without N26 interface supported during EPS interworking procedures.

The SMF allows the 4G to 5G handover and vice-versa only if the EpsInterworkingIndication value is set to WITH\_N26. For other values of EpsInterworkingIndication, the SMF rejects the handovers.

During 4G and 5G PDU session establishment, if the EPS interworking indication is received from the AMF, the SMF includes PGW-C+SMF FQDN for S5/S8 interface in the UDM Registration request.

### With the EPS Interworking Indication Support Enabled:

If the EpsInterworkingIndication value changes from NONE or WITHOUT\_N26 to WITH\_N26 for a created PDU session, follow these steps to support the EPS Interworking Indication change in the PDU modification procedure.

1. The AMF invokes the Nsmf\_PDUSession\_UpdateSMContext request with the changed EpsInterworkingIndication value.
2. The SMF receives the Nsmf\_PDUSession\_UpdateSMContext request from the AMF, and initiates the Namf\_Communication\_EbiAssignmentRequest. This request includes the PDU Session ID and Allocation/Retention Priority (ARP) List.
3. The AMF sends Namf\_Communication\_EbiAssignmentResponse to the SMF. The AMF sends the following through the response:
  - assignedEbiList containing the successfully assigned EBIs.
  - failedArpList containing the failed ARPs for which the EBI assignment failed.
  - 4XX/5XX error along with AssignEbiError representing the EBI assignment failure.
4. The SMF sends N1N2MessageTransfer request message if the EBIs are created successfully. This request includes the following:

- N1:PDU SESSION MODIFICATION COMMAND ([Mapped EPS Bearer Contexts,Create])
- N2:N2\_PDU\_SESSION\_RESOURCE\_MODIFY\_REQUEST\_TRANSFER (QoS Flow Add or Modify Request Item with EPS Radio Access Bearer (E-RAB) ID and QoS Flow ID)



**Note** If the UE is in Idle mode, the SMF skips sending the N2 message.

5. The SMF informs mapped EPS bearer context in the UE using N1 message. The SMF waits for N1: PDU SESSION MODIFICATION COMPLETE message.
6. The SMF informs EBI to QoS Flow Identifier (QFI) mapping to gNodeB using N2 message. The SMF waits for N2: PDU SESSION RESOURCE MODIFY RESPONSE TRANSFER message.
7. The SMF completes the PDU Session Modification procedure.

#### **With the EPS Interworking Indication Support Disabled:**

If the EpsInterworkingIndication value changes from WITH\_N26 to NONE or WITHOUT\_N26 for a created PDU session, follow these steps to support the EPS Interworking Indication change in the PDU modification procedure.

1. The SMF receives the Nsmf\_PDUSession\_UpdateSMContext request with the changed EpsInterworkingIndication value from the AMF.
2. The SMF sends N1N2MessageTransfer request message. This request includes the following:
  - N1:PDU SESSION MODIFICATION COMMAND ([Mapped EPS Bearer Contexts,Delete])
  - N2:N2\_PDU\_SESSION\_RESOURCE\_MODIFY\_REQUEST\_TRANSFER



**Note** If the UE is in Idle mode, the SMF skips sending the N2 message.

3. The SMF deletes Mapped EPS bearer context in UE using N1 message. The SMF waits for N1: PDU SESSION MODIFICATION COMPLETE message.
4. The SMF deletes EBI to QFI mapping to gNodeB using N2 message. The SMF waits for N2: PDU SESSION RESOURCE MODIFY RESPONSE TRANSFER message.
5. The SMF completes the PDU Session Modification procedure.

Use the **show subscriber** command to determine the EPS interworking status of the PDU session, and the EBI mapping for the QoS flows.

## **PDU Session Release Call Flow**

The PDU Session Release procedure is used to release all the resources associated with a PDU session, including:

- The IP address/prefixes allocated for an IP-based PDU session
- Any UPF resource that was used by the PDU session.



- Any access resource that was used by the PDU session.

The SMF notifies any entity associated with the PDU session: PCF, Data Network (DN) (for example, when DN authorization has taken place at PDU session establishment), and so on.

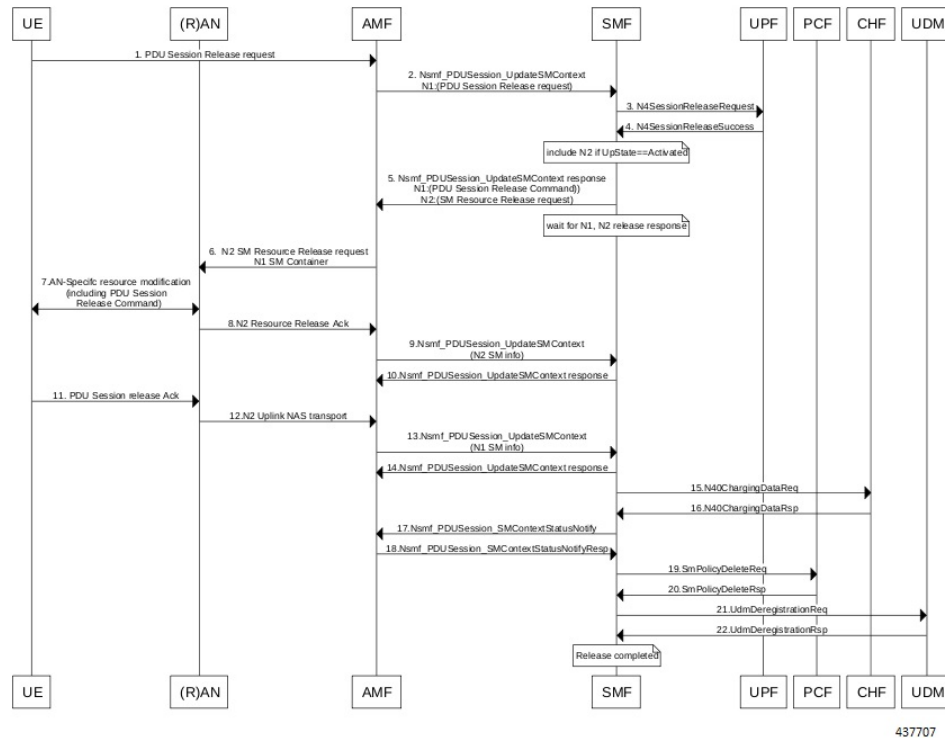
There are different ways to initiate the PDU session release. It can be from UE, network, AMF, or RAN.

**UE-initiated PDU Session Release Call Flow**

The UE-initiated PDU session release procedure allows the UE to request the release of the PDU session. In the case of Local Breakout (LBO), the procedure is as in the case of non-roaming with the difference that the AMF, the SMF, the UPF, and the PCF are located in the visited network.

The following figure depicts the UE-initiated PDU session release procedure to support EPS interworking on the SMF as specified in 3GPP TS 23.502, section 4.3.4.2.

**Figure 51: UE-initiated PDU Session Release Call Flow**



**Table 91: UE-initiated PDU Session Creation Call Flow Description**

Step	Description
1, 2	The UE sends PDU_SESSION_RELEASE_REQUEST in NAS message to the AMF through the RAN. The AMF sends the message to the SMF in SmContextUpdateRequest.
3, 4	The SMF sends N4SessionReleaseRequest to the UPF. The UPF sends response for the same.

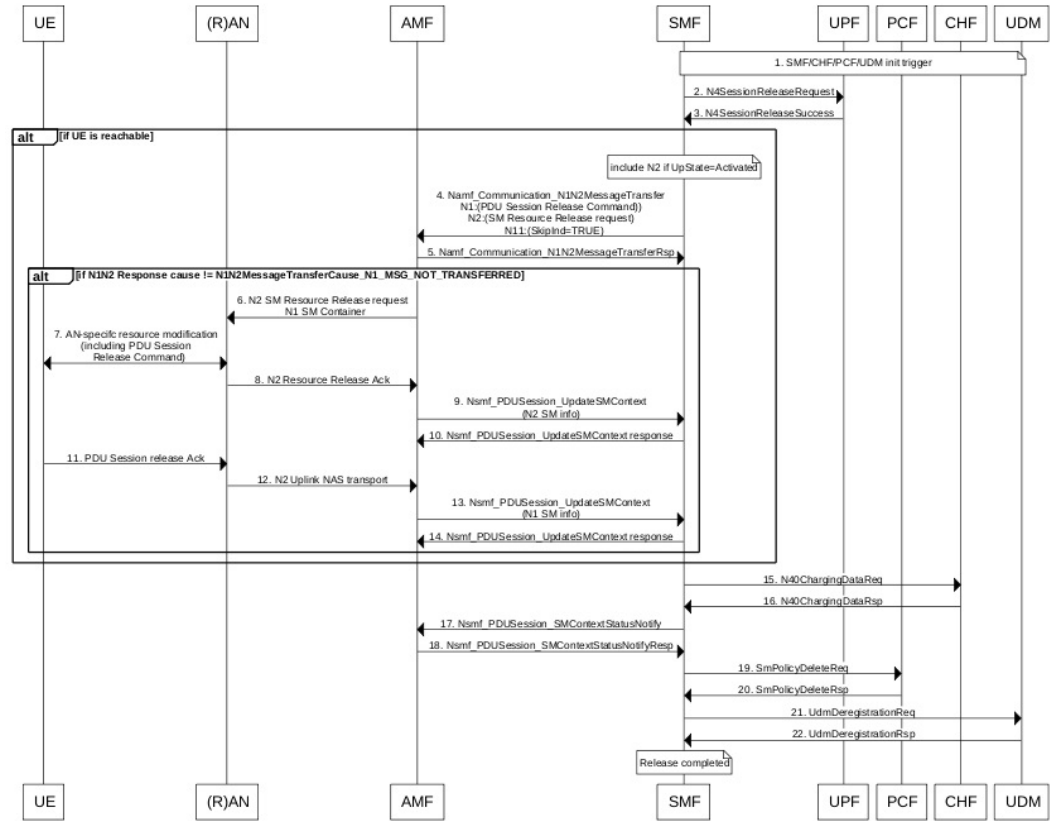
Step	Description
5	The SMF sends SmContextUpdateResponse message with N1 and N2 content. <ul style="list-style-type: none"> <li>• N1: PDU_SESSION_RELEASE_COMMAND</li> <li>• N2: N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND. exclude if the SMF is in IDLE mode. Also, skip the steps 8, 9, and 10.</li> </ul>
6, 7	The AMF exchanges the message with RAN. The RAN forwards it to the UE.
8, 9, 10	The RAN sends N2 release response to the AMF. The AMF sends N2 release response (N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE_TRANSFER) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
11, 12, 13, 14	The UE sends N1 release response in NAS message to the AMF through the RAN. The AMF sends N1 release response (PDU_SESSION_RELEASE_COMPLETE) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
15, 16	The SMF sends delete charging request to the CHF. The CHF responds back to the SMF with delete response.
17, 18	The SMF sends SmContextStausNotify to the AMF. The AMF responds back with SmContextStausNotifyResponse message.
19, 20	The SMF sends delete request to the PCF. The PCF responds back to the SMF with delete response
21, 22	The SMF sends UDM deregistration request. The UDM responds back to the SMF with deregistration response.

### Network-initiated PDU Session Release Call Flow

The network-initiated PDU session release procedure allows the AMF, the SMF or the PCF to initiate the release of a PDU session.

The following figure depicts the network-initiated PDU session release call flow.

Figure 52: Network-initiated PDU Session Release Call Flow



444747

Table 92: Network-initiated PDU Session Creation Call Flow Description

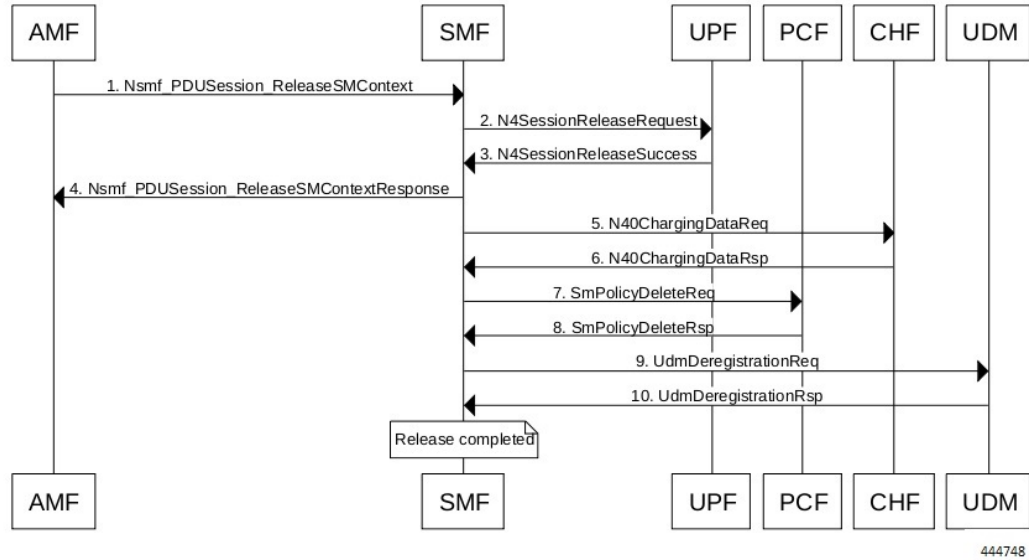
Step	Description
1	This procedure can be triggered by PCF, CHF, UDM, UPF or CLI (clear subscriber) to initiate the release of a PDU session.
2, 3	The SMF sends N4SessionReleaseRequest to the UPF. The UPF sends response for the same. <b>Note</b> Skip the steps 4 to 14 if the AMF has notified that the UE is not reachable.
4	The SMF sends N1N2MessageTransfer message with N11, N1 and N2 content. <ul style="list-style-type: none"> <li>• N11: SkipInd=True</li> <li>• N1: PDU_SESSION_RELEASE_COMMAND</li> <li>• N2: N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND. exclude if the SMF is in IDLE mode. Also, skip the steps 8, 9, and 10.</li> </ul>

Step	Description
5	The AMF responds back to the SMF with the cause included in the N1N2MessageTransferRsp message. <b>Note</b> Skip the steps 6 to 14 if the AMF sends the cause as N1_MSG_NOT_TRANSFERRED in step 5.
6, 7	The AMF exchanges the message with RAN. The RAN forwards it to the UE.
8, 9, 10	The RAN sends N2 release response to the AMF. The AMF transfers N2 release response (N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE_TRANSFER) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
11, 12, 13, 14	The UE sends N1 release response in the NAS message to the AMF through the RAN. The AMF sends the N1 release response (PDU_SESSION_RELEASE_COMPLETE) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
15, 16	The SMF sends delete charging request to the CHF. The CHF responds back to the SMF with delete response.
17, 18	The SMF sends SmContextStausNotify to the AMF. The AMF responds back with the SmContextStausNotifyResponse message.
19, 20	The SMF sends delete request to the PCF. The PCF responds back to the SMF with delete response.
21, 22	The SMF sends UDM deregistration request. The UDM responds back to the SMF with deregistration response.

### AMF-initiated PDU Session Release

The AMF-initiated PDU session release procedure allows the AMF to initiate the release of a PDU session. The following figure depicts the AMF-initiated PDU session release call flow.

Figure 53: AMF-initiated PDU Session Release Call Flow



444748

Table 93: AMF-initiated PDU Session Creation Call Flow Description

Step	Description
1	The AMF sends SmContextReleaseRequest.
2, 3	The SMF sends N4SessionReleaseRequest to the UPF. The UPF sends response for the same.
4	The SMF sends SmContextReleaseResponse to the AMF.
5, 6	The SMF sends delete charging request to the CHF. The CHF responds back to the SMF with delete response.
7, 8	The SMF sends delete request to the PCF. The PCF responds back to the SMF with delete response.
9, 10	The SMF sends UDM deregistration request. The UDM responds back to the SMF with deregistration response.

AMF-initiated PDU Session Release with N11 Release=True

The AMF-initiated PDU session release procedure allows the AMF to initiate the release of a PDU session with the N11 release in the SmContextModifyRequest being set to True.

The following figure depicts the AMF-initiated PDU session release call flow with the N11 release=True.

Figure 54: AMF-initiated PDU Session Release with N11 Release=True

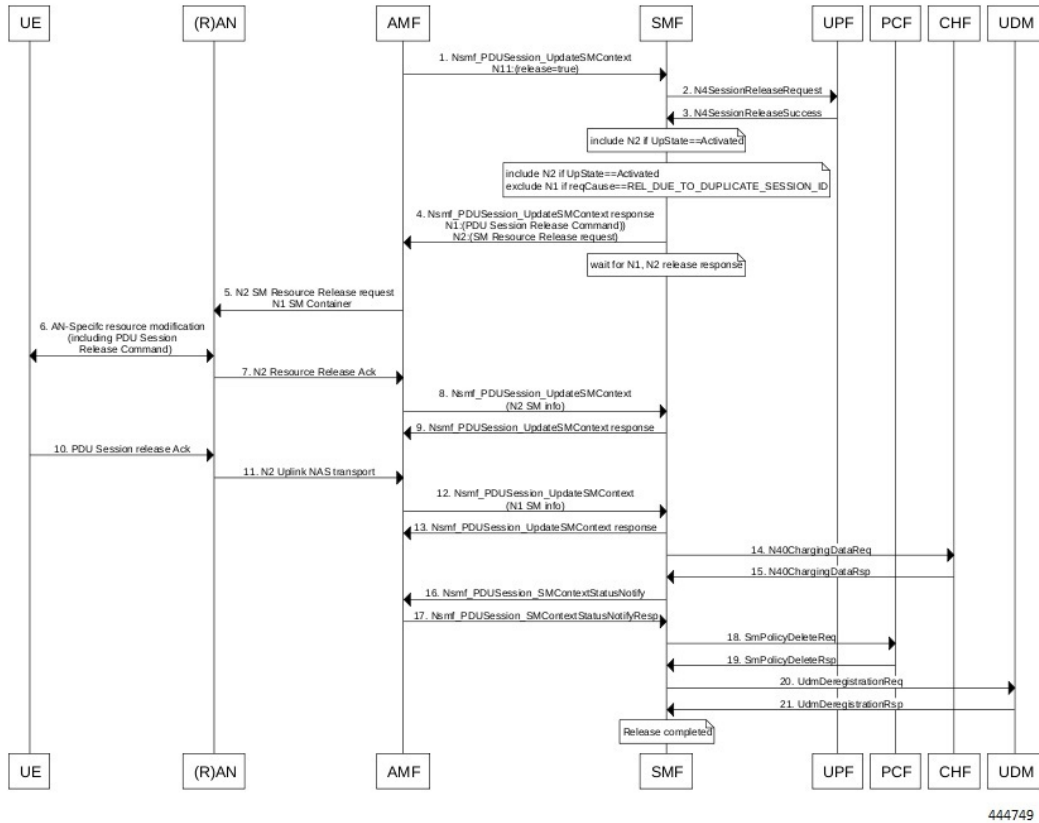


Table 94: AMF-initiated PDU Session Creation Call Flow (N11 release=true) Description

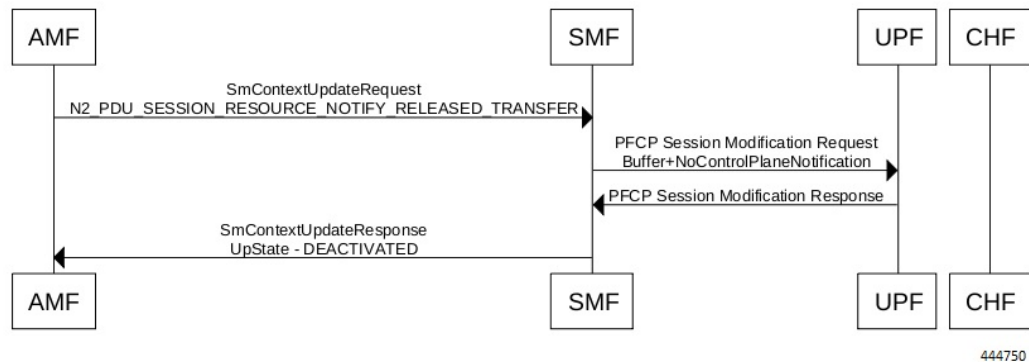
Step	Description
1	The AMF sends SmContextModifyRequest with release=True in 2 causes REL_DUE_TO_DUPLICATE_SESSION_ID or REL_DUE_TO_SLICE_NOT_AVAILABLE.
2, 3	The SMF sends N4SessionReleaseRequest to the UPF. The UPF sends response for the same.
4	The SMF sends SmContextUpdateResponse message with N1 and N2 content. <ul style="list-style-type: none"> <li>• N1: PDU_SESSION_RELEASE_COMMAND, exclude if cause is REL_DUE_TO_DUPLICATE_SESSION_ID, skip steps 10,11,12,13</li> <li>• N2: N2_PDU_SESSION_RESOURCE_RELEASE_COMMAND. exclude if the SMF is in IDLE mode. Also, skip the steps 7, 8, and 9.</li> </ul>
5, 6	The AMF exchanges message with RAN. The RAN forwards it to the UE.
7, 8, 9	The RAN sends N2 release response to the AMF. The AMF sends N2 release response (N2_PDU_SESSION_RESOURCE_RELEASE_RESPONSE_TRANSFER) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.

Step	Description
10, 11, 12, 13	The UE sends N1 release response in NAS message to the AMF through the RAN. The AMF sends N1 release response (PDU_SESSION_RELEASE_COMPLETE) in N11 SmContextUpdateRequest message. The SMF responds back to the AMF as SmContextUpdateResponse.
14, 15	The SMF sends delete charging request to the CHF. The CHF responds back to the SMF with delete response.
16, 17	The SMF sends SmContextStausNotify to the AMF. The AMF responds back with SmContextStausNotifyResponse message.
18, 19	The SMF sends delete request to the PCF. The PCF responds back to the SMF with delete response.
20, 21	The SMF sends UDM deregistration request. The UDM responds back to the SMF with deregistration response.

**RAN-initiated PDU Session Release Call Flow**

The RAN-initiated PDU session release procedure allows the RAN to initiate the release of a PDU session. The following figure depicts the RAN-initiated PDU session release call flow.

**Figure 55: RAN-initiated PDU Session Release Call Flow**



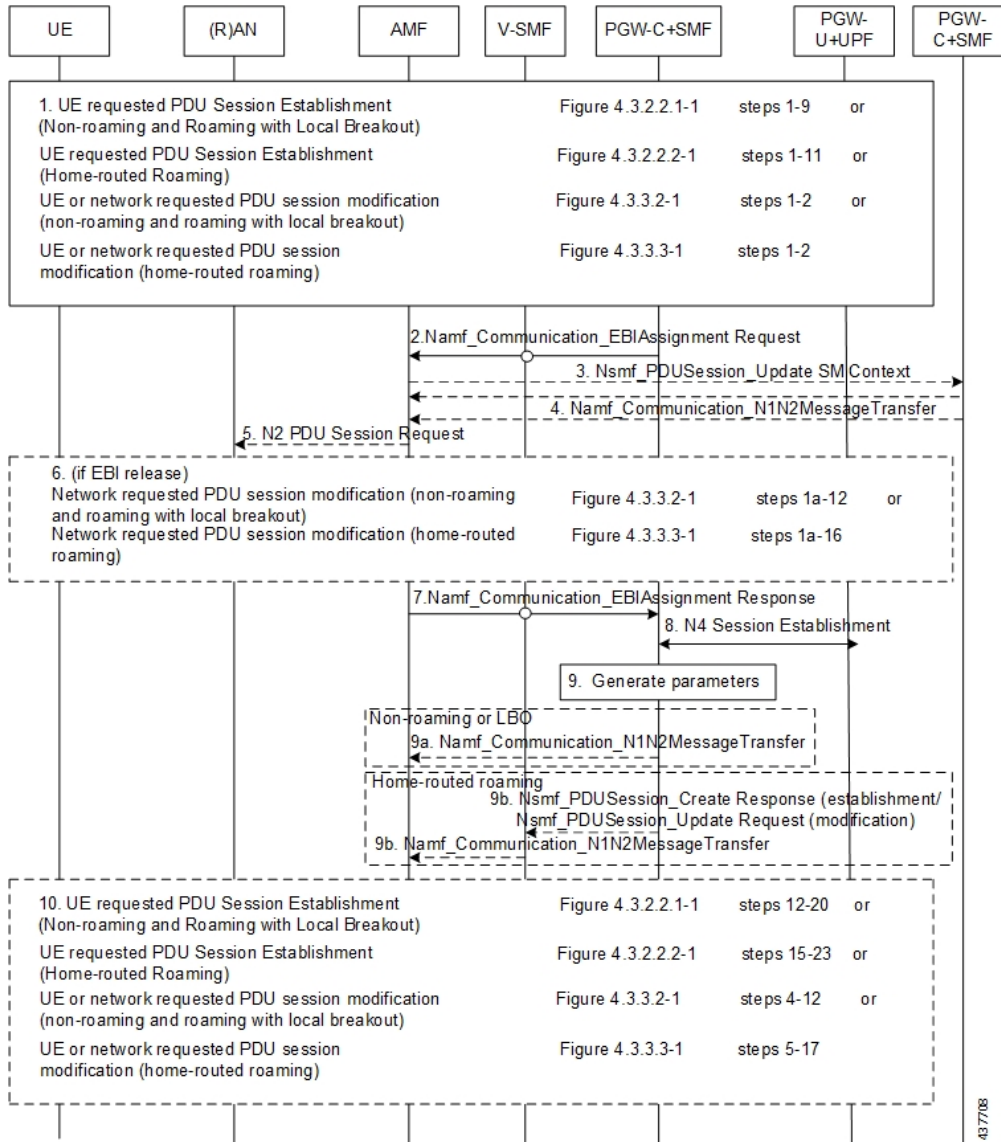
**Table 95: AMF-initiated PDU Session Creation Call Flow Description**

Step	Description
1	The AMF sends SmContextModifyRequest with N2 type: N2_PDU_SESSION_RESOURCE_NOTIFY_RELEASED_TRANSFER.
2, 3	The SMF sends N4SessionModificationRequest to the UPF with changing packet rule to Buffer from Forward. The UPF sends the response for the same, that is, the SMF moving to IDLE state.
4	The SMF sends SmContextUpdateResponse message with UpState as Deactivated.

**EPS Bearer ID Allocation**

This section describes the EPS Bearer ID Allocation procedure.

Figure 56: EPS Bearer ID Allocation Call Flow



**Note** Not all the steps in the preceding call flow are supported. For more details, see the descriptions in the following table.

Table 96: EPS Bearer ID Allocation Call Flow Description

Step	Description
1	The EBI Assignment procedure is initiated as specified in the relevant sections of <i>3GPP TS 23.502</i> . The relevant steps of the procedure are executed as specified in the preceding call flow. <b>Note</b> Roaming scenarios are currently not supported.



Step	Description
2	If the PGW-C+SMF (or H-SMF for home-routed cases) determines that EPS bearer IDs (based on operator policies, S-NSSAI, User Plane Security Enforcement information) need to be assigned to the QoS flows in the PDU session, the PGW-C+SMF invokes Namf_Communication_EBIAssignment Request (PDU Session ID, ARP list).
Step 3 through Step 6 apply only when the AMF needs to revoke EBI that was previously allocated for a UE to serve a new SMF request of EBI for the same UE.	
3	(Conditional) If the AMF has no available EBIs, the AMF may revoke an EBI that was assigned to QoS flows based on the ARPs and S-NSSAI stored during PDU Session Establishment, EBI information in the UE context and local policies. If an assigned EBI is to be revoked, the AMF invokes Nsmf_PDUSession_UpdateSMContext (EBI(s) to be revoked) to request the related SMF (called “SMF serving the released resources”) to release the mapped EPS QoS parameters corresponding to the EBI to be revoked. The AMF stores the association of the assigned EBI, ARP pair to the corresponding PDU Session ID and SMF address.
4	<p>The “SMF serving the released resources” that receives the request in Step 3 invokes Namf_Communication_N1N2Message Transfer (N2 SM information (PDU Session ID, EBI(s) to be revoked), N1 SM container (PDU Session Modification Command (PDU Session ID, EBI(s) to be revoked))) to inform the (R)AN and the UE to remove the mapped EPS QoS parameters corresponding to the EBI(s) to be revoked. In home-routed roaming scenario, the H-SMF includes EBI(s) to be revoked to V-SMF to inform V-SMF to remove the mapped EPS bearer context corresponding to the EBI(s) to be revoked.</p> <p>The SMF can also decide to remove the QoS flow if it is not acceptable to continue the service when no corresponding EPS QoS parameters can be assigned.</p> <p>For home-routed roaming scenario, the "SMF serving the released resources" sends an N4 Session Modification Request to request the PGW-U+UPF to release the N4 session corresponding to the revoked EBI(s).</p> <p>In home-routed roaming case, the V-SMF starts a VPLMN-initiated QoS Modification for the PDU session. The V-SMF invokes the Namf_Communication_N1N2Message Transfer based on the corresponding QoS modification message received from H-SMF.</p>
5	<p>If the UE is in CM-CONNECTED state, the AMF sends N2 PDU Session Request (N2 SM information received from SMF, NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command))) message to the (R)AN.</p> <p>If the UE is in CM-IDLE state and an ATC is activated, the AMF updates and stores the UE context based on the Namf_Communication_N1N2MessageTransfer and Step 5 and Step 6 are skipped. When the UE is reachable, for example, when the UE enters CM-CONNECTED state, the AMF forwards the N1 message to synchronize the UE context with the UE.</p>
6	The relevant steps of the procedure are executed as specified in the preceding figure.
7	<p>If the AMF successfully assigns EBI(s), it responds with the assigned EBI(s). Otherwise, it responds with a cause indicating EBI assignment failure.</p> <p>If a PDU session from another SMF already exists towards the same DNN, the AMF either rejects the EBI assignment request, or revokes the EBI(s) from the existing PDU session(s) to the same DNN but different SMF. The AMF makes the decision based on the operator policy.</p> <p><b>Note</b> The preceding statement applies only when the S-NSSAI(s) for the PDU sessions are different, otherwise the same SMF is selected for PDU sessions to the same DNN.</p>

Step	Description
8	<p>The PGW-C+SMF sends an N4 Session Establishment/Modification Request to the PGW-U+UPF.</p> <p>For home-routed roaming scenario, if the EBI is assigned successfully, the PGW-C+SMF prepares the CN Tunnel Info for each EPS bearer. If the CN Tunnel info is allocated by the PGW-C+SMF, the PGW-U tunnel info for the EPS bearer may be provided to PGW-U+UPF. If the CN Tunnel info is allocated by PGW-U+UPF, the PGW-U+UPF sends the PGW-U tunnel info for the EPS bearer to the PGW-C+SMF. The PGW-U+UPF is ready to receive the uplink packets from E-UTRAN.</p> <p><b>Note</b> In the home-routed roaming scenario, the PGW-C+SMF prepares the CN Tunnel Info for each EPS bearer and provides it to the V-SMF. Thus, when the UE moves to EPS network, the V-SMF does not need to interact with the PGW-C+SMF to get the EPS bearer context(s).</p> <p><b>Note</b> If the CN Tunnel info is allocated by the PGW-C+SMF and not provided to PGW-U+UPF at PDU session establishment, when the UE moves to the target RAT the PGW-U+UPF cannot receive uplink (UL) data until the PGW-C+SMF has provided the Tunnel Info to the PGW-U+UPF in N4 Session Modification. This causes a short interruption to the UL data during the inter-system handover execution.</p>
9	<p>If the PGW-C+SMF receives any EBI(s) from the AMF, it adds the EBI(s) received into the mapped EPS bearer context(s).</p> <p>In home-routed roaming scenario, the PGW-C+SMF generates EPS bearer context, which includes per EPS bearer PGW-U tunnel information. In addition, if the default EPS bearer is generated for the corresponding PDN Connection of PDU Session (that is, during the PDU Session establishment procedure), the PGW-C+SMF generates the PGW-C tunnel information of the PDN connection and includes it in UE EPS PDN connection.</p>
9a	<p>(Conditional) In non-roaming or LBO scenario, the PGW-C+SMF includes the mapped EPS bearer context(s) and the corresponding QoS Flow(s) to be sent to the UE in the N1 SM container. PGW-C+SMF also indicates the mapping between the QoS flow(s) and mapped EPS bearer context(s) in the N1 SM container. PGW-C+SMF also includes the mapping between the received EBI(s) and QFI(s) in the N2 SM information to be sent to the NG-RAN. The PGW-C+SMF sends the N1 SM container and N2 SM information to the AMF via Namf_Communication_N1N2MessageTransfer.</p>
9b	<p>(Conditional) In home-routed roaming scenario, the PGW-C+SMF sends the mapped EPS bearer context(s), the mapping between the received EBI(s) and QFI(s), and EPS bearer context to the V-SMF via Nsmf_PDUSession_Create Response during PDU Session Establishment, or via Nsmf_PDUSession_Update Request during PDU Session Modification. The V-SMF stores the EPS bearer context, and generates N1 SM container and N2 SM information, and forwards them to the AMF via Namf_Communication_N1N2MessageTransfer.</p>
10	<p>The N1 SM container and N2 SM information are sent to the UE and NG-RAN respectively. The relevant steps of the procedure are executed as specified in the preceding figure.</p>

## Standards Compliance

This feature complies with the following standards:

- 3GPP TS 23.401, Version 15.6.0
- 3GPP TS 23.502, Version 15.4.0

## Limitations

TFT IE in mapped EPS bearer context is currently not supported.

## Generating EPS PDN Connection Parameters from 5G PDU Session Parameters

This section describes how to generate the EPS PDN connection parameters from the 5G PDU session parameters in the PGW-C+SMF.

When the PGW-C+SMF is requested to set up or modify a PDN connection or a PDU session that supports interworking between EPS and 5GC, the PGW-C+SMF generates the PDN connection parameters from the PDU session parameters.

When the PGW-C+SMF generates the PDN connection parameters based on the PDU session parameters, the following rules hold:

- **PDN Type:** The PDN type is set to IPv4 or IPv6 if the PDU Session Type is IPv4 or IPv6 respectively. The PDN type is set to Non-IP for Ethernet and Unstructured PDU Session Types.
- **EPS Bearer ID:** The EBI is requested from the AMF during the establishment of a QoS Flow as described in *3GPP TS 23.502, section 4.11.1.4.1*, for PDU sessions that support interworking between EPS and 5GC. The EBI is obtained from MME during the establishment of an EPS bearer (that is triggered by an establishment of the QoS Flow) as defined in *3GPP TS 23.401* for PDN connections hosted by PGW-C+SMF. The association between EBI and QoS Flow is stored by the SMF.
- **APN-AMBR:** APN-AMBR is set according to the operator policy. For example, taking the session AMBR into account.
- **EPS QoS parameters (including ARP, QCI, GBR, and MBR):**
  - If the QoS Flow is mapped to one EPS bearer: ARP, GBR, and MBR of the EPS bearer is set to the respective ARP, GFBR, and MFBR of the corresponding QoS Flow.
  - For standardized 5QIs, the QCI is mapped 1:1 to the 5QI. For non-standardized 5QIs, the PGW-C+SMF derives the QCI based on the 5QI and operator policy.



---

**Note** A GBR QoS flow is mapped 1:1 to a GBR dedicated EPS Bearer if an EBI has been assigned. All other GBR QoS flows will be terminated during interworking. If multiple QoS flows are mapped to one EPS bearer, the EPS bearer parameters are set based on the operator policy. For example, EPS bearer QoS parameters are set according to the highest QoS of all mapped QoS flows.

---



---

**Note** Non-GBR QoS flows for which no EBI has been assigned are mapped to the default EPS bearer.

---

# 5G to EPS Handover Using N26 Interface

## Feature Description

The SMF supports handover of PDU sessions to EPS on 5GC when the N26 interface is present between the MME and the AMF. The handover supports the creation of applicable default and dedicated bearers.

## How it Works

This section describes the 5G to EPS handover procedure and the 5G to EPS handover cancellation procedure.

## Call Flows

This section describes the following call flows:

- 5G to EPS Handover Call Flow
- 5G to EPS Handover Cancellation Flow

### *5G to EPS Handover Call Flow*

This section describes the 5G to EPS handover call flow with N26 interface.

The 5G to EPS Handover procedure for the EPS session is compliant with 3GPP 23.502, section 4.11.1.2.1.

1. The AMF requests the SMF to provide the SM Context using `Nsmf_PDUSession_ContextRequest`.
2. The SMF sends N4 Session Modification to the UPF to establish the CN tunnel for each EPS bearer. The bearer mapping to the 5G QoS and PCC rules received from PCC must already be present with the SMF. The SMF must also have the bearer IDs obtained from the Bearer ID Allocation procedure. The SMF creates new PDRs for the N4 session and gets TEID allocated for each bearer as required by the 4G system.
3. The SMF provides EPS bearer contexts to the AMF. The SMF also provides the CN tunnel information to AMF for all bearers for the uplink traffic from E-UTRAN.
4. If indirect data forwarding applies, the AMF sends the `Nsmf_PDUSession_UpdateSMContext Request` (S-GW address(es) and S-GW DL TEID(s) for data forwarding) to the SMF, for creating the indirect data forwarding tunnel.
5. The SMF sends N4 Modification Request to the UPF to create additional PDRs and FARs to receive the redirected DL data over the indirect tunnel from NG RAN and forwards them to eNodeB. The uplink PDRs must have QFI to match the forwarded DL data from NG-RAN and the associated QER will not have QFI as data needs to be forwarded to the eNodeB. The FAR redirects the received data to the eNodeB over appropriate tunnel based on the QFI.
6. The S-GW sends Modify Bearer Request to the SMF with DL TEIDs on the SMF for the bearers.
7. The SMF sends N4 Modification Request to the UPF to activate the DL data path to E-UTRAN. At this time, both the indirect tunnel and the direct DL path are activated towards the eNodeB.
8. The SMF sends the Modify Bearer Response to S-GW.

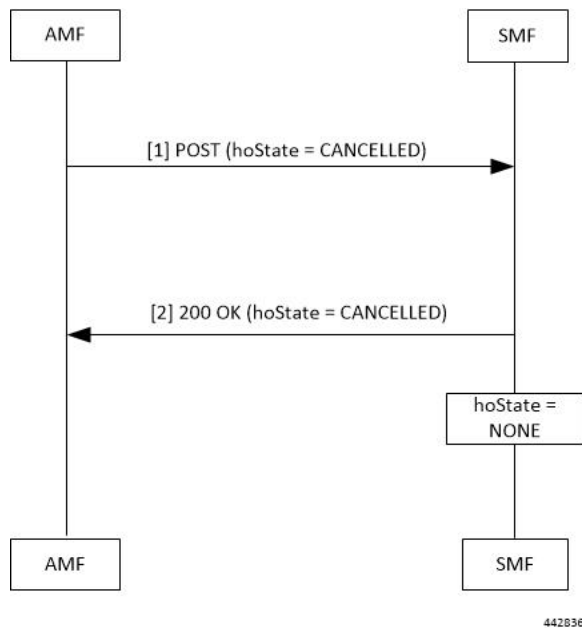
9. The AMF initiates Nsmf\_PDUSession\_UpdateSMContext Request service operation with an indication to release the forwarding tunnels.
10. The SMF sends N4 Modification Request to the UPF to remove the PDRs and FARs for the indirect tunnels. The PDRs and FARs for the 5G session which are not required are also removed.

**5G to EPS Handover Cancellation Call Flow**

When the Source Radio Access Network (RAN) triggers a handover cancellation after the preparation phase, the AMF invokes the "Nsmf\_PDUSession\_UpdateSMContext request (SUPI, Relocation Cancel Indication) toward the SMF. Based on the Relocation Cancel Indication, the SMF deletes the session resources established during the handover preparation phase. That is, the SMF removes all the Packet Detection Rules (PDRs), Forwarding Action Rules (FARs), and other rules that were allocated in preparation of handoff for indirect tunnel and the 5G session.

The following call flow depicts the 5GS to EPS handover cancellation procedure.

**Figure 57: 5GS to EPS Handover Cancellation Call Flow**



**Table 97: 5GS to EPS Handover Cancellation Call Flow Description**

Step	Description
1	The AMF requests the SMF to cancel the handover of an existing PDU session by sending a POST request for Sm Context Update service, with the following information: <ul style="list-style-type: none"> <li>• updating the hoState attribute of the individual SM Context resource in the SMF to CANCELLED</li> <li>• cause information</li> </ul>

Step	Description
2	<p>The SMF returns a 200 OK response message including the following information:</p> <ul style="list-style-type: none"> <li>• hoState attribute set to CANCELLED</li> </ul> <p>The SMF cancels the execution of the handover, for example, releases the resources reserved for the handover to the target RAN. Then, the SMF sets the hoState to NONE and deletes any stored targetServingNfId.</p>

## Standards Compliance

The 5G to EPS Handover feature complies with the *3GPP TS 23.502, version 15.3.0*.

# Create Dedicated Bearer Delay and Retry Support

## Feature Description

The Create Dedicated Bearer Delay and Retry Support feature facilitates the following:

- Delays the creation of the dedicated bearer that is based on the configured time after handover is complete.
- Retries the creation of the dedicated bearer for the IMS bearer in either of the following scenarios:
  - When the MME fails with the handover in progress.
  - When the IMS bearer is temporarily unreachable.
- After the handover is complete, the SMF service starts with the configured timer. Then, the dedicated bearer creation begins.
- If the IMS dedicated bearer creation fails, the maximum retries configuration determines the number of retries the creation process attempts. The configured timeout determines the delay of each retry attempt.

## How It Works

This section provides a brief of how the Create Dedicated Bearer Delay and Retry Support feature works.

## Call Flows

This section includes the following call flow.

Figure 58: EPS Fallback Guard Timer Call Flow

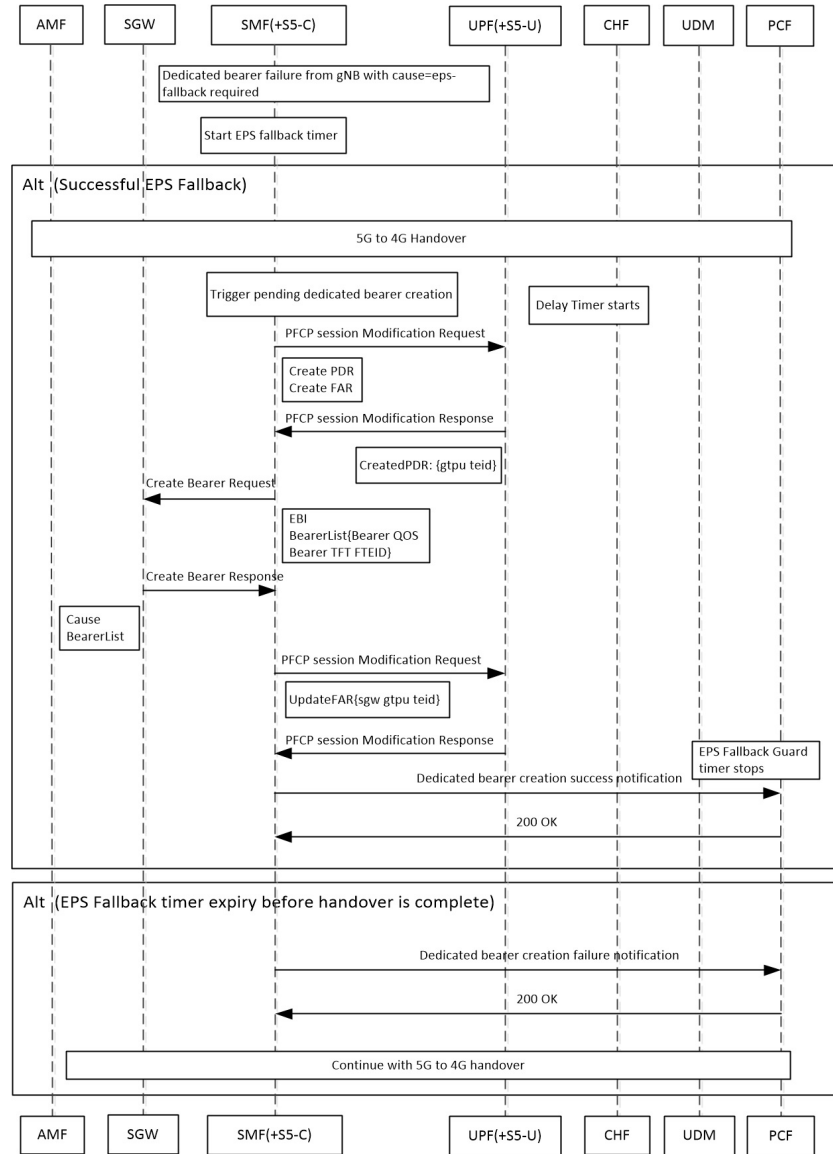


Table 98: EPS Fallback Guard Timer Call Flow Description

Step	Description
1	gNB sends the dedicated bearer creation failure information with the fallback cause through AMF.
2	EPS fallback timer starts.
With the successful EPS fallback following the 5G to 4G handover, steps 3 to 12 occur.	
3	EPS triggers pending dedicated bearer creation.
4	Delay timer starts.
5	SMF (+S5-C) sends the PFCP session modification request to UPF (+S5-U).

Step	Description
6	PDR and FAR are created.
7	UPF (+S5-U) sends the PFCP session modification response to SMF (+S5-C).
8	The information on the created PDR with the GTP-U TEID is available.
9	SMF (+S5-C) sends the Create Bearer Request to S-GW.
10	S-GW sends the Create Bearer Response to SMF (+S5-C).
11	SMF (+S5-C) sends the PFCP Session Modification Request to UPF (+S5-U).
12	UPF (+S5-U) sends the notification of the successful dedicated bearer creation to PCF.
13	EPS Fallback Guard Timer stops.
14	PCF sends the “200 OK” acknowledgment to SMF (+S5-C).
In the EPS fallback timer expiry before handover completion scenario, steps 13 to 15 occur.	
15	SMF (+S5-C) sends the failure notification of the dedicated bearer creation to PCF.
16	PCF sends the “200 OK” acknowledgment to SMF (+S5-C).
17	The 5G to 4G handover procedure continues.

## Configuring Create Dedicated Bearer Delay and Retry Support

This section describes how to configure the Create Dedicated Bearer Delay and Retry Support feature.

### configure

```

profile access accesstemp
  eps-fallback cbr delay delay_time max-retry retry_count
  timeout timeout_value
end

```

### NOTES:

- **delay** *delay\_time*: Specifies the time delay in milliseconds for the creation of the dedicated bearer. The valid values range 0 through 10000 milliseconds. The default is 0.
- **max-retry** *retry\_count*: Specifies the number of times to retry the creation of the dedicated bearer. The valid values range from 0 through 10. The default is 0.
- **timeout** *timeout\_value*: Specifies the time gap in seconds before retrying the creation of the dedicated bearer. The valid values range from 1 through 3 seconds. The default is 1.

### Verifying the Create Dedicated Bearer Delay and Retry Support Configuration

This section describes how to verify the Create Dedicated Bearer Delay and Retry Support configuration.

Use the **show running-config** command to view the configuration.

The following is a sample output of the **show running-config** command.

```

profile smf smf1
service name smf-service
  access-profile access1

```



```
!  
!  
profile access access1  
eps-fallback cbr delay 100 max-retry 5 timeout 2
```

# Handling GTP-U Error Indication for 4G Sessions

## Feature Description

This section describes how the SMF handles GPRS tunneling protocol, user plane (GTP-U) error indication for the 4G sessions.

Serving Gateway (S-GW) sends GTP-U error indication message including the tunnel IDs to UPF when it receives a GTP-U message with an unknown Tunnel Endpoint Identifier (TEID). The UPF on receiving GTP-U error indication sends N4SessionReportRequest towards SMF including error indication (ERIR). The SMF retrieves EBI based on Fteid included in the N4SessionReportRequest, and initiates deletion of the session or bearer. The SMF sends Delete Bearer Request towards S-GW. On receiving the response from S-GW, the SMF sends either an N4 session modification request or N4 session release request to the UPF based on the bearer type, that is, dedicated or default bearer. CHF and PCF are also notified based on the bearer type.



---

**Note** When the SMF receives PFCPSessionReportRequest, the IntSelfTxnN4SessRptReq message is displayed as part of the debug message.

---

## Standards Compliance

The GTP-U Error Indication Handling feature complies with the following standards:

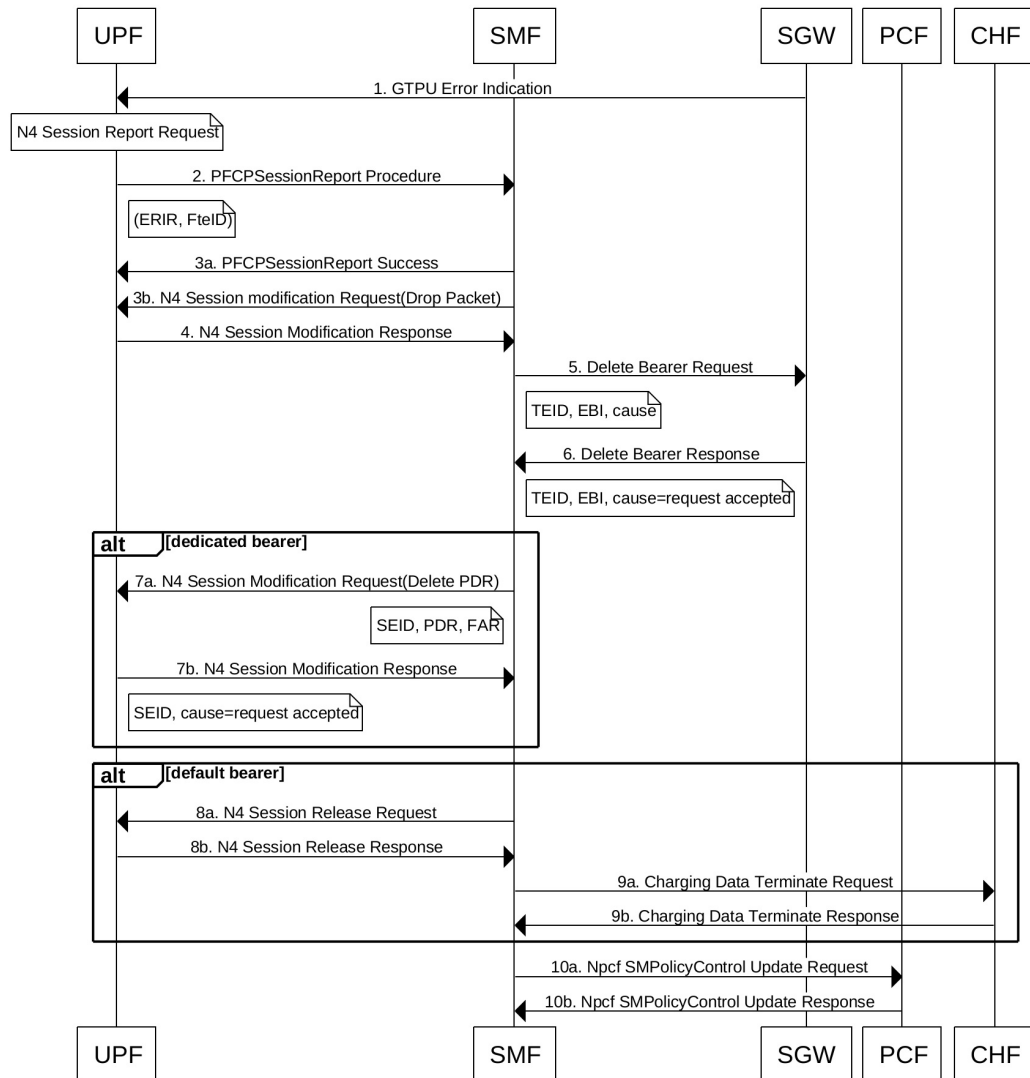
- 3GPP TS 29.244, Version 15.6.0
- 3GPP TS 23.527, Version 15.3.0

## How it Works

### GTP-U Error Handling Procedure

This section describes the call flow associated with the GTP-U error handling procedure for the 4G sessions.

Figure 59: GTP-U Error Indication Handling Call Flow



441621

Table 99: GTP-U Error Handling Call Flow Description

Step	Description
1	S-GW sends GTP-U Error Indication towards UPF, indicating the bearer with the failed bearer ID.
2	After receiving GTP-U error indication, the UPF sends PFCPSessionReport towards SMF along with the failed bearer ID.
3a and 3b	The SMF sends PFCPSessionReport Success message and N4 Session Modification Request for dropped packet towards the UPF.
4	The UPF sends N4 Session Modification Response to the SMF.

Step	Description
5	The SMF sends Delete Bearer Request towards S-GW along with TEID, EBI, and cause.
6	The S-GW sends Delete Bearer Response towards SMF along with TEID, EBI, and cause as request accepted.
7a	If the TEID is a dedicated bearer, then the SMF sends N4 Session Modification Request with Delete PDR.
7b	The UPF sends N4 Session Modification Response.
8a	If it is a default bearer, the SMF sends N4 Session Release Request.
8b	The UPF sends N4 Session Release Response.
9a	The SMF sends Charging Data Terminate Request towards CHF.
9b	The CHF responds with Charging Data Terminate Response.
10a	The SMF sends SMPolicyControl Update Request towards PCF.
10b	The PCF sends SMPolicyControl Update Response to the SMF.

## GTP Path Failure Handling, Restoration, and Recovery

### Feature Description

SMF now supports:

- Handling of the following GTP-C path management messages as per *3GPP TS 29.274*
  - Echo Request
  - Echo Response
- Sending Echo Request message to the newly discovered GTP-C peer as per the configuration.
- Sending Echo Response message as a reply if it receives Echo Request message from GTP-C peer.
- Retransmitting Echo Request message to GTP-C peer for configured number of times if no response is received.
- Clearing all the subscribers associated to a GTP-C peer if no response is received for Echo Request message for configured number of times for that GTP-C peer.
- Clearing all the subscribers associated to a GTP-C peer if a different recovery value is received from that GTP-C peer.

The feature complies with the following standards:

- *3GPP TS 29.274*
- *3GPP TS 23.007*

# Call Flows

The following call flows captures information specific to how GTP-C path management and GTP-C restoration messages are handled.

## GTP-C Path Management

Figure 60: GTP-C Path Management

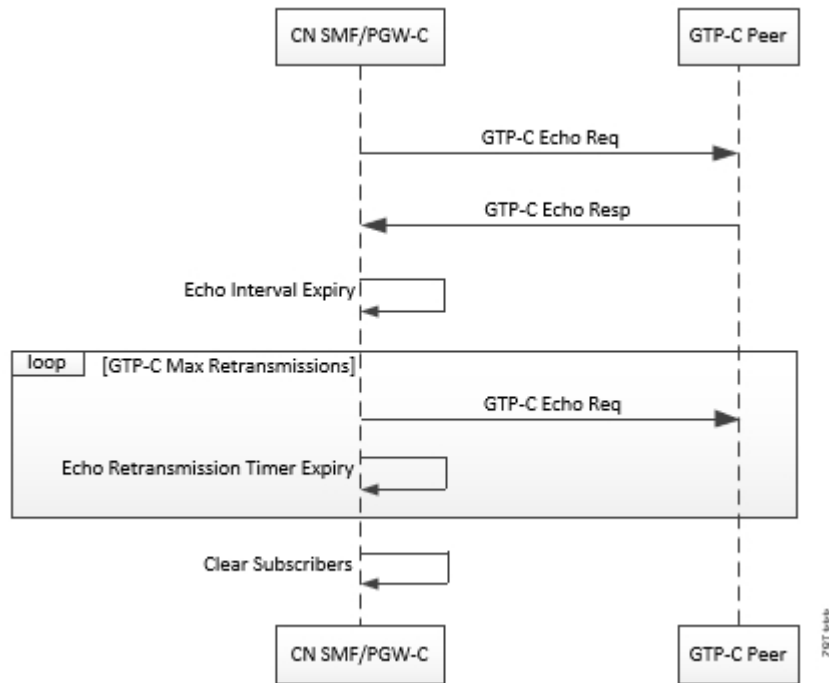


Table 100: GTP-C Path Management

Step	Description
1	Once the GTP-C peer is discovered (an Initial GTP-C Create Session Request or an GTP-C Modify Bearer Request message is received), CN SMF/PGW-C starts sending GTP-C Echo Request Messages periodically to the new GTP-C Peer as per configuration.
2	If GTP-C Echo response is not received, CN SMF/PGW-C retries sending GTP-C Echo Request (configured) N3 times for every configured T3 timer expiry.
3	Once all retries are exhausted, CN SMF/PGW-C clears all the sessions associated to that GTP-C peer.

## GTP-C Echo Request Handling

Figure 61: GTP-C Echo Request Handling

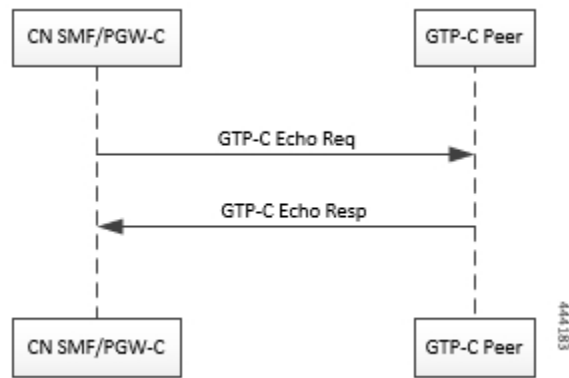


Table 101: GTP-C Echo Request Handling

Step	Description
1	Whenever a GTP-C Echo Request message is received from a GTP-C peer, CN SMF/PGW-C sends GTP-C Echo Response message as a reply.

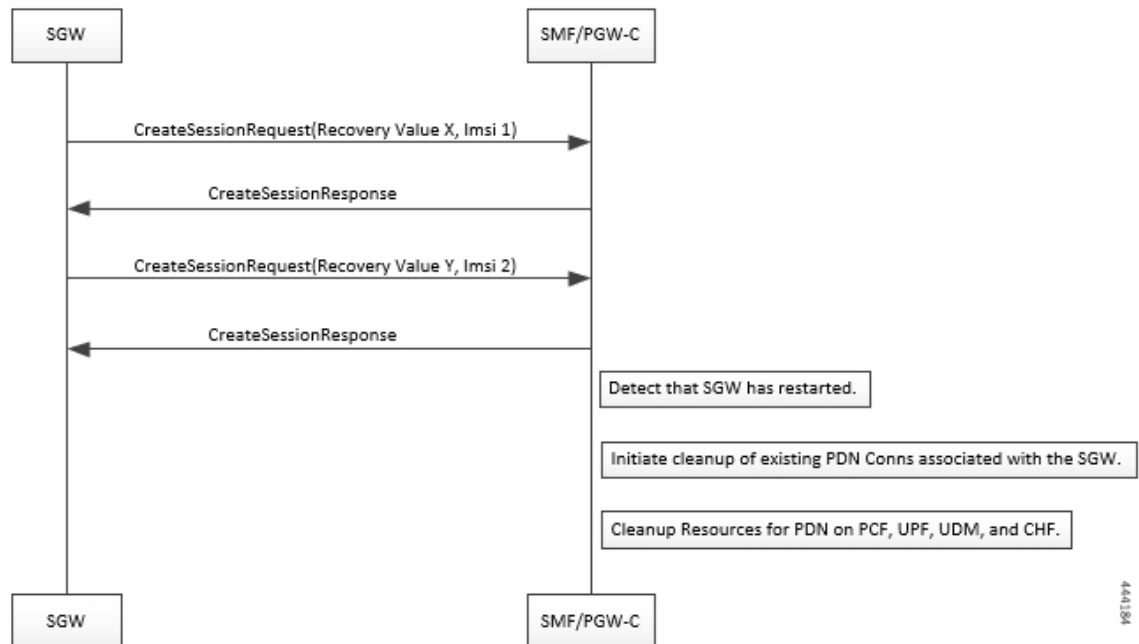
## GTP-C Restoration on PGW-C/SMF

PGW-C/SMF can detect that there is a change in recovery value of SGW. PGW-C/SMF can detect this value from the following messages:

- Create Session Request
- Modify Bearer Request
- Create Bearer Response
- Echo Response

If PGW-C/SMF detects that there is a change in recovery value, then it initiates the cleanup of all the PDN connections associated with the SGW.

Figure 62: GTP Restoration due to SGW Restart



## Memory and Performance Impact

The Node Manager pod to GTP-C peer path mapping is maintained in etcd and also in the local cache of NodeMgr and GTP-C Pods.

## Configuring Echo at GTP Endpoint

Use the following sample configuration to configure the echo parameters at GTP endpoint.

**config**

```

endpoint gtp
  interface { s2b | s5 | s5e | s8 | s11 }
  echo interval echo_interval
  echo retransmission-timeout retransmission_timeout_value
  echo max-retransmissions max_retry_count
  
```

## Sample Configuration

```

[unknown] smf# config
Entering configuration mode terminal

[unknown] smf(config)# endpoint gtp
[unknown] smf(config-endpoint-gtp)#
[unknown] smf(config-endpoint-gtp)# interface
s2b s5 s5e s8 s11
[unknown] smf(config-endpoint-gtp)# interface s5
[unknown] smf(config-interface-s5)# echo interval 60
echo - Enable gtpc path management
  
```

```

interval - Configure echo interval in seconds, ranging from <60-360>
[unknown] smf(config-interface-s5)# echo retransmission-timeout 3
retransmission-timeout - Configure the echo retransmission timeout in seconds, ranging from
<1-20>
[unknown] smf(config-interface-s5)# echo max-retransmissions 10
max-retransmissions - Configure maximum retries for GTP echo request, ranging from <0-10>
[unknown] smf(config-interface-s5)#

```

## Show Command

The `show peers` command displays all the connected GTP peers and their node information.

### Example:

## Bulk Statistics

The following dedicated disconnect reasons are used for PDN connections cleared due to peer GTP-C restart or path failure.

- `disc_pdnrel_gtpc_peer_restart`
- `disc_pdnrel_gtpc_peer_pathfail`

The following bulk statistics are added in `nodemgr` pod.

```

# HELP nodemgr_gtpc_msg_stats Gtpc Msg Stats
# TYPE nodemgr_gtpc_msg_stats counter
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_req_rx",gtpc_peer_ip="10.105.35.209",instance_id="0",service_name="nodemgr"}
1
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_req_tx",gtpc_peer_ip="10.105.35.209",instance_id="0",service_name="nodemgr"}
4
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_res_rx",gtpc_peer_ip="10.105.35.209",instance_id="0",service_name="nodemgr"}
1
nodemgr_gtpc_msg_stats{app_name="SMF",cluster="Local",data_center="DC",
gtpc_msg_type="gtpc_echo_res_tx",gtpc_peer_ip="10.105.35.209",instance_id="0",service_name="nodemgr"}
1
# HELP nodemgr_gtpc_peer_status Gtpc Peer Status
# TYPE nodemgr_gtpc_peer_status counter
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",
gtpc_peer_ip="10.105.35.209",gtpc_peer_status="gtpc_peer_path_down",instance_id="0",service_name="nodemgr"}
1
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",
gtpc_peer_ip="10.105.35.209",gtpc_peer_status="gtpc_peer_path_up",instance_id="0",service_name="nodemgr"}
1
nodemgr_gtpc_peer_status{app_name="SMF",cluster="Local",data_center="DC",
gtpc_peer_ip="10.105.35.209",gtpc_peer_status="gtpc_peer_restarted",instance_id="0",service_name="nodemgr"}
1

```

## Limitations

**From 3GPP TS 23.007, Section 20:** It is recommended that GTPv2 Echo Request should be sent only when a GTP-C entity has not received any GTP response message for a previously sent request message on the GTP-C path for, an implementation dependent time period.

Currently, this is not supported.

Even if SMF receives GTPC echo req from peer, it is considered as path is up. The subsequent Echo Req from SMF is received after the echo interval expiry.

## Configuration Support for Rejecting 4G-only Devices

The SMF provides configuration support to reject calls from 4G-only UE devices.

To reject calls from 4G-only UE devices, use the following configuration:

```
configure
  profile dnn dnnprofile_name
    only-nr-capable-ue true
  end
```

### NOTES:

- **only-nr-capable-ue true:** Enable this command to reject any new call attempt for PDN session creation from a 4G only capable UE device.

## Dynamic Configuration Change Support

### Feature Description

The SMF allows you to change Access Profile configuration dynamically, without any impact on the existing sessions. For instance, when the configuration dynamically updates the current session continues to use the old values in the in-progress call flow or procedure.

### How it Works

This section describes how dynamic change in configuration works for the supported Access Profile configurations.

### Access Profile

The Access Profile defines the various parameters for the access-profile configuration.

The following table lists the configurations that allow dynamic update.

**Table 102: Access Profile Parameters**

Configuration Parameters	Configuration	Dynamic Change	Impact on Existing Sessions
eps-fallback cbr	<b>eps-fallback cbr delay</b> <i>delay</i> <b>max-retry</b> <i>retry_count</i> <b>timeout</b> <i>timeout</i>	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.



Configuration Parameters	Configuration	Dynamic Change	Impact on Existing Sessions
n1 t3591-pdu-mod-cmd	<b>n1 t3591-pdu-mod-cmd timeout</b> <i>timeout max-retry</i> <i>retry_count</i>	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.
n1 t3592-pdu-rel-cmd	<b>n1 t3592-pdu-rel-cmd timeout</b> <i>timeout max-retry</i> <i>retry_count</i>	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.  <b>Note</b> The SMF does not support the timer functionality associated to this configuration.
n2 idft enable	<b>n2 idft enable timeout</b> <i>timeout</i>	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.
n26 idft enable	<b>n26 idft enable timeout</b> <i>timeout</i>	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.
n11 n11-failure-profile	<b>n11 n11-failure-profile</b> <i>failure_profile</i>	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.  If the associated Failure-Handling Profile gets deleted or any of the parameters are modified, then the existing call flows are not impacted, which means that the existing call flows continue using the old value.

Configuration Parameters	Configuration	Dynamic Change	Impact on Existing Sessions
gtpc gtpc-failure-profile	<b>gtpc gtpc-failure-profile</b> <i>failure_profile</i>	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.  If the associated Failure-Handling Profile gets deleted or any of the parameters are modified, then the existing call flows are not impacted, which means that the existing call flows continue using the old value.



## CHAPTER 22

# Flow Failure Handling for Access and Mobility Procedures

- [Feature Summary and Revision History, on page 301](#)
- [Feature Description, on page 302](#)

## Feature Summary and Revision History

### Summary Data

*Table 103: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 104: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

The SMF supports the QoS flow failures for access and mobility procedures. The SMF receives the QoS flow failure details as part of the following call flows from NG-RAN to N2 messages.

- Xn handover
- Service request procedures (UE and network-initiated)
- N2 handover with or without changing AMF
- N26 4G to 5G handover
- N26 5G to 4G handover

## How it Works

The SMF processes N11 messages with N2 message details to determine the accepted and failed QoS flow IDs. For failed QoS flow IDs, the SMF excludes the resources locally and communicates the following information to the external interfaces:

- Sends the N4 Session Modification Request to UPF to delete the QERs, URRs, UL or DL PDRs, UL or DL FARs which are applicable to the QoS flow IDs.
- Sends the Charging Data Update Request to CHF by including multi-unit usage details for the removed URRs. If SMF receives a usage report from UPF, SMF sends this report to CHF.
- Sends the N1 N2 transfer message with N1 message details to UE as the PDU Session Modification Command.
- Based on the received Policy Control Request Triggers and SM Policy Decision last Request Rule Data, SMF sends the Rule Reports SM Policy Control Update to PCF.

## Call Flows

This section describes the following call flows:

- QoS flow failure handling for Xn handover call flow
- QoS flow failure handling for N2 handover call flow
- QoS Flow failure handling for N26 4G to 5G handover call flow
- QoS flow failures for service request procedures
- PDU UE synchronization procedure
- Flow Failure Management Call Flows

### QoS Flow Failure Handling During Xn Handover

This section describes the QoS flow failure handling during the Xn handover.

Figure 63: QoS Flow Failure Handling during Xn Handover

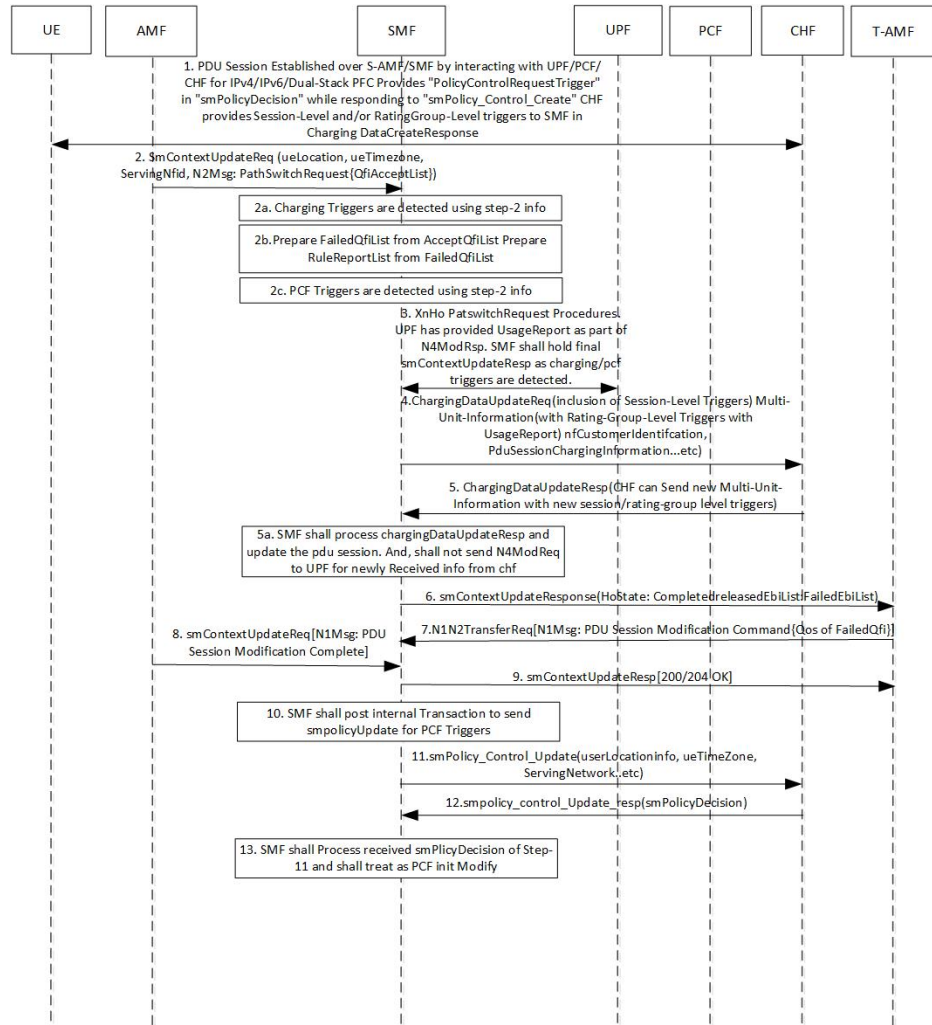


Table 105: QoS Flow Failure Handling Call Flow Description

Step	Description
1	<p>The PDU session is established over S-AMF and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack.</p> <p>The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control.</p> <p>The CHF provides session-level and rating-group-level triggers to the SMF as the Charging Data Create Response.</p>
2	<p>The AMF sends SM Context Update Request to SMF. This request includes the information on UE location, UE time zone, and N2 message path switch request with the list of the accepted QoS Flow Identifier (QFI).</p>

Step	Description
2a	The SMF identifies the access-side modifications that are received in SM Context Update Request. The charging triggers are identified through the information that is received in Step 2.
2b	The SMF extracts the list of failed QFI, failed rule report, and failed EPS bearer ID (EBI) from the received list of the accepted QFIs.
2c	The PCF triggers are identified through the information that is received in Step 2.
3	For Xn handover preparation procedures, the SMF sends the N4 Session Modification Request to the UPF to update the received DL tunnel information of T-gNB. After the tunnel information is updated, the UPF sends the usage report to the SMF as N4 modification response. The SMF retains the final SM Context Update Response as charging or PCF triggers are identified.
4	The SMF sends the Charging Data Update Request to the CHF. This request includes the details, such as session-level triggers, multi-unit information with rating-group-level triggers and usage report, customer identification information, and the PDU session charging information.
5	The CHF sends the Charging Data Update Response to the SMF. This response may include the multi-unit information with new session or rating-group-level triggers.
5a	The SMF processes the Charging Data Update Response and updates the PDU session. SMF does not send the N4 Mode Request to the UPF for the information that is received from the CHF.
6	The SMF sends the SM Context Update Response by including the N2 message path switch request acknowledgment and the list of failed EBI list.
7	The SMF and T-AMF process the N1 N2 Transfer Request for the PDU Session modification for the QoS about failed QFIs. The SMF includes the PDU Session Modification command to communicate the information on the QoS flow failure list to the UE.
8	The AMF sends the SM Context Update Request N1 message to the SMF to communicate about the handover completion.
9	The SMF sends the SM Context Update Response as “200/204 OK” to T-AMF. The SMF does not process the received N1 message from UE.
10	The SMF posts the internal transaction to send the SM Policy Update for PCF triggers to send to the PCF. The SMF posts this information to communicate Rule Report for the failed QFIs or any identified armed access-side triggers.
11	The SMF sends the SM Policy Control Update to the PCF. This update includes details, such as user location information and UE time zone.
12	The PCF sends the SM Policy Control Update Response, which is the SM policy decision, to the SMF.
13	The SMF processes the received SM policy decision and initiates the PCF modify procedures.

### QoS Flow Failure Handling During N2 Handover

This section describes the flow failure handling procedure during the N2 handover.

Figure 64: Flow Failure Handling During N2 Handover

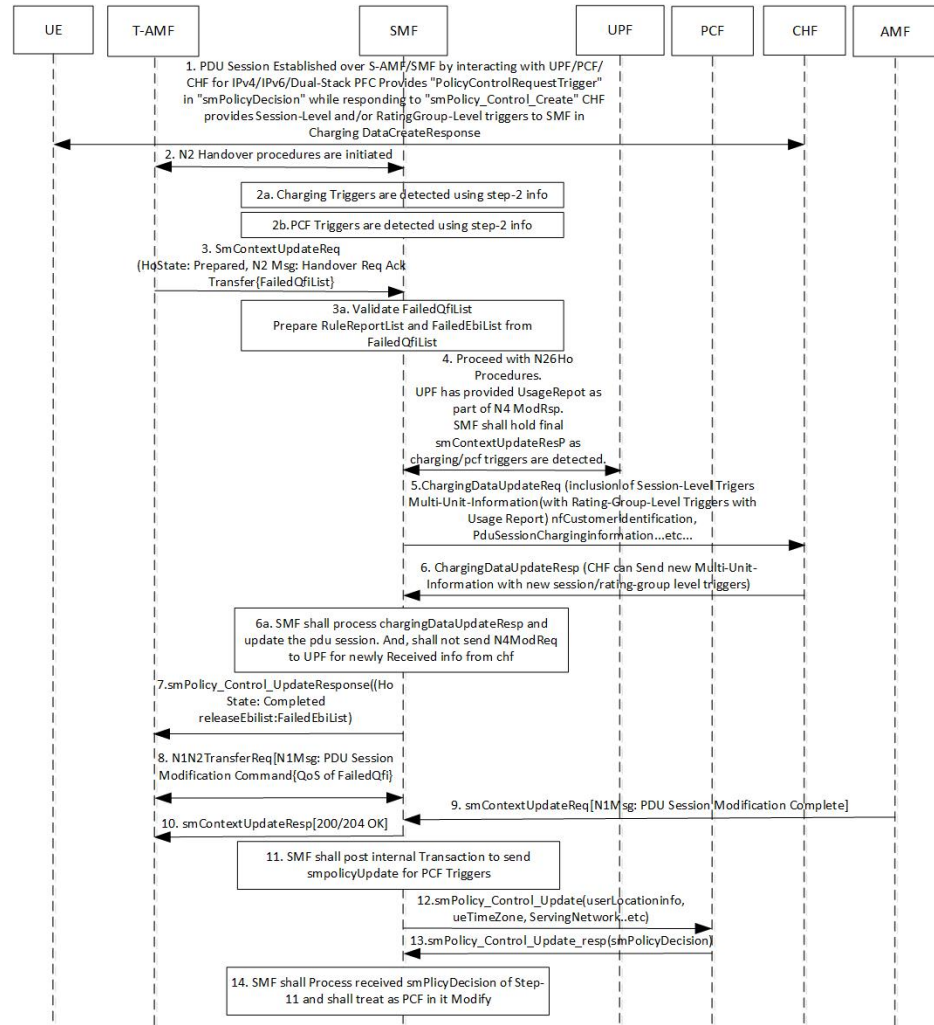


Table 106: Description for Flow Failure Handling During N2 Handover

Step	Description
1	<p>The PDU session is established over S-AMF and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack.</p> <p>The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control.</p> <p>The CHF provides session-level and rating-group-level triggers to the SMF as the Charging Data Create Response.</p>
2	<p>The T-AMF sends SM Context Update Request to the SMF. This request includes the information on handover state as preparing, UE location, UE time zone, target serving NF ID, and serving network. In case of inter-AMF handoff, the AMF includes the target serving NF ID.</p>

Step	Description
2a	The SMF identifies the access-side modifications that are received in SM Context Update Request. The charging triggers are identified through the information that is received in Step 2.
2b	The PCF triggers are identified through the information that is received in Step 2.
3	The T-AMF sends the SM Context Update Request to the SMF. This request includes the information on handover state as prepared along with N2 message on Handover Required Transfer Request. The transfer request includes the list of failed QFIs.
3a	The SMF validates the list of failed QFIs to extract the list of failed rule report and failed EBIs.
4	For N2 handover preparation procedures, the SMF sends the N4 Session Modification Request to the UPF to update the received DL tunnel information of T-gNB. After the tunnel information is updated, the UPF sends the usage report to the SMF as N4 modification response. The SMF retains the final SM Context Update Response as charging or PCF triggers are identified.
5	The SMF sends the Charging Data Update Request to the CHF. This request includes the details, such as session-level triggers, multi-unit information with rating-group-level triggers and usage report, customer identification information, and the PDU session charging information.
6	The CHF sends the Charging Data Update Response to the SMF. This response contains the multi-unit information along with new session-level or rating-group level triggers.
6a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 Mode Request to the UPF for the information that is received from the CHF.
7	The SMF sends the SM Context Update Response to the T-AMF with handover state as completed. This response also includes list of the released EBIs and the failed EBIs.
8	The SMF and T-AMF process the N1 N2 Transfer Request. This request includes the N1 message as PDU Session Modification Command to communicate the information on the QoS flow failure list to the UE.
9	The CHF sends the SM Context Update Request with an N1 message for the completion of the PDU session modification.
10	The SMF sends the SM Context Update Response as “200/204 OK” to the T-AMF. The SMF does not process the received N1 message from the UE.
11	The SMF posts the internal transaction to send the SM Policy Update for PCF triggers. The SMF sends this update to communicate the rule report about the failed QFIs or any armed access-side triggers.
12	The SMF sends the SM Policy Control Update to the PCF. This update includes the details on the user location and UE time zone.
13	The PCF sends the SM Policy Control Update response, which is the SM policy decision, to the SMF.
14	The SMF processes the SM policy decision and treats it as the PCF-initiated PDU Session Modification procedure.

### QoS Flow Failure Handling During N26 4G to 5G Handover

This section describes the flow failure handling procedure during the N26 4G to 5G handover.



Figure 65: QoS Flow Failure Handling During N26 4G to 5G Handover

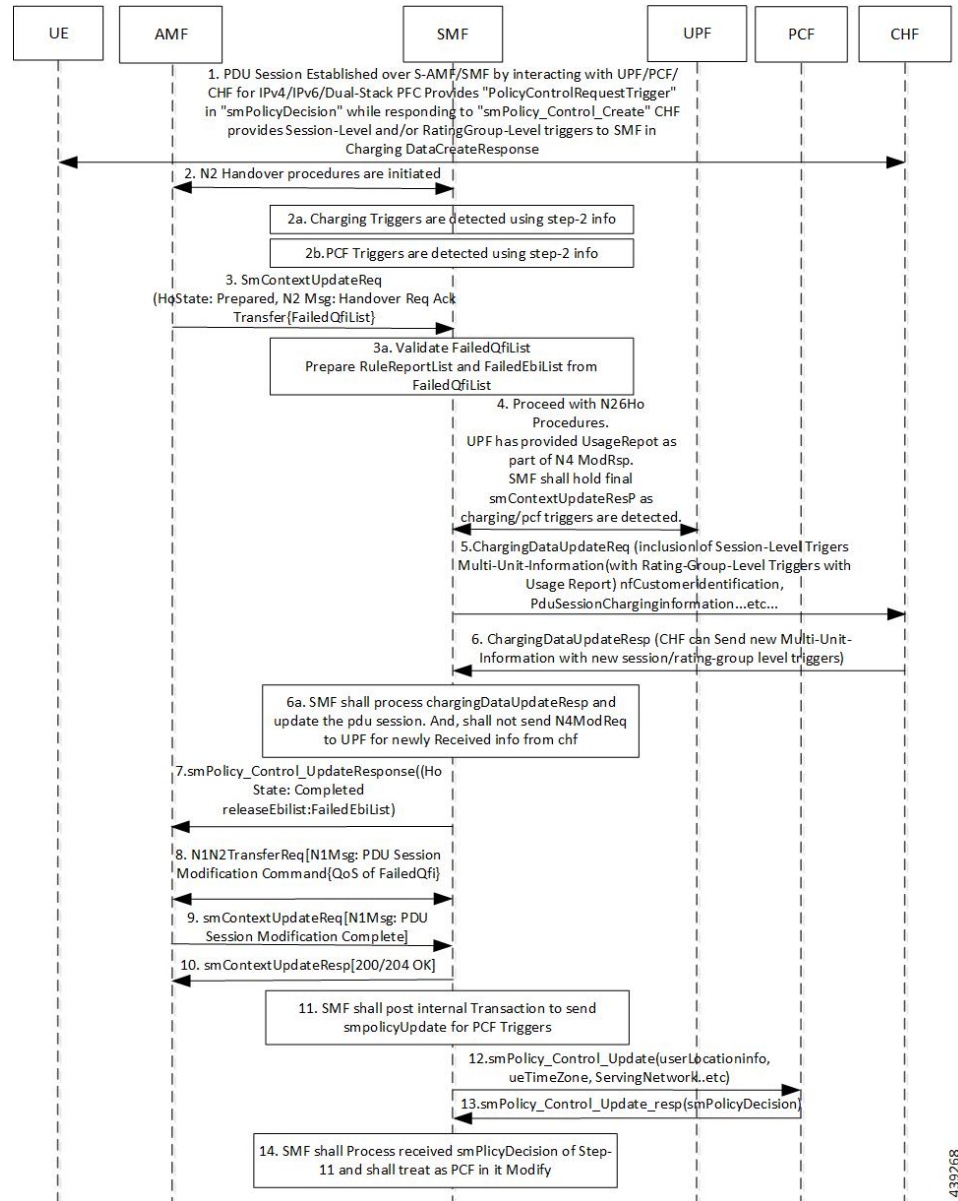


Table 107: Description for QoS Flow Failure Handling During N26 4G to 5G Handover

Step	Description
1	<p>The PDU session is established over S-AMF and SMF by communicating with UPF, PCF, or CHF for IPv4, IPv6, or dual-stack.</p> <p>The PCF provides Policy Control Request trigger for SM policy decision as response to the request for creation of SM policy control.</p> <p>The CHF provides session-level and rating-group-level triggers to the SMF as the Charging Data Create Response.</p>

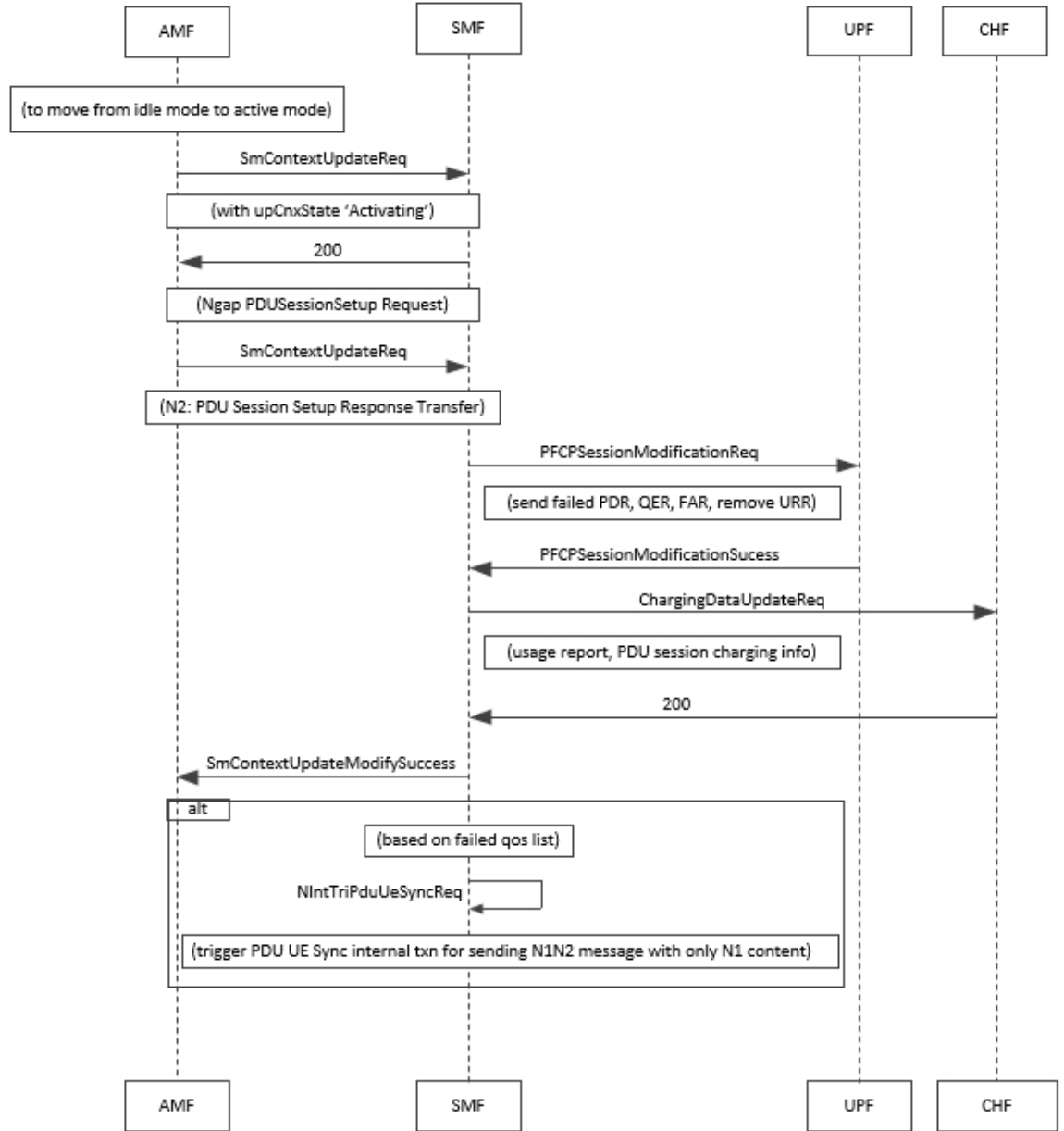
Step	Description
2	The T-AMF sends SM Context Update Request to the SMF. This request includes the information on handover state as prepared, UE location, UE time zone, target serving NF ID, serving network. In case of inter-AMF handoff, the AMF includes the target serving NF ID and the N2 message path switch request with the list of the accepted QFIs to the SMF.
2a	The SMF identifies the access-side modifications that are received in SM Context Update Request. The charging triggers are identified through the information that is received in Step 2.
2b	The PCF triggers are identified through the information that is received in Step 2.
3	The T-AMF sends the SM Context Update Request to the SMF. This request includes the information on handover state as prepared along with N2 message on Handover Required Transfer Request. The transfer request includes the list of failed QFIs.
3a	The SMF validates the list of failed QFIs to extract the list of failed rule report and failed EBIs.
4	For N26 handover preparation procedures, the SMF sends the N4 Session Modification Request to the UPF to update the received DL tunnel information of T-gNB. After the tunnel information is updated, the UPF sends the usage report to the SMF as N4 Modification Response. The SMF retains the final SM Context Update Response as charging or PCF triggers are identified.
5	The SMF sends the Charging Data Update Request to the CHF. This request includes the details, such as session-level triggers, multi-unit information with rating-group-level triggers and usage report, customer identification information, and the PDU session charging information.
6	The CHF sends the Charging Data Update Response to the SMF. This response contains the multi-unit information along with new session-level or rating-group level triggers.
6a	The SMF processes the Charging Data Update Response and updates the PDU session. The SMF does not send the N4 Mode Request to the UPF for the information that is received from the CHF.
7	The SMF sends the SM Context Update Response to the T-AMF with the handover state as completed. This response also includes list of the released EBIs and the failed EBIs.
8	The SMF and T-AMF process the N1 N2 Transfer Request. This request includes the N1 message as PDU Session Modification Command to communicate the information on the QoS flow failure list to the UE.
9	The CHF sends the SM Context Update Request with an N1 message for the completion of the PDU session modification.
10	the SMF sends the SM Context Update Response as “200/204 OK” to the T-AMF. The SMF does not process the received N1 message from the UE.
11	The SMF posts the internal transaction to send the SM Policy Update for PCF triggers. The SMF sends this update to communicate the rule report about the failed QFIs or any armed access-side triggers.
12	The SMF sends the SM Policy Control Update to the PCF. This update includes the details on the user location and UE time zone.
13	The PCF sends the SM Policy Control Update response, which is the SM policy decision, to the SMF.
14	The SMF processes the SM policy decision and treats it as the PCF-initiated PDU Session Modification procedure.

### QoS Flow Failures for Service Request Procedures

The SMF supports both UE and Network Service Request procedures. For these procedures, the SMF processes the received SM Context Update Request to update the N3 tunnel path from idle to active state.

The QoS flow failures for service request procedures are handled in the same way as described in the 3GPP 23.502, Section 4.2.3.2. However, QoS flow failure list is handled with the PDU Session Setup Response Transfer N2 message, which is received as SM Context Update Response when subscriber moves from Idle to Active State.

Figure 66: PDUIM Idle to Active Mode



444185

Table 108: QoS Flow Failures for Service Request Procedure

Step	Description
1	The SMF sends the SM Context Update Request message for the User Plane Connection State as Activated.
2	SMF sends 200 response along with PDU Session Setup Request towards AMF. AMF sends N2 message <b>PDU Session Setup Response Transfer</b> which contains QoS flow failure list.
3	SMF validates failed QFIs to extract failed PCC rules and failed flows.
4	SMF updates received DL tunnel information (gNB, delete PDRs, delete QERs). After the tunnel information is updated, SMF removes URR based on failed flows and sends N4 Session Modification Request towards UPF.
5	UPF provides usage report as part of N4 Session Modification Response. SMF sends SM Context Update Response for User Plane Connection State as Activated along with released EBIs as failed EBIs and triggers internal transaction to process charging and PCF triggers.
6	SMF sends Charging Data Update Request to CHF. This request includes the details, such as session-level triggers, multi-unit information with rating-group-level triggers and usage report, customer identification information, and the PDU session charging information.
7	SMF sends internal transaction based on failed QFIs to initiate PDU UE Sync Procedure to send N1/NAS signalling. Refer to PDU UE Sync Procedure call flow diagram for N1N2 message transfer

## PDU UE Synchronization Procedure

This section describes the UE synchronization procedure.

1. PDU UE synchronization procedure in idle mode receives the failed QFIs, QoS rules and EBIs.
2. UE synchronization procedure fills N1 message PDU Session Modification command with QoS Descriptions, QoS Rules, and EPS Bearer Context from received QFI, QoS rule ID, and EBI respectively.
3. The SMF includes the created N1 container to N11 message without any N2 content.
4. The SMF sends N1N2 Transfer Request message towards AMF and starts the N1N2 retransmission timer. The SMF waits for N1N2 Transfer Response.
5. If N1N2 Transfer Success is received, the SMF waits for SM Context Update Request with N1 update. The N1 update includes resource modify success/resource modify reject information.

## Statistics

This procedure creates statistics for the following events:

- N1N2TransferRequest Attempt
- N1 modify success
- N1 modify failure
- UE sync procedure suspend
- On resuming UE sync procedure if it was suspended by other procedure

### *N1N2 Retransmission*

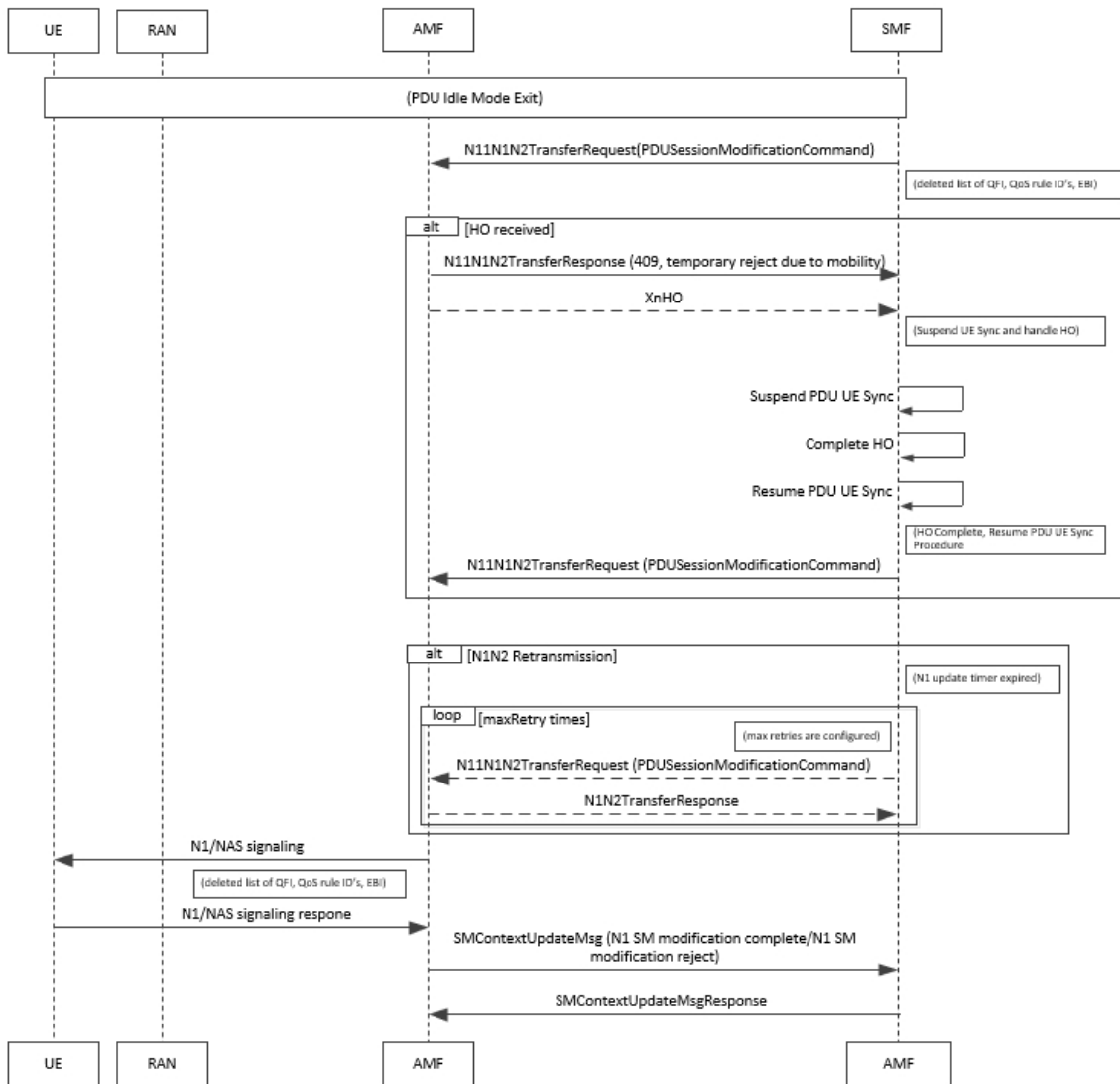
Once N1N2 retransmission timer expires, following action is taken:

1. SMF increments the N1N2 retry counter
2. SMF sends N1N2 Transfer Request message towards AMF and restarts the N1N2 retransmission timer. SMF waits for N1N2 Transfer Response.
3. If N1N2 Transfer Success is received, SMF waits for SM Context Update Request with N1 update. The N1 update includes resource modify success/resource modify reject information.
4. Once the N1N2 retry counter reaches the configured maximum number, the procedure is aborted.

### *Collision Case*

AMF informs SMF about HO procedure by rejecting the N1N2 Transfer Request with temporary reject cause. Also any other procedure can pre-empt the UE synchronization procedure while it is awaiting N1 update from the UE.

Figure 67: Collision Case



444186

Table 109: Collision Case

Step	Description
1	If N1N2 Transfer Failure with cause as <b>Temporary Reject Handover Ongoing</b> is received, SMF awaits HO procedure to pre-empt PDU UE Sync Procedure.
2	While awaiting N1 Update or handover from UE, if any procedure (including handover) is triggered then: <ul style="list-style-type: none"> <li>• If suspended by the handover procedure, it starts the N1N2 retry timer.</li> <li>• If aborted by PDU release or PDU setup procedure, it cleans up all the timers and aborts the N1N2 retry.</li> </ul>

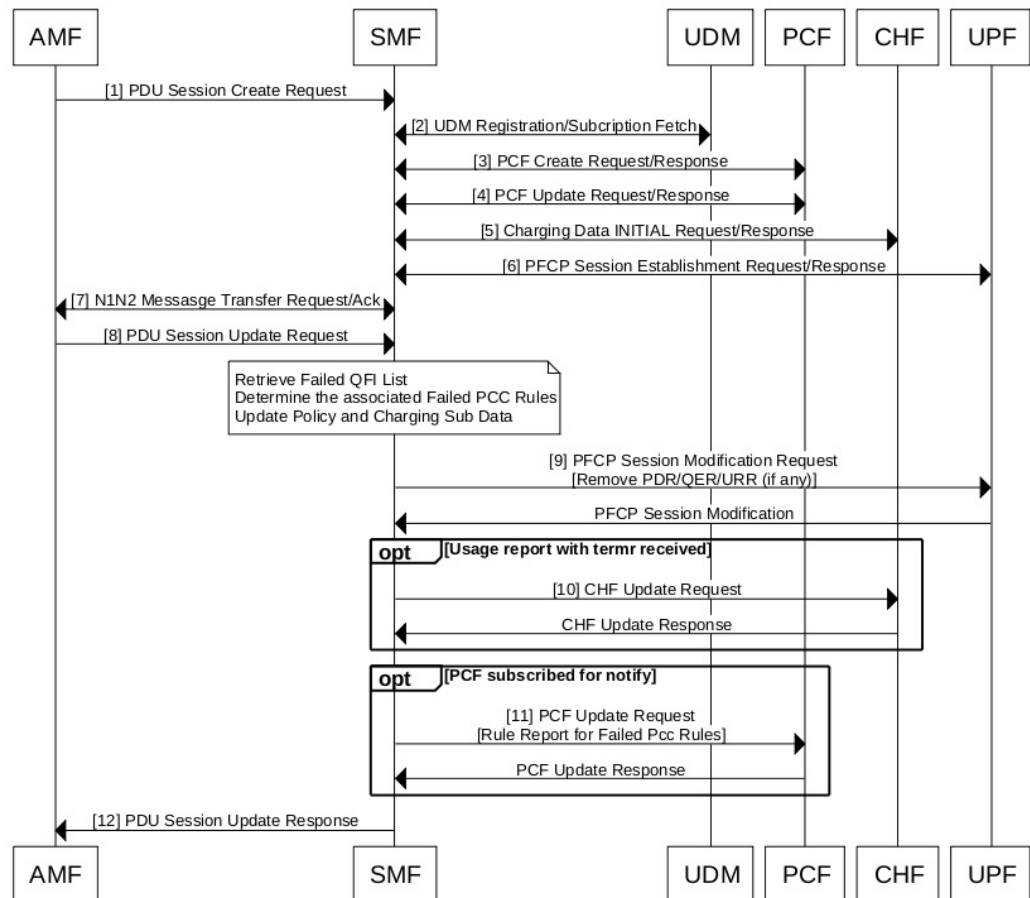
Step	Description
3	In case UE sync procedure is suspended by handover then on expiry of N1N2 Retry Timer, UE sync resumes after handover is processed.
4	On resuming if the UE sync procedure finds that the RAT has changed then it aborts the procedure and stop any timers.
5	On resuming the procedure in the same RAT the UE sync procedure reinitiates N1N2Transfer request message.

### Handling Failed QoS Flow Identifier During PDU Setup Procedure

The SMF supports handling of the failed QoS Flow Identifier (QFI) during the PDU setup procedure.

NG-RAN rejects a QoS flow due to various reasons. When the NG-RAN node reports unsuccessful establishment of a QoS flow, the SMF uses cause value to identify the reason for the unsuccessful establishment.

Figure 68: Handling Failed QFIs During PDU Setup



444991

Table 110: Description for Failed QFI Handling During PDU Setup

Step	Description
1-7	The SMF, AMF, UDM, PCF, CHF, and UPF communicate with each other to perform the PDU setup procedure as defined in the 3GPP specification.
8	The AMF sends SM Context Update Request to the SMF. This request carries N2 payload “PDU Session Resource Setup Response Transfer”. This message includes the list of QoS flows failed to be established, if any, in the QoS Flow Failed to Setup List IE.  The SMF marks the failed PCC rules and the charging descriptors associated with them for deletion.
9	The SMF sends PCF Session Modification message to the UPF. This message carries Remove Packet Detection Rules (PDR), Remove QoS Enforcement Rules (QER), and Remove Usage Reporting Rules (URR) for the failed PCC rules in addition to the existing Update FAR for Downlink (DL) Tunnel Endpoint Identifier (TEID) of the successful PCC rules.
10	The SMF sends the CHF Update Request message to the CHF upon receiving a termination request. The CHF sends the CHF Update Response as an acknowledgment.
11	If the PCF has subscribed for notification on failed PCC rules, the SMF sends PCF Update Request with rule report containing the failed PCC rules dropped by the NG-RAN.
12	The SMF sends the PDU Session Update Response to the AMF.  The SMF triggers internal transaction based on the failed QFI list. Then, the SMF initiates PDU UE Sync Procedure to send N1/NAS signalling.  The SMF notifies the UE about the failed QoS flows using N1 messaging, and the UPF and PCF nodes about the associated failed PCC rules.

### Handling Failed QoS Flow Identifier During PDU Session Modification

The SMF supports handling of the failed QoS flows over N2 interface during the PDU session modification.

If the modification of a PDU session or a QoS flow fails, the NG-RAN node falls back to the older configuration. That is, it falls back to the configuration of the session or the flow that was available before receiving the PDU SESSION RESOURCE MODIFY REQUEST message.

The SMF receives the QoS Flow Identifier for which the flow add/modify failed during the PDU SESSION RESOURCE MODIFY REQUEST.

If the new flow addition fails, the SMF performs the following:

- Removes the failed flow towards N1 (UE)
- Stops sending the failed flow-related information towards N4 (UPF)
- Stops sending the failed flow-related information towards N40 (CHF)
- Checks if the triggers are enabled and then sends the rule report for the failed flow towards N7 (PCF).

If the modification of flow fails, the SMF performs the following:

- Replaces the old information for the failed flow towards N1 (UE)
- Stops sending the modified flow-related information towards N4 (UPF)



- Stops sending the modified flow-related information towards N40 (CHF)
- Checks if the triggers are enabled and then sends the Rule Report for the failed flow towards N7 (PCF).

The following table captures the SMF behavior for the cause values included in the PDU Session Resource Modify Unsuccessful Transfer IE. These cause values are applicable for the PDU session modification procedure.

Cause Group	Cause Value	SMF Behavior	Comment
Radio Network Layer Cause			
	Unspecified		General
	Unknown PDU Session ID	Delete the session	N1 FiveGSM Cause reactivation requested
	Unknown QoS Flow ID	Send delete details to N1 Send PCF report about rule(s)	
	Multiple PDU Session ID Instances	Delete the session	
	Multiple QoS Flow ID Instances	Delete the session	N1 FiveGSM Cause reactivation requested
	Xn handover triggered	Act based on collision handling	
	Not supported 5QI value	Send delete details to N1 Send PCF report about rule(s)	
	IMS voice EPS fallback or RAT fallback triggered	Already supported	
Transport Layer Cause			
	Transport resource unavailable	Send delete details to N1 Send PCF report about rule(s)	
	Unspecified		
NAS Cause			
	Normal release	Delete the session	
	Authentication failure	Delete the session	
	Deregister	Delete the session	
	Unspecified	Delete the session	

Cause Group	Cause Value	SMF Behavior	Comment
Protocol Cause			
	Transfer syntax error	N1 rollback Error log fail procedure	
	Abstract syntax error (reject)	N1 rollback Error log fail procedure	
	Abstract syntax error (ignore and notify)	N1 rollback Error log fail procedure	
	Message not compatible with receiver state	N1 rollback Error log fail procedure	
	Semantic error	N1 rollback Error log fail procedure	
	Abstract syntax error (falsely constructed message)	N1 rollback Error log fail procedure	
	Unspecified	N1 rollback Error log fail procedure	
Miscellaneous Cause			
	Control processing overload	N1 rollback Error log fail procedure	
	Not enough user plane processing resources	N1 rollback Error log fail procedure	
	Hardware failure	Delete the session	
	O&M intervention	N1 rollback Error log fail procedure	
	Unknown PLMN	Delete the session	

### Bulk Statistics

The following statistics provide details about the failed QoS flows over the N2 interface.

- policy\_pdu\_flows\_total
  - total attempted
  - total succeeded

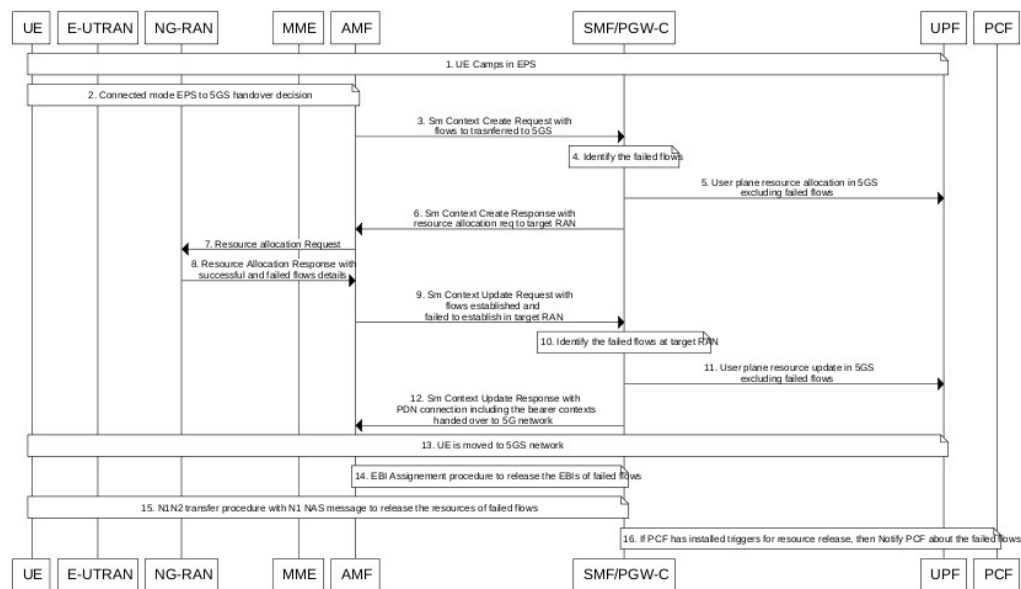
- total failed
- policy\_pdu\_flows\_current
  - current attempted
  - current succeeded
  - current failed

**Flow Failure Management Call Flows**

The following call flow provides the details of the different flow failure scenarios during the EPS to 5GS handover. This call flow also describes how the SMF manages these failures and keeps the flows intact across 5GS network elements and the subscriber.

- Flow failure from source in EPS to 5GS Handover
- Flow failure from target in EPS to 5GS Handover

**Figure 69: Flow Failure Management Call Flow**



442837

**Table 111: Flow Failure Management Call Flow Description**

Step	Description
1	The EPS interworking capable UE initially camps on the EPS network.
2	This step involves taking the connected mode EPS to 5GS handover decision.
3	During the EPS to 5GS handover procedure, the PDN Connection in the Sm Context Create request from the AMF carries the EPS bearer contexts to be handed over to 5GS network.

Step	Description
4	The SMF identifies the bearer contexts that were established in EPS and missing in PDN connection as failed flows.
5	The SMF performs the resource allocation in 5GS network and sends it to the UPF excluding the failed flows.
6	The SMF sends the Sm Context Create Response with resource allocation request to the target RAN.
7	The AMF forwards the resource allocation request to the NG-RAN.
8	The NG-RAN sends the resource allocation response with the details of successful and failed flows to the AMF.  The target RAN node may not be able to allocate the resources for all the requested flows during EPS to 5GS handover procedure. The target RAN shares information about such failed flows in the resource allocation response.
9	The AMF sends the Sm Context Update Request with flows established and failed to establish in the target RAN.
10	The SMF identifies the failed flows at the target RAN.
11	The SMF performs the user plane resource update in 5G network excluding the failed flows.
12	The SMF sends the Sm Context Update Response with PDN connection including the bearer contexts handed over to the 5GS network.
13	The UE is moved to the 5GS network.
14	The SMF uses the EBI assignment procedure to release the EBIs of failed flows.
15	The SMF sends the N1N2 transfer request with the N1 NAS message to the UE to remove the resources of failed flows.
16	If the PCF has installed triggers to release the resources, then the SMF notifies the PCF about the failed flows.

#### Handling of Flow Failures from Source in EPS to 5GS Handover

The following call flow depicts the handling of flow failure from source RAN in EPS to the 5GS handover.

Figure 70: Flow Failure Handling Call Flow (From Source in EPS to 5GS Handover)

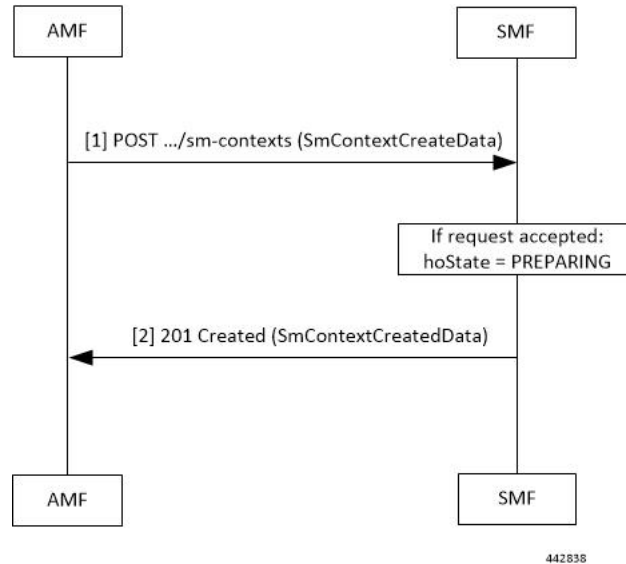


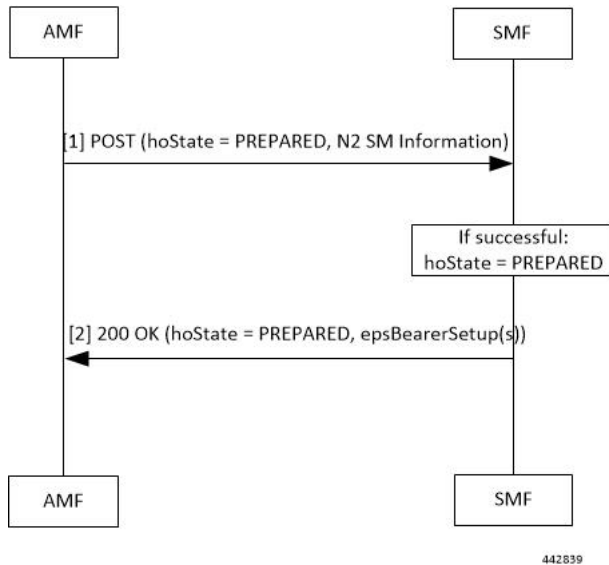
Table 112: Flow Failure Handling Call Flow Description (From Source in EPS to 5GS Handover)

Step	Description
1	<p>The AMF sends a POST request for Sm Context Create Service, with the following additional information:</p> <ul style="list-style-type: none"> <li>• UE EPS PDN connection, including the EPS bearer contexts, representing the individual SM context resource to be created. The UE EPS PDN connection may not carry the flows which source does not want to establish in the 5GS network.</li> <li>• hoState attribute set to PREPARING</li> <li>• targetId identifying the target RAN Node ID and TAI based on the Target ID IE received in the Forward Relocation Request message from the source MME.</li> </ul>
2	<p>If the corresponding PDU session is detected based on the EPS bearer contexts and the handover of the PDN connection to 5GS network is possible, then the SMF returns a 201 Created response including the following information:</p> <ul style="list-style-type: none"> <li>• hoState attribute set to PREPARING and N2 SM information to request the target RAN to assign resources to the PDU session, excluding the flows which are not received in the UE EPS PDN connection.</li> <li>• PDU Session ID corresponding to the default EPS bearer ID of the EPS PDN connection.</li> <li>• allocatedEbiList containing the EBIs allocated to the PDU session.</li> </ul> <p>The POST response includes the Location header and the URI of the created SM context resource.</p> <p>The AMF stores the association of the PDU Session ID and the SMF ID, and the allocated EBIs associated to the PDU Session ID.</p>

## Handling of Flow Failures from Target in EPS to 5GS Handover

The following call flow depicts the handling of flow failure from target RAN in EPS to the 5GS handover.

**Figure 71: Flow Failure Handling Call Flow (From Target in EPS to 5GS Handover)**



**Table 113: Flow Failure Handling Call Flow Description (From Target in EPS to 5GS Handover)**

Step	Description
1	<p>The AMF updates the SM context in the SMF by sending POST request with the following information:</p> <ul style="list-style-type: none"> <li>• hoState attribute set to PREPARED</li> <li>• N2 SM information received from the target RAN, including the transport layer address and tunnel endpoint of the downlink termination point for the user data for this PDU session (that is, GTP-U F-TEID of the target RAN for downlink traffic), if the target RAN succeeded in establishing resources for the PDU session; the target RAN may not be able to establish resources for all the flows; the target RAN includes such failed flows information</li> </ul>
2	<p>If the target RAN succeeded in establishing resources for the PDU sessions, the SMF sets the hoState attribute to PREPARED and returns a 200 OK response including the following information:</p> <ul style="list-style-type: none"> <li>• hoState attribute set to PREPARED</li> <li>• the epsBearerSetup IEs containing the list of EPS bearer contexts successfully handed over to the 5GS and the CN tunnel information for data forwarding, generated based on the list of accepted QFIs received from the RAN; This is the final list of flows handed over to the 5GS network.</li> </ul>

## Standards Compliance

The QoS Flow Failure Handling for Access and Mobility Procedures feature complies with the following standards:

- *3GPP TS 23.502 V16.1.1 (2019-06)*







# CHAPTER 23

## Inter gNodeB Handover

This chapter covers the following topics:

- [Feature Summary and Revision History, on page 323](#)
- [Feature Description, on page 324](#)
- [How it Works, on page 324](#)
- [OAM Support, on page 336](#)

## Feature Summary and Revision History

### Summary Data

*Table 114: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

#### Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

The SMF supports the Xn-based and N2-based handover procedures to hand over a UE from a source NG-RAN node to a target NG-RAN node using the Xn or N2 reference points. Initiation of this procedure can be due to new radio conditions, load balancing or due to a specific service.

The SMF releases the QoS flows that failed to set up on the target NG-RAN during Xn and N2 handovers on the respective interfaces N4 (UPF) and N1 (UE). The SMF sends appropriate notification to N7 (PCF) based on the triggers if armed. The SMF also sends the usage report to N40 (CHF) for the released QoS flows.

## How it Works

### Call Flows

The following sections explain the execution of Xn-based and N2-based handover procedures.

#### Xn-based Inter NG-RAN Handover

This section provides details regarding the Xn-based inter NG-RAN handover without UPF reallocation.

The handover preparation and the execution stages are implemented as specified in *3GPP TS 38.300*. When performing the handover in a shared network, the source NG-RAN determines a PLMN to be used in the target network as specified in *3GPP TS 23.501*. If the serving PLMN changes during the Xn handover, the source NG-RAN node indicates the selected PLMN ID to the target NG-RAN node.

If the AMF generates the N2 downlink signalling and receives a rejection to an N2 interface procedure due to the ongoing Xn handover procedure, the AMF reattempts the same N2 interface procedure either when the handover is complete or the handover is deemed to have failed. The failure is known by expiry of the timer guarding the N2 interface procedure.

Upon reception of an SMF-initiated N1 and/or N2 request(s) with an indication that the request has been temporarily rejected due to the ongoing Xn handover procedure, the SMF starts a locally configured guard timer. The SMF holds signalling messages targeted towards the AMF during the handover preparation phase unless it detects that the handover is completed or the handover has failed or cancelled. The SMF reattempts, up to a pre-configured number of times, when either it detects that the handover is completed or has failed using message reception or at expiry of the guard timer.

The Xn-based inter NG-RAN handover is used to hand over a UE from a source NG-RAN to target NG-RAN using Xn when the AMF is unchanged and the SMF decides to keep the existing UPF.

The following figure depicts the call flow of the Xn-based inter NG-RAN handover without the UPF reallocation.

Figure 72: Xn-based Inter NG-RAN Handover without UPF Reallocation

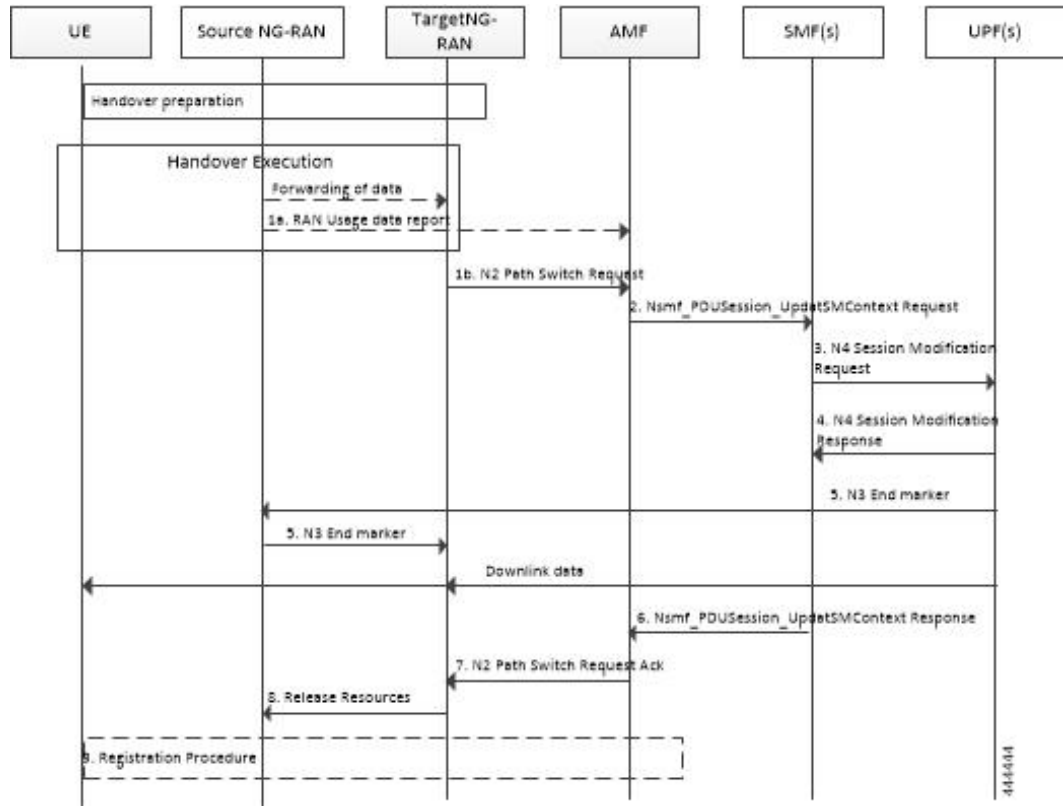


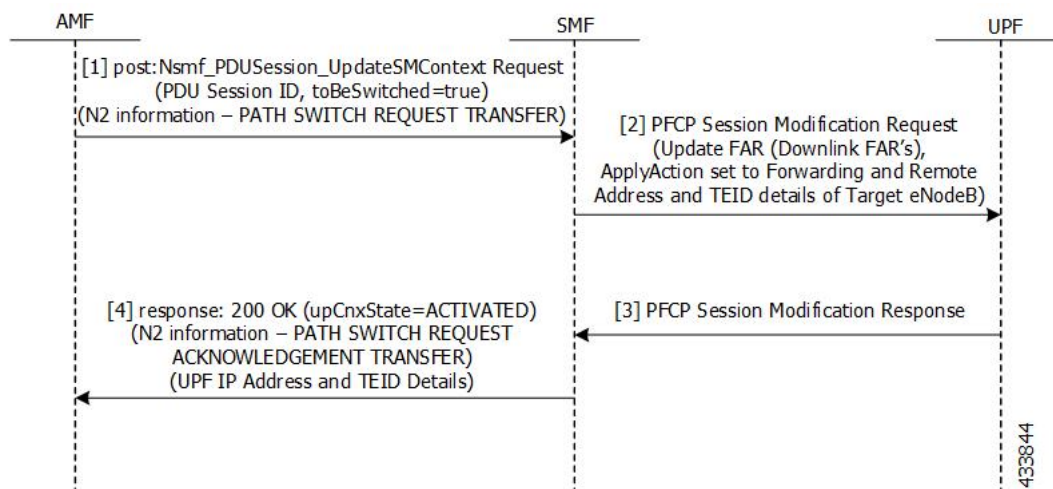
Table 115: Xn-based Inter NG-RAN Handover Call Flow Description (Without UPF Reallocation)

Step	Description
1a	During the handover execution, the source NG-RAN node provides RAN usage data Report to the AMF. The source NG-RAN node provides this report only when the target NG-RAN has confirmed handover over Xn interface.  This report includes N2 SM Information (Secondary RAT usage data), Handover Flag, and Source to Target transparent container. The Handover Flag indicates that the report needs to be buffered by the SMF.
1b	The target NG-RAN sends an N2 Path Switch Request message to the AMF to inform that the UE has moved to a new target cell. The NG-RAN provides a List Of PDU Sessions To Be Switched. The N2 SM Information includes the AN Tunnel Info for each PDU Session to be switched.
2	The AMF sends N2 SM information by invoking the Nsmf_PDUSession_UpdateSMContext request service operation for each PDU session in the lists of PDU Sessions received in the N2 Path Switch Request.
3	The SMF sends an N4 Session Modification Request message to the UPF. The SMF may notify the UPF that originated the Data Notification to discard downlink data for the PDU Sessions and/or to not provide further Data Notification messages.

Step	Description
4	The UPF returns an N4 Session Modification Response message to the SMF after the requested PDU sessions are switched.
5	The UPF sends one or more "end marker" packets for each N3 tunnel on the old path immediately after switching the path. The UPF starts sending downlink packets to the target NG-RAN.
6	The SMF sends an Nsmf_PDUSession_UpdateSMContext response (CN Tunnel Info) to the AMF for PDU sessions which have been switched successfully.  <b>Important</b> Step 6 can occur any time after the receipt of N4 Session Modification Response at the SMF.
7	Once the Nsmf_PDUSession_UpdateSMContext response is received from all the SMFs, the AMF aggregates the received CN Tunnel Info and sends this aggregated information as a part of N2 SM Information along with the Failed PDU Sessions in N2 Path Switch Request Ack to the target NG-RAN. If none of the requested PDU sessions have been switched successfully, the AMF sends an N2 Path Switch Request Failure message to the target NG-RAN.
8	The target NG-RAN confirms success of the handover by sending Release Resources message to the source NG-RAN.
9	The UE initiates Mobility Registration Update procedure if one of the triggers of registration procedure applies.

The following figure shows the detailed call flow of the Xn handover without UPF reallocation.

**Figure 73: Xn Handover Without UPF Relocation Call Flow**



**Table 116: Detailed Call Flow Description for the Xn Handover Without UPF Relocation**

Step	Description
1	The NF Service Consumer (AMF) requests the SMF to switch the user plane connection of the PDU session. The AMF sends a POST request with the following information: <ul style="list-style-type: none"> <li>• The toBeSwitched indication.</li> <li>• N2 SM information received from the 5G-AN (PDU session path switch request transfer IE), including the new transport layer address and tunnel endpoint of the downlink termination point for the user data for this PDU session.</li> <li>• User location and user location timestamp.</li> <li>• Other information, if necessary.</li> </ul>
2	The SMF switches the N3 tunnel of the PDU session after receiving the request. The SMF initiates PFCP session modification procedure toward the UPF with downlink FAR updated with the following option: <ul style="list-style-type: none"> <li>• Forwarding Action is enabled with the remote node “forwarding parameters” details, such as the IP address and GTP-U F-TEID.</li> </ul>
3	The SMF marks the PDU handover as successful after receiving the successful response from the UPF node.
4	The SMF initiates the 200 OK response. This response includes the N2 SM information, which has the transport layer address and tunnel endpoint of the uplink termination point for the user plane data for this PDU session, that is UPF's GTP-U F-TEID for the uplink traffic.

## N2-based Inter NG-RAN Handover

The source NG-RAN decides to initiate an N2-based handover (HO) to the target NG-RAN. Initiation of this procedure could be due to any of the following reasons:

- New radio conditions
- Load balancing
- If there is no Xn connectivity to the target NG-RAN
- An error indication from the target NG-RAN after an unsuccessful Xn-based handover (that is, no IP connectivity between Target RAN (T-RAN) and Source UPF (S-UPF))
- Based on dynamic information learnt by the Source RAN (S-RAN)

The source NG-RAN determines the availability of a direct forwarding path and indicates the same to the SMFs. If the IP connectivity is available between the source and target NG-RAN and security association is in place between them, a direct forwarding path is available. If a direct forwarding path is not available, use the indirect forwarding. The SMFs use the indication from the source NG-RAN to choose the data forwarding path.

When performing the handover in a shared network, the source NG-RAN determines a PLMN for use in the target network as specified by *3GPP TS 23.501*. The source NG-RAN indicates the selected PLMN ID to the AMF as part of the Tracking Area sent in the HO Required message.

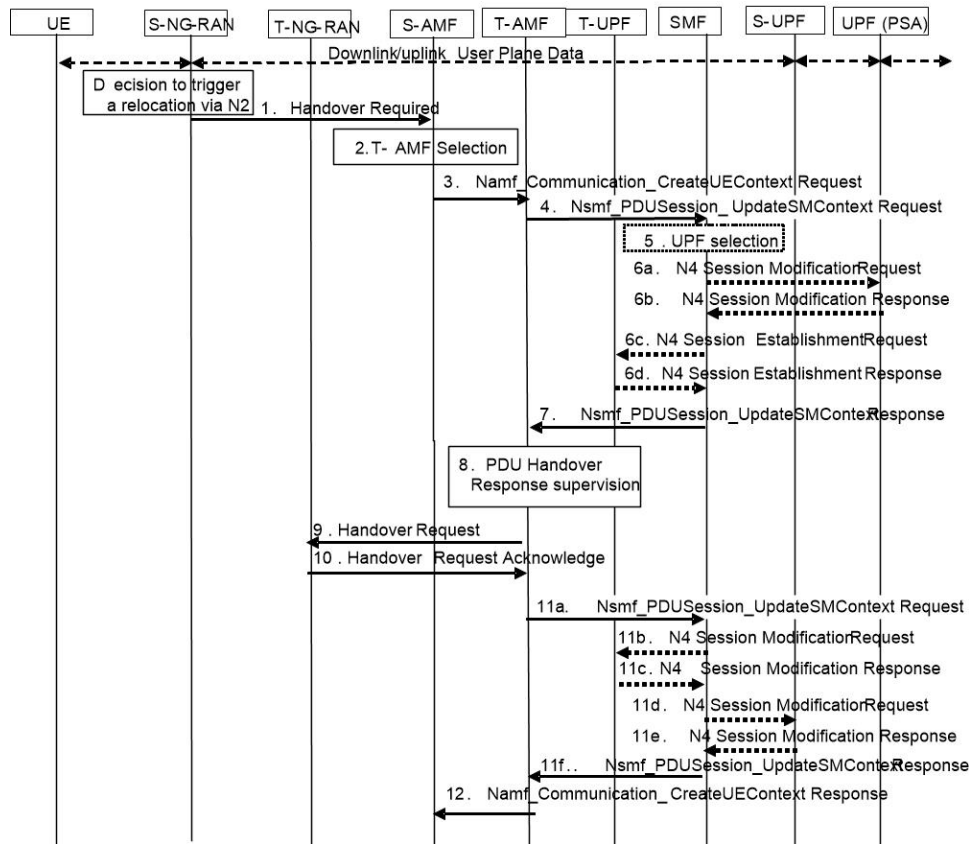
If the AMF generates the N2 downlink signalling and receives a rejection to a N2 interface procedure due to the ongoing N2 handover, the AMF reattempts the same N2 interface procedure either when the handover is complete or the handover is deemed to have failed. If the Inter NG-RAN node handover changes the serving AMF, the source AMF terminates any other ongoing N2 interface procedures except the handover procedure.

If the AMF is still the serving AMF, the AMF pauses non-handover related N2 interface procedures and resumes them after the N2 handover is complete.

If the AMF detects that it needs to be changed, the AMF rejects any SMF-initiated N2 request and includes an indication that the request has been temporarily rejected due to the ongoing N2 handover procedure.

The following figure depicts the call flow for the preparation phase of the N2-based inter NG-RAN handover procedure.

**Figure 74: Inter NG-RAN Node N2-based Handover - Preparation Phase**



444446

Table 117: Inter NG-RAN Node N2-based Handover Call Flow Description - Preparation Phase

Step	Description
1	<p>The Source NG-RAN (S-RAN) sends the Handover Required message to the Source AMF (S-AMF). This message includes the following:</p> <ul style="list-style-type: none"> <li>• Target ID</li> <li>• Source to Target transparent container</li> <li>• SM N2 info list</li> <li>• PDU Session IDs</li> <li>• Intra system handover indication</li> </ul> <p>The Source to Target transparent container includes NG-RAN information for use in Target RAN (T-RAN), and is transparent to 5GC. It also contains the corresponding User Plane Security Enforcement information, QoS flows/DRBs information subject to data forwarding.</p> <p>If direct data forwarding is available, the SM N2 info includes Direct Forwarding Path Availability. Direct Forwarding Path Availability indicates whether direct forwarding is available from the S-RAN to the T-RAN. This indication from S-RAN is based on the presence of IP connectivity and security association between the S-RAN and the T-RAN.</p>
2	<p>When the S-AMF cannot serve the UE anymore, the S-AMF selects the T-AMF as described in clause 6.3.5 on "AMF Selection Function" in <i>TS 23.501</i>.</p>
3	<p>The S-AMF initiates Handover resource allocation procedure by invoking the Namf_Communication_CreateUEContext service operation towards the T-AMF.</p> <p>The Namf_Communication_CreateUEContext Request includes the following:</p> <ul style="list-style-type: none"> <li>• N2 Information <ul style="list-style-type: none"> <li>• Target ID</li> <li>• Source to Target transparent container</li> <li>• SM N2 information list</li> <li>• PDU Session IDs</li> </ul> </li> <li>• UE context information <ul style="list-style-type: none"> <li>• SUPI</li> <li>• Service area restriction</li> <li>• Allowed NSSAI for each Access Type if available</li> <li>• Tracing Requirements</li> <li>• The list of PDU Session IDs along with the corresponding SMF information and the corresponding S-NSSAI(s), PCF ID(s), and DNN</li> </ul> </li> </ul> <p>When the S-AMF can still serve the UE, this step and step 12 are not needed.</p>

Step	Description
4	<p>For each PDU session indicated by S-RAN, the AMF invokes the Nsmf_PDUSession_UpdateSMContext Request to the associated SMF. However, if the S-NSSAI associated with PDU session is not available in the T-AMF, the T-AMF does not invoke Nsmf_PDUSession_UpdateSMContext for this PDU session.</p> <p>If the T-AMF detects that the UE moves into a restricted area based on Service area restrictions, the T-AMF notifies that the UE is only reachable for regulatory prioritized services to each NF consumer which has subscribed for UE reachability event.</p>
5	Based on the Target ID, the SMF checks the acceptance of N2 handover for the indicated PDU session. The SMF also checks the UPF Selection Criteria. If the UE has moved out of the service area of the UPF connecting to NG-RAN, the SMF selects a new intermediate UPF.
6a	If the SMF selects a new UPF to act as intermediate UPF for the PDU session, and the different CN Tunnel Info need to be used, the SMF sends N4 Session Modification Request message to UPF (PDU Session Anchor (PSA)). If the SMF allocates the CN Tunnel Info, it provides the CN Tunnel Info on N9, and the UPF (PSA) associates CN Tunnel Info with UL Packet detection rules.
6b	The UPF (PSA) sends an N4 Session Establishment Response message to the SMF. If the UPF (PSA) allocates CN Tunnel Info (on N9) of UPF (PSA), it provides CN Tunnel Info (on N9) to the SMF. The UPF (PSA) associates the CN Tunnel Info (on N9) with UL Packet detection rules provided by the SMF.
6c	If the SMF selects a new intermediate UPF (T-UPF) and if the T-UPF allocates the CN Tunnel Info, the SMF sends an N4 Session Establishment Request message to the T-UPF. This request enables the Packet detection, enforcement, and reporting rules to be installed on the T-UPF. The T-UPF receives the CN Tunnel Info (on N9) of UPF (PSA) for this PDU session, which is used to set up N9 tunnel.
6d	The T-UPF sends an N4 Session Establishment Response message to the SMF with DL CN Tunnel Info and UL CN Tunnel Info (that is, N3 tunnel info). The SMF starts a timer to release the resource of S-UPF, which is to be used in step 13a of the Execution Phase.
7	<p>If N2 handover for the PDU session is accepted, the SMF includes the N2 SM Information in the Nsmf_PDUSession_UpdateSMContext response. The N2 SM Information contains the N3 UP address and the UL CN Tunnel ID of the UPF and the QoS parameters indicating that the N2 SM Information is for the Target NG-RAN.</p> <p>If the N2 SM information received at step 4 does not include the Direct Forwarding Path Availability and the SMF knows that there is no indirect data forwarding connectivity between source and target, the N2 SM Information includes a Data forwarding not possible indication.</p> <p>If the N2 handover for the PDU session is not accepted as described in step 5, the SMF does not include the N2 SM Information to avoid establishment of radio resources at the target NG-RAN. The SMF provides a reason for non-acceptance. If the SMF receives notification from T-AMF that UE is only reachable for regulatory prioritized service, the SMF deactivates the PDU session.</p>
8	The AMF supervises the Nsmf_PDUSession_UpdateSMContext Response messages from the involved SMFs. At the expiry of maximum wait time or when all Nsmf_PDUSession_UpdateSMContext Response messages are received, the AMF continues with the N2 Handover procedure (Handover Request message in step 9).

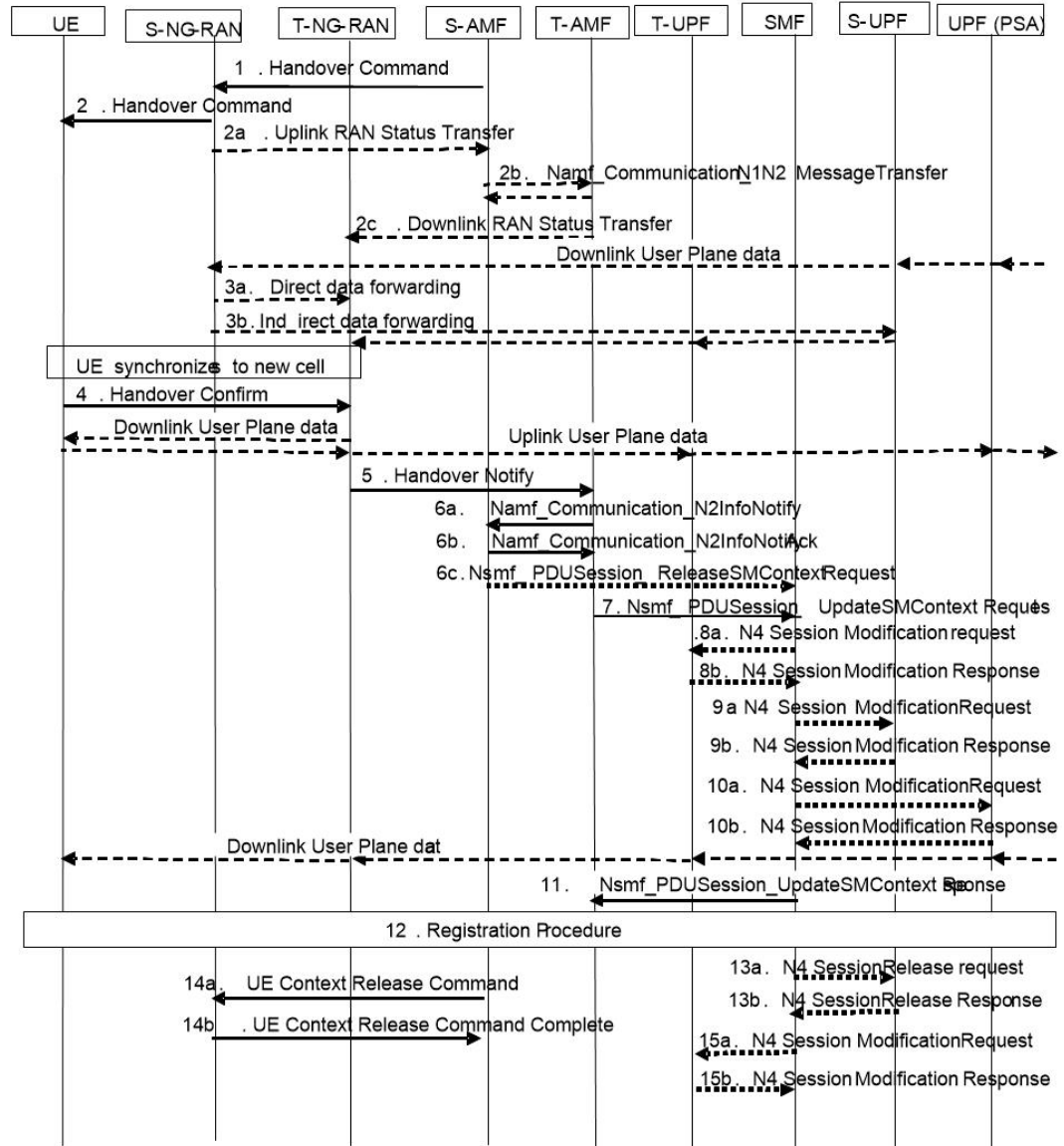


Step	Description
9	<p>If the subscription information includes Tracing Requirements, the target AMF provides the target RAN with Tracing Requirements in the Handover Request.</p> <p>The Handover request includes Source to Target transparent container, N2 MM Information, N2 SM Information list, and Tracing Requirements.</p> <p>The T-AMF determines T-RAN based on Target ID. T-AMF allocates a 5G-GUTI valid for the UE in the AMF and target TAI.</p> <p>N2 MM Information includes, for example, security information and Mobility Restriction List if available in the T-AMF. N2 SM Information list includes N2 SM Information for the T-RAN in the Nsmf_PDUSession_UpdateSMContext Response messages received within allowed max delay supervised by the T-AMF in step 8.</p>
10	<p>The T-RAN sends Handover Request Acknowledge to the T-AMF. The Acknowledge message includes Target to Source transparent container, List of PDU Sessions to Hand-over with N2 SM information, List of PDU Sessions that failed to be established with the failure cause given in the N2 SM information element.</p>
11a	<p>The AMF sends Nsmf_PDUSession_UpdateSMContext Request (PDU Session ID, N2 SM response) to the SMF.</p> <p>For each N2 SM response received from the T-RAN, the AMF sends the N2 SM response to the SMF indicated by the respective PDU Session ID.</p> <p>If no new T-UPF is selected, the SMF stores the N3 tunnel info of T-RAN from the N2 SM response if N2 handover is accepted by T-RAN.</p> <p>The SMF/UPF allocates the N3 UP address and Tunnel IDs for indirect data forwarding corresponding to the data forwarding tunnel endpoints established by T-RAN.</p> <p>If a PDU session is indicated as a rejected PDU session by the Target NG-RAN, the SMF triggers the release of this PDU session. In all other cases of PDU Session rejection, the SMF decides whether to release the PDU session or to deactivate the UP connection of this PDU session.</p> <p>If some of the QoS Flows of a PDU Session are not accepted by the Target NG-RAN, the SMF initiates the PDU Session Modification procedure to remove the non-accepted QoS Flows from the PDU Session(s) after the handover is completed.</p>
11b	<p>The SMF sends N4 Session Modification Request to the T-UPF. This request includes T-RAN SM N3 forwarding Information list, and indication to allocate DL forwarding tunnel(s) for indirect forwarding.</p>
11c	<p>The T-UPF allocates Tunnel Info and returns an N4 Session Modification Response message to the SMF. The T-UPF SM N3 forwarding info list includes T-UPF N3 address, T-UPF N3 Tunnel identifiers for forwarding data.</p>
11d	<p>The SMF sends N4 Session Modification Request to the S-UPF. This request includes T-RAN SM N3 forwarding Information list or T-UPF SM N3 forwarding Information list, and an indication to allocate DL forwarding tunnel(s) for indirect forwarding.</p>

Step	Description
11e	The S-UPF allocates Tunnel Info and returns an N4 Session establishment Response message to the SMF.  The S-UPF SM N3 forwarding Information list includes S-UPF N3 address and S-UPF N3 Tunnel identifiers for DL data forwarding.
11f	The SMF sends an Nsmf_PDUSession_UpdateSMContext Response message per PDU session to the T-AMF.
12	The AMF supervises the Nsmf_PDUSession_UpdateSMContext Response message from the involved SMFs. At the expiry of maximum wait time or when all Nsmf_PDUSession_UpdateSMContext Response messages are received, the T-AMF sends the Namf_Communication_CreateUEContext Response to the S-AMF.

The following figure depicts the call flow for the execution phase of the N2-based inter NG-RAN handover procedure.

Figure 75: Inter NG-RAN Node N2-based Handover - Execution Phase



445019

Table 118: Inter NG-RAN Node N2-based Handover Call Flow Description - Execution Phase

Step	Description
1	<p>The Source AMF (S-AMF) sends the Handover Command to the Source NG-RAN (S-RAN).</p> <p>The Handover Command includes Target to Source transparent container, List Of PDU Sessions to be handed-over with N2 SM information containing information received from T-RAN during the handover preparation phase, and List Of PDU Sessions failed to be set up.</p> <p>The SM forwarding info list includes T-RAN SM N3 forwarding info list for direct forwarding or S-UPF SM N3 forwarding info list for indirect data forwarding.</p> <p>The S-RAN uses the PDU Sessions failed to be setup list and the indicated reason for failure to decide whether to proceed with the N2 handover procedure.</p>
2	<p>The S-RAN sends Handover Command (UE container) to the UE.</p> <p>The UE container is a UE part of the Target to Source transparent container which is sent transparently from T-RAN via AMF to S-RAN and is provided to the UE by the S-RAN.</p>
2a - 2c	<p>The S-RAN sends the Uplink RAN Status Transfer message to the S-AMF. The S-RAN refrains from sending this message if none of the radio bearers of the UE are treated with Packet Data Convergence Protocol (PDCP) status preservation.</p>
3	<p>The T-RAN sends the uplink packets to the T-UPF and UPF (PSA). The UPF (PSA) sends the downlink packets to the S-RAN via S-UPF.</p> <p>The S-RAN forwards the downlink data towards the T-RAN for QoS flows or Data Radio Bearers (DRBs) subject to data forwarding. The data forwarding path is either direct (step 3a) or indirect forwarding (step 3b).</p>
4	<p>After the UE has successfully synchronized to the target cell, it sends a Handover Confirm message to the T-RAN.</p>
5	<p>The T-RAN sends Handover Notify message to the T-AMF. This message is sent to indicate that the handover is successful.</p>
6a.	<p>The T-AMF notifies to the S-AMF about the N2 handover notify received from the T-RAN by invoking the Namf_Communication_N2InfoNotify.</p> <p>The S-AMF uses a timer to supervise the release of resources in S-RAN.</p>
6b	<p>The S-AMF acknowledges by sending the Namf_Communication_N2InfoNotify ACK to the T-AMF.</p>
6c	<p>The S-AMF sends Nsmf_PDUSession_ReleaseSMContext Request to the SMF. This request includes SUPI, PDU Session ID, and N2 SM Information (Secondary RAT Usage Data).</p> <p>If the PDU Session(s) is not accepted by the T-AMF, the S-AMF triggers PDU Session Release procedure after the reception of N2 Handover Notify.</p>
7	<p>The T-AMF sends Nsmf_PDUSession_UpdateSMContext Request to the SMF. This request includes Handover Complete indication for PDU Session ID, UE presence in LADN service area, and N2 SM Information (Secondary RAT usage data).</p> <p>The T-AMF sends Handover Complete indication per each PDU Session to the corresponding SMF to indicate the success of the N2 handover.</p>

Step	Description
8a	If a new T-UPF is inserted or an existing intermediate S-UPF is reallocated, the SMF sends N4 Session Modification Request indicating DL AN Tunnel Info of T-RAN to the T-UPF.
8b	The T-UPF acknowledges by sending N4 Session Modification Response message to the SMF.
9a	If the UPF is not reallocated, the SMF sends N4 Session Modification Request indicating DL AN Tunnel Info of T-RAN to the S-UPF.
9b	The S-UPF acknowledges by sending N4 Session Modification Response message to SMF.
10a	For non-roaming or local breakout roaming scenario, the SMF sends N4 Session Modification Request message to PDU Session Anchor UPF, UPF (PSA). If a new T-UPF is inserted or an existing intermediate S-UPF is reallocated, the SMF provides N3 AN Tunnel Info of T-RAN or the DL CN Tunnel Info of T-UPF.  If the T-UPF is not inserted or an existing intermediate S-UPF is not reallocated, skip the step 10a and step 10b.
10b	The UPF (PSA) sends N4 Session Modification Response message to the SMF.  When there are multiple UPFs (PSA), perform step 10a and step 10b for each UPF (PSA).
11	The SMF sends Nsmf_PDUSession_UpdateSMContext Response (PDU Session ID) to the T-AMF. The SMF confirms reception of Handover Complete.
12	The UE initiates Mobility Registration Update procedure as defined in <i>3GPP TS 23.502</i> .
13a	If there is a source intermediate UPF, the SMF initiates resource release by sending an N4 Session Release Request (Release Cause) to the source UPF. This message is also used to release the indirect data forwarding resource in the S-UPF.
13b	The S-UPF acknowledges with an N4 Session Release Response message to confirm the release of resources.  In case of indirect data forwarding, the resource of indirect data forwarding is also released.
14a	After the expiry of timer (defined in step 6a), the AMF sends UE Context Release Command.
14b	The source NG-RAN releases its resources related to the UE and responds with a UE Context Release Complete () message.
15a	If indirect forwarding applies and the UPF is reallocated, after the timer of indirect data forwarding expires, the SMF sends N4 Session Modification Request to the T-UPF. Then, the T-UPF releases the indirect data forwarding resources.
15b	The T-UPF acknowledges with an N4 Session Modification Response message to confirm the release of indirect data forwarding resources.

## Limitations

The Xn-based handover with UPF reallocation is currently not supported.

# OAM Support

This section describes the operations, administration, and maintenance information for this feature.

## Statistics Support

The "smf\_ran\_failed\_flows" metric is added to identify the number of QoS flows released by RAN as part of various call flow procedures including the Xn and N2 handover procedures.

The SMF uses the "xn\_handover" label to account for Xn handovers. Similarly for the N2 handovers, the SMF uses the "n2\_handover" label.



# CHAPTER 24

## IP Address Management

- [Feature Summary and Revision History, on page 337](#)
- [Feature Description, on page 338](#)
- [How it Works, on page 338](#)
- [IPAM Integration in SMF, on page 339](#)
- [Static IP Support, on page 352](#)
- [Dual-Stack Static IP Support Through IPAM, on page 357](#)
- [IPAM Offline Mode Support, on page 358](#)
- [IPAM Redundancy Support Per UPF, on page 360](#)
- [IPAM Static IP Pool Enhancements, on page 361](#)
- [IPAM Quarantine Timer Support, on page 365](#)
- [Configuring IPAM Quarantine Qsize Support Feature, on page 369](#)
- [Overlapping IP Address Pools Support, on page 370](#)
- [Virtual Routing and Forwarding Function, on page 371](#)

## Feature Summary and Revision History

### Summary Data

*Table 119: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

## Revision History

*Table 120: Revision History*

Revision Details	Release
VRF Support introduced.	2020.02.5
First introduced.	Pre-2020.02.0

## Feature Description

IP Address Management (IPAM) is a method of tracking and managing IP addresses of a network. IPAM is one of the core components of the subscriber management system. Traditional IPAM functionalities are insufficient in Cloud-Native network deployments. Hence, IPAM requires additional functionalities to work with the Cloud-Native subscriber management system. The Cloud-Native IPAM system is used in various network functions, such as SMF and PCF.

The IPAM system includes the following functionalities to serve the Cloud Native and Control and User Plane Separation (CUPS) architecture:

- **Centralized IP Resource Management**—Based on the needs of the Internet Service Provider (ISP), the Control Plane (CP) is deployed either on a single (centralized) cluster or multiple (distributed) clusters. For multiple cluster deployments, the IPAM automatically manages the single IP address space across the multiple CPs that are deployed in the distributed environment.
- **IP Address-Range Reservation per User Plane**—For subscribers connecting to the Internet core, the User Plane (UP) provides the physical connectivity. The UP uses the summary-routes to advertise subscriber routes to the Internet core. For CPs that are managing multiple UPs, the CP reserves a converged IP subnet to the UPs. In such a scenario, the IPAM splits the available address space into smaller address-ranges and assigns it to different UPs.
- **IP Address Assignment from Pre-Reserved Address-Ranges**—When subscribers request for an IP address, the IPAM assigns addresses from the pre-reserved address range of their respective UP.

## How it Works

IPAM uses the following sub-modules for the Cloud-Native subscriber management system:

- **IPAM Server**—This module manages the complete list of pools and address-space configurations. The IPAM server splits the configured address ranges into smaller address-ranges statically or dynamically to distribute them to IPAM cache modules. The IPAM server is deployed as a centralized entity to serve group of Cloud-Native clusters or can be an integrated entity within a single cluster.
- **IPAM Cache**—This module receives the free address-ranges from the IPAM server and allocates the individual IP addresses to the IPAM clients. Usually, the IPAM cache is deployed in a distributed mode running within each cluster to communicate with the co-located or remotely-located IPAM server. The IPAM cache also handles address-range reservation per UP and pool threshold monitoring. The IPAM server and cache modules can run as an integrated mode.



- **IPAM Client**—This module handles the request and release of an individual IP address from the IPAM cache for each IP managed end-device. The IPAM client is tightly coupled with a respective network-function.

# IPAM Integration in SMF

## Feature Description

The IP Address Management (IPAM) is a technique for tracking and managing the IP address space of a network. A core component of the subscriber management system, the IPAM provides all the functionalities necessary for working with the Cloud-Native subscriber management system. Also, the IPAM acts as a generic IP address management system for the different network functions such as the SMF, Policy Control Function (PCF), and so on.

The IPAM is integrated with the SMF in the Application Services layer.

## Architecture

This section describes the IPAM integration in the SMF architecture.

## IPAM Integration in SMF

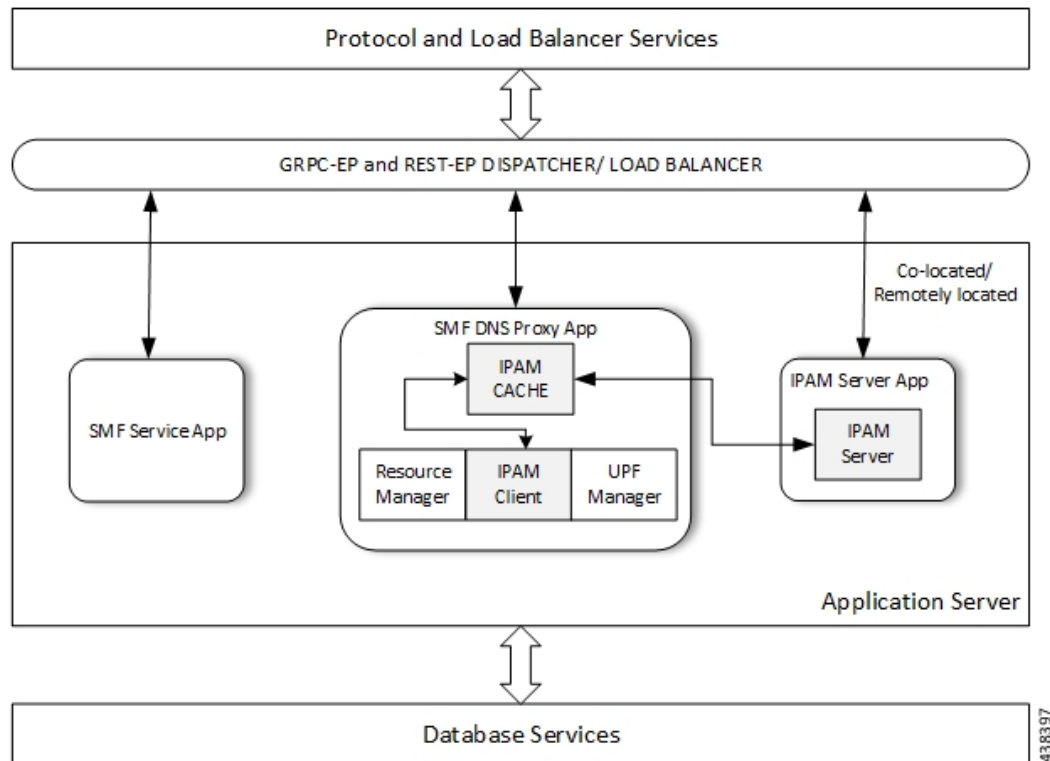
The SMF comprises of loosely coupled microservices that enables the SMF to perform session management (session establishment, modification, and release) and other associated functions. The decomposition of these microservices is based on the following three-layered architecture:

1. Layer 1: Protocol and Load Balancer Services (Stateless)
2. Layer 2: Application services (Stateless)
3. Layer 3: Database Services (Stateful)

The IPAM and SMF integration happens in the Application Services layer.

The following describes the SMF and IPAM integration architecture in the Application Services layer.

Figure 76: IPAM Integration in SMF



- **SMF Node-Manager Application** – The SMF Node-Manager application takes care of the UPF, ID resource, and IP address management. Therefore, the SMF Node-Manager application integrates IPAM Cache and IPAM client modules. The UPF Manager uses the IPAM Client module for address-range-reservation per UPF.
- **SMF Service Application** – The SMF Service application provides PDU session services. During session establishment and termination, the IP addresses are requested and released back. The SMF Service application invokes the IPC to RMGR in Node Manager, which receives (free) the IP from the IPAM module.
- **IPAM Server Application** – Based on the deployment model, the IPAM Server application can run as an independent microservice, as a part of the same cluster, or in a remote-cluster. For standalone deployments, the IPAM Servers are an integral part of the IPAM cache.

## Components

This section describes the different components of the IPAM system.

### IPAM Sub-Modules

The IPAM system includes the following sub-modules:

- **IPAM Server** – The IPAM Server module manages the complete list of pools and address-space configuration. It splits the configured address-ranges into smaller address-ranges (statically and dynamically) and distributes it to the IPAM Cache modules. You can deploy the IPAM Server either as

a centralized entity to serve a group of cloud native clusters or as an integrated entity within a single cluster.

- **IPAM Cache** – The IPAM Cache acquires free address-ranges from the IPAM Server and allocates individual IP addresses to the IPAM clients. Deployed in a distributed mode running within each cluster, the IPAM Cache communicates with co-located and remotely located IPAM Servers. Additionally, the IPAM Cache takes care of the address-range reservation per Data-Plane and pool threshold monitoring.
- **IPAM Client** – The IPAM Client module handles the request and release of the individual IP addresses from the IPAM Cache for each IP managed end-device. Based on the use cases, the IPAM Client module caters the needs of specific network functions (such as SMF, PCF, and so on).

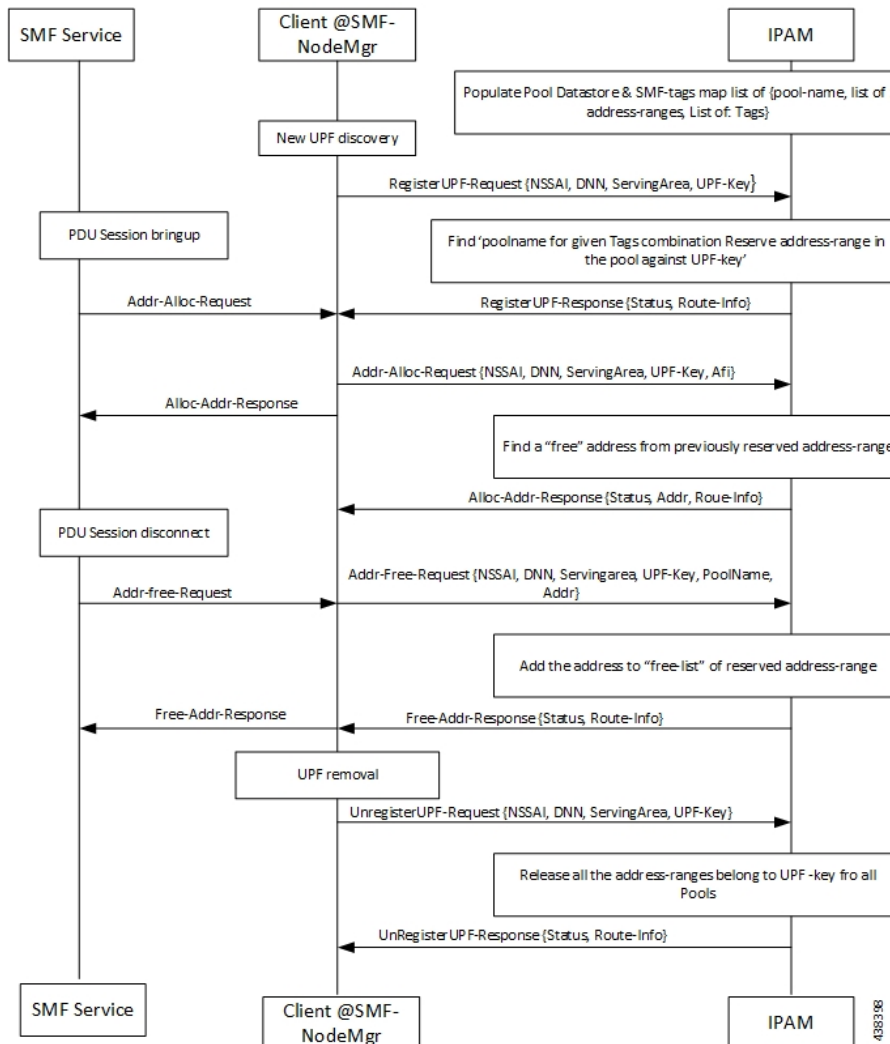
## How it Works

This section describes the call flows pertaining to the integration of the IPAM in the SMF.

### Call Flows

The following call flow depicts the integration of the IPAM in the SMF.

Figure 77: Integration of IPAM in SMF Call Flow



## Configuring the IPAM Feature

This section describes how to configure the IPAM in the SMF.

Configuring the IPAM in the SMF involves the following steps:

1. Configuring IPv4 address ranges.
2. Configuring IPv6 address ranges.
3. Configuring IPv6 prefix ranges.
4. Configuring SMF tags.
5. Configuring IPv4 threshold.
6. Configuring IPv6 address range threshold.

7. Configuring IPv6 prefix range threshold.
8. Configuring IPv4 address range split.
9. Configuring IPv6 address and prefix address range split.
10. Configuring global threshold.
11. Configuring IPAM source.

## Configuring IPv4 Address Ranges

Use the following configuration to configure the IPv4 address ranges.

```
configure
ipam
  address-pool pool_name
    vrf-name string
  ipv4
    address-range start_ipv4_address end_ipv4_address
  commit
```

### NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool\_name*: Configures the address pool configuration. *pool\_name* must be the name of the address pool.
- **vrf-name** *string*: Configures the Virtual routing and forwarding (VRF) name of the pool.
- **ipv4**: Enters the IPv4 mode of the pool.
- **address-range** *start\_ipv4\_address end\_ipv4\_address*: Configures the IPv4 range. *start\_ipv4\_address* specifies the starting IPv4 address. *end\_ipv4\_address* specifies the ending IPv4 address.

The following is a sample configuration:

```
configure
ipam
  address-pool p1
    vrf-name one
  ipv4
    address-range 1.1.1.10 1.1.1.255
    address-range 2.2.2.1 2.2.2.255
```

## Configuring IPv6 Address Ranges

Use the following configuration to configure the IPv6 address ranges:

```
configure
ipam
  address-pool pool_name
    vrf-name string
  ipv6
    address-range start_ipv6_address end_ipv6_address
  commit
```

**NOTES:**

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool\_name*: Configures the address pool configuration. *pool\_name* must be the name of the address pool.
- **vrf-name** *string*: Configures the VRF name of the pool.
- **ipv6**: Enters the IPv6 mode of the pool.
- **address-range** *start\_ipv6\_address end\_ipv6\_address*: Configures the IPv6 range. *start\_ipv6\_address* specifies the starting IPv6 address. *end\_ipv6\_address* specifies the ending IPv6 address.

The following is a sample configuration:

```
configure
 ipam
   address-pool pl
     vrf-name one
     ipv6
       address-range 1::1 1::1000
       address-range 2::1 2::1000
```

## Configuring IPv6 Prefix Ranges

Use the following configuration to configure the IPv6 prefix ranges:

```
configure
 ipam
   address-pool pool_name
     vrf-name string
     ipv6
       prefix-ranges
         prefix-range prefix_value prefix-length length
         commit
```

**NOTES:**

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool\_name*: Configures the address pool configuration. *pool\_name* must be the name of the address pool.
- **vrf-name** *string*: Configures the VRF name of the pool.
- **ipv6**: Enters the IPv6 mode of the pool.
- **prefix-ranges**: Enters the prefix ranges mode.
- **prefix-range** *prefix\_value* **prefix-length** *length* : Configures the IPv6 prefix range. **prefix-range** *prefix\_value* specifies the IPv6 prefix range. **prefix-length** *length* specifies the IPv6 prefix length.

The following is a sample configuration:

```
configure
 ipam
   address-pool p3
     vrf-name three
     ipv6
```

```

prefix-ranges
  prefix-range 1:1:: prefix-length 48
  prefix-range 2:1:: prefix-length 48

```

## Configuring SMF Tags

Use the following configuration to configure the SMF tags.

```

configure
  ipam
    address-pool pool_name
      tags
        nssai string
        dnn string
        -serving-area string
      commit

```

### NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool\_name*: Configures the address pool configuration. *pool\_name* must be the name of the address pool.
- **tag** : Enters the tag section of the pool.
- **nssai** *string*: Specifies the NSSAI value.
- **dnn** *string* : Specifies the DNN value.
- **-serving-area** *string*: Specifies the serving-area value.

The following is a sample configuration:

```

configure
  ipam
    address-pool p1
      tags
        nssai one
        dnn two
        serving-area three

```

## Configuring IPv4 Threshold

Use the following configuration to configure the IPv4 threshold:

```

configure
  ipam
    address-pool pool_name
      ipv4
        threshold
          upper-threshold percentage
        commit

```

### NOTES:

- **ipam**: Enters the IPAM Configuration mode.

- **address-pool** *pool\_name*: Configures the address pool configuration. *pool\_name* must be the name of the address pool.
- **ipv4** : Enters the IPv4 mode of the pool.
- **threshold** : Enters the threshold sub-mode.
- **upper-threshold** *percentage*: Specifies the IPv4 upper threshold value in percentage.

The following is a sample configuration:

```
configure
 ipam
   address-pool p1
     ipv4
       threshold
         upper-threshold 80
```

## Configuring IPv6 Address Range Threshold

Use the following configuration to configure the IPv6 address range threshold.

```
configure
 ipam
   address-pool pool_name
     ipv6
       address-ranges
         threshold
           upper-threshold percentage
         commit
```

### NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool\_name*: Configures the address pool configuration. *pool\_name* must be the name of the address pool.
- **ipv6** : Enters the IPv6 mode of the pool.
- **address-ranges**: Enters the IPv6 address ranges sub-mode.
- **threshold** : Enters the threshold sub-mode.
- **upper-threshold** *percentage*: Specifies the IPv6 upper-threshold value in percentage.

The following is an example configuration:

```
configure
 ipam
   address-pool p2
     ipv6
       address-ranges
         threshold
           upper-threshold 75
```

## Configuring IPv6 Prefix-Range Threshold

Use the following configuration to configure the IPv6 prefix-range threshold.



```

configure
  ipam
    address-pool pool_name
      ipv6
        prefix-ranges
          threshold
            upper-threshold percentage
          commit

```

**NOTES:**

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool\_name*: Configures the address pool configuration. *pool\_name* must be the name of the address pool.
- **ipv6** : Enters the IPv6 mode of the pool.
- **prefix-ranges**: Enters the IPv6 prefix ranges sub-mode.
- **threshold** : Enters the threshold sub-mode.
- **upper-threshold** *percentage*: Specifies the IPv6 upper-threshold value in percentage.

The following is an example configuration:

```

configure
  ipam
    address-pool p3
      ipv6
        prefix-ranges
          threshold
            upper-threshold 78

```

## Configuring IPv4 Address Range Spilt

Use the following configuration to configure the IPv4 address range spilt.

```

configure
  ipam
    address-pool pool_name
      ipv4
        spilt-size per-cache integer
        spilt-size per-dp integer
      commit

```

**NOTES:**

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool\_name*: Configures the address pool configuration. *pool\_name* must be the name of the address pool.
- **ipv4** : Enters the IPv4 mode of the pool.
- **spilt-size per-cache** *integer*: Specifies the size of the IPv4 range to be split for each IPAM cache allocation. The IPAM server consumes this configuration.

- **spilt-size-per-dp** *integer*: Specifies the size of the IPv4 range to be spilt for each Data-Plane (User-Plane) allocation. The IPAM cache consumes this configuration.

The following is a sample configuration:

```
configure
  ipam
    address-pool pl
      ipv4
        split-size per-cache 1024
        split-size per-dp 256
```

## Configuring IPv6 Address and Prefix Address-Range-Split

Use the following configuration to configure the IPv6 address and prefix address range split.

```
configure
  ipam
    address-pool pool_name
      ipv6
        address-ranges
          spilt-size per-cache integer
          spilt-size per-dp integer
        commit
      prefix-ranges
        spilt-size per-cache integer
        spilt-size per-dp integer
      commit
```

### NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool\_name*: Configures the address pool configuration. *pool\_name* must be the name of the address pool.
- **ipv6** : Enters the IPv6 mode of the pool.
- **address-ranges**: Enters the IPv6 address-ranges sub-mode.
- **spilt-size per-cache** *integer*: Specifies the size of the IPv6 address-ranges or prefix-ranges to be split for each IPAM cache allocation. The IPAM server consumes this configuration.
- **spilt-size-per-dp** *integer*: Specifies the size of the IPv6 address-ranges or prefix-ranges to be split for each Data-Plane (User-Plane) allocation. The IPAM cache consumes this configuration.
- **prefix-ranges**: Enters the IPv6 prefix ranges sub-mode.

The following is a sample configuration:

```
configure
  ipam
    address-pool pl
      ipv6
        address-ranges
          split-size per-cache 4096
          split-size per-dp 1024
        !
      prefix-ranges
```

```
split-size per-cache 8192
split-size per-dp 2048
```

## Configuring Global Threshold

Use the following configuration to configure the global threshold.

```
configure
 ipam
  threshold
    ipv4-addr percentage
    ipv6-addr percentage
    ipv6-prefix percentage
  commit
```

### NOTES:

- **ipam**: Enters the IPAM Configuration mode.
- **threshold**: Enters the threshold sub-mode.
- **ipv4-addr *percentage*** : Specifies the IPv4 threshold value in percentage.
- **ipv6-addr *percentage*** : Specifies the IPv6 threshold value in percentage.
- **ipv6-prefix *percentage*** : Specifies the IPv6 prefix threshold value in percentage.

The following is a sample configuration:

```
configure
 ipam
  threshold
    ipv4-addr 80
    ipv6-addr 75
    ipv6-prefix 70
```

## Configuring IPAM Source

Use the following configuration to configure the IPAM source.

```
configure
 ipam
  source local
  source external ipam
    host ip_address
    port integer
    vendor type
  commit
```

### NOTES:

- **ipam**: Enters the IPAM Configuration mode.
- **source local**: Enters the local datastore as the pool source.
- **source external ipam** : Enters the external IPAM server as the pool source.
- **host *ip\_address*** : Specifies the host name of the external IPAM server.
- **port *integer*** : Specifies the port of the external IPAM server.

- **vendor type**: Specifies the vendor type of the external IPAM server.

The following is a sample configuration:

```
configure
ipam
  source external ipam
  host 1.1.1.1
  port 10000
  vendor cisco
```

## Verifying the IPAM Integration Configuration

This section describes how to verify the IPAM integration in the SMF feature configuration.

Use the **show ipam pool** command to view the summary of current threshold of each pool.

The following is a sample output of the **show ipam pool** command.

```
show ipam pool
=====
PoolName      Ipv4Threshold  Ipv6AddrThreshold  Ipv6PrefixThreshold
=====
p1             80%             80%                 0%
p2             75%             0%                  70%
=====
```

Use the **show ipam pool pool\_name** command to view more details of a specific pool name.

The following is a sample output of the **show ipam pool pool\_name** command.

```
show ipam pool p1
-----
Ipv4Addr      [Total/Used/Threshold] = 7680 / 7680 / 80%
Ipv6Addr      [Total/Used/Threshold] = 512 / 512 / 80%
Ipv6Prefix    [Total/Used/Threshold] = 0 / 0 / 0%
-----
```

Use the **show ipam pool\_name ipv4-addr** command to view the IPv4-address ranges for the given pool-name. Based on the configuration, the address ranges are dynamically split. You can also view whether the address range is free or allocated to a Data Plane (User Plane) using this command.

The following is a sample output of the **show ipam pool\_name ipv4-addr** command.

```
show ipam pool p1 ipv4-addr
=====
StartAddress   EndAddress      AllocContext
=====
1.1.1.0        1.1.3.255      Upf-100
1.1.4.0        1.1.7.255      Upf-200
1.1.8.0        1.1.10.255     Free
2.2.1.0        2.2.3.255      Upf-100
2.2.4.0        2.2.7.255      Upf-300
2.2.8.0        2.2.10.255     Free
3.3.1.0        3.3.3.255      Free
3.3.4.0        3.3.7.255      Free
3.3.8.0        3.3.10.255     Free
=====
```

Use the **show ipam pool *pool\_name* ipv6-prefix** command to view the prefix-ranges for the given pool-name. Based on the configuration, the address ranges are dynamically split. You can also view whether the address range is free or allocated to a Data Plane (User Plane) using this command.

The following is a sample output of the **show ipam pool *pool\_name* ipv6-prefix** command.

```
show ipam pool p2 ipv6-prefix
=====
Prefix                               AllocContext
=====
aaaa:bbbb:ccc0::/64                 Upf-100
aaaa:bbbb:ccc1::/64                 Free
aaaa:bbbb:dd00::/64                 Upf-200
=====
```

Use the **show ipam dp** command to view the summary of the current threshold for each Data Plane (User Plane).

The following is a sample output of the **show ipam dp** command.

```
show ipam dp
=====
DpName      Ipv4Threshold  Ipv6AddrThreshold  Ipv6PrefixThreshold
=====
UPF-100     20%            40%                70%
UPF-200     40%            20%                20%
=====
```

Use the **show ipam dp *dataplane\_name*** command to view more details of a specific Data Plane (User Plane).

The following is a sample output of the **show ipam dp *dataplane\_name*** command.

```
show ipam dp UPF-100
-----
Ipv4Addr   [Total/Used/Threshold] = 512 / 100 / 20%
Ipv6Addr   [Total/Used/Threshold] = 512 / 200 / 40%
Ipv6Prefix [Total/Used/Threshold] = 512 / 300 / 70%
-----
```

Use the **show ipam dp *dataplane\_name* ipv4-addr** command to view the IPv4-address ranges assigned to a data plane.

The following is a sample output of the **show ipam dp *dataplane\_name* ipv4-addr** command.

```
show ipam dp UPF-100 ipv4-addr
=====
StartAddress  EndAddress  AllocContext  Route
=====
1.1.1.1      1.1.1.255  Pool-1        1.1.1.0/24
2.2.1.1      2.2.1.255  Pool-2        2.2.1.0/24
=====
```

Use the **show ipam dp *dataplane\_name* ipv6-addr** command to view the IPv6-address ranges assigned to a data plane.

The following is a sample output of the **show ipam dp *dataplane\_name* ipv6-addr** command.

```
show ipam dp UPF-100 ipv6-addr
=====
```

```

StartAddress      EndAddress      AllocContext    Route
=====
100::1           100::100       Pool-1          100::/120
00::1           200::100       Pool-2          200::/120
=====

```

Use the **show ipam dp *dataplane\_name* ipv6-prefix** command to view the IPv6-address ranges assigned to a data plane.

The following is a sample output of the **show ipam dp *dataplane\_name* ipv6-prefix** command.

```

show ipam dp UPF-100 ipv6-prefix
=====
Prefix            AllocContext      Route
=====
aaaa:bbbb:cccc::/64  Pool-1           aaaa:bbbb:cccc::/48
aaaa:bbbb:dd00::/64  Pool-1           aaaa:bbbb:dd00::/40
=====

```

# Static IP Support

## Feature Description

IPAM is the core component of the subscriber management system. Traditional IPAM functionalities prove insufficient in the Cloud Native network deployments. Hence, IPAM requires more functionalities to work with the Cloud Native subscriber management system.

The Static IP Support feature enables the support of static IP on the SMF using IPAM. This feature supports the following functionalities:

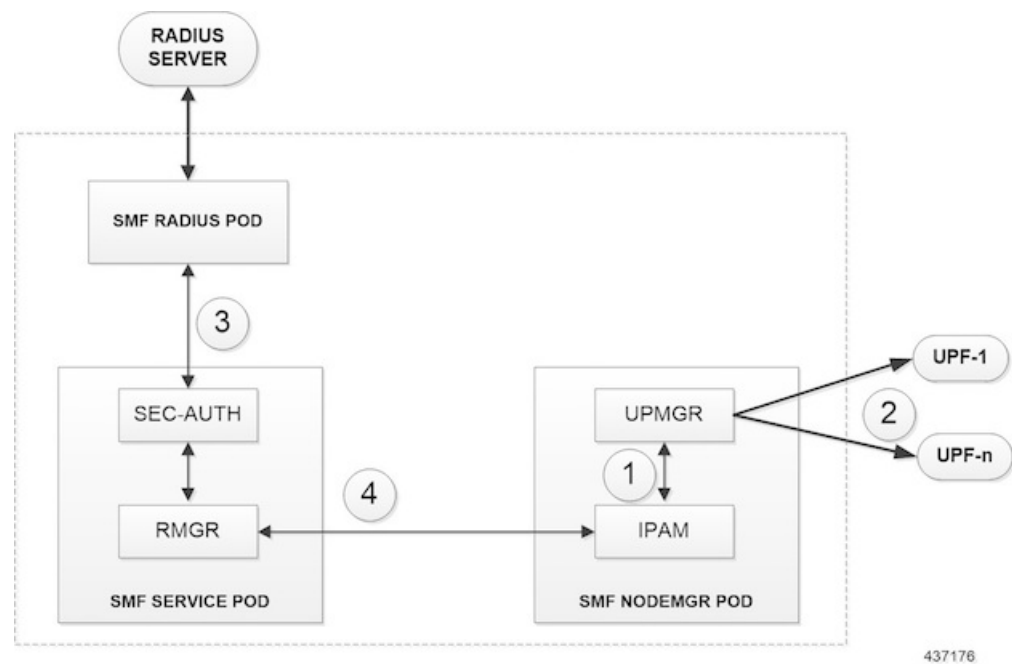
- Static pool configuration
- Splits static address-ranges into smaller chunks and associates them with the configured UPFs
- Enables program routes according to static address-range reservation during UPF association
- Enables secondary authentication under the DNN profile
- Selects UPF based on reserved address-range and Framed-IP received from the Authentication response

## How it Works

This section provides a brief of how the Static IP Support feature works.

The SMF receives a framed-IP address of the subscriber from external AAA servers such as RADIUS. While IPAM is not involved in individual IP address management in this scenario, it still handles the route management and UPF management for static address-ranges.

IPAM splits the 'static' address-ranges equally according to number of UPFs present in the SMF configuration. Unlike dynamic IP, IPAM splits all static-IP address-ranges and assigns them for all configured UPFs. IPAM involves and selects an UPF when the external AAA server returns the framed-IP of the subscriber. IPAM looks for the route which includes this static-IP and then selects the UPF where the route is already configured.



### Procedure

1. IPAM splits the static ranges into equal number of address-ranges based on number of configured UPFs.
2. The UPMGR programs the corresponding static routes on the associated UPFs.
3. Subscribers get static IP from Radius server authorize response.
4. SMF service selects the right UPF based on ADDR ranges and UPF map allocation from the Node Manager.

### Address-Range Split

Splitting a given address-range into smaller address-ranges is a key functionality of the IPAM server and IPAM cache. The following guidelines determine address-range split:

1. Size of a split address-range depends upon the 'configured' value or the 'default' value as per the AFI type.
2. Size of a split address-range must be a 'power-of-2' or at least to the closest of it. That is, it should be able to represent the split range in "subnet/mask" notation such that a route can be added in the Data Plane (User Plane) if required.
3. 'Configured' or 'default' address-range-size must be at the 'power-of-2'.

The address-range must be split into smaller ranges immediately on configuration or initial start-up. This helps in better sorting of address-ranges based on size and faster allocation during actual address-range-allocation requests. The address-range exchange between modules is always in the mentioned size.

Table 121: Examples of IPv4 Address-Range Split

Address-Range	Split-Size (number of addresses per range)	Split-ranges (* Odd sized ranges)	Route Notation
1.1.1.0 - 1.1.1.255	128	[1] 1.1.1.0 – 1.1.1.127 [2] 1.1.1.128 – 1.1.1.255	[1] 1.1.1.0/25 [2] 1.1.1.128/25
1.1.0.0 – 1.1.10.255	256	[1] 1.1.0.0 – 1.1.0.255 [2] 1.1.1.0 – 1.1.1.255 [3] 1.1.2.0 – 1.1.2.255 ... [n] 1.1.10.0 – 1.1.10.255	[1] 1.1.0.0/24 [2] 1.1.1.0/24 [3] 1.1.2.0/24 ... [n] 1.1.10.0/24
1.1.0.5 – 1.1.2.200	256	[1] 1.1.0.5 – 1.1.0.255 * [2] 1.1.1.0 – 1.1.1.255 [3] 1.1.2.0 – 1.1.2.200 *	[1] 1.1.0.0/24 [2] 1.1.1.0/24 [3] 1.1.2.0/24

Table 122: Examples of IPv6 Address-Range Split

Address-Range	Split-Size (number of addresses per range)	Split-ranges (* Odd sized ranges)	Route Notation
1:: - 1::1000	1024	[1] 1:: – 1::3FF [2] 1::400 – 1::7FF [3] 1::800 – 1::BFF [4] 1::C00 – 1::FFF	[1] 1::/118 [2] 1::400/118 [3] 1::800/118 [4] 1::C00/118
1::3 - 1::1DEF	1024	[1] 1::3 – 1::3FF * [2] 1::400 – 1::7FF [3] 1::800 – 1::BFF ... [n] 1::1C00 – 1::1DEF *	[1] 1::/118 [2] 1::400/118 [3] 1::800/118 ... [n] 1::1C00/118

### Examples of IPv6 Address-Range Split

Prefix split needs two length fields for performing the split.

- Network length
- Host length

Prefixes are split between these and a new route is calculated.

Example 1: network-length = 48, prefix-length = 64



Total (64-48) = 16 bits (that is, 65536 prefixes are available for the split)

Example 2: network-length = 32, prefix-length = 56

Total (56-32) = 24 bits (that is, 16 million prefixes available for the split)



**Note** For Cloud-Native 5G SMF, the host-length is hard-coded as '64'. Only network-length can be configured via the CLI.

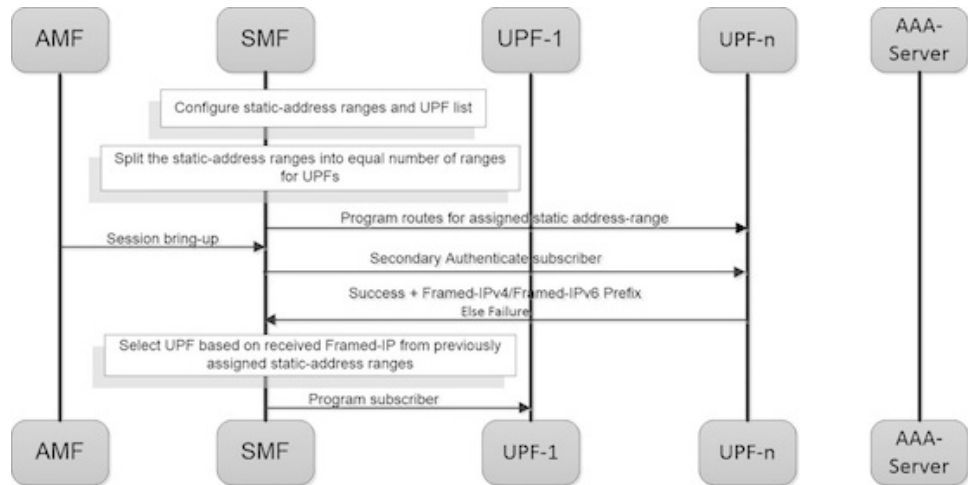
**Table 123: Examples of IPv6 Address-Range Split**

Prefix-Range	Split-Size (number of addresses per range)	Split-ranges (* Odd sized ranges)	Route Notation
1:2:3:: Nw-len = 48 Host-len = 64	8192	[1]1:2:3:: ... 1:2:3:1fff [2]1:2:3:2000:: ... 1:2:3:2fff:: [3]1:2:3:3000:: ... 1:2:3:3fff:: ...	[1]1:2:3::/51 [2]1:2:3:2000/51 [3]1:2:3:3000/51 ...

## Call Flows

This section describes the static IP call flow.

**Figure 78: Static IP Call Flow**



437175

**Table 124: Static IP Call Flow Description**

Step	Description
1	Configure the static-address ranges and UPF list.
2	Split the static-address ranges into equal number of ranges for UPFs.
3	Enable program routes for the assigned static address-range.
4	Bring up the session.
5	Enable secondary authentication under the DNN profile.
6	The SMF sends the Authentication Request to the RADIUS server. The RADIUS server sends an Authentication Response with the 'static-ip' of the subscriber. The SMF selects the UPF based on the 'static-ip' and continues with the programming.
7	Complete the subscriber programming.

## Limitations

The Static IP Support feature has the following limitations:

- Change of a pool from dynamic to static and vice-versa is not supported when in system-running mode.
- Addition or removal of UPF is not supported when in system-running mode.
- The address-range split must be optimal based on the number of UPFs and number of addresses in the ranges.

**For example:**

- If there are 2 UPFs and 1024 addresses specified in the range, then specify the per-dp-split-size as 512.
- If there are 3 UPFs and 1024 addresses, then specify the per-dp-split-size as 256.

## Configuring Static IP Support

Use the following commands to configure the Static IP Support feature.

```

configure
  ipam
    address-pool pool_name
      static
    end

```

**NOTES:**

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool\_name*: Specifies the name of the address pool to enter the pool configuration. *pool\_name* must be the name of the address pool.
- **static**: Enables the static IP mode.

# Dual-Stack Static IP Support Through IPAM

## Feature Description

The SMF supports dual-stack static IP using IPAM. For dual-stack sessions, the AAA server sends both the IPv4 and IPv6 address prefixes as part of the Access-Accept message. In the SMF-IPAM configuration, both the IPv4 and IPv6 address prefixes are added in the same pool. The IPAM assigns both the IPv4 and IPv6 routes to a single UPF.

During the UPF selection, the Node Manager application uses the UPF for both the IPv4 and IPv6 addresses from the IPAM to handle them accordingly.

## How it Works

The SMF supports dual-stack static IP through IPAM in the following ways:

- Pool to UPF mapping—Based on the number of UPFs available, the IPv4 address-ranges and IPv6 prefix-ranges are split into smaller chunks. Then, the pair (chunk) is configured into the same IPAM pool.

IPAM assigns all the addresses and prefixes that are configured in one dual-stack pool to a UPF in the manner they are received. The AAA server returns the dual-stack addresses from the same pair. From these addresses, SMF selects one UPF for dual-stack programming.

The load-balancing of number of addresses and prefixes are managed. IPAM performs only the dual-stack static-pool to UPF mapping.

- Address-range no-split configuration—IPAM uses the "no-split" configuration to prevent splitting the address-ranges into smaller chunks. This configuration helps to prevent having multiple routes programming for a specific range.

The following table lists the errors or exceptions and how to handle them:

**Table 125: Error and Exception Handling**

Error or Exception	Exception Handling
IPv4 UPF and IPv6 UPF are configured incorrectly	<ol style="list-style-type: none"> <li>1. Select an active UPF. In case both the UPFs are active, select the UPF with the IPv4 address.</li> <li>2. Reset the IP information of the other stack and update the PDU session type accordingly.</li> </ol>
IPv4 address is invalid or null	Select the UPF with IPv4 address and update the PDU session type accordingly.
IPv6 prefix is invalid or null	Select the UPF with IPv6 address and update the PDU session-type accordingly.
IPv4 address and IPv6 prefix are invalid	Both the IPv4 address and IPv6 prefix are rejected.

## Limitations

The dual-stack static IP support using IPAM feature has the following limitation:

When the system is in running mode, the change in 'no-split' configuration is not supported.

## Configuring Dual-Stack Static IP Support Using IPAM Feature

This section describes how to configure the dual-stack static IP support using IPAM.

### Configuring IPAM No-Split

This section describes how to configure the IPAM no-split.

```
configure
 ipam
   address-pool pool_name
   ipv4
     split-size no-split
   exit
   ipv6 prefix_ranges
     split-size no-split
   exit
 exit
```

#### NOTES:

- **split-size no-split**—Prevents the IPv4 address-ranges or IPv6 prefix-ranges from splitting into smaller chunks.

## IPAM Offline Mode Support

### Feature Description

The SMF supports the addition of a dynamic pool, IPv4, or IPv6 address-range to a dynamic pool by default. The new chunks are added to the respective tags, such as DNN, and are assigned from the same pool.

To delete a dynamic pool or an IPv4 or IPv6 address-range from a dynamic pool:

1. Configure the pool or address-range as offline. The IPAM then stops assigning addresses from the respective pool or address-range.
2. Use the following **clear-subscriber** CLI commands to delete the subscribers based on respective pool or address range that are configured to offline mode:
  - **clear subscriber ipv4-pool** *pool\_name*
  - **clear subscriber ipv4-range** *pool\_name/start\_of\_range*
  - **clear subscriber ipv6-pool** *pool\_name*
  - **clear subscriber ipv6-range** *pool\_name/start\_of\_range*

3. Use the following **cdl show** CLI commands and wait until all the subscribers are deleted:
  - **cdl show sessions count summary filter { key ipv4-pool: *pool\_name* condition match }**
  - **cdl show sessions count summary filter { key ipv4-range: *pool\_name/start\_of\_range* condition match }**
  - **cdl show sessions count summary filter { key ipv6-pool: *pool\_name* condition match }**
  - **cdl show sessions count summary filter { key ipv6-range: *pool\_name/start\_of\_range* condition match }**
4. After all the subscribers are deleted, delete the pool or address-range from the IPAM configuration.

## Configuring the IPAM Offline Mode

This section describes how to configure the IPAM offline feature for pool, IPv4 address-range, and IPv6 prefix-ranges.

### Configuring Pool to Offline Mode

Use the following command to configure the entire pool to offline mode.

```
configure
ipam
  address-pool pool_name
  offline
  ...
  exit
exit
```

#### NOTES:

- **address-pool *pool\_name***—Specifies the name of the pool to enter the pool configuration. *pool\_name* must be the name of the address pool.
- **offline**—Configures the pool to offline mode.

### Configuring IPv4 Address-Range to Offline Mode

Use the following command to configure the IPv4 address-range to offline mode.

```
configure
ipam
  address-pool pool_name
  vrf-name vrf_name_value
  ip4
    address-range start_ipv4_address end_ipv4_address offline
    address-range start_ipv4_address end_ipv4_address
  !
  !
  !
```

**NOTES:**

- **address-pool** *pool\_name*—Specifies the name of the pool to enter the pool configuration. *pool\_name* must be the name of the address pool.
- **ipv4**—Enters the IPv4 mode.
- **address-range** *start\_ipv4\_address end\_ipv4\_address*—Specifies the IP addresses for the start and end IPv4 address-range.
- **offline**—Configures the selected address-range to offline mode.

## Configuring IPv6 Prefix-Ranges to Offline Mode

Use the following commands to configure IPv6 prefix-range to offline mode.

```

configure
 ipam
   address-pool pool_name
   vrf-name vrf_name_value
   ipv6
     prefix-ranges
       prefix-range prefix_value length length_value offline
       prefix-range prefix_value length length_value
     !
   !
 !

```

**NOTES:**

- **address-pool** *pool\_name*—Specifies the name of the pool to enter the pool configuration. *pool\_name* must be the name of the address pool.
- **ipv6**—Enters the IPv6 mode.
- **prefix-ranges**—Enters the prefix-ranges mode.
- **prefix-range** *prefix\_value length length\_value*—Specifies the prefix-range and prefix-length of the IPv6 prefix-range.
- **offline**—Configures the selected address-range to offline mode.

# IPAM Redundancy Support Per UPF

## Feature Description

The SMF supports IPAM redundancy and load-balancing for each UPF. The IPAM running in the Node Manager microservice has two IPAM instances that are associated to each UPF. When one IPAM instance is inactive, the other IPAM instance manages the address allocation requests for the UPF.

The IPAM redundancy support per UPF feature supports the following functionality:

## How it Works

This section provides a brief of how the IPAM redundancy support per UPF feature works.

- Peer Selection—The Node Manager peer is selected during the UPF association.
- UPF Registration with Peer IPAM—IPAM is notified with the instance ID of the peer for the UPF during the registration of the UPF call. IPAM allocates routers from the local data for the specific DNN and checks if the peer IPAM instance is in active or inactive state.

If the peer IPAM instance is active, a REST call is sent to it to register to the same UPF in the local instance and to receive the routes as response.

If the peer IPAM instance is inactive, the local instance takes over the IPAM context of the remote instance. Then, the local instance registers to the UPF, receives the routes, and keeps the data back in the cache-pod. After the peer instance is active, it restores the same data from the cache-pod.

Routes from both the instances are sent to UPF for load-balanced address allocations from both the instances.

- Address Allocation in Load-Balanced Model—As one UPF is registered to two IPAM servers, SMF sends the address allocation requests to any peer that is load-balanced. Respective IPAM instances assign new addresses from their local address bitmap. If one peer instance is inactive, the other peer instance handles all the requests.
- Address-Release Request Handling—In IPAM, the Address Release request is sent to the instance that had allocated the IP the first time. If that peer is inactive, the Address Release request is sent to the peer IPAM.

The IPAM instance that receives the address releases for remote instances, keeps buffering these instances locally and updates the cache-pod periodically. After the remote peers are active, they handle the buffered address-release requests.

- Release of the UPF—When a peer IPAM is active during the release of a UPF, a REST call is sent to clear the data. If the peer IPAM is inactive, the existing IPAM instance takes over the operational data of the remote IPAM, clears the UPF information, and updates the cache-pod.

## IPAM Static IP Pool Enhancements

### Feature Description

The IPAM Static IP Pool Enhancement feature in SMF provides the following functionality:

- Dynamically add a static IP pool or static IP address range when the system is running.
- Dynamically delete an IP pool or static IP address range when the system is running.
- Handle UPF addition, deletion, and Sx path failure.
- Add a DNN to an existing UPF.

## How it Works

The following sections describe the sequence of operation for this feature in SMF.

### Adding a DNN

This section describes the sequence of operation for adding a DNN.

1. Create static IP pool in IPAM with the corresponding DNN.
2. Add a DNN Profile.
3. If applicable, add the UPFs.
4. Associate the IP address ranges of the DNN to available UPFs.

**Note**

The route is added as part of RegisterUpf requests during explicit Sx association.

### Adding a Static IP Address Range

This section describes the sequence of operation for adding a static IP address range in SMF.

- If new static IP address range is added to a single stack IP pool, the IP address ranges are split according to the configuration and associated with available UPFs in load-sharing manner.
  1. Similar to initial association, intermediate association is also done based on the number of IP addresses against the number of configured UPFs.
  2. If UPF is already registered with IPAM:
    - Route addition is triggered, or else
    - No immediate action is taken
- If a dual stack pool is configured, all IP address ranges, both IPv4 and IPv6 are associated with the UPF, which is the least loaded.
  - If UPF is already registered with IPAM:
    - Route addition is triggered, or else
    - No immediate action is taken

### Adding a Static IP Pool

This section describes the sequence of operation for adding a static IP pool in SMF.

- If a single stack IP pool is configured, the IP address ranges are split according to the configuration and associated with available UPFs in load-sharing manner.
  1. Similar to initial association, intermediate association is also done based on the number of IP addresses against the number of configured UPFs.



2. If UPF is already registered with IPAM:
  - Route addition is triggered, or else
  - No immediate action is taken
- If a dual stack pool is configured, all IP address ranges, both IPv4 and IPv6 are associated with the UPF, which is the least loaded.
  - If UPF is already registered with IPAM:
    - Route addition is triggered, or else
    - No immediate action is taken

## Adding the UPF

This section describes the sequence of operation for adding the UPF.

1. When a UPF is added, NodeMgr sends the list of IPs to IPAM.
2. When new static IP pool or static IP address ranges are configured, this feature enables route association for UPFs based on load-balancing model.




---

**Note** The same procedure is applicable when a new or existing DNN is added to a new or existing UPF respectively.

---

3. To redistribute existing static IP pools or ranges to the new UPF, use the following MOP:
  - Mark a pool/range offline
  - Clear subscribers
  - Delete IP pool or range
  - Add the IP pool or range again.

This step allocates the chunks to the new UPF.

## Deleting the UPF

This section describes the sequence of operation for deleting an existing UPF.

1. To delete an existing UPF, first it is marked "offline".  
Run the appropriate CLI commands to manually clear the sessions.
2. The NodeMgr notifies IPAM about the UPF removal.
3. IPAM moves the static address ranges from all DNNs of the removed UPF to other available UPFs.
4. The Nodemgr initiates ReleaseUpf to IPAM. IPAM releases dynamic address-ranges to the free-list.
5. The Nodemgr sends an N4-Association-Release message to UPF and to cleanup UPF from the cache.



**Note** If the UPF is not marked offline and a manual clean-up is not performed before its removal, the system behavior might be erratic.

## Deleting a Static IP Address Range

This section describes the sequence of operation for deleting a static IP address range in SMF.

1. To delete an IP address range from a static IP pool, first it is marked "offline".
2. Reject new calls, which have the IP address assigned from the offline IP address range.
3. Remove the existing subscribers. To remove the existing subscribers, run the following CLI commands.

```
clear subscriber ipv4-range { pool_name | start_of_range }
clear subscriber ipv6-range { pool_name | start_of_range }
```

4. Remove the static IP address range configuration and trigger route deletion to registered UPFs.

## Deleting a Static IP Pool

This section describes the sequence of operation for deleting a static IP pool in SMF.

1. To delete a static IP pool, first it is marked "offline".
2. Reject new calls, which have the IP address assigned from the offline IP pool.
3. Remove the existing subscribers. To remove the existing subscribers, run the following CLI commands.

```
clear subscriber ipv4-pool pool_name
clear subscriber ipv6-pool pool_name
```

4. After all the subscribers are deleted, remove the IP pool configuration and trigger route deletion to registered UPFs.

## Removing Sx Association with an Offline UPF

This section describes the sequence of operation for removing association with an offline UPF.

1. Set UPF as offline in **profile-network-element-upf** configuration.
 

SMF stops selecting and associating dynamic IPs to the specific UPF for new sessions.
2. NodeMgr receives configuration change notification about an offline UPF.
 

SMF stops selecting and associating static IPs to the specific UPF for new sessions or associations.
3. NodeMgr acknowledges the heart-beat messages for an already associated UPF.
4. NodeMgr acknowledges the N4 association update from the UPF with release indication.

This step does not impact the static and dynamic chunk allocations for IPAM.

The IPAM module is unaware of the offline status for the UPF. It might include the offline UPF to add new IP pool or addr-ranges.

## Sx Path Failure on UPF

This section describes the sequence of operation for Sx path failure on UPF.

1. The NodeMgr initiates the **subscriber clear** command.
2. The NodeMgr sends **UnRegisterUpf** to IPAM.
3. IPAM releases any dynamic IP address ranges and moves it to free range list.
4. IPAM retains any static IP address ranges for the UPF. Sx path failure does not impact static IP address mappings.

## Limitations

The IPAM Static IP Pool Enhancement feature has the following limitations:

- When the system is running, the DNN cannot be removed from a UPF.
- Changing dual-stack IPAM pool to single-stack or changing single-stack IPAM pool to dual-stack is not supported.

# IPAM Quarantine Timer Support

## Feature Description

The IPAM Quarantine Timer Support feature supports the IPAM quarantine timer for the IP pool address. This feature keeps the released IP address busy until the quarantine timer expires to prevent the reuse of that IP address. Each IP pool must be configured with a timer value. This value determines the duration of a recently released address to be in the quarantine state before it is available for allocation. After the timer expires, the IP address is available in the list of free addresses for allocation by the subscriber. A released IP address with no address quarantine timer is considered to be in use for allocation. If a subscriber attempts to reconnect when the address quarantine timer is armed even if it is the same subscriber ID, the subscriber does not receive the same IP address.

## Configuring the IPAM Quarantine Timer Support Feature

This section describes how to configure the IPAM quarantine timer support feature.

### Configuring IPAM Quarantine Timer

This section describes how to configure the IPAM quarantine timer.

```
configure
  ipam
    address-pool pool_name
      address-quarantine-timer quarantine_timer_value
      vrf-name vrf_name_value
    ip4
      address-range start_ipv4_address end_ipv4_address
```

```

    address-range start_ipv4_address end_ipv4_address
  !
!

```

**NOTES:**

- **ipam**—Enter the IPAM configuration.
- **address-pool** *pool\_name*—Specifies the name of the pool to enter the pool configuration. *pool\_name* must be the name of the address pool.
- **address-quarantine-timer** *quarantine\_timer\_value*—Specifies the value of the quarantine timer in seconds. *quarantine\_timer\_value* must be in the range of 4-3600 seconds. The default value is 4.
- **vrf-name** *vrf\_name\_value*—Specifies the name of the VPN routing and forwarding (VRF) for the pool.
- **ipv4**—Enters the IPv4 mode.
- **address-range** *start\_ipv4\_address end\_ipv4\_address*—Specifies the IP addresses for start and end IPv4 address-range.

## show ipam pool

Field	Description
PoolName	Name of the Address Pool.
Ipv4Utilization	Utilization percentage for IPv4 address for this pool.
Ipv6AddrUtilization	Utilization percentage for IPv6 address for this pool.
Ipv6PrefixUtilization	Utilization percentage for IPv6 prefix address for this pool.

## show ipam pool <pool-name>

Field	Description
Ipv4Addr [Total/Used/Utilization]	Total IPv4 address available(configured for this pool) / Number of used address / Utilization percentage for IPv4 address.
Ipv6Addr [Total/Used/Utilization]	Total IPv6 address available(configured for this pool) / Number of used address / Utilization percentage for IPv6 address.
Ipv6Prefix [Total/Used/Utilization]	Total IPv6 prefix address available(configured for this pool) / Number of used address / Utilization percentage for IPv6 prefix

**show ipam pool <pool-name> ipv4-addr**

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
AllocContext	Name of data plane to which this address range is allocated.
Flag	Flag Indicate weather pool is Static or if it is offline.

**show ipam pool <pool-name> ipv6-addr**

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
AllocContext	Name of data plane to which this address range is allocated.
Flag	Flag Indicate weather pool is Static or if it is offline.

**show ipam pool <pool-name> ipv6-prefix**

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
AllocContext	Name of data plane this address range is allocated.
Flag	Flag Indicates whether pool is Static or if it is offline, S(Static) and O(Offline).

**show ipam dp**

Field	Description
DpName	Name of the data plane which is registered.
Ipv4Utilization	Utilization percentage for IPv4 by this data plane.
Ipv6AddrUtilization	Utilization percentage for Ipv6 address by this data plane.

**show ipam dp <dataplane-name>**

Field	Description
Ipv6PrefixUtilization	Utilization percentage for Ipv6 prefix by this data plane.

**show ipam dp <dataplane-name>**

Field	Description
Ipv4Addr [Total/Used/Utilization]	Total IPv4 address available(configured for this data plane) / Number of used address / Utilization percentage for IPv4.
Ipv6Addr [Total/Used/Utilization]	Total IPv6 address available(configured for this data plane) / Number of used address / Utilization percentage for IPv6.
Ipv6Prefix [Total/Used/Utilization]	Total IPv6 prefix address available(configured for this data plane) / Number of used address / Utilization percentage for IPv6 prefix.

**show ipam dp <dataplane-name> ipv4-address**

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
Route	Route allocated for this data plane.
N/P	Display the NodeMgr instance IDs from which it received routes Flag Indication S(Static) and O(Offline).

**show ipam dp <dataplane-name> ipv6-addr**

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
AllocContext	Name of pool to which this address range belongs.
Route	Route allocated for this data plane.
N/P	Display the NodeMgr instance IDs from which it received routes.

Field	Description
Flag	Flag Indicate whether pool is Static or if it is offline, Flag Indication S(Static) and O(Offline).

## show ipam dp <dataplane-name> ipv6-prefix

Field	Description
StartAddress	Start address of the range.
EndAddress	End address of the range.
AllocContext	Name of pool to which this address range belongs.
Route	Route that is allocated for this data plane.
N/P	Displays the NodeMgr instance IDs from which it received routes Indication, N(Native InstId) and P(Peer InstId).
Flag	Flag Indicate weather pool is Static or if it offline Flag Indication, S(Static) and O(Offline).

## show ipam

Field	Description
PoolName	Displays Ipv4Utilization, Ipv6AddrUtilization, and Ipv6PrefixUtilization.
DpName	Displays Ipv4Utilization, Ipv6AddrUtilization, and Ipv6PrefixUtilization.

# Configuring IPAM Quarantine Qsize Support Feature

This section describes how to configure the IPAM quarantine queue size support feature.

## Configuring IPAM Quarantine Queue Size

This section describes how to configure the IPAM quarantine timer.

```

configure
 ipam
   address-pool pool_name
     address-quarantine-qsize quarantine_queue_size

```

```

    exit
  exit

```

**NOTES:**

- **ipam**—Enter the IPAM configuration.
- **address-pool** *pool\_name*—Specifies the name of the pool to enter the pool configuration. *pool\_name* must be the name of the address pool.
- **address-quarantine-qsize** *quarantine\_queue\_size*—Specifies the value of the quarantine queue size. The default value is 0.

During QT processing, excess IP addresses in quarantine-queue are released to Free-list irrespective of quarantine-timer expiry by force.

# Overlapping IP Address Pools Support

## Feature Description

The Overlapping IP Address Pools feature improves flexibility in assigning IP addresses dynamically. This feature allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces.

You can configure overlapping IP address range across different pools with unique DNN and VRF type.

## Configuring Overlapping IP Address Pools

Use the following sample configuration to configure overlapping static IP address pools.

```

configure
ipam
source local
address-pool pool1
  static
  vrf-name vrf1@ISP
  tags
  dnn dnn1
  exit
  ipv4
  split-size
  per-cache 256
  per-dp 256
  exit
  address-range 12.0.0.1 12.0.10.254
  exit
exit
address-pool pool2
  static
  vrf-name vrf2@ISP
  tags
  dnn dnn2
  exit
  ipv4
  split-size
  per-cache 256

```



```
        per-dp    256
    exit
    address-range 12.0.0.1 12.0.10.254
    exit
exit
exit
```

Use the following sample configuration to configure overlapping IP address pools.

```
configure
ipam ipam
source local
address-pool pool1
    vrf-name vrf1@ISP1
    tags
        dnn dnn1
    exit
    ipv4
        split-size
            per-cache 256
            per-dp    256
        exit
        address-range 12.0.0.1 12.0.10.254
    exit
exit
address-pool pool2
    vrf-name vrf2@ISP2
    tags
        dnn dnn2
    exit
    ipv4
        split-size
            per-cache 256
            per-dp    256
        exit
        address-range 12.0.0.1 12.0.10.254
    exit
exit
exit
exit
```

# Virtual Routing and Forwarding Function

## Feature Description

Different mobile virtual network operators (MVNOs) have the same IP address range in the deployment. The SMF supports this functionality using the Virtual Routing and Forwarding (VRF) configuration, where the same IP address range can exist in different VRFs. In such cases, IP pool configuration includes the VRF name. In these scenarios, the SMF sends IP address chunk details along with the configured VRF name to UPF. This helps UPF to map the IP address to VRF configured within UPF.

## Configuring VRF

This section describes how the SMF configures the VRF.

## Configuring VRF Name

Enable VRF name in the configuration of address pool. When “vrf-name” in the IP pool is configured with “@” character, the first part before “@” is treated as “VRF” name which is sent to UPF and the second part after “@” is sent as context name in N4 Association Update message.

When “vrf-name” in the IP pool is configured without “@” character, the entire name is sent as context name (existing behaviour) in N4 Association Update message.

The SMF sends the VRF name in N4 Session Establishment request if it is configured with “@” in the pool in “UE IP VRF” IE.

Use the following configuration to configure the VRF name:

```
configure
  ipam
    address-pool pool_name
      vrf-name vrf_name
    end
```

### NOTES:

- **ipam**: Enters the IPAM configuration mode.
- **address-pool** *pool\_name*: Configures the address pool configuration. *pool\_name* must be the name of the address pool.
- **vrf-name** *vrf\_name* : Specifies the name of the VRF for the pool.



# CHAPTER 25

## Local Breakout-based Roaming Support

- [Feature Summary and Revision History, on page 373](#)
- [Feature Description, on page 373](#)
- [Architecture, on page 374](#)

### Feature Summary and Revision History

#### Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 126: Revision History*

Revision Details	Release
First introduced.	2021.01.0

### Feature Description

SMF supports local breakout based roaming with this release. Following roaming features are supported:

- Roaming for 5G sessions connected via NR
- Roaming for 4G/WiFi sessions connected via EUTRAN

- LI support
- Deployment model with/with out SEPP

**Important**

Refer "Multiple PLMN Support" section for Roaming Status of the subscriber and to determine the Serving PLMN in detail.

## Architecture

### How Roaming Status is Derived

CLI-based Roaming Status derivation

- Checking Subscriber Policy
- User reference for Multi PLMN
- If UE PLMN and serving PLMN both belong to SMF PLMN list, then it's a home subscriber.  
If UE PLMN doesn't belong to SMF PLMN and serving PLMN belongs to PLMN list, then it's a visitor-lbo subscriber.

Roaming Status configuration has higher precedence.

### LBO SMF

SMF supports local breakout functionality for in-roamers, following key features supported by SMF.

- Detection of in-roamers – based on local configuration and MCC/MNC in the SUPI received.
- N11
  - Determination of LBO (or HR) for the in-roamers, if LBO can't support, SMF sends Error to AMF so that AMF reinitiates the PDU session establishment procedure with HR.
  - Support of PCF ID that is V-PCF from AMF.
- N2
  - SMF provides S-NSSAI of VPLMN in the N2 SM Information.
- N7
  - Selection of PCF in VPLMN
  - vPCF interacts with AF in HPLMN for PCC rule generation (ex: IMS), however, PCC rules are otherwise generated using roaming policies and vPCF doesn't have access to the subscribed policies in HPLMN. Also vPCF doesn't interact with CHF for spending limits. Given this, PCC rules in LBO are expected to be restricted in capabilities.
- N40

- Selection of CHF in VPLMN, apart from selecting CHF from VPLMN, vSMF considers additional parameters of the HPLMN ID that CHF has to service the roamer status (in-roamer) of the UE.
- N10
  - Selection of UDM in HPLMN
- NRF
  - SMF uses the “chf-supported-plmn” in query parameters while discovering vCHF servicing HPLMN.
  - During EPS procedures, if the PGW-C+SMF supports more than one S-NSSAI and the APN is valid for more than one S-NSSAI, before the PGW-C+SMF provides an S-NSSAI to the UE, it has to use the Nnssf\_NSSelection\_Get service operation to retrieve a mapping of the Subscribed S-NSSAIs to Serving PLMN S-NSSAI values.

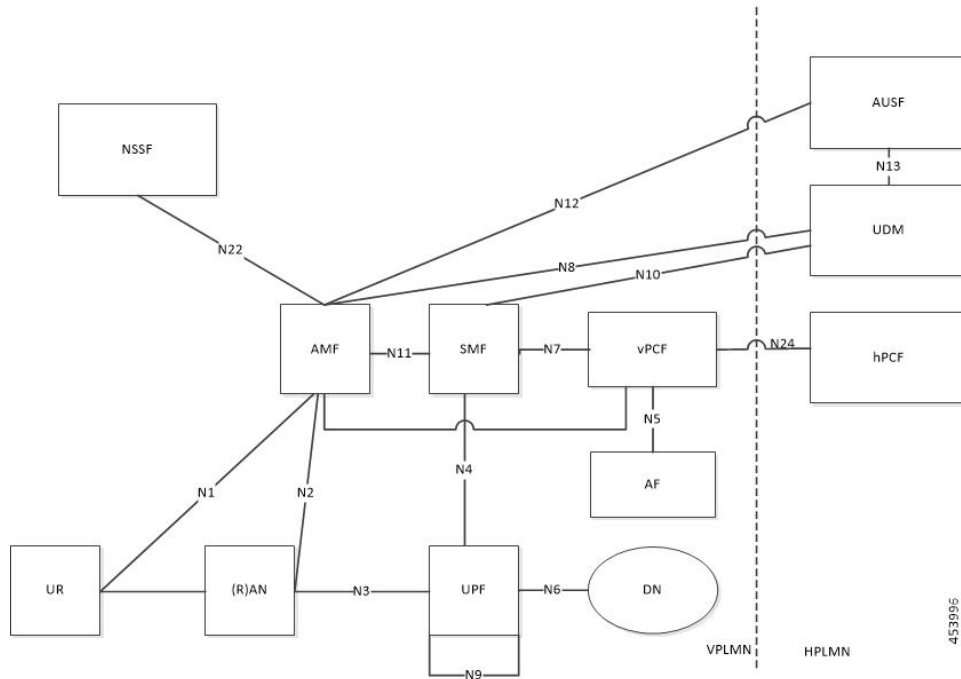
#### Node Selection considerations

- When roaming is enabled, each SMF registers interPlmnFqdn with NRF. This helps AMF to select hSMF in a different PLMN.
- SMF supports target-plmn-list and requester-plmn-list as part of query parameters.
- All NF discovery queries happen to NRF in the serving PLMN.

#### 5G-NR LBO Scenario

The following diagram shows a 3GPP reference point for nodes in VPLMN and HPLMN for a local breakout case for the 5G sessions:

Figure 79: Local Breakout Roaming Architecture for 5G Sessions

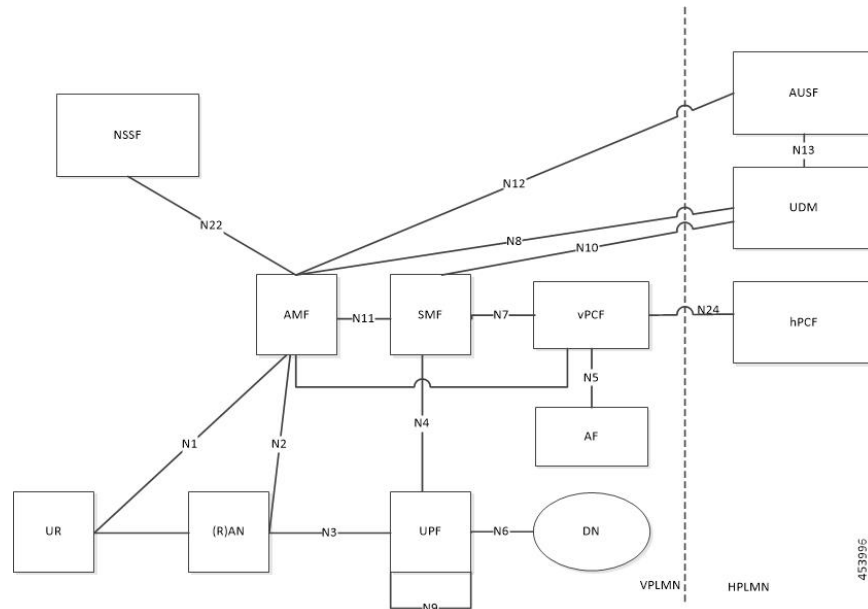


As shown in the preceding diagram, the SMF resides in the VPLMN. Only AUSF and UDM are the NFs in the HPLMN. The PCF in the VPLMN can communicate with PCF in the HPLMN over N24 interface to get the policies related to the subscriber session and pass them to SMF.

### EPC LBO

The following diagram displays the local roaming architecture breakout for the 4G sessions connected to the SMF + PGW-C in EPC interworking case:

Figure 80: Local Breakout Roaming Architecture for 4G Sessions



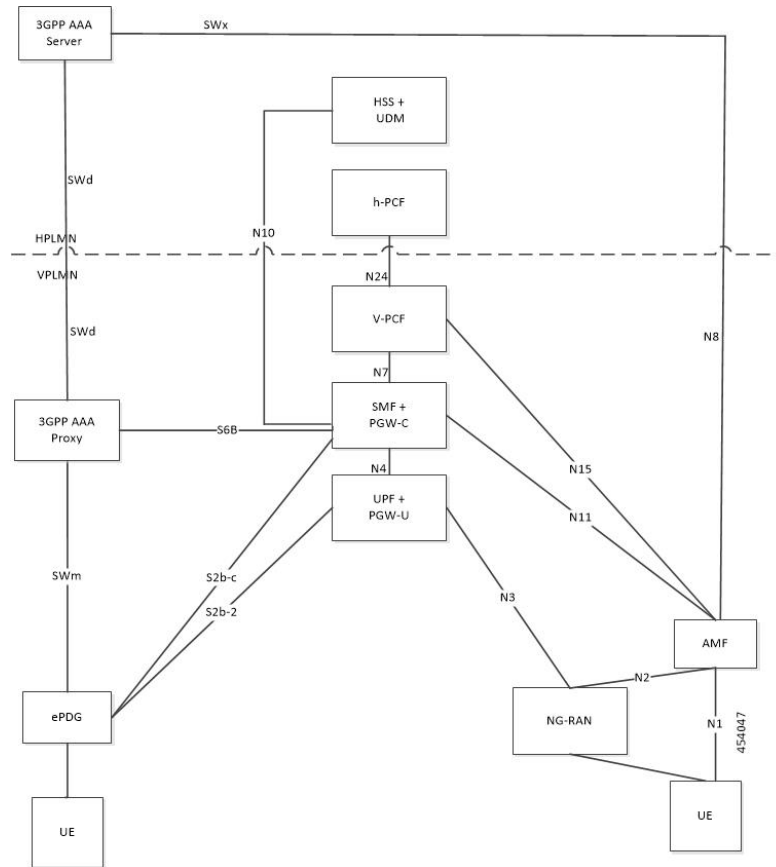
During LBO roaming for 4G sessions, the SGW and the SMF+PGW-C both reside in VPLMN. All northbound SBI interfaces are common for 4G and 5G case.

- SMF-IWK resides in vPLMN
- SMF-IWK interacts with vPCF, vCHF
- SMF-IWK interacts with UDM (in hPLMN).
- SMF-IWK supports S5-c interface towards SGW.

### ePDG LBO

The following diagram displays the local roaming architecture breakout for the Wi-Fi sessions connected to the SMF + PGW-C in EPC interworking case:

Figure 81: Local Breakout Roaming Architecture for Wi-Fi Sessions



- SMF+IWF resides in vPLMN.
- SMF-IWK interacts with vPCF, vCHF.
- SMF-IWK interacts with UDM (in hPLMN).
- SMF-IWK doesn't support S6b towards 3GPP AAA proxy, instead N10 is used (N10->SWx->SWd).

### 5G PDU Establishment During LBO

This section describes the requirements on SMF for PDU session establishment in LBO roaming case:

1. If SMF at vSMF isn't able to handle or process any parameter in the NAS PDU SESSION ESTABLISHMENTT REQUEST it would send a SmContextCreateError back to AMF with cause HOME\_ROUTED\_ROAMING\_REQUIRED so that AMF can reinitiate the process with home routed roaming. The example for this is when NAS PDU SESSION ESTABLISHMENTT REQUEST has requested SSC mode as 3 and allowed SSC mode in vSMF doesn't support this.
2. SMF receives both hplmnSnsai and sNssai. The validation of Nssai against the vSMF's supported Nssai is done using sNssai.
3. On N40 interface:



- a. vSMF will fill the PDUSessionChargingInformation □ userInformation □ roamerInOut attribute value towards CHF in the CDR message. The value should be filled as IN\_BOUND for in-roamers and OUT\_BOUND for out-roamers.
  - b. vSMF fills the PDUSessionInformation □ chargingCharacteristicsSelectionMode IE with appropriate value (HOME\_DEFAULT, ROAMING\_DEFAULT and VISITING\_DEFAULT) for non-roaming and roaming cases.
  - c. hPlmnId and servingCNPlmnId fields in the PDUSessionInformation IE must be filled as per the roaming status of the UE.
4. During N1N2MessageTransfer the sNSSAI provided in N2 content should be the VPLMN sNSSAI.
  5. For LBO roaming scenario, the PDU Session Establishment Accept includes the S-NSSAI from the Allowed NSSAI for the VPLMN and also it includes the corresponding S-NSSAI of the HPLMN from the Mapping Of Allowed NSSAI that SMF received from AMF.
  6. For an emergency session, even if the local configuration allows UDM registration for authenticated UE, vSMF shouldn't do it for roaming cases.
  7. SMF uses HPLMN for UDM discovery for LBO Roaming.

#### 4G PDN Establishment During LBO

The SGW sends Serving Network IE to the PGW with the PLMN id where the SGW belongs. SMF uses that PLMN as VPLMN for validation, node selection and passing on the VPLMN to other north bound interfaces.

The N40 interface related requirements and the emergency session related requirements applicable for 5G session creation, also apply for the 4G and Wi-Fi sessions.

#### Session Management

- With roaming considerations, SMF sessions can be categorized into the following flavors.
  - Non-roaming sessions
  - LBO Sessions
  - vSMF-HO sessions
  - hSMF-HO sessions
- SMF supports all flavors of sessions in the same network function deployment, also the SMF service pods service sessions of all the mentioned flavors.
- UE1 – in-bound roamer, LBO (262-06)
- UE2 – in-bound roamer, HR (302-610)
- UE3 – out-bound roamer, HR (310-310)
- UE4 – homer (310-240)
- SMF – Operator's SMF
  - List of home PLMNs – configured under service profile. When multiple PLMNs are configured, one is marked as primary home PLMN.

- 310-310, 310-240\*(primary)
- List of (roaming) serving PLMNs (excluding home PLMNs), optional – configured under service profile
  - 262-06, 302-610
- AMF1 – Operator’s AMF serving 310-240
- AMF2 – Operator’s AMF serving 310-310
- AMFp – Partner’s AMF serving 262-06; 302-610
- SMFp – Partner’s SMF serving Operator’s 310-310; 310-240

### PLM Usage

Interface	Attribute	Home(UE4)	In-roamer(LBO)(UE1)	Out-roamer(HR)(UE3)	In-roamer(HR)(UE2)
	UE PLMN	310-240	262-06	310-310	302-610
NRF	plmn-list in nrf Discover to discover UDM (queryParam)	310-240(UE plmn)	262-06(UE plmn)	310-310 (UE plmn)	NA
NRF	plmn-list in nrf Discover to discover RCH (queryParam)	310-240(UE plmn)	310-310(serving plmn)	310-310(UE plmn)	310-310(serving plmn)
N10	plmn in smfRegistration IE in N10 registration	310-240(serving plmn)	310-310(serving plmn)	310-240(primary home plmn)	NA
N10	plmn in GET subscription URI	310-240(serving plmn)	310-310(serving plmn)	310-240(primary home plmn)	NA
N10	plmn in sdmSubscription IE in N10 subscription	310-240(serving plmn)	310-310(serving plmn)	310-240(primary home plmn)	NA
N40	plmn in N40 charging data request	310-240(primary home plmn)	310-240(primary home plmn)	310-240(primary home plmn)	310-240(primary home plmn)

Interface	Attribute	Homer(UE4)	In-roamer(LBO)(UE1)	Out-roamer(HR)(UE3)	In-roamer(HR)(UE2)
N40	hPlmnId In PDUSession IE in plmnChgReq in chargingDataRequest	310-240(UE plmn)	262-06(UE plmn)	310-310 (UE plmn)	302-610(UE plmn)
N40	Servingplmn in PDUSession IE in plmnChgReq in chargingDataRequest	310-240(serving plmn)	310-310(serving plmn)	310-240(primary home plmn)	310-310(serving plmn)
N7	plmn in pcf notify for <del>ACN</del> trigger	310-240(serving plmn)	310-310(serving plmn)	310-240(primary home plmn)	NA
N7	plmn in create request to PCF	310-240(serving plmn)	310-310(serving plmn)	310-240(primary home plmn)	NA
Radius	plmn in 3GPP ue location IE radius authentication	310-240(serving plmn)	310-310(serving plmn)	NA	
Radius	plmn in 3GPP GGSN MCCMNC in radius authentication	310-240(primary home plmn)	310-240(primary home plmn)	NA	
N4	plmn in Xheader of N4 requests	310-240(serving plmn)	310-310(serving plmn)	310-240(primary home plmn)	NA

### Roaming Status Determination

SMF home PLMN supported values:

(home PLMNs)310+310

310+320 (Opr-1 (SMF profile)

(Partner PLMN) 600+300 (Opr 2/Opr-1 that require roaming treatment) (Subscriber policy – 600+300)

1. UE – 310+310 comes from 310+320 => homer (my UE + my serving network).
2. UE – 600+300 comes from 310+310 => in-LBO or in-hrt based on policy/subscription (other UE + my serving network) WRONG CASE.

3. UE – 310+310 comes from 600+300 => out-hrt (my UE + other serving network).
4. UE- 600+300 comes from 600+300=> In-LBO or In-HRT.

## HO Scenarios



**Note** Once roamer status is determined, there wont be change to the status even if the configuration or PLMN values change post HO.

## Local Policies

In HO scenarios, vSMF has to support local policy for the following attributes to enable vPLMN operators to override the signaled parameter from hPLMN domain as per the roaming agreements.

- To allow always-on session requests.
- Paging policy differentiation feature
- PDU session setup in HR or LBO mode
- Subscriber QoS as per the roaming agreement
- Allow ARP priority levels 1-8 for HO roaming sessions.
- Secondary RAT usage support towards vCHF (LBO), towards hSMF (HO)

In case of home routed roaming, as per the local QoS policies governed by roaming agreements and/or SLAs, if vSMF can't accept the requested QoS from hSMF, it performs the following:

- If the vSMF doesn't accept the PDU Session, the vSMF triggers the vSMF initiated PDU Session Release procedure during PDU setup or modifications.
- When the vSMF accepts at least one QoS flow, it transfers (via the AMF) the corresponding N2 (and NAS) request towards the 5G AN (and the UE) but doesn't issue requests for the QoS Flow(s) it has rejected due to these policies. The vSMF notifies the hSMF about the rejected QoS Flows.

## Other Procedures

**Paging Policy Differentiation (PPD):** SMF needs a config per PLMN to allow different PPD profile for different roaming partners. The vSMF picks the appropriate config for the HPLMN and applies the same for the roaming session.

### PCF and UDM Selection:

1. In case of roaming the AMF may select both vPCF and hPCF and can send the vPCF Id to SMF and hPCF Id to the vPCF during policy association. SMF selects the PCF using the received vPCF Id. Later during AMF relocation, target AMF may select a new vPCF and hPCF. When this happens SMF may receive a redirection indication with PCF ID from the existing PCF for the PDU session, the SMF shall terminate the current SM Policy Control association and reselects a PCF based on the received PCF ID. The SMF shall then establish an SM Policy Control association with the reselected PCF.

2. For selection of PCF and UDM based on local configuration the locally configured addresses should map to the VPLMN and HPLMN respectively since the PCF is in VPLMN and UDM is in HPLMN for roaming with LBO case.
3. For NRF-based discovery of PCF and UDM, the query criteria should include VPLMN for PCF discovery and HPLMN for UDM discovery. The AMF can also send the UDMGroup Id to enable SMF select UDM based on UDM group Id. The S-NSSAI used by SMF to select PCF should be the VPLMN S-NSSAI received from AMF. It should be HPLMN N-SSAI for the UDM selection.

**Lawful Interception:** For IRI events reporting from SMF, the sNSSAI information is sent in the message to mediation device. The sNSSAI of the VPLMN is used for roaming cases.





# CHAPTER 26

## Monitoring Support

- [Feature Summary and Revision History](#), on page 385
- [Monitor Subscriber and Monitor Protocol](#), on page 386
- [RPC Remote Host Management](#), on page 392

## Feature Summary and Revision History

### Summary Data

*Table 127: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 128: Revision History*

Revision Details	Release
Added show commands for the RPC feature in App-Infra SMF.	2020.03.0
First introduced.	Pre-2020.02.0

# Monitor Subscriber and Monitor Protocol

## Feature Description

The SMF supports the Monitor Subscriber and Monitor Protocol on the Kubernetes environment. This feature allows to capture messages of subscribers and protocols.

## Converged Core Refactoring Changes

This section describes the changes related to converged core refactoring in this chapter.

The **monitor subscriber supi** CLI command is enhanced to add the **namespace** option to display the output pertaining to the respective namespace.

## Configuring the Monitor Subscriber and Monitor Protocol Feature

### Monitoring the Subscriber

Use the following sample configuration to monitor the subscriber in the SMF.

```
monitor subscriber [ capture-duration duration_sec | imsi imsi_value |
internal-messages [ yes ] | namespace [ sgw | smf ] | supi supi_id |
transaction-logs [ yes ] ]
```

#### NOTES:

- **capture-duration** *duration\_sec*: Specify the duration in seconds during which monitor subscriber is enabled. The default value is 300 seconds (5 minutes). This is an optional parameter.
- **imsi** *imsi\_value*: Specify the subscriber IMSI. For example: 123456789, \*
- **internal-messages** [ yes ]: Enable internal messages when set to yes. By default, it is disabled. This is an optional parameter.
- **namespace** [ **sgw** | **smf** ]: Enable the specified namespace. By default, namespace is set to none. This is an optional parameter.




---

**Important** This keyword is deprecated in release 2021.02.0 and replaced with **nf-service** keyword.

---

- **supi** *supi\_id*: Specify the subscriber identifier. For example: imsi-123456789, imsi-123\*
- **transaction-logs** [ yes ]: Enable transaction logs when set to yes. By default, it is disabled. This is an optional parameter.

The **monitor subscriber** CLI command can be run simultaneously on multiple terminals. For example, run the CLI simultaneously in two SMF Ops Center terminals for two subscribers (for example, imsi-123456789012345 and imsi-456780123456789) to implement the following:

- Monitor the duration when the monitor subscriber is enabled.



- View internal messages for the specified subscriber.
- View transaction logs for the specified subscriber

Terminal 1: The following command monitors and displays subscriber messages for the specified subscriber.

```
monitor subscriber supi imsi-123456789012345 capture-duration 1000 internal-messages yes
```

Terminal 2: The following command monitors and displays transaction logs for the specified subscriber.

```
monitor subscriber supi imsi-456780123456789 capture-duration 500 internal-messages yes
transaction-logs yes
```

After the capture-duration is over or to stop the CLI, use the **Ctrl+C** keys. The captured messages are reordered and stored in a file. To retrieve the list of stored files, use the **monitor subscriber list** CLI command.

For example:

```
monitor subscriber list
RELEASE_NAMESPACE: 'smf'
'monsublogs/subscriberID_imsi-*_AT_2019-10-22T09:19:05.586237087.txt.sorted'
monsublogs/subscriberID_imsi-123456789012345_AT_2019-10-22T09:20:11.122225534.txt.sorted
```

## Enabling or Disabling the Transaction Messages

Use the following CLI command to enable or disable the presence of request response messages in the transaction logs.

```
config
 logging transaction message [ enable | disable ]
 commit
end
```

NOTES:

- **logging transaction message**: Specifies the transaction messages in the transaction logs.
- **enable**: Enables the presence of transaction messages in the transaction logs.
- **disable**: Disables the presence of transaction messages in the transaction logs.

## Viewing the Sorted File on SMF Ops Center

Use the following CLI command to view the sorted file on the SMF Ops Center screen.

```
monitor subscriber dump filename filename
```

For example:

```
monitor subscriber dump filename
monsublogs/subscriberID_imsi-123456789012345_AT_2019-10-22T09:20:11.122225534.txt.sorted
```

## Monitoring the Interface Protocol

Use the following sample configuration to monitor the interface protocol on the SMF.

```
monitor protocol interface endpoint_name [ capture-duration duration_sec |
gr-instance gr_instance_id ]
```

NOTES:

- **interface** *endpoint\_name*: Specify the endpoint name on which PCAP is captured. This CLI allows the configuration of multiple endpoint names in a single CLI command.
- **capture-duration** *duration\_sec*: Specify the duration in seconds during which the monitor subscriber is enabled. The default is 300 seconds (5 minutes).
- The configured endpoint names can be retrieved using the **show endpoint** CLI command.

The **monitor protocol** CLI can be run simultaneously on multiple terminals. Also, the **interface** *endpoint\_name* CLI allows the configuration of multiple endpoint names in a single CLI command. For example:

```
monitor protocol interface sbi,N4:10.86.73.161:8805,gtpc capture-duration
1000
```

## Viewing Transaction History Logs

Use the following CLI command to view the transaction history on an OAM pod shell. On another terminal, use the **kubectl** command to tail the logs of the OAM pod and then run the following CLI from the Ops Center.

```
dump transactionhistory
```



**Note** In this release, the most recent transaction logs are stored in a circular queue of size 1024 transaction logs.

## Sample Transaction Log

The following is an example of transaction log collected in Monitor Subscriber during SMF PDU session establishment.

```
Transaction Log received from Instance: smf.smf-rest-ep.unknown.smf.0
***** TRANSACTION: 00010 *****
TRANSACTION SUCCESS:
    Txn Type           : N10RegistrationRequest(33)
    Priority            : 1
    Session State      : No_Session
LOG MESSAGES:
    2020/03/03 05:31:39.345 [DEBUG] [infra.transaction.core] Processing transaction Id: 10
    Type: 33 SubscriberID: imsi-123456789012345 Keys: []
    2020/03/03 05:31:39.345 [DEBUG] [infra.transaction.core] Trace is disabled
    2020/03/03 05:31:39.346 [TRACE] [infra.message_log.core] >>>>>>
IPC message
Name: N10RegistrationRequest
MessageType: N10RegistrationRequest
Key:
--body--
{"regInfo":{"ueId":"imsi-123456789012345","pduSessionId":5},"regReq":{"dnn":"intershat",
"pduSessionId":5,"pgwFqdn":"cisco.com.apn.epc.mnc456.mcc123","plmnId":{"mcc":"123","mnc":"456"},
"smfInstanceId":"c388eec5-e2ff-4bda-8154-b5dd9f10ad97","supportedFeatures":"0","singleNssai":{"sd":"Abf123","sst":2}},
"regReq":{"Type":2,"ServiceName":4,"Versions":{"vi"},"ProfileName":"UPI","FailureProfile":"FI","SvcMgtType":3,"Filter":{"BitrateFields":2,"Dm":"intershat"}}
    2020/03/03 05:31:39.346 [DEBUG] [nrfClient.Discovery.nrf] Message send Metadata [Type:UDM
    ServiceName:nudm-uecm
    Method:"Register"
```

```

Payload:"\022\030\n\024imsi-123456789012345\020\005\032o\n\tintershat\030\005"\037cisco.com.apn.epc.mnc456.

mcc123*\n\n003123\022\0034562Sc388ec5-e2ff-4bda-8154-b5dd9f10ad97:\0010B\n\n\006Abf123\020\002\%\010\002\030\004J\002v1b\

    003UP1j\r\010\002\022\tintershat\272\001\003FH1\300\001\003" Versions:"v1" MsgType:33
    ProfileName:"UPI" FailureProfile:"FH1"
    SvcMsgType:UdmUecmRegisterSMF Filter:<Bitmapfields:2 Dnn:"intershat" > ] client
locality [] Preferred locality [], Geo Locality []
    2020/03/03 05:31:39.347 [DEBUG] [nrfClient.generic.Int] GetAvailableSLAINMS returned
timeoutInMS [0]
    2020/03/03 05:31:39.347 [DEBUG] [infra.transaction.core] Requested host Setname: Name:
    http://10.86.73.209:9020/nudm-uecm/v1 Version: ApiRoot:
    2020/03/03 05:31:39.347 [DEBUG] [infra.transaction.core] Exact match found. Selected
remote host is Id 2
    Name: http://10.86.73.209:9020/nudm-uecm/v1 Setname: Host: Port: 0 Url:
http://10.86.73.209:9020/nudm-uecm/v1
    2020/03/03 05:31:39.347 [INFO] [infra.transaction.core] Calling RPC UDM on host
http://10.86.73.209:9020/nudm-uecm/v1 proc-name UDM proc-method: Register
    2020/03/03 05:31:39.348 [DEBUG] [rest_ep.app.n10] Sending registration request to udm:
    /imsi-123456789012345/registrations/
    smf-registrations/5 with payload
{"dnn":"intershat","pduSessionId":5,"pgwFqdn":"cisco.com.apn.epc.mnc456.mcc123",
"plmnId":{"mcc":"123","mnc":"456"},"singleNssai":{"sd":"Abf123","sst":2},"smfInstanceId":"388ec5-e2ff-4bda-8154-b5dd9f10ad97","supportedFeatures":"0"}

    2020/03/03 05:31:39.348 [DEBUG] [infra.rest_client.core] Sending rest message to
http://10.86.73.209:9020/nudm-uecm/v1/imsi-123456789012345/registrations/smf-registrations/5

    2020/03/03 05:31:39.348 [TRACE] [infra.message_log.core] <<<<<<<<
Request
Name: UdmRegistrationRequest
Host:
http://10.86.73.209:9020/nudm-uecm/v1/imsi-123456789012345/registrations/smf-registrations/5
Method: PUT
RequestURI:
--- Headers ---
Content-Type: application/json
Body:{"dnn":"intershat","pduSessionId":5,"pgwFqdn":"cisco.com.apn.epc.mnc456.mcc123",
"plmnId":{"mcc":"123","mnc":"456"},"singleNssai":{"sd":"Abf123","sst":2},"smfInstanceId":"388ec5-e2ff-4bda-8154-b5dd9f10ad97","supportedFeatures":"0"}

    2020/03/03 05:31:39.376 [TRACE] [infra.message_log.core] >>>>>>>
Response
Name:
Response Status 201
--- Headers ---
Location:
http://10.86.73.209:9020/nudm-uecm/v1/imsi-123456789012345/registrations/smf-registrations/5
Content-Length: 225
Content-Type: application/json
Body:{"pgwFqdn": "cisco.com.apn.epc.mnc456.mcc123", "plmnId": {"mcc": "123", "mnc": "456"},
"dnn": "intershat",
"smfInstanceId": "524f5f8a-b584-47b8-86f5-a5292eabcdef", "pduSessionId": 5, "singleNssai":
{"sd": "Abf123", "sst": 2}}
    2020/03/03 05:31:39.377 [INFO] [rest_ep.app.n10] Received registration success response
with status = 201 and body =
{"pgwFqdn": "cisco.com.apn.epc.mnc456.mcc123", "plmnId": {"mcc": "123", "mnc": "456"},
"dnn": "intershat",
"smfInstanceId": "524f5f8a-b584-47b8-86f5-a5292eabcdef", "pduSessionId": 5,
"singleNssai": {"sd": "Abf123", "sst": 2}}
    2020/03/03 05:31:39.377 [DEBUG] [infra.transaction.core] Last stage ( init_done ) ->
Next stage ( finished )
    2020/03/03 05:31:39.378 [TRACE] [infra.message_log.core] <<<<<<<<
IPC message
Name: N10RegistrationSuccess

```

```

MessageType: N10RegistrationSuccess
Key:
--body--
{"regRes":{"dnn":"intershat","pduSessionId":5,"pgwFqdn":"cisco.com.apn.epc.mnc456.mcc123","plmnId":{"mcc":"123","mnc":"456"},

"smfInstanceId":"c388eec5-e2ff-4bda-8154-b5dd9f10ad97","supportedFeatures":"0","singleNssai":{"sd":"Abf123","sst":2}},

"msgRsp":{"Type":2,"Http2_Status":201,"MsgType":34,"ServiceName":4,"SelectedVersion":"v1","SelectedEndPoint":

{"ipv4Address":"10.86.73.209","port":9020,"transport":1},"SelectedProfileName":"UP1","SelectedEndPointName":"EP1",

"SelectedEndPointProfile":"EP1","SelectedLocality":"LOC1","FailureProfile":"FH1","GroupID":"UDM-dnn=intershat;}}

    2020/03/03 05:31:39.378 [DEBUG] [infra.transaction.core] no response message sent for
10
*****
Transaction Log received from Instance: smf.smf-rest-ep.unknown.smf.0
***** TRANSACTION: 00011 *****
TRANSACTION SUCCESS:
    Txn Type           : N10SubscriptionFetchReq(36)
    Priority            : 1
    Session State      : No_Session
LOG MESSAGES:
    2020/03/03 05:31:39.384 [DEBUG] [infra.transaction.core] Processing transaction Id: 11
    Type: 36 SubscriberID: imsi-123456789012345 Keys: []
    2020/03/03 05:31:39.384 [DEBUG] [infra.transaction.core] Trace is disabled
    2020/03/03 05:31:39.384 [TRACE] [infra.message_log.core] >>>>>>
IPC message
Name: N10SubscriptionFetchReq
MessageType: N10SubscriptionFetchReq
Key:
--body--
{"subInfo":{"ueId":"imsi-123456789012345"},"uriParams":{"supportedFeatures":"0","singleNssai":{"sd":"Abf123","sst":2},

"dnn":"intershat","plmnId":{"mcc":"123","mnc":"456"},"msgReq":{"Type":2,"ServiceName":3,"Versions":["v1"],"ProfileName":

"UP1","FailureProfile":"FH1","SvcMsgType":1,"Filter":{"Bitmapfeilds":2,"Dnn":"intershat"}}}

    2020/03/03 05:31:39.384 [DEBUG] [nrfClient.Discovery.nrf] Message send Metadata [Type:UDM
ServiceName:nudm-sdm Method:"Subscription"

Payload:"\022\026\n\024imsi-123456789012345\032&\n\0010\022\n\n\006Abf123\020\002\032\tintershat\n\n\n\003123\022\003456

    \%010\002\030\003J\002v1b\003UP1j\r\010\002\022\tintershat\272\001\003FH1\300\001\001"
Versions:"v1" MsgType:36
    ProfileName:"UP1" FailureProfile:"FH1" SvcMsgType:UdmSdmGetUESMSSubscriptionData
Filter:<Bitmapfeilds:2 Dnn:"intershat" > ]
    client locality [] Preferred locality [], Geo Locality []
    2020/03/03 05:31:39.385 [DEBUG] [nrfClient.generic.Int] GetAvailableSLAINMS returned
timeoutInMS [0]
    2020/03/03 05:31:39.385 [DEBUG] [infra.transaction.core] Requested host Setname: Name:
http://10.86.73.209:9020/nudm-sdm/v1 Version: ApiRoot:
    2020/03/03 05:31:39.385 [DEBUG] [infra.transaction.core] Exact match found. Selected
remote host is Id 1 Name: http://10.86.73.209:9020/
    nudm-sdm/v1 Setname: Host: Port: 0 Url: http://10.86.73.209:9020/nudm-sdm/v1
    2020/03/03 05:31:39.385 [INFO] [infra.transaction.core] Calling RPC UDM on host
http://10.86.73.209:9020/nudm-sdm/v1 proc-name
    UDM proc-method: Subscription
    2020/03/03 05:31:39.385 [DEBUG] [rest_ep.app.n10] Sending sm subscription request to

```

```

udm: /imsi-123456789012345/sm-data?

dnn=intershat&plmn-id=%7B%22mcc%22%3A%22123%22%2C%22mnc%22%3A%22456%22%7D&single-nssai=%7B%22sd%22%3A%22Abf123%22%2C%22sst%22%3A%22%7D&supported-features=0
2020/03/03 05:31:39.385 [DEBUG] [infra.rest_client.core] Sending rest mesage to
http://10.86.73.209:9020/nudm-sdm/v1/

imsi-123456789012345/sm-data?dnn=intershat&plmn-id=%7B%22mcc%22%3A%22123%22%2C%22mnc%22%3A%22456%22%7D&single-nssai=%7B%22sd%22%3A%22Abf123%22%2C%22sst%22%3A%22%7D&supported-features=0
2020/03/03 05:31:39.385 [TRACE] [infra.message_log.core] <<<<<<<<<
Request
Name: UdmSubscriptionRequest
Host:
http://10.86.73.209:9020/nudm-sdm/v1/imsi-123456789012345/sm-data?dnn=intershat&plmn-id=%7B%22mcc%22%3A%22123%22%2C%22mnc%22%3A%22456%22%7D&single-nssai=%7B%22sd%22%3A%22Abf123%22%2C%22sst%22%3A%22%7D&supported-features=0
Method: GET
RequestURI:
--- Headers ---
Content-Type: application/json
2020/03/03 05:31:39.400 [TRACE] [infra.message_log.core] >>>>>>>
Response
Name:
Response Status 200
--- Headers ---
Content-Length: 812
Content-Type: application/json
Body: [{"sharedDnnConfigurationsIds": "012345", "internalGroupIds": ["1aAbB00866564",
"dhsjdha67673AA"], "singleNssai": {"sd": "Abf123",
"sst": 2}, "dnnConfigurations": {"intershat": {"3gppChargingCharacteristics": "1",
"5gQosProfile": {"5qi": 5, "arp": {"preemptVuln":
"NOT_PREEMPTABLE", "preemptCap": "NOT_PREEMPT", "priorityLevel": 15}, "priorityLevel":
1}, "sscModes": {"allowedSscModes": ["SSC_MODE_1",
"SSC_MODE_2"], "defaultSscMode": "SSC_MODE_1"}, "ladnIndicator": true, "pduSessionTypes":
{"defaultSessionType": "IPV4",
"allowedSessionTypes": ["IPV6", "IPV4V6", "UNSTRUCTURED", "ETHERNET"]}, "staticIpAddress":
[{"ipv4Addr": "1.1.1.1"}, {"ipv6Addr": "::1"}],
"upSecurity": {"upIntegr": "REQUIRED", "upConfid": "PREFERRED"}, "sessionAmbr": {"downlink":
"125 Mbps", "uplink": "100 Mbps"},
"iwkEpsInd": false}}]}
2020/03/03 05:31:39.400 [INFO] [rest_ep.app.n10] Received sm subscription success
response with status = 200 and body =
[{"sharedDnnConfigurationsIds": "012345", "internalGroupIds": ["1aAbB00866564",
"dhsjdha67673AA"], "singleNssai": {"sd":
"Abf123", "sst": 2}, "dnnConfigurations": {"intershat": {"3gppChargingCharacteristics":
"1", "5gQosProfile": {"5qi": 5, "arp":
{"preemptVuln": "NOT_PREEMPTABLE", "preemptCap": "NOT_PREEMPT", "priorityLevel": 15},
"priorityLevel": 1}, "sscModes":
{"allowedSscModes": ["SSC_MODE_1", "SSC_MODE_2"], "defaultSscMode": "SSC_MODE_1"},
"ladnIndicator": true, "pduSessionTypes":
{"defaultSessionType": "IPV4", "allowedSessionTypes": ["IPV6", "IPV4V6", "UNSTRUCTURED",
"ETHERNET"]}, "staticIpAddress":
[{"ipv4Addr": "1.1.1.1"}, {"ipv6Addr": "::1"}], "upSecurity": {"upIntegr": "REQUIRED",
"upConfid": "PREFERRED"}, "sessionAmbr":
{"downlink": "125 Mbps", "uplink": "100 Mbps"}, "iwkEpsInd": false}}]}
2020/03/03 05:31:39.401 [INFO] [rest_ep.app.n10] Unmarshalled smData:
smData:<dnnConfiguration:<key:"intershat" value:
< 3gppChargingCharacteristics:"1" ladnIndicator:true
pduSessionTypes:<allowedSessionTypes:IPV6 allowedSessionTypes:IPV4V6
allowedSessionTypes:UNSTRUCTURED allowedSessionTypes:ETHERNET defaultSessionType:IPV4
> sessionAmbr:<downlink:"125 Mbps"
uplink:"100 Mbps" > sscModes:<allowedSscModes:SSC_MODE_1 allowedSscModes:SSC_MODE_2

```

```

defaultSscMode:SSC_MODE_1 >
  upSecurity:<upConfid:PREFERRED > subsQosProfile:<_5qi:5 arp:<preemptCap:NOT_PREEMPT
preemptVuln:NOT_PREEMPTABLE priorityLevel:15 >
  priorityLevel:1 > staticIpAddress:<ipv4Addr:"1.1.1.1" > staticIpAddress:<ipv6Addr:"::1"
> > > singleNssai:<sd:"Abf123" sst:2 >
  internalGroupIds:"1aAbB00866564" internalGroupIds:"dhsjdha67673AA"
sharedDnnConfigurationsIds:"012345" >
  2020/03/03 05:31:39.402 [DEBUG] [infra.transaction.core] Last stage ( init_done ) ->
Next stage ( finished )
  2020/03/03 05:31:39.403 [TRACE] [infra.message_log.core] <<<<<<<<<
IPC message
Name: N10SubscriptionFetchSuccess
MessageType: N10SubscriptionFetchSuccess
Key:
--body--
{"subInfo":{"ueId":"imsi-123456789012345"},"uriParams":{"supportedFeatures":"0","singleNssai":{"sd":"Abf123","sst":2},"dnn":"intershat",

"plmnId":{"mcc":"123","mnc":"456"},"srData":[{"dnnConfiguration":{"intershat":{"_3oppChargingCharacteristics":"1","lchIndicator":true,

"pduSessionTypes":{"allowedSessionTypes":[2,3,4,5],"defaultSessionType":1},"sessionAmbr":{"downlink":"125
Mbps","uplink":"100 Mbps"}},

"ssModes":{"allowedSsdModes":[1,2],"defaultSsdMode":1},"upSecurity":{"upConfid":2},"subsQosProfile":{"_5qi":5,"arp":{"preemptCap":1,

"preemptVuln":1,"priorityLevel":15},"priorityLevel":1},"staticIpAddress":{"ipv4Addr":"1.1.1.1"},"ipv6Addr":"::1"}},"singleNssai":

{"sd":"Abf123","sst":2},"internalGroupIds":["1aAbB00866564","dhsjdha67673AA"],"sharedDnnConfigurationsIds":"012345"}],"msgRsp":

{"Type":2,"Http2_Status":200,"MsgType":37,"ServiceName":3,"SelectedVersion":"v1","SelectedEndPoint":{"ipv4Address":"10.86.73.209",

"port":9020,"transport":1},"SelectedProfileName":"UE1","SelectedEndPointName":"EP1","SelectedEndPointProfile":"EP1","SelectedLocality":

"LOC1","FailureProfile":"FH1","GroupID":"UDM-dnn=intershat;"}
  2020/03/03 05:31:39.403 [DEBUG] [infra.transaction.core] no response message sent for
11
*****
*
```

# RPC Remote Host Management

## Feature Description

The SMF supports the Monitor Subscriber and Monitor Protocol on the Kubernetes environment. This feature allows to capture messages of subscribers and protocols.

## RPC Remote Host Management OAM Support

This section provides information regarding show commands available to monitor and troubleshoot the SMF RPC Remote Host Management.

## show-rpc

This command lists all the RPCs from all the pods with RPC and remote host information.

POD

- POD INSTANCE - Displays the Instance info of the POD
- NAME - Displays the Name of the RPC registered in POD
- REMOTE ADDRESS - Displays IP address and Port of remote endpoint
- REMOTE HOST - Displays name of the RPC host
- TYPE - Displays the type of connection like Rest, Grpc, GrpcStream etc
- SET NAME- Displays the RPC set name for group of RPC hosts
- STATUS - Displays the current state of the RPC host, possible status values are Started, Starting and Stopped
- CONNECTED TIME - Displays the time when the RPC host was connected
- DISCONNECTED TIME - Displays the time when the RPC host was disconnected
- MONITOR RPC HOST - Indicates whether the RPC host is being monitored for connection status
- PROCESSING INSTANCE INFO - Indicates the if the processing instance name if available
- VERSION - Displays the version of the RPC host API if available







## CHAPTER 27

# Multiple and Virtual DNN Support

- [Feature Summary and Revision History, on page 395](#)
- [Feature Description, on page 396](#)
- [How It Works, on page 397](#)
- [Configuring the Virtual DNN Feature, on page 398](#)
- [DNN Profile Offline Mode Support, on page 401](#)
- [Dynamic Configuration Change Support, on page 404](#)
- [IP Pool Allocation per DNN, on page 406](#)

## Feature Summary and Revision History

### Summary Data

*Table 129: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

## Revision History

*Table 130: Revision History*

Revision Details	Release
The limit for the following configurations in SMF is increased from 512 to 2048: <ul style="list-style-type: none"> <li>• Precedence</li> <li>• Operator policy</li> <li>• DNN policy</li> <li>• DNN profile</li> </ul>	2021.01.0
SMF supports case insensitive DNN configuration.	2020.02.5.t1
First introduced.	Pre-2020.02.0

## Feature Description

The multi-DNN support enables the SMF to have multiple PDN connections for end users to provide different services including Internet and VoNR services.

The SMF fetches the locally configured profile-based DNN in PDU Session Establishment Request from the AMF. Then, the SMF maintains the PDN connections based on using SUPI and PDU Session ID. The SMF includes the received DNN in all SBI interfaces to authorize the end user to fetch subscription information, policy, and charging related information. The SMF provisions the forward path information to the UPF. The SMF integrates the multi-DNN support with the IP Address Management (IPAM) module to allocate address to the end-user based on received DNN. The SMF maps the DNN-profile that is derived from subscriber policies. The SMF also fetches DNN and IPv4 and IPv6 path information based on IPAM pool configuration and updates the UPF as part of node association interactions.



**Note** Multiple DNN is supported only for 5GS procedures and is not qualified for EPS Session using SBI interfaces.

The SMF supports virtual DNN mapping based on a subscriber profile. It supports mapping of a UE-requested DNN to a configured DNN and sends the selected DNN profile towards the configured network interfaces.

### DNN Case Insensitive Support

The DNN configuration in SMF is case insensitive. The configuration accepts a string from 1 through 62 alphanumeric characters, that is case insensitive. It can also contain dots (.) and/or dashes (-).

This enhancement is extended to support all DNN configurations and validations.

### IPv6 Interface ID Generation

In releases prior to 2021.01, the SMF generated the IPv6 interface ID in EUI-64 format based on configured or default virtual-mac under DNN. The interface ID is common for all subscribers under DNN. This operation resulted in apps like Google Duo to reject connections due to security policy.

In release 2021.01 and later, the SMF generates unique 64-bit interface ID which is non-EUI-64 format by using SBI VIP address and CommonId of the subscriber.

That is, IPv6 interface ID = VIP-IP (4 bytes) + CommonId (4 bytes)

By default, **virtual-mac** CLI command is now disabled under DNN configuration.

**Table 131: Interface ID for Different Messages**

Call Model	PDU Session Establishment Accept	Create Session Response
5G	N11-SBI-VIP+CommonID	Not Applicable
4G	Not Applicable	GTP-VIP+CommonID
WiFi	Not Applicable	GTP-VIP+CommonID
5G->4G	Not Applicable	Not Applicable (N26 HO - there are NAS contents during handover)
4G->5G	Not Applicable (N26 HO - there are NAS contents during handover)	Not Applicable
4G->WiFi	Not Applicable	GTP-VIP+CommonID (Same as 4G)
WiFi->4G	Not Applicable	GTP-VIP+CommonID (Same as 4G)
5G->WiFi	Not Applicable	N11-SBI-VIP+CommonID (Same as 5G)
WiFi->5G	GTP-VIP+CommonID (Same as WiFi)	Not Applicable

## How It Works

The DNN profile lookup is based on subscriber policy or DNN policy. They are associated in the SMF profile configuration. The subscriber policy has a higher precedence over the DNN policy when both the configurations are present.

The subscriber policy consists of a list of precedence values, and the selection of the precedence is based on the subscriber's SUPI, GPSI, Serving PLMN, and NSSAI value. Each precedence has an associated operator policy and the DNN policy is picked from the selected operator-policy.

The DNN policy can have a DNN profile configuration for each UE-requested DNN. The DNN profile has a Virtual or Mapped DNN with its list of interfaces.

The order of selection for a Virtual DNN is as follows:

- Based on subscriber policy, the order of selection is as follows: smf-profile > smf-service > subscriber-policy > precedence > operator-policy > dnn-policy > dnn-profile (based on UE requested DNN) > Virtual DNN mapping.
- Based on the DNN policy, the order of selection is as follows: smf-profile > dnn-policy > dnn-profile (based on UE requested DNN) > Virtual DNN mapping.

PCF, CHF, UDM, UPF, and RMGR are the supported interfaces for Virtual DNN mapping.

If the Virtual DNN mapping is not configured, the UE-requested DNN is used across all the interfaces.

## Limitations

The SMF includes first-configured DNN profile in "dnnSmfInfoList" of NFProfile during registration with NRF.

## Configuring the Virtual DNN Feature

This section describes how to configure the Virtual DNN feature.

Configuring the Virtual DNN feature involves the following steps:

1. [Configuring Subscriber Policy, on page 398](#)
2. [Configuring Operator Policy and Associating a DNN Policy, on page 399](#)
3. [Configuring a DNN Policy, on page 399](#)
4. [Configuring a Virtual DNN under a DNN Profile, on page 400](#)
5. [Associating Subscriber Policy under the SMF Service, on page 400](#)

## Configuring Subscriber Policy

Use the following configuration to configure the subscriber policy:

```
configure
  policy subscriber policy_name
    precedence precedence_value operator-policy policy_name
  end
```

### NOTES:

- **precedence** *precedence\_value*: Specifies the precedence value associated with the subscriber policy.  
In releases prior to 2021.01.0: The maximum limit for precedence is 512.  
In 2021.01.0 and later releases, the limit for precedence is increased from 512 to 2048.
- **operator-policy** *policy\_name*: Specifies the operator policy to be associated with the subscriber policy.  
In releases prior to 2021.01.0: The maximum limit for operator policy is 512.  
In 2021.01.0 and later releases, the limit for operator policy is increased from 512 to 2048.

## show full

The output of this command displays the following information based on the configuration:

- policy subscriber *policy\_name*

## Configuring Operator Policy and Associating a DNN Policy

To configure the operator policy, use the following configuration:

```
configure
  policy operator operator_policy_name
    policy dnn policy_name secondary secondary_dnn_policy_name dnn-list dnn_list
  exit
exit
```

NOTES:

- **policy dnn** *policy\_name*: Specifies the primary DNN policy to be associated with the operator policy.
- **secondary** *secondary\_dnn\_policy\_name*: Specifies the secondary DNN policy.

## Verifying the Configuration

This section describes how to verify the above configuration.

### show full

The output of this command displays the following information based on the configuration:

- policy subscriber *policy\_name*

## Configuring a DNN Policy

To configure the DNN policy, use the following configuration:

```
configure
  policy dnn policy_name
    dnn dnn_name profile profile_name dnn-list dnn_list
  exit
exit
```

NOTES:

- **policy dnn** *policy\_name*: Specifies the DNN policy. *policy\_name* must be an alphanumeric string.  
In releases prior to 2021.01.0: The maximum limit for DNN policy is 512.  
In 2021.01.0 and later releases, the limit for DNN policy is increased from 512 to 2048.
- **dnn** *profile\_name*: Maps the specified Virtual DNN profile with the specified network DNN profile. *profile\_name* must be an alphanumeric string.
- **profile** *profile\_name*: Specifies the network DNN profile. *profile\_name* must be an alphanumeric string.

In releases prior to 2021.01.0: The maximum limit for DNN profile is 512.

In 2021.01.0 and later releases, the limit for DNN profile is increased from 512 to 2048.

- **dnn-list** *dnn\_list*: Specifies the list of DNN supported by the UPF node.

## Verifying the Configuration

This section describes how to verify the above configuration.

### show full

The output of this command displays the following information based on the configuration:

- policy subscriber *policy\_name*

## Configuring a Virtual DNN under a DNN Profile

To configure a virtual DNN under a DNN profile, use the following configuration:

```
configure
  profile dnn profile_name
    dnn profile_name network-function-list [ chf | pcf | upf ]
  profile profile_name
end
```

### NOTES:

- **dnn** *profile\_name*: Specifies the DNN profile name. *profile\_name* must be an alphanumeric string.
- **network-function-list**: Specifies the network functions that the selected DNN profile will be sent. Supported values are **chf**, **pcf**, and **upf**.

## Verifying the Configuration

This section describes how to verify the above configuration.

### show full

The output of this command displays the following information based on the configuration:

- policy subscriber *policy\_name*

## Associating Subscriber Policy under the SMF Service

To associate a subscriber policy under SMF service, use the following configuration:

```
configure
  profile smf smf_profile_name
    service name nsmf-pdu
    subscriber-policy subscriber_policy_name
end
```

**NOTES:**

- **subscriber-policy** *subscriber\_policy\_name*: Specifies the subscriber policy name. *policy\_name* must be an alphanumeric string.

## Verifying the Configuration

This section describes how to verify the above configuration.

**show full**

The output of this command displays the following information based on the configuration:

- policy subscriber *policy\_name*

# DNN Profile Offline Mode Support

## Feature Description

The DNN (Data Network Name) Profile Offline Mode Support feature allows new sessions, or subsequent messages of existing sessions, to use the updated configuration values when the DNN is in offline mode. This feature enables the NF to switch the DNN to offline mode.

**Note**

You must clear the subscriber sessions before putting DNN to offline mode while changing the configuration for which dynamic change is not allowed. New session requests are rejected until the DNN is put back to online mode.

## How it Works

This section describes how the DNN Profile Offline Mode Support feature works for the supported SMF configurations.

## DNN Policy

DNN Policy configuration defines the DNN Profile mapping with the DNN. After the DNN to profile mapping is changed, new subscriber for the same DNN uses the updated DNN Profile. So, there is no impact on existing subscribers.

## DNN Profile

DNN Profile defines the various parameters for a DNN.

The following table describes if the configuration change can be dynamically allowed or if you must set the DNN to an offline mode.

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
DnsServers	Allowed	No impact

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
DnnInfo	Allowed	New values are used after database reload of the session
NetworkElementProfile	Not recommended (See NOTES)	
Timeout	Allowed	No impact
ChargingProfile	Not recommended (See NOTES)	
RemoteVmac	Allowed	No impact
PcscfProfile	Allowed	No impact
PpdProfile	Allowed	Immediate (new values are used)
DefaultSscMode	Allowed	No impact
DefaultPduSession	Allowed	No impact
AllowedPduSession	Allowed	No impact
QosProfile	Allowed	Immediate (new values are used)
UpfApn	Allowed	No impact
SecondaryAuthen	Allowed	No impact
LocalAuthorization	Allowed	No impact

**Note**

- In this release, we do not recommend changing (modify or delete) the NetworkElementProfile and ChargingProfile configuration parameters. If they are changed, the behavior for:
  - NetworkElementProfile: Messages for the existing sessions may be sent on new servers.
  - ChargingProfile: There may be some inconsistency between SMF and UPF related to URRs.
- For modifying the DNN Profile mapping, the DNN Profile must be in the offline mode.
- We recommend that you review the messages shown in the help string before you run the CLI commands.
- You can switch the DNN profile to an offline mode when dynamically configuring the parameters. This step avoids the network impact, which is caused by the configuration changes.

**Limitations**

The following limitations apply when the DNN is in the offline mode:

- The subsequent 5G calls for the offline DNN are rejected with the HTTP Cause - HTTP\_STATUS\_CODE\_503\_SERVICE\_UNAVAILABLE, and 5GSMCause as “Service option temporarily out of order”.
- The subsequent 4G calls for the offline DNN are rejected with the GTP cause “No resources available”.



## Configuring the DNN Profile Offline Mode Support Feature

This section describes how to enable the offline mode for a DNN Profile.

### Configuring the DNN Profile to Offline Mode

Use the following command to configure the DNN Profile to offline mode.

```
config
  profile dnn profile_name
    mode offline
  end
```

#### NOTES:

- **config**: Enters the configuration mode.
- **profile dnn *profile\_name***: Specifies the DNN profile.
- **mode**: Specifies the mode of operation. The default value is **online**.
- **offline**: Specifies the mode as offline.

### Verifying the DNN Profile Offline Mode Configuration

This section describes how to verify if the DNN Profile is configured in the offline mode.

The following configuration is a sample output of the **show running-config profile dnn *profile\_name*** command:

```
show running-config profile dnn intershat
profile dnn intershat
mode offline/online [default: online]
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udml
charging-profile chgprf1
virtual-mac          b6:6d:47:47:47:47
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV6 IPV4V6 ]
upf apn intershat
dcnr                  true
exit
```

## DNN Profile Offline Mode OAM Support

This section describes operations, administration, and maintenance information for this feature.

### Statistics

The following label is introduced as part of this feature:

- **LABEL\_DISC\_PDUSETUP\_DNN\_OFFLINE**: This label is defined to indicate that the call is rejected because the DNN is in the offline mode.

# Dynamic Configuration Change Support

## Feature Description

The Dynamic Configuration Change Support feature allows new sessions, or subsequent messages of existing sessions, to use the updated configuration values.

This feature supports the following SMF configurations:

- DNN Policy
- DNN Profile
- Subscriber Policy

## How it Works

This section describes how dynamic change in configuration works for the supported SMF configurations.

### DNN Policy

DNN Policy configuration defines the DNN Profile mapping with the DNN. After the DNN to profile mapping is changed, new subscriber for the same DNN uses the updated DNN Profile. So, there is no impact on existing subscribers.

### DNN Profile

DNN Profile defines the various parameters for a DNN.

The following table describes if the configuration change can be dynamically allowed or if you must set the DNN to an offline mode.

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
DnsServers	Allowed	No impact
DnnInfo	Allowed	New values are used after database reload of the session
NetworkElementProfile	Not recommended (See NOTES)	
Timeout	Allowed	No impact
ChargingProfile	Not recommended (See NOTES)	
RemoteVmac	Allowed	No impact
PcscfProfile	Allowed	No impact
PpdProfile	Allowed	Immediate (new values are used)
DefaultSscMode	Allowed	No impact
DefaultPduSession	Allowed	No impact

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
AllowedPduSession	Allowed	No impact
QosProfile	Allowed	Immediate (new values are used)
UpfApn	Allowed	No impact
SecondaryAuthen	Allowed	No impact
LocalAuthorization	Allowed	No impact

**Note**

- In this release, we do not recommend changing (modify or delete) the NetworkElementProfile and ChargingProfile configuration parameters. If they are changed, the behavior for:
  - NetworkElementProfile: Messages for the existing sessions may be sent on new servers.
  - ChargingProfile: There may be some inconsistency between SMF and UPF related to URRs.
- For modifying the DNN Profile mapping, the DNN Profile must be in the offline mode.
- The SMF may report a warning when the configurations are modified. These modifications may have an impact on the ongoing calls. We recommend that you review the warning messages and take the appropriate action.
- You can switch the DNN profile to an offline mode when dynamically configuring the parameters. This step avoids the network impact, which is caused by the configuration changes.

**Subscriber Policy**

Subscriber Policy is used for selecting operator policy based on SUPI range, slice information, and so on. Change in Subscriber Policy configuration can be applied dynamically as it has no impact on existing sessions. Operator policy for the new sessions are selected based on the updated configurations.

**Limitations**

The following limitations apply when the DNN is in the offline mode:

- The subsequent 5G calls for the offline DNN are rejected with the HTTP Cause - HTTP\_STATUS\_CODE\_503\_SERVICE\_UNAVAILABLE, and 5GSMCause as “Service option temporarily out of order”.
- The subsequent 4G calls for the offline DNN are rejected with the GTP cause “No resources available”.

**Configuring Dynamic Configuration Change Support**

This section describes how to enable dynamic configuration for the DNN Profile.

**Configuring the DNN Profile to Offline Mode**

Use the following command to configure the DNN Profile to offline mode.

```

config
  profile dnn profile_name
    mode offline
  end

```

**NOTES:**

- **config**: Enters the configuration mode.
- **profile dnn** *profile\_name*: Specifies the DNN profile.
- **mode**: Specifies the mode of operation.
- **offline**: Specifies the mode as offline.

**Verifying the DNN Profile Offline Mode Configuration**

This section describes how to verify if the DNN profile is configured in the offline mode.

The following configuration is a sample output of the **show running-config profile dnn** *profile\_name* command:

```

show running-config profile dnn intershat
profile dnn intershat
mode offline/online [default: online]
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
charging-profile chgprf1
virtual-mac          b6:6d:47:47:47:47
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV6 IPV4V6 ]
upf apn intershat
dcnr                 true
exit

```

**Dynamic Configuration Change OAM Support**

This section describes operations, administration, and maintenance information for this feature.

**Statistics**

The following label is introduced as part of this feature:

- **LABEL\_DISC\_PDUSETUP\_DNN\_OFFLINE**: This label is defined to indicate that the call is rejected because the DNN is in the offline mode.

**IP Pool Allocation per DNN****Feature Description**

The IP Pool Allocation per DNN feature supports mapping of a UE-requested DNN to a configured DNN for IP Pool selection. This feature is supported for the SMF and PGW-C in 5GC and 4G.

The IP Pool Allocation per DNN feature supports the following functionalities:

- Enables SMF to support the new configuration under the DNN profile to enable mapping of the UE-requested DNN to IP pool DNN.
- Sends the mapped DNN over GRPC to the Resource Manager functionality under Node Manager service for IP allocation.
- Supports the new configuration for IP Pool DNN over the virtual DNN with Redundancy Manager, if present
- Sends the UE-requested DNN when both the new configuration for IP pool and the virtual DNN are not present.

## How it Works

This section provides a brief of how the IP Pool Allocation per DNN feature works.

- The DNN profile lookup is based on the subscriber policy or DNN policy. The DNN profiles are associated in the SMF profile configuration. The subscriber policy takes precedence over the DNN policy when both the configurations are present.
- The subscriber policy contains a list of precedence values. The selection of the precedence is based on the SUPI, GPSI, serving PLMN, and NSSAI value of the subscriber.
- Each precedence has an associated operator policy. The DNN policy is picked from the selected operator policy.
- The DNN policy can have a DNN profile configuration for each of the UE-requested DNN.
- The DNN profile contains the virtual or mapped DNN with its list of interfaces. This is an existing configuration and Redundancy Manager is also in the list of interfaces. For more information, see the “Configuring a Virtual DNN under a DNN Profile” section.
- The new configuration under the DNN profile contains the mapping of the UE-requested DNN to IP Pool DNN.
- The DNN profile selection occurs in the following order:
  - Based on subscriber policy, the order of selection is as follows: smf-profile > smf-service > subscriber-policy > precedence > operator-policy > dnn-policy > dnn-profile (based on UE-requested DNN) > Virtual DNN mapping.
  - Based on the DNN policy, the order of selection is as follows: smf-profile > dnn-policy > dnn-profile (based on UE requested Dnn) > Virtual DNN mapping.

**Note**

- New IP pool DNN mapping takes precedence over the existing virtual DNN configuration if the Redundancy Manager configuration exists.
- If both the configurations for the Redundancy Manager are not present, the UE-requested DNN is used to select the IP pool.
- If the mapped DNN does not have the IP pool configured, then IP allocation fails, and the call is deleted.
- Both the EPS and 5G calls follow the same principles for IP allocation for a DNN.

## Configuring IP Pool Allocation

This section describes how to configure the IP Pool Allocation per DNN feature.

Configuring the IP Pool Allocation per DNN involves either one of the following steps:

1. Configuring virtual DNN under DNN profile. For more information, see the “Configuring a Virtual DNN under a DNN Profile” section.

**Note**

This is a generic configuration along with other interfaces as an option.

2. Allocating the IP pool per DNN.

**Note**

This configuration is specifically only for IP allocation.

## Allocating the IP Pool per DNN

To allocate the IP pool per DNN, use the following commands:

```
configure
  profile dnn pool_name
    dnn rmgr rmgr_name
  end
```

**NOTES:**

- **profile dnn *pool\_name***: Maps the Virtual DNN profile with the specified network DNN profile. *pool\_name* must be the name of the address pool.
- **dnn rmgr *rmgr\_name***: Specifies the Redundancy Manager to which the DNN profile will be sent. *rmgr\_name* must be an alphanumeric string.



## CHAPTER 28

# Multiple PLMN Support

- [Feature Summary and Revision History, on page 409](#)
- [Feature Description, on page 410](#)
- [How it Works, on page 410](#)
- [Configuring Multiple PLMN, on page 410](#)

## Feature Summary and Revision History

### Summary Data

*Table 132: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 133: Revision History*

Revision Details	Release
First introduced.	2021.01.0

## Feature Description

The multi-PLMN feature supports multiple PLMNs for homer and roamer networks. A maximum number of 32 PLMNs can be configured.

The primary PLMN configured under profile DNN is used by SMF for peer discovery. The feature supports homer and roamer networks with different session type configuration. Homer with IPv6 session type configuration and roamer with IPv4 or IPv6 session type is a typical configuration.

The feature supports emergency calls from 4G and 5G RATs from roamer UEs with SIM (unauthenticated IMSI) and without SIM. For emergency calls without IMSI, if primary-PLMN is not configured (no PLMN ID and no primary PLMN under profile DNN), then one of the PLMNs in the PLMN list is used as primary PLMN for external messaging.

SMF validates UE PLMN on getting SmContextCreate or CreateSessionRequest message and populates the PLMN in external messaging.

## How it Works

The operator PLMNs configured under PLMN list includes all UE PLMNs and serving PLMNs.

On receiving the Create Request from 4G or 5G RAT (SmContextCreate or Create Session Request), the SMF extracts UE PLMN from SUPI. SMF compares the UE PLMN and serving PLMN with the configured PLMN list and populates the PLMN in external messaging.

## Configuring Multiple PLMN

This section describes how to configure the multi-PLMN feature.

## Configuring Peer Network Function

This section describes how to configure the use of NRF discovery or local configuration for selecting peer network function.

The configuration under profile network-element allows the user to have different selection logic linked to subscriber policy. For example, the user can configure peer NF logic for homers, roamers or visitors.

```

config
  profile network-element amf amf_profile_name
    skip-nf-discovery
    exit
  exit

```

### NOTES:

- **skip-nf-discovery**: Skips network function discovery.



## Configuring PLMN ID

This section describes how to configure the PLMN ID.

```
config
  profile smf smf_profile_name
    plmn-id mcc mcc_value mnc mnc_value
  exit
```

### NOTES:

- **plmn-id**: Specifies the PLMN ID.
- **mcc *mcc\_value***: Specifies the mobile country code.
- **mnc *mnc\_value***: Specifies the mobile network code.

## Configuring PLMN List

This section describes how to configure the PLMN list.

```
config
  profile smf smf_profile_name
    plmn-list mcc mcc_value mnc mnc_value
  exit
```

### NOTES:

- **plmn-list**: Specifies the PLMN list.
- **mcc *mcc\_value***: Specifies the mobile country code.
- **mnc *mnc\_value***: Specifies the mobile network code.
- A maximum number of 32 PLMNs can be configured.
- All operator PLMNs are configured under PLMN list including all UE-PLMNs and serving PLMNs.

## Configuring Primary PLMN

This section describes how to configure the primary PLMN under DNN profile.

This configuration provides an option to configure the primary PLMN used by SMF, to discover if query parameters are configured appropriately.

```
config
  profile dnn intershat
    primary-plmn mcc mcc_value mnc mnc_value
  exit
```

### NOTES:

- **primary-plmn**: Configures the primary PLMN.
- **mcc *mcc\_value***: Specifies the mobile country code.
- **mnc *mnc\_value***: Specifies the mobile network code.

## Configuring PLMN in NRF Discovery

This section describes how to configure the PLMN in NRF Discovery.

```
config
  profile network-element pcf pcf_profile_name
    query-params target-plmn [ ue-plmn | serving-plmn | primary-plmn ]
  exit
```

### NOTES:

- **ue-plmn**: The UE PLMN is sent in target PLMN if configured.
- **serving-plmn**: The serving PLMN is sent in target PLMN if configured.
- **primary-plmn**: The primary PLMN is sent in target PLMN if configured.

## Configuring Serving PLMN MNC list

This section describes how to configure the MNC list for serving PLMN.

```
config
  policy subscriber policy_name
    precedence precedence_value
    serving-plmn mcc mcc_value mnc-list mnc_list_values
  exit
```

### NOTES:

- **mnc-list**: Configures the list of MNC values. For example: [580 660]
- This configuration is backward compatible. If both **mnc** and **mnc-list** are configured, both are considered while selecting the operator policy.

## Configuring Roamer in Operator Policy

This section describes how to configure the roamer network in Operator Policy.

```
config
  policy operator policy_name
    roamer [ visitor-lbo | visitor-hrt | roamer ]
  exit
```

### NOTES:

- **roamer**: Specifies the roamer network.
- **visitor-lbo**: Specifies the visitor-lbo session.
- **visitor-hrt**: Specifies the visitor-hrt session.
- Visitors can be either visitor-lbo or visitor-hrt. The 5G visitor sessions are marked as visitor-lbo or visitor-hrt based on whether hsmfUri is received in SmContextCreate.
- The roamer configuration under operator policy can be used to override the roamer status derived based on hsmfUri.



## CHAPTER 29

# Network-initiated Messages Support

- [Feature Summary and Revision History, on page 413](#)
- [Feature Description, on page 413](#)
- [How it Works, on page 414](#)
- [OAM Support, on page 421](#)

## Feature Summary and Revision History

### Summary Data

*Table 134: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 135: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

Connection Management (CM) includes the functions to establish and release a NAS signaling connection between a UE and the Access and Mobility Management Function (AMF) over the N1 interface. This signaling connection enables the NAS signaling exchange between the UE and the core network.

The 5GS CM states determine the NAS signaling connection of the UE with the AMF. The following are the CM states:

- **CM-Idle**—When a UE is in the CM-Idle state, the UE has no NAS signaling connection established with the AMF over the N1 interface. The AN signaling connection, N2 connection, and N3 connection do not exist in this state.
- **CM-Connected**—When a UE is in the CM-Connected state, the UE has a NAS signaling connection with the AMF over the N1 interface. A NAS signaling connection uses an RRC Connection between the UE and the NG-RAN and an NGAP UE association between the AN and the AMF for the 3GPP access.

The CM states for the 3GPP access and the non-3GPP access are independent of each other. It implies that both the access can be in the CM-Idle state and the CM-Connected state simultaneously.

SMF supports network-initiated messages when a UE is either in the CM-Idle state or in the CM-Connected state.

## How it Works

When connected to the 5G core, a UE can be in CM-Connected with RRC Inactive state too. This state is between the CM-Idle and CM-Connected states.

The SMF cannot identify the UE CM state when the state is between UE and AMF. The SMF only identifies the user plane connection state. This state and the N1 and N2 transfer message response status control the behavior of SMF for network-initiated messages. These messages are for signaling modification or downlink data-related user plane activation procedures. The details for these procedures are described in the following call flows.

## Call Flows

This section describes the following call flows:

- Downlink Data Notification User Plane Activation Call Flow for UE in CM-Connected State
- Downlink Data Notification User Plane Activation Call Flow for UE in CM-Idle State
- Network-Initiated Modification Call Flow for Active User Plane and UE in CM-Connected State
- Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Idle State
- Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Connected State

### Downlink Data Notification User Plane Activation Call Flow for UE in CM-Connected State

This section describes the downlink data notification User Plane activation call flow when UE is in the CM-Connected state.

Figure 82: Downlink Data Notification User Plane Activation Call Flow for UE in CM-Connected State

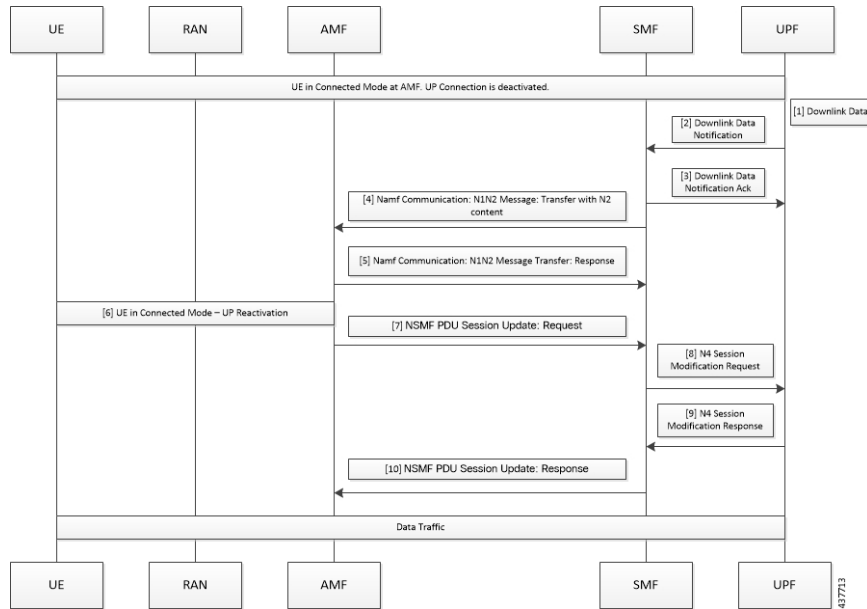


Table 136: Downlink Data Notification User Plane Activation Call Flow Description for UE in CM-Connected State

Step	Description
1	When the UPF receives the downlink data for a PDU session and if no AN tunnel information is saved in the UPF for the PDU session, the UPF buffers the downlink data. The buffering is done based on the instruction from the SMF.
2	The UPF sends data notification towards SMF. This notification includes the N4 session ID, the information to identify the QoS flow for the DL data packet, and the DSCP details.
3	The SMF sends the acknowledgement data notification to the UPF.
4	The SMF initiates the NAMF communication N1 and N2 message transfer towards the AMF. This message transfer includes details, such as PDU session ID, N2 SM information (QFIs, QoS profiles), CN N3 tunnel information, S-NSSAI, ARP, Paging Policy Indicator, 5QI, N1 and N2 transfer failure notification target address, and the PDU session resource setup request IE.
5	As the UE is in CM-Connected state, the AMF initiates N1 and N2 transfer response. This response includes the “200 OK” status code and the “N1_N2_TRANSFER_INITIATED” cause.
6	The User Plane Reactivation procedures begin. The reactivation procedures set up the radio resources and activate the user plane to establish the N3 tunnel.
7	The AMF sends the NSMF PDU Session Update SM Context Request toward SMF. This request contains the SM information of the N2 interface. The connection state of user plane is activated.
8	The SMF sends the N4 modification procedure toward the UPF to activate the session and to update the AN tunnel information, which is the IP and TEID. The session is activated by performing the remove buffer action and the set forward action.
9	The UPF modifies the session and sends the acknowledgement of the modification to the SMF.

Step	Description
10	The SMF responds back to the AMF with “200 OK” status code for NSMF PDU Session Update SM Context Request with the connection state of user plane as activated.

**Note**

The following N1 and N2 response error cases are handled:

- For 404 Context Not Found status, a PDU session is released.
- For 504 or 403 status with the "UE\_IN\_NON\_ALLOWED\_AREA" and "NOT\_REACHABLE" cause, an N4 modification request is sent to drop the buffered packets and to not send the CP notification for the downlink data.
- For the N1 and N2 transfer notification failure, the N4 modification request is sent to drop the buffered packets and to not send the CP notification for downlink data.
- For 409 status code with the Retry After timer value, the N1 and N2 transfer is re-initiated after the timeout value.
- For the 409 status code with "HIGHER\_PRIORITY\_REQUEST\_ONGOING" cause, the lower priority N1 and N2 transfers are not allowed. Only the higher priority transfers are communicated to the AMF.

## Downlink Data Notification User Plane Activation Call Flow for UE in CM-Idle State

This section describes the downlink data notification User Plane activation call flow when UE is in CM-Idle state.

Figure 83: Downlink Data Notification User Plane Activation Call Flow for UE in CM-Idle State

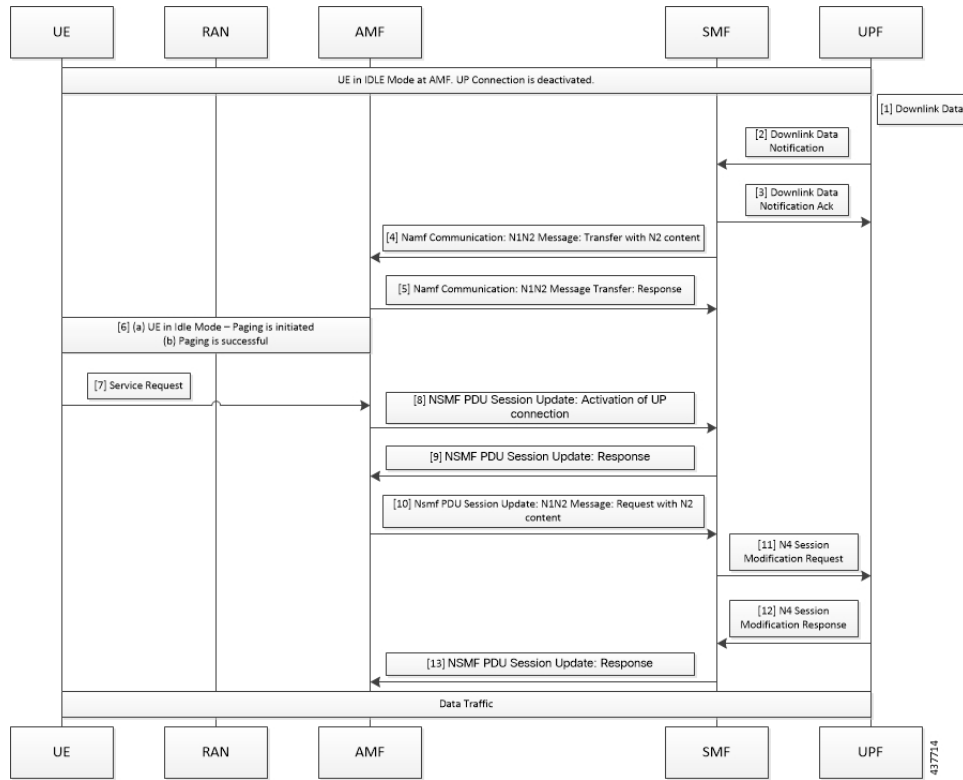


Table 137: Downlink Data Notification User Plane Activation Call Flow Description for UE in CM-Idle State

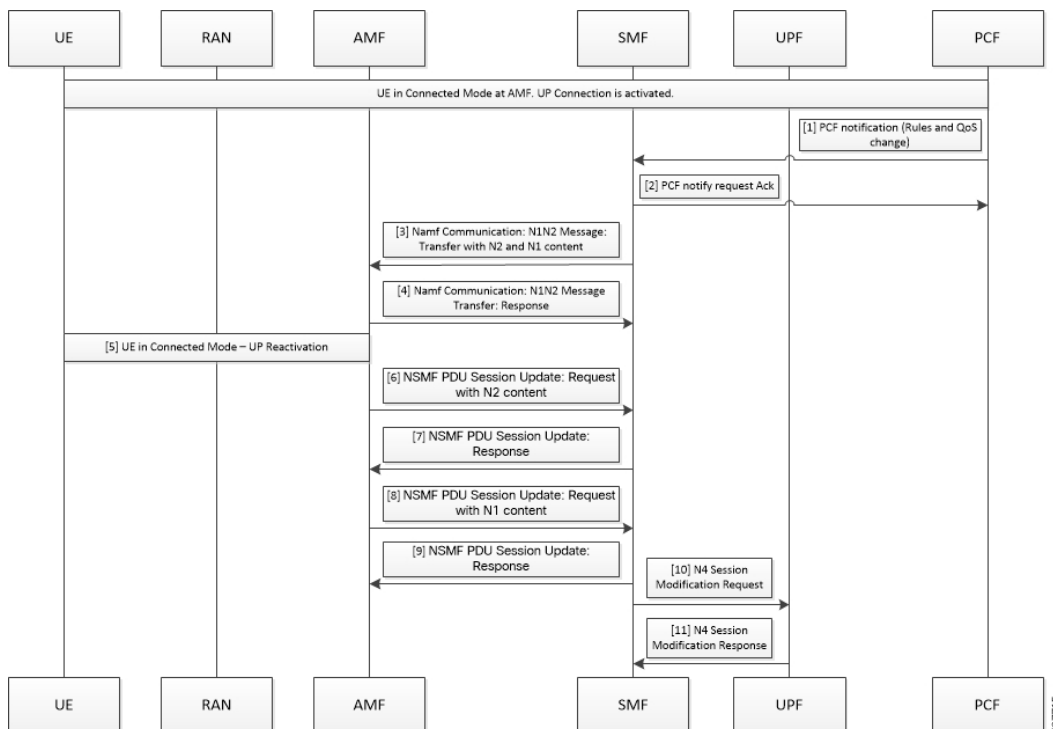
Step	Description
1	When the UPF receives the downlink data for a PDU session and if no AN tunnel information is saved in the UPF for the PDU session, then based on the instruction from the SMF, the UPF buffers the downlink data.
2	The UPF sends data notification towards the SMF. This notification includes the N4 Session ID, the information to identify the QoS flow for the DL data packet, and the DSCP details.
3	The SMF sends the acknowledgement data notification to the UPF.
4	The SMF initiates the NAMF communication N1 and N2 message transfer toward AMF. This message transfer includes details, such as PDU session ID, N2 SM information (QFIs, QoS profiles), CN N3 tunnel information, S-NSSAI, ARP, Paging Policy Indicator, 5QI, and N1 and N2 transfer failure notification target address.
5	As the UE is in CM-Connected state, the AMF initiates N1 and N2 transfer response. This response includes the “202 Accepted” status code and “ATTEMPTING_TO_REACH_UE” cause.
6	The AMF triggers the paging procedure towards the UE.
7	The UE receives the paging request and initiates the requested service to activate the session.
8	The AMF initiates the NSMF PDU Session Update SM Context Request towards SMF with connection state of user plane configured as activating.

Step	Description
9	The SMF responds back to the AMF with “200 OK” status code for the NSMF PDU Session Update SM Context Request. This request includes details, such as N2 SM information (QFIs, QoS profiles), CN N3 tunnel information, S-NSSAI, ARP, Paging Policy Indicator, 5QI, N1 and N2 transfer failure notification target address, and the PDU session resource setup request IE.
10	The AMF sends the NSMF PDU Session Update SM Context Request towards the SMF. This request contains the SM information of the N2 interface. The connection state of user plane is Activating.
11	The SMF initiates the N4 modification procedure towards the UPF to activate the session and to update the AN tunnel information, which is the IP and TEID. The session is activated by performing the remove buffer action and set forward action.
12	The UPF modifies the session and sends the acknowledgement of the modification to the SMF.
13	The SMF responds back to the AMF with “200 OK” status code for NSMF PDU Session Update SM Context Request with connection state of user plane as Activated.

## Network-Initiated Modification Call Flow for Active User Plane and UE in CM-Connected State

This section describes the network-initiated modification call flow when the UE is in CM-Connected State and the User Plane is activated. The network can be PCF, UDM, or SMF.

**Figure 84: Network-Initiated Modification Call Flow for UE in CM-Connected State and Activated User Plane**



437715



**Table 138: Network-Initiated Modification Call Flow Description for UE in CM-Connected State and Activated User Plane**

Step	Description
1	The PCF sends the notification towards SMF with policy decision to apply.
2	The SMF sends an acknowledgement for the policy notification to the PCF.
3	The SMF identifies the changes in QoS model that occur due to policy decision and triggers the NAMF Communication N1 and N2 message transfer toward AMF. This message transfer includes details, such as PDU Session ID, N2 SM information, N1 SM information, and N1 and N2 transfer failure notification target address. N2 includes the PDU session resource modify request transfer IE and N1 includes the PDU session modification request.
4	As UE is in CM-Connected state, the AMF initiates N1 and N2 transfer response. This response includes the “200 OK” status code and “N1_N2_TRANSFER_INITIATED” cause.
5	The user plane modification procedures begin both towards RAN and UE.
6	After receiving a response from RAN, the AMF sends the NSMF PDU Session Update SM Context Request towards the SMF. This request contains the SM information of the N2 interface.
7	The SMF responds back to the AMF with “200 OK” status code for the NSMF PDU Session Update SM Context Request.
8	After receiving a response from the UE, the AMF sends the NSMF PDU Session Update SM Context Request toward SMF. This request contains the SM information of the N1 interface.
9	The SMF responds back to the AMF with “200 OK” status code for NSMF PDU Session Update SM Context Request.
10	Based on the new QoS information, the SMF initiates the N4 Modification procedure towards the UPF to modify the session.
11	The UPF modifies the session and sends the acknowledgement of modification to the SMF.

## Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Connected State

This section describes the network-initiated modification procedure when the UE is in CM-Connected state and the User Plane (UP) context is deactivated.

1. The PCF sends a policy update notification to the SMF for a PDU session with rules and QoS change. The SMF handles the updated policy rules when received in a notification from the PCF.
2. The SMF returns the “200 OK” status code to the PCF.
3. The SMF sends only N1 message PDU Session Modification Command to the UE with the modified rules and QoS change, using the NAMF Communication N1 N2 Message Transfer service operation towards the AMF.
4. The AMF sends the NAMF Communication N1 N2 Message Transfer response to the SMF. This response includes the “200 OK” status code and the “N1N2\_TRANSFER\_INITIATED” cause.
5. The SMF waits for the Nsmf\_PDUSESSION\_UpdateSMContext message from the AMF.
6. After receiving the response from UE, the SMF updates the subscriber’s session in the UPF with the modified parameter values and the UP context state remains as deactivated.

7. The SMF sends N4 Session Modification request to the UPF updating the User Plane tunnel modified rules and the QoS details.
8. The UPF sends the N4 Session Modification response for the PDU session.
9. The SMF activates the UP connection as a result of the trigger to send downlink or uplink data.

## Network-initiated Modification Call Flow for Inactive User Plane and UE in CM-Idle State

This section describes the network-initiated modification procedure when the UE is in CM-Idle state and the User Plane (UP) context is deactivated.

The SMF supports the following use cases during the network-initiated PDU session modification procedure:

- When the UE turns active with the service request for PDN activation
- When the UE turns active with the control service request

### Use case 1: When the UE turns active with the service request for PDN activation

1. The PCF sends a policy update notification to the SMF for a PDU session with rules and QoS change. The SMF handles the updated policy rules when received in a notification from the PCF.
2. The SMF returns the “200 OK” status code to the PCF.
3. The SMF sends only N1 message PDU Session Modification Command to the UE with the modified rules and QoS change, using the NAMF Communication N1 N2 Message Transfer service operation towards the AMF.
4. The AMF sends the NAMF Communication N1 N2 Message Transfer response to the SMF. This response includes the “200 OK” status code and the “ATTEMPTING\_TO\_REACH\_UE” cause.
5. The SMF stops the retransmission of the N1 - PDU Session Modification response message to the UE. Further, it stops the N1 PDU Modification Command retransmission timer and waits for a response from the UE.



#### Note

The N1 PDU Modification Command retransmission timer is configurable. Use the **n1 t3591-pdu-mod-cmd timeout timeout max-retry retry\_count** command in Access Profile Configuration mode to configure the timeout value and maximum attempts for the retransmission of N1 PDU Modification Command. The default timeout value is 2 seconds and the default retry count is 2.

6. The UE receives the paging request from the AMF and initiates the requested service to activate the PDU session. The UE includes the PDU Session ID in PDU Session-to-Activate list only if the UP context needs to be activated.  
The SMF initiates the Idle-to-Active PDU Session transition procedure and suspends the current modification procedure.
7. After the Idle-to-Active procedure is complete, the SMF restarts the modification procedure and sends both the N1 and N2 content in N1 N2 transfer message and waits for both N1 and N2 response from the UE and gNB respectively.
8. The SMF receives the N2 response from gNB, and the N1 response from the UE respectively.

9. The SMF sends N4 Session Modification request to the UPF updating the User Plane tunnel modified rules and the QoS details.
10. The UPF sends the N4 Session Modification response for the PDU session.

#### Use case 2: When the UE turns active with the control service request

1. The PCF sends a policy update notification to the SMF for a PDU session with rules and QoS change. The SMF handles the updated policy rules when received in a notification from the PCF.
2. The SMF returns the “200 OK” status code to the PCF.
3. The SMF sends only N1 message PDU Session Modification Command to the UE with the modified rules and QoS change, using the NAMF Communication N1 N2 Message Transfer service operation towards the AMF.
4. The AMF sends the NAMF Communication N1 N2 Message Transfer response to the SMF. This response includes the “200 OK” status code and the “ATTEMPTING\_TO\_REACH\_UE” cause.
5. The SMF stops the retransmission of the N1 - PDU Session Modification response message to the UE. Further, it stops the N1 PDU Modification Command retransmission timer and waits for a response from the UE.
6. The AMF initiates the paging procedure towards the UE and the UE turns active with the Service Request for control message.
7. The SMF receives the N1 response from the UE.
8. The SMF sends N4 Session Modification request to the UPF updating the User Plane tunnel modified rules and the QoS details. Then, the SMF sets the Forwarding Action Rule (FAR) action for the new rules as ‘drop’.
9. The UPF sends the N4 Session Modification response for the PDU session.

## Limitations

In this release, this feature has the following limitation:

- Temporary rejections due to ongoing handover and registration procedures are not handled.

## Standards Compliance

The network-initiated messages support for UE in CM-Idle or CM-Connected state feature complies with the *3GPP TS 23.502, V15.6.0 (2019-10)*.

## OAM Support

This section describes the operations, administration, and maintenance information for this feature.

## Statistics Support

The SMF maintains the following statistics triggered during the network-initiated modification procedure.

- Total number of attempted network-initiated modifications triggered when the UP context is deactivated.
- Total number of succeeded network-initiated modifications triggered when the UP context is deactivated.
- Total number of failed network-initiated modifications triggered when the UP context is deactivated.
- Total number of "ATTEMPTING\_TO\_REACH\_UE" status received when the network-initiated modification procedure is triggered and the UP context is deactivated.
- Total number of "N1N2\_TRANSFER\_INITIATED" status received when the network-initiated modification procedure is triggered and the UP context is deactivated.



# CHAPTER 30

## Network-Initiated Service Request

- [Feature Summary and Revision History, on page 423](#)
- [Feature Description, on page 423](#)
- [How it Works, on page 424](#)
- [Configuring N3 Tunnel Profile, on page 432](#)

### Feature Summary and Revision History

#### Summary Data

*Table 139: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 140: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

### Feature Description

The N3 tunnel profile helps in defining the forwarding action rules while moving from active to idle transition. The N3 tunnel profile configuration includes:

- Enabling control plane notification (notify)
- Enabling buffering on UPF (buffer UPF)

# How it Works

## Call Flows

### UE-initiated Idle to Active Transition

The following call flow depicts the UE-initiated idle to active transition.

**Figure 85: Idle to Active Transition (UE-Initiated) Call Flow**

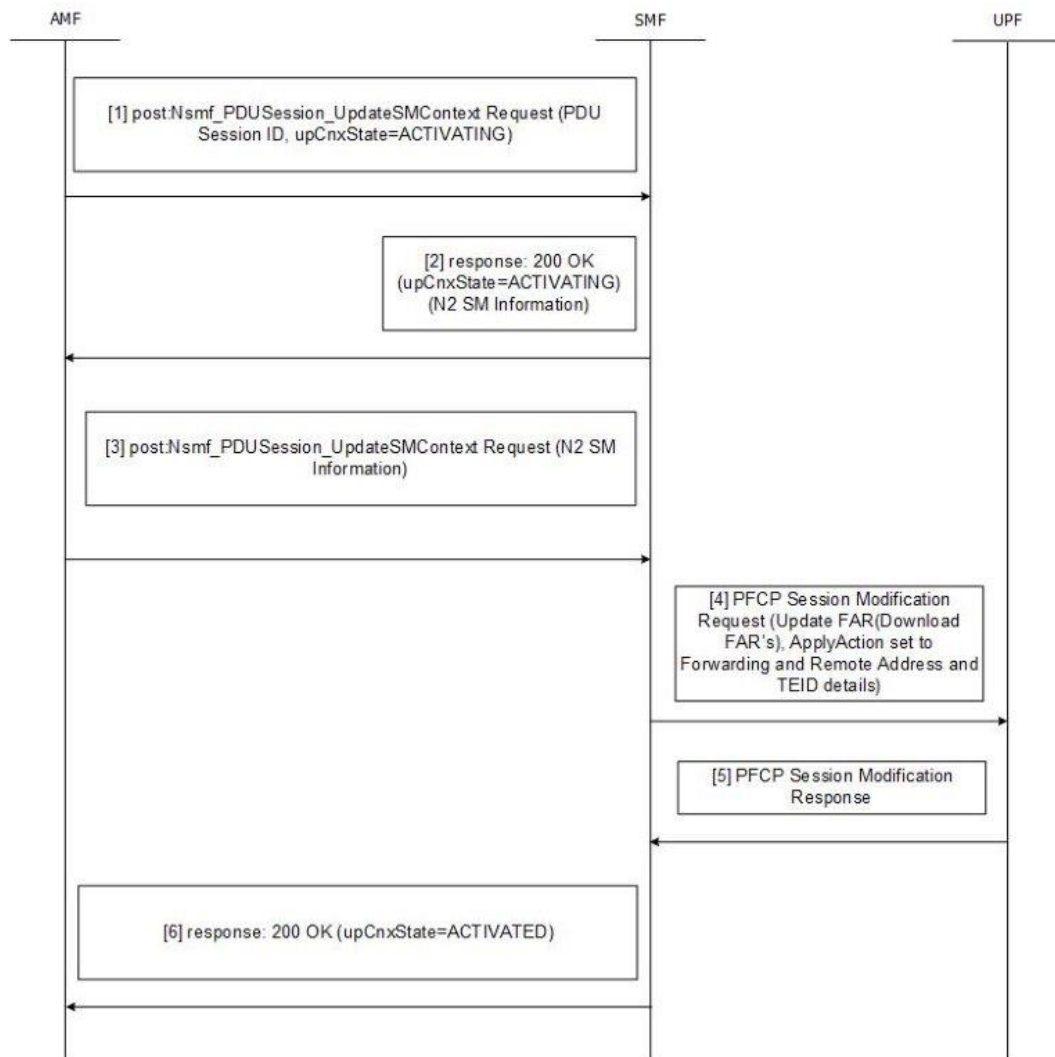


Table 141: Idle to Active Transition (UE-Initiated) Call Flow Description

Step	Description
1	The AMF requests SMF to activate the user plane connection of the PDU session by sending a POST request with the following information: <ul style="list-style-type: none"> <li>• upCnxState attribute set to ACTIVATING.</li> <li>• User location, user location timestamp and access type associated to the PDU session (if modified).</li> <li>• Other information (if necessary).</li> </ul>
2	Upon receipt of the request, the SMF starts activating the N3 tunnel of the PDU session. The SMF returns a 200 OK response with the following information: <ul style="list-style-type: none"> <li>• upCnxState attribute set to ACTIVATING;</li> <li>• N2 SM information to request the 5G-AN to assign resources to the PDU session including the transport layer address and tunnel endpoint of the uplink termination point for the user plane data for the current PDU session (i.e. UPF's GTP-U F-TEID for uplink traffic).</li> </ul>
3	Subsequently, the AMF requests the SMF by sending POST request with the following information: <ul style="list-style-type: none"> <li>• N2 SM information received from the 5G-AN, including the transport layer address and tunnel endpoint of the downlink termination point for the user data for the current PDU session (i.e. 5G-AN's GTP-U F-TEID for downlink traffic), if the 5G-AN succeeded in establishing resources for the PDU sessions.</li> </ul>
4	The SMF initiates PFCP Session Modification Procedure towards UPF with down link FAR updated with the following options: <ul style="list-style-type: none"> <li>• Forwarding Action enabled along with remote node “forwarding parameters” details like the IP address and GTP-U F-TEID.</li> </ul>
5	Upon receipt of successful response from UPF node, the SMF sets the upCnxState attribute to ACTIVATED for the PDU session.
6	SMF then initiates 200 OK response including the upCnxState attribute set to ACTIVATED towards AMF.

## Network-initiated Idle to Active Transition

The following call flow depicts the network-initiated idle to active transition.

Figure 86: Idle to Active Transition (Network-initiated) Call Flow

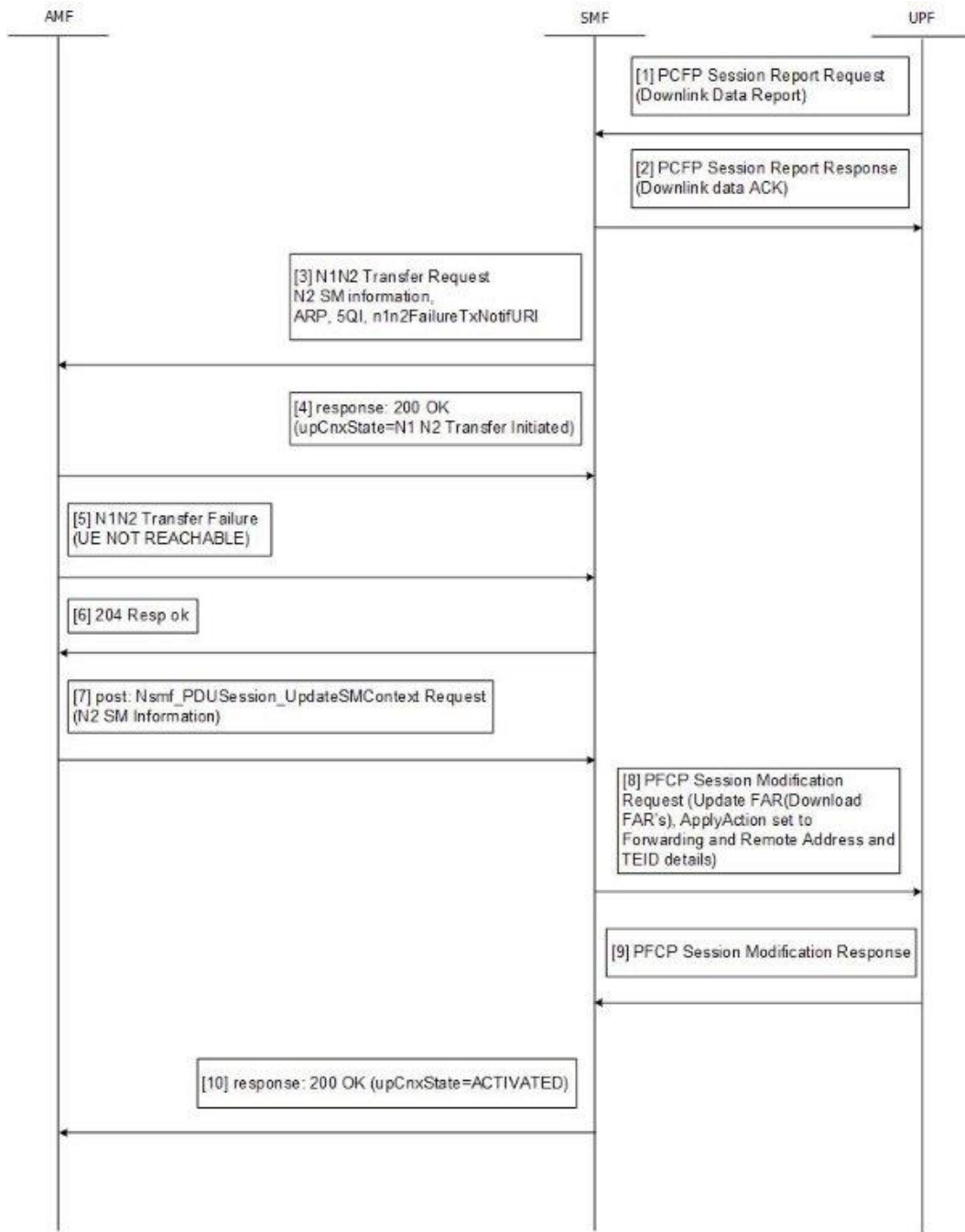




Table 142: Idle to Active Transition (Network-initiated) Call Flow Description

Step	Description
1	The UPF sends "PCFP session report request" to the SMF. <ul style="list-style-type: none"> <li>• Report Type as DLDR (Downlink Data Report).</li> <li>• The "Downlink Data Report" IE contains corresponding "PDR ID".</li> </ul>
2	The SMF sends the PCFP session report response.
3	The SMF sends "N1N2MessageTransfer" to AMF with the following attributes: <ul style="list-style-type: none"> <li>• SUPI, PDU Session ID,</li> <li>• N2SMInformation as "ngapIeType":77 (id-PDUSessionResourceSetupListSUReq), "ngapMessageType":27 (id-PDUSessionResourceSetup).</li> <li>• PDUSessionResourceSetupListSUReq has the PDU session id, QFI, QoS profile, UPF's GTP-U F-TEID for uplink traffic, QFI, QoS profile, S-NSSAI, User Plane Security Enforcement, UE Integrity Protection Maximum Data Rate, and Cause.</li> <li>• Area of validity for N2 SM information, ARP, Paging Policy Indication, 5QI, N1N2TransferFailure Notification Target Address (n1n2FailureTxnNotifURI).</li> </ul>
4	The SMF receives the "N1N2TransferResponse" with the following status codes: <ul style="list-style-type: none"> <li>• 200/202 OK and cause as "N1_N2_TRANSFER_INITIATED" (proceed to Step 6).</li> <li>• 409/504 and Cause "UE_IN_NON_ALLOWED_AREA" (proceed to Step 7).</li> </ul>
5	The AMF sends the N1N2 Transfer failure response. If the UE is not reachable, move to Step 7.
6	Subsequently, the AMF requests the SMF by sending POST request with the following information: <ul style="list-style-type: none"> <li>• N2 SM information received from the 5G-AN, including the transport layer address and tunnel endpoint of the downlink termination point for the user data for the current PDU session (i.e. 5G-AN's GTP-U F-TEID for downlink traffic), if the 5G-AN succeeded in establishing resources for the PDU sessions.</li> </ul>

Step	Description
7	<p>The SMF initiates PFCP Session Modification Procedure towards UPF with down link FAR updated with following options:</p> <ul style="list-style-type: none"> <li>• If N2 Transfer is successful, Forwarding Action is enabled along with remote node “forwarding parameters” details like IP address and GTP-U F-TEID.</li> <li>• If the cause of transfer failure is ATTEMPTING_TO_REACH_UE or UE_IN_NON_ALLOWED_AREA: <ul style="list-style-type: none"> <li>• Update FAR &gt; Apply Action &gt; NOCP: 1</li> <li>• Update FAR &gt; Apply Action &gt; DROP:1</li> <li>• PFCPSMReq-Flags &gt; DROBU:1</li> </ul> </li> <li>• If the cause of transfer failure is UE_NOT_REACHABLE: <ul style="list-style-type: none"> <li>• Update FAR &gt; Apply Action &gt; NOCP: 0</li> <li>• Update FAR &gt; Apply Action &gt; DROP:1</li> <li>• PFCPSMReq-Flags &gt; DROBU:1</li> </ul> </li> </ul>
8	Upon receipt of successful response from UPF node, the SMF sets the upCnxState attribute to ACTIVATED for the PDU session.
9	The SMF then initiates 200 OK response including the upCnxState attribute set to ACTIVATED towards AMF (Only if Step 6 is completed and response is received from Step 8).

## Network Initiated Service Request

During network initiated service request, SMF handles the temporary reject for N1N2 response message from AMF as mentioned in *3GPP TS 23.502, section 4.2.3.3*.

Figure 87: Temporary Reject during Network Triggered Service Request - 1

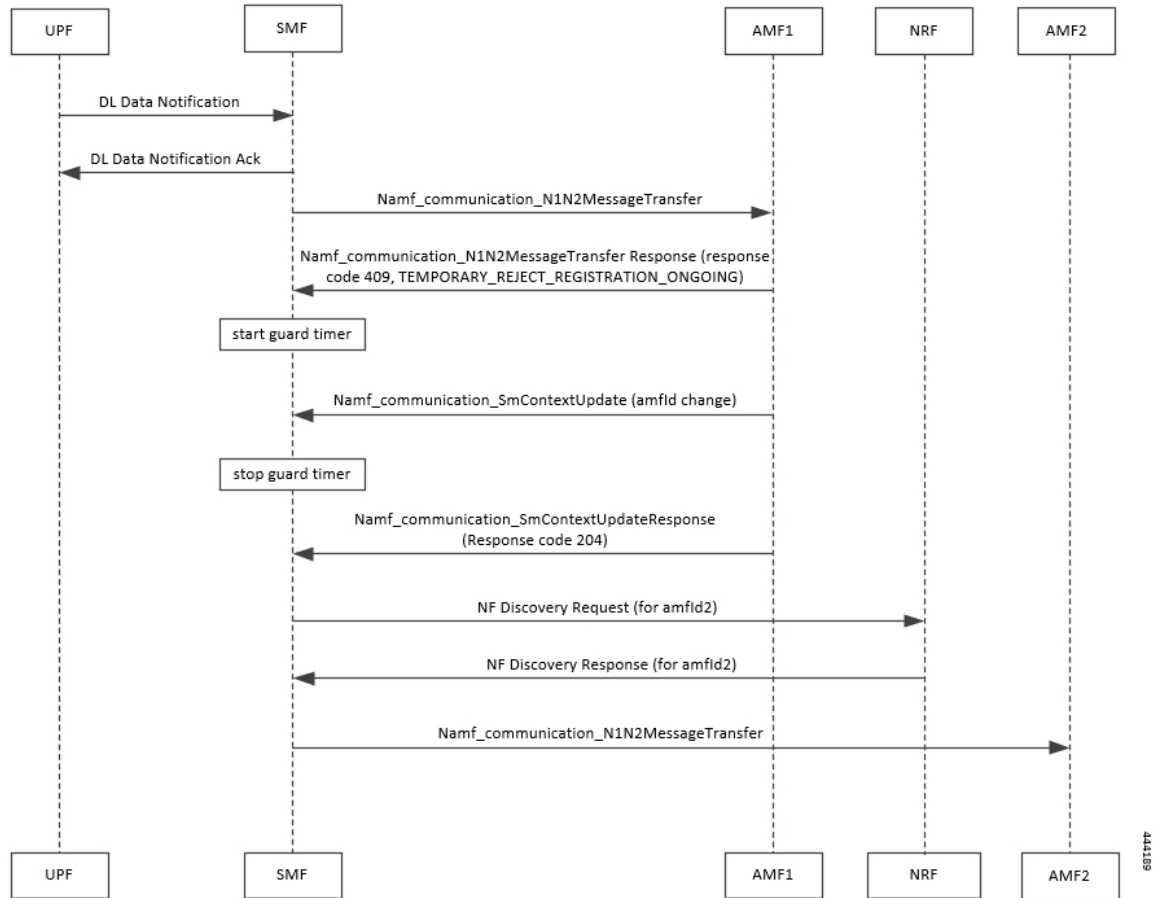


Table 143: Temporary Reject during Network Triggered Service Request - 1

Step	Description
1	On getting a trigger for service request in UP IDLE session state, SMF initiates a N1N2 message towards the AMF as part of Idle mode exit procedure.
2	If UE registration procedure with new AMF is in progress then AMF responds with temporary reject for N1N2 message with response code 409 and cause as: TEMPORARY_REJECT_REGISTRATION_ONGOING OR TEMPORARY_REJECT_HANDOVER_ONGOING SMF
3	On receiving the response, SMF starts a guard timer of 2 seconds that is configured locally.
4	While guard timer is running, SMF expects either a SM Context Update with AMF ID change or SM Context Update for handover.

Step	Description
5	<p>On receiving SM Context Update with AMF ID change, SMF:</p> <ol style="list-style-type: none"><li>1. Stops the guard timer.</li><li>2. Removes the reference to the discovery information for old AMF.</li><li>3. Stores the new UE location information, PLMN information and AMF information.</li><li>4. Send SM Context Update response success without content.</li><li>5. Reinitiates N1N2 message transfer to the new AMF. This involves NF discovery and subsequent transmission to the new AMF.</li></ol>
6	<p>On receiving SM Context Update for N2 handover, SMF:</p> <ol style="list-style-type: none"><li>1. Starts the Handover procedure.</li><li>2. Suspends the Idle mode exit procedure and stops the guard timer.</li><li>3. As part of the Handover procedure completion, old AMF details are removed and new AMF information is stored.</li><li>4. Idle mode exit procedure resumes after Handover procedure is complete.</li><li>5. Reinitiates N1N2 message transfer, if required, to the new AMF. This involves NF discovery and subsequent transmission to new AMF.</li></ol>

Figure 88: Temporary Reject during Network Triggered Service Request - 2

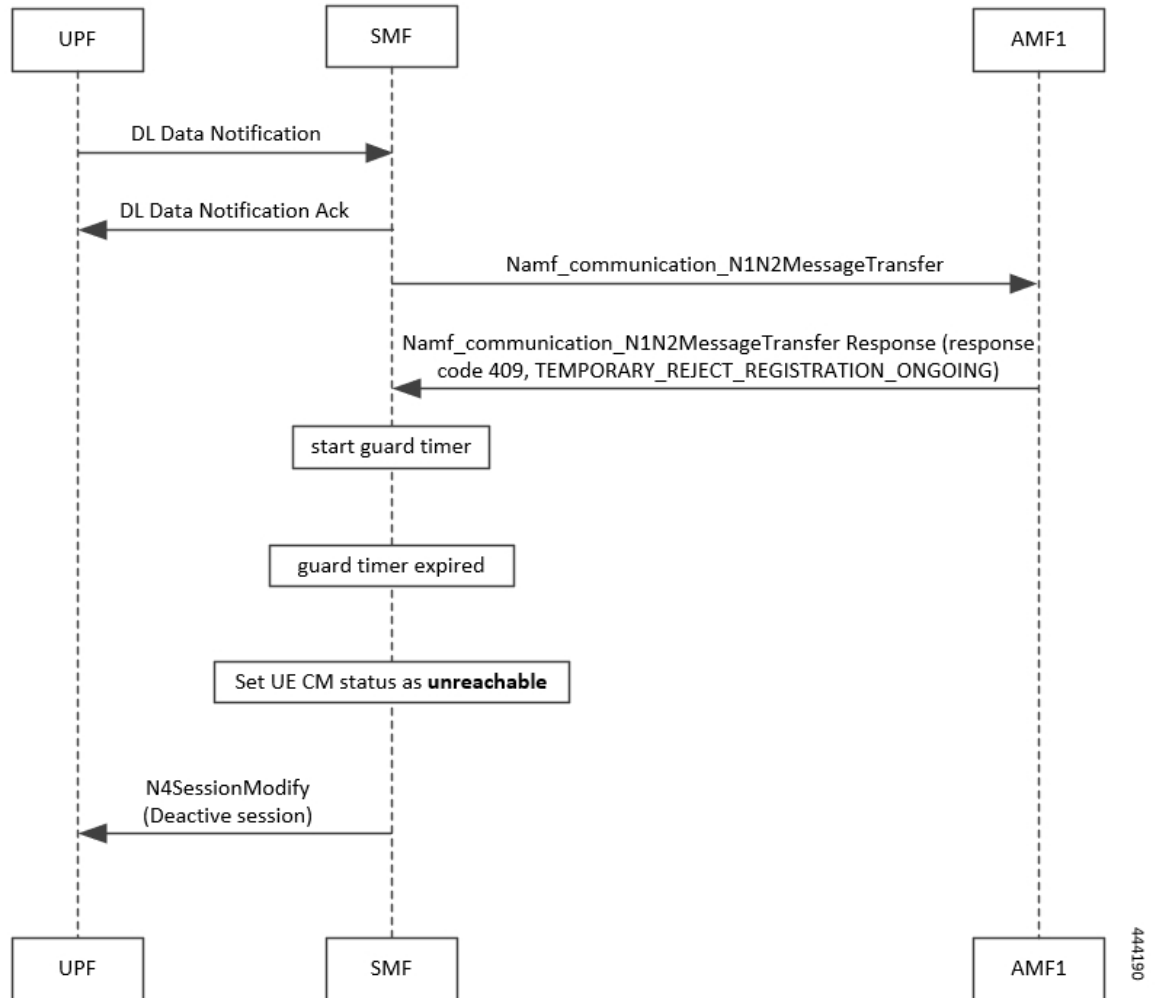


Table 144: Temporary Reject during Network Triggered Service Request - 2

Step	Description
1	On getting a trigger for service request in UP IDLE session state, SMF initiates a N1N2 message towards the AMF as part of Idle mode exit procedure.
2	If UE registration procedure with new AMF is in progress then AMF responds with temporary reject for N1N2 message with response code 409 and cause as: TEMPORARY_REJECT_REGISTRATION_ONGOING OR TEMPORARY_REJECT_HANDOVER_ONGOING SMF
3	On receiving the response, SMF starts a guard timer of 2 seconds that is configured locally.

Step	Description
4	<p>Once guard timer expires, SMF:</p> <ol style="list-style-type: none"> <li>1. Sets the UE CM status as <i>NotReachable</i>.</li> <li>2. Deactivates the UP session state.</li> </ol>

## Limitations

The following are limitations in this release:

- It does not support location update and access-type changes.
- It does not support QoS flow modifications/errors.

## Configuring N3 Tunnel Profile

To configure the N3 tunnel profile, use the following configuration:

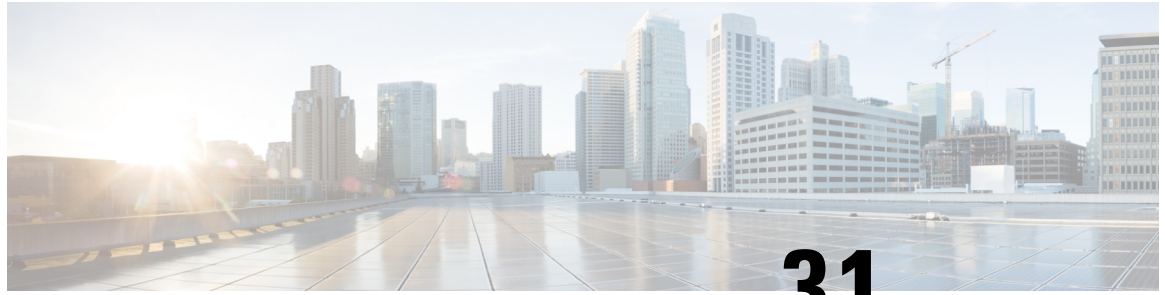
```

config
  n3-tunnel-profile profile_name
    buffer upf
    notify
  end

```

### NOTES:

- **buffer** *upf*: Configures buffering for Downlink Data.
- **notify**: Enables data notification from UPF.



# CHAPTER 31

## NRF Discovery

- [Feature Summary and Revision History, on page 433](#)
- [Feature Description, on page 434](#)
- [NF Heartbeat Support, on page 437](#)
- [Caching Support for NF Discovery, on page 440](#)
- [NRF Support for SMF Subscription and Notification, on page 443](#)
- [NRF Interface per Endpoint, on page 449](#)
- [NRF Failure Handling Support, on page 456](#)
- [Local Configuration for NF Management, on page 461](#)
- [Fallback to Static IP Address Support, on page 469](#)
- [NF Profile Update, on page 476](#)
- [Configuration Support for List of Tracking Areas and Tracking Area Ranges, on page 479](#)
- [Dynamic Configuration Change Support, on page 481](#)
- [NRF Show Command Enhancements , on page 481](#)

## Feature Summary and Revision History

### Summary Data

*Table 145: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

## Revision History

*Table 146: Revision History*

Revision Details	Release
<p>Introduced support for individual NF Profile member changes through NRF notification</p> <p>Included the following new parameters as part of the NRF discovery query:</p> <ul style="list-style-type: none"> <li>• limit</li> <li>• max-payload-size</li> <li>• requester-snssais</li> </ul>	2020.03.0
First introduced.	Pre-2020.02.0

## Feature Description

The 3GPP-defined architecture model for 5G systems provides data connectivity based on techniques such as network function virtualization, software defined networking, and service-based interfaces. Some of the key principles are:

- Separate the User Plane (UP) functions from the Control Plane (CP) functions allowing independent scalability, evolution, and flexible deployments, such as centralized location or distributed (remote) location.
- Support "stateless" NFs where the "compute" resource is decoupled from the "storage" resource.

This feature discovers the set of NF instances (and their associated NF service instances), represented by their NF profile, that are currently registered in Network Repository Function (NRF) and satisfy several input query parameters.

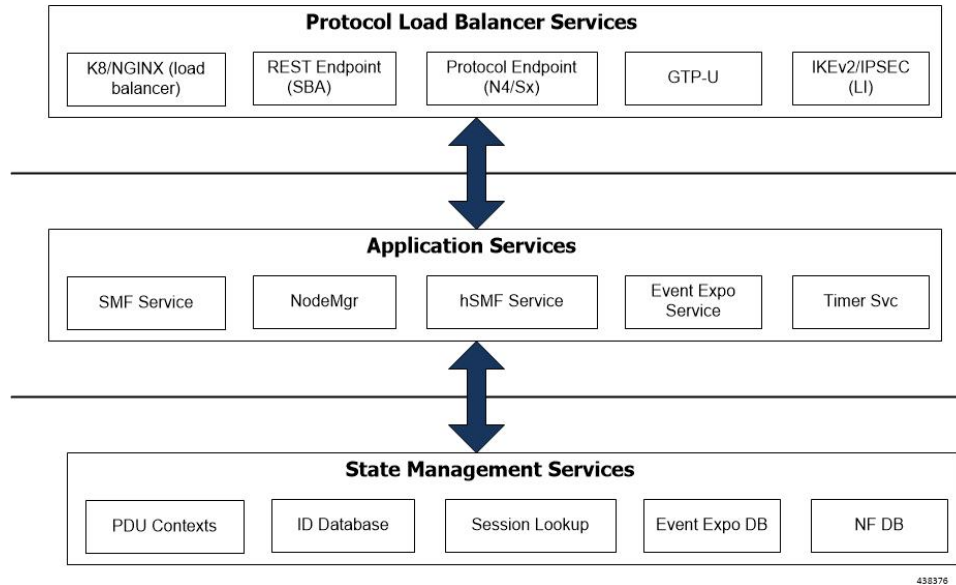
## Architecture

The SMF NF comprises of loosely coupled microservices. Microservice decomposition is based on three-layered architecture philosophies:

1. Layer 1: Protocol and Load Balancer Services (Stateless)
2. Layer 2: Application Services (Stateless)
3. Layer 3: Database Services (Stateful)



Figure 89: SMF 3-layered Micro Services Architecture



## How it Works

The service operation is executed by querying the "nf-instances" resource. The request is sent to an NRF in the same PLMN of the NF service consumer.

## Call Flows

The Service Discovery Request call flow described in 3GPP TS 29.510 v15.2.0 illustrates the NF-level messages for NF discovery.

### Service Discovery Request Call Flow

This section describes the Session Discovery Request call flow.

Figure 90: Service Discovery Request Call Flow

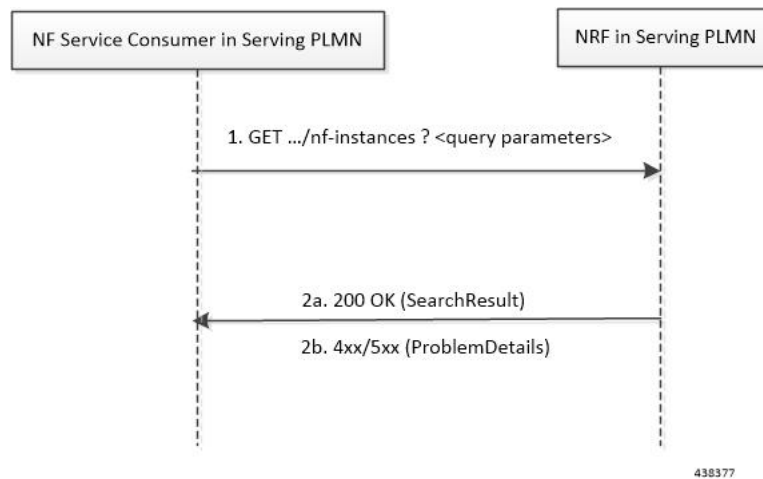


Table 147: Service Discovery Request Call Flow Description

Step	Description
1	The NF Service Consumer sends an HTTP GET request to the resource URI "nf-instances" collection resource. The input filter criteria for the discovery request is included in query parameters.
2a	On success, "200 OK" is returned. The response body contains a validity period, during which the search result can be cached by the NF Service Consumer, and an array of NF profile object that satisfy the search filter criteria (for example, all NF Instances offering a certain NF Service name).
2b	<p>If the NF Service Consumer is not allowed to discover the NF services for the requested NF type provided in the query parameters, the NRF returns "403 Forbidden" response.</p> <p>If the discovery request fails at the NRF due to errors in the input data in the URI query parameters, the NRF returns "400 Bad Request" status code with the "ProblemDetails" IE providing details of the error.</p> <p>If the discovery request fails at the NRF due to NRF internal errors, the NRF returns "500 Internal Server Error" status code with the "ProblemDetails" IE providing details of the error.</p>

The NF profile objects that are returned in a successful result contains generic data of each NF instance, applicable to any NF type, and it can also contain NF-specific data, for those NF instances belonging to a specific type (for example, the attribute "udrInfo" is typically present in the NF profile when the type of the NF instance takes the value "UDR"). In addition, the attribute "customInfo" can be present in the NF profile for NF instances with custom NF types. For NF instances, the "customInfo" attribute is returned by NRF, if available, as part of the NF profiles returned in the discovery response.

SMF service communicates with different NFs, such as UDM, AMF, PCF, CHF and so on, when the session is brought up. The NF discovery is based on set of filters that are associated with the session. The SMF service discovers the NFs, matching the filter criteria for the session, to send messages to NF.

NRF Library (NRF-LIB) provides APIs to discover and send a message to an NF matching a set of filter parameters. The NRF-LIB performs NF discovery for the filter and caches the discovered NFs in a local cache. The following filter parameters are supported:

- Dnn
- Tai
- TargetNfQdn
- TargetPlmnList
- TargetNfInstanceId
- Snssais
- Preferred locality

The discovered NFs are cached with the filter as the key. The endpoint selection for sending the message is based on probabilistic load balancing algorithm (IETF RFC 2782) using the priority and capacity parameters. The NF discovery response carries a validity time, which decides the cache validity period.

NRF-LIB sends the messages to a new target based on the Location header URL in response to initial messages sent to NF.

NRF-LIB supports stickiness wherein the endpoint, service instance, and NF instance details of the selected endpoint for a message that is sent, will be provided to the App/Rest-Ep so that the same can be specified in subsequent message (instead of discovery filter). This helps maintaining stickiness for a session to a selected NF.

## Standards Compliance

The NF Discovery feature complies with the following standards:

- 5G System; Network Function Repository Services; Stage 3 (Release 15):
  - *3GPP TS 29.510 version 15.0.0 (2018-06)*
  - *3GPP TS 29.510 version 15.2.0 (2018-12)*

## Limitations

The following are known limitations of this feature:

- The cache maintained is local to the library. Therefore, in case of deployment with multiple replicas of Rest-Ep, if two Discovery/Send messages with the same discovery filter land on different pods, then the NF discovery will be triggered by both pods.
- Only UDM, PCF, CHF, and AMF discovery and load balancing are supported. UPF discovery is not supported.
- Dynamic configuration changes of NRF endpoints are not supported.

## NF Heartbeat Support

### Feature Description

The NF heartbeat implementation helps the NFs to notify the NRF that the NF is operational. Each NF registered with the NRF contacts the NRF periodically by invoking the NFUpdate service operation. The time interval at which the NRF is contacted is deployment-specific and is returned by the NRF to the NF Service Consumer as a result of a successful registration.

### How it Works

#### Call Flows

##### NF Heartbeat Procedure

The following figure illustrates the NF Heartbeat call flow.

Figure 91: NF Heartbeat Call Flow

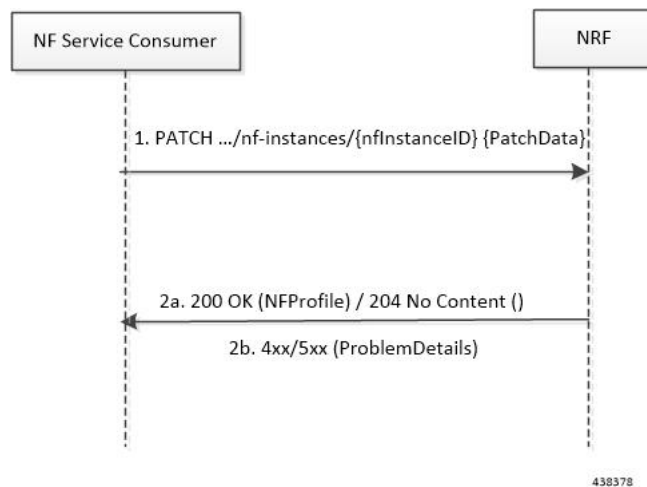


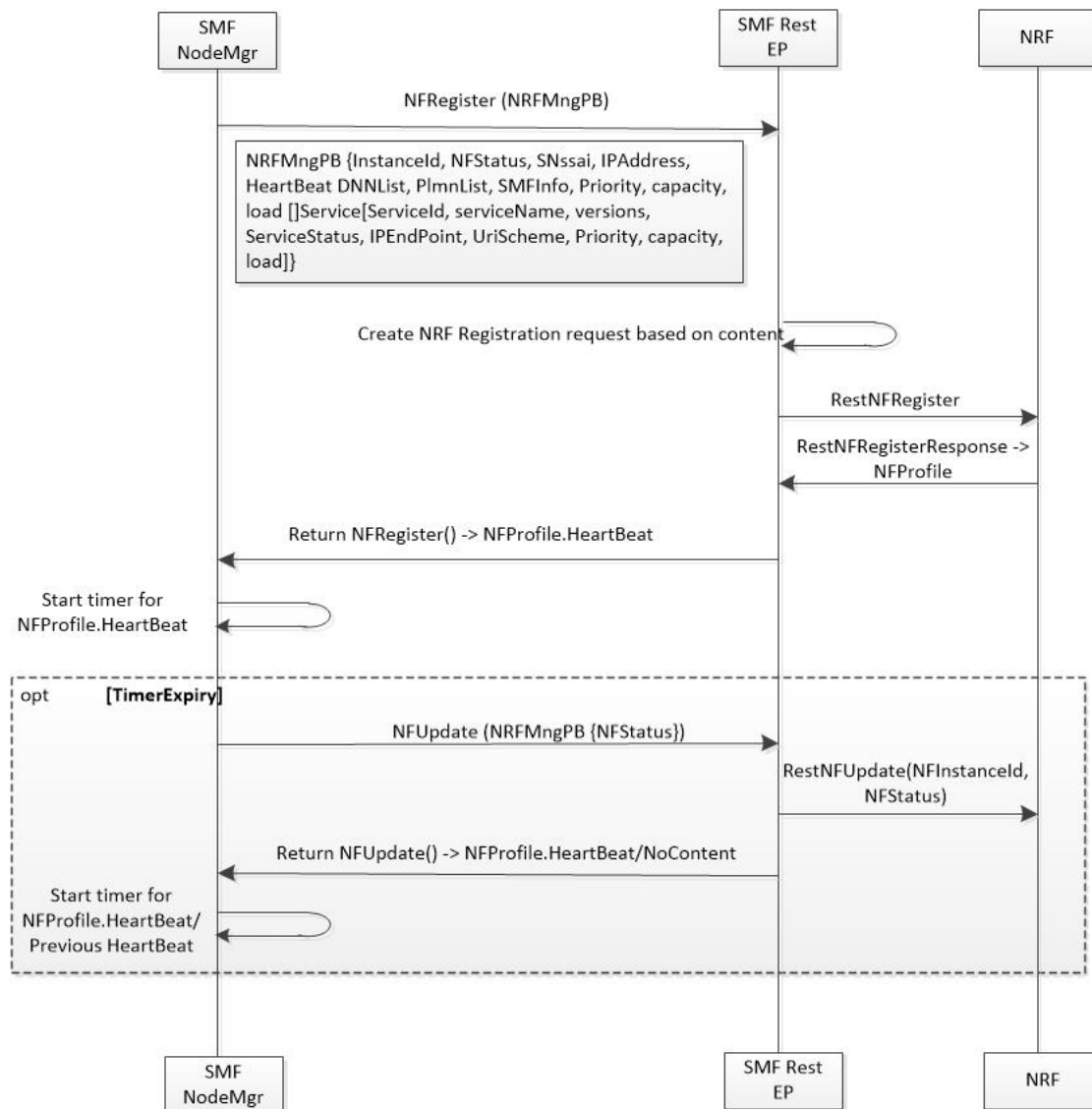
Table 148: NF Heartbeat Call Flow Description

Step	Description
1	The NF Service Consumer sends a PATCH request to the resource URI representing the NF instance. The payload body of the PATCH request contains a replace operation on the nfStatus attribute of the NF Profile of the NF instance, and set it to the value REGISTERED.
2	On success, if the NF Profile changes, the NRF returns "200 OK" along with the full NF Profile data in the response body; otherwise, "204 No Content" is returned.
3	If the NF instance, identified by the "nfInstanceID", is not found in the list of registered NF instances in the NRF's database, the NRF returns "404 Not Found" status code with the ProblemDetails IE providing details of the error. Example: <pre> <b>PATCH .../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64</b> <b>Content-Type: application/json-patch+json</b> [   { "op": "replace", "path": "/nfStatus", "value": "REGISTERED" } ] <b>HTTP/2 204 No Content</b> <b>Content-Location:</b> .../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64 </pre>

## NRF Heartbeat Internal Call Flow

The following figure shows the internal call flow related to the NRF Heartbeat feature.

Figure 92: NRF Heartbeat Internal Call Flow



438382

The SMF NF heartbeat implementation helps in notifying the NRF that the SMF is operational. The default heartbeat frequency is once in 10 seconds. If the NRF returns a different heartbeat frequency, the same is used for the periodic heartbeat. As part of the heartbeat, HTTP PATCH Request to the resource URI representing the NF instance is sent to the NRF. The payload body of the PATCH Request contains a "replace" operation on the "nfStatus" attribute of the NF profile of the NF instance, and sets it to the value "REGISTERED". Other parameters like load and capacity are not supported in this release.

Like NF registration, NF heartbeat is also triggered from the elected master node manager. Also, the heartbeat continues even on the elected node manager restart.

## Standards Compliance

The NF Heartbeat feature complies with 3GPP TS 29.510, Version 15.2.0.

# Caching Support for NF Discovery

## Feature Description

The SMF provides caching support for discovered caching profiles. It uses the NF discovery (nmrf-disc) function to discover profiles such as AMF, UDM, PCF, and CHF. The received discovery response is associated with validity time. SMF caches the discovery response and uses the same response for future NF selections until the cache is valid. This caching support helps in reducing the number of NRF interactions during an ongoing session.

## Relationships

Caching support for NF Discovery has functional relationship with the following features:

- NRF Support for SMF Subscription and Notification
- NRF Interface Per Endpoint

## How it Works

The SMF maintains the cache data in a Cache pod. It uses the cache pod to share the NF discovery cache across multiple instances of SBI pods. The SBI pod periodically updates the cache pod on receiving an NF discovery response. All SBI pods refreshes its cache data periodically with the help of the cache pod.

Currently, the SMF does not invalidate the NF discovery cache entry even on the expiration of the validity time. If a message is sent to a NF that meets a specific criterion, the SMF looks up the cache data for further processing. During a cache look-up:

- On a cache hit without an expired entry, the selected cached NF response is used to send a message for an endpoint selection.
- On a cache hit with an expired entry, SMF sends NF discovery requests to NRF to fetch a new list of NF discovery responses.
- If there is a cache miss, the SMF sends the NF discovery request again to the NRF to retrieve a new list of discovery responses.

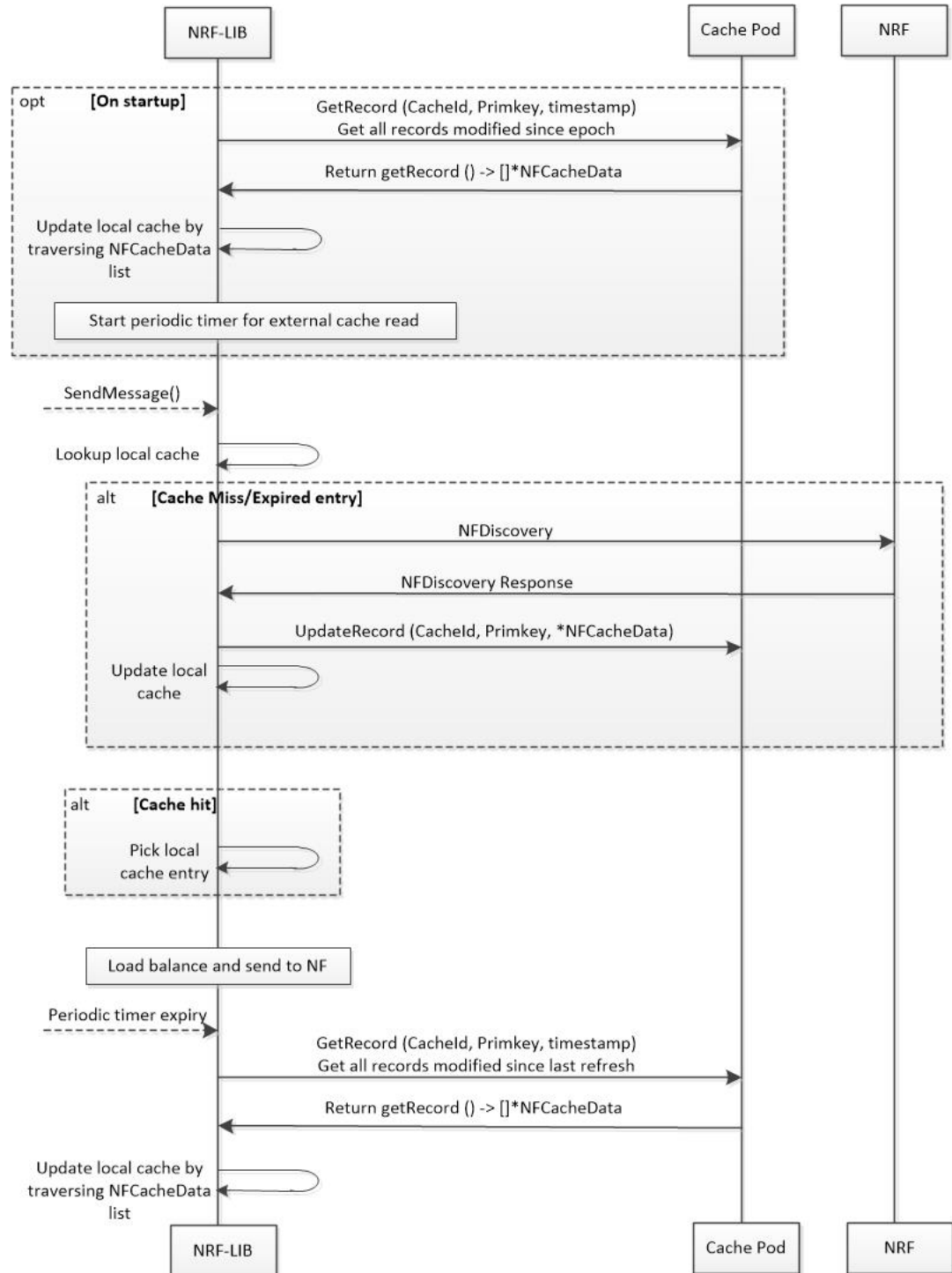
## Call Flows

### Cache Lookup Call Flow

This section describes the Cache Lookup call flow.

NRF-LIB (in smf-rest-ep/SBI) maintains a local cache and updates the external cache (cache-pod). The key for a cache is a combination of nfType and filter (a string that is prepared from multiple filter parameters in "key1=value, key2=value2" format).

Figure 93: Caching Support Call Flow



438379

Table 149: Caching Support Call Flow Description

Step	Description
1	<p>On Startup, NRF-LIB (in smf-rest-ep/SBI):</p> <ol style="list-style-type: none"> <li>1. Retrieves all the cache entries that were modified since epoch from cache-pod so that it can build the local cache. Once the local cache is built, the same cache is used in the sendmessage flow for lookup.</li> <li>2. A periodic refresh routine is initiated to refresh the local cache using the cache-pod.</li> </ol>
2	<p>Periodic Refresh, NRF-LIB (in smf-rest-ep/SBI):</p> <p>Local cache is periodically refreshed by getting all records from the cache-pod that were modified since last refresh. The resultant record list is traversed, and the local cache is updated.</p>
3	<p>Send Message NRF-LIB (in smf-rest-ep/SBI):</p> <ol style="list-style-type: none"> <li>1. When smf-rest-ep (SBI) triggers a send message (say to UDM), NRF-LIB looks up the local cache for the cache entry with the nfType and filter key: <ol style="list-style-type: none"> <li>a. When a cache lookup miss occurs, a discovery query is sent to NRF to fetch NF profiles from NRF. If NRF responds with NF profiles, then these NF profiles are stored in a local cache and updated in cache-pod.</li> <li>b. On a successful lookup, the cached entry is used to send a message for endpoint selection.</li> </ol> </li> <li>2. The NF profiles are load-balanced, and a message is sent to the selected endpoint.</li> </ol>

## Standards Compliance

The Caching Support for NF Discovery feature complies with the following standards:

- 3GPP TS 29.510, V15.2.0
- 3GPP TS 29.510, V15.0.0

## Limitations

The Caching Support for NF Discovery feature has the following limitations:

- This feature only supports UDM, PCF, AMF discovery, and load-balancing.
- It does not support UPF discovery.
- It does not support Dynamic Configuration changes of NRF endpoints.
- It does not support Liveliness check of the NRF endpoints.
- NF Discovery is always attempted on primary host followed by the secondary and then tertiary host.



# NRF Support for SMF Subscription and Notification

## Feature Description

The SMF uses the NRF-provided Subscribe service to subscribe to NF status changes that the NF receives as a discovery response. This helps in updating the cached NF discovery responses.

The SMF honors only the notification changes in load, capacity, status at the NF level, and at the service level. It ignores all other parameter changes in the notification.

After the successful subscription for notification service, the SMF receives notifications of registration and deregistration of NF Instances, or notifications of changes of the NF profile of a given NF Instance.

The SMF supports the "NFProfile" field and "ChangeItem" field in the "NotificationData". If the notification event type is set to "NF\_PROFILE\_CHANGED", the SMF receives notification on either the profile level changes or a list of individual change items for the NFProfile parameters along with the nfInstanceUri.

The "ChangeItem" field includes the following parameters:

- op - Indicates the type of change that happens to the resource.
- path - Contains JSON pointer value which indicates the target location within the resource.
- from - Indicates the path of the JSON element being moved or copied to the location indicated by "path" attribute. It will be present if the "op" attribute is of value "MOVE".
- origValue - Indicates the original value at the target location within the resource specified in the "path" attribute.
- newValue - Indicates a new value at the target location within the resource specified in the "path" attribute.



**Note** The SMF currently supports only the ADD, REPLACE, and REMOVE operations as part of the "op" parameter.

The following is an example of the notification payload sent from the NRF when an NF instance has changed its profile by updating the IP address value and the TCP port for the first NF Service's first endpoint.

Example 1:

```
{
  "event": "NF_PROFILE_CHANGED",
  "nfInstanceUri": ".../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64",
  "profileChanges": [
    {
      "op": "REPLACE",
      "path": "/nfServices/0/ipEndpoints/0/ipAddress", ==> Change ipAddress to ipv4Address

      "newValue": "10.10.10.0"
    },
    {
      "op": "REPLACE",
      "path": "/nfServices/0/ipEndpoints/0/port",
      "newValue": 8080
    }
  ]
}
```

```
    }
  ]

```

Example 2:

```
{
  "event": "NF_PROFILE_CHANGED",
  "nfInstanceUri": ".../nf-instances/4947a69a-f61b-4bc1-b9da-47c9c5d14b64",
  "nfProfile": <Newly updated complete profile>
}
```

## How it Works

The NRF Support for 5G-SMF Subscription and Notification feature uses the NF Subscribe service to subscribe to changes on the status of NF instances that the NF receives as discovery responses. The SMF sends a subscription for the response validity period for each of the NF profiles that it receives in the discovery response. The SMF checks if an existing NF instance subscription time needs an extension or not depending on the current response time validity. If a subscription needs an extension, a subscription PATCH is sent with the extended validity time.

During subscription, the NRF may respond with a modified validity time. This validity time might differ from the SMF validity time request. In such a scenario, the SMF tracks the required subscription time and the actual subscription time returned by the NRF.

The SMF periodically (every two minutes) checks in database if there is any subscription with the actual subscription time ending soon (as in next five minutes) but has required validity time more than the actual validity time. In this scenario, the SMF sends a PATCH subscription to extend the subscription validity time.

The SMF fills the Status Notification URI based on the interface NRF configuration that is specified in the configuration. The notification vip ip and vip port are used to frame the status notification URI.

```
http://{nrfinterface.vip-ip}:{ nrfinterface.vip-port}/{notifResourceURI}
```

On status notification, the SMF updates the local cache and the external cache (cache pod) with the changed attributes.

## Call Flows

This section provides the call flows for this feature.

### Subscription(PATCH) Call Flow

The NRF updates the subscription to notifications on NF Instances to refresh the validity time, when the specified time is due to expire. The SMF can request a new validity time to the NRF. The NRF can assign and provide a new validity time to the NF, if the operation is successful.

Updating the "subscriptionID" resource, initiates the Subscription(PATCH) operation. Issuing an HTTP PATCH request on the URI representing the individual resource, starts the operation.

Figure 94: Subscription to NF Instances in the Same PLMN

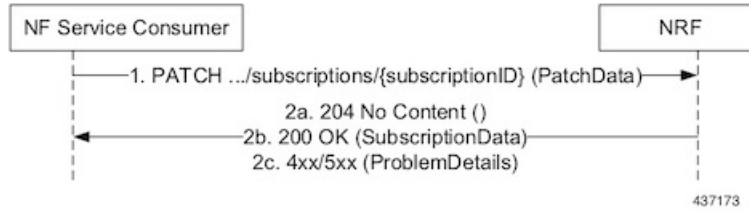


Table 150: Call Flow Description for Subscription to NF Instances in the Same PLMN

Step	Description
1	The SMF sends a PATCH request to the resource URI identifying the individual subscription resource. The payload body of the PATCH request contains a "replace" operation on the "validityTime" attribute of the SubscriptionData structure. The request also contains a new suggested value for the "validityTime" attribute. This replace operation does not replace any other attribute of the resource.
2a	When a subscription is successful, the NRF sends a "204 No Content" response. This indicates that the NRF accepts: <ul style="list-style-type: none"> <li>• Extension of the lifetime of the subscription</li> <li>• Value of the "validityTime" attribute</li> </ul>
2b	The NRF returns a "400 Bad Request" status code with the problem details if the subscription fails due to errors in the JSON Patch object in the request body.
2c	The NRF returns a "500 Internal Server Error" with the problem details if the subscription fails due to internal errors in the NRF.  Example:  <pre> PATCH .../subscriptions/2a58bf47 Content-Type: application/json-patch+json [   { "op": "replace", "path": "/validityTime", "value": "2018-12-30T23:20:50Z" }, ]                     </pre>

### Subscription(POST) Call Flow

The Subscription service operation allows to:

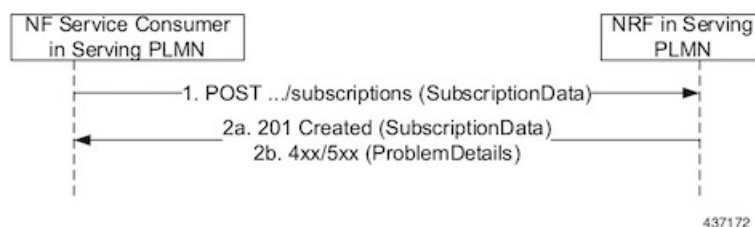
- Create a subscription such that the SMF can request notification (depending on certain filters) in the following scenarios:
  - When there is a registration or deregistration in the NRF.
  - When there is a modification to a profile.
- Create a subscription to a specific NF instance such that the SMF can request notification in the following scenarios:
  - When there is a modification to an NF instance.

- When there is a deregistration of an NF instance.



**Important** Currently, SMF only supports subscription of NF instances that the NF receives as its discovery response.

**Figure 95: Subscription to NF Instances in the Same PLMN**



Implementing the subscription to notifications on NF instances creates a new individual resource under the collection resource "subscriptions." Issuing a POST request starts the operation on the Uniform Resource Identifier (URI) representing the "subscriptions" resource.

**Table 151: Call Flow Description for Subscription to NF Instances in the Same PLMN**

Step	Description
1	<p>The NF Service Consumer sends a POST request to the resource URI representing the "subscriptions" collection resource.</p> <p>The request body includes data that indicates the type of notifications that the SMF has subscribed to receive. It also contains a callback URI, where the SMF prepares to receive the actual notification from the NRF. The notification contains the SMF suggested validity time, which represents the time span during which the subscription remains active.</p> <p>The subscription request may also include more parameters indicating the list of attributes in the NF Profile to monitor (or to exclude from monitoring). This request determines if the NRF must send a notification, when there is a change in any of the attributes of the profile.</p>
2a	<p>When a subscription is successful, the NRF sends a "201 Created" response. This response contains newly created subscription data that includes the NRF-determined validity time beyond which, the subscription is invalid. When the subscription expires, the SMF creates a new subscription in the NRF to continue receiving status notifications.</p>
2b	<p>The NRF returns a "400 Bad Request" status code with the problem details if the subscription fails due to errors in the subscription data.</p> <p>The NRF returns a "500 Internal Server Error" with the problem details if the subscription fails due to internal errors in the NRF.</p>

## NFStatus Notify Call Flow

Issuing a POST request to each callback URI of the various subscribed NF Instances, initiates the NFStatus Notify operator.

Figure 96: Notification from NRF in the Same PLMN

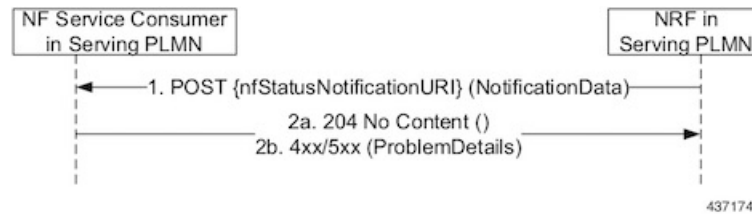


Table 152: Call Flow Description for Notification from NRF in the Same PLMN

Step	Description
1	<p>The NRF sends a POST request to the callback URI.</p> <p>The request body for a profile change notification request includes the following:</p> <ul style="list-style-type: none"> <li>• <b>event</b>: This attribute indicates the notification type. It can be one of the following: <ul style="list-style-type: none"> <li>• NF_REGISTERED</li> <li>• NF_DEREGISTERED</li> <li>• NF_PROFILE_CHANGED</li> </ul> </li> <li>• <b>nfInstanceUri</b>: Uniform Resource Identifier (URI) of the NF Instance associated to the notification event.</li> <li>• <b>nfProfile</b>: Indicates the new or updated NF profile.</li> <li>• <b>profileChanges</b>: This attribute identifies changes on the profile of the NF Instance associated to the notification event. This attribute is available when the event notification type is "NF_PROFILE_CHANGED".</li> </ul>
2a	When the notification is successful, the NRF sends a "204 No content" response.
2b	The SMF returns a "404 Not Found" status code with the problem details if the SMF disregards the "nfStatusNotificationURI" as a valid notification URI. For example, if the URI does not belong to any of the existing subscriptions that the SMF has created in the NRF.

## Limitations

In this release, the NRF Support for SMF Subscription and Notification feature has the following limitations:

- NF status notification supports only NF profile load, NF profile capacity, NF profile status, service load, service capacity, and service status parameter changes.
- SMF supports only the NFPofile field in the "NotificationData." It does not support the "Change item" field.
- The SMF supports notification of the following parameter changes:
  - nfProfile
  - nfStatus

- ipv4Address
- ipv6Address
- priority
- capacity
- load
- nfService
  - version




---

**Note** Change to a new version is permitted but not the deletion and modification of the existing version.

---

- scheme




---

**Note** Currently, http is only supported

---

- nfServiceStatus
  - ipEndPoints
  - apiPrefix
  - capacity
  - load
  - priority
- The SMF currently supports only the ADD, REPLACE, and REMOVE operations as part of the "op" parameter in the "ChangeItem" field.

## Configuring NRF Support for SMF Subscription and Notification

This section describes how to configure the NRF Support for SMF Subscription and Notification feature.

Use the following commands to configure the NRF interface, vip-ip, vip-port, and loopback port to open the server endpoints for the NF status notification.

**config**

```

endpoint sbi
  replicas integer
  vip-ip ip_address
  interface nrf
    vip-ip ip_address
  
```

```

vip-port port_number
loopbackPort port_number
end

```

**NOTES:**

- **endpoint sbi**: Specify the service-based interface (sbi) as the endpoint.
- **replicas**: Specify the number of instances of the service-based interface.
- **vip-ip ip\_address**: Specify the virtual IP address of the virtual host.
- **interface nrf**: Specify the interface as NRF.
- **vip-ip ip\_address**: Specify the virtual IP address of the virtual host. The SMF uses this as the listening IP address for the status notification.
- **vip-port port\_number**: Specify the port number of the virtual host. The SMF uses this as the listening port for the status notification.
- **loopbackPort port\_number**: Specify the internal port number of the loopback host. The SMF uses this port for the NF status notification.

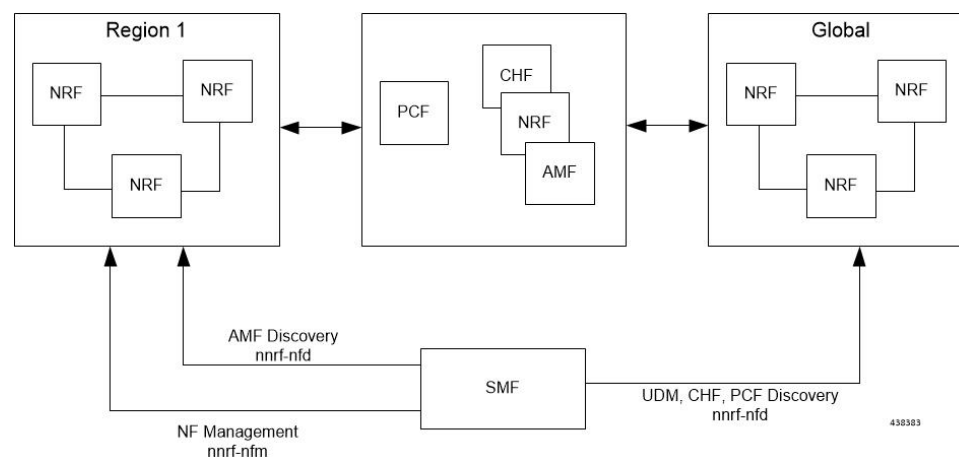
# NRF Interface per Endpoint

## Feature Description

The Network Repository Function (NRF) deployment can be logically segmented as global, regional, and so on, for a reliable network management. You can accomplish this segmentation by specifying different NRF endpoint groups for the discovery of different network functions. With associating a single NRF interface for each endpoint, the self-management of an NF improves the productivity.

For example, the SMF interacts with Region 1 NRF endpoints for management and AMF discovery. For UDM, CHF, and PCF discovery, the SMF communicates with the Global NRF endpoints.

**Figure 97: NRF Deployment**



## Standards Compliance

The NRF Interface Per Endpoint feature complies with the following standards:

- 3GPP TS 29.510 V15.2.0 (2018-12)
- 3GPP TS 29.510 V15.0.0 (2019-06)

## Limitations

The NRF Interface Per Endpoint feature has the following limitations:

- The NF discovery and load-balancing capabilities are available only for UDM, PCF, CHF, and AMF.
- The dynamic configuration changes of NRF endpoints is not available.
- Support for the liveness check of the NRF endpoints is not available.
- The SMF attempts the NF discovery first on the primary host. In the absence of the primary host, SMF attempts the discovery on the secondary host and switches to the tertiary if both primary and secondary are unavailable.

## Configuring the NRF Interface Per Endpoint

This section describes how to configure the NRF Interface Per Endpoint feature.

Configuring the NRF Interface Per Endpoint feature involves the following steps:

1. Associating a Discovery Group with NF Type
2. Configuring Locality for NF Types
3. Associating NRF Management and SMF Locality to NRF Endpoint
4. Configuring the NRF Group
5. Configuring Locality for SMF
6. Configuring NF Profiles for a DNN
7. Configuring Network Element Profile Parameters for the NF

### Associating a Discovery Group with NF Type

Use the following CLI commands for pairing a discovery group with NF types.

```
configure
  profile nf-pair nf-type nf_type
  profile nf-pair nf-type nf_type
  nrf-discovery-group nrf_discovery_group_name
end
```

#### NOTES:

- **nf-type** *nf\_type*: Specifies the NF type. The *nf\_type* can be: 5G\_EIR, AF, AMF, AUSE, BSF, CHF, GMLC, LMF, N3IWF, NEF, NRF, NSSF, NWDAF, PCF, SEPP, SMF, SMSF, UDM, UDR, UDSF, UPF, or range.



- **nrf-discovery-group** *nrf\_discovery\_group\_name*: Specifies the discovery group name.
- Discovery group is the logical link to the NRF endpoint groups (nrf-group). For each NF type, you can associate a discovery group and the locality information.

## Configuring Locality for NF Types

The SMF provides locality aware NF discovery.

Use the following configuration to configure locality for NF types.

```
configure
  profile nf-pair nf-type nf_type locality { client client_name
    | geo-server geo_server_name | preferred-server preferred_server_name }
  end
```

### NOTES:

- **client** *client\_name*: Specifies the client locality information. Client locality is the SMF's locality and is a mandatory parameter.
- **geo-server** *geo\_server\_name*: Specifies the geo-server locality information. Geo-server locality is geo redundant site for the preferred locality and is generally used as the next best server locality after preferred locality, during NF discovery.
- **preferred-server** *preferred\_server\_name*: Specifies the preferred server locality information. Preferred server locality is the locality that should be considered as the locality of preference during the corresponding NF discovery.

## Verifying the Association of the Discovery Group and Locality Configuration

This section describes how to verify the discovery group association and locality configuration for NF.

```
show running-config profile nf-pair
profile nf-pair nf-type UDM
  nrf-discovery-group DISC1
  locality client LOC1
  locality preferred-server PREF_LOC
  locality geo-server GEO
exit
```

## Associating NRF Management and SMF Locality to NRF Endpoint

Use the following CLI commands for configuring NRF Management (nrf-group) and SMF Locality and associating them to NRF Endpoint.

```
configure
  group nf-mgmt mgmt_name
    nrf-mgmt-group nrf_group_name
    locality locality_name
  end
```

## Verifying the Association of the NRF Management and SMF Locality to NRF Endpoint

This section describes how to verify the configuration that associates the NRF Management and SMF Locality to NRF Endpoint.

```
show running-config group nf-mgmt
group nf-mgmt NFMGMT1
  nrf-mgmt-group MGMT
  locality      LOC1
exit
```

## Configuring the NRF Endpoints Profile Parameters

The SMF provides CLI for configuring NRF endpoints for different services that are supported by NRF, such as **nnrf-nfm** (NF management) and **nnrf-nfd** (NF Discovery).



**Note** For a discovery group, only the **nnrf-disc** service can be configured. For management service, only **nnrf-nfm** can be configured.

The CLI configuration allows configuring multiple endpoints under each endpoint profile. The SMF uses the priority and capacity parameters to load balance between these endpoints. Primary, secondary, and tertiary host [ip:port] can be configured within each endpoint. Both IPv4 and IPv6 address can be specified. If both are specified, then IPv4 address is preferred.

A URI uniquely identifies a resource. In the 5GC SBI APIs, when a resource URI is an absolute URI, its structure is specified as follows:

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

"apiRoot" is a concatenation of the following parts: scheme ("http" or "https")



**Note** In this release of the specification, both HTTP and HTTPS scheme URIs are allowed. See *3GPP TS 33.501, subclause 13.1* for further details on security of service-based Interfaces.

- the fixed string "://"
- authority (host and optional port) as defined in IETF RFC 3986
- an optional deployment-specific string (API prefix) that starts with a "/" character. [api-root in CLI]

### configure

```
group nrf { mgmt mgmt_name | discovery discovery_name }
  service type nrf { nnrf-nfm | nnrf-disc }
  endpoint-profile epprofile_name
    priority priority_value
    capacity capacity
    api-root api_string
    api-uri-prefix uri_prefix_string
    uri-scheme { http | https }
    endpoint-name ep_name { capacity capacity | primary ip-address
    { ipv4 ipv4_address | ipv6 ipv6_address | port port_num }
    | secondary ip-address { ipv4 ipv4_address | ipv6 ipv6_address
    | port port_num } | tertiary ip-address { ipv4 ipv4_address
    | ipv6 ipv6_address | port port_num } }
    version [ uri-version version_num full version version_num ]
  end
```

**NOTES:**

- **api-root** *api\_string*: Specifies the deployment-specific service API prefix that is used within the { apiRoot }.
- **api-uri-prefix** *uri\_prefix\_string*: Specifies the {apiName}. If not configured, it takes the standard API name for the service as per the specification.
- **capacity** *capacity*: Specifies the profile capacity.
- **endpoint-name** *ep\_name* { **capacity** *capacity* | **primary ip-address** { **ipv4** *ipv4\_address* | **ipv6** *ipv6\_address* | **port** *port\_num* } | **secondary ip-address** { **ipv4** *ipv4\_address* | **ipv6** *ipv6\_address* | **port** *port\_num* } | **tertiary ip-address** { **ipv4** *ipv4\_address* | **ipv6** *ipv6\_address* | **port** *port\_num* } }: Specifies the endpoint name. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.
- **capacity** *capacity*: Specifies the node capacity for the endpoint. *capacity* must be an integer in the range of 0-65535.
- The endpoint selection for sending the message is based on probabilistic load-balancing algorithm (IETF RFC 2782) using the priority and capacity parameters.
- **primary ip-address** { **ipv4** *ipv4\_address* | **ipv6** *ipv6\_address* | **port** *port\_num* }: Specifies the primary endpoint IPv4 address, IPv6 address or port.
- **secondary ip-address** { **ipv4** *ipv4\_address* | **ipv6** *ipv6\_address* | **port** *port\_num* }: Specifies the secondary endpoint IPv4 address, IPv6 address or port.
- **tertiary ip-address** { **ipv4** *ipv4\_address* | **ipv6** *ipv6\_address* | **port** *port\_num* }: Specifies the tertiary endpoint IPv4 address, IPv6 address, or port.
- **priority** *priority\_value*: Specifies the priority for the service to select the appropriate profile using the load-balancing logic. *priority* must be an integer in the range of 0-65535.
- **uri-scheme** { **http** | **https** }: Specifies the URI scheme, as **http** or **https**.
- **version** [ **uri-version** *version\_num* **full version** *version\_num* ]: Specifies the api/Version. The full version format is <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

**Verifying the NRF Endpoints Profile Parameters**

This section describes how to verify the configuration of the NRF Endpoints Profile Parameters.

```
show running-config group nrf
group nrf discovery udm-discovery
service type nrf nnrf-disc
endpoint-profile epprof
capacity 10
priority 1
api-uri-prefix nudm-sdm
api-root root
uri-scheme http
version
uri-version v1
full-version 1.1.1.[1]
exit
endpoint-name endpointName
priority 1
```

```

capacity 100
primary ip-address ipv4 231.1.1.1
primary ip-address port 3021
exit
exit
exit
exit

```

## Configuring Locality for SMF

This section describes how to configure the locality for SMF.

This is a mandatory configuration if the SMF performs NF discovery using the NRF.

```

configure
  profile smf smf_profile_name
    locality value
  end

```

### NOTES:

- **locality** *value*: Specifies the SMF locality. *value* must be an alphanumeric string representing the deployed SMF locality. By default, this CLI command is disabled.
- To disable this configuration, use the **no locality** *value* command.

## Configuring NF Profiles for a DNN

This section describes how to configure the NF profile that the configured Data Network Name (DNN) uses.

```

configure
  profile dnn dnn_profile_name
    network-element-profiles { amf | chf | pcf | udm } nf_profile_name
  end

```

### NOTES:

- **network-element-profiles** { **amf** | **chf** | **pcf** | **udm** } *nf\_profile\_name*: Specifies one or more NF types such as AMF, CHF, PCF, and UDM as the network element profile. *nf\_profile\_name* must be an alphanumeric string representing the corresponding network element profile name.
- This is an optional configuration. By default, this CLI command is disabled.
- You can configure multiple profiles within a given service.
- To disable this configuration, use the **no network-element-profiles** { **amf** | **chf** | **pcf** | **udm** } *nf\_profile\_name* command.

## Configuring Network Element Profile Parameters for the NF

This section describes how to configure the network element profile parameters for the configured NF.

```

configure
  profile network-element { { amf | chf | pcf | udm } nf_profile_name }
    failure-handling-profile profile_name
    nf-client-profile profile_name

```

```

    query-params { dnn | limit | max-payload-size | requester-snssais
| supi | tai | target-nf-instance-id | target-plmn }
    end

```

**NOTES:**

- **failure-handling-profile** *profile\_name*: Specifies the NRF failure handling network profile for the configured NF type. *profile\_name* must be an alphanumeric string representing the corresponding NRF failure handling network profile name.
- **nf-client-profile** *profile\_name*: Specifies the local NF client profile. *profile\_name* must be an alphanumeric string representing the corresponding NF client profile name.
- **query-params { dnn | limit | max-payload-size | requester-snssais | supi | tai | target-nf-instance-id | target-plmn }**: Specifies one of the following query parameters to include in the NF discovery request towards the NRF.
  - **dnn**: Specifies a DNN as the query parameter in the NF discovery request towards the NRF.
  - **limit**: Specifies a limit for the maximum number of profiles that the NRF sends in the NF discovery response.
  - **max-payload-size**: Specifies the maximum payload size as the query parameter in the NF discovery request towards the NRF.
  - **requester-snssais**: Specifies the list of Single Network Slice Selection Assistance Information (S-NSSAIs) as the query parameter in the NF discovery request towards the NRF.
  - **supi**: Specifies a SUPI as the query parameter in the NF discovery request towards the NRF.
  - **tai**: Specifies a TAI as the query parameter in the NF discovery request towards the NRF.
  - **target-nf-instance-id**: Specifies a target NF instance Identifier as the query parameter in the NF discovery request towards the NRF.
  - **target-plmn**: Specifies a target PLMN as the query parameter in the NF discovery request towards the NRF.
- This is an optional configuration. By default, these CLI commands are disabled.
- To disable this configuration, use the **no** variant of these commands. For example, **no nf-client-profile** CLI command.

**Verifying the Local Configuration for the NRF Interface Per Endpoint**

This section describes how to verify the configuration for the NRF Interface Per Endpoint feature.

```

config
profile dnn cisco
  network-element-profiles chf chf1
  network-element-profiles amf amf1
  network-element-profiles pcf pcf1
  network-element-profiles udm udm1
  ssc-mode 2 allowed [ 3 ]
  session type IPV4 allowed [ IPV4V6 ]
  upf apn intershat
exit

profile smf smf1

```

```
node-id          12b888e1-8e7d-49fd-9eb5-e2622a57722
locality        LOC1
bind-address ipv4 127.0.0.1
bind-port       8008
fqdn cisco.com.apn.epc.mnc456.mcc123
plmn-id mcc 123
plmn-id mnc 456
exit

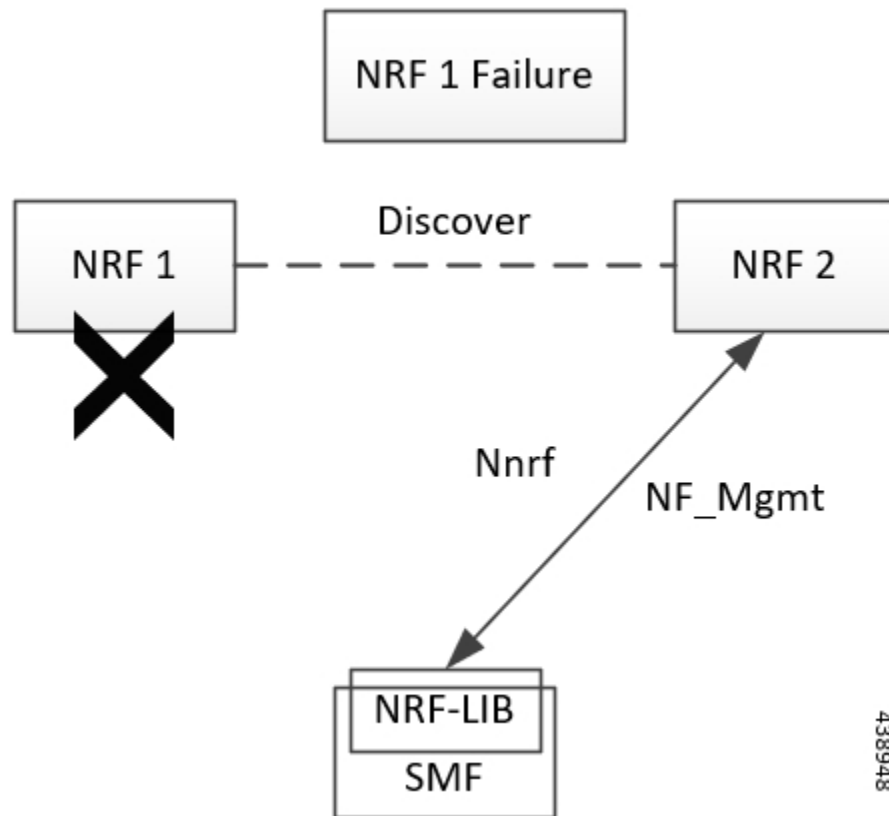
profile network-element amf amf1
nf-client-profile      AMF-L1
failure-handling-profile FH1
query-params [ target-nf-instance-id ]
exit
profile network-element pcf pcf1
nf-client-profile      PCF-L1
failure-handling-profile FH1
exit
profile network-element udm udm1
nf-client-profile      UDM-L1
failure-handling-profile FH1
exit
profile network-element chf chf1
nf-client-profile      CHF-L1
failure-handling-profile FH2
exit
end
```

# NRF Failure Handling Support

## Feature Description

The Network Repository Function (NRF) communication failure handling logic is implemented within the NRF client library. The NRF client library uses the NF registration messages for tracking the management NRF group operational status.

## How it Works



In the preceding diagram, NRF 1 is Primary and NRF 2 is secondary for SMF. On bringing up, the SMF registers (NF registration) with NRF 1 and starts NF heartbeat with NRF 1. The SMF uses the heartbeat response to track the operational status.

In case, the SMF detects NRF 1 failure by missing NF heartbeat response, the SMF registers to NRF 2 (secondary NRF) and starts sending NF heartbeat. The SMF continues to send NF Register message1 to NRF 1 to keep track of its status.

If the SMF receives register response from NRF 1, it detects that the NRF 1 is up again. The SMF marks NRF 1 as active once it recovers and stops sending NF heartbeats to NRF 2.



**Note** NF Reregistration (default behavior) on failover and fallback should be configuration driven. When NRF 2 detects that the SMF has stopped sending heartbeats, it checks from NRF 1 if it has received SMF registration by using discovery with SMF instance ID.

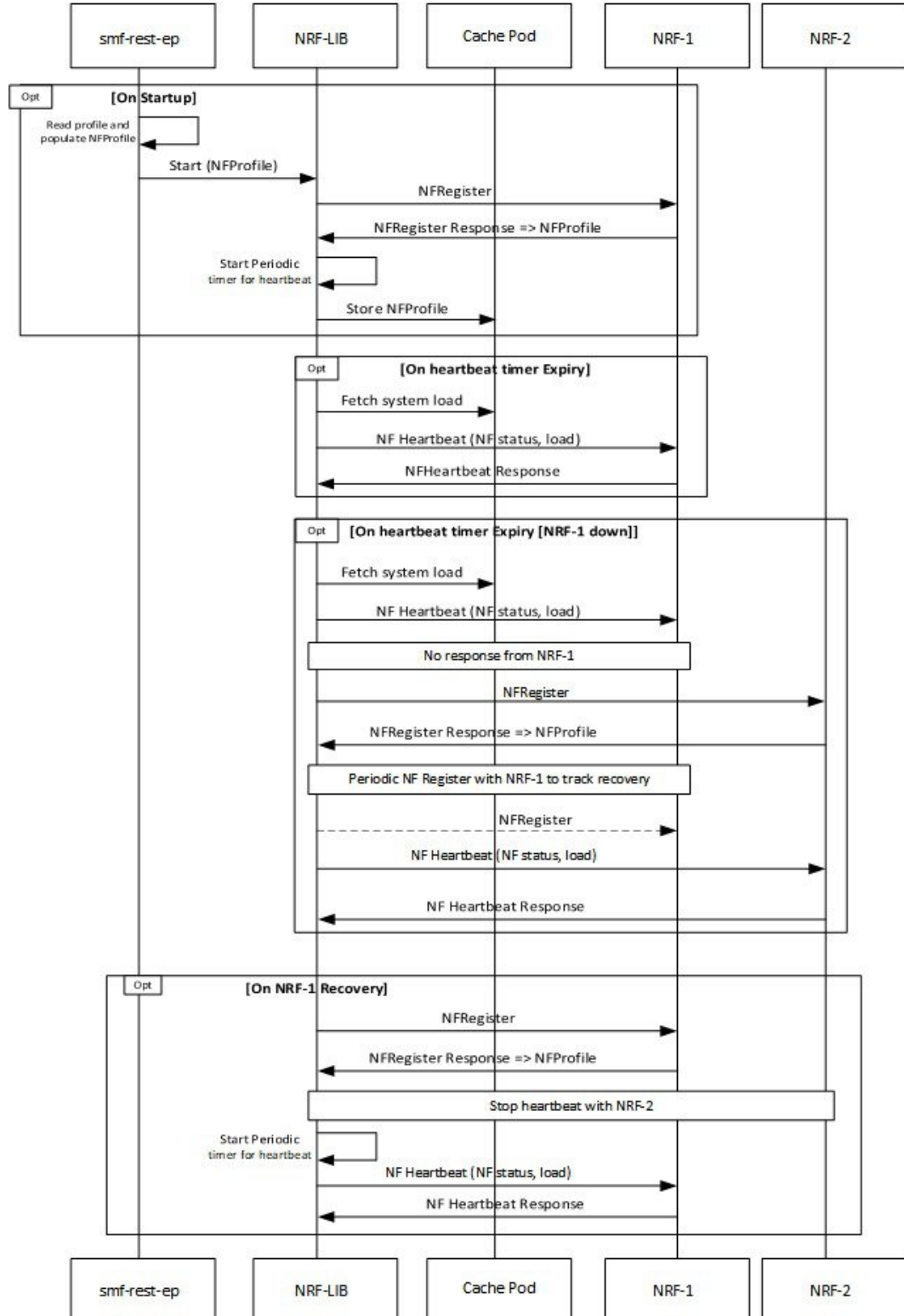
As the management and discovery endpoint groups are separate, the Registration based operation status check is not used for NRF failure handling during NF discovery. During NF discovery, the configured NRF endpoints within the group are attempted in the priority order. If the first choice NRF endpoint is not responding the next best NRF endpoint is chosen and so on.

## Call Flow

The following diagram shows the basic NF management call flow covering the NF registration, NF management and the NRF failure handling.



Figure 98: NF Management Call Flow



## Verifying the NRF Failure Handling

### NF Management Failure Handling

Management NRF endpoint configuration sample is shown below.

```
product smf# show running-config group nf-mgmt
group nf-mgmt MGM
  nrf-mgmt-group mgmt_group
  locality      LOC1
exit
product smf# show running-config group nrf mgmt
group nrf mgmt mgmt_group
  service type nrf nnrf-nfm
  endpoint-profile epprof
  uri-scheme http
  endpoint-name EP1
  priority 2
  primary ip-address ipv4 10.105.227.219
  primary ip-address port 8082
  secondary ip-address ipv4 10.105.227.220
  secondary ip-address port 8082
exit
  endpoint-name EP2
  priority 10
  primary ip-address ipv4 10.1.227.21
  primary ip-address port 8082
  secondary ip-address ipv4 10.1.227.22
  secondary ip-address port 8082
exit
exit
exit
product smf#
```

In the sample configuration, EP1 is the higher priority endpoint name as its priority is lesser than EP2 (2 against 10). So on bringing up, SMF sends NF registration to primary ip:port of EP1 [10.105.227.219:8082]. SMF uses secondary ip:port of EP1 if primary is down. SMF failovers to EP2 only if all ip:port of EP1 is down.

On successful registration with EP1 primary, SMF starts heartbeat with EP1 primary. If EP1 primary goes down, SMF detects the same by missing heartbeat response. On detecting EP1 primary down, SMF sends heartbeat to EP1 secondary [no reregistration]. Also, it periodically sends NF Heartbeat to EP1 primary to detect if it has recovered.

If SMF detects that EP1 primary and secondary is down, SMF failovers to EP2. When SMF failovers to EP2 primary, it sends reregistration (default behavior). It is assumed that all the endpoints with an endpoint name shares the database and so reregistration is only supported when failover is across endpoint names. In this case, EP1 primary and secondary shares the database. EP2 has a separate database and EP2 primary and secondary shares the database. On failover to EP2 primary, periodic NF registration is sent to primary of the EP1 only (to detect recovery).

Whenever a higher priority endpoint name is detected to be recovered, SMF falls back to the recovered IP:Port. For example, here the current active NRF endpoint is EP2 primary and SMF detects that EP1 primary has recovered, then SMF does reregistration with EP1 primary (default behavior) and stops heartbeat on EP2 primary.

Within endpoint NF heartbeat is used to track operational status. Across endpoints, registration is used to track the operational status. Message send timeout/RPC error and HTTP response codes 408, 429, 500, 501, 502, 503 are considered as failure to move to next NRF.

## NF Discovery Failure Handling

Discovery NRF endpoint configuration sample is shown below.

```
product smf# show running-config profile nf-pair nf-type UDM
profile nf-pair nf-type UDM
  nrf-discovery-group others_group
  locality client LOC1
exit
product smf# show running-config group nrf discovery others_group
group nrf discovery others_group
  service type nrf nrf-disc
  endpoint-profile epl
  capacity 30
  priority 50
  uri-scheme http
  endpoint-name ED1
  priority 56
  primary ip-address ipv4 110.105.227.219
  primary ip-address port 8082
  secondary ip-address ipv4 110.105.227.220
  secondary ip-address port 8082
  exit
  endpoint-name ED2
  priority 10
  primary ip-address ipv4 110.1.227.21
  primary ip-address port 8082
  secondary ip-address ipv4 110.1.227.22
  secondary ip-address port 8082
  exit
  exit
  exit
exit
product smf#
```

In the sample configuration, ED1 has the higher priority endpoint name as its priority is lesser than ED2 (2 against 10). So, whenever there is a NRF discovery required primary ip:port of ED1 [110.105.227.219:8082] is attempted. SMF uses secondary ip:port of ED1 if primary is down. SMF failovers to ED2 only if all ip:port of ED1 is down. There is no state maintained regarding NRF discovery failure with any NRF endpoint. Every time SMF needs to send NRF discovery, SMF starts with ED1 primary and failovers to ED1 secondary in case of failure, followed by ED2 primary and so on.

# Local Configuration for NF Management

## Feature Description

The SMF learns about the other NF endpoints such as Unified Data Management (UDM), Access and Mobility Management Function (AMF), Policy Control Function (PCF), Charging Function (CHF) and so on, through NF discovery service exposed by Network Repository Function (NRF) or through the CLI configuration. The SMF prioritizes the NF discovery through the NRF. If the NRF is not available, then the SMF uses the local configuration of NF endpoints to discover the NFs.

## Relationships

The Local Configuration for NF Discovery feature depends on the configuration of NRF endpoints, and the response from NRF. That is, the SMF uses the locally configured endpoints of the NFs only if the NRF endpoints remain unconfigured or if the NRF did not return any NFs matching the preferred server locality or geo locality.

For more information, see the [NRF Interface per Endpoint, on page 449](#) section in this chapter.

## Standards Compliance

The Local Configuration for NF Discovery feature complies with *3GPP TS 29.510, Versions 15.0.0 and 15.2.0*.

## Limitations

The Local Configuration for NF Discovery feature has the following limitations:

- Discovery and load balancing are available only for the UDM, PCF, CHF, and AMF but not for the UPF.
- Support for the liveness check of the NF endpoints is currently not available.
- The SMF attempts the NF discovery first on the primary host. In the absence of the primary host, the SMF attempts the discovery on the secondary host and switches to the tertiary if both the primary and secondary are unavailable.

## Configuring the NFs for NF Discovery

This section describes the Local Configuration for NF Discovery feature.

Configuring the NF for NF Discovery feature involves the following steps:

1. Configuring Locality for SMF
2. Configuring NF Profiles for a DNN
3. Configuring Network Element Profile Parameters for the NF
4. Configuring NF Client Profile
5. Defining Locality within NF Profile
6. Configuring NF Endpoint Profile Parameters

### Configuring Locality for SMF

This section describes how to configure the locality for SMF. This is a mandatory configuration if the SMF performs the NF discovery using the NRF.

```
configure
  profile smf smf_profile_name
    locality value
  end
```

NOTES:

- **locality value**: Specifies the SMF locality. *value* must be an alphanumeric string representing the deployed SMF locality. By default, this CLI command is disabled.
- To disable this configuration, use the **no locality value** command.

## Configuring NF Profiles for a DNN

This section describes how to configure the NF profile that the configured Data Network Name (DNN) uses.

```
configure
  profile dnn dnn_profile_name
    network-element-profiles { amf | chf | pcf | udm } nf_profile_name
  end
```

### NOTES:

- **network-element-profiles { amf | chf | pcf | udm } *nf\_profile\_name*** : Specifies one or more NF types such as AMF, CHF, PCF, and UDM as the network element profile. *nf\_profile\_name* must be an alphanumeric string representing the corresponding network element profile name.
- This is an optional configuration. By default, this CLI command is disabled.
- You can configure multiple profiles within a given service.
- To disable this configuration, use the **no network-element-profiles { amf | chf | pcf | udm } *nf\_profile\_name*** command.

## Configuring Network Element Profile Parameters for the NF

This section describes how to configure the network element profile parameters for the configured NF.

```
configure
  network-element-profiles { { amf | chf | pcf | udm } nf_profile_name }
    failure-handling-profile profile_name
    nf-client-profile profile_name
    query-params { dnn | limit | max-payload-size | requester-snsais
  | supi | tai | target-nf-instance-id | target-plmn }
  end
```

### NOTES:

- **failure-handling-profile *profile\_name***: Specifies the NRF failure handling network profile for the configured NF type. *profile\_name* must be an alphanumeric string representing the corresponding NRF failure handling network profile name.
- **nf-client-profile *profile\_name***: Specifies the local NF client profile. *profile\_name* must be an alphanumeric string representing the corresponding NF client profile name.
- **query-params { dnn | limit | max-payload-size | requester-snsais | supi | tai | target-nf-instance-id | target-plmn }**: Specifies one of the following query parameters to include in the NF discovery request towards the NRF.
  - **dnn**: Specifies a DNN as the query parameter in the NF discovery request towards the NRF.

- **limit**: Specifies a limit for the maximum number of profiles that the NRF sends in the NF discovery response.
  - **max-payload-size**: Specifies the maximum payload size as the query parameter in the NF discovery request towards the NRF.
  - **requester-snssais**: Specifies the list of Single Network Slice Selection Assistance Information (S-NSSAIs) as the query parameter in the NF discovery request towards the NRF.
  - **supi**: Specifies a SUPI as the query parameter in the NF discovery request towards the NRF.
  - **tai**: Specifies a TAI as the query parameter in the NF discovery request towards the NRF.
  - **target-nf-instance-id**: Specifies a target NF instance Identifier as the query parameter in the NF discovery request towards the NRF.
  - **target-plmn**: Specifies a target PLMN as the query parameter in the NF discovery request towards the NRF.
- This is an optional configuration. By default, these CLI commands are disabled.
  - To disable this configuration, use the **no** variants of these commands. For example, **no nf-client-profile** CLI command.

## Configuring NF Client Profile

This section describes how to configure the NF endpoints for AMF, CHF, PCF, and UDM.

```
configure
  profile nf-client { nf-type { amf amf-profile | chf chf-profile |
    pcf pcf-profile | udm udm-profile } nf_profile_name }
end
```

### NOTES:

- **profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile } nf\_profile\_name }**: Specifies the required NF client profiles and provides the local configuration for any of the following configured NFs:

- **amf**: Enables the AMF local configuration
- **chf**: Enables the CHF local configuration
- **pcf**: Enables the AMF local configuration
- **udm**: Enables the AMF local configuration

For example, if you are configuring the **amf amf-profile** keyword, then this command enables the AMF local configuration. The same approach applies for the other configured NFs too.

*nf\_profile\_name* must be an alphanumeric string representing the corresponding NF client profile name.

- You can configure multiple NF profiles within a given service.
- To disable this configuration, use the **no profile nf-client { nf-type { amf amf-profile | chf chf-profile | pcf pcf-profile | udm udm-profile } nf\_profile\_name }** command.

## Defining Locality within NF Profile

This section describes how to define the locality of the NF endpoints. For the NF endpoint selection, the SMF first considers the preferred locality that is configured with the **profile nf-pair** CLI command. The admin determines the preferred locality based on the proximity of the locality and the network function. The SMF then uses the geo-server locality configurations as the next preferred locality for the NF discovery. For information on the **profile nf-pair** command, see [Configuring Locality for NF Types, on page 451](#) in the *NRF Interface per Endpoint, on page 449* section.

The SMF selects the other locality endpoints if the **profile nf-pair** CLI command does not include the preferred server locality configuration, or if the **profile nf-client** CLI command does not include the endpoint configured with the preferred server or geo server locality. For the other locality endpoint selection, the SMF uses the **priority** configuration within the **locality** CLI command.

### configure

```
profile nf-client { nf-type { amf amf-profile | chf chf-profile |
pcf pcf-profile | udm udm-profile }nf_profile_name}
  locality locality_name [ priority priority | service name type
  service_types { endpoint-profile eprofile_name } ]
end
```

### NOTES:

- **locality** *locality\_name*: Specifies the locality of the NF endpoint. The SMF uses the locality configurations (that is, the preferred server locality and geo server locality) to select the appropriate NF endpoints.
- **priority** *priority*: Specifies the priority for the locality configuration.
- **service name type** *service\_types*: Specifies the configured NF service types. The service types vary depending the configured service.

The AMF service supports the following service types:

- namf-comm
- namf-evts
- namf-loc
- namf-mt

The CHF service supports the following service types:

- nchf-convergedcharging
- nchf-spendinglimitcontrol

The PCF service supports the following service types:

- npcfc-am-policy-control
- npcfc-bdtpolicycontrol
- npcfc-eventexposure
- npcfc-policyauthorization
- npcfc-smpolicycontrol
- npcfc-ue-policy-control

The UDM service supports the following service types:

- nudm-ee
  - nudm-pp
  - nudm-sdm
  - nudm-ueau
  - nudm-uecm
- **endpoint-profile** *epprofile\_name*: Specifies the endpoints at a per NF service level. The NF-specific services are available within the locality configuration.
  - You can configure multiple endpoints per profile name for the configured NF.

## Configuring NF Endpoint Profile Parameters

This section describes how to configure the NF endpoint profiles within the service, and its associated parameters.

The CLI configuration allows configuring multiple endpoints under each endpoint profile. The SMF uses the priority and capacity parameters to load balance between these endpoints. All endpoints under an endpoint profile share the session context. That is, when selecting an endpoint profile for initial message of a session, then the SMF sends the subsequent messages (for example, update, delete, and so on) of the session to any of the endpoints in the endpoint profile.

NRF Library (NRF-LIB) provides APIs to discover and send a message to an NF matching a set of filter parameters.

A URI uniquely identifies a resource. In the 5GC SBI APIs, when a resource URI is an absolute URI, its structure is specified as follows:

```
{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}
```

"apiRoot" is a concatenation of the following parts:

- scheme ("http" or "https")
- the fixed string "://"
- authority (host and optional port) as defined in IETF RFC 3986
- an optional deployment-specific string (API prefix) that starts with a "/" character. [api-root in CLI]

### configure

```
profile nf-client { nf-type { amf amf-profile | chf chf-profile |
pcf pcf-profile | udm udm-profile } nf_profile_name }
locality locality_name [ priority priority |
service name type service_types]
endpoint-profile epprofile_name
api-root api_string
api-uri-prefix uri_prefix_string
capacity capacity
endpoint-name ep_name { capacity capacity | primary ip-address
{ ipv4 ipv4_address | ipv6 ipv6_address
```



```

    | port port_num } | secondary ip-address { ipv4
    ipv4_address | ipv6 ipv6_address | port
    port_num } | tertiary ip-address { ipv4 ipv4_address | ipv6
    ipv6_address
    | port port_num } }
    priority priority_value
    uri-scheme { http | https }
    version [ uri-version version_num full version version_num ]
end

```



### Important

In this release of the specification, both HTTP and HTTPS scheme URIs are allowed. See *3GPP TS 33.501, subclause 13.1* for further details on security of service-based interfaces.

### NOTES:

- **api-root** *api\_string*: Specifies the deployment-specific service API prefix that is used within the { apiRoot }.
- **api-uri-prefix** *uri\_prefix\_string*: Specifies the {apiName}. If not configured, it takes the standard API name for the service as per the specification.
- **capacity** *capacity*: Specifies the profile capacity.
- **endpoint-name** *ep\_name* { **capacity** *capacity* | **primary ip-address** { **ipv4** *ipv4\_address* | **ipv6** *ipv6\_address* | **port** *port\_num* } | **secondary ip-address** { **ipv4** *ipv4\_address* | **ipv6** *ipv6\_address* | **port** *port\_num* } | **tertiary ip-address** { **ipv4** *ipv4\_address* | **ipv6** *ipv6\_address* | **port** *port\_num* } }: Specifies the endpoint name. You can configure the primary, secondary, and tertiary host (IP: Port) within each endpoint for NF server failover handling. The server failover configuration accepts both the IPv4 and IPv6 addresses. However, the SMF gives preference to the IPv4 address.
  - **capacity** *capacity*: Specifies the node capacity for the endpoint. *capacity* must be an integer in the range of 0-65535.  
The endpoint selection for sending the message is based on probabilistic load balancing algorithm (IETF RFC 2782) using the priority and capacity parameters.
  - **primary ip-address** { **ipv4** *ipv4\_address* | **ipv6** *ipv6\_address* | **port** *port\_num* }: Specifies the primary endpoint IPv4 address, IPv6 address or port.
  - **secondary ip-address** { **ipv4** *ipv4\_address* | **ipv6** *ipv6\_address* | **port** *port\_num* }: Specifies the secondary endpoint IPv4 address, IPv6 address or port.
  - **tertiary ip-address** { **ipv4** *ipv4\_address* | **ipv6** *ipv6\_address* | **port** *port\_num* }: Specifies the tertiary endpoint IPv4 address, IPv6 address or port.
- **priority** *priority\_value*: Specifies the priority for the service to select the appropriate profile using the load-balancing logic. *priority* must be an integer in the range 0-65535.
- **uri-scheme** { **http** | **https** }: Specifies the URI scheme as **http** or **https**.
- **version** [ **uri-version** *version\_num* **full version** *version\_num* ]: Specifies the api/Version. The full version format is <Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>].

## Verifying the Local Configuration for NF Discovery Feature

This section describes how to verify the Local Configuration for NF Discovery feature.

Use the following show command to verify the feature configuration details.

### show running-config

The following is a sample output of this show command.

```

config
profile dnn cisco
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udml
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV4V6 ]
upf apn intershat
exit

profile smf smf1
node-id          12b888e1-8e7d-49fd-9eb5-e2622a57722
locality         LOC1
bind-address ipv4 127.0.0.1
bind-port       8008
fqdn            cisco.com.apn.epc.mnc456.mcc123
plmn-id mcc 123
plmn-id mnc 456
exit

profile network-element amf amf1
nf-client-profile      AMF-L1
failure-handling-profile FH1
query-params [ target-nf-instance-id ]
exit
profile network-element pcf pcf1
nf-client-profile      PCF-L1
failure-handling-profile FH1
exit
profile network-element udm udml
nf-client-profile      UDM-L1
failure-handling-profile FH1
exit
profile network-element chf chf1
nf-client-profile      CHF-L1
failure-handling-profile FH2
exit
end

profile nf-client nf-type udm
udm-profile PROF1
locality PREF_LOC
priority 10
service name type nudm-sdm
endpoint-profile epprof
api-uri-prefix nudm-sdm
api-root      root
uri-scheme    http
version
uri-version v1
full-version 1.1.1.[1]
exit

```

```
exit
endpoint-name endpointName
priority 1
capacity 100
primary ip-address ipv4 231.1.1.1
primary ip-address port 3021
exit
exit
exit
exit
exit
exit
```

# Fallback to Static IP Address Support

## Feature Description

The SMF follows a priority order for the different NF selection options. It prioritizes the NF discovered from the network repository function (NRF) over the local configuration. The SMF uses the locally configured NFs in the following scenarios:

- When the NRF endpoints (for discovery) are not configured.
- When the NF discovery response has no valid NFs.

Depending on the deployment, the preferred server and geo locality server are configured for each of the NFs. The general rule is to select NFs in the preferred server locality followed by NFs in the geo locality server in case the preferred server NFs fail.

For each NF, the SMF provides an option to configure preferred and geo server locality [ **profile nf-pair** ]. For more details, see [Configuring Locality for NF Types, on page 451](#) in the [NRF Interface per Endpoint, on page 449](#) section.

In addition, each NF discovery response comes with associated validity time. The SMF caches this NF discovery response and uses it to fetch subsequent sessions. The SMF performs the NF discovery in the following conditions:

- The NF discovery response cache has no matching entries.
- The NF discovery response cache has matching entries, but the validity has expired.

## Relationships

The Fallback to Static IP Address feature has functional relationship with the following features:

- NF Discovery, NF Selection, and Load Balancing
- NRF Interface Per Endpoint
- Caching Support for NF Discovery

## How it Works

The SMF follows this sequence for NF selection:

1. It looks up the local cache (NF discovery response cache) for the NF
2. If the NF is a valid entry (not expired), it uses that entry. Else, SMF proceeds to Step 3.
3. The SMF reaches NRF for discovery [see, NRF Discovery (Priority 1)]. Else, SMF moves to Step 4.
4. If SMF cannot use the NRF for discovery, it uses the expired NF cache [see, Expired NF Cache ( Priority 2)]. If expired NF cache is not available, SMF moves to Step 5.
5. If SMF does not find the NF in the local cache nor is it able to get it in the NRF discovery response, it uses the locally-configured NF [see, NF Local configuration (Priority 3)].

The priority order for NF selection is as follows:

#### 1. NRF Discovery (Priority 1)

The SMS uses the NRF-provided, NF discovery service to discover NFs like AMF, UDM, and PCF. The SMF sets the preferred locality as provided in the "**profile nf-pair**" configuration in the discovery query. (For more details about the "**profile nf-pair nf-type**" CLI configuration, see [Configuring Locality for NF Types, on page 451](#) in the [NRF Interface per Endpoint, on page 449](#) section.) For each NF, the query parameters are configurable. (For more details, see [Configuring Network Element Profile Parameters for the NF, on page 454](#) in the [NRF Interface per Endpoint, on page 449](#) section) The NRF returns all the NFs matching the query criteria. When present, the NRF prefers NF profiles with a locality attribute that matches the preferred-locality. The NRF could return more NFs in the response, which are not matching the preferred target NF location. This occurs when there is no NF profile that is found matching the preferred target NF location. To avoid this, the NRF could set a lower priority for any additional NFs on the response not matching the preferred target NF location than those matching the preferred target NF location. The locality-aware NF selection logic of SMF is as follows:

- a. If the NF has both the preferred and geo locality server configurations, all the NFs in the response that are matching these are cached. SMF ignores the balance NFs. The load-balancing logic first selects the preferred locality NFs. If the preferred locality NFs fail, SMF picks the geo locality NFs for a retry. If N retry is allowed, N-1 retries are on the preferred locality and the last retry is on the geo locality NF. If the N-1 endpoints are unavailable in the preferred locality, SMF attempts all the endpoints of the preferred locality. Else, SMF picks up the geo locality endpoints for the remaining retries. Multiple retries on the same host (port) is not attempted.
- b. If the NF has only the preferred locality configuration, all the NFs in the response that match the preferred locality are cached. The load-balancing logic selects the endpoints from these NFs.
- c. If the NF does not have the preferred locality or geo locality configuration, then SMS caches all the discovery response NFs. The load-balancing logic selects from these NFs.



#### Note

- The load-balancing logic is based on priority, capacity, and load. The logic is similar to server selection as defined in IETF RFC 2782. But the weight is considered as "capacity \* (100 - load)".
- If SMF selects the NRF-discovered NFs (in any of the three cases), even when all attempts to reach preferred and geo locality fail, the SMF does not fall back to the local configuration NFs for a retry.

#### 2. Expired NF Cache (Priority 2)

The SMF performs an NF discovery only in the following scenarios:

- If the matching entries are not present for the query filter in its NF discovery cache
- If matching entries are present in its NF discovery cache but the validities of these entries have expired

The retention of an expired cache entry is configuration-based. If the expired cache entry is present and the NRF is not reachable or returns an error, then SMF uses the expired cache entry for NF selection. You can configure the SMF to control the cache entry usage with the following options:

- Invalidate the cache entry on expiration of validity.
- Use the invalidated cache entry for a configurable time period (timeout) and fallback to the static configuration after the timeout expires.




---

**Note** The SMF controls the cache entry usage - only when the NRF is down - through these options. The configurations are based on the **profile nf-pair**. Additionally, the SMF provides flexibility in configuring different cache usage rule for different NFs. For instance, the SMF always uses the expired cache to discover PCF when the NRF is down. But, for discovering the UDM, the SMF uses the expired cache for a timeout period of 10 milliseconds (ms) when the NRF is down.

---

### 3. NF Local Configuration (Priority 3)

The locally configured NFs are the last option for NF endpoint selection. (For more details, see the [Local Configuration for NF Management, on page 461](#) section.) The local configuration too considers the preferred and geo server locality for NF selection. The priority order is as follows:

- If the preferred server is configured for the NF [ in **profile nf-pair** ], SMF selects the NF endpoints under the preferred locality, first. The load-balancing logic is applicable for endpoint profiles and endpoints within the locality as per the configured priority and capacity values.
- If the geo locality is configured for the NF [ in **profile nf-pair** ], SMF selects the NF endpoints under the geo locality as the fallback option. That is, if the preferred server locality NF endpoints fail or preferred server locality endpoints are not configured. The load-balancing logic is applicable for endpoint profiles and endpoints within the locality as per the configured priority and capacity values.
- If the preferred server and geo locality server are not applicable, SMF picks up the locality based on the priority that is configured for each locality in the local NF configuration. The load-balancing logic is applicable for endpoint profiles and endpoints within the locality as per the configured priority and capacity values.




---

**Note** The priority under locality is applicable only if the preferred and geo locality servers are not applicable.

---

The failure template is configurable for each of the NFs. Also, the message type in the template can set the retry count and action for the possible HTTP return codes. For a sample configuration, see the [Configuring the Fallback to Static IP Address Support Feature, on page 472](#) section.

## Standards Compliance

The Fallback to Static IP Address Support feature complies with the following standards:

- 3GPP TS 29.510 V15.2.0 (2018-12)
- 3GPP TS 29.510 V15.0.0 (2019-06)

## Limitations

The Fallback to Static IP Address Support feature has the following limitation:

There is no support for dynamic configuration changes of NRF endpoints.

## Configuring the Fallback to Static IP Address Support Feature

This section describes how to configure the Fallback to Static IP Address Support feature.

### Configuring the Failure Template

This section describes how to configure the failure template.

```
configure
  profile nf-client-failure { nf-type { amf | chf | pcf | udm }
    profile failure-handling failure_handling_name
  end
```

#### NOTES:

- **profile nf-client-failure { nf-type { amf | chf | pcf | udm }:** Specifies the required NF client failure profile and provides the local configuration support for the following configured NF:

- **amf:** Enables the AMF local configuration
- **chf:** Enables the CHF local configuration
- **pcf:** Enables the PCF local configuration
- **udm:** Enables the UDM local configuration

For example, if the NF type that is selected is **udm**, then this command enables the UDM local configuration. The same approach applies for the other configured NFs.

- **profile failure-handling profile\_name:** Specifies the failure handling profile name. For example, "udmFail".

## Sample Configurations

The following is a sample configuration of the failure template mapping to dnn:

```
profile dnn cisco
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcf1
network-element-profiles udm udm1
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV4V6 ]
```

```
upf apn intershat
exit
```

The following is a sample configuration of the failure template mapping to smf:

```
profile smf smf1
  node-id          12b888e1-8e7d-49fd-9eb5-e2622a57722
  locality         LOC1
  bind-address ipv4 127.0.0.1
  bind-port        8008
  fqdn             cisco.com.apn.epc.mnc456.mcc123
  plmn-id mcc 123
  plmn-id mnc 456
exit
```

```
profile network-element amf amf1
  nf-client-profile      AMF-L1
  failure-handling-profile FH1
  query-params [ target-nf-instance-id ]
exit
```

```
profile network-element pcf pcf1
  nf-client-profile      PCF-L1
  failure-handling-profile FH1
exit
```

```
profile network-element udm udm1
  nf-client-profile      UDM-L1
  failure-handling-profile FH1
exit
```

```
profile network-element chf chf1
  nf-client-profile      CHF-L1
  failure-handling-profile FH2
exit
end
```

For more information, see [Configuring NF Profiles for a DNN](#), on page 454 in the [NRF Interface per Endpoint](#), on page 449 section.

## Configuring NF Service and Message Type

This section describes how to configure the NF service and its different message types.

### configure

```
profile nf-client-failure { nf-type { amf | chf | pcf | udm }
  profile failure-handling failure_handling_name
    service name type service_type
    message type message_type
  end
end
```

### NOTES:

- **service name type *service\_type***: Specifies the configured NF service types and provides the local configuration support for the following configured NF. The service types vary depending on the configured service.

The AMF service supports the following service types:

- **namf-comm**
- **namf-evts**
- **namf-loc**
- **namf-mt**

The CHF service supports the following service types:

- **nchf-convergedcharging**
- **nchf-spendinglimitcontrol**

The PCF service supports the following service types:

- **npcf-am-policy-control**
- **npcf-bdtpolicycontrol**
- **npcf-eventexposure**
- **npcf-policyauthorization**
- **npcf-smpolicycontrol**
- **npcf-ue-policy-control**

The UDM service supports the following service types:

- **nudm-ee**
- **nudm-pp**
- **nudm-sdm**
- **nudm-ueau**
- **nudm-uecm**

For example, if the *service\_type* that is selected is **nudm-sdm**, then this command enables the UDM local configuration. The same approach applies for the other configured NFs.

- **message type** *message\_type*: Specifies the configured NF message type and provides the local configuration support for the following configured NF.

The message types are varied depending on the configured profile and service type.

The following example provides a sample of the configured profile, service, and message type options.

Profile	Service Type	Message Type Options
amf	namf-comm	<ul style="list-style-type: none"> <li>• AmfCommEBIAssignment</li> <li>• AmfCommN1N2MessageTransfer</li> <li>• AmfCommSMStatusChangeNotify</li> <li>• range</li> </ul>
chf	nchf-convergedcharging	<ul style="list-style-type: none"> <li>• ChfConvergedchargingCreate</li> <li>• ChfConvergedchargingDelete</li> <li>• ChfConvergedchargingUpdate</li> <li>• range</li> </ul>



Profile	Service Type	Message Type Options
pcf	npcf-am-policy-control	<ul style="list-style-type: none"> <li>• PcfSmpolicycontrolCreate</li> <li>• PcfSmpolicycontrolDelete</li> <li>• PcfSmpolicycontrolUpdate</li> <li>• Range</li> </ul>
udm	nudm-sdm	<ul style="list-style-type: none"> <li>• UdmRegistrationReq</li> <li>• UdmSdmGetUESMSSubscriptionData</li> <li>• UdmSdmSubscribeToNotification</li> <li>• UdmSubscriptionReq</li> <li>• UdmUecmRegisterSMF</li> <li>• UdmUecmUnregisterSMF</li> <li>• UdmSdmUnsubscribeToNotification</li> <li>• range</li> </ul>



**Note** The example does not cover all the message options that are provided for each profile and service type.

## Configuring NF Failure Retry, Action, and Message Type

This section describes how to configure the failure retry and action for each service of the NF and its different message types.

```

configure
  profile nf-client-failure { nf-type { amf | chf | pcf | udm }
  profile failure-handling failure_handling_name
    service name type service_type
      message type message_type
        status-code httpv2 { integer }
        retry integer
        action { continue | retry-and-continue |
          retry-and-terminate | terminate }
      end
    end
  end

```

### NOTES:

- **status code httpv2 { integer }**: Specifies the status code for the retry and action for the NF service. Currently only "http" status code is provided. *integer* specifies the status code. *integer* must be an integer in the range of 300-599.
- **retry integer**: Specifies the number of times the NF service must retry before proceeding with the action.
- **action**: Specifies the action. The different actions supported are:

- **continue**: Specifies to continue the session without any retry. The retry count configuration is invalid with this action.
- **retry-and-continue**: Specifies to retry as per the configured retry count and continue the session.
- **retry-and-terminate**: Specifies to retry as per the configured retry count and terminate the session in case all retry fails.
- **terminate**: Specifies to terminate the session without any retry. Retry count configuration is invalid with this action.

The retry and action for a message send is picked based on the first send status code failure. A different status code in the retry does not lead to picking a new retry count and action.

## Configuring Invalidate (Purge) NF Discovery Cache

This section describes how to configure the cache entry invalidation (purge) for the NF discovery cache.

```
configure
  profile nf-pair nf-type { amf | chf | pcf | udm }
    cache invalidation { false | true [ timeout integer ] }
  end
```

### NOTES:

- **cache invalidation { false | true [ timeout integer ] }**: Configures the interval and cache invalidation rule. The default value is false.
  - **false**: Specifies that the cache entry will never be invalidated.
  - **true timeout integer**: Specifies that the cache entry will be invalidated. **timeout integer** specifies the time period in milliseconds (ms) for controlling the usage of the expired cache entry (when NRF is unreachable). The default value is 0 ms.

The following is a sample configuration that sets the cache invalidation to false for the UDM discovery:

```
profile nf-pair nf-type UDM
  cache invalidation false
end
```

The following is a sample configuration that sets the cache invalidation to true for the UDM discovery:

```
profile nf-pair nf-type UDM
  cache invalidation true timeout 10
end
```

# NF Profile Update

## Feature Description

The SMF invokes NF Update service operation when there are changes to the NF registration parameters due to the SMF profile configuration change.

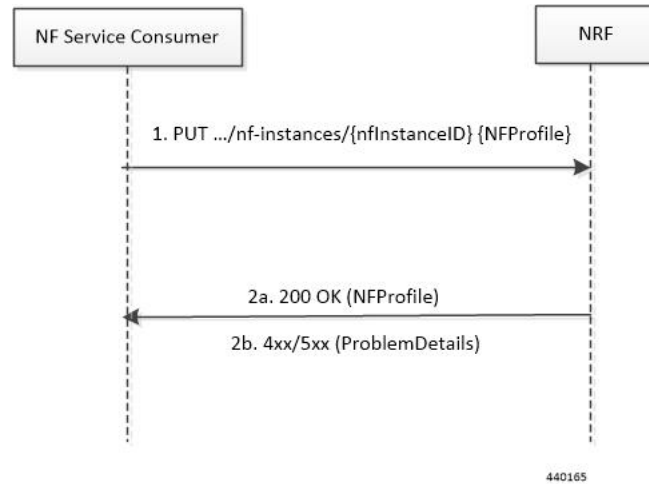
NF Update service updates the profile of NF that was previously registered in the NRF by providing the updated profile of the requesting NF to the NRF. The update operation could be a whole NF profile update

(complete replacement of the existing profile with a new profile), or an update to only a subset of the NF profile parameters (including adding, deleting, or replacing services to the NF profile).

## How it Works

The following figure illustrates a call flow representing the complete NF profile replacement.

**Figure 99: NF Profile Complete Replacement**

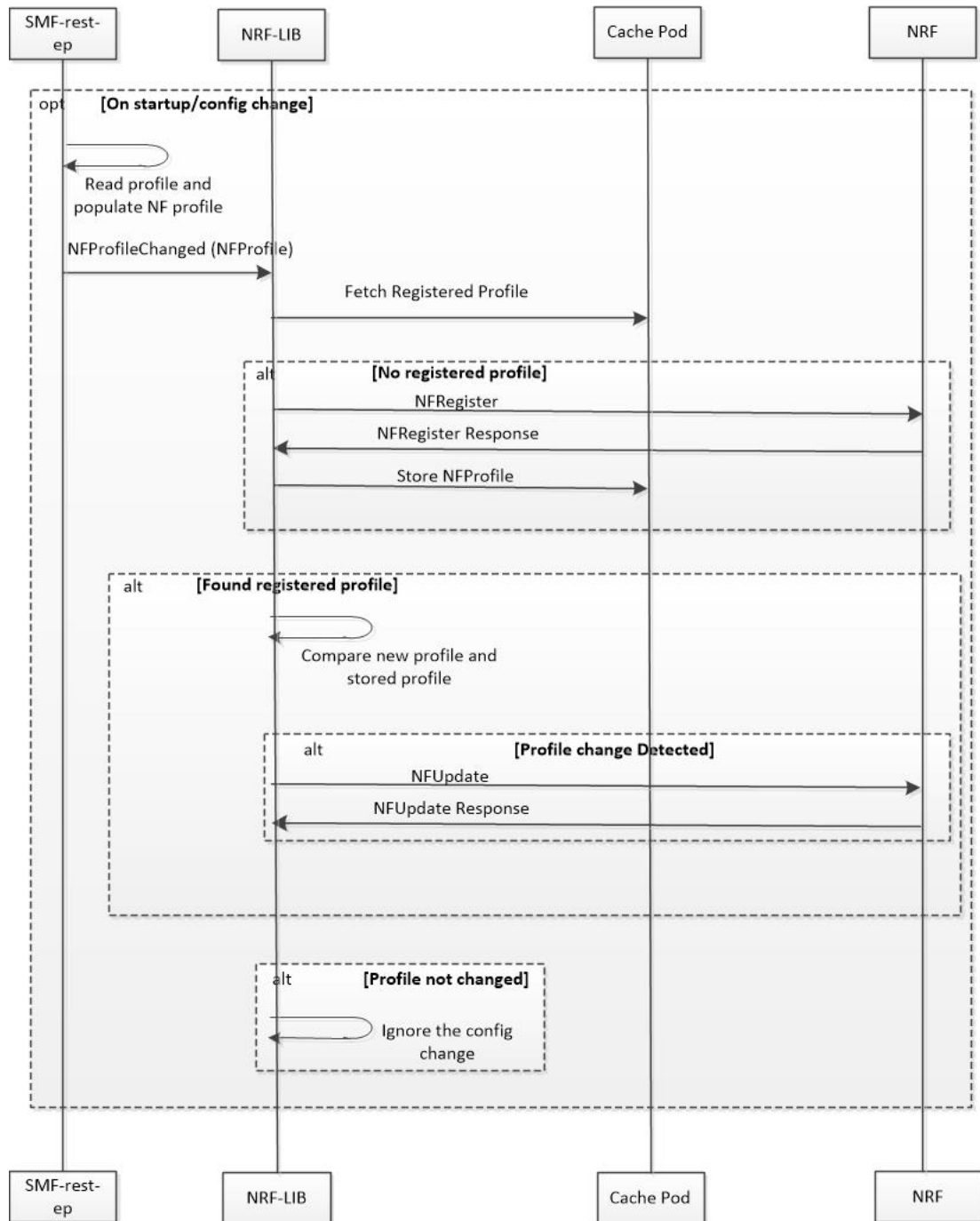


**Table 153: NF Update Call Flow Description**

Step	Description
1	The NF Service Consumer sends a PUT request to the resource URI representing the NF instance. The payload body of the PUT request contains an update operation on the NF Profile of the NF instance
2a	On success, if the NF Profile changes, the NRF returns "200 OK" along with the full NF Profile data in the response body.
2b	If the NF instance, identified by the "nfInstanceID", is not found in the list of registered NF instances in the NRF database, the NRF returns 4xx or 5xx status code with the ProblemDetails IE providing details of the error.

The following figure illustrates the call flow representing the NF registration and NF update messaging from NRF client library on NF profile change trigger from SMF-rest-ep.

Figure 100: NF Registration and NF Update Call Flow



440166

1. The SMF rest-ep, on start-up, reads the SMF profile configuration and accordingly populates the NF management Profile. The rest-ep then triggers NRF-LIB to indicate the NF Profile change.
2. NRF library (NRF-LIB) maintains the NF registration status and the registered profile in an external cache pod. The NRF client detects whether the NF registration with NRF is completed. If the NRF client detects

that the registration is not completed during NF profile change handling, perform Step 3. If the NF registration is complete, perform Step 4.

3. The NRF-LIB sends NF Register to NRF. It allows an NF Instance to register its NF profile in the NRF. It includes the registration of the general parameters of the NF Instance along with the list of services exposed by the NF Instance.
4. NRF-LIB fetches the registered NF profile and then compares it with the new profile.
5. The NRF-LIB NF sends NF update (PUT) request to the NRF when any of the parameters in the NF management profile changes due to SMF profile configuration change.
6. The NRF-LIB ignores the trigger if there is no change detected.



---

**Important** The NF update is sent only from the elected master.

---

Load parameter is not set as part of NF update PUT message. Heartbeat is set as the current active heartbeat interval.

## Standards Compliance

The NF Profile Update feature complies with the *3GPP TS 29.510, V15.2.0 (2018-12)*.

## Limitations

The SMF currently supports only the complete replacement of NF profile.

# Configuration Support for List of Tracking Areas and Tracking Area Ranges

## Feature Description

The SMF provides an optional configuration to configure the supported list of Tracking Areas and Tracking Area Ranges for a Public Land Mobile Network (PLMN). When a new configuration is present, the SMF sends the configured Tracking Area Identity (TAI), that is, TAIList and TAIRangeList, to the Network Function (NF) Repository Function (NRF) during the SMF Service Registration.



---

**Important** Any change in the configuration results in SMF Service update towards the NRF with the new configured TAIList and TAIRangeList values.

---

The PLMN value sent in the NRF discovery message remains the same as the PLMN configured on the SMF.

---

For more details on the NF Registration and NF Registration Update, see the [NF Profile Update, on page 476](#) section.

## Configuring TAI Group

This section describes how to configure the TAI Group.

### Configuring TAC List

Use the following configuration to configure the TAC list within TAI profile.

```
configure
  profile tai-group tai_group_name
    mcc mcc_value mnc mnc_value
    tac list [ tac_list_values ]
  end
```

#### NOTES:

- **tac list [ tac\_list\_values ]**: Configures the list of TAC values. For example, [ 1111 2222 3333 ]

### Configuring TAC Range List

Use the following configuration to configure the TAC range list within TAI profile.

```
configure
  profile tai-group tai_group_name
    mcc mcc_value mnc mnc_value
    tac range start start_value end end_value
  end
```

#### NOTES:

- **tac range start start\_value end end\_value**: Configures a specific TAC range or multiple TAC range lists. For example, **tac range start DDDD end EEEE**

You can configure a maximum of 16 values in a range.

- Use the **no tac range start start\_value end end\_value** command to remove a specific TAC range or TAC Ranges.

## Verifying the TAI Group Configuration

Use the following show command to verify the TAI group configuration.

```
show running-config profile tai-group tai_group_name
```

The following is an example of the **show command** configuration.

```
show running-config profile tai-group t1
profile tai-group t1
mcc 111 mnc 222
  tac list [ 1111 2222 3333 ]
  tac range start 4444 end 5555
exit
exit
mcc 333 mnc 44
  tac list [ AAAA BBBB CCCC ]
  tac range start DDDD end EEEE
exit
exit
```

exit

# Dynamic Configuration Change Support

## Feature Description

Global configuration table was built for NRF configurations and rebuilt each time when there was a change in configuration. NRF transaction/procedure (such as discovery, management, and so on) picked the configuration for the respective transaction/procedure from the global configuration tables. Therefore, the ongoing transactions were impacted if the configurations were modified in the middle of the transaction/procedure.

With this feature:

- NRF transaction/procedure picks a configuration version (v1) and uses the same version till the NRF transaction/procedure complete.
- If a user changes the configuration during an ongoing NRF transaction, then a new configuration version (v2) is created. However, the new configuration is not applied to the ongoing transaction.

The dynamic configuration changes are for the following data structures:

- NrfFailureProfileSt
- NrfCntProfileSt
- NrfGrpSt
- NrfPairProfileSt
- NrfMgmtGrpSt

## NRF Show Command Enhancements

### show nrf registration-info

Field	Description
NF Status	Displays the NRF registration information.
Registration Time	Displays the time of registration with NRF.
Active MgmtEP Name	Displays the active NRF management endpoint name.
Heartbeat Duration	Displays the heartbeat duration.
Uri	Displays the Uri information.

Field	Description
Host Type	Displays the NRF host type information.

## show nrf subscription-info

Field	Description
NF Instance Id	Displays the NF instance identity.
SubscriptionID	Displays the subscription identity information.
Actual Validity Time	Displays the actual validity time received from NRF server.
Requested Validity Time	Displays NF requested validity subscription time.

## show nrf discovery info

Field	Description
NF Type	Displays the NF type information.
Number of Discovery Filters	Displays the number of discovery filters.
Number of NF Profiles	Displays the number of NF profiles.

## show nrf discovery-info AMF discovery-filter

Step	Description
Discovery Filter	Displays the discovery filter information.
Expiry Time	Displays the expiry time for discovery filter.

## shownrfdiscovery-infoAMFdiscovery-filterdnn=intershatnf-discovery-profile

show nrf discovery-info AMF discovery-filter dnn=intershat nf-discovery-profile

Field	Description
NF InstanceId	Displays the NF Instance Identity.
NF Type	Displays the NF Type Information.
Discovery Filter	Displays the Discovery Filter Information.



```
show nrf discovery-info AMF discovery-filter dnn=intershat nf-discovery-profile f9882966-a253-32d1-8b82-c785b34a7cc9 nf-service
```

Field	Description
NF Status	Displays the NF Status Information.
Priority	Displays the Priority Information.
Capacity	Displays the NF Profile Capacity Information.
Load	Displays the Load Information.
Locality	Displays the Locality Information.
ipv4 address	Displays IPv4 Address received from the discovery response for this NF profile.
ipv6 address	Displays the IPv6 Address received from the discovery response for this NF profile.

## **shownrfdiscovery-infoAMFdiscovery-filterdnn=intershatnf-discovery-profile f9882966-a253-32d1-8b82-c785b34a7cc9 nf-service**

```
show nrf discovery-info AMF discovery-filter dnn=intershat nf-discovery-profile
f9882966-a253-32d1-8b82-c785b34a7cc9 nf-service
```

Field	Description
ServiceInstanceId	Displays the NF Service Instance ID.
ServiceName	Displays the NF Service Name.
UriScheme	Displays the Uri Scheme Information.

```
show nrf discovery-info AMF discovery-filter dnn=intershat nf-discovery-profile f9882966-a253-32d1-8b82-c785b34a7cc9 nf-service
```



## CHAPTER 32

# PDU Session Establishment from 4G-Only and Option 3x Capable Devices

- [Feature Summary and Revision History, on page 485](#)
- [Feature Description, on page 486](#)
- [Configuring Support for Packet Data Unit Sessions Establishment from 4G-Only and Option 3x Capable Devices, on page 489](#)
- [Packet Data Unit Sessions Establishment from 4G-Only and Option 3x Capable Devices OA&M Support, on page 492](#)

## Feature Summary and Revision History

### Summary Data

**Table 154: Summary Data**

Applicable Product(s) or Functional Area	5G-SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

## Revision History

**Table 155: Revision History**

Revision Details	Release
4g-UE and Option-3x Support phase-2 includes: <ul style="list-style-type: none"> <li>• DCNR based UPF selection</li> <li>• Handling SecondaryRatDataUsageReport from SGW/MME and relaying it to CHF</li> <li>• UE Presence-Reporting Feature Support</li> <li>• Handling Gtpv1 Messages for 4g-3g HO</li> <li>• SUPI+IP session and affinity key for 4G/WIFI HO</li> <li>• Avoiding sending of 5G QoS for 4G-Only UE</li> <li>• Handling 5GCNRS and 5GCNRI indication flags from SGW/MME</li> </ul>	2021.01.0
First introduced.	2020.03.0

## Feature Description

The dual connectivity enabled UEs support 4G-LTE and 5G-NR. Such UEs send a signal to the 4G Core Network, indicating that it's a dual connectivity enabled device.

When the Dual Connectivity New Radio (DCNR) capable UE attempts to register in MME, the MME sets "UP Function Selection Indication Flags" IE with DCNR flag set to 1 in the "Create Session Request" message. After the S-GW receives this IE over S11, it sends this IE over S5 to P-GW. This IE transmission helps the SGW-C and PGW-C to select SGW-U and UPF, which supports dual connectivity with NR.

The SMF/P-GW-C supports Packet Data Unit (PDU) sessions from only 5G capable UE in 4G radio. Now, the SMF/PGW-C extends support for the PDU sessions from the 4G-only capable device and Option 3x Capable device (NR & LTE radio connected to the EPC).

SMF handles periodic Secondary RAT Usage Data Report from MME over S5/S8 interface in Modify-Bearer-Request, Delete-Session-Request, Delete-Bearer-Response, and Delete-Bearer-Command based on IRPGW (Intended Receiver P-GW) flag. SMF retains the Usage-Report if IRPGW = 1. SMF supports Multiple instances of Secondary RAT Usage Data Report IEs, reports are stored until they are sent out to CHF based on the triggers.

If CBR/UBR success/failure response comes without PRA ID, then in next GTP request P-GW sends the PRA again.

With release 2021-01-0 SMF supports the following features:

- DCNR based UPF selection.
- Handling SecondaryRatDataUsageReport from SGW/MME and relaying it to CHF.

- UE Presence-Reporting Feature Support.
- Handling Gtpv1 Messages for 4g-3g HO.
- SUPI+IP session and affinity key for 4G <-> WIFI HO.
- Avoiding sending of 5G QoS for 4G-Only UE ( Qos rules and Qos flow description).
- Handling 5GCNRS and 5GCNRI indication flags from SGW/MME.

## How it Works

The SMF generates a PDU session ID (pdu-session-id) upon receiving a Create Session Request from the 4G-only UE. The SMF validates if the request has the 5G-IWK indication without the PDU session ID in the Protocol Configuration option. The UDM provides the IWK indication to the SMF per DNN. The SMF does not use this indication for deciding whether the UE is 5G capable.

The SMF generates a pdu-session-id based on lbi. For the 4G Create Session Request, the SMF generates pdu-session-id=lbi+64 and for WiFi sessions it generates pdu-session-id=lbi+80.

The SMF allows you to configure the default NSSAI under the profile DNN, which it includes in sliceInfo IE in the Policy Create Request directed towards the PCF during session creation from 4g-only UEs. If the default slice is not configured, then SMF selects one of the configured slices. When the UE is DCNR capable, and the DCNR is enabled for the session, the SMF considers the UE capable of supporting dual connectivity. You can configure DCNR per DNN and other NFs, such as UPF.

The SGW notifies the DCNR support to PGW through the 'UPF Selection Indication Flags IE'.

### DCNR-Based UPF Selection

SMF selects DCNR supported UPF for DCNR enabled session when DCNR is configured under query params. DCNR isn't a mandatory query parameter for UPF selection. DCNR can be configured in profile network-element upf. Query parameters / Filter criteria configuration under nf-profile is enhanced to include DCNR support.

### SecondaryRatData Usage Report Handling

SMF/UPF cannot differentiate usage in RAN, whether it is on NR or LTE for NSA devices while It is being tracked on eNB. SMF receives usage data ports on S5 interface in various messages, which it reports usage towards CHF.

SMF handles periodic Secondary RAT Usage Data Report from MME over S5/S8. The report is stored till it is sends out to CHF based on triggers mentioned below. SMF sends out the stored secondary RAT usage data report when any of the charging triggers are met.

### UePresenceReporting Support

Presence Reporting Area is an area defined within 3GPP Packet Domain for the purposes of reporting of UE presence within that area due to policy control and/or charging reasons. In the case of E-UTRAN, a Presence Reporting Area may consist in a set of neighbor or non-neighbor Tracking Areas, or eNBs and/or cells. There are two types of Presence Reporting Areas: "UE-dedicated Presence Reporting Areas" and "Core Network pre-configured Presence Reporting Areas" that apply to an MME pool. SMF supports "Core Network pre-configured Presence Reporting Areas".

### 2g/3g HO Support

During 4G to 2G/3G handover, SMF receives GTPv1 message, SMF has to drop the GTPv1 message, however, if SMF drops the request, it will delay the handover failure and subsequent attach to 2G/3G. In order to expedite the re-attach and reduce the UE service disruption, SMF supports the rejection of GTPv1 messages.

## Limitations

Following are the known limitations for Packet Data Unit Sessions Establishment from 4G-Only and Option 3x Capable Devices feature:

- For PresenceAreaReporting (PRA) feature, only the PRA-ID will be sent in ‘Presence reporting area action’ IE on S5 interface, user location info won’t be sent.
- For PresenceAreaReporting (PRA) feature, only the PRA-ID will be sent in ‘repPraInfos’ IE on N7 interface, user location info won’t be sent.
- For PRA feature, PRA Set is not supported, due to which “Additional PRA Information” sent on S5/N7 interfaces is also not supported.
- Maximum of 4 PraIds will be processed in a single PCF update message, if any PCF update has more than 4 PraIds then the other PraIds are ignored.
- PRA is applied only based on RAT from which device is connecting, not based on device type. So it is applied to both 4G and 5G devices, when connected from LTE
- SecondaryRatDataUsage Report supports only Option3 and Option3x (NR secondary RAT) UEs on S5 interface.
- SecondaryRatDataUsage Report isn’t supported on N2 interface for E-UTRAN Secondary RAT.
- PresenceAreaReporting (PRA) feature is supported only towards PCF and not towards CHF.
- Ultralow latency QCIs aren’t supported.

## Standards Compliance

The Packet Data Unit Sessions Establishment from 4G-Only and Option 3x Capable Devices feature complies with the following standards:

- *3GPP TS 23.003 [2]*
- *3GPP TS 24.301 [23]*
- *3GPP TS 29.272 [70]*
- *3GPP TS 29.274*

# Configuring Support for Packet Data Unit Sessions Establishment from 4G-Only and Option 3x Capable Devices

This section describes how to configure the support for PDU sessions establishment from the 4G-only and Option 3x capable devices.

## Configuring the NSSAI

This section describes how to configure the default NSSAI in SMF, which it includes in sliceInfo IE in the Policy Create Request message. The SMF sends this message towards the PCF during the session creation from 4G-only UEs.

To configure the default NSSAI in the SMF, use the following sample configuration:

```
config
  profile dnn profile_name
  nssai
  sd sd_value
  sst sst_value
end
```

### NOTES:

- **profile dnn *profile\_name***: Specifies the DNN profile name. *profile\_name* must be an alphanumeric string.
- **nssai**: Enters the NSSAI configuration.
- **sd *sd\_value***: Specifies the slice descriptor (sd). The *sd\_value* accepts a 6-digit hex string ([0-9a-fA-F]{6} - 000000 – ffffff). For example, 1A2B3c
- **sst *sst\_value***: Specifies the slice type (sst) value. The accepted range is 0–255.

## Configuring the Sessions as Dual Connectivity New Radio

This section describes how to mark the sessions as DCNR enabled for SMF and UPF.

To enable SMF to consider the sessions as DCNR capable, use the following configuration:

```
configure
  profile dnn profile_name
  dcnr boolean_value
end
```

### NOTES:

- **profile dnn *profile\_name*** – Specifies the DNN profile name. *profile\_name* must be an alphanumeric string.
- **dcnr *boolean\_value*** – Enable this command by configuring the dcnr to true. The SMF marks the session as “dcnr enabled session” only when the UE is DCNR capable, and the DCNR is configured under profile DNN.

## Verifying the Dual Connectivity New Radio Capability Configuration

This section describes how to validate if the UE is DCNR capable.

To view if the UE is DCNR enabled, use the following configuration:

```
show subscriber supi supi_id
```

The show output for DCNR support displays any one of the following options:

- dcnr: Enabled
- dcnr: None
- dcnr: UE Requested and Enabled

The following configuration is a sample output of the **show subscriber supi** command:

```
unknown] smf# show subscriber supi imsi-123456789012345
subscriber-details
{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        .....
      },
      "sScMode": 1,
      "chargEnabled": true,
      "uetimeZone": "+00:15+1",
      "allocatedIp": "12.0.4.0",
      "eUtranLocation": {
        "ecgi": {
          "mcc": "123",
          "mnc": "456",
          "eutraCellId": "1234567"
        },
        "tai": {
          "mcc": "123",
          "mnc": "456",
          "tac": "1820"
        }
      },
      "alwaysOn": "None",
      "dcnr": "Enabled",    -> The possible values are None, UE Requested and Enabled
    }
  ]
}
.....
```

## Configuring DCNR based UPF

This section describes how to enable DCNR flag in profile upf-group and link the group in upf network-element profile, also configures appropriate precedence for DCNR.

To configure the default NSSAI in the SMF, use the following configuration:

```
profile dnn profile_name
upf-selection-policy policy_name
exit
```

```
policy upf-selectionupf1
precedence precedence_1
```



```

[ dnn dcnr ]
exit
precedence precedence_2
[ dnn ]
exit
exit

profile upf-group profile_name
dcnr [ true | false ]
exit

```

**NOTES:**

- **profile dnn** *profile\_name* – Specifies the DNN profile name. *profile\_name* must be an alphanumeric string.

## Configuring Secondary RAT Usage Report

This section describes configuration for storing number of Secondary RAT Usage Reports before being sent to CHF.

Use the following configuration to configure Secondary RAT Usage Report:

```

configure
  profile charging profile_name
    max-secondary-rat-reports report_range
  end

```

**NOTES:**

- **max-secondary-rat-reports** *report\_range* Configures maximum number of secondary RAT usage reports that can be configured. *report\_range* must be an alphanumeric string 0–50.

## Configuring Presence Reporting

This section describes how to enable DCNR flag in profile upf-group and link the group in upf network-element profile, also configures appropriate precedence for DCNR.

To configure the default NSSAI in the SMF, use the following configuration:

```

profile dnn intershat
upf apn intershat
presence-reporting true
exit

```

**NOTES:**

- **presence-reporting true** – Enables presence reporting.

# Packet Data Unit Sessions Establishment from 4G-Only and Option 3x Capable Devices OA&M Support

This section describes operations, administration, and maintenance information for this feature.

## Statistics Support

The SMF uses the “dcnr” label in the session gauge “smf\_session\_counter” and “smf\_service\_stats” for collecting the DCNR session count. Only when the SMF session is a DCNR supported, then the “dcnr” label value is enabled. The label doesn’t support non-dcnr sessions.

The following is a sample query to count the DCNR active SMF session:

```
nts{action_type="rejected",app_name="smf",cluster="smf",data_center="unknown",
failure_type="hdr_decode_failure",hdr_decode_fail_reason="",instance_id="0",interface_type="
",message_type="",reject_cause="",service_name="gtpc-ep"} 2
smf_session_counter: sum (smf_session_counters{dcnr_on="enable"}) by (dcnr)
smf_service_stats: sum (smf_session_stats{dcnr_on="enable"}) by (dcnr, status, reason)
smf_session_counters{ presence-reporting = "enable"}) by (presence-reporting)
```

### DCNR Session Count

For DCNR, Session Count added a new label “dcnr” in the existing session gauge “smf\_session\_counter”. If SMF session is a DCNR session, then “dcnr” label value is “enable” otherwise it is “disable” for DCNR session.

Sample query to count DCNR active SMF sessions:

```
sum (smf_session_counters{dcnr_on="enable"}) by (dcnr)
```

For DCNR statistics added a new label “dcnr” in the existing counter “smf\_service\_stats”. For DCNR session this counter pegs with below labels values:

- Attempt Statistics - dcnr= “enable” and status= “attempted”
- Success Statistics – dcnr= “enable” and status= “success”
- Failure Statistics - dcnr= “enable” and status= “failures”

Sample query for DCNR statistics:

```
sum (smf_session_stats{dcnr_on="enable"}) by (dcnr, status, reason)
```

### Secondary Rat Data Usage Reports

For Secondary-Rat-Data-Usage-Reports added new counter “smf\_secondary\_rat\_usage\_report\_stats”

Labels for these stats include ebi, qfi, rat\_type, reason, service\_name, status. For this counter pegs with below labels values:

- ebi=ebi-val
- qfi=qfi-val
- rat\_type=NR

- reason=success/failure
- service\_name=smf-service
- status=ReceivedFromSgw/SentToChf

Sample query for DCNR statistics:

```
sum (smf_secondary_rat_usage_report_stats") by (qfi, status, reason)
```

### Presence Reporting

For Presence-Reporting Session Count added a new label “pra” in the existing session gauge “smf\_session\_counter”. If SMF session has presence-reporting enabled then. “presence-reporting” label value is “enable” otherwise it is “none” if presence-reporting is not enabled.

Sample query to count DCNR active SMF session:

```
sum (smf_session_counters{ pra ="enable"}) by (pra)
```

For Presence-Reporting statistics added a new label “presence-reporting” in the existing counter “smf\_service\_stats”. For presence-reporting session this counter pegs with below labels values.

- Attempt Statistics - pra = “enable” and status= “attempted”
- Success Statistics – pra = “enable” and status= “success”
- Failure Statistics - pra = “enable” and status= “failures”

Sample query for DCNR statistics:

```
sum (smf_session_stats{ pra ="enable"}) by (pra, status, reason)
```

## Bulk Statistics

The following bulk statistics are modified for release 2020.03.0:

Bulk Statistics Name	Statistics Type	Trigger	Description
smf_session_counters	Gauge	Increments/decrements for session attach or detach.	Indicates the total number of currently active SMF sessions. You can filter the active session based on the labels such as “dcnr=enable” for the DCNR session count..
smf_session_stats	Counter	Increments for success/failures of the call flow like attempted.	Indicates the statistics for call flow states such as attempted, success, and failures. You can filter the statistics based on labels such as “dcnr=enable” for only DCNR statistics.

Following new Bulk Stat is introduced to support Secondary Rat Data Usage Report in SMF schema in release 2021.01.0:

Bulk Statistics Name	Statistics Type	Trigger	Description
smf_secondary_rat_usage_report_stats	Counter	Increments for the status of the secondaryRatDataUsage Report processing.	The statistics displays secondaryRatUsageReports processing, for call flow status like 'ReceividFromSgw' and 'SentToCHF'. This can be also be filtered as per the labels like reason and QFI.

Following Stats are modified to support Secondary Rat Data Usage Report in SMF schema in release 2021.01.0:

Bulk Statistics Name	Statistics Type	Trigger	Description
smf_session_counters	Gauge	Increments/decrements for session attach or detach.	The total number of current active SMF sessions and this can be filtered as per the labels like "dcnr=enable" for the DCNR session count.
smf_session_stats	Counter	Increments for success/failures of the call flow like attempted.	The statistics for call flow status like attempted/success/failures and this can be filtered as per the labels like "dcnr=enable" for only DCNR statistics.
smf_session_counters	Gauge	Increments/decrements for session attach or detach.	The total number of current active SMF sessions and this can be filtered as per the labels like "pra=enable" for the presence-reporting enabled session count.
smf_session_stats	Counter	Increments for success/failures of the call flow like attempted.	The statistics for call flow status like attempted/success/failures and this can be filtered as per the labels like "pra=enable" for only presence-reporting statistics.



## CHAPTER 33

# Peer NF Failure Handling Support

- [Feature Summary and Revision History, on page 495](#)
- [Feature Description, on page 496](#)
- [Offline Failover Support for Charging, on page 496](#)
- [SMF Failover to Secondary PCF, on page 502](#)
- [Unified Data Management Failure Handling, on page 506](#)
- [User Plane Function Failure Handling, on page 512](#)

## Feature Summary and Revision History

### Summary Data

**Table 156: Summary Data**

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

**Table 157: Revision History**

Revision Details	Release
RAT type FHT support and graceful timeout handling and its related statistics introduced.	2021.01.0
First introduced.	Pre-2020.02.0

## Feature Description

The SMF utilizes the failover support for all the network functions such as Charging Function (CHF), Policy Control Function (PCF), Unified Data Management (UDM), and User Plane Function (UPF). The failure handling feature provides flexibility for the operator to take action upon failure, based on the message type and failure status code received.

The SMF uses the NRF Client Profile configuration and the NRF Failure Profile configuration to achieve the NF failover functionality.

This chapter describes how the SMF implements the failure handling functionality for CHF, PCF, UDM, and UPF.

## Offline Failover Support for Charging

### Feature Description

The SMF supports offline failover for charging when a CHF server fails. When the SMF continues after the CHF server failure, the SMF relays the offline charging services to the offline CHF server.

Failure Handling Profile contains the configurations that are invoked when a failure occurs. The Failure Handling feature supports the N11 and GTPC interfaces. With the dynamic configuration, you can change the dynamic attributes associated with the Failure Handling Profile while the SMF is running.

### How it Works

The offline failover support for the charging feature works as follows.

#### Selecting a CHF Server

The CHF server selection involves the following steps:

1. The smf-service sends packets to rest-ep. The NF library of rest-ep attempts to search a CHF server through NRF discovery. This library receives a CHF server IP address or the list along with the priority as a search result.
2. The NF library selects the CHF server based on the priority from the list that is received through NRF discovery. If no CHF server is selected, NF library falls back to the static configuration that exists in the CHF network profile.

After selecting a CHF server or a list, NF library relays the message to the first CHF server according to the priority.

#### Handling a CHF Server Failure

The CHF server failure occurs when the selected CHF sends failure response or sends no response. For a CHF server failure, the NF library sends status code that is based on the failure template. This template is associated with the CHF network profile. The smf-service sends the profile information to smf-rest-ep while sending the IPC message.

The failure template is configured with the list of HTTP error codes and the associated failure actions and retry count, as required. Following are the failure actions as available in the feature template for this feature:

- **Retry and Continue**—For this failure action, NF library attempts until the configured number of times before fallback. After the configured number of times completes, the NF library falls back to the lower priority CHF server IP address. If the failure or no response is received from CHF server, the "continue" action is returned to the smf-service.
- **Terminate**—For this failure action, NF library does not attempt to send message to other CHF servers. The library sends a reply to smf-service with the action as "terminate". For the "terminate" failure action, the smf-service deletes the session.
- **Continue**—For this failure action, the smf-service continues the session and sends the charging message to the offline CHF server. This server is configured as part of the local static CHF profile that is meant for the offline purpose. In addition, the failure handling profile for offline CHF is configured.



---

**Note** For the "continue" failure action, you must configure the offline CHF server at SMF in a separate profile. SMF will use this profile after the CHF server failure. If the offline CHF server is not configured, the session is continued without imposing any charging.

---

### Relaying to an Offline CHF Server

After CHF server failure, when the SMF continues, it converts the ongoing charging services as follows:

- Converts the services with both online and offline charging method to the offline charging method.
- Converts the services with online charging method to the offline charging method.
- Makes no change for the services with the offline charging method.

### Failure Handling Profile

The Failure Handling Profile defines the various parameters for failure handling.

The following table lists the configurations that allow dynamic update.

Table 158: Failure Handling Profile Parameters

Configuration Parameters	Configuration	Dynamic Change	Impact on Existing Sessions
profile failure-handling	<p><b>profile failure-handling</b> <i>name</i>  <b>interface</b> <i>gtpc/n11</i> <b>message</b> <i>message</i>  <b>cause-code</b> <i>cause_code</i> <b>action</b> <i>action</i>  <b>timeout</b> <i>timeout</i> <b>max-retry</b> <i>retry_count</i></p> <p><b>Supported values:</b></p> <ul style="list-style-type: none"> <li>• interface: gtpc or n11</li> <li>• message: <ul style="list-style-type: none"> <li>• gtpc-message: <ul style="list-style-type: none"> <li>• S5S8CreateBearerReq</li> <li>• S5S8CreateBearerReq</li> <li>• S5S8CreateBearerReq</li> </ul> </li> <li>• N11-message: n1n2transfer</li> </ul> </li> <li>• cause-code: <ul style="list-style-type: none"> <li>• gtpc-cause-code: temp-fail</li> <li>• N11-cause-code: temp-reject-handover/ temp-reject-register</li> </ul> </li> <li>• action: retry/clear/terminate</li> <li>• timeout: Range: [1000-5000] (default: 1000)</li> <li>• max-retry: Range: [0-5] (default: 1)</li> </ul> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• The timeout and max-retry parameters are applicable only if the action is set to 'retry'.</li> <li>• The CLI supports only the 'retry' action.</li> </ul>	Allowed	Sessions that use the old value in a call flow and procedure continues to use the old value.

## HTTP Cause Code Mapping with Failure Actions

Following table lists the mapping of failure actions with the associated HTTP cause code. Based on the network requirements, you can change the mapping.



Table 159: HTTP Cause Code Mapping with Failure Actions

Http-2 Cause Codes and Description		Converged CHF Failure Action			Offline CHF Failure Actions		
Code	Description	CDR-I	CDR-U	CDR-T	CDR-I	CDR-U	CDR-T
400	Bad Request	Terminate	No config	No config	Terminate	No config	No config
403	Forbidden	Terminate	No config	No config	Terminate	No config	No config
404	Not found	Terminate	No config	No config	Terminate	No config	No config
405	Method Not allowed	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	No config	No config
408	Request Timeout	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
500	Internal Server Error	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
503	Service Unavailable	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
508	Gateway Timeout	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue
0	No reply from server	Retry and Continue	Retry and Continue	Retry and Continue	Terminate	Retry and Continue	Retry and Continue

## SMF Behaviour for Failure Actions

The following table describes the SMF behaviour on receiving different failures (Continue, Ignore, and Terminate) in CDR-(I/U/T).

CHF Failure Actions	Converged CHF			Offline CHF		
	CDR-I	CDR-U	CDR-T	CDR-I	CDR-U	CDR-T
Continue	Send CDR to offline CHF. If offline CHF is not configured, continue the session without charging.	Send CDR to offline CHF. If offline CHF is not configured, continue the session without charging.	Send CDR to offline CHF if offline CHF is configured	Continue the session without charging	Continue the session without charging	Continue the session deletion
Terminate	Delete the session	Delete the session	Continue the session deletion	Delete the session	Delete the session	Continue the session deletion

CHF Failure Actions	Converged CHF			Offline CHF		
	CDR-I	CDR-U	CDR-T	CDR-I	CDR-U	CDR-T
Ignore	Delete the session	No action taken. Record(s) will be reattempted in the next CDR request.	Continue the session deletion	Delete the session	No action taken. Record(s) will be reattempted in the next CDR request.	Continue the session deletion

## Standards Compliance

The offline failover support for charging feature complies with the following standards:

- 3GPP TS 32.255
- 3GPP TS 32.290
- 3GPP TS 32.291

## Limitations

The offline failover support for charging feature has the following limitations:

- Session Level Limits are mandatory from CHF or you must configure them locally. As per the 3GPP specification, the last linked URR cannot be removed when online URR needs to be delinked from the offline URR.

## Configuring the Offline Failover Support for Charging

This section describes how to configure the offline failover support for charging.

Configuring the offline failover support for charging feature involves the following steps:

1. [Configuring Failure Handling Profile in an NF Library, on page 500](#)
2. [Configuring an Offline Server Client and an Offline Failure Handling Profile, on page 501](#)

### Configuring Failure Handling Profile in an NF Library

Use the following sample configuration to configure the failure handling profile in an NF library.

You can configure the HTTP status code with the corresponding action for the CHF Create, Update, or Release messages. Based on the configuration of the failure handling profile, the NF library takes an action when the CHF server failure occurs.

```

config
  profile nf-client-failure nf-type nf_name
    profile failure-handling failurehandling_name
      service name type servicename_type
      message type messagetype_value

```

```

status-code httpv2 statuscode_value
action failureaction_value
exit

```

**NOTES:**

- **profile nf-client-failure nf-type** *nf\_name*: Specify the name of the network function that is required after the NF client failure.
- **profile failure-handling** *failurehandling\_name*: Specify the name of the profile for failure handling.
- **service name type** *servicename\_type*: Specify the name of the service type. *servicename\_type* can be one of the following values:
  - nchf-convergedcharging
  - nchf-spendinglimitcontrol
- **message type** *messagetype\_value*: Specify the value for type of message. *messagetype\_value* can be one of the following values:
  - ChfConvergedchargingCreate
  - ChfConvergedchargingUpdate
  - ChfConvergedchargingDelete
- **status-code** *statuscode\_value*: Specify the status code as per the configured failure template. *statuscode\_value* must be an integer in the range of 0–599. The range of status codes is separated by either '-' or '!':
- **action** *failureaction\_value*: Specify the value for the failure action as per the configured failure template. *failureaction\_value* can be one of the following values:
  - continue
  - retry-and-continue
  - retry-and-ignore
  - retry-and-terminate
  - terminate

## Configuring an Offline Server Client and an Offline Failure Handling Profile

This section describes how to configure the offline server client and offline failure handling profile.

Use this CLI to configure the offline client profile and offline failure handling profile for the selected CHF server.

**configure**

```

profile network-element chf chf_name
nf-client-profile nf_client_profile_name
failure-handling-profile failure_handling_profile_name
query-params [ dnn ]
nf-client-profile-offline nf_client_profile_offline_IP_port_number

```

```

failure-handling-profile-offline failure_handling_profile_offline_name
exit

```

**NOTES:**

- profile-network-element chf – Enter the name of the CHF server.
- nf-client-profile – Enter the name of the client profile.
- failure-handling-profile – Enter the name of the failure handling profile.
- query-params – Enter the query parameter value, which is the data network name.
- nf-client-profile-offline – Enter the name of the offline client profile.
- failure-handling-profile-offline – Enter the name of the offline failure handling profile.

# SMF Failover to Secondary PCF

## Feature Description

The SMF utilizes the NF Failover support to achieve the PCF failover functionality.

The NF Failover feature supports the following functionality:

- Multiple endpoints for a service as primary and secondary endpoints. The endpoints can be configured using the NRF Client Profile configuration and the NRF Failure Profile configuration.
- Failure behavior based on:
  - Message Type
  - HTTP Status Codes in the response messages

## SMF PCF Failure Handling

This section describes the working of SMF for message-level failure handling and the corresponding HTTP status code-based failure.

The SMF PCF failover supports the following messages that are initiated from the SMF.

- PcfSmpolicycontrolCreate
- PcfSmpolicycontrolUpdate
- PcfSmpolicycontrolDelete

During the PDU session lifecycle, the SMF exchanges the messages at various stages with the PCF. Depending on the HTTP status code configured in the NRF failure profile, the SMF receives one of the following actions:

- Ignore
- Continue
- Terminate

Table 160: Relationship between SMF PCF Failover Messages and Actions

	PcfSmpolicy controlCreate	PcfSmpolicy controlUpdate	PcfSmpolicy controlDelete
Ignore	Continue with locally configured/UDM-provided policy parameters. <b>Note</b> Do not contact PCF for subsequent messages. <b>PCF-Interaction Status: OFF</b>	Continue with ‘currently available snapshot’ of policy parameters. Contact PCF for subsequent messages. <b>PCF-Interaction Status: ON</b>	Current failure ignored. Session is deleted. <b>PCF-Interaction Status: Session deleted</b>
Continue	Continue with locally configured/UDM-provided policy parameters. <b>Note</b> Do not contact PCF for subsequent messages. <b>PCF-Interaction Status: OFF</b>	Continue with ‘currently available snapshot’ of policy parameters. <b>Note</b> Do not contact PCF for subsequent messages. <b>PCF-Interaction Status: OFF</b>	Current failure ignored. Session is deleted. <b>PCF-Interaction Status: Session deleted</b>
Terminate	Terminate the session.	Terminate the session.	Terminate the session.

## PCF Interaction Status

This feature supports the following status messages for SMF-initiated and PCF-initiated messages:

- **PCF-Interaction Status: ON**

SMF-initiated messages—The SMF continues to initiate the messages towards the PCF whenever the criteria is met.

PCF-initiated messages—The SMF continues to accept all the messages initiated from the PCF towards the SMF.

- **PCF-Interaction Status: OFF**

SMF-initiated messages—The SMF does not initiate or send the messages towards the PCF whenever the criteria is met. The SMF treats the PCF as if it is not available and continues further actions.

PCF-initiated messages—There are two messages initiated by the PCF.

- SmPolicyUpdateNotifyReq: On receiving this message, the SMF sends a 404 error code in response and cleans up the session and does not send the Delete Request to the PCF.



**Note** The SMF also sends FIVEGSM\_CAUSE value as **REACTIVATION REQUESTED** in the FIVEG\_PDU\_SESSION\_RELEASE\_COMMAND to UE for 5G. In case of 4G, the SMF sends cause **REACTIVATION REQUESTED** in DELETE BEARER REQUEST message to the S-GW.

- **SmPolicyAssociationTerminationReq**—On receiving this message, the SMF sends a success response and cleans up the session. As part of this interaction, the SMF sends a Delete Request to the PCF.




---

**Note** This is an exception when the PCF-Interaction Status is set to OFF.

---

## Configuring SMF Failover to Secondary PCF Support

### Configuring the PCF Failure Handling Profile

Use the following sample configuration to configure the PCF failure handling profile with action.

```

config
  profile nf-client-failure nf-type pcf
    profile failure-handling fhprofile_name
      service name type npcf-smpolicycontrol
      message type PcfSmpolicycontrolCreate
      status-code httpv2 status_code
      action { continue | retry-and-continue | retry-and-ignore |
retry-and-terminate } retry retry_value
      exit

```

#### NOTES:

- **profile failure-handling** *fhprofile\_name*: Specify the failure handling profile name.
- **service name type** *npcf-smpolicycontrol*: Specify the PCF service name type.
- **message type** *PcfSmpolicycontrolCreate*: Specify the message type.
- **status-code** *httpv2 status\_code*: Specify the HTTPv2 status code as an integer in the range of 0–599, separated by either '-' or ' '.
- **action { continue | retry-and-continue | retry-and-ignore | retry-and-terminate } retry** *retry\_value*: Specify the action and the number of retry attempts. *retry\_value* must be an integer in the range of 1–10.

### Configuring the Association of Failure Handling Profile

Use the following sample configuration to configure the association of FH profile in the respective network element.

```

config
profile network-element pcf pcfprofile_name
  nf-client-profile nfprofile_name
  failure-handling-profile fhprofile_name
  query-params [ dnn ]
  rulebase-prefix rbprefix_name
  predefined-rule-prefix preruleprefix_name
  exit

```

#### NOTES:

- **nf-client-profile** *nfprofile\_name*: Specify the NF client profile name.
- **failure-handling-profile** *fhprofile\_name*: Specify the failure handling profile name.
- **query-params** [ *dnn* ]: Specify the query parameter for NF discovery.
- **rulebase-prefix** *rbprefix\_name*: Specify the rulebase prefix to be added.
- **predefined-rule-prefix** *preruleprefix\_name*: Specify the predefined rule prefix to be added.

## Configuring Secondary and Tertiary IP Addresses

Use the following sample configuration to configure secondary and tertiary IP addresses:

```

config
  profile nf-client nf-type pcf
    pcf-profile PP1
    locality LOC1
    priority 30
    service name type npcf-smpolicycontrol
      endpoint-profile EP1
        capacity 30
        uri-scheme http
        endpoint-name EP1
        priority 56
        primary ip-address ipv4 primary_ipv4
        primary ip-address port 8098
        secondary ip-address ipv4 secondary_ipv4
        secondary ip-address port 9098
      exit
    exit

```

### NOTES:

- **primary ip-address** **ipv4** *primary\_ipv4*: Specify the primary IPv4 address.
- **primary ip-address** **port** *8098*: Specify the port number of the primary IPv4 address.
- **secondary ip-address** **ipv4** *secondary\_ipv4*: Specify the secondary IPv4 address.
- **secondary ip-address** **port** *9098*: Specify the port number of the secondary IPv4 address.

## SMF Failover to Secondary PCF OAM Support

This section describes operations, administration, and maintenance information for this feature.

### Statistics Support

The following statistics are added in support of SMF Failover to Secondary PCF feature.

- PcfSmpolicyControlCreate
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses

- PcfSmPolicyControlUpdate
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- PcfSmpolicyControlDelete
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- PolicyUpdateNotifyReq
  - Number of accepted requests
  - Number of rejected requests
  - Number of skipped requests
- PolicyDeleteReq
  - Number of accepted requests
  - Number of rejected requests
  - Number of skipped requests
- PolicyUpdateRequest
  - Number of accepted requests
  - Number of rejected requests
  - Number of skipped requests
- Gauge counter for number of subscribers with policy type local/pcf.

# Unified Data Management Failure Handling

## Feature Description

The Unified Data Management (UDM) is responsible for primarily storing the subscriber data, which SMF accesses for managing the user sessions on the network.

The UDM failure handling support on SMF introduces a new failure handling template (FHT) profile. This profile is associated with the UDM profile in SMF.

The FHT template provides flexibility for SMF to fine tune its interactions with UDM over N10 for the sessions. It supports the SMF to handle the HTTP status codes in response from UDM for both new and existing sessions.



The NF failover support is available in the SMF using the NRF Client profile configuration and the NRF failure profile configuration. This feature supports the following functionality:

- Configure multiple endpoints for a service as primary and secondary endpoints.
- Specify the failure handling behavior based on:
  - Message Type
  - HTTP Status Codes in the response messages

## How it Works

The SMF utilizes the NF Failover to achieve the UDM failover support functionality. This section provides information on how the SMF handles message-level failures and the corresponding HTTP status code-based failures.

The UDM failover supports the following messages that are initiated from the SMF.

- UE-Connection-Management (UE-CM)
  - Nudm\_UECM\_Registration
  - Nudm\_UECM\_DeRegistration
- UE-Subscription-Management (UE-SDM)
  - Nudm\_SDM\_Get
  - Nudm\_SDM\_Subscribe
  - Nudm\_SDM\_Unsubscribe

During the PDU session lifecycle, the SMF exchanges the preceding messages at various stages with the UDM. Depending on the HTTP status code configured in the NRF failure profile, the SMF performs one of the following actions:

- Ignore
- Continue
- Terminate

The SMF provides the following actions to attempt the same request to other available UDM servers.

- retry-and-terminate
- retry-and-ignore
- retry-and-continue

When all the retry attempts fail, the SMF takes the appropriate failure handling action. For example, if the FH action is retry-and-terminate, the SMF terminates the call after all the attempts fail.



**Note** The SMF allows dynamic changes to the failure handling template configuration. Any changes to the configuration apply only to the new calls.

**Table 161: Relationship between N10 Messages and Failover Actions**

Scenario	Service	Message	Condition	Action	Success Response	Handling of Failure Response		
						Terminate	Continue	Ignore
PDU Session Creation procedures in 5G, 4G, WiFi  Inter-RAT Handover procedures	UECM	Nudm_UECM_Registration	If the Nudm UECM Registration is not done and the access type is not 4G	Send the message	Mark the Registration is successful	Terminate call	Continue call	Continue call
		Nudm_UECM_DeRegistration	If the Nudm UECM Registration is done	Send the message	No action	Terminate call	Terminate call	Terminate call
PDU Session Creation procedures in 5G, 4G, WiFi	SDM	Nudm_SDM_Get	If skipping the subscription fetch config is not enabled	Send the message	Mark the subscription fetch is successful	Terminate call	Continue call	Continue call
		Nudm_SDM_Subscribe	If the subscription fetch is successful	Send the message	No action	Terminate call	Continue call if the subscription is not done	Continue call if the subscription is not done
PDU Session Release procedures in 5G, 4G, WiFi	SDM	Nudm_SDM_Unsubscribe	If the subscription fetch is successful and the registration is successful	Send the message	No action	Terminate call	Continue call	Continue call

**Note**

- **Terminate:** The SMF terminates the call in any message type.
- **Continue:** The SMF ignores the current failure and skips the subsequent interaction for the other messages in the same service group.
- **Ignore:** The SMF ignores failure only for the current interaction and proceeds with the call. The SMF processes the subsequent message interaction.
- Perform UDM subscription fetch only during the session establishment in EPS and NR network.  
If the UDM subscription fetch fails and the FH action is 'Ignore' or the configuration to skip subscribe-to-notification is enabled, then the SMF skips the subscribe-to-notification interaction.
- When the UDM failure handling template is not configured, the default failure handling action is 'Terminate'.

## Configuring UDM Failure Handling Support

### Configuring UDM Failure Handling Profile

Use the following sample configuration to configure the UDM failure handling profile with action.

```

config
  profile nf-client-failure nf-type udm
    profile failure-handling fh_profile_name
      service name type { nudm-ee | nudm-pp | nudm-sdm | nudm-ueau
        | nudm-uecm }
      message type { UdmRegistrationReq | UdmSdmGetUESMSSubscriptionData
        | UdmSdmSubscribeToNotification | UdmSubscriptionReq
        | UdmUecmRegisterSMF | UdmUecmUnregisterSMF |
        UdmSdmUnsubscribeToNotification }
      status-code httpv2 0
      action { continue | retry-and-continue | retry-and-ignore
        | retry-and-terminate | terminate }
    end
  end

```

### Configuring Association of FH profile

Use the following sample configuration to configure the association of FH profile in the respective network element.

```

config
  profile network-element udm udmprofile_name
    nf-client-profile profile_name
    failure-handling-profile fh_profile_name
    failure-handling-profile-rat nr fh_rat_profile_name
    query-params [ dnn ]
    rulebase-prefix cbn#
    predefined-rule-prefix crn#
  end

```

```
response-timeout timeout_duration
exit
```

**NOTES:**

- **failure-handling-profile-rat nr** *fh\_rat\_profile\_name*: Specify the failure handling profile specific to RAT type. *fh\_rat\_profile\_name* must be a string representing the corresponding NRF failure handling network profile name.
- **response-timeout** *timeout\_duration*: Specify the response timeout in milliseconds.

Default: 4000

**Verifying the RAT based FH Profile**

This section describes how to verify RAT based FH profile in the respective network element.

Use the **show running-config profile network-element udm profile network-element udm** *udmprofile\_name* command to verify the feature configuration details.

The following is a sample output.

```
nf-client-profile UPl
failure-handling-profile FH1
query-params [ dnn ]
failure-handling-profile-rat nr
failure-handling-profile FH4
exit
exit
```

**Configuring Secondary and Tertiary IP Addresses**

Use the following sample configuration to configure secondary and tertiary IP addresses.

```
config
  profile nf-client nf-type udm
    udm-profile udmprofile_name
    locality LOC
    priority priority_value
    service name type { nudm-ee | nudm-pp | nudm-sdm |
      nudm-ueau | nudm-uecm }
    endpoint-profile epprofile_name
    capacity capacity_value
    uri-scheme http
    endpoint-name endpoint_name
    priority priority_value
    primary ip-address ipv4 primary_ipaddress
    primary ip-address port port_num
    secondary ip-address ipv4 secondary_ipaddress
    secondary ip-address port port_num
  end
```

**Configuring Response Timeout Handling**

Use the following configuration to configure response timeout for fail-open support over the UDM interface (N10).

```

config
  profile network-element udm udm_profile_name
    response-timeout timeout_value
  exit

```

**NOTES:**

- **response-timeout** *timeout\_value*: Configures the response timeout in milliseconds.

**Verifying the Response Timeout Handling Configuration**

The following is a sample configuration.

```

[unknown] smf# show running-config profile network-element udm
profile network-element udm udm1
nf-client-profile UP1
failure-handling-profile FH4
query-params [ dnn ]
response-timeout 2000
exit
[unknown] smf#

```

**Statistics**

New statistics added for all the UDM message status with status as Attempted/Success/Skipped/Failed for all UDM services and message combination.

```

udm_msg_processing_status{app_name="SMF",cluster="Local",data_center="DC",
instance_id="1",msg_status="attempted",rat_type="nr",service_name="smfservice",
udm_end_point="",udm_msg="UdmSmSubscription"} 1

udm_msg_processing_status{app_name="SMF",cluster="Local",data_center="DC",
instance_id="1",msg_status="skipped",rat_type="nr",service_name="smfservice",udm_end_point="",
udm_msg="UdSmSubscription"} 1

```

**UDM Failure Handling OAM Support**

This section describes the operations, administration, and maintenance information for this feature.

**Statistics Support**

The SMF maintains the following statistics in support of the UDM Failure Handling feature.

- Nudm\_UECM\_Registration
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- Nudm\_UECM\_DeRegistration
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses

- Nudm\_SDM\_Get
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- Nudm\_SDM\_Subscribe
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses
- Nudm\_SDM\_Unsubscribe
  - Number of ignore responses
  - Number of continue responses
  - Number of terminate responses

The "udm\_msg\_processing\_status" statistic in smf-service tracks the number of UDM messages with status as — Attempted, Success, Skipped, Failed

For example:

```
udm_msg_processing_status
{app_name="SMF",cluster="Local",data_center="DC",instance_id="1",msg_status="attempted",
rat_type="nr",
service_name="smf-service",udm_end_point="",udm_msg="UdmSmSubscription"} 1
udm_msg_processing_status
{app_name="SMF",cluster="Local",data_center="DC",instance_id="1",msg_status="skipped",
rat_type="nr",
service_name="smf-service",udm_end_point="",udm_msg="UdSmSubscription"} 1
```

# User Plane Function Failure Handling

## Feature Description

During a session, if the User Plane function (UPF) is in congested state, it rejects the Packet Forwarding Control Protocol (PFCP) establishment messages from SMF with a cause code in the response message. To reduce call loss, the SMF retries to send PFCP establishment messages to a different UPF. Then, SMF selects a UPF based on priority (configuration) and capacity (load information from UPF).

The UPF failure handling support on N4 interface feature in SMF introduces a new failure handling template (FHT) profile for PFCP. This profile is associated with the UPF profile in SMF (in network elements).

The FHT template provides flexibility for SMF to fine tune its interactions with UPFs for sessions. It supports SMF to handle the error cause codes in response from UPF for both new and existing sessions. Based on the error cause codes in response from UPF, this feature provides the following configurable actions:

- terminate

- `retry-terminate`

## Configuring the UPF Failure Handling on N4 Interface

Use the following sample configuration to configure the UPF failure handling on N4 interface.

```
config
  profile failure-handling pfcp_name
    interface pfcp message { N4SessionEstablishmentReq |
N4SessionModificationReq }
    cause-code pfcp-entity-in-congestion
    action retry-terminate max-retry value
  end
```

### NOTES:

- **profile failure-handling**: Specify the UPF profile that is associated with FHT.
- **interface pfcp message { N4SessionEstablishmentReq | N4SessionModificationReq }**: Specify the failure handling for N4SessionEstablishmentReq (for new sessions) and N4SessionModificationReq messages (for existing sessions).




---

**Note** UPF reselection is not applicable for message type N4SessionModificationReq because the session is already active on a UPF.

---

- **cause-code { pfcp-entity-in-congestion | mandatory-ie-incorrect | mandatory-ie-missing | session-ctx-not-found | system-failure | service-not-supported | no-resource-available | no-response-received | reject }**: Specifies the error codes that SMF receives in the failure response message from UPF.




---

**Note**

- The **no-response-received** cause code is introduced in this feature to identify the scenarios where SMF does not receive any response from UPF.
- FHT does not support the following cause codes, which are configured with their default behaviour:  
**request-reject-unspecified, cond-ie-missing, invalid-length, invalid-fw-policy, invalid-fteid-alloc-opt, no-established-pfcp-assoc, rule-creation-mod-failure.**

---

- **pfcp-entity-in-congestion**: Specify the cause code when UPF is congested.
- **reject**: Specify the option to handle the cause codes in the failure response message from UPF, which are not configured by using the CLI commands available for this feature.
- **action { retry-terminate | terminate }**: Specify the action to perform based on the error cause code received in the failure response message from UPF.
  - **retry-terminate**: Specifies a retry attempt to an alternate UPF. If the retry attempt fails, the session is terminated.




---

**Note** If all UPFs are in congested state, call fails even if the action is set to **continue**.

---

- **max-retry**: Specifies the number of retry attempts to reselect an alternate UPF.
  - **Default value**: 2
  - **Maximum value**: 5

### Verifying the UPF Failure Handling Configuration

Use the **show running-config** command to view the configuration.

The following is a sample output of the **show running-config** command.

```
show running-config
profile network-element upf upf1
pfcpl pfcpl-failure-profile pfcpl
node-id      n4-peer-upf1
n4-peer-address ipv4 1.1.1.1
n4-peer-port 0000
keepalive    60
dnn-list     [ uncarrier.5g ]
capacity     10
priority     1
exit
profile failure-handling pfcpl
interface pfcpl message N4SessionEstablishmentReq
cause-code pfcpl-entity-in-congestion
action retry-terminate max-retry 2
exit
exit
interface pfcpl message N4SessionModificationReq
cause-code mandatory-ie-incorrect
action terminate
exit
exit
exit
```

## Configuring the Failure Profile Association

Use the following sample configuration to configure the failure profile association.

```
config
  profile upf-group upf upf_group_name
    failure-profile pfcpl_name
  end
```

#### NOTES:

- **profile upf-group upf upf\_group\_name**: Specify the UPF group.
- **failure-profile pfcpl\_name**: Specify the FHT profile for PFCP.



## Configuration Matrix

This section describes the configuration options available for N4 Session Establishment Request and N4 Session Modification Request messages.

Message Type	Applicable Action	Applicable Cause Code	Default Behaviour
N4SessionEstablishmentReq	retry-terminate	<ul style="list-style-type: none"><li>• pfc-p-entity-in-congestion</li><li>• system-failure</li><li>• service-not-supported</li><li>• no-resource-available</li><li>• no-response-received</li></ul>	terminate
N4SessionModificationReq	terminate	<ul style="list-style-type: none"><li>• mandatory-ie-incorrect</li><li>• session-ctx-not-found</li><li>• no-response-received</li></ul>	continue





# CHAPTER 34

## PDU RAN Tunnel Endpoint Identifier Session

- [Feature Summary and Revision History, on page 517](#)
- [Feature Description, on page 518](#)
- [Always-On PDU Session Support, on page 521](#)

### Feature Summary and Revision History

#### Summary Data

*Table 162: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 163: Revision History*

Revision Details	Release
Introduced support for the selection of UPF nodes based on the query parameters such as DNN, location, and PDU session type.	2020.03.0
First introduced.	Pre-2020.02.0

## Feature Description

The SMF supports activation and deactivation of the user plane connection of a PDU session.

### How it Works

The SMF-service labels account for the active-to-idle and idle-to-active transitions. Existing idle and connected counters track the number of PDU sessions that are currently active or idle.

Label	Description
PROCEDURE TYPE	Supported counters for the label: ue_req_active_to_idle ue_req_idle_to_active

### Deactivation of the User Plane Connection of a PDU Session

This procedure is used to release the logical NG-AP signaling connection and the associated N3 user plane connections, and (R)AN RRC signaling and resources.

The following reasons may trigger the initiation of AN release:

- (R)AN-initiated with cause. For example, O&M Intervention, unspecified failure. (R)AN (For example, Radio) link failure, user inactivity, inter-system redirection, request for establishment of QoS flow for IMS voice, release due to UE generated signaling connection release, mobility restriction and so on.
- AMF-initiated with cause. For example, unspecified failure.

### Limitations

- In this release, SMF supports only UE-initiated deactivation.
- Location update is not supported.

Call Flow

Figure 101: Deactivation of the User Plane Connection of a PDU Session Call Flow

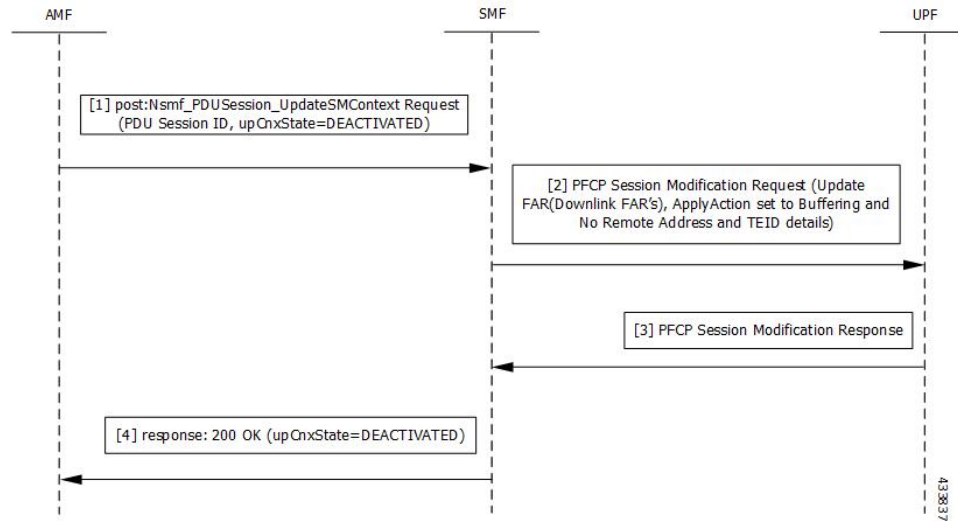


Table 164: Deactivation of the User Plane Connection of a PDU Session Call Flow Description

Step	Description
1	NF Service Consumer requests the SMF to deactivate the user plane connection of the PDU session by sending a POST request with the following information: <ul style="list-style-type: none"> <li>• upCnxState attribute set to DEACTIVATED.</li> <li>• User location and user location timestamp.</li> <li>• Cause of the user plane deactivation. The cause may indicate a cause received from the 5G-AN or due to an AMF internal event.</li> <li>• Other information (if required).</li> </ul>
2	SMF deactivates and releases the N3 tunnel of the PDU session after receiving such a request. SMF initiates PFCP session modification procedure towards UPF with downlink FAR updated with the following options: <ul style="list-style-type: none"> <li>• Buffering Action is enabled without remote node “forwarding parameters” details like IP address and GTP-U F-TEID.</li> </ul> <p><b>Note</b> NOCP (Notify the CP function) is not enabled. Support for notification is not available on SMF.</p>
3	SMF sets the upCnxState attribute to DEACTIVATED for the PDU session after receiving successful response from UPF node.
4	SMF initiates 200 OK response including the upCnxState attribute set to DEACTIVATED towards AMF.

## Activation of the User Plane Connection of a PDU Session

The service request procedure is used when the UE is in CM-IDLE and in CM CONNECTED to activate a user plane connection for an established PDU session. The UE in CM IDLE state initiates the service request procedure to send uplink signaling messages, user data or as a response to a network paging request.

### Limitations

- In this release, SMF supports only UE-initiated service requests.
- Paging and network-initiated service requests are not supported.
- Location update and access-type changes are not supported.
- QoS flow modifications and errors are not supported.

### Call Flow

**Figure 102: Activation of the User Plane Connection of a PDU Session Call Flow**

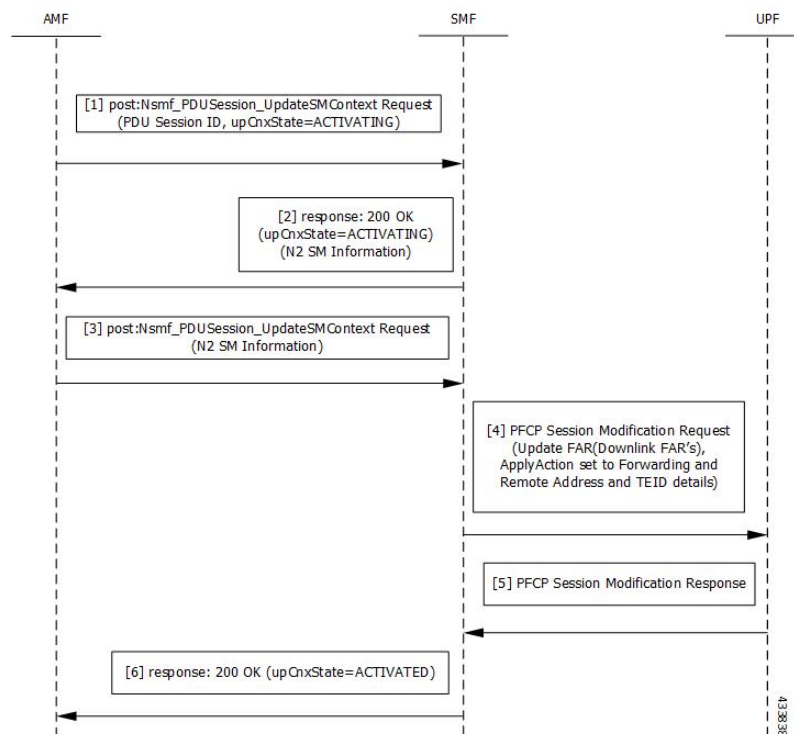


Table 165: Activation of the User Plane Connection of a PDU Session Call Flow Description

Step	Description
1	AMF requests the SMF to activate the user plane connection of the PDU session by sending a POST request with the following information: <ul style="list-style-type: none"> <li>• upCnxState attribute set to ACTIVATING.</li> <li>• User location, user location timestamp, and access type associated to the PDU session (if modified)</li> <li>• Other information (if required).</li> </ul>
2	SMF starts activating the N3 tunnel of the PDU session after receiving the request. SMF returns a 200 OK response including the following information: <ul style="list-style-type: none"> <li>• upCnxState attribute set to ACTIVATING.</li> <li>• N2 SM information to request the 5G-AN to assign resources to the PDU session including the transport layer address and tunnel endpoint of the uplink termination point for the user plane data for this PDU session that is UPF's GTP-U F-TEID for uplink traffic.</li> </ul>
3	AMF requests the SMF by sending POST request, with the following information: <ul style="list-style-type: none"> <li>• SM information received from the 5G-AN, including the transport layer address and tunnel endpoint of the downlink termination point for the user data for this PDU session, 5G-AN's GTP-U F-TEID for downlink traffic if the 5G-AN succeeded in establishing resources for the PDU sessions.</li> </ul>
4	SMF initiates PFCP session modification procedure towards UPF with down link FAR updated with following options: <ul style="list-style-type: none"> <li>• Forwarding Action is enabled with remote node “forwarding parameters” details like IP address and GTP-U F-TEID.</li> </ul>
5	SMF sets the upCnxState attribute to ACTIVATED for the PDU session after receiving successful response from UPF node.
6	SMF initiates 200 OK response including the upCnxState attribute set to ACTIVATED towards AMF.

## Always-On PDU Session Support

### Feature Description

Applications like the IP Multimedia Subsystem (IMS) require an always-on Protocol Data Unit (PDU) session that the User Plane resource establishes for every transition from the 5GMM-IDLE mode to the 5GMM-CONNECTED mode. The UE requests the establishment of a PDU session as an always-on PDU session based on the request indication of the upper layers. It is the network that decides whether to establish a PDU session as an always-on PDU session.

# How it Works

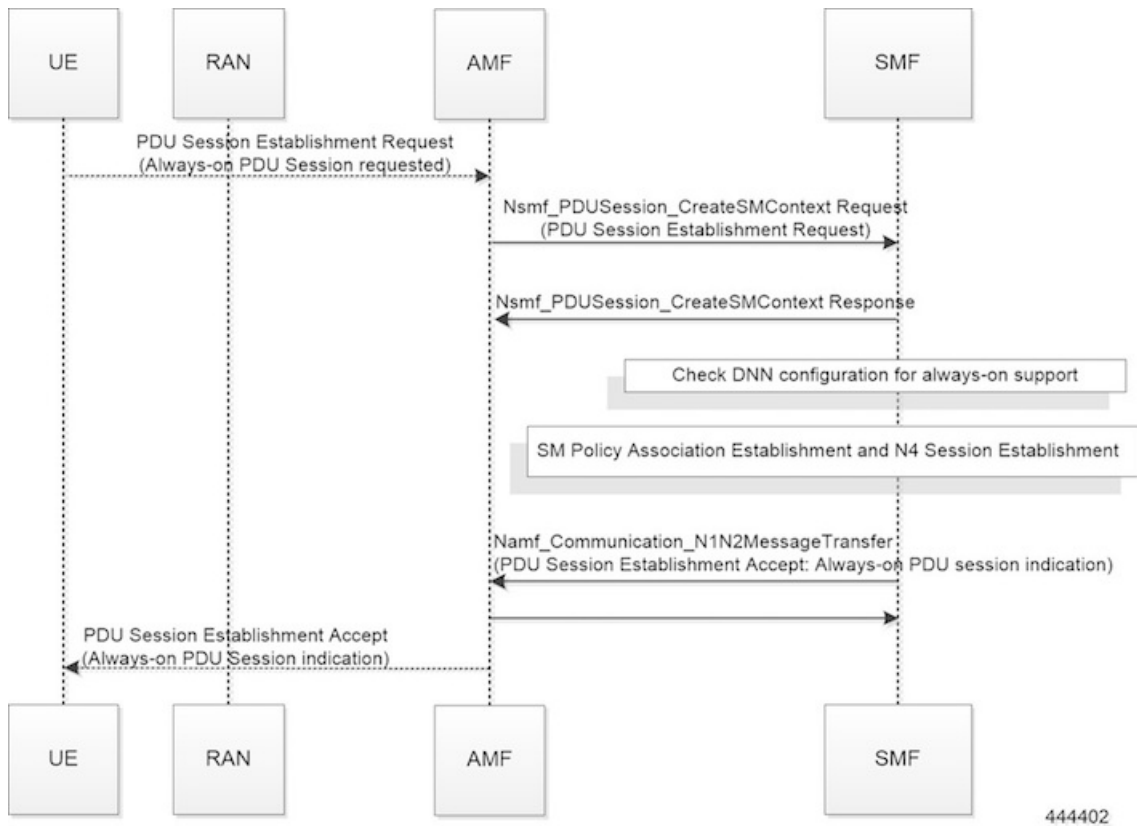
## Call Flows

This section describes the following call flows.

### PDU Session Establishment Call Flow

This section describes the call flow of the PDU session establishment.

Figure 103: PDU Session Establishment Call Flow



444402

Table 166: PDU Session Establishment Call Flow Description

Step	Description
1	If the UE requests to establish an always-on PDU session, the UE includes an "Always-on PDU Session Requested" IE in the PDU Session Establishment Request message.
2	The SMF checks the DNN profile to determine whether the always-on support is enabled.

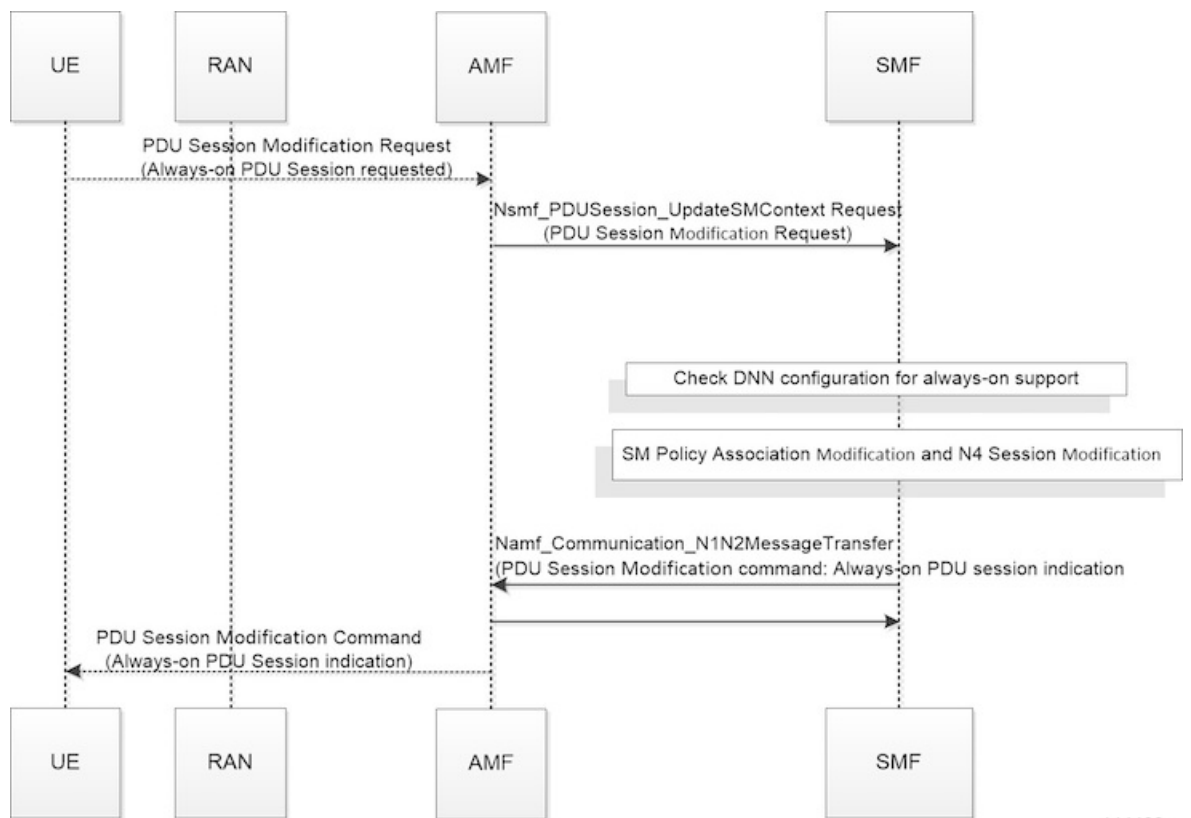


Step	Description
3	<p>The SMF includes an "Always-on PDU Session Indication" in the PDU Session Establishment Accept message if any one of the following is true:</p> <ul style="list-style-type: none"> <li>"Always-on PDU Session Indication" is sent with value as "enabled" if the always-on configuration is enabled under the DNN profile.</li> <li>"Always-on PDU Session Indication" is sent with value as "disabled" when the "Always-on PDU Session Request" IE is received and configuration is disabled.</li> </ul>
4	<p>The SMF does not include an "Always-on PDU Session Indication" only when both these conditions are true:</p> <ul style="list-style-type: none"> <li>If the UE did not send an "Always-on PDU Session Requested" IE.</li> <li>If always-on configuration is disabled in the DNN profile.</li> </ul>

**UE-Requested PDU Session Modification Call Flow**

This section describes the call flow of the UE-requested PDU session modification.

*Figure 104: UE-Requested PDU Session Modification Call Flow*



444403

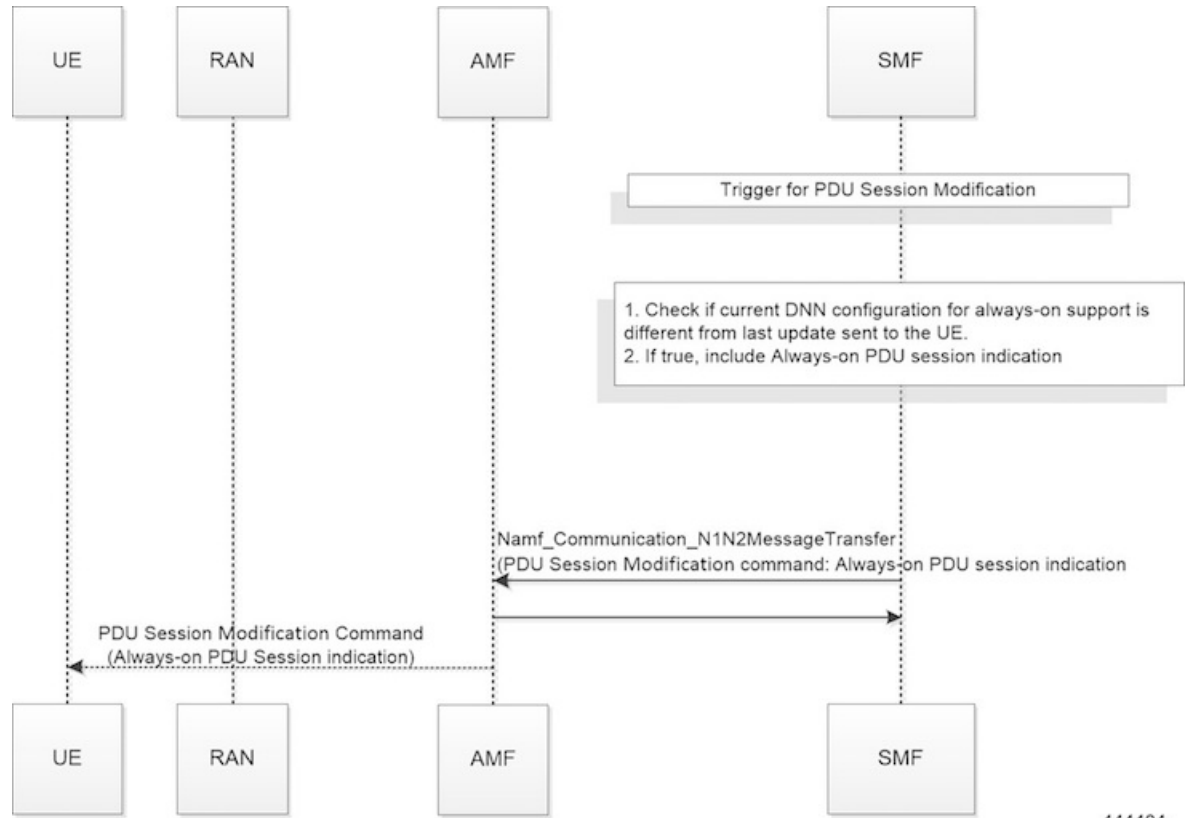
Table 167: UE-Requested PDU Session Modification Call Flow Description

Step	Description
1	The UE sends an "Always-on PDU Session Requested" IE in the PDU Session Modification Request message.
2	The SMF checks the DNN profile to determine whether the always-on support is enabled.
3	The SMF includes "Always-on PDU Session Indication" in the PDU Session Modification Command when any one of the following is true: <ul style="list-style-type: none"> <li>• "Always-on PDU Session Indication" is sent with the value as "enabled" when the always-on configuration is enabled under the DNN profile.</li> <li>• "Always-on PDU Session Indication" is sent with the value as "disabled" when the "Always-on PDU Session Request" IE is received and configuration is disabled.</li> </ul>
4	The SMF does not include the "Always-on PDU Session Indication" only when both these conditions are true: <ul style="list-style-type: none"> <li>• If the UE did not send the "Always-on PDU Session Requested" IE.</li> <li>• If always-on configuration is disabled in the DNN profile.</li> </ul> <p><b>Note</b> As per 3GPP TS 23502, for a PDU session that was established in the EPS, when the UE moves from EPS to 5GS for the first time, the UE includes an "Always-on PDU Session Requested" indication in the PDU Session Modification Request message if it wants to change the PDU session to an "always-on" PDU session.</p>

### Network-Requested PDU Session Modification Call Flow

This section describes the call flow of the network-requested PDU session modification.

Figure 105: Network-Requested PDU Session Modification Call Flow



444404

Table 168: Network-Requested PDU Session Modification Call Flow Description

Step	Description
1	The SMF decides to trigger a PDU Session Modification due to PCF, UDM, or RAN initiated procedures.
2	The SMF checks the DNN profile to determine whether the always-on support is enabled.
3	The SMF determines whether the current DNN configuration for always-on is different from the last indication sent to UE. If it differs, the SMF includes the "Always-on PDU Session Indication" IE in the PDU Session Modification Command message.

## Configuring Always-On PDU Session Support

Use the following sample configuration to configure always-on PDU session under the DNN profile.

```

config
  profile dnn name
    always-on { true | false }
  end
    
```

- **always-on** { **true** | **false** }: Enables or disables always-on PDU session support.

- **true**: Enables always-on PDU session.
- **false**: Disables always-on PDU session.

## Verifying Always-On PDU Session Support

Use the **show subscriber supi *supi\_id*** CLI command to verify the always-on PDU session support.



**Note** The show output for always-on PDU session support displays any one of the following options:

- “alwaysOn”: “UE Requested”
- “alwaysOn”: “Enabled”
- “alwaysOn”: “UE Requested & Enabled”

The following is a sample output of the command:

```
show subscriber supi imsi-123456789012345
subscriber-details
{
  "status": true,
  "genericInfo": {
    "supi": "imsi-123456789012345",
    "pei": "imei-123456786666660",
    "pduSessionId": 5,
    "pduSesstype": "Ipv4PduSession",
    "accessType": "ACCESS_5G",
    "dnn": "intershat",
    "plmnId": {
      "mcc": "123",
      "mnc": "456"
    },
    "sScMode": 1,
    "uetimeZone": "UTC+12:00",
    "allocatedIp": "12.0.4.4",
    "nrLocation": {
      "ncgi": {
        "mcc": "123",
        "mnc": "456",
        "nrCellId": "123456789"
      },
      "tai": {
        "mcc": "123",
        "mnc": "456",
        "tac": "1820"
      }
    }
  },
  "alwaysOn": "UE Requested"
},
"accessSubData": {
  "amfID": "AFbe08",
  "amfPlmnId": {
    "mcc": "123",
    "mnc": "456"
  },
  "ueCmStatus": "UeCMConnected",
  "amfNrfID": "76517361-338e-4d77-bc76-713a79779574"
```

```

    },
    "policySubData": {
      "TotalDynamicRules": 1,
      "TotalFlowCount": 1,
      "TotalNonGBRFlows": 1,
      "pccRuleList": [
        {
          "pccRuleId": "defaultrule",
          "qfi": 1,
          "mbrDl": 125000000,
          "mbrUl": 100000000,
          "flowInformation": [
            {
              "flowDirection": 3,
              "flowDescription": "permit out ip from any to any"
            }
          ]
        }
      ]
    },
    "qosFlow": [
      {
        "qfi": 1,
        "GBRFlow": "False",
        "bindingParameters": {
          "x5Qi": 5,
          "arp": {
            "preemptCap": 1,
            "preemptVuln": 1,
            "priorityLevel": 15
          },
          "priorityLevel": 1
        },
        "AggregatedULMFbr": 100000000,
        "AggregatedDLMFbr": 125000000,
        "pccRuleList": "defaultrule"
      }
    ]
  },
  "chargingData": {},
  "upfServData": {
    "numberOfTunnels": 1,
    "smfSeid": 21790984727,
    "UPState": "Activated",
    "mapping": {
      "tunnelMapping": [
        {
          "TunnelID": 1,
          "tunnelName": "gnbTunnel"
        }
      ]
    }
  }
}

```

## Always-On PDU Session OAM Support

This section describes operations, administration, and maintenance information for this feature.

### Bulk Statistics Support

The Always-On PDU Session feature supports the following bulk statistics.

Table 169: Always-On PDU Session Bulk Statistics

Bulk Statistics	Description
always-on-pdu	Tracks the number of always-on PDU sessions.
Always-on-pdu-requested	Requests the always-on PDU session.
always-on-pdu-accepted	Accepts the always-on PDU session request.
Always-on-pdu-rejected	Rejects the always-on PDU session request.
pdusetup_req_alwayson_requested	The number of session establishment requests received with "Always-On PDU Session Requested".
pdusetup_acc_alwayson_allowed	The number of session establishment accept messages sent with "Always-On PDU Session Indication" enabled.
pdusetup_acc_alwayson_not_allowed	The number of session establishment accept messages sent with "Always-On PDU Session Indication" disabled.
pdumod_req_alwayson_requested	The number of session modification requests received with "Always-On PDU Session Requested".
pdumod_cmd_alwayson_allowed	The number of session modification commands sent with "Always-On PDU Session Indication" enabled.
pdumod_cmd_alwayson_not_allowed	The number of session modification commands sent with "Always-On PDU Session Indication" disabled.
pdumod_cmd_nw_init_alwayson_allowed	The number of network initiated session modification commands sent with "Always-On PDU Session Indication" enabled.
smf_session_counters	The gauge to show the number of active always-on PDU sessions.



## CHAPTER 35

# Policy and User Plane Management

- [Feature Summary and Revision History, on page 529](#)
- [Feature Description, on page 530](#)
- [QoS Management on SMF, on page 531](#)
- [Handling of Authorized QoS for Default Bearer, on page 538](#)
- [SMF Affinity, on page 541](#)
- [Dynamic Configuration Change Support, on page 542](#)
- [Dynamic PCC Rules Enforcement, on page 544](#)
- [Static PCC Rules Support, on page 554](#)
- [Predefined PCC Rules, on page 570](#)
- [Support for Configuring the Bandwidth ID, on page 571](#)
- [Generating UE Camping Report for PCF, on page 573](#)
- [UPF Node Selection, on page 573](#)
- [Support for UPF Node Reports and Proprietary Session Reports, on page 585](#)
- [Support for Session Report Rejection Procedure, on page 590](#)
- [Outer Header Format, on page 592](#)

## Feature Summary and Revision History

### Summary Data

**Table 170: Summary Data**

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

## Revision History

*Table 171: Revision History*

Revision Details	Release
Introduced support for the following: <ul style="list-style-type: none"> <li>• Co-located UPF Selection</li> <li>• Enhanced Limits for Maximum Groups in Bandwidth Policy Configuration</li> <li>• Handling Session Report Rejection Procedure</li> <li>• New Format of Outer Header information element (IE)</li> </ul>	2021.01.0
Introduced support for the following: <ul style="list-style-type: none"> <li>• UPF node selection based on DNN and PDU Session type</li> <li>• Modification of authorized default QoS</li> <li>• Additional session report and UPF node report request</li> </ul>	2020.03.0
First introduced.	Pre-2020.02.0

## Feature Description

The SMF is one of the control plane NFs that provide the Session Management service in the 5G core network. The SMF manages the PDU session lifecycle through the following session management procedures:

- PDU Session Establishment
- PDU Session Modification
- PDU Session Release

This chapter describes the policy and user plane management features.

- **Policy Management**—Policy Control Function (PCF) or the local configuration controls the policies managed on SMF. The PCF sends Policy and Charging Control (PCC) rules along with the applicable QoS and charging information to the SMF. The SMF uses this information to define QoS flows and apply QoS enforcement (via User Plane Function (UPF) and charging towards Charging Function (CHF). The PCC rules can be configured locally as well. The locally configured policy rules are labelled as static or predefined rules.
- **User Plane Management**—The user plane management on SMF includes selection of UPF and maintaining per session and node level user plane data. The SMF performs Path management of the UPF nodes. At a per session level, SMF publishes the Packet Detection Rules (PDRs), QoS Enforcement Rules (QERs),



Forwarding Action Rules (FARs), and Usage Reporting Rules (URRs) to the UPF. Then, the SMF enforces the policy rules received from PCF or configured locally.

# QoS Management on SMF

## Feature Description

The primary functionality of the SMF is to manage the flow-based QoS model. SMF interacts with the Unified Data Management (UDM) and Policy Control Function (PCF) to get the subscribed and authorized QoS parameters for GBR and non-GBR flows and passes on the relevant information to UE (NAS), gNB (NGAP), and UPF (PFCP) so that all nodes on the network provide the desired QoS to the PDU session.

## Use Cases

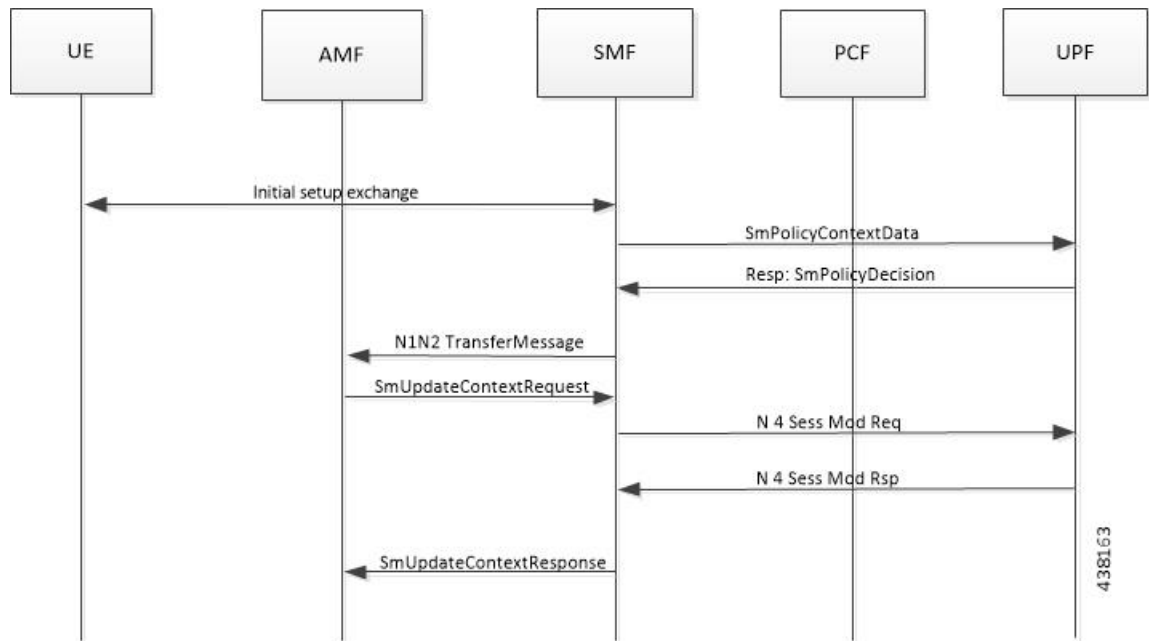
This section describes the various use case scenarios that can lead to creation, modification, and deletion of QoS-Profile and the corresponding actions taken.

QoS-Profile associated to the PDU Context will be modified in the following scenarios:

- Response from PCF for SMPolicyContextData
- Update Notify from PCF
- Update response from PCF on behalf of Update request sent initially from SMF
- Update request from SMF will be triggered in the following cases:
  - UE triggered modify request
  - AN triggered modify request
  - UDM triggered modify request

## Setup Creation

Figure 106: Setup Creation

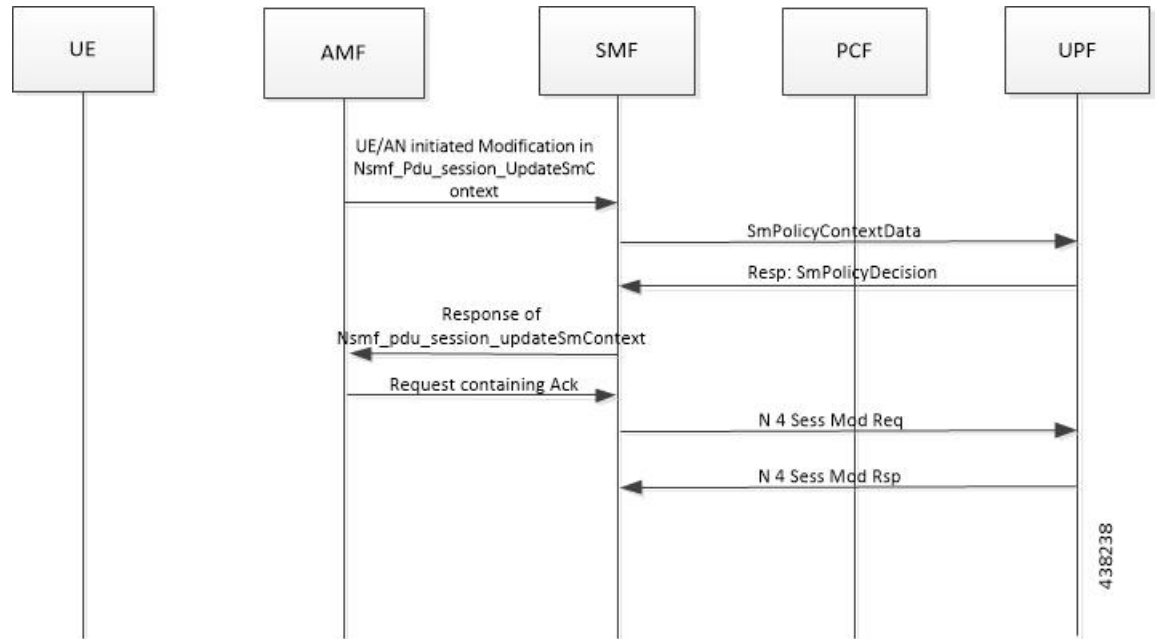


Based on the content received in SMPolicyDecision, SMF pushes the following towards various interfaces.

- UPF:
  - Set of PDR derived from PCC rules
  - Set of QER derived from QoS flows which in turn are derived from QoSDescription/QoSCharacteristics from PCF
  - One extra QER that will be shared will be derived from SessRules
- N1:
  - Set of QoS rules derived from QoSFlows
  - Each QoSRule has its associated packet filter
- N2:
  - Set of QoS Flow information

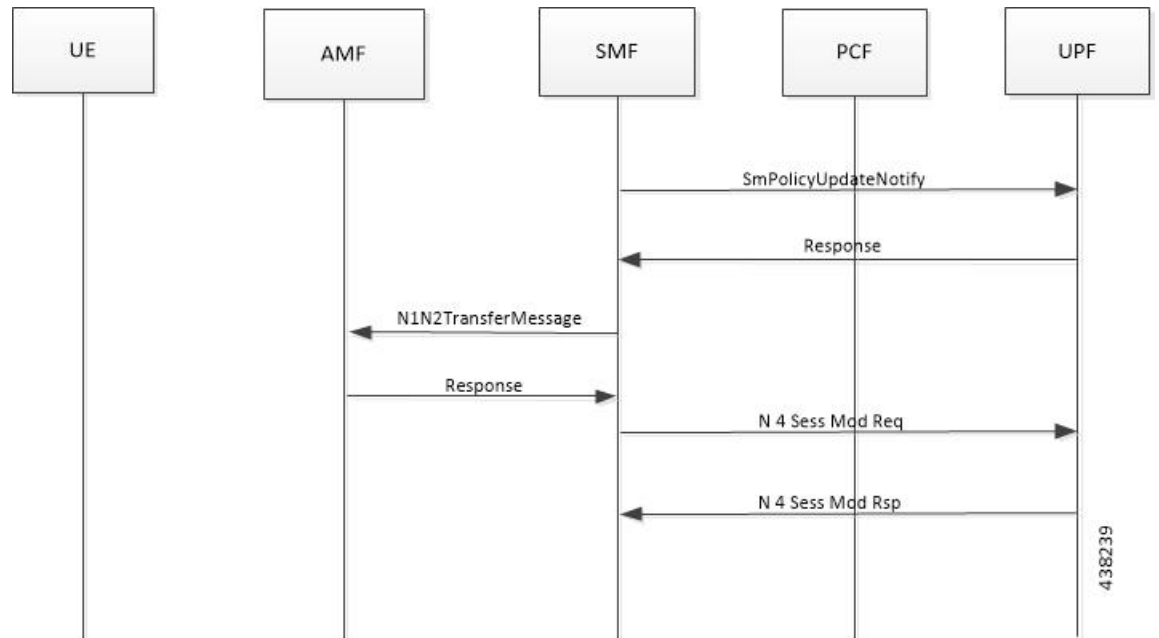
UE/AN-initiated Modify

Figure 107: UE/AN-initiated Modify



UDM/PCF-initiated Modify

Figure 108: UDM/PCF-initiated Modify



• N1:

- PDU Session Modification command will be triggered from SMF. It can change Session-AMBR and QoS rules.
- PDU Session Modification Request will be triggered from UE. It can change the QoS rules and maximum number of support-ed packet filters.

In either case, the QoS rule change can happen from the following:

- Packet filter add/delete/replace
  - Rule Precedence of QoS Rule
  - QoS Parameter – 5QI/MBR/GBR
- N2:
    - PDU Session Resource Modify Request will be triggered from SMF. It can change the existing QoS flow that is installed or delete the QoS flow already installed. If the Modify request is received, the parameters - ARP, GBR/MBR, Priority level, and so on, can change.
    - PDU Session Resource Notify will be triggered from AN. This happens when certain flow is to be released, not fulfilled any-more and fulfilled again.

## Subscribed QoS

The UDM NF maintains the subscribed QoS for the UE in the Session Management Subscription Data. During the PDU setup procedure, the SMF posts an HTTP2 GET request (see *3GPP TS 29.503*) for a resource URI "/{supi}/sm-data" to fetch the Session Management Subscription Data. The subscription data has a set of DNN configurations, one for each DNN which the subscriber is allowed to access. Each DNN configuration consists of the following parameters:

- sessionAMBR: The maximum aggregated uplink and downlink bit rates to be shared across all non-GBR QoS flows in each PDU session.
- 5gQosProfile: The default 5G QoS Indicator (5QI) and default ARP values are provided to the SMF in the Session Management Subscription Data in this attribute of the DNN configuration.

The SMF saves the subscribed QoS parameters and sends this across to the PCF during the SM Policy Association Establishment procedure.

## QoS Negotiation

The SMF negotiates the QoS with the PCF by initiating a Policy Association Establishment procedure as defined in *3GPP TS 23.502, section 4.16.4*. The sessionAMBR and 5gQosProfile parameters that are received from subscription are included in the Npcf\_SMPolicyControl\_Create request to PCF. The response from PCF may contain the following:

- Session Rules: A session rule consists of policy information elements that are associated with the PDU session. The QoS related information is Authorized session AMBR and Authorized default QoS.
- Policy Charging and Control (PCC) Rules: The PCC rule includes the FlowDescription, FlowDirection, and RefQosData parameters among other information. There could be one or more PCC rules in the response from PCF.

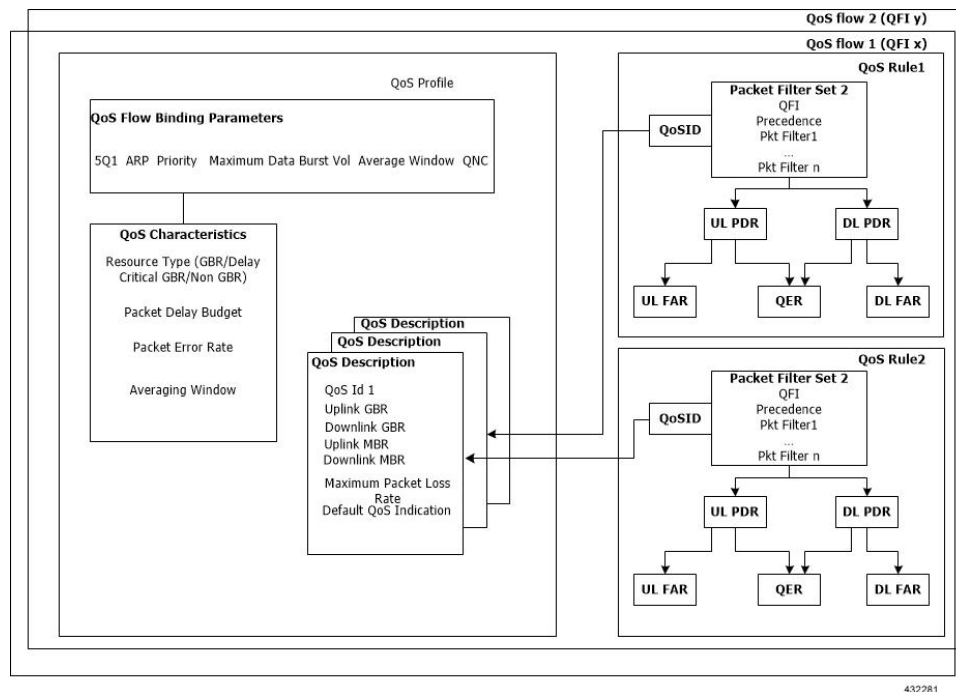
- FlowDescription: This parameter contains packet filters for IP flows. For IP PDU Session Type, the Packet Filter Set supports packet filtering based on at least any combination of:
  - Source / Destination IP address or IPv6 prefix
  - Source / Destination port number
  - Protocol ID of the protocol above IP/Next header type
  - Type of Service (TOS) (IPv4) / Traffic class (IPv6) and mask
  - Flow Label (IPv6)
  - Security parameter index
- FlowDirection: This parameter indicates the direction of data traffic on which the rule has to be applied. This could be UPLINK, DOWNLINK, or BIDIRECTIONAL.
- RefQoSData: This parameter refers to the QoS description to be applied to this PCC Rule. This matches the QoSId of at least one of the QoS Description entries in the response from PCF.
- QoS Characteristics: The QoS characteristics include parameters such as:
  - Resource Type (GBR, Delay critical GBR, or non-GBR)
  - Priority Level
  - Packet Delay Budget
  - Packet Error Rate
  - Averaging Window
  - Maximum Data Burst Volume (for the Delay-critical GBR resource type only)  
This attribute in the response from PCF is meant to be used only for non-standard 5QI values. For standard 5QI values, the characteristics are already defined in *3GPP TS 23.501, section 5.7.4*.
- QoS Description: The QoS Description parameter consists of the following:
  - 5QI: Standard or non-standard from the QoS Characteristics attribute
  - Uplink and Downlink GBR
  - Uplink and Downlink MBR
  - Maximum Packet Loss Rate
  - QoSId – Referenced in PCC rules
  - Default QoS IndicationThere could be more than one QoS Description attribute in the response from PCF.

## QoS Flow Management

The information, that is received from PCF in the Npcf\_SMPolicyControl\_Create response, is used to create and update QoS Flows in the SMF. Each QoS flow has a unique QoS Flow ID (QFI) and one or more PCC rules map to a single QoS flow.

The following figure illustrates how to manage the QoS information at the SMF.

**Figure 109: QoS Information Management at SMF**



Each QoS Flow in SMF is a combination of three sets of information:

- QoS profile: A QoS profile stores all QoS attributes for a particular QoS Flow.
  - Some QoS parameters known as the QoS flow binding parameters make a unique combination for one QoS Flow of one PDU Session. This means that, for a PDU session, each unique combination of these parameters represents a separate QoS Flow. These parameters are – 5QI, ARP, Priority, Maximum Data Burst Volume, Average Window and QNC.
  - If the 5QI for the QoS profile of a QoS Flow is non-standard, some additional QoS characteristics such as Resource Type, Packet Delay Budget, Packet Error rate, and Averaging Window are also saved in the QoS profile.
  - The QoS profile also maintains multiple QoS Descriptions, each with a unique QoSId for a specific PDU session. Each QoS Description contains the uplink and downlink GBR, uplink and downlink MBR, maximum packet loss rate and default QoS indication.
- QoS Rules: A QoS rule is a collection of packet filters that associates with a particular QoS Description in the QoS profile of the QoS flow. The packet filters directly map to the flow descriptions received in the PCC rules in the Npcf\_SMPolicyControl\_Create response from PCF. The QoS rules have a reference to the QoSId of the QoS Descriptions that the rules associate with.

- PDRs: Each QoS rule maps to two Packet Detection Rules (PDR) to be sent to the UPF. One PDR is for uplink direction and the other PDR is for downlink direction. The Service Data Flow (SDF) filters in the Packet Detection Information (PDI) attribute within the PDRs map the packet filters of the QoS rule. Each PDR then maps to a Forwarding Action Rule (FAR), which determines the forwarding action for the packets matching the SDF filters. Each PDR is also associated to a QoS Enforcement Rule (QER) which carries the QoS information and it maps to the QoS description associated with the QoS rule.

## QoS Communication on 3GPP Interfaces

The negotiated QoS mainly needs to be communicated to the UE (N1 interface using NAS protocol), gNB (N2 interface using NGAP protocol), and UPF (N4 interface using PFCP protocol).

- N1 Interface: On the N1 interface, the session management messages are exchanged between UE and SMF through AMF. The NAS messages are encoded into an N1 container and sent to SMF or received from SMF.
  - All the negotiated/authorized QoS related information that needs to be sent out to the UE are found in the Authorized QoS rules and Session-AMBR attributes of the PDU SESSION ESTABLISHMENT ACCEPT message in an N1 container, during the PDU session establishment (see *3GPP TS 24.501, section 8.3.2*).
  - The PDU SESSION MODIFICATION REQUEST message from UE contains the Requested QoS Rules during the UE initiated QoS modification.
  - The Authorized QoS rules and Session-AMBR attributes are also present in the PDU SESSION MODIFICATION COMMAND message sent from SMF to UE during the PCF/SMF initiated QoS modification.
  - The format of the QoS Rule NAS attribute is defined in *3GPP TS 24.501, section 9.10.4.9*. This attribute mainly consists of the packet filter list, QFI, and QoS parameters on a per QoS rule basis. This information is available in the QoS rule within the QoS flow.
- N2 Interface: On the N2 interface, SMF sends an N2 container to the gNB through AMF. The N2 container is ASN.1 encoded data and consists of specific information elements of NGAP messages. All the QoS related information to gNB is encoded and sent/received in N2 containers to/from SMF. The NGAP IEs and the corresponding NGAP messages that will finally carry the IE from AMF to gNB are listed in *3GPP TS 29.502, section 6.1.6.4.3*.
  - During the PDU session setup, the SMF sends N1N2MessageTransfer to AMF with the N2 container in the PDU Session Re-source Setup Request Transfer IE. This IE contains PDU Session Aggregate Maximum Bit Rate and QoS Flow Setup Request List. The QoS Flow Setup Request List contains QoS Flow Level QoS Parameters (GBR flow information, 5QI, and so on). These are defined in *3GPP TS 38.413, section 9.3.1*.
  - Similar information (QoS Flow Level QoS Parameters) is also sent by SMF in the PDU Session Resource Modify Request Transfer IE in an N2 container during the PCF/SMF initiated QoS Modification procedure.
 

The information required to create the N2 container in SMF is present in the QoS profile of a QoS flow as described in the previous section.
- N4 Interface: On the N4 interface, the SMF sends the QoS information in the form of Packet Detection Rule (PDR), Forwarding Action Rule (FAR), and QoS Enforcement Rule (QER).

- The PDR contains the SDF filters in the PDI IE. These SDF filters are the packet filters set in the QoS Rule of a QoS flow.
- The QER contains the QoS parameters as per the QoS Description to which the QoS rule is associated. The contents of PDR, FAR, and QER are defined in *3GPP TS 29.244*.

## QoS Modification

QoS modification may result in one of the following scenarios:

- **QoS Flow Addition:** Whenever a negotiated QoS is received from PCF either as part of UE initiated modification or PCF initiated QoS modification, the SMF extracts the received QoS Flow Binding Parameters (5QI, ARP, Priority, Max Data Burst Volume, QNC). If there is no QoS Flow with the received combination of the flow binding parameters, SMF adds a new QoS flow and the received PCC rules will be mapped against the new QoS flow. As a result, the new QoS flow rules/QoS descriptions/PDR/QER are created and the corresponding interfaces (N1, N2, and N4) are updated by creating new flows.
- **QoS Flow Modification:** Whenever a negotiated QoS is received from PCF either as part of UE initiated modification or PCF initiated QoS modification, the SMF extracts the received QoS Flow Binding Parameters (5QI, ARP, Priority, Maximum Data Burst Volume, QNC). If there exists a QoS flow with the same combination of binding parameters, the QoS profile, QoS rules, PDR, and QER for that QoS flow are updated on N1, N2 and N4 interfaces.

# Handling of Authorized QoS for Default Bearer

## Feature Description

The CHF server interacts with PCF to report the user quota exhaustion. Then, the PCF initiates a policy update request towards SMF to modify the authorized default Quality of Service (QoS) of a session rule. The QoS can be QoS Class Identifier (QCI) or 5G QoS Indicator (5QI), session Aggregate Maximum Bit Rate (AMBR), or both QCI/5QI and session AMBR.

Whenever the quota of user exhausts, this QoS modification results in downgrading:

- the DSCP marking of the data packets for the session
- the AMBR of the session

When you replenish the quota, the PCF reverts to the previous authorized QoS for the default bearer.

Be aware of the following changes whenever the QCI/5QI changes for the default flow or bearer.

- The QCI/5QI information is updated in the Event Data Record (EDR) generated for that session. Then, the SMF sends the updated bearer level information over Packet Forwarding Control Protocol (PFCP) message to support the EDR functionality.
- DSCP marking for the data packets is updated for all Packet Detection Rules (PDRs) pertaining to the default bearer or flow.
- Any QCI information sent in LI packets are updated.



- Rulebase change and Ruledef activation or deactivation work as expected along with 5QI change and session AMBR change.
- Any modified QoS is sent in Charging Data Request (Update) message to the CHF. Also, change in QCI/5QI in the authorized QoS is treated as a QoS change trigger for charging and CDR-U is sent.

## How it Works

This section provides detailed changes in SMF to support change of QCI/5QI value in authorized QoS once the PDU session is established.

### Default-Bearer QoS Handling for 4G and WiFi Sessions

The following procedure explains how the SMF handles the modification of authorized default QoS in 4G and WiFi sessions.

1. The SMF receives SmPolicyUpdateNotify from PCF with changed QCI/5QI in AuthorizedDefaultQoS and/or a different session AMBR value.
2. The SMF initiates Update Bearer Request towards S-GW for the default bearer.
  - a. In the Update Bearer Request, Bearer Context IE is included for the default bearer and the corresponding Bearer QoS is updated with the changed QCI value.
  - b. For the 4G session, the extended Protocol Configuration Options (ePCO), if supported, is included in the Update Bearer Request message. The ePCO includes 5G Authorized QoS Flow Information with updated QCI value for the default flow when the interworking (IWF) is enabled for the session. Otherwise, PCO IE is sent with the same details.
  - c. For the WiFi session, Additional Protocol Configuration Options (APCO) is included in the Update Bearer Request message. The APCO contains 5G Authorized QoS Flow Information with updated QCI value for the default flow.
3. The SMF accepts the Update Bearer Response from S-GW.
4. On the N4 interface, the following changes are done:
  - a. New instance of the BearerLvlInfo IE is included with the changed QCI value for default bearer tunnel.
  - b. Update PDR is sent for all PDRs which are a part of default flow to reflect the association with the new BearerLvlInfo IE.
  - c. FAR associated with all PDRs in the default flow is updated with the new DSCP marking value if the 5QI-DSCP mapping configuration has a different value for the changed 5QI.

### Default-Bearer QoS Handling for 5G Sessions

The following procedure explains how the SMF handles the modification of authorized QoS for the default bearer in a 5G session.

1. The SMF receives SmPolicyUpdateNotify from PCF with changed 5QI in AuthorizedDefaultQoS and/or a different session AMBR value.

2. The SMF initiates N1N2MessageTransfer procedure with AMF to send N1 PDU Session Modification Command and N2 PDU Session Resource Modify Request Transfer IE in this message.
  - a. In the N1 message, the default QoS flow is modified in Authorized QoS Flow Description IE to update the 5QI value.
  - b. In the N1 message, the Mapped EPS Bearer Context IE is modified to update the QCI of the default bearer.
  - c. In the N2 message, the QoS flow level QoS parameter for the default flow is modified to update the 5QI value.
3. The SMF accepts the SMContextUpdate Request from AMF with the responses for the N1 and N2 requests sent in N1N2Message Transfer message.
4. On the N4 interface, the following changes are done:
  - a. New instance of the BearerLvlInfo IE is included with the changed 5QI to QFI mapping.
  - b. Update PDR is sent for all PDRs which are a part of default flow to reflect the association with the new BearerLvlInfo IE.
  - c. Forwarding Action Rule (FAR) associated with all PDRs in the default flow is updated with the new DSCP marking value if the 5QI-DSCP mapping configuration has a different value for the changed 5QI.

## Default-Bearer QoS Handling During WiFi Handovers

The following procedure explains how the SMF handles the modification of authorized default QoS during WiFi handover and other handovers.

1. The SMF sends SMPolicy Update Request to the PCF at the end of each handover procedure. For example, when the PCF arms different policy triggers, the SMF sends SMPolicy Update Request to the PCF. The response from PCF contains the changed QCI in Session Rule (Authorized Default QoS). The SMF initiates the modification procedure towards RAN/UE, and communicates the same information on N1, N2, N4, and S5 interfaces.
2. For all handovers (excluding WiFi-NR/EPS and NR/EPS-WiFi), the SMF sends SMPolicy Update Request to the PCF indicating the RAT type change. The response from PCF contains the changed QCI in Session Rule (Authorized Default QoS). The SMF initiates the modification procedure towards RAN/UE, and communicates the same information on N1, N2, N4, and S5 interfaces.

The handovers involving WiFi are different from the other handovers. The SMF triggers SMPolicy Update Request towards PCF during the handover and not after the handover. For the handovers involving WiFi, the target RAN installs the flows and bearers as new instead of an update. The SMF sends the latest QCI received in the response from PCF while installing the default flow and bearer during the handover.

## Default-Bearer QoS Modification During Failure Handling

For a 5G session, the modification of QCI/5QI typically does not fail on the N1 or N2 interface as the default flow is a non-GBR flow and no resource reservation is required for the QCI/5QI modification. However, if the modification procedure fails due to no N1 or N2 responses from AMF, the modification is rolled back and the session continues with the old QCI/5QI and session AMBR values. If the N2 rejects the flow modification, the session is deleted as it cannot remain without the default flow.

For a 4G session, the Update Bearer response does not fail for default bearer modification. However, if the Update bearer Response is missing or if it fails, the modification is rolled back and the session continues with the old 5QI and session AMBR values.

For both 4G and 5G sessions, if the N4 update fails or the response is not received, then the SMF takes the action according to the UPF failure handling template configuration. For 4G and WiFi sessions, if there is a failure on the N4 interface, another Update Bearer Request is sent with the old 5QI and AMBR values to S-GW and ePDG respectively.

The failure handling mechanism remains the same for the PCF-initiated modification procedure.

## Limitations

The Authorized QoS Handling for Default Bearer feature has the following limitations:

- The SMF supports only the standard QCI/5QI change in authorized default QoS IE of the Session Rules. It does not support any change to the Guaranteed Bit Rate (GBR) QCI/5QI of authorized QoS. The SMF rejects any request for modification of QCI/5QI of a QoS data associated with Policy and Charging Control (PCC) rule.
- The SMF does not support QCI/5QI change for dynamic rules.
- The SMF supports QCI/5QI change only for predefined and static rules that are associated to the default bearer. If a predefined rule is associated with a non-default flow or bearer, the SMF does not support QCI/5QI change for that rule.
- The combination of QoS flow binding parameters, such as 5QI, ARP, and so on, for the authorized QoS never remains the same as that of a dedicated bearer or flow. That is, change in QCI/5QI should not result in the default flow having the binding parameters similar to another flow.
- The SMF does not support changes to any other binding parameter including Allocation and Retention Priority (ARP) except the QCI/5QI (with or without session AMBR) in the Session Rules.
- When the QCI/5QI changes, the existing default bearer flow is modified towards N1, N2, and N4 interfaces. In this case, the SMF does not delete the existing flow instead creates a new flow.

## Authorized QoS Handling OAM Support

This section describes operations, administration, and maintenance information for this feature.

### Statistics Support

The SMF maintains the label "SESSRULE\_CHANGE" to indicate any changes to the AMBR value, QCI/5QI value, or a combination of both AMBR and QCI/5QI values.

## SMF Affinity

The SMF Affinity support is required in the CN architecture to facilitate stateless architecture.

When a session management procedure is ongoing for a subscriber session in some SMF service instance and another event from the network comes for the same subscriber in the meantime. Then, the SMF protocol layer micro-services such as "smf-rest-ep" and "smf-protocol" direct these events towards the concerned SMF

service instance. This ensures that all network events pertaining to an ongoing procedure of a subscriber session are handled by the same SMF service instance until the completion of the procedure.

Upon completion of the procedure, the subscriber session information is updated in the database and the session affinity towards the SMF service instance is removed. Subsequent network events can be handled by any of the available SMF service instances, by fetching the relevant subscriber session information from the database.

# Dynamic Configuration Change Support

## Feature Description

The Dynamic Configuration Change Support feature allows new sessions, or subsequent messages of existing sessions, with the updated configuration values.

This feature supports the following SMF configurations:

- SMF Profile
- SMF Service Profile

SMF provides flexibility to support Maintenance Operational Procedure for certain SMF Profile/Service-Profile configuration parameters. This Maintenance Operational Procedure operation helps to keep the SMF system in maintenance mode so that it doesn't impact the system by rejecting the new sessions. Also, Maintenance Operational Procedure provides flexibility to operators to clear subscribers manually by executing **clear subscriber all** command.

SMF updates configuration parameters change to NRF by sending "NFUUpdate" using PUT Method.

## How it Works

This section describes the Maintenance Operational Procedure and how dynamic change in configuration works for the supported SMF configurations.

### Maintenance Operational Procedure

1. Shutdown (offline) SMF by executing **mode offline** CLI command under SMF Profile.  
SMF sends NFUUpdate with Method PUT and NFStatus as "UNDISCOVERABLE"
2. Clean up the sessions using **clear subscriber sess all** CLI command.
3. Change the configurations and remove **mode offline** CLI command.  
SMF sends NFUUpdate with Method PUT and NFStatus as "Registered".

### SMF Profile and SMF-Service Profile

The following table describes how dynamic change in configuration works for the supported SMF configurations.

Configuration parameters	Dynamic Change	Impact on Existing Sessions	NRF Update	Maintenance Operational Procedure
locality	Allowed	Sessions will start using the newer values.	Not Required	Allowed
node-id	Not Applicable	No Impact	Not Applicable	Not Applicable
fqdn	Allowed	SMF always fetches the latest FQDN value for sessions while interacting with UDM.	Allowed	Allowed
allowed-nssai	Allowed	Sessions will start using the newer values.	Allowed	Allowed
plmn-id	Allowed	Sessions will start using the newer values.	Allowed	Allowed
service name, schema, service-id, version	Allowed	Sessions will start using the newer values.	Allowed	Allowed
http-endpoint	Allowed	Sessions will start using the newer values.	Allowed	Allowed
icmpv6-profile	Allowed	Sessions will start using the newer values.	Not Required	Not Required
compliance-profile	Allowed	SMF might perform parse-failure because of incompatibility issues between SMF and other NFs for various SBI interfaces.	Not Required	Not Required
access-profile	Allowed	Sessions will start using the newer values.	Not Required	Not Required
subscriber-policy	Allowed	Sessions will start using the newer values.	Not Required	Not Required

## Configuring Dynamic Configuration Change Support

Use the following configuration to enable offline mode of operation under SMF profile.

```
configure
  profile smf profile_name
    mode offline
  end
```

### NOTES:

- **mode:** Specifies the mode of operation.

- **offline**: Specifies the mode is offline and new sessions are rejected.

## Verifying Dynamic Configuration Change Support Configuration

Use the **show running-config profile smf** CLI command to verify if the feature is enabled. When enabled, the following field will be displayed as part of the show command output:

- mode offline

# Dynamic PCC Rules Enforcement

## Feature Description

SMF uses either the Policy and Charging Control (PCC) rules from Policy Control Function (PCF) or the locally configured policy rules to control the policy management. The PCF sends the PCC rules along with the applicable QoS and charging information to the SMF. The SMF uses this information to define the QoS flows and apply the QoS enforcement (via UPF) and charging towards CHF.

The PCC rules can be configured locally as well. The locally configured policy rules are labelled as static or predefined rules.

The following sections provide information on the features that are implemented for the dynamic policy management.

## Supported Features Negotiation

The SMF and the PCF negotiate the supported features during Policy Context Creation and during PDU session establishment. Based on the negotiated features, the PCF provides the relevant information.

The following table lists the features that can be negotiated as defined in the 3GPP specification 29.512.

**Table 172: Supported Negotiated Features**

Feature Number	Feature Name	Description
1	TSC	This feature indicates support for traffic steering control in the (S)Gi-LAN or routing of the user traffic to a local Data Network identified by the DNN per Application Function (AF) request. If the SMF supports this feature, the PCF performs the functions as described in 3GPP specification 29.512, subclause 4.2.6.2.20.
2	ResShare	This feature indicates the support of service data flows that share resources. If the SMF supports this feature, the PCF performs the functions as described in 3GPP specification 29.512, subclause 4.2.7.4.
4	ADC	This feature indicates the support of application detection and control.
6	NetLoc	This feature indicates the support of the Access Network Information Reporting for 5GS.
7	RAN-NAS-Cause	This feature indicates the support for the detailed release cause code information from the access network.

The SMF sends supportedFeatures attribute in the Npcf\_SMPolicyControl\_Create message, and further includes a bitmap representing the supported features. The PCF also sends the supportedFeatures attribute in the response message. The response should either match or be a subset of the request.

The string contains a bitmask indicating supported features in hexadecimal representation. Each character in the string takes a value of "0" to "9" or "A" to "F" and represents the support of the features as described in the preceding table. The most significant character representing the highest-numbered features appears first in the string, and the character representing features 1–4 appears last in the string. The list of features and their numbering (starting with 1) are defined separately for each API.

## Provisioning and Management of Session AMBR and Default QoS

For the N4 interface, the SMF sends the QoS information in the form of:

- Packet Detection Rule (PDR)
- Forwarding Action Rule (FAR)
- QoS Enforcement Rule (QER)

The SessionAMBR includes the maximum aggregated uplink and downlink bit rates to be shared across all non-GBR QoS flows in each PDU session. The SMF sends the session level QER for non-GBR flows along with existing QER to the UPF.

The SMF receives sessionRule from PCF in SmPolicyDecision during PDU session creation. The sessionRule consists of authSessAmbr and authDefQos. The authorized AMBR consists of the Uplink (UL) and Downlink (DL) MBR at a session level and authDefQos contains the 5Qi, ARP, and other QoS binding parameters for the default QoS flow.

The SMF performs the following actions:

- Any PCC rules received from the PCF that have an associated QoS Desc with the same binding parameters as received in authDefQos are tagged with the default QoS flow.
- On the N4 interface, the UL and DL Packet Detection Rules (PDRs) are created for each PCC rule that is associated with the default QoS flow. For session AMBR enforcement, the SMF creates a QoS Enforcement Rule (QER) with appropriate AMBR and associates it with all PDRs for non-GBR rules.
- On the N1 interface, the "QoS Flow Description" attribute in the PDU SESSION ESTABLISHMENT ACCEPT message contains the QFI and MFBR and 5Qi values. The Session AMBR is also sent in this message.
- On the N2 interface, the PDU Session Resource Setup Transfer Request IE contains the AMBR and the "QoS flow level QoS parameters" (5Qi, ARP, and so on) and QFI.
- The SMF supports the UDM-initiated Session AMBR modification. In this case:
  - The SMF sends Npcf\_SMPolicyControl\_Update to the PCF along with the new subscribed session AMBR within the "subsSessAmbr" attribute and the SE\_AMBR\_CH policy control request trigger within the "repPolicyCtrlReqTriggers". On receiving the change of session AMBR, the PCF provisions the new authorized session AMBR to the SMF in the response.
  - Update the QERs on N4 interface for Session AMBR enforcement.
  - Initiate N1N2MessageTransfer towards the AMF with Sess AMBR in PDU SESSION MODIFICATION COMMAND message in N1 interface and PDU Session Resource Modify Request transfer IE in N2 container having the new AMBR.

## Provisioning of Policy Revalidation Time

### Feature Description

The PCF instructs the SMF to trigger PCF interaction to request PCC rule from the PCF if not provided yet. The PCF performs this operation by providing revalidation time within the "revalidationTime" attribute and the RE\_TIMEOUT policy control request trigger within the "policyCtrlReqTriggers" attribute in SmPolicyDecision. The PCF can change the revalidation time by including a new value for the "revalidationTime" attribute. The PCF can also disable the revalidation function by removing RE\_TIMEOUT policy control request trigger if it has been provided.

If the SMF receives the existing revalidation time or the new revalidation time, the SMF stores the received value and starts the timer based on it. Then, the SMF sends the PCC rule request before the indicated revalidation time. If the RE\_TIMEOUT policy control request trigger is removed, the SMF stops the timer for revalidation.




---

**Note** When the RE\_TIMEOUT is removed, the revalidation time value previously provided to the SMF is no longer applicable.

---

### How it Works

Revalidation time is a string of the format "date-time" as defined in OpenAPI specification. The SMF, on receiving the revalidation time in "revalidationTime" attribute and RE\_TIMEOUT trigger in "policyCtrlReqTriggers" attribute, starts a timer for the difference duration (revalidationTime – currentTime – 5 seconds buffer). Once the timer expires, the SMF initiates the PCF interaction to request PCC rules.

### Standard Compliance

The Policy Revalidation Time feature complies with *3GPP TS 29.512, v15.2.0*.

## Provisioning and Management of Additional QoS Flows

The PCF can create, modify, or delete multiple GBR and non-GBR PCC rules.

The following scenarios are possible:

1. Multiple non-GBR and GBR PCC rules are activated during PDU session establishment. In this case:
  - a. The SMF creates the QoS flow according to the QoS flow binding principle as described in the QoS Management section.
  - b. On the N4 interface, the UL and DL PDRs are created for each PCC rule that is associated with all the flows. For flow-level QoS enforcement, the SMF creates QERs with the MFBR and GFBR (for GBR flows) values and associates it with each PDR of a flow.
  - c. On the N1 interface, the "QoS Flow Description" attribute in the PDU SESSION ESTABLISHMENT ACCEPT message contains the QFI and MFBR, GFBR, and 5Qi values. The packet filters associated with each QoS rule are sent on the N1 interface in the "Authorized QoS Rules" attribute.
  - d. Different types of packet filters are supported on both the N4 and the N1 interfaces. This list includes:

```
Packet filter component type identifier
Bits
8 7 6 5 4 3 2 1
```



```

0 0 0 0 0 0 0 1 Match-all type
0 0 0 1 0 0 0 0 IPv4 remote address type
0 0 0 1 0 0 0 1 IPv4 local address type
0 0 1 0 0 0 0 1 IPv6 remote address/prefix length type
0 0 1 0 0 0 1 1 IPv6 local address/prefix length type
0 0 1 1 0 0 0 0 Protocol identifier/Next header type
0 1 0 0 0 0 0 0 Single local port type
0 1 0 0 0 0 0 1 Local port range type
0 1 0 1 0 0 0 0 Single remote port type
0 1 0 1 0 0 0 1 Remote port range type

```

- e. On the N2 interface, the PDU Session Resource Setup Transfer Request IE contains the "QoS flow level QoS parameters" (5Qi, ARP, and so on) and QFIs for each of the flows. The "GBR QoS Flow Information" field of the IE contains the MFBR and GFBR of the GBR flows.

2. Modification of PCC rules after PDU session establishment. In this case, the following scenarios are observed:

- a. Modification, addition, and removal of packet filters of one or more PCC rules:

1. In this case, the SDF filters of the PDR on the N4 interface are changed by invoking N4 session modification.
2. The SMF initiates N1N2MessageTransfer towards the AMF with "Authorized QoS Rules" attribute in PDU SESSION MODIFICATION COMMAND message in N1 interface. The rule operation code in this attribute is one of the following:

```

0 1 1 Modify existing QoS rule and add packet filters
1 0 0 Modify existing QoS rule and replace all packet filters
1 0 1 Modify existing QoS rule and delete packet filter

```

- b. Change in QoS associated with one or more PCC rules:

1. The SMF performs QoS flow binding evaluation which in turn results in the following operations:
  1. Addition of a new QoS flow results in change of QFI on the N4 interface for some of the PDRs.
  2. Movement of a PCC rule from one QoS flow to another QoS flow. In this case, the PDR/QER of impacted PCC rules are modified to update the QFI.
  3. Removal of a QoS flow when the last PCC rule in that flow is moved to a different QoS flow. In this case, the PDR/QER of impacted PCC rules are modified to update the QFI.
2. In the preceding cases, on the N1 interface the Authorized QoS Rules and Authorized QoS Descriptors are sent with the operation code as one of the following:

```

0 0 1 Create new QoS flow description
0 1 0 Delete existing QoS flow description
0 1 1 Modify existing QoS flow description

```

3. On the N2 interface, QoS Flow Level QoS parameters of the PDU Session Resource Modify Request transfer IE carry the modified GFBR, MFBR, 5Qi and so on. For any flow removal, the QoS Flow to re-lease List is included in this IE.

- c. PCC rule removal:

1. In this case, the SMF removes all the PDRs associated with a QoS flow on the N4 interface.

- On the N1 interface, the Authorized QoS Rules and Authorized QoS Descriptors are sent with the operation code as one of the following:

```
0 1 0 Delete existing QoS flow description
```

- On the N2 interface, the PDU Session Resource Modify Request transfer IE carries the QoS Flow to release List.

## QoS Enforcement

The SMF enforces QoS at PCC rule (SDF) level, QoS flow level, and session level by creating one QER:

- per PCC rule level to enforce MBR/GBR as per the associated QoS Desc supplied by PCF and associated to the given PCC rule.
- at QoS flow level which has aggregated MBR/GBR of all the PCC rules associated with a QFI.
- at session level to enforce the Session AMBR for all non-GBR QoS flows.

Once these QERs are created, the SMF associates:

- the session level QER to all PDRs belonging to the non-GBR QoS category.
- the SDF level QER to each individual PCC rule.

For any QoS modification including movement of the PCC rules from one flow to another and QoS modification within flow, the SMF modifies the GFBR/MFBR (or Session AMBR) and updates the QERs accordingly on the N4 interface.

## Policy Control Request Triggers

The PCF provides one or more policy control request trigger(s) by including the triggers in the "policyCtrlReqTriggers" attribute(s) in the SmPolicyDecision data structure.

During the lifetime of the PDU session, the PCF updates or removes the policy control request triggers. To update the trigger, the PCF provides a new complete list of applicable policy control request triggers by including the trigger(s) in the "policyCtrlReqTriggers" attribute.

The PCF removes all previously provided triggers by providing a "policyCtrlReqTriggers" attribute set to NULL value. Upon reception of a policy control request trigger with this value, the SMF does not inform PCF of any trigger except for those triggers that are always reported and does not require provisioning from the PCF.

Whenever the PCF provisions the trigger, unless otherwise specified in the trigger's value definition, the SMF sends the corresponding currently applicable values (for example, access type, RAT type, user location information, and so on) to the PCF within the UeCampingRep data structure in the response of the HTTP POST message. In this case, the "repPolicyCtrlReqTriggers" attribute is not included.

The list of supported triggers is as follows:

Trigger	Description
---------	-------------

RES_MO_RE	A request for resource modification has been received by the SMF. This is a mandatory trigger.  <b>Note</b> This request is sent from SMF to PCF when UE/AMF requested QoS modification is triggered.
UE_IP_CH	UE IP address change. This is a mandatory trigger.
DEF_QOS_CH	Default QoS Change. This is a mandatory trigger.
SE_AMBR_CH	Session AMBR Change. This is a mandatory trigger.
SAREA_CH	Location Change about the Serving Area in N11 update.
SCNN_CH	Location Change about the Serving CN node. See the following section for details on how the SMF supports this trigger during the different handover scenarios.
RE_TIMEOUT	Indicates that the SMF has generated the request because there has been a PCC revalidation timeout (that is, Enforced PCC rule request as defined in Table 6.1.3.5.-1 of <i>3GPP TS 29.503</i> ).

### Support SCNN\_CH Trigger in Handovers

The SMF supports the serving network change trigger in the following handovers:

- **Inter AMF Handover:** If the "SCNN\_CH" is provisioned, when the SMF detects a change of serving Network Function (for example, the AMF), the SMF includes the "SCNN\_CH" within the "repPolicyCtrlReqTriggers" attribute and the current serving Network Function in the "servNfId" attribute. When the serving Network Function is an AMF, the SMF includes the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute.
- **5G to 4G handover:** When the UE handed over from the 5GS to EPC/E-UTRAN, the SMF includes, if the "SCNN\_CH" policy control request trigger is provisioned and met, the "servNfId" attribute including the S-GW identification within the "anGwAddr" attribute.
- **4G to 5G handover:** The SMF includes the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute.
- **WiFi to 5G handover:** The SMF includes the AMF Network Function Instance Identifier within the "servNfInstId" attribute and the Globally Unique AMF Identifier within the "guami" attribute.
- **5G to WiFi handover:** When the UE handed over from the 5GS to EPC non-3GPP access, the SMF includes, if the "SCNN\_CH" policy control request trigger is provisioned and met, the ePDG identification within the "anGwAddr" attribute included in the "servNfId" attribute.

## Gating Control

### Feature Description

Gating control is the capability to block or allow IP packets belonging to a certain IP flow, based on the decisions by the PCF. The PCF could, for example, make gating decisions based on session events (start and stop of service) reported by the AF.

The AF instructs the PCF to temporarily block the user traffic corresponding to a specific PCC rule on uplink or downlink direction, or both the directions.

To enable the PCF gating control decisions, the AF reports session events (for example, session termination, modification) to the PCF. For example, session termination, in gating control, triggers the blocking of packets or "closing the gate".




---

**Note** Gating Control applies only for service data flows of IP type.

---

## How it Works

The Gating Control feature works in the following manner:

1. PCF sends flowStatus attribute in TrafficControlData referenced by the PCC rule. The value of this attribute is set to "enabled", "disabled", "enable\_uplink", or "enable\_downlink" based on the PCF decision.
2. On receiving this attribute, the SMF instructs the UPF to open or close the GATE for the UL or DL Packet Detection Rule (PDR), or both UL and DL PDRs for the associated PCC rule. The Gate Status Information Element (IE) in Create QoS Enhancement Rule (QER) or Update QER associated with the PDR is set to OPEN or CLOSED.
3. If there is any subsequent change, the PCF triggers a N4 modification request to change the GATE status.

## Standard Compliance

The Gating Control feature complies with *3GPP TS 29.512, v15.2.0*.

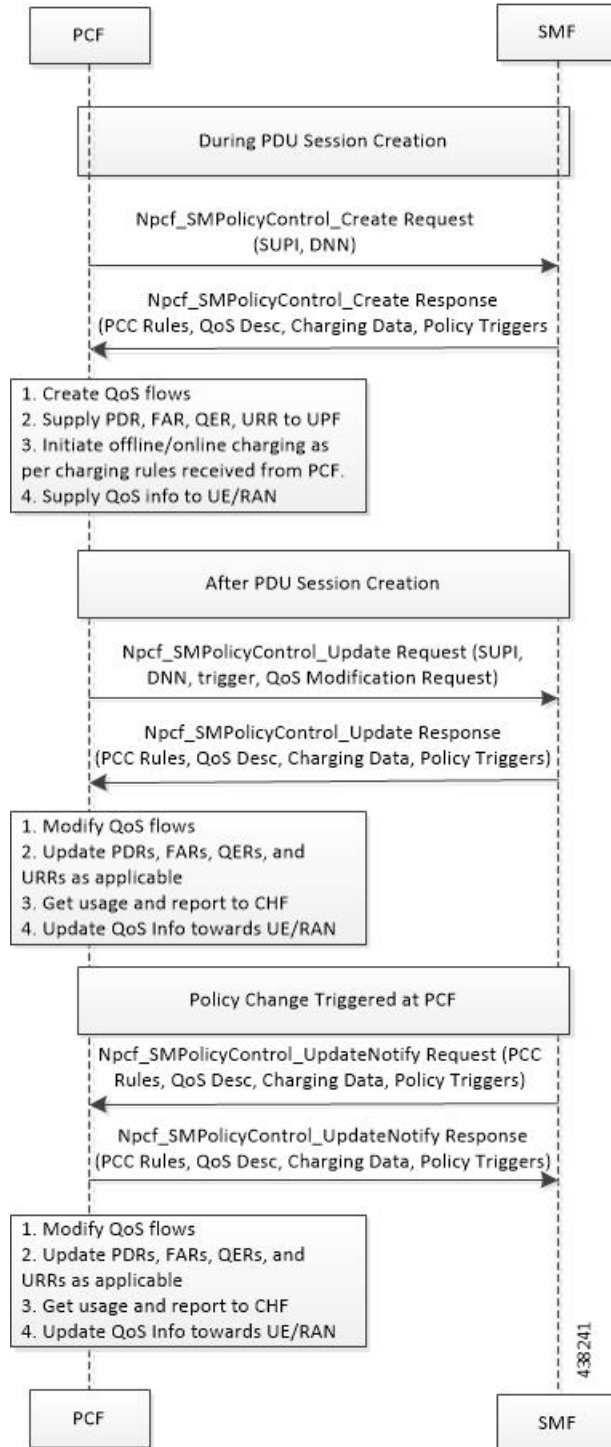
## How it Works

The SMF requests the policy information from PCF. The PCF in turn provides the policy rules during and after PDU session creation to enable the dynamic policy application. Dynamic policy management involves the following operations:

- Policy Context Creation: This operation is performed at the time of PDU session create and the PCF sends the PCC rules and the associated QoS, Charging and other policy data in the response message.
- Policy Context Update: For any RAN-initiated or UE-initiated policy updates and for notification of trigger events, the SMF initiates a policy context update. In response, the PCF sends the changed policy data that impacts the QoS and charging.
- Policy Context Update Notification: During the lifecycle of a PDU session, the PCF can initiate a policy update based on interaction with the AF or local configuration changes at PCF. The SMF handles the updated policy rules when received in a notification from the PCF.
- Policy Context Delete: At the end of a PDU session, the SMF terminates the Policy Context with PCF.

The following figure illustrates the dynamic policy management procedure for a PDU session.

Figure 110: Dynamic Policy Management Call Flow



## Standards Compliance

The Dynamic PCC Rules Enforcement feature complies with the *3GPP TS 29.512, Release 15.2.0*.

## Limitations

The Dynamic PCC Rules Enforcement feature has the following limitations:

- SMF supports only the following combination of operations:
  - Creation of new PCC Rule with new QoS descriptor to create new QoS Flow
  - Addition of new PCC Rule to an existing QoS Flow
  - Removal of PCC rule
  - Updating of GBR/MBR parameters associated with the rule
  - Session AMBR Changes
  - Session AMBR Changes and PCC Rules cannot be combined in the same update operation
- The current implementation supports only QoS Descriptors with standard 5QI and ignores the non-standard ones. If all the QoS Desc received are non-standard, then all are ignored and the default one created by SMF is used.

## Configuring the Dynamic PCC Rules Enforcement Feature

This section describes how to configure the Dynamic PCC Rules Enforcement feature.

Configuring the Dynamic PCC Rules Enforcement feature involves the following steps:

1. Creating QoS Profile
2. Configuring QoS Parameters
3. Defining QoS Profile in DNN Profile Configuration

### Creating QoS Profile

This section describes how to create an instance of a quality of service (QoS) profile.

```
configure
  profile qos qos_profile_name
end
```

#### NOTES:

- **qos qos\_profile\_name**: This command creates a quality of service profile and provides access to the QoS Profile Configuration mode to use the commands to configure the QoS parameters. See the qos-profile section of the Command Line Interface Reference for command information. *qos\_profile\_name* must be an alphanumeric string uniquely identifying the QoS profile.

### Configuring QoS Parameters

This section describes how to configure the QoS parameters.

```
configure
  profile qos qos_profile_name
    ambr { ul uplink_ambr | dl downlink_ambr }
```

```

arp { preempt-cap preemption_capability |
preempt-vuln preemption_vulnerability |
priority-level priority_level }
max data-burst burst_volume
priority qos_priority
qi5 5qi_value
end

```

**NOTES:**

- **ambr** { **ul** *uplink\_ambr* | **dl** *downlink\_ambr* }: Defines the Aggregate Maximum Bit Rate (AMBR) for the uplink (subscriber to network) and the downlink (network to subscriber) traffic.
- **arp preempt-cap** *preemption\_capability*: Specifies the preemption capability flag. Options are:
  - MAY\_PREEMPT: Bearer may be preempted
  - NOT\_PREEMPT: Bearer cannot be preempted
- **arp preempt-vuln** *preemption\_vulnerability*: Specifies the preemption vulnerability flag. Options are:
  - PREEMPTABLE: Bearer may be preempted
  - NOT\_PREEMPTABLE: Bearer cannot be preempted
- **arp priority-level** *priority\_level*: Defines the Allocation and Retention Priority (ARP) for the service data. The default value of *priority\_level* is 8.
- **max data-burst** *burst\_volume*: Defines the maximum data burst volume. *burst\_volume* must be an integer value in the range of 1–4095.
- **priority** *qos\_priority*: Specifies the 5QI priority level. *qos\_priority* must be an integer value in the range of 1–127.
- **qi5** *5qi\_value*: Specifies the 5G QoS Identifier (5QI) for the authorized QoS parameters. *5qi\_value* must be an integer value in the range of 0–255.

## Defining QoS Profile in DNN Profile Configuration

This section describes how to configure the QoS profile in the existing DNN profile configuration.

```

configure
  profile dnn dnn_profile_name
    qos-profile qos_profile_name
  end

```

**NOTES:**

- **qos-profile** *qos\_profile\_name*: This command defines locally configured default QoS profile. This profile is configured under the existing DNN Profile Configuration. *qos\_profile\_name* must be the name of the configured QoS profile.

## Verifying the Dynamic PCC Rules Enforcement Feature Configuration

This section describes how to verify the Dynamic PCC Rules Enforcement feature configuration.

Use the following show command to verify the feature configuration details.

### show full-configuration

The following is an example of this show command output.

```
show full-configuration
profile dnn dnn1
qos-profile qos1
!
profile qos qos1
ambr ul 1024
ambr dl 1024
qi5 128
arp priority-level 8
arp preempt-cap NOT_PREEMPT
arp preempt-vuln NOT_PREEMPTABLE
priority 9
max data-burst 2048
exit
```

## Troubleshooting Information

This section provides information for troubleshooting any issues that may arise during the feature operation.

The SMF maintains various logs such as trace logs, event logs, and so on. Use **kubectl get pods -n namespace** CLI command to check all the pods and the services that are currently running. Then, use **kubectl logs podname -n namespace** command to display the log in a pod.

If you encounter any error during the operation of this feature, use the SMF service logs for a particular subscriber session to identify the issues and determine the solution to your problem.

## Static PCC Rules Support

### Feature Description

Static PCC rules are configured in the SMF. These rules can be activated immediately upon PDU session establishment. Static rule is identified by the ruledef configuration using the **action priority** CLI command.

The local configuration on SMF represents the rulebase which is sent to the UPF during session establishment. The SMF uses the configuration representing the PCC rules, QoS Desc, and Charging Data received from PCF to perform QoS flow binding. This configuration is present in the UPF as well. The SMF does not send the PDRs, QERs, and FARs, instead sends only the rulebase name in a default PDR (referred as rulebase PDR) over the N4 interface. The UPF generates the PDRs, FARs, QERs, and URRs for predefined rules based on the rulebase configuration.



#### Important

The Static PCC Rules Support on SMF is applicable to both 4G and 5G calls.

### Relationships

This feature utilizes the functionalities provided by PDU Session Lifecycle feature.



## Converged Core Refactoring Changes

This section describes the changes related to converged core refactoring in this chapter.

The **host-pool** CLI command in the ACS Rule Definitions mode is deprecated in 2021.01 and later releases.

## How it Works

PCF must send the rulebase name to enable the static PCC rule support on SMF.

When the PCF provides the rulebase name, the SMF performs the following steps during the PDU session creation:

1. The SMF sends Npcf\_SMPolicycontrolCreate message to PCF. In response to this message, the PCF may send SMPolicyDecision with a PccRule. If the rule ID of the PccRule is in cbn# rulebase name format, the SMF assumes that the rule id is representing a rulebase name.
2. The SMF sends the rulebase name to the UPF in PFCP Session Establishment Request in a proprietary IE within Create PDR IE.

**Note**

The SMF sends this name only in the default PDR which does not have any SDF filters. No other PDR, FAR, QER, and URR are sent to the UPF for the static rules. The UPF can derive the same from the rulebase name.

## Pre-processing During Configuration

Once the Active Charging Service configuration is done (including rulebase, associated ruledefs, and charging actions), SMF processes the configured values and derives PCC Rules, QoSData, and ChargingData from the configured values. The following principles are used to create these entities:

1. QoSData:
  - a. Each configured charging action results in a QoSDesc creation.
  - b. The **flow-limit-bandwidth** configured under charging action provides the GBR/MBR for the QoSData.
  - c. The QCI and ARP configured in charging action constitute the 5QI and ARP of the QoSData. If no QCI and ARP are configured, the 5QI and ARP of the default QoS flow are associated with this QoSData.
2. ChargingData:
  - a. The **billing-action** configuration under charging action determines whether offline charging is enabled in the created ChargingData.
  - b. The **cca charging credit** configuration under charging action determines whether online charging is enabled in the created ChargingData.
  - c. The rating group and service ID of the ChargingData are provided by content-id and service-identifier configuration under charging action.
3. PCCRule:
  - a. Each ruledef under a rulebase results in creation of a PCCRule.

- b. The **packet-filter** configured under charging action is used for the FlowInformation in the PCCRule.
- c. The QoSData and ChargingData associated with this ruledef in the rulebase configuration form the refQoS and refChg for this PCCRule.

All the created PCCRules, QoSData, and ChargingData are saved per rulebase.

## During PDU Session Creation

1. During PDU session creation, PCF sends the rulebase name (value configured under upf-apn is selected if the PCF does not send it) as PCCRule with ID set to cbn# configured rulebase name. It may also send any predefined rule to be activated as another PCCRule with ID set to crn# configured ruledef name. All such PCC rules will have only the RuleId attribute present.
2. On receiving such a request, SMF selects the constructed PCCRules, QoSData, and ChargingData which correspond to the received rulebase and ruledef names, and uses these to create QoS flows in QoSModel.
3. On the N4 interface, the SMF sends the rulebase name in the CreatePDR IE in a Cisco Proprietary IW named "rulebase".
4. For all activated predefined rules, SMF sends one uplink and one downlink PDR containing the ruledef name in "Activate Predefined Rule" IE.
5. The UPF also has similar configuration for active charging service. From the rulebase name and ruledef names, it can create the corresponding QER and URR.
6. On N1 and N2 interfaces, the processing of the predefined and static rules are the same as that of dynamic rule.
7. For all static and activated predefined rules, QoSRules are sent on N1 interface if packet-filters were configured.
8. The GFBR and MFBR of a flow are computed using the GBR/MBR of the QoSData associated with all static and activated predefined rules at any point of time and the same is sent on N2 interface in an AuthorisedQoSDescription IE on N1 interface.

## During PDU Session Modification

1. During PDU session modification, PCF sends the rulebase name as PCCRule with ID set to cbn#configured rulebase name. In case of predefined rule PCF can activate new rule crn#configured ruledef name or delete the existing rule (crn#"nil"). All such PCC Rules will have only the RuleId attribute present.
2. On receiving new rule addition request, SMF selects the constructed PCCRules, QoSData and ChargingData which correspond to the received rulebase and ruledef names, and uses these to create QoS flows in QoSModel.
3. On receiving an existing rule deletion request, if the SMF received a ruledef name with nil value or a rulebase name different from the existing one, the SMF deletes the QoS flows which correspond to previous rulebase name or ruledef in QoSModel.
4. On N4 interface, SMF sends the new rulebase name in the CreatePDR IE in a Cisco Proprietary IW named "rulebase" and RemovePDR with PDR ID which correspond to the old rulebase name.

5. For all activated predefined rules, SMF sends one uplink and one downlink PDR containing the ruledef name in "Activate Predefined Rule" IE.
6. For all deactivated predefined rules, SMF sends RemovePDR with PDR ID which corresponds to the predefined rule.
7. The UPF also has similar configuration for active charging service. From the rulebase name and ruledef names, it can create or delete the corresponding QER and URR.
8. On N1 and N2 interfaces, the processing of the predefined and static rules are the same as that of dynamic rule.
9. For all static and activated/deactivated predefined rules, QoS Rules are sent on N1 interface if packet-filters were configured.
10. The GFBR and MFBR of a flow are computed using the GBR/MBR of the QoSData associated with all static and activated/deactivated predefined rules at any point of time and the same is sent on N2 interface in an AuthorisedQoSDescription IE on N1 interface.

## Limitations

The Dynamic PCC Rules Enforcement feature has the following limitations:

- SMF supports only the following combination of operations:
  - Creation of new PCC Rule with new QoS descriptor to create new QoS Flow
  - Addition of new PCC Rule to an existing QoS Flow
  - Removal of PCC rule
  - Updating of GBR/MBR parameters associated with the rule
  - Session AMBR Changes
  - Session AMBR Changes and PCC Rules cannot be combined in the same update operation
- The current implementation supports only QoS Descriptors with standard 5QI and ignores the non-standard ones. If all the QoS Desc received are non-standard, then all are ignored and the default one created by SMF is used.

## Configuring the Static PCC Rules Support

This section describes how to configure the Static PCC Rules Support on SMF.

The configuration for static and predefined rules is based on the ECS configuration of the StarOS based P-GW. This is to ensure that the UPF can work seamlessly with the SMF.

Configuring the Static PCC Rules Support involves the following steps:

1. Configuring ACS
2. Configuring Charging Action
3. Configuring Packet Filter
4. Configuring ACS Ruledef

5. Configuring ACS Group of Ruledefs
6. Configuring Rulebase and Predefined Rule Prefix
7. Configuring ACS Rulebase (ACS Configuration Mode)
8. Configuring URR ID
9. Configuring GTPP Group
10. Configuring Access Point Name (APN)
11. Associating GTPP Group with APN
12. Configuring ACS Rulebase (APN Configuration Mode)
13. Defining UPF APN Profile in DNN Profile Configuration
14. Configuring QoS Parameters
15. Associating Default Session Rule to DNN Profile

## Configuring ACS

ACS provides flexible, differentiated, and detailed billing to subscribers through Layer 3 through Layer 7 packet inspection and the ability to integrate with back-end billing mediation systems.



### Important

In this release, only one active charging service can be configured per system.

This section describes how to configure ACS.

```
configure
  active-charging service service_name
end
```

### NOTES:

- **active-charging service** *service\_name*: Specifies the name of an Active Charging Service. *service\_name* must be an alphanumeric string of 1 to 15 characters.
- If the named ACS does not exist, it is created, and the CLI mode changes to the ACS Configuration Mode wherein the service can be configured. If the named ACS already exists, the CLI mode changes to the ACS Configuration Mode. The ACS Configuration mode is used to manage ACS or enhanced charging service (ECS) configurations.

## Configuring Charging Action

This section describes how to configure charging action. The charging action represents actions to be taken when a configured rule is matched. Actions could range from generating an accounting record (for example, an EDR) to dropping the IP packet, and so on. The charging action will also determine the metering principle—whether to count retransmitted packets and which protocol field to use for billing (L3, L4, L7, and so on).

The charging action configuration is used to define the QoS and charging related parameters associated with ruledefs.

#### configure

```

active-charging service service_name
  charging-action charging_action
    allocation-retention-priority priority [ pci pci_value
      | pvi pvi_value billing-action egcdr cca
    ]
    charging credit [ rating-group coupon_id
      ] [ preemptively-request ]
    content-id content_id
    flow action { discard [ downlink | uplink ] | redirect-url
      redirect_url | terminate-flow }
    flow limit-for-bandwidth { { direction { downlink | uplink }
      }
    }
    peak-data-rate bps peak-burst-size bytes violate-action
      { discard | lower-ip-precedence } [ committed-data-rate
      bps committed-burst-size bytes
      ] [ exceed-action { discard | lower-ip-precedence
      } ] ] } | { id id } }
    nexthop-forwarding-address ipv4_address/ipv6_address
    qos-class-identifier qos_class_identifier
    service-identifier service_id
    tft packet-filter packet_filter_name
    tft-notify-ue
    tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32
      | af33 | af41 | af42 | af43 | be | ef | lower-bits tos_value
    } [ downlink | uplink ]
  end

```

#### NOTES:

- **charging-action** *charging\_action\_name*: Specifies the name of a charging action. *charging\_action\_name* must be an alphanumeric string of 1 to 63 characters and can contain punctuation characters. Each charging action must have a unique name.
- If the named charging action does not exist, it is created, and the CLI mode changes to the ACS Charging Action Configuration Mode wherein the charging action can be configured.
- If the named charging action already exists, the CLI mode changes to the ACS Charging Action Configuration Mode for that charging action.
- **allocation-retention-priority** *priority* [ **pci** *pci\_value* | **pvi** *pvi\_value* ]: Configures the Allocation Retention Priority (ARP). *priority* must be an integer value in the range of 1-15.
  - **pci** *pci\_value* : Specifies the Preemption Capability Indication (PCI) value. The options are:
    - MAY\_PREEMPT - Flow can be preempted. This is the default value.
    - NOT\_PREEMPT - Flow cannot be preempted
  - **pvi** *pvi\_value*: Specifies the Preemption Vulnerability Indication (PVI) value. The options are:
    - NOT\_PREEMPTABLE - Flow cannot be preempted. This is the default value.
    - PREEMPTABLE - Flow can be preempted

- **billing-action**: Configures the billing action for packets that match specific rule definitions.
- **cca charging credit**: Enables or disables Credit Control Application (CCA) and configures the RADIUS/Diameter prepaid charging behavior.
- **content-id**: Configures the rating group.
- **flow action**: Specifies the action to take on packets that match rule definitions.
- **flow limit-for-bandwidth**: Configures the QoS parameters such as MBR, GBR, and so on.
  - **peakdatarate(MBR)**: Default is 3000 bps
  - **peakburstsize**: Default is 3000 bytes
  - **committedDataRate(GBR)**: Default is 144000 bps
  - **committedBurstSize**: Default is 3000 bytes
- **nexthop-forwarding-address** *ipv4\_address/ipv6\_address*: Configures the nexthop forwarding address.
- **qos-class-identifier** *qos\_class\_identifier*: Configures the QoS Class Identifier (QCI) for a charging action. *qos\_class\_identifier* must be an integer value in the range of 1-9 or from 128-254 (Operator specific).
- **service identifier** *service\_id*: Configures the service identifier to use in generated billing records. *service\_id* must be an integer value in the range of 1-2147483647.
- **tft packet-filter** *packet\_filter\_name*: Specifies the packet filter to add or remove from the current charging action. *packet\_filter\_name* must be the name of a packet filter, and must be an alphanumeric string of 1 to 63 characters.
- **tft-notify-ue**: Control the TFT updates towards the UE based on certain trigger conditions.
- **tos**: Configures the Type of Service (ToS) octets.

## Configuring Packet Filter

This section describes the commands that are used to configure packet filter.

### configure

```

active-charging service service_name
  packet-filter packet_filter_name
    direction { bi-directional | downlink | uplink }
    ip local-port { = port_number | range start_port_number to
      end_port_number }
    ip protocol = protocol_number
    ip remote-port { = port_number | range start_port_number to
      end_port_number }
    ip tos-traffic-class = { type-of-service | traffic class }
    mask { = mask-value }
    priority priority
  end

```

### NOTES:

- **packet-filter** *packet\_filter\_name*: Configures the packet filters to be sent to UE. *packet\_filter\_name* must be the name of the packet filter, and must be an alphanumeric string of 1 to 15 characters.
- **direction** { **bi-directional** | **downlink** | **uplink** }: Configures the direction in which the packet filter has to be applied. The default value is **bi-directional**.
- **ip local-port**: Configures the IP 5-tuple local port(s) for the current packet filter.
- **ip protocol**: Configures the IP protocol(s) for the current packet filter.
- **ip remote-address**: Configures the IP remote address(es) for the current packet filter.
- **ip remote-port**: Configures the IP remote port(s) for the current packet filter.
- **ip tos-traffic-class**: Configures Type of Service (TOS)/Traffic class under charging action in the Packet filter mode.
- **priority** *priority*: Configures the current packet filter's priority.

## Configuring ACS Ruledef

A ruledef represents a set of matching conditions across multiple L3 – L7 protocol based on protocol fields and state information. Each ruledef can be used across multiple rulebases within the active charging service.

This section describes how to create, configure, or delete ACS rule definitions.

### configure

```

active-charging service service_name
  ruledef ruledef_name
    ip any-match [ = | != ] [ TRUE | FALSE ]
    ip dst-address { operator { { ipv4_address | ipv6_address
    } | { ipv4_address/mask | ipv6_address/mask } |
    address-group ipv6_address } | { !range | range }

    rule-application { charging | post-processing | routing }
  end

```

### NOTES:

- **ruledef** *ruledef\_name*: Specifies the ruledef to add, configure, or delete. *ruledef\_name* must be the name of an ACS ruledef, and must be an alphanumeric string of 1 to 63 characters, and can contain punctuation characters. Each ruledef must have a unique name. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names.
- If the named ruledef does not exist, it is created, and the CLI mode changes to the ACS Ruledef Configuration Mode wherein the ruledef can be configured.
- If the named ruledef already exists, the CLI mode changes to the ACS Ruledef Configuration Mode for that ruledef. The ACS Ruledef Configuration Mode is used to create and manage rule expressions in individual rule definitions (ruledefs).
- **ip any-match** [= | !=] [TRUE | FALSE]: This command defines the rule expressions to match IPv4/IPv6 packets. The *operator* and *condition* in the command specifies the following:
  - *operator*
    - !=: Does not equal

- <=: Equals
- *condition*
  - FALSE
  - TRUE
- **ip dst-address** { *operator* { { *ipv4\_address* | *ipv6\_address* } | { *ipv4\_address/mask* | *ipv6\_address/mask* } | **address-group** *ipv6\_address* } | { **!range** | **range** } **host-pool** *host\_pool\_name* }: This command allows defining rule expressions to match IP destination address field within IP headers.
  - *ipv4\_address* | *ipv6\_address*: Specifies the IP address of the destination node for outgoing traffic. *ipv4\_address* | *ipv6\_address* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
  - *ipv4\_address/mask* | *ipv6\_address/mask*: Specifies the IP address of the destination node for outgoing traffic. *ipv4\_address/mask* | *ipv6\_address/mask* must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.
  - *address-group ipv6\_address*: Specifies a group of IPv6 addresses configured with wildcard input and/or specialized range input. Multiple wildcard characters can be accepted as input and only one 2 byte range input will be accepted. Both wildcard character input and 2-byte range input can be configured together within a given IPv6 address.
  - The *operator* in the command specifies the following:
    - !=: Does not equal
    - <: Lesser than or equals
    - =: Equals
    - >=: Greater than or equals
- **multi-line-or all-lines**: This command allows a single ruledef to specify multiple URL expressions. When a ruledef is evaluated, if the multi-line-or all-lines command is configured, the logical OR operator is applied to all the rule expressions in the ruledef to decide if the ruledef matches or not. If the multi-line-or all-lines command is not configured, the logical AND operator is applied to all the rule expressions.
- **rule-application** { **charging** | **post-processing** | **routing** }: This command specifies the rule application for a rule definition.
  - **charging**: Specifies that the current ruledef is for charging purposes.
  - **post-processing**: Specifies that the current ruledef is for post-processing purposes. This enables processing of packets even if the rule matching for them has been disabled.
  - **routing**: Specifies that the current ruledef is for routing purposes. Up to 256 rule definitions can be defined for routing in an Active Charging Service. Default: Disabled.



## Configuring ACS Group of Ruledefs

A group-of-ruledefs can contain optimizable ruledefs. Ruledef group optimization depends on the optimization ability of ruledefs in the group-of-ruledefs, and the optimization configuration of the group in a rulebase.

Upon adding a new ruledef, the following checks occur:

- Determines if the new ruledef is part of any existing group of ruledefs
- Identifies if the new ruledef requires optimization

Use the following configuration to combine a set of ruledefs together to apply the same charging action on them.

### configure

```

active-charging service service_name
  group-of-ruledefs ruledef_group_name
    add-ruledef priority ruledef_priority ruledef ruledef_name
  end

```

### NOTES:

- **group-of-ruledefs** *ruledef\_group\_name* : Specifies the ruledef group name to add, configure, or delete. This command allows up to a maximum of 128 group of ruledef configurations.
- **add-ruledef**: This command allows you to add or remove ruledefs from a group-of-ruledefs. This command allows up to a maximum of 128 ruledef configurations.
- **priority**: Specifies the priority of the ruledef in the current group of ruledefs. *ruledef\_priority* is an integer from 1 through 10000.
- **ruledef** *ruledef\_name*: Specifies name of the ruledef to add to the current group-of-ruledefs. *ruledef\_name* must be the name of an ACS ruledef, and must be an alphanumeric string of 1 to 63 characters.

## Configuring Rulebase and Predefined Rule Prefix

Rulebase and predefined rule prefix configuration is mandatory for static rule installation from PCF. The SMF supports the predefined rule installation with prefix and without prefix. The SMF also supports the group-of-ruledef installation for both predefined and static rules.

Use the following configuration to configure the rulebase prefix and predefined rule prefix.

### configure

```

profile network-element pcf pcf_service_name
  predefined-rule-prefix predef_rule_prefix
  rulebase-prefix rulebase_prefix
end

```

### NOTES:

- **predefined-rule-prefix** *predef\_rule\_prefix* : Specifies the predefined rule prefix to be added. For example, the prefix for predefined rule is **cbr**.
- This is an optional configuration for the predefined rule. When there is no prefix defined within the PCF network element profile, the predefined rule application behaves as defined in the *3GPP TS 29.244* specification.

- **rulebase-prefix** *rulebase\_prefix* : Specifies the rulebase prefix to be added. For example, the prefix for rulebase is **rbn**. This is a mandatory configuration for the static rule.

## Configuring ACS Rulebase (APN Configuration Mode)

This section describes how to enable and configure an ACS rulebase to be used for subscribers who use the configured APN.

```
configure
  apn apn_name
    active-charging rulebase rulebase_name
  end
```

### NOTES:

- **active-charging rulebase** *rulebase\_name*: Specifies the name of the ACS rulebase. *rulebase\_name* must be an alphanumeric string of 1 to 63 characters.

## Configuring URR ID

This section describes how to configure the Usage Reporting Rules (URR) ID for the rating and service groups.

```
configure
  active-charging service service_name
    urr-list list_name
      rating-group rating_id service-identifier service_id_value
      urr-id urr_id_value
    end
```

### NOTES:

- **urr-list** *list\_name*: Specifies the name of the URR list, and must be an alphanumeric string of 1 to 63 characters.
- **rating-group** *rating\_id*: Specifies the rating ID used in charging. *rating\_id* must be an integer value in the range of 0-2147483647.
- **service-identifier** *service\_id\_value*: Configures the service identifier value. *service\_id\_value* must be an integer value in the range of 0-2147483647.
- **urr-id** *urr\_id\_value*: Configures URR identifier for rating/service group. *urr\_id\_value* must be an integer value in the range of 1-8388607.
- The URR ID configuration is per rating group and service ID. For different rating group and service ID combinations, use the URR ID configuration command as many times as needed.

## Configuring GTPP Group

This section describes the commands that are used to configure GTPP group.

```
configure
  gtpg group group_name
```

```

    gtpb trigger { time-limit | volume-limit }
end

```

**NOTES:**

- **gtpb group** *group\_name*: Specifies the GTPB group name. *group\_name* must be an alphanumeric string of 1 to 63 characters.
- **gtpb trigger { time-limit | volume-limit }**: Configures triggers for CDR.
  - **time-limit**: Enables time-limit trigger for the CDR.
  - **volume-limit**: Enables volume-limit trigger for the CDR.

## Configuring Access Point Name (APN)

This section describes how to create APN templates. This APN configuration represents the access point configuration in the UPF and further facilitates configuring a rulebase name within.

```

configure
  apn apn_name
end

```

**NOTES:**

- **apn** *apn\_name*: Specifies a name for the APN template as an alphanumeric string of 1 to 62 characters and is case insensitive.

## Associating GTPB Group with APN

This section describes how to associate the GTPB group with the configured APN.

```

configure
  apn apn_name
  gtpb group group_name
end

```

**NOTES:**

- **gtpb group** *group\_name*: Associates the defined GTPB group with the already configured APN.

## Configuring ACS Rulebase (ACS Configuration Mode)

This section describes how to create, configure, or delete an ACS rulebase. A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matching flow. The default rulebase is used when a subscriber/APN is not configured with a specific rulebase to use.

Rulebase configuration is the one that combines all the specified configurations together to construct the static and predefined PCC rules.

```

configure
  active-charging service service_name
  rulebase rulebase_name
  action priority action_priority { [ dynamic-only ]

```

```

| static-and-dynamic | timedef timedef_name ]
{ group-of-ruledefs ruledefs_group_name |
ruledef ruledef_name } charging-action charging_action_name
[ monitoring-key monitoring_key ] [ description description ] }
cca quota { holding-time holding_time content-id content_id
| retry-time retry_time [ max-retries retries ] }
cca quota time-duration algorithm { consumed-time seconds
[ plus-idle ] | continuous-time-periods seconds |
parking-meter seconds} [ content-id content_id]
credit-control-group cc_group_name
dynamic-rule order { always-first | first-if-tied }
egcdr threshold { interval interval
[ regardless-of-other-triggers ] | volume { downlink | total |
uplink } bytes }
route priority route_priority ruledef ruledef_name
analyzer { dns | file-transfer | ftp-control | ftp-data | h323
| http | imap | mipv6 | mms | pop3 | pptp | radius | rtcp | rtp
| rtsp | sdp | secure-http | sip [ advanced | basic-and-advanced
]
| smtp | tftp | wsp-connection-less | wsp-connection-oriented }
[ description description ]
tcp check-window-size
tcp mss tcp_mss { add-if-not-present | limit-if-present }
tcp packets-out-of-order { timeout timeout_duration|
transmit [ after-reordering | immediately ] }
end

```

**NOTES:**

- **rulebase** *rulebase\_name*: Specifies the name of the ACS rulebase. *rulebase\_name* must be an alphanumeric string of 1 to 63 characters.
- **action priority** *action\_priority* { [ **dynamic-only** ] | **static-and-dynamic** | **timedef** *timedef\_name* ] { **group-of-ruledefs** *ruledefs\_group\_name* | **ruledef** *ruledef\_name* } **charging-action** *charging\_action\_name* [ **monitoring-key** *monitoring\_key* ] [ **description** *description* ] }: Configures the priority order in which ruledefs are matched and the associated charging action.
  - *priority* must be an integer value in the range of 1-65535.
  - *monitoring\_key* must be an integer value in the range of 100000-4000000000.

Use the **no action priority** *action\_priority* command to remove the configured ruledef, group-of-ruledefs, and charging action.




---

**Important** Currently, the SMF does not support individual removal of ruledef, group-of-ruledefs, and charging action.

---

- **cca quota** { **holding-time** *holding\_time* **content-id** *content\_id* | **retry-time** *retry\_time* [ **max-retries** *retries* ] }: Configures the quota for the online charging.
  - *holding\_time*: must be an integer value in the range of 1-4000000000

- *content\_id*: must be an integer value in the range of 1-2147483647
- *retry\_time*: must be an integer value in the range of 0-86400
- *retries*: must be an integer value in the range of 1-65535
- **cca quota time-duration algorithm { consumed-time *seconds* [ plus-idle ] | continuous-time-periods *seconds* | parking-meter *seconds* } [ content-id *content\_id* ]**
  - **consumed-time**: must be an integer value in the range of 1-4294967295
  - **content-id**: must be an integer value in the range of 1-2147483647
  - **continuous-time-periods**: must be an integer value in the range of 1-4294967295
  - **parking-meter**: must be an integer value in the range of 1-4294967295
- **credit-control-group *cc\_group\_name***: Configures the online charging parameters used by this rulebase. *cc\_group\_name* must be an alphanumeric string of 1 to 63 characters.
- **dynamic-rule order**: Configures the order of dynamic rule matching vs the static rules in a rulebase.
- **egcdr threshold { interval *interval* [ regardless-of-other-triggers ] | volume { downlink | total | uplink } bytes }**: Configures the threshold for offline charging.
  - **interval**: must be an integer value in the range of 60-40000000.
  - **downlink**: must be an integer value in the range of 100000-4000000000. Default: 4000000000.
  - **uplink**: must be an integer value in the range of 100000-4000000000. Default: 4000000000.
  - **total**: must be an integer value in the range of 100000-4000000000.
- **route priority *route\_priority* ruledef *ruledef\_name* analyzer { dns | file-transfer | ftp-control | ftp-data | h323 | http | imap | mipv6 | mms | pop3 | pptp | radius | rtcp | rtp | rtsp | sdp | secure-http | sip [ advanced | basic-and-advanced ] | smtp | tftp | wsp-connection-less | wsp-connection-oriented } [ description *description* ]**: This command is used only on UPF.
  - *route\_priority* must be an integer value in the range of 0-65535.
  - *ruledef\_name* must be an alphanumeric string of 1 to 63 characters.
- **tcp check-window-size**: This command is used only on UPF.
- **tcp mss *tcp\_mss***: This command is used only on UPF. *tcp\_mss* must be an integer value in the range of 496-65535.
- **tcp packets-out-of-order { timeout *timeout\_duration* | transmit [ after-reordering | immediately ] }**: This command is used only on UPF.
  - *timeout\_duration* must be an integer value in the range of 100-30000. Default value is 5000.

## Defining UPF APN Profile in DNN Profile Configuration

This section describes how to configure the UPF APN profile in the existing DNN Profile Configuration.

```

configure
  profile dnn dnn_profile_name
    upf apn apn_name
  end

```

**NOTES:**

- **upf apn *apn\_name***: This command enables UPF APN profile configuration. This profile is configured under the existing DNN profile configuration. *apn\_name* must be the name of the APN template, and must be an alphanumeric string of 1 to 62 characters.

## Configuring QoS Parameters

This section describes how to configure the QoS parameters.

```

configure
  profile qos qos_profile_name
    ambr { ul uplink_ambr | dl downlink_ambr }
    arp { preempt-cap preemption_capability |
    preempt-vuln preemption_vulnerability |
    priority-level priority_level }
    max data-burst burst_volume
    priority qos_priority
    qi5 5qi_value
  end

```

**NOTES:**

- **ambr { ul *uplink\_ambr* | dl *downlink\_ambr* }**: Defines the Aggregate Maximum Bit Rate (AMBR) for the uplink (subscriber to network) and the downlink (network to subscriber) traffic.
- **arp preempt-cap *preemption\_capability***: Specifies the preemption capability flag. Options are:
  - MAY\_PREEMPT: Bearer may be preempted
  - NOT\_PREEMPT: Bearer cannot be preempted
- **arp preempt-vuln *preemption\_vulnerability***: Specifies the preemption vulnerability flag. Options are:
  - PREEMPTABLE: Bearer may be preempted
  - NOT\_PREEMPTABLE: Bearer cannot be preempted
- **arp priority-level *priority\_level***: Defines the Allocation and Retention Priority (ARP) for the service data. The default value of *priority\_level* is 8.
- **max data-burst *burst\_volume***: Defines the maximum data burst volume. *burst\_volume* must be an integer value in the range of 1–4095.
- **priority *qos\_priority***: Specifies the 5QI priority level. *qos\_priority* must be an integer value in the range of 1–127.
- **qi5 *5qi\_value***: Specifies the 5G QoS Identifier (5QI) for the authorized QoS parameters. *5qi\_value* must be an integer value in the range of 0–255.

## Verifying the Static PCC Rules Support Feature Configuration

This section describes how to verify the Static PCC Rules Support configuration.

Use the following show command to verify the feature configuration details.

### show full-configuration

The following is an example of this show command output.

```
active-charging service acs
charging-action cal
  arp priority-level 15 preempt-cap MAY_PREEMPT preempt-vuln PREEMPTABLE
  cca charging credit preemptively-request
  content-id 320001
  flow limit-for-bandwidth direction uplink peak-data-rate 1000000 peak-burst-size 1000000
  violate-action discard committedDataRate 2000000 committed-burst-size 2000000 exceed-action
  lower-ip-precedence
  nexthop-forwarding-address fa00:965a:c263:25::16/128
  qos-class-identifier 9
  service-identifier 32000
  tft packet-filter pfl
  tft-notify-ue
  tos af11 downlink
rulebase rb1
  cca quota time-duration algorithm parking-meter 1000 content-id 18000
  credit-control-group cg1
  dynamic-rule order first-if-tied
  egcdr threshold volume total 400000
  tcp packets-out-of-order transmit immediately
  action priority 95 timedef ruledef rd6 charging-action ca6 description ruledef
  action priority 96 ruledef rd3 charging-action ca5
  action priority 97 group-of-ruledefs grd3 charging-action ca4 monitoring-key 200000
  action priority 98 static-and-dynamic group-of-ruledefs grd2 charging-action ca2
  action priority 99 dynamic-only ruledef rd1 charging-action ca1 monitoring-key 100000
  action priority 100 dynamic-only group-of-ruledefs grd1 charging-action ca1 monitoring-key
  100000 description gruledefs
  route priority 1 ruledef rd1 analyzer dns description dns
exit
packet-filter pk1
  direction uplink
  ip local-port = 23
  ip protocol = 23
  ip remote-address = 10.10.10.0/24
  ip remote-port = 23
  ip tos-traffic-class = 23 mask = 10
  priority 4
exit
ruledef prepaidBgl
  multi-line-or all-lines
  rule-application charging
  ip any-match = TRUE
  ip server-ip-address range host-pool 12
  ip dst-address = 10.10.10.10
exit
urr-list urrlocal
  rating-group 1 service-identifier 1 urr-id 2
  rating-group 1 service-identifier 3 urr-id 2
exit
exit
```

Use the following show command to verify the group-of-ruledefs configuration details.

### show running-config

The following is an example of this show command output.

```
show running-config
profile network-element pcf pcf1
rulebase-prefix rbn
predefined-rule-prefix cbr
!
active-charging service acs1
group-of-ruledefs IPV6-whtlst-https_2300
  add-ruledef priority 1 ruledef IPV6-whtlst-https_2300_01
  add-ruledef priority 2 ruledef IPV6-whtlst-https_2300_02
  add-ruledef priority 3 ruledef IPV6-whtlst-https_2300_03
  add-ruledef priority 4 ruledef IPV6-whtlst-https_2300_04
  add-ruledef priority 5 ruledef IPV6-whtlst-https_2300_05
  add-ruledef priority 6 ruledef IPV6-whtlst-https_2300_06
  add-ruledef priority 7 ruledef IPV6-whtlst-https_2300_07
  add-ruledef priority 8 ruledef IPV6-whtlst-https_2300_08
  add-ruledef priority 9 ruledef IPV6-whtlst-https_2300_09
  add-ruledef priority 10 ruledef IPV6-whtlst-https_2300_10
  add-ruledef priority 11 ruledef IPV6-2dns-whtlst-https_2300_01
  add-ruledef priority 12 ruledef IPV6-2dns-whtlst-https_2300_02
  add-ruledef priority 13 ruledef IPV6-2dns-whtlst-https_2300_03
exit
group-of-ruledefs rdg1
  add-ruledef priority 10 ruledef rd2
  add-ruledef priority 12 ruledef rd1
exit
exit
```

## Predefined PCC Rules

### Feature Description

Most of the concepts applicable for static rules also apply for predefined rules. The configuration set, mechanism for QoS binding and pre-constructed QoS model remain the same.



#### Important

Predefined PCC Rules are applicable to both 4G and 5G calls.

### Predefined Rules vs Static Rules

This section lists the differences between the predefined and static rules.

- Predefined rule is identified by the **dynamic-only** keyword in the action priority associated with a ruledef under rulebase configuration.
- Predefined rules are not activated automatically but are enabled or disabled by PCF on a per rule basis. The PCF sends a PCC rule with the ruledef name alone or ruledef and rulebase names together as the rule ID to activate the predefined rule and sends the PCC rule map with null entry for the ruledef previously activated to deactivate a predefined rule.
- The QoS binding and modelling is not done for predefined rules at the time of configuration unlike the static rule. Instead during PDU session activation/modification the ECS configuration of activated ruledefs are considered to create or change the QoS model applicable for the session.



- On N4 interface, one PDR and corresponding FAR per ruledef activated by the PCF is sent to the UPF with ruledef name in the Activate predefined Rule IE and rulebase name is sent in Rulebase IE in default PDR. On rule removal, the corresponding PDR is removed.



**Note** The PCF sends the predefined rules, and activates these rules only if the UPF APN is configured with "rulebase" name. Otherwise, the PCF must send the rule name along with the "rulebase" name.

## Combined Application of Static, Predefined, and Dynamic Rules

All three static, predefined, and dynamic rules can coexist for a session. In such a case:

- Pre-constructed QoS model is prepared only for static rules. During PDU session activation/modification, any dynamic and predefined rules are evaluated to modify the QoS model and accordingly modifications are done on N1, N2, and N4 interfaces.
- If the rating-group and service ID for a dynamic rule are the same as that of a configured predefined and static rule, then the URR ID for the static and predefined rule is retained even for the dynamic rule.

# Support for Configuring the Bandwidth ID

## Feature Description

The SMF expects the user to configure the bandwidth limitation, for both downlink and uplink packets, in all charging actions, even if the bandwidth limitation configuration is the same for all the charging actions.

To optimise these configurations, the SMF allows the user to define a bandwidth ID to include all bandwidth related configurations and associate the bandwidth ID under the charging actions.

If the bandwidth value is changed, the new subscribers use the configured bandwidth values while the existing subscribers continue to use the old values.

## Limitations

The SMF imposes the following limitations related to the configuration of bandwidth-policy.

- Allows up to 64 k flow ID configurations within the bandwidth-policy
- Allows configuring up to a maximum of 64 bandwidth policies
- The maximum number of groups that can be configured per bandwidth policy is 1000.
- The maximum number of bandwidth IDs that can be configured per bandwidth policy is 1000.

## Configuring Bandwidth ID

Use the following configuration to define the bandwidth ID within the charging action.

```

configure
  active-charging service service_name
    bandwidth-policy policy_name
    flow limit-for-bandwidth id bandwidth_id group-id group_id
    group-id group_id direction { downlink | uplink }
    peak-data-rate peak_data_rate peak-burst-size
    peak_burst_size violate-action { discard | lower-ip-precedence }
    [ committed-data-rate committed_data_rate committed-burst-size
    committed_burst_size [ exceed-action { discard | lower-ip-precedence
    } ] ]
  exit
  active-charging service service_name
  charging-action charging_action_name
    flow limit-for-bandwidth bandwidth_id
  end

```

- **bandwidth-policy** *policy\_name*: Specifies the name of the bandwidth policy. This CLI option allows configuring up to a maximum of 64 bandwidth policies.
- **flow limit-for-bandwidth id** *bandwidth\_id*: Defines a bandwidth ID to include all the bandwidth related configurations within the charging action for predefined and static rules.

*bandwidth\_id* is an integer ranging from 1 to 65535.




---

**Note** The maximum number of bandwidth IDs that can be configured per bandwidth policy is 1000.

---

- If the bandwidth ID is configured and the individual uplink and downlink limit-for-bandwidth are also configured in the charging actions, then the bandwidth ID configuration takes the precedence.
- **group-id** *group\_id*: This command specifies the group ID as an integer ranging from 1 to 65535. The group ID identifies the QoS parameters such as MBR, GBR, and so on. Each group ID is mapped to a particular bandwidth ID.
- The maximum number of groups that can be configured per bandwidth policy is 1000.

## Verifying Bandwidth ID Configuration

Use the following show command to verify the bandwidth ID configuration.

```
show config-error
```

This show command helps in identifying any invalid configurations such as the configured bandwidth ID being removed but still defined in the charging action. For such invalid configurations, this show command displays appropriate errors as shown in the following example output:

```
show-config-error
```

```

ERROR COMPONENT          ERROR DESCRIPTION
-----
RuleBase                  Default bandwidth policy does not exist in rulebase <rba1> for charging
action <cal> .Dropping ruleDef <rdal>
RuleBase                  Default bandwidth policy does not exist in rulebase <rba6> for charging

```

```
action <ca1>.Dropping ruleDef <rda60>
RuleBase          Default bandwidth policy does not exist in rulebase <rba6> for charging
action <ca1>.Dropping ruleDef <rda61>
ChargingAction   Packet filter <pkt1234> configured for charging action <ca4> associated
with rulebase <rbl> does not exist
BandwidthPolicy  Uplink peak data rate less than committed data rate in charging action
<ca6>Dropping ruleDef <rd6>
```

# Generating UE Camping Report for PCF

## Feature Description

PCF needs to be aware of UE location, RAT type, access type, and other details to provision relevant policies during the PDU session life cycle. To facilitate this, during PCF initiated policy update procedure, the SMF sends "UeCampingRep" attribute in the response message based on the triggers enabled by PCF.

The SMF sends the UeCampingRep to PCF as per the Table 5.5.2.2-2 defined in 3GPP specification 29.512. When validation of all the PCF provided rules succeed, the SMF sends the UeCampingRep in the update response message to the PCF.

If validation of any of the rules fail, then the SMF sends the ueCampingRep in "PartialSuccessReport" as defined in 4.2.3.2 section of 3GPP specification 29.512.

The fields in the "UeCampingRep" IE are populated based on the following triggers set by PCF.

- Access type (AC\_TY\_CH)
- RAT change (RAT\_TY\_CH)
- User location change (SAREA\_CH)
- PLMN Change (PLMN\_CH)

The SMF supports the following attributes:

- accessType
- ratType
- servingNetwork
- userLocationInfo



### Important

The SMF currently does not support the ueTimeZone attribute.

## UPF Node Selection

The UPF Selection feature enables the 5GS and EPS core networks, during subscriber's session creation, to select an UPF for reduced latency on user plane and priority-based serviceability.

The SMF performs UPF selection based on certain query parameters such as DNN, PDU session type, and so on, and also based on the priority and load information of the UPF.

The network operator leverages this functionality for efficient handling of the user plane traffic based on priority, PDU session type, and so on. This functionality is also used for effective load balancing of the user plane connections across multiple UPFs.

## UPF Selection Based on Query Parameters

This section describes how the SMF selects the UPF based on certain selection parameters.

### Feature Description

The SMF performs UPF selection from a list of all UPFs having an active association based on certain selection criteria including the query parameters. These parameters consist of DNN, pdn-type-subscription, pdn-type-session, priority, load, and Dual Connectivity with New Radio (DCNR) (only for EPS).

The 5GS and EPS core networks apply the selection mechanism to select a UPF node during the creation of a subscriber session.

The UPF selection can be based on the load of the UPFs. The load-based UPF selection distributes calls among active UPFs associated with SMF. 3GPP specifies Load Control feature as optional feature over N4 reference points. This enables UPF to send its load information to CP functions.

To support load-based UPF selection, the SMF uses UPF-provided Load Control information in the following Packet Forwarding Control Protocol (PFCP) messages:

- Session Establishment Response
- Session Modification Response
- Session Deletion Response
- Session Report Request

Load Control procedure details are mentioned in *3GPP TS 29.244 v14.0.0 Release 14, section 6.2.3* and SMF adheres to the CP functionality.

### How it Works

The UPF initiates an N4 Association Setup request to set up an association with SMF.

The following is a high-level summary of how SMF selects the UPF node for the core network:

- The SMF selects the UPF node for EPS and 5GS sessions based on the following parameters:
  - DNN
  - DCNR (only for EPS calls)
  - pdn-type-subscription
  - pdn-type-session
- The SMF/PGW-C enables you to define the UPF selection criteria which it uses to query the appropriate node.

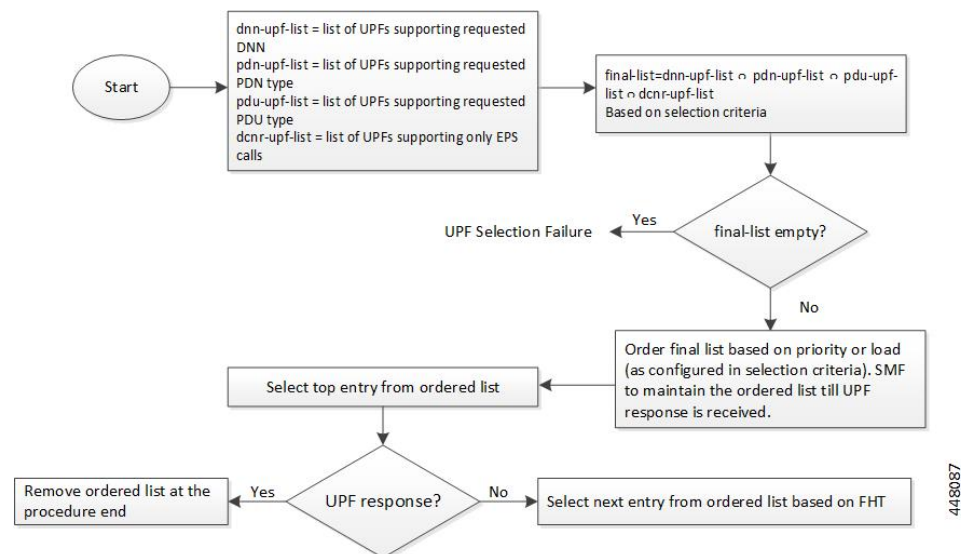
- If multiple UPFs match the SMF's selection criteria, then SMF selects the active UPFs and sorts them based on their priority and load information. The SMF then attempts to access the UPF one by one until the N4 Session Establishment is successful.
- The SMF stores the load information provided by UPF and uses it in selecting the UPF for new sessions being established. The SMF selects the less loaded UPF among the candidate (DNN based) active UPFs.
- The SMF considers priority and capacity configured statically against each UPF. In cases where UPF does not send the load information statically, configured capacity is considered while selecting the UPFs.

## UPF Selection Algorithm

The SMF determines the UPF node based on an algorithm.

The following figure depicts the UPF node selection workflow.

**Figure 111: UPF Node Selection Workflow**



The SMF lists the UPF nodes based on the priority assigned to the node. When there are multiple nodes with the same priority value, then the SMF selects a UPF experiencing the lowest level of load. The load parameter is applied only for UPFs that have the same priority.

When load is not available as a selection criteria, then SMF selects a random UPF when there are multiple UPFs with the same priority.

The SMF stores UPF order list based on priority. When a failure occurs, the SMF selects the next entry in the list based on failure handling template (FHT) configuration.

If priority is not available as a selection criteria and load is available as a selection criteria, then SMF selects least loaded UPF from the list of selected UPFs.



### Important

The SMF performs UPF selection only during initial call establishment. In 2021.01 and earlier releases, the support for UPF reselection during HO does not exist.

## Standards Compliance

The Load-based UPF Selection complies with *3GPP TS 29.244, Release 14* specification.

## Limitations

Post nodemgr POD restart, UPF association should be re-established for subsequent PDU session establishments to be successful.

## Configuring the UPF Selection Feature

This section describes how to configure the UPF Selection feature.

Configuring the UPF Selection feature involves the following steps:

1. [Defining the UPF Group, on page 579](#)
2. [Associating the UPF Group with UPF Network Element, on page 580](#)
3. [Defining UPF Selection Query Parameters, on page 581](#)
4. [Associating UPF Selection Query Parameters with DNN Profile, on page 582](#)

## Creating the ECGI-Group Profile for EPS Session

This section describes how to create an instance of the ECGI-Group Profile.

The ECGI-Group Profile allows you to configure the list of individual ECGI values and range.

Use the following configuration to create an ECGI-Group.

```

configure
  profile ecgi-group profile_name
  mcc mcc_value mnc mnc_value
  ecgi list [ ecgi_value1 ecgi_value2 ecgi_valueN ]
  ecgi range start start_value end end_value
end

```

### NOTES:

- **configure**: Enters the global configuration mode.
- **profile ecgi-group** *profile\_name*: Specifies the name of the ECGI Group Profile to enter the profile configuration. The **profile ecgi-group** supports configuration of maximum 16 PLMNs under an ecgi-group.
- **mcc** *mcc\_value* **mnc** *mnc\_value*: Specifies the MCC and MNC values.
- **ecgi list** [ *ecgi\_value1 ecgi\_value2 ecgi\_valueN* ]: Specifies the list of ECGI values to be configured. Accepted value is the 7-digit hex string E-UTRAN Cell ID. The SMF supports configuration of 64 ECGI values in the **ecgi list** under a PLMN.
- **ecgi range start** *start\_value* **end** *end\_value*: Specifies the start and end range of ECGI. Accepted start and end range of ECGI is the 7-digit hex string E-UTRAN Cell ID. **ecgi range** is an optional attribute. You can configure multiple ECGI range values. The SMF supports a maximum of 64 ECGI range under a PLMN.




---

**Important** The SMF ignores ECGI range values if the start range value is greater than the end range value.

---

### Verifying the ECGI-Group Profile Creation

This section describes how to verify if the ECGI-Group Profile is created.

The following configuration is a sample output of the **show running-config profile ecgi-group** command:

```
profile ecgi-group e1
mcc 123 mnc 45
  ecgi list [ 1234567 abcdef0 ]
  ecgi range start 1111111 end ffffffff
exit
exit
exit
```

### Creating the NCGI-Group Profile for 5GS Session

This section describes how to create an instance of the NCGI-Group Profile.

The NCGI-Group Profile allows you to configure the list of individual NCGI values and range.

Use the following configuration to create an NCGI-Group.

```
configure
profile ncgi-group profile_name
mcc mcc_value mnc mnc_value
ncgi list [ ncgi_value1 ncgi_value2 ncgi_valueN ]
ncgi range start start_value end end_value
end
```

#### NOTES:

- **configure**: Enters the global configuration mode.
- **profile ncgi-group** *profile\_name*: Specifies the name of the NCGI Group Profile to enter the profile configuration. The **profile ncgi-group** supports configuration of maximum 16 PLMNs under a *ncgi-group*.
- **mcc** *mcc\_value* **mnc** *mnc\_value*: Specifies the MCC and MNC values.
- **ncgi list** [ *ncgi\_value1 ncgi\_value2 ncgi\_valueN* ]: Configures the list of NCGI values to be configured. Accepted value is the 9-digit hex string NR Cell ID. The SMF supports configuration of 64 NCGI values in the **ncgi list** under a PLMN.
- **ncgi range start** *start\_value* **end** *end\_value*: Configures a specific NCGI range or multiple NCGI range lists. Accepted start and end range is the 9-digit hex string NR Cell ID. **ncgi range** is an optional attribute. You can configure multiple NCGI range values. The SMF supports a maximum of 64 NCGI range under a PLMN.




---

**Important** The SMF ignores NCGI range values if the start range value is greater than the end range value.

---

### Verifying the NCGI-Group Profile Creation

This section describes how to verify if the NCGI-Group Profile is created.

The following configuration is a sample output of the **show running-config profile ncgi-group** command:

```
profile ncgi-group n1
mcc 123 mnc 45
  ncgi list [ 123456789 12ab34CD9 ]
  ncgi range start 111111111 end FFFFFFFF
  exit
exit
exit
```

### Creating the Location-Area-Group Profile

The SMF associates one or more serving location details to a peer UPF. Location details include individual tracking areas and/or a range of tracking areas along with optional supported cells details.

Use the following configuration to create an instance of the location area group profile which is added under the ecgi-group and ncgi-group.

```
configure
  profile location-area-group profile_name
    tai-group tai_group_name
    ecgi-group ecgi_group_name
    ncgi-group ncgi_group_name
  end
```

#### NOTES:

- **tai-group** *tai\_group\_name*: Enters the global configuration mode.
- **profile location-area-group** *profile\_name* : Specifies the name of the location area group to enter the profile configuration.
- **tai-group** *group\_name*: Specifies the name of TAI group.
- **ecgi-group** *group\_name*: Specifies the name of ECGI group. This configuration is optional.
- **ncgi-group** *group\_name*: Specifies the name of NCGI group. This configuration is optional.

### Verifying the Location-Area-Group Profile Creation

This section describes how to verify if the Location-Area-Group Profile is created.

The following configuration is a sample output of the **show running-config profile location-area-group** command:

```
profile location-area-group lal
tai-group t1
ecgi-group e1
ncgi-group n1
exit
```

### Configuring Tracking Area Identity Group

The SMF provides configuration to define the supported list of Tracking Areas and Tracking Area Ranges for a PLMN. Upon enabling this configuration, the SMF sends the configured Tracking Area Identity (TAI) to the NRF during the SMF Service Registration.



Use the following configuration to define multiple TAI groups with different names.

```
configure
  profile tai-group group_name
    mcc mcc_value mnc mnc_value
    tac list [ tac_value1 tac_value2 tac_valueN ]
    tac range start tac_start_value end tac_end_value
  end
```

#### NOTES:

- **configure**: Enters the global configuration mode.
- **profile tai-group group\_name**: Specifies the name of the TAI Group to enter the profile configuration.
- **mcc mcc\_value**: Specifies the mobile country code.
- **mnc mnc\_value**: Specifies the mobile network code.
- **tac list [ tac\_value1 tac\_value2 tac\_valueN ]**: This keyword allows you to configure —
  - multiple PLMNs and TAC values within the specified TAI group
  - a maximum of 16 PLMNs within the specified TAI group
  - a maximum of 64 TAC values under a PLMN
- **tac range start tac\_start\_value end tac\_end\_value**: This keyword allows you to configure —
  - multiple TAC range values
  - a maximum of 64 TAC ranges under a PLMN




---

**Important** The SMF ignores TAC range values if the start range value is greater than the end range value.

---

- The SMF derives TAC list and TAC range from TAI group or NCGI group configuration. If the NCGI list already includes a TAC, you can skip the TAC configuration under TAI group. However, if the TAC is associated to a different UPF, this behavior is not applicable.

## Defining the UPF Group

This section describes how to configure the UPF group, and define pdn-session-type and other parameters for the UPF group profile.

Use the following configuration to define the UPF group profile.

```
configure
  profile upf-group upfgroup_name
    pdn-session-type [ ipv4 | ipv4v6 | ipv6 ]
    dcnr { false | true }

  end
```

#### NOTES:

- **configure**: Enters the global configuration mode.
- **profile upf-group** *upfgroup\_name*: Specify a name for the UPF group that must be associated to the specified UPF network configuration.
- **pdn-session-type** [ **ipv4** | **ipv4v6** | **ipv4v6** ]: Configures the PDN session type that is supported by UPF. The query parameters for **pdn-session-type** accept the "pdn-type-subscription" and "pdn-type-session". This parameter selects the pdn-type from UDM returned subscription or UE session, respectively.




---

**Note** If both "pdn-type-subscription" and "pdn-type-session" parameters are configured, SMF considers "pdn-type-subscription".

---

The SMF provides this CLI option to associate the UPF to servicing different PDN session types such as IPv4, IPv6, and IPv4v6. An UPF serves more than one PDN session type.

- **dcnr** { **true** | **false** }: Configures the Dual Connectivity with New Radio (DCNR) capability. The default configuration is false.




---

**Note** The DCNR capability is applicable only for 4G calls.

---

### Verifying the UPF Group Profile Configuration

This section describes how to verify if the UPF Group Profile is configured.

The following configuration is a sample output of the **show running-config profile upf-group** *upfgroup\_name* command:

```
profile upf-group ugl
pdn-session-type      ipv4v6
slice-group-list     [ slice1 ]
location-area-group-list [ loc1 ]
dcnr                  true
exit
```

### Associating the UPF Group with UPF Network Element

Use the following configuration to associate the defined UPF group with the UPF network element.

The UPF profile contains a list of UPFs configured in the SMF.

```
configure
  profile network-element upf upf_name
    upf-group-profile upfgroup_name
    capacity service_capacity
    priority priority_value
    dnn-list dnn_list
  end
```

#### NOTES:

- **profile network-element upf** *upf\_name*: Configures the UPF network configuration to which the defined UPF group is associated.

- **upf-group-profile** *upf\_group*: Configures the UPF group name that must be associated to the specified UPF network configuration.
- **capacity** *service\_capacity*: Indicates the static weight relative to other UPFs of the same type. *server\_capacity* must be an integer value in the range of 0-65535. Default: 10.
- **priority** *priority\_value*: Indicates the static priority relative to other UPFs of the same type. *priority\_value* must be an integer value in the range of 0-65535. Default: 1
- **dnn-list** *dnn\_list*: Specifies the list of DNNs supported by the UPF node.

### Verifying the UPF Configuration

This section describes how to verify the UPF configuration and the association of UPF group with UPF network element.

The following configuration is a sample output of the **show configuration** command:

```
profile network-element nrf nrf1
http-endpoint base-url http://1.1.1.111:8082
...
profile network-element upf upf2
upf-group-profile ug1
capacity 10
priority 1
n4-peer-address ipv4 1.2.3.4
n4-peer-port 8805
keepalive 60
dnn-list [ dnn1 intershat cisco.com ]
...
```

### Defining UPF Selection Query Parameters

This section describes how to configure parameters that enable SMF to select the UPF using the selection query.

Use the following configuration to define the UPF selection policy specific configuration.

```
configure
  policy upf-selection upfpolicy_name
    precedence priority_value [ dcnr | dnn | pdn-type-session |
pdn-type-subscription ]
  end
```

#### NOTES:

- **configure**: Enters the global configuration mode.
- **policy upf-selection** *upfpolicy\_name*: Specifies the UPF policy name that must be associated with the DNN profile. The SMF selects the UPF node with the lowest precedence value. The SMF selects the node with the highest precedence selection-criteria when the previous lower precedence criteria did not return any UPF. If the configured criteria are exhausted, and nodes are not selected, then the UPF selection policy fails.  
  
Within the precedence value, the intersection of UPFs from each criterion is performed to retrieve the UPF list.
- **precedence** *priority\_value* [ **dcnr** | **dnn** | **pdn-type-subscription** | **pdn-type-session** ]: Assigns the precedence value to the UPF policy. Specifies the DNN and other parameters for the UPF selection. The

**precedence** keyword allows a maximum of four precedence values to be configured under the UPF selection policy.

If the DNN profile does not have any UPF selection policy associated with it, then the SMF performs UPF selection using DNN, priority, and load information.

### Verifying the UPF Selection Policy Configuration

This section describes how to verify if the the UPF selection policy is configured.

The following configuration is a sample output of the **show running-config policy upf-selection** command:

```
#show running-config policy upf-selection
policy upf-selection polUpf1
  precedence 1
    [dnn location pdn-type-subscription]
  exit
  precedence 2
    [dnn pdn-type-session slice]
  exit
  precedence 3
    [dnn]
  exit
exit
```

### Associating UPF Selection Query Parameters with DNN Profile

This section describes how to associate UPF selection query parameters with DNN profile.

To associate the UPF selection policy with DNN profile, use the following configuration:

```
configure
  profile dnn profile_name
    upf-selection-policy upfpolicy_name
  end
```

#### NOTES:

- **configure**: Enters the global configuration mode.
- **profile dnn** *profile\_name*: Specifies the DNN profile name. *profile\_name* must be an alphanumeric string.
- **upf-selection-policy** *upfpolicy\_name*: Specifies the name of UPF selection policy that must be associated to the DNN profile.

### Verifying the Association of UPF Selection Policy and DNN Profile

This section describes how to verify if the UPF selection policy association with the DNN profile is established.

The following configuration is a sample output of the **show running-config profile dnn** *profile\_name* command:

```
profile dnn intershat
upf-selection-policy upfPoll
end
```

## UPF Selection OA&M Support

This section describes operations, administration, and maintenance information for this feature.

## Statistics

The following statistics are added in support of UPF node selection based on DNN, pdn-type-session, priority, and load.

- upf-selector

```
req_type="upf-selector",
```

```
status="Precedence:2 Dnn-Upf-List:3 Pdn-Type-Upf-List:2 Dcnr-Upf-List:0"
```

```
status="upf_selector_empty_upf_list"
```

```
status="upf_selector_invalid_upf_selection_policy"
```

Example:

```
smf_service_resource_mgmt_stats{app_name="SMF",cluster="Local",
data_center="DC",dnn="intershat",emergency_call="",instance_id="0",ip_req_type
="upf-selector",pdu_type="ipv4",procedure_type="PDU Session Establishment",
rat_type="NR",service_name="smf-service",status="Precedence:2 Dnn-Upf-List:3
Pdn-Type-Upf-List:2 Dcnr-Upf-List:0"} 1
```

## Co-located UPF Selection During Initial EPS Attach

This section describes how the SMF performs UPF selection during the initial EPS Attach procedure.

### Feature Description

The SMF performs co-located UPF selection based on the SGW-U node name received in the Create Session Request (CSR) message.

### How it Works

The SMF performs the following steps to handle co-located UPF selection during PDN Session Establishment in 4G network.

1. Upon receiving the CSR request, the SMF fetches the "SGW-U node name" and compares with the FQDN defined in UPF configuration.  
The SMF skips the existing UPF selection logic and uses the UPF selected by SGW-C.
2. In the absence of the SGW-U node name, the SMF follows the existing UPF selection algorithm.
3. The SMF uses the existing selection logic if it is unable to derive the UPF from the configuration based on the SGW-U node name.

### Configuring Node ID

Use the following configuration to select the co-located UPF.

```
configure
  profile network-element upf upf_name
    node-id value
  end
```

NOTES:

- **profile network-element upf** *upf\_name*: Specify a profile name for the UPF.
- **node-id** *value*: This keyword aids in configuring the node ID of UPF. The SMF compares this node name with SGW-U node name to select the co-located UPF. *value* is an alphanumeric string.

## Statistics Support

The SMF maintains the following statistics in support of this feature.

### **upf\_selection\_stats**

Description: Displays the total number of times the same co-located UPF is selected by SMF.

Metrics-Type: Counter

Labels:

- upf\_selection\_type
- upf\_fqdn
- preferred
- upf\_not\_associated
- upf\_profile\_not\_found
- upf\_not\_active
- n4\_failed
- pdu\_session\_type
- pdu\_subscription\_type
- snssai

Status:

- attempted
- failure

Reason: If the status is failure, the value can be one of the following:

- upf\_not\_associated
- upf\_profile\_not\_found
- upf\_not\_active
- n4\_failed

# Support for UPF Node Reports and Proprietary Session Reports

## Feature Description

The SMF triggers Packet Forwarding Control Protocol (PFCP) Node Report procedure as per the *3GPP TS 29.244, section 6.2.9*. The UPF sends this report to indicate a user plane path failure affecting all the PFCP sessions towards a remote GTP-U peer. The UPF notifies this failure to the SMF through User Plane Path Failure Report (UPFR). When the UPF detects a GTP-U path failure, the SMF clears the PDU sessions belonging to the GTP-U peer and UPF node ID.

In addition to the existing UPF session report, the SMF supports the following new proprietary report types:

- Graceful Termination Report (GTER) – This type of report is sent when the UPF is unable to recover a PDU session during Session Recovery (SR) or Inter-Chassis Session Recovery (ICSR).
- Session Replacement Report (SRIR) – This type of report is sent to replace a session due to identical GTP-U tunnel endpoint identifier (TEID) allocated by gNB. This is possible with the restart of gNB. In this case, the old session with the same TEID is deleted.
- Self-protection Termination Report (SPTER) – This type of report is sent to terminate a PFCP session during overload scenarios.

## Converged Core Refactoring Changes

This section describes the changes related to converged core refactoring in this chapter.

- The **namespace** keyword is added to the **show subscriber** CLI command to display the output pertaining to the respective namespace.
- For Node Report and Session Report SMF-protocol statistics:
  - **n4** prefix in the message names are removed
  - **smf** prefix in the statistic names are removed
  - **interface\_type** label is added in the query expression

## How it Works

This section describes how the SMF supports the UPF node report and the proprietary session reports.

### PFCP Node Report Handling

For proper handling of PFCP node report, the GTP-U peer address must include a non-unique secondary session key. The Common Data Layer (CDL) stores the peer address and the UPF IP address along with the session details. If the GTP-U peer address changes during idle to active transition procedure, N2 handover (HO), 5G to 4G HO, or 4G to 5G HO, the CDL database deletes the old key and adds the new one.

1. The UPF sends PFCP Node Report Request to the SMF along with the IP address of the failed GTP-U peer.

2. The SMF protocol checks the node ID, that is, the UPF IP address included in the request. If the node ID is not found or if the node ID is not in associated state, the SMF protocol sends a failure response.
3. If the node ID is found, the node manager queries the CDL for EPS session with the GTP-U peer IP address and node ID. The node manager sends bulk notification to the CDL to clear the corresponding sessions.
4. The CDL sends the notification to rest endpoint (REST-EP) pod to clear the sessions.
5. The REST-EP pod sends the subscriber clear notification to the SMF service based on the affinity. The SMF service clears the sessions on all interfaces.

## PFCP Session Report Handling

The UPF sends PFCP session report along with GTER, SRIR, and SPTER to the SMF. If the session is found, the SMF sends a successful PFCP session report response. Then, the SMF triggers the PDU session release procedure and deletes the sessions on all interfaces.

## Collision Handling

For the newly supported messages (node report and session report), the SMF triggers the PDU session release procedure. If the PDU session release procedure collides with the HO procedure, the SMF does not abort the HO procedure as the GTP-U peer IP changes during the HO. To achieve this, the PDU release procedure involves comparing the GTP-U peer IP address received in release request with the one present in the PDU session. If the two addresses are different, then the SMF aborts the release procedure.



### Important

The collision handling depends on the arrival time of the incoming HO message and **clear subscriber** command triggered by node report.

## Resiliency Handling

The SMF uses a retry timer to check and report any pending session deletions for a GTP-U peer. After the restart of SMF node manager, if any sessions are not deleted, then these sessions remain as is.

## Standards Compliance

The UPF Node Report and Session Report Support feature complies with *3GPP TS 29.244, version 15.6.0*.

## Limitations

This feature has the following limitations:

- If the CDL notifications are lost and the sessions are not cleared, the SMF node manager retries the bulk deletion operation only once after 10 minutes.
- If the node report request arrives and the system is in overload state, some CDL notifications are dropped. In this case, the SMF performs the session clean-up based on error indication report request from the UPF.
- The UPF currently sends only one Remote GTP-U peer in the Node Report request. So, the SMF can validate only one remote GTP-U peer.



## OAM Support

This section describes operations, administration, and maintenance information for this feature.

### Monitoring Support

An alarm is added to indicate that a GTP-U peer for a particular UPF has gone down. The alarm data includes GTP-U peer IP and UPF IP addresses.

Use the following commands to configure alert rules related to the UPF Node Report Request.

```
configure
  alerts rules group alert_group_name
  interval-seconds seconds
  rule rule_name
    expression promql_expression
    severity severity_level
    type alert-type
    annotation annotation_name
    value annotation_value
  exit
exit
```

- **alerts rules:** Specifies the Prometheus alerting rules.
- **group *alert\_group\_name*:** Specifies the Prometheus alerting rule group. One alert group can have multiple lists of rules. *alert-group-name* is the name of the alert group. The *alert-group-name* must be a string in the range of 0–64 characters.
- **interval-seconds *seconds*:** Specifies the evaluation interval of the rule group in seconds.
- **rule *rule\_name*:** Specifies the alerting rule definition. *rule\_name* is the name of the rule.

The following is a sample configuration.

```
configure
  alerts rules group NodeReportGTPURemotePeer
  interval-seconds 300
  rule NodeReportGTPURemotePeerDown
    expression smf_protocol_udp_res_msg_total{message_name="n4_node_report_req",
message_direction= \"inbound\", status=\"accepted\"}
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the UPF Sends Node Report Request to SMF"
  exit
exit
```

### Show Command Support

Use the **show subscriber all** command to view the configuration related to GTP-U peer IP address.

The following is a sample output.

```
[unknown] smf# show subscriber all nf-service smf
subscriber-details
```

```
{
  "subResponses": [
    [
      "supi:imsi-123456789012345",
      "gpsi:msisdn-223310101010101",
      "pei:imei-123456786666660",
      "psid:5",
      "dnn:intershat",
      "emergency:false",
      "rat:e-utran",
      "access:3gpp access",
      "connectivity:4g",
      "udm-sdm:10.84.17.111",
      "pcfGroupId:PCF-dnn=",
      "policy:2",
      "pcf:10.84.17.111",
      "upf:10.84.17.111",
      "upfEpKey:10.84.17.111:10.84.17.112",
      "ipv4-addr:poolv4/12.0.0.1",
      "ipv4-pool:poolv4",
      "ipv4-range:poolv4/12.0.0.1",
      "ipv4-startrange:poolv4/12.0.0.1",
      "gtp-peer:10.84.17.112",
      "peerGtpuEpKey:10.84.17.111:10.84.17.111",
      "namespace:smf"
    ]
  ]
}
```

Use the **show subscriber count peerGtpuEpKey** command to view the number of sessions associated with the specified GTP-U peer and the UPF node.



### Important

Use the **show subscriber count peerGtpuEpKey** command carefully and sensibly as it might impact the system performance.

The following is a sample output of **show subscriber count peerGtpuEpKey** command.

```
smf# show subscriber count peerGtpuEpKey 30.30.30.63:50.50.0.58
subscriber-details
{
  "sessionCount": 12568
}
```

## Statistics Support

The SMF maintains the following statistics to track the total number of attempted, successful, and failed node-level and session-level requests.

- SMF\_SERVICE\_STATS for the following procedure types:
  - upf\_node\_report\_pdu\_sess\_rel
    - attempted: Total number of attempted PDU session release requests triggered due to the node report.
    - successful: Total number of successful PDU session release requests triggered due to the node report.
    - failure: Total number of failed PDU session release requests triggered due to the node report.
  - upf\_sess\_report\_gter\_pdu\_sess\_rel

attempted: Total number of attempted PDU session release requests triggered due to the session report "GTER".

successful: Total number of successful PDU session release requests triggered due to the session report "GTER".

failure: Total number of failed PDU session release requests triggered due to the session report "GTER".

- SMF\_PROTOCOL\_UDP\_REQ\_MSG\_TOTAL for the following message types:
  - n4\_node\_report\_req
    - attempted: Total number of attempted N4 requests triggered due to the node report.
    - successful: Total number of successful N4 requests triggered due to the node report.
    - failure: Total number of failed N4 requests triggered due to the node report.
  - n4\_session\_report\_req
    - attempted: Total number of attempted N4 requests triggered due to the session report.
    - successful: Total number of successful N4 requests triggered due to the session report.
    - failure: Total number of failed N4 requests triggered due to the session report.
- SMF\_PROTOCOL\_UDP\_RES\_MSG\_TOTAL for the following message types:
  - n4\_node\_report\_res
    - attempted: Total number of attempted N4 responses triggered due to the node report.
    - successful: Total number of successful N4 responses triggered due to the node report.
    - failure: Total number of failed N4 responses due to the node report.
  - n4\_session\_report\_res
    - attempted: Total number of attempted N4 responses triggered due to the session report.
    - successful: Total number of successful N4 responses triggered due to the session report.
    - failure: Total number of failed N4 responses due to the session report.
- SMF\_DISCONNECT\_STATS triggered for the following disconnect reasons:
  - gtpu\_peer\_path\_failure : This statistic is triggered when the session is deleted due to the node report.
  - upf\_sess\_report\_gter\_pdu\_sess\_rel: This statistic is triggered when the session is deleted due to the session report.

The following is an example of the statistics:

Node Report SMF-service stats:

```
smf_service_stats{app_name="SMF",cluster="Local",data_center="DC",dnn="intershat",
emergency_call="false",instance_id="0",pdu_type="ipv4",
procedure_type="upf_node_report_pdu_sess_rel",qos_5qi="",rat_type="NR",
reason="",service_name="smf-service",status="attempted",up_state=""}
```

```
smf_service_stats{app_name="SMF",cluster="Local",data_center="DC",dnn="intershat",
emergency_call="false",instance_id="0",pdu_type="ipv4",
```

```
procedure_type="upf_node_report_pdu_sess_rel", qos_5qi="", rat_type="NR",
reason="", service_name="smf-service", status="success", up_state="" } 1
```

#### Session Report SMF-service stats:

```
smf_service_stats{always_on="", app_name="smf", cluster="smf", data_center="unknown",
dcnr="", dnn="intershat", emergency_call="false", instance_id="0", pdu_type="ipv4",
procedure_type="upf_sess_report_gter_pdu_sess_rel", qos_5qi="", rat_type="NR",
reason="", service_name="smf-service", status="attempted", up_state="" } 1
```

```
smf_service_stats{always_on="", app_name="smf", cluster="smf", data_center="unknown",
dcnr="", dnn="intershat", emergency_call="false", instance_id="0", pdu_type="ipv4",
procedure_type="upf_sess_report_gter_pdu_sess_rel", qos_5qi="", rat_type="NR",
reason="", service_name="smf-service", status="success", up_state="" } 1
```

#### Node Report SMF-protocol stats:

```
smf_proto_udp_req_msg_total{app_name="smf", cluster="smf", data_center="unknown",
instance_id="0", message_direction="inbound", message_name="n4_node_report_req",
msgpriority="", service_name="smf-protocol", status="accepted",
transport_type="origin"} 15
```

```
smf_proto_udp_res_msg_total{app_name="smf", cause="1", cluster="smf",
data_center="unknown", instance_id="0", message_direction="outbound",
message_name="n4_node_report_res", msgpriority="", service_name="smf-protocol",
status="accepted", transport_type="origin"} 15
```

#### Session Report SMF-protocol stats:

```
smf_proto_udp_req_msg_total{app_name="smf", cluster="smf", data_center="unknown",
instance_id="1", message_direction="inbound", message_name="n4_session_report_req",
msgpriority="", service_name="smf-protocol", status="accepted",
transport_type="origin"} 43
```

```
smf_proto_udp_res_msg_total{app_name="smf", cause="1", cluster="smf",
data_center="unknown", instance_id="1", message_direction="outbound",
message_name="n4_session_report_res", msgpriority="", service_name="smf-protocol",
status="accepted", transport_type="origin"}
```

The SMF also maintains labels to track the number of session deletions due to the node report and session report types – GTER, SRIR, and SPTR.

For example, the label "LABEL\_DISC\_PDNREL\_GTER\_SESSION\_REP" is added to track the session deletion due to the presence of GTER.

## Support for Session Report Rejection Procedure

### Feature Description

The SMF rejects the UPF-originated Session Report Request with a specific cause code during any mismatch in the charging configuration of SMF and UPF.

For any session report rejection by the SMF, the UPF locally purges the sessions. The SMF is unaware of the purging operation and continues to send the N4 message to the UPF. This action triggers the UPF to send “context not found” message to the SMF for the locally purged sessions.

This behavior impacts the UE experience and results in the loss of charging data. So, the current implementation of handling the session report errors is modified to avoid local purging of sessions on the UPF and also to support graceful clearing of sessions.

With this modification, the UPF ignores the Session Report Error Response. The SMF triggers the Session Deletion Request followed by the rejection of Session Report. The UPF responds to the delete request and clears the session gracefully.

The existing Failure Handling (FH) configuration introduces a new parameter “N4SessionReportReq” to control the UPF from locally purging the rejected sessions. This CLI also triggers the SMF to send a Session Deletion Request after the Session Report rejection.

## Relationships

This feature involves implementing some behavioral changes to the SMF and the UPF. The new CLI configuration aids in controlling this behavior. For details on the UPF behavioral changes, see the *UCC 5G UPF Configuration and Administration Guide*.

## Configuring FH Action for Handling Session Report Errors

This section describes how to define the parameter within the UPF failure handling configuration to gracefully handle the session report errors.

When the SMF rejects the Session Report Request message and the failure handling configuration includes the parameter, the SMF supports the following failure handling actions:

- **ignore**: Ignores the error and does not take any further action
- **terminate**: Terminates the session (Triggers the Session Deletion Request)

During this scenario, if the failure handling configuration is unavailable, the SMF does not initiate the Session Deletion Request.

### configure

```
profile failure-handling profile_name
  interface pfcpc message N4SessionReportReq
    cause-code cause_ID
    action { ignore | terminate }
  end
```

### NOTES:

- **profile failure-handling**: Specifies the UPF profile that is associated with Failure Handling Template (FHT).
- **interface pfcpc message N4SessionReportReq**: Specifies the failure handling for N4 Session Report Request.
- **cause-code cause\_ID**: Specifies the error codes that the SMF receives in the failure response message from the UPF. *cause\_ID* can be any integer from 2 through 255. The cause code value can be separated by either '-' or ',' or both. For example, **cause-code 72-74,76,78-100**
- **action { ignore | terminate }**: Specifies the action to perform based on the error cause code received in the failure response message from the UPF.
  - **ignore**: Specifies to ignore the session.
  - **terminate**: Specifies to terminate the session.

## Verifying the Feature Configuration

Use the **show running-config** CLI command to verify if the feature is enabled.

### **show running-config**

The following configuration is a sample output of the **show running-config** command:

```
show running-config profile failure-handling interface pfcf
profile failure-handling FH1
interface pfcf message N4SessionEstablishmentReq
  cause-code pfcf-entity-in-congestion action retry-terminate max-retry 2
  cause-code system-failure action terminate
  cause-code service-not-supported action terminate
  cause-code no-resource-available action retry-terminate max-retry 3
  cause-code no-response-received action retry-terminate max-retry 1
  cause-code reject action terminate
exit
interface pfcf message N4SessionModificationReq
  cause-code mandatory-ie-incorrect action terminate
  cause-code session-ctx-not-found action terminate
  cause-code reject action terminate
exit
interface pfcf message N4SessionReportReq
  cause-code 69 action terminate
  cause-code 72-74,76,78-100 action terminate
exit
exit
```

## OAM Support

This section describes operations, administration, and maintenance information for this feature.

## Statistics Support

The SMF supports the following disconnect reasons as part of “smf\_disconnect\_stats”:

- smf\_sess\_pdn\_rel\_peer\_request\_reject — This disconnect reason is applicable for 4G and WiFi calls.
- smf\_sess\_pdu\_rel\_peer\_request\_reject — This disconnect reason is applicable for 5G calls.

## Outer Header Format

The SMF accepts the new format of the Outer Header information element (IE) from the UPF. The Packet Detection Rule (PDR) of Packet Forwarding Control Protocol (PFCP) session includes this IE. The Outer Header IE is present in the N4 Session Establishment Request message sent over the Sx interface. The version 16.4.0 of 3GPP TS 29.244 specification defines the format of this IE.

The following table identifies the encoding format of Outer Header Creation Description field. It takes the form of a bitmask where each bit indicates the outer header to be added to the outgoing packet. Note that the receiver (SMF) ignores the spare bits.

Octet / Bit	Outer Header Created in the Outgoing Packet
5/1	GTP-U/UDP/IPv4
5/2	GTP-U/UDP/IPv6

Octet / Bit	Outer Header Created in the Outgoing Packet
5/3	UDP/IPv4
5/4	UDP/IPv6
5/5	IPv4
5/6	IPv6
5/7	C-TAG
5/8	S-TAG
6/1	N19 Indication
6/2	N6 Indication
6/3	TCP/IPv4
6/4	TCP/IPv6

**NOTE:**

- Currently, the UP or UPF does not support the following values of Outer Header Creation Description:
  - IPv4
  - IPv6
  - C-TAG
  - S-TAG
  - N19 Indication
  - N6 Indication
- The third and fourth bits of sixth Octet (that is, 6/3 and 6/4) are spare bits (that is, not part of 3GPP TS) used for LI over TCP.

**Important**

The SMF and the UPF must support the same version of Outer Header IE for a successful session establishment.







## CHAPTER 36

# RADIUS Client for SMF

- [Feature Summary and Revision History, on page 595](#)
- [Feature Description, on page 596](#)
- [How it Works, on page 601](#)
- [Configuring the RADIUS Client, on page 621](#)
- [RADIUS Test CLI support, on page 634](#)
- [RADIUS Client OA&M Support, on page 636](#)

## Feature Summary and Revision History

### Summary Data

**Table 173: Summary Data**

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

## Revision History

*Table 174: Revision History*

Revision Details	Release
Added support for the following: <ul style="list-style-type: none"> <li>• PAP, CHAP, and MSCHAP-based RADIUS authentication</li> <li>• Multiple RADIUS NAS-IP source addresses</li> <li>• Handling RADIUS Disconnect and CoA Requests</li> <li>• RADIUS Accounting on SMF</li> <li>• New attributes in the RADIUS Access Response message</li> </ul>	2020.02.5.t1
First introduced.	Pre-2020.02.0

## Feature Description

Remote Authentication Dial-In User Service (RADIUS) is a client and server protocol. The RADIUS client is typically a Network Access Server (NAS) and the RADIUS server is usually a daemon process running on a UNIX or Windows NT machine. The client passes user information to designated RADIUS servers and acts on the response that is returned. RADIUS servers receive user connection requests, authenticate the user, and then return the configuration information necessary for the client to deliver service to the user.

RADIUS provides Authentication and Accounting services to the users. The SMF provides the following configuration support to —

- add RADIUS server details
- enable RADIUS accounting and authentication
- add RADIUS interface as an option for virtual APN configuration within DNN profile
- enable CC trigger reporting
- define volume and time limits

The RADIUS Client feature supports the following functions:

- **Server Selection**

RADIUS servers are configured with IP:Port as the key. The **algorithm** CLI specifies the failover or load balancing algorithm to select the RADIUS server to which the authentication or accounting request must be sent. Servers that are marked "dead" are not considered for selection until they are marked "alive". The supported algorithms are first-server and round-robin.

- **First-server**—Specifies that the request must be sent to RADIUS server with the highest priority. If the server becomes unreachable, the request is sent to the server with the next highest configured priority. This is the default algorithm.
- **Round-robin**—Specifies that the request must be sent based on load balancing in a circular queue manner. The server that is last used is stored to maintain the round-robin selection. The order of the list is purely based on the configuration sequence.

- **Monitor Server and Dead Server Detection**

Monitor Server revisits the server database and marks the server which has not received response beyond the configured "response-timeout" value after the first request is sent. The server is marked "dead" and remains in dead-state for minutes configured as "deadtime". After the "deadtime" elapses, the server's dead-variable is reset again to mark it as ready to process requests. If the server is still not reachable, it is marked "dead" as part of the next request response timeout.

- **Timeout and Retry**

After a server is selected and request is sent to the server, an entry is maintained in the request queue until response is received from the RADIUS server or until timeout occurs. Monitor Requests is called to check on the requests queue for response timeouts and retry. It walks through all the entries and checks if any request timeout value configured as "timeout" is hit. For such requests, if the number of retries is less than the configured "max-retries" value, the request is resent to the RADIUS server. Else, if the "max-retries" count is reached, the request is deleted from the request queue. After a request is deleted, even if response comes for such requests, the response is discarded and not sent to the user.

## Architecture

### RADIUS Integration in Mobile CNAT Architecture

The Mobile CNAT architecture has four distinct layers:

1. **Cloud**—Host OS + Kubernetes installation.
2. **Runtime**—Plugins to Kubernetes provided by the Cloud. This layer includes the container runtime (docker version) and Kubernetes plugins for volume (storage), networking, and load balancing.
3. **Orchestration**—Kubernetes functionality. Kubernetes provides abstractions for provided plugins (networking, volumes, load balancing) so that the CNAT components can be unaware of them.
4. **Mobile CNAT Components**—Application layer where the applications are built for mobility depending only on Kubernetes as much as possible.

5GC Network Functions (NFs) run in the Application or CNAT Component layer of this architecture. RADIUS Client is an integral part of the SMF.

### RADIUS Client Integration in SMF

The SMF consists of loosely coupled microservices. The microservice decomposition is based on the following three-layered architecture:

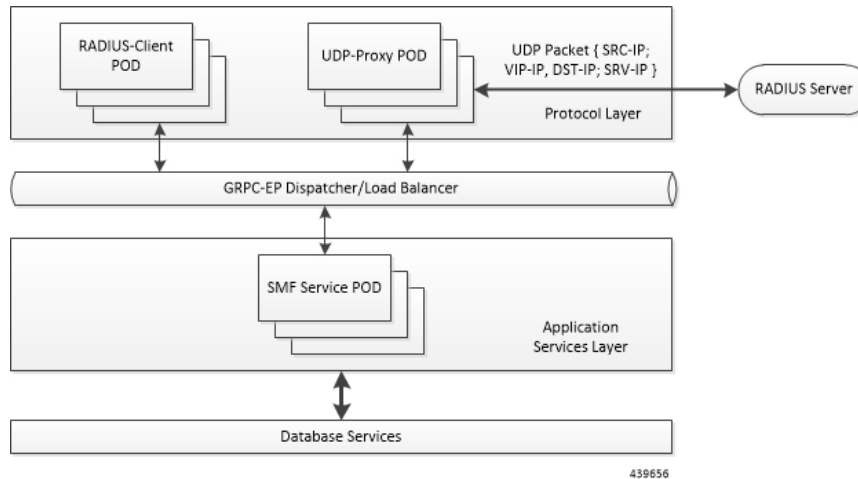
1. **Layer 1**—Protocol and Load Balancer services (stateless)
2. **Layer 2**—Application services (stateless)

### 3. Layer 3—Database services (stateful)

The Protocol layer integrates with the RADIUS Client POD.

The following figure illustrates the integration of RADIUS Client in SMF.

**Figure 112: RADIUS Client Integration**



**Radius-EP App (RADIUS-Client POD)**—The RADIUS Client functionality is added in a new POD. It handles RADIUS protocol-specific functions such as authentication and accounting.

**SMF Service App (SMF Service POD)**—The SMF Service App provides PDU session service. During session establishment, the SMF service decides if the secondary authentication is required or not, and acts accordingly.

**UDP-Proxy App (UDP-Proxy POD)**—The UDP-Proxy App is enabled with host-networking and, sends and receives packets using external Virtual-IPs. All RADIUS packets are transmitted and received from an outside cluster using this application.

## RADIUS Authentication

Authentication and key management are fundamental to the security of mobile networks because they provide mutual authentication between users and the network.

5G defines various authentication methods to authenticate a user. In the 5G architecture, the serving network authenticates the Subscription Permanent Identifier (SUPI), and key agreement between the UE and the network using primary authentication mechanism.

5G supports EAP-based secondary authentication between the UE and the network. The SMF performs the role of the EAP Authenticator and relies on external AAA server (for example, RADIUS server) to authenticate and authorize the UE's request for PDU session establishment.

The RADIUS Client function resides within the SMF to enable the generic Cloud Native 5G RADIUS functionality for authentication purposes. When the RADIUS Client feature is enabled, the SMF performs secondary authentication with the configured external RADIUS server as per 3GPP TS 23.501.

For information on enabling the RADIUS Client feature, see [Configuring the RADIUS Client, on page 621](#).

## RADIUS Accounting

Accounting collects and sends subscriber usage and access information used for billing, auditing, and reporting. For example, user identities the start and stop times, performed actions, number of packets, and number of bytes. Accounting enables an operator to analyze the services that the users access and the amount of network resources they consume. Accounting records comprise accounting Attribute Value Pairs (AVPs) and are stored on the accounting server. This accounting information can then be analyzed for network management, client billing, and/or auditing.

The SMF implements the RADIUS Accounting functionality through the use of CLI configuration. For more details on the configuration, see [Configuring the RADIUS Client, on page 621](#).

If the RADIUS accounting is enabled and server-group is configured within the DNN profile, the SMF sends server-group as AAA group in charging-params in N4 session establishment request. When the SMF sends AAA group which is not present on UPF, then it does not account the traffic for static and predefined rules in RADIUS URR and fails to report. In this scenario, the SMF considers only the dynamic rules traffic for accounting in the RADIUS URR.

## RADIUS Access Management

RADIUS supports the following timeout functionality:

- **Idle Timeout**—The SMF supports CP-Idle-Timeout which handles the Idle Timeout functionality of Control-Plane. The same functionality is leveraged for the idle timeout value received in the Radius-Access-Accept message.

The RADIUS returned values have higher precedence over the configuration unless there is a specific configuration to choose between RADIUS returned values and the pre-existing configuration in SMF.

- **Session Timeout**—The SMF supports Absolute-Session-Timeout which handles the Session Timeout functionality of a session. This functionality is leveraged for the session timeout value received in the Radius-Access-Accept message.

The RADIUS returned values have higher precedence over the configuration unless there is a specific configuration to choose between RADIUS returned values and the pre-existing configuration in SMF.

## RADIUS NAS-IP Support

SMF supports the RADIUS NAS-IP address functionality for accounting and authentication requests.

In releases prior to 2021.1.0, only one common RADIUS NAS-IP address was used for all requests. This feature is extended to support multiple RADIUS NAS-IP source addresses.

The NAS-IP configuration is supported at the following levels:

- Global NAS-IP
- Global accounting NAS-IP
- Per server-group common NAS-IP
- Per server-group accounting NAS-IP

The selected NAS-IP is encoded in authentication or accounting requests as per RFC2865 and is also used in the "source-ip" address of outbound UDP packets. This feature supports only the IPv4 NAS-IP address.

For more information, see the [Configuring RADIUS NAS-IP, on page 626](#) section.

## Handling RADIUS Disconnect and CoA Requests

Dynamic Authorization Client (DAC) initiates Disconnect-Request packet through UDP port to terminate the user session(s) on Network Access Server (NAS). It also discards all the associated session contexts.

The NAS responds with a Disconnect-ACK message if the session is identified, removed, and no longer valid. The NAS sends a Disconnect-NAK message if it is unable to disconnect the session.

This feature uses a combination of the following session keys to identify the sessions for termination:

- 3GPP-IMSI + 3GPP-NSAPI
- ACCT-SESSION-ID
- CALLED-STATION-ID (DNN) + FRAMED-IP-ADDR
- CALLED-STATION-ID (DNN) + FRAMED-IPV6-PREFIX



### Important

If multiple key combination is provided for the same session, it is accepted. However, if the multiple key combination leads to multiple session contexts or non-existing session context, the behavior is non-deterministic.

The SMF supports only one session context per Disconnect-Message (DM) request. The SMF supports the following attributes in the DM request to identify the NAS and the user sessions to be terminated.

Attribute	Reference Specification	Encoding Type
3GPP-IMSI	3GPP 29.061 - 16.4.7.2-1	String
3GPP-NSAPI	3GPP 29.061 - 16.4.7.2-10 3GPP 29.561 – 11.3	String
Accounting-Session-Id	RFC2866	String
FRAMED-IP	RFC2865 - 5.1	IPV4 Address
FRAMED-IPV6-PREFIX	RFC3162	PrefixLen & String
CALLED-STATION-ID (DNN)	RFC2865 - 5.30	String
NAS-IP-Address	RFC2865 – 5.4 (optional)	String
NAS-Identifier	RFC2864 – 5.32 (optional)	String

The SMF silently discards other attributes present in the DM request if the packet decoding is successful.

The SMF supports the following attributes in the DM ACK or NAK response.

Attribute	Reference Specification	Encoding Type
ERROR-CAUSE	RFC5176 – 3.5	Integer
REPLY-MESSAGE	RFC2865 – 5.18	String

The RADIUS endpoint (radius-ep) pod supports the following error codes if the Disconnect Request is rejected by radius-ep:

- 402 (Missing Attribute) - Triggered due to invalid key combination
- 403 (NAS Identification Mismatch) - Triggered if NAS-IP attribute in DM request does not match the endpoint COA-NAS VIP-IP or if NAS-Identifier attribute in the request does not match NAS identifier configuration within RADIUS Dynamic Authorization or CoA configuration
- 407 (Invalid Attribute) - Triggered due to format error, encode error, and so on
- 405 (Unsupported Service) - Triggered if the request is not a disconnect request
- 503 (Session Context Not Found) - Triggered if the session cannot be located

For more information on configuring this feature, see the [Configuring the Session Disconnect Feature, on page 632](#) section.

## How it Works

This section describes how the SMF supports RADIUS authentication and accounting functionality.

### RADIUS Interaction for Authentication

The RADIUS server supports various methods to authenticate the user. When the server is provided with the username and original password of the user, it can support Point-to-Point Protocol (PPP), Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), or Microsoft CHAP (MSCHAP), UNIX login, and other authentication methods.

In releases prior to 2021.01.0: The SMF uses only MSISDN values for user authentication.

In release 2021.01.0 and later: The SMF supports user authentication using PAP, CHAP, or MSCHAP protocol. The SMF configuration aids in the protocol selection for the user authentication. If the secondary authentication is enabled in DNN profile, the SMF interacts with the RADIUS server to perform RADIUS authentication. To implement the authentication, the RADIUS client residing within the SMF sends the User-Name and User-Password attributes in Access-Request message to the RADIUS server.

The SMF uses more attributes to facilitate the RADIUS authentication function. For the complete list of attributes supported, see the [RADIUS Attribute Definition, on page 612](#) section.

The RADIUS server validates the user with the authentication information. If the validation is successful, the server sends the Access-Accept response to the SMF.

#### PAP-, CHAP-, MSCHAP-based Authentication

The SMF decodes the Protocol Configuration Options (PCO), Extended PCO (ePCO), or Additional PCO (APCO) IE received from UE. Then, the SMF retrieves the values related to PAP (User Name and Password), CHAP (Challenge and Response), or MSCHAP (Challenge and Response) from the IE. If any of the protocols have higher precedence in configured priority under DNN, the SMF sends the received values in RADIUS Access-Request message to the RADIUS server.



**Note** The SMF does not include the authentication information received from the UE in the RADIUS Access-Request message if the priority is not configured.

By default, the SMF uses the configured host password under DNN for authentication until additional configuration is enabled to use the password received in PCO, ePCO, or APCO. The SMF allows the operator to configure the host password at DNN profile either in plain-text or encrypted form and always displays the same in encrypted format only wherever applicable.

The SMF sends MSISDN as the User Name if the UE does not provide the username explicitly in PCO IE for PAP-based authentication.

For CHAP-based authentication, the SMF converts the received CHAP Challenge and Response to MSCHAP if the **convert-to-mschap** command option is enabled, CHAP is enabled, and the received CHAP Response length is 49 bytes. By default, the SMF uses MSCHAPv1 as the authentication algorithm.

For MSCHAP-based authentication, the SMF sends User Name, Challenge, and Response received in PCO to the RADIUS server if Protocol ID is LCP and LCP container specifies the algorithm as CHAP/MSCHAPv1 (128) as per RFC 2433 or CHAP/MSCHAPv2 (129) as per RFC 2795.

The SMF forwards the authentication information from RADIUS server to UE in Create-Session-Response PCO/EPCO/APCO IE for a 4G/Wi-Fi session, and in N1 Container EPCO IE for a 5G session.

Consider the following important points while implementing the RADIUS authentication functionality.

- Perform the length validation of different AVPs applicable for this feature based on RFC 2865. Also, reject the authentication if any violation is identified.
  - The minimum length of CHAP Challenge is 5 bytes (even though it is 1 byte as per RFC 1334 and RFC 1994).
- The SMF sends the received authentication information from UE to RADIUS server based on the configured authentication algorithm at DNN level. The SMF does not manipulate any data received from UE and it only applies the configurations related to authentication before sending the information to RADIUS server.
- The SMF does not validate the use case of incrementing the Identifier value for every authentication as it does not allow multiple authentication during the PDU session lifetime.
- The SMF sends the encrypted NULL (empty) password in Access-Request when it receives empty password from UE and no host level password configured at SMF or **password-use-pco** option is enabled.
- The SMF falls back to the default authentication where Access-Request carries the configured server secret as User Password in the following scenarios:
  - If none of the algorithm preference is enabled with priority
  - If the UE provided information is not applicable for the configured algorithm preferences, if any
  - When the UE sends the empty PAP or CHAP containers without any data (the container length is 0)
- The SMF rejects the authentication in the following scenarios:
  - When there is no other algorithm configured for authentication



- Whenever there is a mismatch in CHAP identifier received in both CHAP Challenge and CHAP Response containers (the SMF currently copies the CHAP-ID from CHAP Challenge container)
  - CHAP-ID in CHAP Password must be taken from CHAP Response as per RFC 2865.
  - Response Identifier must be copied from the Identifier field of the Challenge Response as per RFC 1334.
  - Whenever the validation criteria of the current algorithm fails
- The SMF allows to configure the same priority through CLI for different algorithms because configuring 0 explicitly disables the configuration. In this scenario, any one of the algorithms is considered and the selection is purely implementation dependent. It is the responsibility of operator to ensure different algorithms have different priorities to resolve the conflicts whenever UE sends multiple authentication containers to the SMF.
- The SMF allows to configure the **password-use-pco** option without configuring PAP due to the limitation of Yang defined syntax format. The same is applicable for **convert-to-mschap** option. But the functionality will work only if the corresponding algorithm is enabled with the valid priority.
- By default, the SMF encrypts the operator given Host level password using AES-128-CFB encryption algorithm, if it's a plain-text. It ignores the encryption if the operator gives the already encrypted password which has to meet the AES-128-CFB encryption standard.
- By default, the SMF considers the authentication algorithm as MSCHAPv1(128) whenever the received CHAP Challenge and Response converted to MSCHAP if received CHAP-Response length is 49 bytes and **convert-to-mschap** option is enabled.
- The following are the list of MSCHAP specific AVPs supported at SMF and its RFC references:
  - MSCHAP-CHALLENGE (MSCHAP) □ RFC2548 Section 2.1.2
  - MSCHAP-RESPONSE □ RFC2548 Section 2.1.3
  - MSCHAP2-RESPONSE □ RFC2548 Section 2.3.2
  - MSCHAP-ERROR □ RFC2548 Section 2.1.5
  - MS-CHAP2-Success (RFC 2548, Section 2.3.3) is not supported as there is no clear information on MS-CHAP success AVP for v1 in RFC 2548.
- When the RADIUS server sends both MSCHAP-Error and Reply-Message AVPs in Access-Reject message, the preference is given to MSCHAP-ERROR while filling the CHAP container for NACK in PCO/APCO/EPCO. MSCHAP-Error is common for both MSCHAPv1 and MSCHAPv2 algorithm and it is encapsulated in the Message field of the CHAP Failure container.
- In MSCHAP, only the authentication functionality is supported.

**Important**

The SMF uses the inbuilt encryption algorithm “AES-128-CFB” for encrypting the host level password (outbound password) provided by NETCONF-YANG data model. The SMF Ops Center creates a global key, for AES-128-CFB encryption, which is used for encrypting the operator given plain-text password. It shares the key with all the pods via SSH for decrypting the encrypted data in the respective pods. The key is exported as a ENV variable “CONFD\_AES\_KEY” in SMF-SERVICE pod. If the operator wishes to configure the already encrypted password, then the AES-CFB-128 encrypted string should be prefixed with “\$\$” as follows, \$\$<encrypted-data> to indicate that the given input is already AES-128-CFB encrypted string to NETCONF-YANG model.

For CLI details associated with authentication, see the [Configuring the RADIUS Client, on page 621](#) section.

## RADIUS Authentication Attributes

### RADIUS Access Request Attributes

The following table lists the supported attributes in the RADIUS Access-Request message.

Attribute	Reference Specification	Encoding Type
USER-NAME	RFC2865 - 5.1	String
PASSWORD	RFC2865 - 5.2	Encrypted String
CALLING-STATION-ID	RFC2865 - 5.31	String
CALLED-STATION-ID	RFC2865 - 5.30	String
NAS-IP-ADDRESS	RFC2865 - 5.4	IPv4 Address
NAS-IDENTIFIER	RFC2865 - 5.32	String
SERVICE-TYPE	RFC2865 - 5.6	Octets - 4 bytes
FRAMED-PROTOCOL	RFC2865 - 5.7	Octets - 4 bytes
NAS-PORT-TYPE	RFC2865 - 5.41	Octets - 4 bytes
NAS-PORT	RFC2865 - 5.5	Octets - 4 bytes
3GPP-IMSI	3GPP 29.061 - 16.4.7.2-1	String
3GPP-CHARGING-ID	3GPP 29.061 - 16.4.7.2-2	Octets - 4 bytes
3GPP-PDP-TYPE	3GPP 29.061 - 16.4.7.2-3	Octets - 4 bytes
3GPP-CHARGING-GATEWAY-ADDR	3GPP 29.061 - 16.4.7.2-4	IPv4 Address
3GPP-GPRS-NEG-QOS-PROFILE	3GPP 29.061 - 16.4.7.2-5 3GPP 29.274 - 8.7	Special Encoded Octets
3GPP-SGSN-ADDRESS	3GPP 29.061 - 16.4.7.2-6	IPv4 Address
3GPP-GGSN-ADDRESS	3GPP 29.061 - 16.4.7.2-7	IPv4 Address
3GPP-IMSI-MCC-MNC	3GPP 29.061 - 16.4.7.2-8	String
3GPP-GGSN-MCC-MNC	3GPP 29.061 - 16.4.7.2-9	String

Attribute	Reference Specification	Encoding Type
3GPP-NSAPI	3GPP 29.061 - 16.4.7.2-10 3GPP 29.561 – 11.3	String
3GPP-SELECTION-MODE	3GPP 29.061 - 16.4.7.2-12	String
3GPP-CHARGING-CHARACTERISTICS	3GPP 29.061 - 16.4.7.2-13	String
3GPP-SGSN-MCC-MNC	3GPP 29.061 - 16.4.7.2-18	String
3GPP-IMEISV	3GPP 29.061 - 16.4.7.2-20	String
3GPP-RAT-TYPE	3GPP 29.061 - 16.4.7.2-21	Octet - 1 byte
3GPP-USER-LOCATION	3GPP 29.061 - 16.4.7.2-22 3GPP 29.274 - 8.21-4, 8.21-5 3GPP 38.413 – 9.3.1.7, 9.3.3.10	Special Encoded Octets
3GPP-MS-TIMEZONE	3GPP 29.061 - 16.4.7.2-23 3GPP 29.274 - 8.44	Special Encoded Octets
3GPP-NEGOTIATED-DSCP	3GPP 29.061 - 16.4.7.2-26	Octet - 1 byte
CHAP-PASSWORD (CHAP)	RFC2865 – 5.3	String
CHAP-CHALLENGE (CHAP)	RFC2865 – 5.40	String
MSCHAP-CHALLENGE (MSCHAP)	RFC2548 – 2.1.2	String
MSCHAP-RESPONSE	RFC2548 – 2.1.3	Octets
MSCHAP2-RESPONSE	RFC2548 – 2.3.2	Octets
MSCHAP-ERROR	RFC2548 – 2.1.5	String
REPLY-MESSAGE	RFC2865 – 5.18	String



**Note** The WiFi call attributes are the same as the 4G call.

### RADIUS Access Response Attributes

The following table lists the supported attributes in the RADIUS Access-Response message.

Attribute	Reference Specification	Encoding Type
FRAMED-IP	RFC2865 - 5.1	IPv4 Address
FRAMED-IPv6-PREFIX	RFC3162	PrefixLen and String
IDLE-TIMEOUT	RFC2865 - 5.28	Integer
SESSION-TIMEOUT	RFC2865 - 5.27	Integer



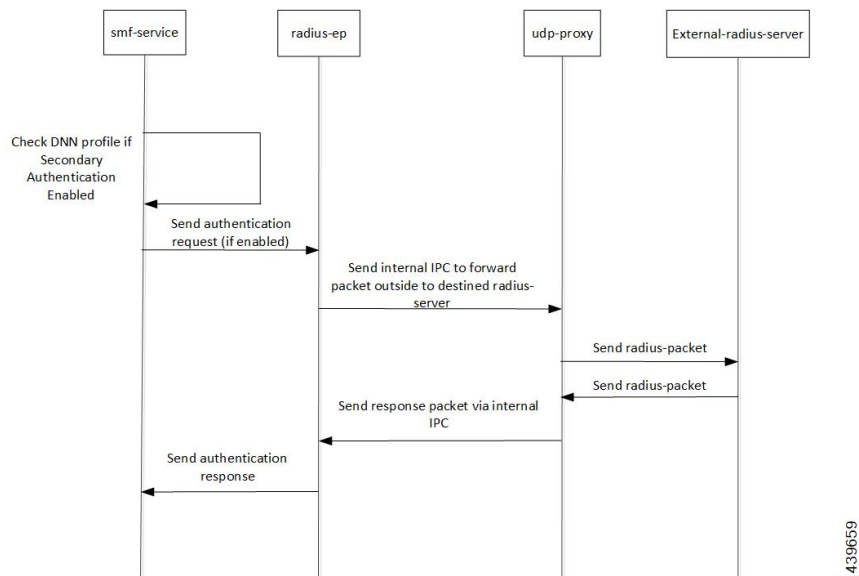
**Note** The WiFi call attributes are the same as the 4G call.

For complete description of the RADIUS authentication attributes, see the [RADIUS Attribute Definition](#), on page 612 section in this guide.

## Call Flows

### RADIUS Authentication Call Flow

The following figure illustrates the end to end call flow between the SMF server and RADIUS-EP.



**Table 175: RADIUS Authentication Call Flow**

Step	Description
1	Bringing up RADIUS-POD: Add the respective endpoint configuration, with VIP-IP similar to Protocol-EP VIP-IP. Add the RADIUS-server information to the profile-RADIUS configuration.
2	Add the secondary authentication configuration to the required DNN profiles.
3	During session-bringup, the DNN profile checks if secondary authentication is enabled after successful UDM validation. <ul style="list-style-type: none"> <li>• If authentication is not enabled, continue with PCF.</li> <li>• If authentication is enabled, send inter-process communication (IPC) message to RADIUS-POD to authenticate the subscriber.</li> </ul>
4	The RADIUS-POD prepares the Access Request packet that is destined to a configured RADIUS-server, sends the packet to UDP Proxy pod to proxy the packet out.

Step	Description
6	The UPD Proxy pod creates a socket (if not already present) and sends the packet to the RADIUS-server.
7	The RADIUS-server validates the Access Request. If accepted, it responds with the Access Accept message. Else, it responds with the Access Reject message.
8	The UDP Proxy responds to the respective RADIUS-EP instance.
9	The RADIUS-EP instance validates the response, fetches the framed-IP (if present), and updates the SMF-service.
10	The SMF-service, upon successful response from RADIUS-EP, continues with the PCF flow. Else, the SMF-service disconnects from the subscriber.

## RADIUS Interaction for Accounting

The SMF exchanges the following messages with RADIUS server through the RADIUS-client RADIUS-EP.

- **Accounting-Request:** This message carries any of the following packets to relay the accounting information to the RADIUS server.

- **Accounting Start packet:** This packet describes the type of service being delivered and the user it is being delivered to.

The SMF sends accounting-start packet during the session establishment procedure. The RADIUS Accounting server returns an acknowledgement upon receiving the accounting-start packet.

For details on configuring the RADIUS Accounting, see [Configuring the RADIUS Client, on page 621](#) section.

- **Accounting Stop packet:** This packet describes the type of service that was delivered and optionally statistics such as elapsed time, input and output octets, or input and output packets.

At the end of service delivery, the SMF sends the accounting-stop packet for all session deletion scenarios and when the RADIUS accounting is enabled during the call setup.

- **Accounting-Request Interim-Update:** During the session, the SMF sends the updated cumulative usage report to the RADIUS accounting server.

- **Accounting-Response:** For each successfully processed accounting request, the RADIUS server returns an accounting acknowledgment confirming the receipt of the information.

For CLI details associated with accounting, see the [Configuring the RADIUS Client, on page 621](#) section.

## RADIUS Accounting Attributes

The following table lists the RADIUS accounting attributes supported in the accounting-request message.

Attribute	Reference Spec	Encoding Type	Supported Accounting Type
USER-NAME	RFC 2865 - 5.1	String	Start, Stop, Interim update
CALLING-STATION-ID	RFC 2865 - 5.31	String	Start, Stop, Interim update
CALLED-STATION-ID	RFC 2865 - 5.30	String	Start, Stop, Interim update

Attribute	Reference Spec	Encoding Type	Supported Accounting Type
NAS-IP-ADDRESS	RFC 2865 - 5.4	IPV4 Address	Start, Stop, Interim update
NAS-IDENTIFIER	RFC 2865 - 5.32	String	Start, Stop, Interim update
SERVICE-TYPE	RFC 2865 - 5.6	Octets - 4 bytes	Start, Stop, Interim update
FRAMED-PROTOCOL	RFC 2865 - 5.7	Octets - 4 bytes	Start, Stop, Interim update
NAS-PORT-TYPE	RFC 2865 - 5.41	Octets - 4 bytes	Start, Stop, Interim update
NAS-PORT	RFC 2865 - 5.5	Octets - 4 bytes	Start, Stop, Interim update
3GPP-IMSI	3GPP 29.061 - 16.4.7.2-1	String	Start, Stop, Interim update
3GPP-CHARGING-ID	3GPP 29.061 - 16.4.7.2-2	Octets - 4 bytes	Start, Stop, Interim update
3GPP-PDP-TYPE	3GPP 29.061 - 16.4.7.2-3	Octets - 4 bytes	Start, Stop, Interim update
3GPP-CHARGING-GATEWAY-ADDR	3GPP 29.061 - 16.4.7.2-4	IPV4 Address	Start, Stop, Interim update
3GPP-GPRS-NEG-QOS-PROFILE	3GPP 29.061 - 16.4.7.2-5 3GPP 29.274 - 8.7	Special Encoded Octets	Start, Stop, Interim update
3GPP-SGSN-ADDRESS	3GPP 29.061 - 16.4.7.2-6	IPV4 Address	Start, Stop, Interim update  This attribute is not included in the 5G accounting-start message.
3GPP-GGSN-ADDRESS	3GPP 29.061 - 16.4.7.2-7	IPV4 Address	Start, Stop, Interim update
3GPP-IMSI-MCC-MNC	3GPP 29.061 - 16.4.7.2-8	String	Start, Stop, Interim update
3GPP-GGSN-MCC-MNC	3GPP 29.061 - 16.4.7.2-9	String	Start, Stop, Interim update
3GPP-NSAPI	3GPP 29.061 - 16.4.7.2-10	String	Start, Stop, Interim update
3GPP-SELECTION-MODE	3GPP 29.061 - 16.4.7.2-12	String	Start, Stop, Interim update
3GPP-CHARGING-CHARACTERISTICS	3GPP 29.061 - 16.4.7.2-13	String	Start, Stop, Interim update
3GPP-SGSN-MCC-MNC	3GPP 29.061 - 16.4.7.2-18	String	Start, Stop, Interim update
3GPP-IMEISV	3GPP 29.061 - 16.4.7.2-20	String	Start, Stop, Interim update
3GPP-RAT-TYPE	3GPP 29.061 - 16.4.7.2-21	Octet - 1 byte	Start, Stop, Interim update

Attribute	Reference Spec	Encoding Type	Supported Accounting Type
3GPP-USER-LOCATION	3GPP 29.061 - 16.4.7.2-22 3GPP 29.274 - 8.21-4 3GPP 29.274 - 8.21-5	Special Encoded Octets	Start, Stop, Interim update
3GPP-MS-TIMEZONE	3GPP 29.061 - 16.4.7.2-23 3GPP 29.274 - 8.44	Special Encoded Octets	Start, Stop, Interim update
3GPP-NEGOTIATED-DSCP	3GPP 29.061 – 16.4.7.2-26	Octet – 1 byte	Start, Stop, Interim update This attribute is sent only if the associated configuration is present.
Acct-Status-Type	RFC 2866	Start/Stop/Interim	Start, Stop, Interim update
Accounting-Session-Id	RFC 2866	String	Start, Stop, Interim update
Acct-Delay-time	RFC 2866	Octet	Start, Stop, Interim update
Acct-Input-Octets	RFC 2866	Integer	Stop, Interim update
Acct-Output-Octets	RFC 2866	Integer	Stop, Interim update
Acct-Input-Gigawords	RFC 2869	Integer	Stop, Interim update
Acct-Output-Gigawords	RFC 2869	Integer	Stop, Interim update
Acct-Input-packets	RFC 2866	Integer	Stop, Interim update
Acct-Output-Packets	RFC 2866	Integer	Stop, Interim update
Acct-Session-Time	RFC 2866	Integer	Stop, Interim update
Acct-Terminate-Cause	RFC 2866	String	Stop
Framed-MTU	RFC 2866	String	Start, Stop, Interim update
3GPP-Session-Stop-Indicator	3GPP 29.061	Bit String	Stop
Framed-Ip-Addr	RFC 2866	IPV4 Address	Start, Stop, Interim update
Acct-Authentic	RFC 2866	String	Start, Stop, Interim update
EventTimeStamp	RFC 2869	String	Start, Stop, Interim update



**Note** The WiFi call attributes are the same as the 4G call.

For complete description of the RADIUS accounting attributes, see the [RADIUS Attribute Definition](#), on page 612 section in this guide.

## Call Flows

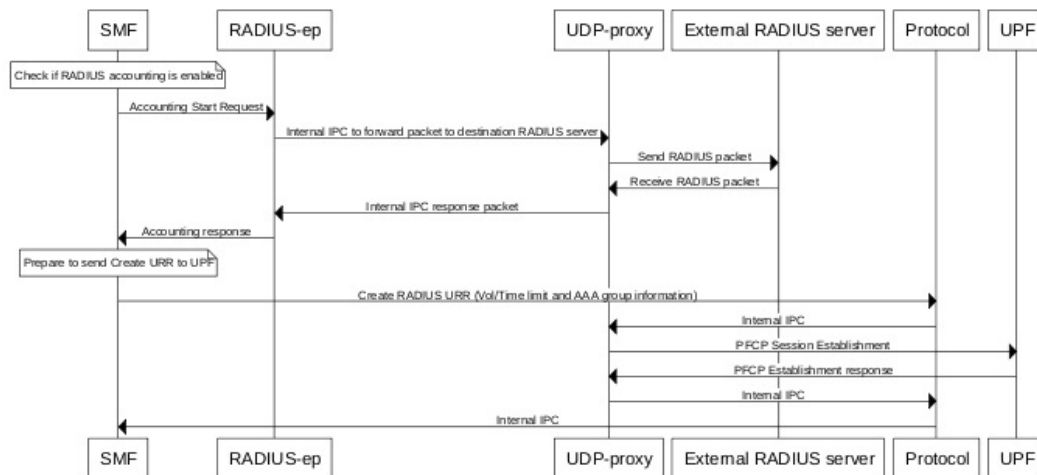
This section describes the following call flows:

- RADIUS Accounting Start Call Flow
- RADIUS Accounting Stop Call Flow
- RADIUS Accounting Interim-update Asynchronous Call Flow
- RADIUS Accounting Interim-update Synchronous Call Flow

### RADIUS Accounting Start Call Flow

This section describes the call flow associated with the initiation of RADIUS accounting procedure.

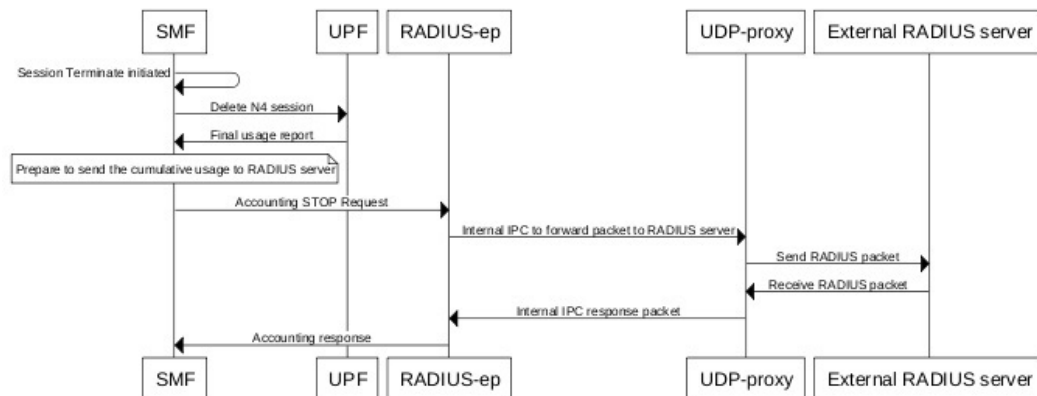
**Figure 113: RADIUS Accounting Start Call Flow**



### RADIUS Accounting Stop Call Flow

This section describes the call flow associated with the termination of RADIUS accounting procedure.

**Figure 114: RADIUS Accounting Stop Call Flow**



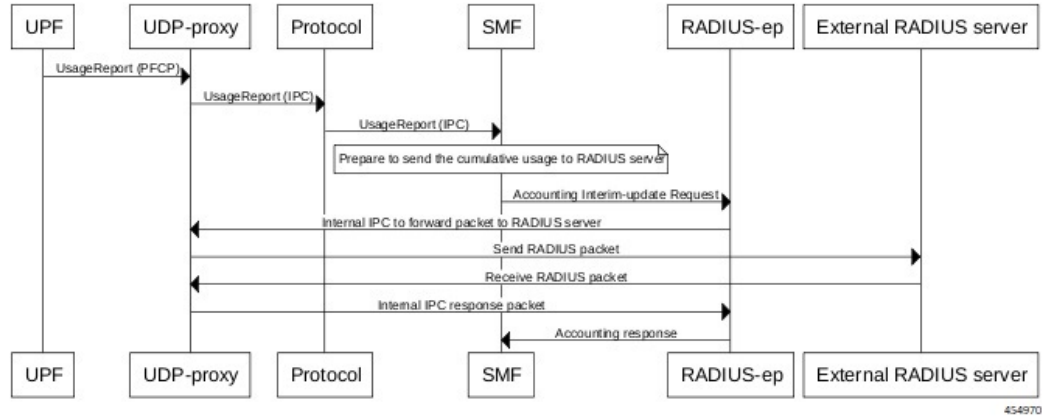
454969



### Asynchronous Accounting Interim-Update Call Flow

This section describes the call flow associated with the asynchronous interim-update request.

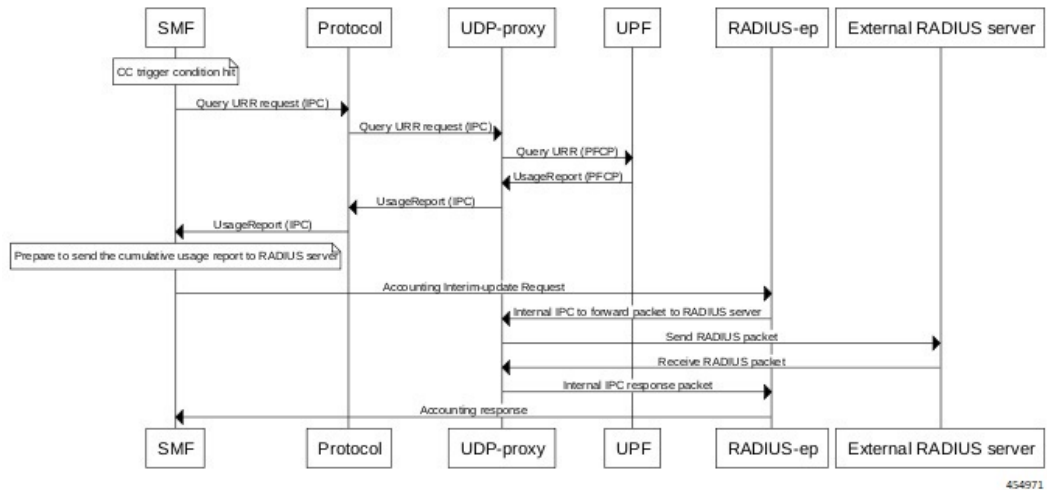
Figure 115: Asynchronous Accounting Interim-Update Call Flow



### Synchronous Accounting Interim-Update Call Flow

This section describes the call flow associated with the synchronous interim-update request.

Figure 116: Synchronous Accounting Interim-Update Call Flow



## Processing of Usage Reporting Rules

After enabling the RADIUS accounting, the SMF creates the Usage Reporting Rule (URR) and relays the rule to the UPF through the Create URR Information Element (IE). The Create URR IE is present in the N4 Session Establishment Request and it contains the volume and time limits as per the configuration.

The SMF associates the RADIUS URR only to the dynamic Packet Detection Rules (PDRs) and not for the static and predefined rules. With AAA group name in N4 session establishment request, the UPF associates the static and predefined PDRs with the RADIUS URR. The UPF sends the usage report for the RADIUS URR when the Volume limit or the Time limit is hit. Then, the SMF sends the usage in the Interim-Update Accounting-Request message to the RADIUS server.

The SMF receives the usage report for RADIUS URR in N4 Modification Response or N4 Deletion Response when any one of the following conditions are met:

- CC event condition is hit and the SMF performs Query URR
- Session Delete Response is sent

The SMF stores the values of Volume and Time thresholds reported for a previous session and reports the cumulative usage by adding the currently reported value to the stored value. The SMF sends the cumulative usage report in Accounting-Request Interim-Update and Accounting-Stop messages.

On receiving the usage report from UPF, the SMF identifies the URR IDs that are to be sent to the CHF server and to the RADIUS server. For example, if the URR ID is associated to “0x80 00 00 09”, then the SMF sends this URR ID to the RADIUS server, and the other URR IDs to the CHF server.

## Dynamic Configuration Update

The SMF allows you to dynamically change the RADIUS accounting configuration without impacting the existing sessions.

The following table identifies the impact of dynamic update to the various RADIUS accounting configurations.

**Table 176: Dynamic Update of RADIUS Accounting Configuration**

Configuration	Dynamic Change	Impact on Existing Sessions
Enabling and disabling of RADIUS accounting configuration	Allowed at the system level	The existing sessions continue to use the old value.
CC trigger updates	Allowed as per current pod replica	The existing session uses the new value.
Volume and time limit changes	Allowed at the system level	The existing sessions continue to use the old value.

## RADIUS Attribute Definition

The detailed description of each attribute is as follows:

- USER-NAME

**Description:** String value encoded as per RFC 2865.

- 5G call: GPSI value is used, with stripped-off "msisdn-"
- 4G call: MSISDN value is used, with stripped-off "msisdn-"



**Note** PAP, CHAP, and MSCHAP authentication methods are not supported in releases prior to 2020.02.x.

In release 2020.02.x and beyond, the PAP, CHAP, and MSCHAP authentication methods are supported.

- **PASSWORD**  
**Description:** Encrypted string value encoded as per RFC 2865.  
For both 5G and 4G calls, selected RADIUS server's "secret" is set as user-password.
- **CALLING-STATION-ID**  
**Description:** String value encoded as per RFC 2865.  
5G call: GPSI value is used, with stripped of "msisdn-"  
4G call: MSISDN value is used, with stripped of "msisdn-"
- **CALLED-STATION-ID**  
**Description:** String value encoded as per RFC 2865.  
For both 5G and 4G calls, DNN value is set as called-station-id.
- **NAS-IP-ADDRESS**  
**Description:** IPv4 address value encoded as per RFC 2865.  
For both 5G and 4G calls, user-configured RADIUS Client interface-type's VIP-IP is used.
- **NAS-IDENTIFIER**  
**Description:** String value encoded as per RFC 2865.  
For both 5G and 4G calls, user-configured nas-identifier attribute value is used.
- **SERVICE-TYPE**  
**Description:** 4-byte octet (int) value encoded as per RFC 2865.  
For both 5G and 4G calls, "FRAMED (2)" value is set.
- **FRAMED-PROTOCOL**  
**Description:** 4-byte octet (int) value encoded as per RFC 2865.  
For both 5G and 4G calls, "GPRS-PDP-CONTEXT (7)" value is set.
- **NAS-PORT-TYPE**  
**Description:** 4-byte octet (int) value encoded as per RFC 2865.  
For both 5G and 4G calls, "WIRELESS-OTHER (18)" value is set.
- **NAS-PORT**  
**Description:** 4-byte octet (int) value encoded as per RFC 2865.  
For both 5G and 4G calls, the base value of respective instance is used. That is:  
0x4000... 0x407F is set for replica-0  
0x4080... 0x40FF is set for replica-1
- **3GPP-IMSI**  
**Description:** String value encoded as per *3GPP TS 29.061*.  
5G call: SUPI value is used.  
4G call: IMSI value is used.

- 3GPP-CHARGING-ID

**Description:** 4-byte octet (int) value encoded as per *3GPP TS 29.061*.

For both 5G and 4G calls, charging-ID is set.

- 3GPP-PDP-TYPE

**Description:** 4-byte octet (int) value encoded as per *3GPP TS 29.061*.

For both 5G and 4G calls, pdp-type is set as follows:

- 0 = IPv4
- 2 = IPv6
- 3 = IPv4v6

- 3GPP-CHARGING-GATEWAY-ADDR

**Description:** 4-byte octet (IPv4-address) value encoded as per *3GPP TS 29.061*.

For both 5G and 4G calls, charging gateway address is set.

- 3GPP-GPRS-NEG-QOS-PROFILE

**Description:** Octets (special encoding) value encoded as per *3GPP TS 29.061* and *29.274*.

For 5G call, the values from default-qos profile of the system are used and the encoding is performed as follows:

**Table 177: Non-GBR case**

1-2	<Release indicator>- = "15" (UTF-8 encoded)
3	"-" (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	5QI (UTF-8 encoded)
8-9	UL Session-AMBR length (UTF-8 encoded)
10-m	UL Session-AMBR (UTF-8 encoded)
(m+1) - (m+2)	DL Session-AMBR length (UTF-8 encoded)
(m+3) – n	DL Session-AMBR (UTF-8 encoded)

**Table 178: GBR case**

1-2	<Release indicator> = "15" (UTF-8 encoded)
3	"-" (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	5QI (UTF-8 encoded)
8-9	UL MFBR length (UTF-8 encoded)
10-m	UL MFBR (UTF-8 encoded)

(m+1)-(m+2)	DL MFBR length (UTF-8 encoded)
(m+3)-n	DL MFBR (UTF-8 encoded)
(n+1)-(n+2)	UL GFBR length (UTF-8 encoded)
(n+3)-o	UL GFBR (UTF-8 encoded)
(o+1) – (o+2)	UL GFBR length (UTF-8 encoded)
(o+3) - p	DL GFBR (UTF-8 encoded)

For 4G call, the values from the default-qos profile of the system are used and the encoding is performed as follows:

**Table 179: Non-GBR case**

1-2	<Release indicator>- = "08" (UTF-8 encoded)
3	"-" (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	5QI (UTF-8 encoded)
8-11	UL Session-AMBR (UTF-8 encoded)
12-15	DL Session-AMBR (UTF-8 encoded)

**Table 180: GBR case**

1-2	<Release indicator> = "08" (UTF-8 encoded)
3	"-" (UTF-8 encoded)
4-5	ARP (UTF-8 encoded)
6-7	5QI (UTF-8 encoded)
8-11	UL MBR (UTF-8 encoded)
12-15	DL MBR (UTF-8 encoded)
16-19	UL GBR (UTF-8 encoded)
20-23	DL GBR (UTF-8 encoded)

- 3GPP-SGSN-ADDRESS

**Description:** 4-byte octet (IPv4-address) value encoded as per *3GPP TS 29.061*.

For 5G call, the AMF address is set.

For 4G call, the S-GW address is set.

- 3GPP-GGSN-ADDRESS

**Description:** 4-byte octet (IPv4-address) value encoded as per *3GPP TS 29.061*.

For both 5G and 4G calls, the SMF-Service IP is set.

- 3GPP-IMSI-MCC-MNC

**Description:** String value encoded as per *3GPP TS 29.061*.

For 5G call, SUPIs MCC and MNC values are set.

For 4G call, IMSIs MCC and MNC values are set.

MCC is first 3 bytes, MNC is next 2 or 3 bytes.

If MCC value is any of the following, then MNC will be of 3 bytes, else MNC will be of 2 bytes.

300 302 310 311 312 313 316 334 338 342 344 346 348 354 356 358 360 365 376 405 708 722 732

- 3GPP-GGSN-MCC-MNC

**Description:** String value encoded as per *3GPP TS 29.061*.

For both 5G and 4G calls, configured MCC and MNC value of SMF is used.

MCC is first 3 bytes, and MNC is next 2 or 3 bytes.

- 3GPP-SGSN-MCC-MNC

**Description:** String value encoded as per *3GPP TS 29.061*.

For 5G call, AMFs MCC and MNC values are set.

For 4G call, SGWs MCC and MNC values are set.

MCC is first 3 bytes, and MNC is next 2 or 3 bytes.

- 3GPP-NSAPI

**Description:** String value encoded as per *3GPP TS 29.061*.

For 5G call, QFI value from the defaultQos profile is set.

For 4G call, EPS bearer ID is set.

- 3GPP-SELECTION-MODE

**Description:** String value encoded as per *3GPP TS 29.061*.

For both 4G and 5G calls, the value is set to "0".

- 3GPP-CHARGING-CHARACTERISTICS

**Description:** String value encoded as per *3GPP TS 29.061*.

For both 4G and 5G calls, generic charging character is set.

- 3GPP-IMEISV

**Description:** String value encoded as per *3GPP TS 29.061*.

For 5G call, PEI value is set.

For 4G call, IMEI value is set.

- 3GPP-RAT-TYPE

**Description:** 1-byte octet encoded as per *3GPP TS 29.061*.

For 5G call, value "NR (51)" is set.

For 4G call, value "EUTRAN (6)" is set.

For WLAN call, value "WLAN (3)" is set.

- 3GPP-USER-LOCATION

**Description:** Special octet value encoded as per *3GPP TS 29.061*.

For 5G call, the following encoding logic is used:

1	Location-Type Only TAI = 136 Only NCGI = 135 Both TAI + NCGI =137
2-7	TAI-Encoding (if present)
8-15	NCGI-Encoding (if present)

TAI Encoding header:

1	MCC digit 2	MCC digit 1
2	MNC digit 3	MCC digit 3
3	MNC digit 2	MNC digit 1
4-6	TAC value	

NCGI Encoding header:

1	MCC digit 2	MCC digit 1
2	MNC digit 3	MCC digit 3
3	MNC digit 2	MNC digit 1
4	SPARE	NCI
5-8	NR Cell Identifier (NCI)	

For 4G call, the following encoding logic is used:

1	Location-Type
	Only TAI = 128
	Only ECGI = 129
	Both TAI + ECGI =130
2-6	TAI-Encoding (if present)
7-13	ECGI-Encoding (if present)

TAI Encoding header:

1	MCC digit 2	MCC digit 1
2	MNC digit 3	MCC digit 3
3	MNC digit 2	MNC digit 1
4-5	TAC value	

ECGI Encoding header:

1	MCC digit 2	MCC digit 1
2	MNC digit 3	MCC digit 3
3	MNC digit 2	MNC digit 1
4	Spare	ECI
5-7	EUTRAN Cell Identifier (ECI)	

- 3GPP-MS-TIMEZONE

**Description:** Special octet value encoded as per *3GPP TS 29.061*.

Timezone string (for example: -07:00+1) is encoded as two-byte value as mentioned in the following table.

1	TIMEZONE The first byte timezone is encoded as per 3GPP 29.061, 3GPP 29.274, 3GPP 24.008, and 3GPP 23.040 (section 9.2.3.11).
2	DAYLIGHT SAVING 0, or +1 or +2 The second byte daylight consists of two bits used (00-0, 01-+1, 10-+2, 11 – Unused).

- 3GPP-NEGOTIATED-DSCP

**Description:** 1-byte octet encoded as per *3GPP TS 29.061*

For both 5G and 4G calls, DSCP configuration from DNN qos-profile configuration is used.

Sub -> DNN profile -> QosProfile -> DSCPMap -> Qi5 value check -> ARP priority check

- Acct-Status-Type

**Description:** Enum value encoded as per RFC 2866. The value of this attribute can be one of the following:

- 1 - Start
- 2 - Stop
- 3 - Interim Update

- Acct-Delay-Time

**Description:** Integer value encoded as per RFC 2866. This attribute represents the amount of time client is trying to send the accounting record.

- Acct-Input-Octets

**Description:** Integer value encoded as per RFC 2866. This attribute represents the amount of bytes received. This attribute contains 4 bytes.

The SMF wraps values when the number crosses the maximum value.

- Acct-Output-Octets

**Description:** Integer value encoded as per RFC 2866. This attribute represents the amount of bytes transmitted. This attribute contains 4 bytes.



The SMF wraps values when the number crosses the maximum value.

- Acct-Input-Packets

**Description:** Integer value encoded as per RFC 2866. This attribute represents the amount of packets received. This attribute contains 4 bytes.

The SMF wraps values when the number crosses the maximum value.

- Acct-Output-Packets

**Description:** Integer value encoded as per RFC 2866. This attribute represents the amount of packets transmitted. This attribute contains 4 bytes.

The SMF wraps values when the number crosses the maximum value.

- Acct-Input-Gigawords

**Description:** Integer value encoded as per RFC 2869. This attribute indicates how many times the Acct-Input-Octets counter has wrapped around  $2^{32}$  over the course of this service being provided. This value is incremented whenever Acct-Input-Octets is wrapped.

- Acct-Output-Gigawords

**Description:** Integer value encoded as per RFC 2869. This attribute indicates how many times the Acct-Output-Octets counter has wrapped around  $2^{32}$  over the course of this service being provided. This value is incremented whenever Acct-Output-Octets is wrapped.

- Acct-Session-Id

**Description:** String value encoded as per RFC 2866. This attribute represents the unique accounting ID of subscriber. The accounting ID is unique to make it easy to match start and stop records in a log file. The start and stop records for a given session **MUST** have the same Acct-Session-Id. An Accounting-Request packet **MUST** have an Acct-Session-Id.

An Access-Request packet **MAY** have an Acct-Session-Id; if it does, then the NAS **MUST** use the same Acct-Session-Id in the Accounting-Request packets for that session. The Acct-Session-Id contains UTF-8 encoded 10646 characters.

- Acct-Session-Time

**Description:** Integer value encoded as per RFC 2866. This attribute represents the amount of time the subscriber is active.

- Framed-MTU

**Description:** This attribute indicates the Maximum Transmission Unit to be configured for the user, when it is not negotiated by some other means (such as PPP). The default value is 1500.

It **MAY** be used in Access-Accept packets. It **MAY** be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that value, but the server is not required to honour the hint.

- Acct-Terminate-cause

**Description:** Enum value encoded as per RFC 2866. This attribute represents the reason for termination of subscriber.

- FRAMED-IP

The IPv4 address value decoded as per RFC 2865.

For both 4G and 5G calls, the received value is set as the IPv4 address for the subscriber.

- FRAMED-IPv6-PREFIX

The IPv6 Prefix + Length value decoded as per RFC 3162.

For both 4G and 5G calls, the received value is set as the IPv6 prefix for the subscriber.



---

**Important** If the received prefix-length is !=64, the SMF overrides to 64.

---

- IDLE-TIMEOUT

The 4-byte octet (integer) value encoded as per RFC 2865. This attribute is supported in the inbound RADIUS packet.

For both 4G and 5G calls, the received value is used as the maximum number of consecutive seconds of idle time that the user is permitted before being disconnected by the NAS.

- SESSION-TIMEOUT

The 4-byte octet (integer) value encoded as per RFC 2865. This attribute is supported in the inbound RADIUS packet.

For both 4G and 5G calls, the received value is used as the maximum number of seconds that the user is allowed to remain connected by the NAS.



---

**Note** The WiFi call attributes are the same as the 4G call.

---

## Standards Compliance

The RADIUS Client feature complies with the following standards:

- RFC 2865: Remote Authentication Dial in User Service (RADIUS)
- RFC 2866: RADIUS Accounting
- RFC 3162: RADIUS and IPv6
- 3GPP TS 29.061
- 3GPP TS 29.274

## Limitations and Restrictions

The SMF has the following limitations:

- The SMF supports only single RADIUS attribute profile, and does not support dictionary selection.
- If RADIUS accounting is enabled and server-group is configured within DNN profile, the SMF sends server-group as AAA group in charging-params in N4 session establishment. The UPF displays an error if there is a server group mismatch between SMF and UPF.

In this scenario, static and predefined usage are not accounted in the RADIUS URR. However, the dynamic rules traffic is accounted in the RADIUS URR.

- Currently, VLAN tagging for outbound RADIUS packets is based on the static routes configured on SMF. So, the overlapping AAA server addresses for different MVNOs where the VLAN tag must be different from SMF is not supported.

## Configuring the RADIUS Client

The RADIUS client provides both RADIUS authentication and accounting functionalities. For using these functionalities, it is important to enable the RADIUS authentication and accounting framework through the associated CLI configuration.

This section describes how to configure the RADIUS client.



### Important

Configuring the VIP-IP of the RADIUS client interface is mandatory for the RADIUS client to work. Also, the VIP-IP must be the same as the IP of the UDP proxy pod.

Configuring the RADIUS Client feature involves the following:

- [Configuring RADIUS Server, on page 621](#)
- [Configuring RADIUS Server Selection Logic, on page 623](#)
- [Configuring RADIUS Attributes, on page 623](#)
- [Configuring RADIUS Detect Dead Server, on page 624](#)
- [Configuring RADIUS Dead Time, on page 624](#)
- [Configuring RADIUS Retries, on page 625](#)
- [Configuring RADIUS Timeout, on page 625](#)
- [Configuring RADIUS Pod, on page 626](#)
- [Configuring RADIUS NAS-IP, on page 626](#)
- [Configuring Secondary Authentication Method, on page 627](#)
- [Configuring PAP, CHAP, or MSCHAP-based Authentication, on page 628](#)
- [Enabling RADIUS Accounting, on page 629](#)
- [Defining RADIUS Server Group in DNN Profile, on page 630](#)
- [Configuring RADIUS Accounting Options, on page 631](#)
- [Configuring RADIUS Accounting Server Group, on page 632](#)
- [Configuring the Session Disconnect Feature, on page 632](#)

## Configuring RADIUS Server

Use the following sample configuration to configure the RADIUS server.

```

config
  profile radius
    server ipv4_address port_num
      secret secret_key
      priority priority_value
      type { acct | auth }
    commit

```

**NOTES:**

- **profile radius:** Enter the RADIUS configuration mode.
- **server *ipv4\_address port\_num*:** Specify the IPv4 address and port of the RADIUS server.
- **secret *secret\_key*:** Specify the secret key.
- **priority *priority\_value*:** Specify the server priority.
- **type { acct | auth }:** Specify the type of the RADIUS server. The server can be one of the following:
  - **acct:** RADIUS server used for the accounting requests
  - **auth:** RADIUS server used for the authentication requests
- **commit:** Commit the configuration.

**Example**

The following is an example of the RADIUS server configuration.

```

profile radius
  server 1.2.3.4 1812
    secret $8$73a0i4G3ILj0Np+8tn2QOoWDj3QkB+oefPc2ZK6RE6A=
    priority 1
  exit
  server 1.2.5.6 1812
    secret $8$VccEEUVou7m5ptA9WZRPR7KDmxQ/L3K1J3QqgHjexkk=
    priority 2
  exit
exit

```

**Verifying the RADIUS Configuration**

Use the **show radius** command to display information about the RADIUS servers (both accounting and authentication) that are configured in the system.

The following configuration is a sample output of the **show radius** command:

```

bng# show radius
radius
-----
Server: 10.0.0.1, port: 1812, status: up, port-type: Auth
2 requests, 0 pending, 0 retransmits
1 accepts, 1 rejects, 0 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 4 ms latest rtt
-----
Server: 10.0.0.1, port: 1813, status: up, port-type: Acct
3 requests, 0 pending, 0 retransmits
3 responses, 0 timeouts

```

```
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 1 ms latest rtt
-----
```

## Configuring RADIUS Server Selection Logic

Use the following sample configuration to configure the RADIUS server selection logic.

```
config
  profile radius
    algorithm { first-server | round-robin }
  commit
```

### NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **algorithm { first-server | round-robin }**: Define the algorithm for selecting the RADIUS server.
  - **first-server**: Set the selection logic as highest priority first. This is the default behavior.
  - **round-robin**: Set the selection logic as round-robin order of servers.
- **commit**: Commit the configuration.

### Example

The following is an example of the RADIUS server selection logic configuration.

```
config
  profile radius
    algorithm round-robin
  exit
```

## Configuring RADIUS Attributes

Use the following sample configuration to configure the RADIUS attributes for authentication and accounting.

```
config
  profile radius
    attribute { nas-identifier value | nas-ip ipv4_address }
  commit
```

### NOTES:

- **profile radius**: Enter the RADIUS configuration mode.
- **attribute { nas-identifier value | nas-ip ipv4\_address }**: Configure the RADIUS identification parameters.
  - **nas-identifier value**: Specify the attribute name by which the system will be identified in Accounting-Request messages. *value* must be an alphanumeric string.
  - **nas-ip ipv4\_address**: Specify the NAS IPv4 address. *ipv4\_address* must be an IPv4 address in dotted decimal notation.
- **commit**: Commit the configuration.

**Example**

The following is an example of the RADIUS attributes configuration.

```
config
  profile radius
    attribute
      nas-identifier CiscoSmf
    exit
  exit
```

## Configuring RADIUS Detect Dead Server

Use the following sample configuration to configure the RADIUS detect dead server.

```
config
  profile radius
    detect-dead-server response-timeout value
  commit
```

**NOTES:**

- **profile radius:** Enter the RADIUS configuration mode.
- **detect-dead-server response-timeout *value*:** Set the timeout value that marks a server as "dead" when a packet is not received for the specified number of seconds.  
*value* must be an integer in the range of 1–65535. Default: 10 seconds.
- **commit:** Commit the configuration.

**Example**

The following is an example of the RADIUS detect dead server configuration.

```
config
  profile radius
    detect-dead-server response-timeout 100
  exit
```

## Configuring RADIUS Dead Time

Use the following sample configuration to configure the RADIUS dead time.

```
config
  profile radius
    deadtime value
  commit
```

**NOTES:**

- **profile radius:** Enter the RADIUS configuration mode.
- **deadtime *value*:** Set the time to elapse between RADIUS server marked unreachable and when we can reattempt to connect.  
*value* must be an integer in the range of 1–65535. Default: 10 minutes.
- **commit:** Commit the configuration.

### Example

The following is an example of the RADIUS dead time configuration.

```
config
  profile radius
    deadtime 15
  exit
```

## Configuring RADIUS Retries

Use the following sample configuration to configure the maximum RADIUS retries.

```
config
  profile radius
    max-retry value
  commit
```

### NOTES:

- **profile radius:** Enter the RADIUS configuration mode.
- **max-retry *value*:** Set the maximum number of times that the system will attempt retry with the RADIUS server.  
*value* must be an integer in the range of 0–65535. Default: 2
- **commit:** Commit the configuration.

### Example

The following is an example of the RADIUS retries configuration.

```
config
  profile radius
    max-retry 2
  exit
```

## Configuring RADIUS Timeout

Use the following sample configuration to configure the RADIUS timeout.

```
config
  profile radius
    timeout value_in_seconds
  commit
```

### NOTES:

- **profile radius:** Enter the RADIUS configuration mode.
- **timeout *value\_in\_seconds*:** Set the time to wait for response from the RADIUS server before retransmitting.  
*value\_in\_seconds* must be an integer in the range of 1–65535. Default: 2 seconds.
- **commit:** Commit the configuration.

**Example**

The following is an example of the RADIUS timeout configuration.

```
config
  profile radius
    timeout 4
  exit
```

## Configuring RADIUS Pod

Use the following sample configuration to configure the RADIUS pod.

```
config
  endpoint radius
    replicas number_of_replicas
  commit
```

**NOTES:**

- **endpoint radius:** Enter the RADIUS endpoint configuration mode.
- **replicas *number\_of\_replicas*:** Set the number of replicas required.
- **commit:** Commit the configuration.

**Example**

The following is an example of the RADIUS pod configuration.

```
config
  endpoint radius
    replicas 3
  exit
```

## Configuring RADIUS NAS-IP

This section describes how to configure the RADIUS NAS-IP.

**Multiple RADIUS NAS-IP Configuration**

Use the following sample configuration to configure multiple RADIUS NAS-IP addresses at various levels.

```
config
  profile radius
    attribute nas-ip-address ipv4_address
    accounting attribute nas-ip-address ipv4_address
    server-group group_name attribute nas-ip-address ipv4_address
    server-group group_name accounting attribute nas-ip-address ipv4_address

  commit
```

**NOTES:**

- **profile radius:** Enter the RADIUS configuration mode.



- **attribute nas-ip-address *ipv4\_address***: Set the global NAS-IP address value.
- **accounting attribute nas-ip-address *ipv4\_address***: Set the global accounting NAS-IP address value.
- **server-group *group\_name* attribute nas-ip-address *ipv4\_address***: Set the per server-group common NAS-IP address value.
- **server-group *group\_name* accounting attribute nas-ip-address *ipv4\_address***: Set the per server-group accounting NAS-IP address value.
- **commit**: Commit the configuration.

### Example:

The following is an example of the multiple RADIUS NAS-IP configuration.

```
config
profile radius
attribute
nas-ip-address 1.2.3.4
exit
accounting
attribute
nas-ip-address 1.2.3.5
exit
exit
server-group grp1
attribute
nas-ip-address 1.2.3.6
exit
accounting
attribute
nas-ip-address 1.2.3.7
exit
exit
server-group grp2
attribute
nas-ip-address 1.2.3.78
exit
accounting
attribute
nas-ip-address 1.2.3.9
exit
exit
exit
exit
```

## Configuring Secondary Authentication Method

Use the following sample configuration to configure the secondary authentication method.

```
config
profile dnn dnn_name
authentication secondary radius [ group group_name ]
commit
```

### NOTES:

- **profile dnn *dnn\_name***: Enter the DNN Profile configuration mode.

- **authentication secondary radius [ group *group\_name* ]**: Enable secondary authentication under the DNN profile and sets method as RADIUS.  
**group *group\_name***: This keyword is optional. This keyword defines the RADIUS server group name.
- **commit**: Commit the configuration.

### Example

The following is a configuration example of the secondary authentication method.

```
config
  profile dnn intershat
  ...
  authentication secondary radius
exit
```

## Verifying the RADIUS Authentication Configuration

Use the **show radius auth-server** command to display detailed statistics for RADIUS authentication server and port.

The following configuration is a sample output of the **show radius auth-server** command:

```
bng# show radius auth-server
-----
Server: 10.0.0.1, port: 1812, status: up, port-type: Auth
2 requests, 0 pending, 0 retransmits
1 accepts, 1 rejects, 0 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 4 ms latest rtt
-----
```

## Configuring PAP, CHAP, or MSCHAP-based Authentication

This section provides the configuration to enable the PAP, CHAP, and MSCHAP-based RADIUS authentication. This configuration aids in converting the CHAP Challenge and Response received in PCO IE as MSCHAP Challenge and Response.

### Defining Priority for Authentication Algorithm

Use the following sample configuration to define the priority for different authentication algorithms (PAP or CHAP or MSCHAP) for RADIUS-based authentication in SMF.

```
config
  profile dnn profile_name
    authentication { { secondary radius [ group group_name ] | { algorithm
  { pap priority_value [ password-use-pco ] | chap priority_value [
convert-to-mschap ] | mschap priority_value } }
    end
```

#### NOTES:

- **password-use-pco**: This keyword overrides the DNN configured password with PCO password. The default setting is disabled.

If the host level password is not configured at DNN, then the SMF uses the UE given password for PAP-based authentication even though this configuration is disabled.

- **convert-to-mschap**: This keyword converts the received CHAP Challenge and Response to MSCHAP if the CHAP Response length is 49 bytes. Otherwise, the SMF sends as CHAP only even though this configuration is explicitly enabled.
- The default priority for PAP, CHAP, and MSCHAP algorithms is 0 which means that the configuration is disabled. The valid values are 1, 2, and 3. Lower the value, higher is the priority. It is used to resolve conflicts if the UE sends multiple authentication parameters in the PCO, EPCO, or APCO IE.

## Configuring Host Password

Use the following sample configuration to specify the host password at DNN level which is used as a password for PAP-based authentication.

```
config
  profile dnn profile_name
    outbound password password
  end
```

### NOTES:

- **profile dnn *profile\_name***: Specify the DNN profile name as an alphanumeric string to enter the DNN configuration mode.
- **outbound password *password***: Specify the DNN host password for authentication. By default, the SMF sends this password in PAP user-password if it is not explicitly overridden using the **password-use-pco** option.

By default, the SMF encrypts the given password using AES-128-CFB encryption algorithm.

## Enabling RADIUS Accounting

Use the following sample configuration to enable RADIUS accounting on SMF and configure the RADIUS accounting specific parameters.

```
config
  profile charging charging_profile_name
    accounting limit { duration value | volume { downlink value | total
value | uplink value } }
    accounting triggers [ ambr-change | plmn-change | qos-change |
rat-change | serv-node-change | ue-time-change | user-loc-change ]
    commit
```

### NOTES:

- **profile charging *charging\_profile\_name***: Specify the charging profile name. *charging\_profile\_name* must be an alphanumeric string.
- **accounting**: Specify this option to enable RADIUS accounting on SMF for the subscribers.
- **limit { duration *value* | volume { downlink *value* | total *value* | uplink *value* } }**: Specify the volume and time limits for RADIUS accounting.
  - duration *value***: Specify the time duration value as an integer in the range of 0–2147483647.
  - downlink *value***: Specify the downlink volume limit for interim generation in bytes, as an integer in the range of 100000–4000000000.

**total value:** Specify the total volume limit for interim generation in bytes, as an integer in the range of 100000–4000000000.

**uplink value:** Specify the uplink volume limit for interim generation in bytes, as an integer in the range of 100000–4000000000.

- **accounting triggers** [ **ambr-change** | **plmn-change** | **qos-change** | **rat-change** | **serv-node-change** | **ue-time-change** | **user-loc-change** ]: Enable the appropriate RADIUS accounting triggers according to the following conditions:
  - AMBR change
  - PLMN change
  - Quality of Service change
  - Routing Area Information change
  - Serving node change
  - Traffic Flow Template (TFT) change
  - UE time change
  - User Location Information change - applicable only for P-GW and GGSN.




---

**Important** Enabling any one of these triggers turns off the remaining triggers.

---

- **commit:** Commit the configuration.

## Defining RADIUS Server Group in DNN Profile

Use the following sample configuration to set RADIUS server-group to use for accounting in DNN profile. All subscribers under the specified DNN will have RADIUS accounting enabled.

```
configure
  profile dnn dnn_profile_name
    accounting server-group group_name
  commit
```

### NOTES:

- **profile dnn** *dnn\_profile\_name*: Specify the DNN profile name to enter the DNN configuration mode. *dnn\_profile\_name* must be an alphanumeric string.
- **accounting server-group** *group\_name*: Specify the RADIUS server-group to use for accounting in the configured DNN profile. *group\_name* must be an alphanumeric string.
- **commit:** Commit the configuration.

## Configuring RADIUS Accounting Options

Use the following sample configuration to configure the RADIUS accounting options.

```
config
  profile radius accounting
    algorithm { first-server | round-robin }
    attribute { nas-identifier value | nas-ip ipv4_address }
    deadtime value
    detect-dead-server response-timeout value
    max-retry value
    timeout value
  commit
```

### NOTES:

- **profile radius accounting:** Enter the RADIUS accounting configuration mode.
- **algorithm { first-server | round-robin }:** Define the algorithm for selecting the RADIUS server.
  - **first-server:** Set the selection logic as highest priority first. This is the default behavior.
  - **round-robin:** Set the selection logic as round-robin order of servers.
- **attribute { nas-identifier value | nas-ip ipv4\_address }:** Configure the RADIUS identification parameters.
  - **nas-identifier value:** Specify the attribute name by which the system will be identified in Accounting-Request messages. *value* must be an alphanumeric string.
  - **nas-ip ipv4\_address:** Specify the NAS IPv4 address. *ipv4\_address* must be an IPv4 address in dotted decimal notation.
- **deadtime value:** Set the time to elapse between RADIUS server marked unreachable and when we can re-attempt to connect.  
*value* must be an integer from 0 through 65535. Default: 10 minutes.
- **detect-dead-server response-timeout value:** Set the timeout value that marks a server as "dead" when a packet is not received for the specified number of seconds.  
*value* must be an integer from 1 through 65535. Default: 10 seconds.
- **max-retry value:** Set the maximum number of times that the system will attempt retry with the RADIUS server.  
*value* must be an integer in the range of 0–65535. Default: 2
- **timeout value:** Set the time to wait for response from the RADIUS server before retransmitting.  
*value* must be an integer in the range of 1–65535. Default: 2 seconds.
- **commit:** Commit the configuration.
- All the keyword options under the RADIUS accounting configuration mode are also available within the RADIUS configuration mode.

## Configuring RADIUS Accounting Server Group

Use the following sample configuration to configure the RADIUS server group.

```
config
  profile radius
    server-group group_name
  commit
```

### NOTES:

- **profile radius:** Enter the RADIUS configuration mode.
- **server group *group\_name*:** Specify the name of server group for use in RADIUS accounting. *group\_name* must be an alphanumeric string.
- **commit:** Commit the configuration.

## Verifying the RADIUS Accounting Configuration

Use the **show radius acct-server** command to display statistics for RADIUS accounting server and port.

The following configuration is a sample output of the **show radius acct-server** command:

```
bng# show radius acct-server
-----
Server: 10.0.0.1, port: 1813, status: up, port-type: Acct
3 requests, 0 pending, 0 retransmits
3 responses, 0 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 1 ms latest rtt
-----
```

## Configuring the Session Disconnect Feature

This section describes how to configure the Session Disconnect feature.

Configuring the Session Disconnect feature in SMF involves the following steps:

- [Configuring the Dynamic Authorization Service, on page 632](#)
- [Configuring the CoA-NAS Interface, on page 633](#)

## Configuring the Dynamic Authorization Service

Use the following sample configuration to enable the NAS as an authentication, authorization, and accounting (AAA) server for the dynamic authorization service. This service supports the RADIUS Disconnect and Change of Authorization (CoA) functionality.

```
config
  profile radius-dynamic-author
    client ipv4_address [ secret shared_secret ]
    nas-identifier value
    secret shared_secret
  end
```

### NOTES:

- **profile radius-dynamic-author**: Enter the dynamic authorization configuration mode.
- **client ipv4\_address [ secret shared\_secret ]**: Specify the IP address of the Dynamic Authorization Client. *ipv4\_address* must be in standard IPv4 dotted decimal notation.

You can add a list of client IPs from which the Disconnect message is accepted.

**secret shared\_secret**: This is an optional keyword. Specify the secret key at the client level.




---

**Important** Configuring the server key at the client level overrides the server key configured at the global level.

---

- **nas-identifier value**: Specify the dynamic authorization specific NAS-Identifier value. *value* must be an alphanumeric string of 1 to 64 characters.

If this keyword is configured, it is validated against the value received in DM request. If this keyword is not configured, the input value is silently ignored. That is, the DM requests from unlisted or unauthenticated clients are silently discarded.

- **secret shared\_secret**: Specify the global shared secret key of the server.

## Verifying the Session Disconnect Feature Configuration

This section describes how to verify the configuration associated with the Session Disconnect feature.

To view the information about the RADIUS Dynamic Authorization Clients that are configured in the system, use the **show radius-dyn-auth** command.

The following is a sample output of the **show radius-dyn-auth** command.

```
[unknown] smf# show radius-dyn-auth
radius-dyn-auth
-----
IP: 10.0.0.2
-----
COA:
0 total-requests      0 inprocess-requests
  0 retry-request-drops 0 invalid-requests
  0 bad-authenticators 0 internal-errors
0 ack-sent            0 nak-sent
-----
DISCONNECT:
0 total-requests      0 inprocess-requests
  0 retry-request-drops 0 invalid-requests
  0 bad-authenticators 0 internal-errors
0 ack-sent            0 nak-sent
-----
UnknownTypesRcvd: 0
-----
```

## Configuring the CoA-NAS Interface

Use the following sample configuration to define Change of Authorization (CoA) NAS interface in the RADIUS endpoint.

```
config
    endpoint radius
```

```
interface coa-nas
  vip-ip ipv4_address vip-port port_number
end
```

**NOTES:**

- **endpoint radius:** Enter the RADIUS endpoint configuration mode.
- **interface coa-nas:** Enter the CoA NAS interface configuration mode. This keyword defines a new interface "coa-nas".
- **vip-ip ipv4\_address vip-port port\_number:** Specify the IP address of the host. *ipv4\_address* must be in standard IPv4 dotted decimal notation.

You can configure a list of VIP-IPs to listen to the inbound CoA or DM requests.

**vip-port port\_number:** Specify the port number of the UDP proxy. By default, the port number is 3799. This default value is used only when the VIP-IP is specified.




---

**Important** This configuration allows only port to be specified per IP.

---

The SMF (udp-pxy) listens to the inbound CoA or DM request messages on these ports, and ACK or NAK messages sent with the respective source IP and port.

## RADIUS Test CLI support

The **RADIUS test** CLI provides a mechanism for testing network connectivity with and configuration of RADIUS authentication and accounting servers.

This functionality is useful in determining the accuracy of the system RADIUS configuration, the configuration of the subscriber profile on the RADIUS server and troubleshooting the server response time.

## Testing a RADIUS Accounting Server

When used to test a RADIUS accounting server, the tool generates an accounting request message for a specific username.

**Note**


---

The user name must already be configured on the RADIUS authentication server prior to executing the test.

---

To execute the RADIUS authentication test tool, enter the following command:

```
test-radius accounting { all | server-group group_name | server server_name
port server_port } { user_name client_nas_ip_address }
```

**NOTES:**

- **all:** Specify that all configured RADIUS accounting servers be tested.
- **radius group group\_name:** Specify the configured RADIUS authentication servers in a RADIUS server group named *group\_name* for server group functionality.



- *server\_name*: Specify the IP address of a specific RADIUS accounting server to test.
- *server\_port*: Specify the TCP port over that the system must use when communicating with the RADIUS accounting server to test.
- *user\_name*: Specify a username that is supplied to the RADIUS server for accounting.
- *client\_nas\_ip\_address*: Specify the IP address of the source NAS that is supplied to the RADIUS server for accounting.

### Example

The following command verifies all the RADIUS servers.

```
test-radius accounting all
```

The following command verifies the RADIUS accounting for user *user1* for the *sampleServer*.

```
test-radius accounting server sampleServer port 5000 username user1
```

The following command verifies the RADIUS accounting server group *star1* for user *user1*.

```
test-radius accounting server-group star1 username user1
```

## Testing a RADIUS Authentication Server

When used to test a RADIUS authentication server, the tool generates an authentication request message for a specific user name.



**Note** The user name must already be configured on the RADIUS authentication server prior to executing the test.

To execute the RADIUS authentication test tool, in the Exec mode, use the following command:

```
test-radius authentication { all | server-group group_name | server server_name
port server_port } { user_name password client_nas_ip_address }
```

### NOTES:

- **all**: Specify that all configured RADIUS authentication servers be tested.
- **radius group** *group\_name*: Specify the configured RADIUS authentication servers in a RADIUS server group named *group\_name* for server group functionality.
- *server\_name*: Specify the IP address of a specific RADIUS authentication server to test.
- *server\_port*: Specify the TCP port over that the system must use when communicating with the RADIUS authentication server to test.
- *user\_name*: Specify a username that is supplied to the RADIUS server for authentication.
- *password*: Specify the password associated with the username that is supplied to the RADIUS server for authentication.
- *client\_nas\_ip\_address*: Specify the IP address of the source NAS that is supplied to the RADIUS server for accounting.

### Example

The following command verifies all the RADIUS servers.

```
test-radius authentication all
```

The following command verifies the RADIUS authentication for user *user1* for the *sampleServer*.

```
test-radius authentication server sampleServer port 5000 username user1  
password dummyPwd
```

The following command verifies the RADIUS authentication server group *star1* for user *user1*.

```
test-radius authentication server-group star1 username user1
```

## RADIUS Client OA&M Support

This section describes operations, administration, and maintenance information for this feature.

### Statistics Support

#### RADIUS Authentication Statistics

This feature supports the following statistics related to RADIUS Authentication:

- SMF-Service:
  - Number of Secondary-Authentication requests sent
  - Number of Secondary-Authentication response received
- RADIUS-EP:
  - Number of Secondary-Authentication requests sent
  - Number of Secondary-Authentication response received
  - Number of RADIUS packets sent
  - Number of RADIUS packets received

#### RADIUS Accounting Statistics

The SMF maintains the following statistics to track the total number of attempted, successful, and failed RADIUS Accounting Start, Accounting Update Interim and Accounting Terminate requests and responses.

- SMF\_SERVICE\_STATS for the following procedure types:
  - radius\_initial: This counter gets incremented for Accounting Start request and response.
  - radius\_update: This counter gets incremented for Accounting Interim Update request and response.
  - radius\_terminate: This counter gets incremented for Accounting Terminate request and response.

### RADIUS Access Management Statistics

The following statistics track the number of times the AVP is received in the RADIUS Access-Accept messages at SMF.

- SmfRadiusMessageStats

INBOUND:

- radius\_access\_accept
  - radius\_avp\_session\_timeout
  - radius\_avp\_idle\_timeout

### PAP, CHAP, or MSCHAP-based Authentication Statistics

The SMF supports the following statistics to track the number of times the AVP sent in Access-Request messages.

**Group:** smf\_radius\_message\_stats

**Format:** {app\_name, cluster, data\_center, direction, instance\_id, message\_type, radius\_avp\_type, rat\_type, service\_name}

**message\_type:** radius\_access\_request

**radius\_avp\_type:**

- radius\_avp\_pap\_user\_password
- radius\_avp\_pap\_username
- radius\_avp\_chap\_challenge
- radius\_avp\_chap\_response
- radius\_avp\_mschap\_challenge
- radius\_avp\_mschap\_response

#### Example:

```
smf_radius_message_stats{app_name="SMF",cluster="Local",data_center="DC",direction="outbound",instance_id="0",message_type="radius_access_request",radius_avp_type="radius_avp_pap_user_password",rat_type="NR",service_name="smf-service"} 1
```

```
smf_radius_message_stats{app_name="SMF",cluster="Local",data_center="DC",direction="outbound",instance_id="0",message_type="radius_access_request",radius_avp_type="radius_avp_pap_username",rat_type="NR",service_name="smf-service"} 1
```

The SMF supports these additional statistics to track the number of attempted, successful and failed responses received due to PAP, CHAP, and MSCHAP authentication.

**Group:** radius\_authentication\_message\_stats

**Format:** {app\_name, cluster, data\_center, dnn, instance\_id, radius\_auth\_algorithm, rat\_type, reason, service\_name, status}

**radius\_auth\_algorithm:**

- radius\_auth\_algorithm\_default

- radius\_auth\_algorithm\_pap
- radius\_auth\_algorithm\_chap
- radius\_auth\_algorithm\_mschap

**rat\_type:**

- NR
- EUTRA
- WLAN

**status:**

- decode\_failed
- encode\_failed
- attempted
- success
- failed
- timeout

**reason:**

- parse\_error
- invalid\_code
- invalid\_option
- invalid\_pco
- invalid\_epco
- invalid\_apco
- write\_error

**Example:**

```
radius_authentication_message_stats{app_name="SMF",cluster="Local",
data_center="DC",dnn="intershat2",instance_id="0",
radius_auth_algorithm="radius_auth_algorithm_default",rat_type="NR",reason="",
service_name="smf-service",status="attempted"} 2

radius_authentication_message_stats{app_name="SMF",cluster="Local",
data_center="DC",dnn="intershat2",instance_id="0",radius_auth_algorithm="radius_auth_algorithm_default",
rat_type="NR",reason="",service_name="smf-service",status="success"} 2

radius_authentication_message_stats{app_name="SMF",cluster="Local",data_center="DC",
dnn="intershat",instance_id="0",radius_auth_algorithm="radius_auth_algorithm_chap",
rat_type="EUTRA",reason="",service_name="smf-service",status="attempted"} 2

radius_authentication_message_stats{app_name="SMF",cluster="Local",
data_center="DC",dnn="intershat",instance_id="0",radius_auth_algorithm="radius_auth_algorithm_chap",
rat_type="EUTRA",reason="",service_name="smf-service",status="failed"} 2
```

### **RADIUS Disconnect and CoA Request Related Statistics**

The RADIUS endpoint (radius-ep) pod supports the following statistics.

#### **Radius\_Server\_Status**

Description: Display the active or inactive status of RADIUS server.

Metrics-Type: Gauge

Metrics-Value: 1 – ActiveServer, 0 – Inactive Server

Labels:

- Label: radSvrIP
  - Description: Server IP Address
  - Value: <any-ip-address>
  
- Label: radSvrPort
  - Description: Server Port
  - Value: <any-port>
  
- Label: radSvrPortType
  - Description: Authentication or Accounting type
  - Value: Auth, Acct

#### **Radius\_Requests\_Current**

Description: Displays the outstanding authentication and accounting requests

Metrics-Type: Gauge

Labels:

- Label: radMsgCode
  - Description: RADIUS Message Type
  - Values: SecondaryAuthenReq, RadiusAcctReq, TestAuth, TestAcct
  
- Label: radSvrIP
  - Description: Server IP Address
  - Value: <any-ip-address>
  
- Label: radSvrPort
  - Description: Server Port
  - Value: <any-port>
  
- Label: radSvrPortType
  - Description: Authentication or Accounting type

- Value: Auth, Acct
- Label: dnn
  - Description: DNN of subscriber
  - Value: <string>
- Label: procType
  - Description: Procedure-type
  - Value: <string>
- Label: ratType
  - Description: RAT type of subscriber
  - Value: <string>
- Label: sessType
  - Description: Session-type of subscriber
  - Value: <string>

### **Radius\_Requests\_Statistics**

Description: Displays the total authentication and accounting requests transmitted, retransmitted, and responses received

Metrics-Type: Counter

Labels:

- Label: radMsgCode
  - Description: Radius Message Type
  - Values: SecondaryAuthenReq, RadiusAcctReq, TestAuth, TestAcct
- Label: radPacketType
  - Description: Direction of packet
  - Value: Tx, Rx, Retry\_Tx
- Label: radResult
  - Description: Result of operation
  - Value: Success, Failed, Timeout, Failure\_Reject, ...
- Label: radSvrIP
  - Description: Server IP Address
  - Value: <any-ip-address>

- Label: radSvrPort
  - Description: Server Port
  - Value: <any-port>
- Label: radSvrPortType
  - Description: Authentication or Accounting type
  - Value: Auth, Acct
- Label: dnn
  - Description: DNN of subscriber
  - Value: <string>
- Label: procType
  - Description: Procedure-type
  - Value: <string>
- Label: ratType
  - Description: RAT type of subscriber
  - Value: <string>
- Label: sessType
  - Description: Session-type of subscriber
  - Value: <string>

### **Radius\_CoaDM\_Requests\_Current**

Description: Displays the outstanding CoA and DM requests being processed.

Metrics-Type: Gauge

Labels:

- Label: radMsgCode
  - Description: RADIUS Message Type
  - Values: DisconnectRequest, CoARequest
- Label: radSvrIP
  - Description: Server IP Address
  - Value: <any-ip-address>

### **Radius\_CoaDM\_Requests\_Statistics**

Description: Displays the total CoA and DM requests received and processed.

Metrics-Type: Counter

Labels:

- Label: radMsgCode
  - Description: Radius Message Type
  - Values: DisconnectRequest, DisconnectACK, DisconnectNAK, CoARequest, CoaDMReq, CoAACK
- Label: radPacketType
  - Description: Direction of packet
  - Value: Tx, Rx
- Label: radResult
  - Description: Result of operation
  - Value: Success, Failure\_Invalid\_Request, Failure\_Drop\_Retry\_Coa, Failure\_Unknown\_Error...
- Label: radSvrIP
  - Description: Server IP Address
  - Value: <any-ip-address>
- Label: nakErrorCause
  - Description: Error-cause set during COA-NAK / DM-NAK (not applicable for other cases)
  - Value: Missing-Attribute, NAS-Identification-Mismatch, Unsupported-Service, Invalid-Attribute-Value, Session-Context-Not-Found, Internal-Error





## CHAPTER 37

# RPC Remote Host Management

- [Feature Summary and Revision History, on page 643](#)
- [Feature Description, on page 643](#)
- [RPC Remote Host Management OAM Support, on page 643](#)

## Feature Summary and Revision History

*Table 181: Revision History*

Revision Details	Release
First introduced.	2020.03.0

## Feature Description

Show RPC feature in App-Infra provides RPCs to connect to remote NFs. These RPCs are managed in App-Infra. This CLI shows the information about the RPC and RPC remote host information in tabular format.

## RPC Remote Host Management OAM Support

This section provides information regarding show commands available to monitor and troubleshoot the SMF RPC Remote Host Management.

### show-rpc

This command lists all the RPCs from all the pods with RPC and remote host information.

POD

- **POD INSTANCE** - Displays the Instance info of the POD
- **NAME** - Displays the Name of the RPC registered in POD
- **REMOTE ADDRESS** - Displays IP address and Port of remote endpoint

- REMOTE HOST - Displays name of the RPC host
- TYPE - Displays the type of connection like Rest, Grpc, GrpcStream etc
- SET NAME- Displays the RPC set name for group of RPC hosts
- STATUS - Displays the current state of the RPC host, possible status values are Started, Starting and Stopped
- CONNECTED TIME - Displays the time when the RPC host was connected
- DISCONNECTED TIME - Displays the time when the RPC host was disconnected
- MONITOR RPC HOST - Indicates whether the RPC host is being monitored for connection status
- PROCESSING INSTANCE INFO - Indicates the if the processing instance name if available
- VERSION - Displays the version of the RPC host API if available



## CHAPTER 38

# Resource Management

- [Feature Summary and Revision History, on page 645](#)
- [Feature Description, on page 645](#)
- [How it Works, on page 646](#)

## Feature Summary and Revision History

### Summary Data

*Table 182: Feature Summary*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 183: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

The UE IP address and ID allocation and management (resource management) feature is used by the SMF service and supported by the NodeMgr.

The Master NodeMgr initializes the following in Redis-DB:

- IP pools for all DNN profiles
- Running counter for ID
- Free list for ID

The NodeMgr hosts the resource management server functionality and exposes the APIs for:

- IP allocation and management
  - IP allocation
  - IP release
  - IP reallocation (release the current IP and allocate new IP for UE)
- ID allocation and management
  - ID allocation
  - ID release
  - ID reallocation (release the current ID and allocate new ID)

The SMF service runs the resource management client to use the Rmgr services.

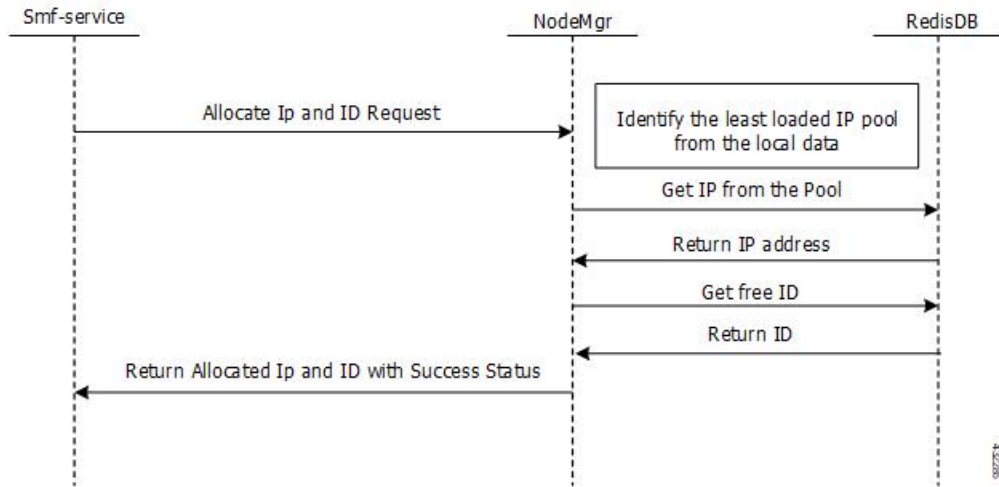
## How it Works

### Call Flows

#### IP and ID Allocation

The following figure illustrates the IP and ID allocation call flow.

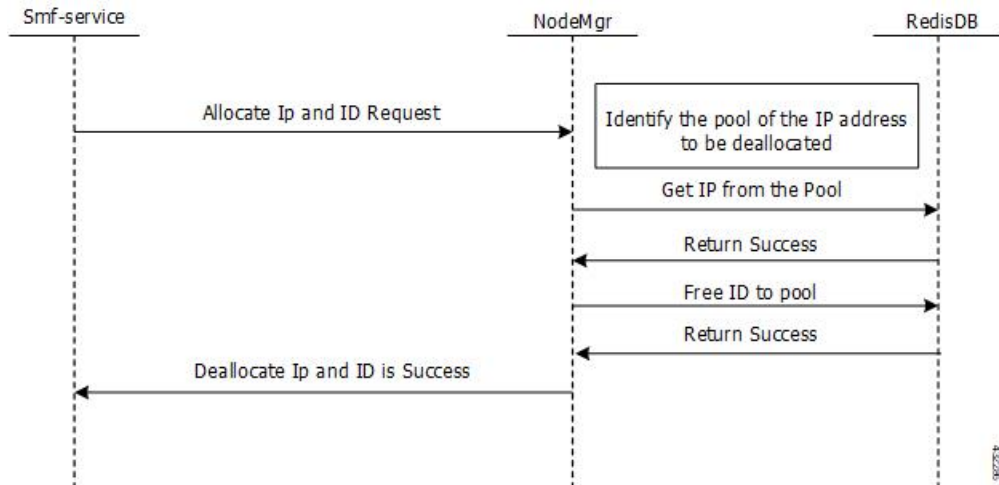
Figure 117: IP and ID Allocation Call Flow



## IP and ID Deallocation

The following figure illustrates the IP and ID deallocation call flow.

Figure 118: IP and ID Deallocation Call Flow







## CHAPTER 39

# Router Solicit and Router Advertisement

- [Feature Summary and Revision History, on page 649](#)
- [Feature Description, on page 649](#)
- [ICMPv6 Profile Configuration, on page 651](#)

## Feature Summary and Revision History

### Summary Data

*Table 184: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 185: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

To comply to IPv6 Stateless Auto-configuration, SMF supports ICMPv6 Router Solicit and Advertisement.

The following ICMPv6 options are supported in Router Advertisement:

- Prefix Information: Allocated UE IPv6 Prefix is sent.

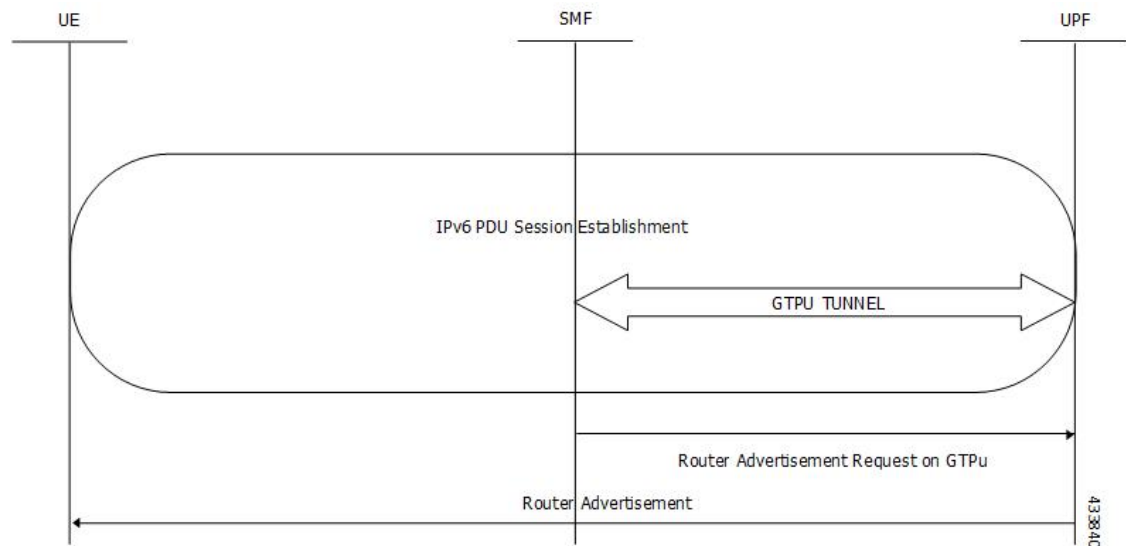
- MTU: Value is taken from configuration. Default is 1500.
- Source Link Layer Address: Value is taken from configuration local virtual mac.

In releases prior to 2020.02, the SMF queued the Router Advertisement (RA) and Router Solicitation (RS) messages when the PCF-initiated PDU Modification Request is triggered immediately after the Session Create Request.

In this release, the SMF sends the RA message and also responds to the RS message when the PCF-initiated PDU Modification Request is triggered immediately after the Session Create Request. That is, the SMF prioritizes the processing of RA and RS messages over the PCF-initiated PDU Modification Request.

## Unsolicited Router Advertisement

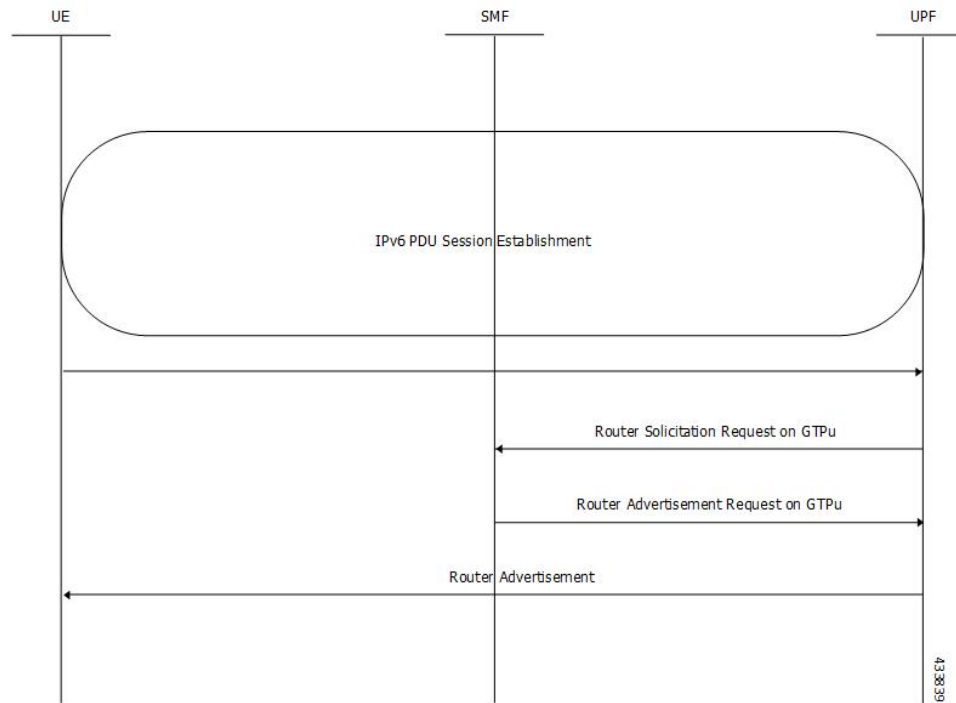
SMF sends unsolicited router advertisement on successful PDU session establishment to share the allocated IPv6 prefix to UE. RA message is sent over the GTPU tunnel, which is created between the SMF and UPF during the Session Establishment procedure. SMF also installs PDRs and FARs on the UPF to enable routing for RS/RA messages.



## Solicited Router Advertisement

To get the allocated IPv6 prefix, UE can send a router solicit message. On receiving router solicit message, SMF sends router advertisement message towards UE containing the allocated UE IPv6 prefix.





## ICMPv6 Profile Configuration

The following configuration is used to configure Router Advertisement parameters:

```

scheduler(config-icmpv6-profile-icmp1# show full
icmpv6-profile icmp1
local-virtual-mac ac:de:48:00:11:22
hop-limit          64      default 255
router-lifetime    100 (seconds) default 65535
reachable-time     30 (milliseconds) default 0
retrans-timer      1 (milliseconds) default 0
mtu                1500 default 1500
!

dnn-profile dnn1
remote-virtual-mac fa:00:4c:a8:22:05 default(00:14:22:01:23:45)
ipv6-pool name pool1
    prefix          2001:300:4001::/48
    prefix-lifetime 3456 (seconds) default 4294967295
!
!
smf-profile prof
service name srv1
    associate-icmpv6-profile icmp1
!
!

```

**NOTES:**

- /48 is the only prefix supported in this release.



# CHAPTER 40

## Session and Service Continuity Mode

- [Feature Summary and Revision History, on page 653](#)
- [Feature Description, on page 653](#)
- [Configuring SSC Mode, on page 655](#)

### Feature Summary and Revision History

#### Summary Data

*Table 186: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 187: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

### Feature Description

The Session and Service Continuity (SSC) support in 5G system architecture addresses the various continuity requirements of different applications and services for the User Equipment (UE). The 5G system supports

different SSC modes. The SSC mode associated with a PDU session does not change during the lifespan of a PDU session. The SSC feature supports the following three modes:

- SSC mode 1—The network preserves the connectivity service provided to the UE. For the PDU session of IPv4 or IPv6 or IPv4v6 type, the IP address is preserved.
- SSC mode 2—The network may release the connectivity service delivered to the UE and also release the corresponding PDU sessions. For IPv4 or IPv6 or IPv4v6 type, the release of the PDU session induces the release of IP addresses allocated to the UE.
- SSC mode 3—Changes to the user plane can be visible to the UE while the network ensures that the UE suffers no loss of connectivity. A connection through new PDU session anchor point is established before the previous connection is terminated for better service continuity. For IPv4 or IPv6 or IPv4v6 type, the IP address is not preserved in this mode when the PDU session anchor changes.

## SSC Mode Selection

The SSC mode selection policy determines the type of mode associated with an application or group of applications for the UE. As part of the subscription information from UDM, the SMF receives the list of supported SSC modes and the default SSC mode per DNN and per S-NSSAI.

To select the SSC mode, when UE sends SSC mode in PDU Session Establishment Request, the allowed SSC mode is determined by checking against the subscriber data and local SMF configuration.




---

**Important** SMF supports only SSC mode-1 in this release.

---

## Priority for Choosing SSC Mode

The priority levels for choosing SSC mode are:

- Priority #1—Subscriber data from UDM has the highest priority. UDM sends DefaultSscMode and AllowedSscMode.
- Priority #2—Local SSC mode configuration data present in DNN profile contains ssc-mode and allowed-ssc-mode.

## SSC Mode Selection Method

The SSC mode supports the following selection methods:

- The SMF verifies if UE sent SSC mode is part of either default SSC mode or allowed SSC mode in order of priority. If it is found, PDU Establishment procedure continues. Otherwise, PDU Session Establishment Reject message will be sent to the UE with allowed SSC modes in reject message.
- If the SMF does not receive SSC mode from the UE, then default SSC mode in order of priority is chosen and used to establish the PDU session.
- This release only supports SSC mode-1. If UE sends any other modes, the PDU Session Establishment will be rejected.

When UE requests SSC mode-2 or mode-3, if the UE's subscription (in order of priority: UDM or Local configuration on SMF) allows SSC mode-1 along with mode-2 or mode-3, then SMF sends PDU Session Establishment Reject with 5GSM cause 68 (Not supported SSC mode) and Allowed SSC mode as 01. This method allows the UE to retry with SSC mode-1. As per 3GPP TS 24.501, the 5GSM cause 68 is sent when the requested SSC mode is not supported by the subscription.

To honor PDU Session Establishment, the SMF expects SSC mode either through UDM subscription or local configuration. If SMF does not have SSC mode as part of UDM subscription or local configuration, the SMF rejects PDU Session Establishment with 5GSM cause 31 (Request rejected and unspecified).

## Configuring SSC Mode

Use the following sample configuration to configure the SSC mode in the SMF DNN profile.

```
config
  profile dnn dnn_name
    ssc-mode sscmode_value allowed allowed_sscmode_value
  exit
```

### NOTES:

- **profile dnn *dnn\_name***: Enter the DNN profile configuration mode.
- **ssc-mode *sscmode\_value* allowed *allowed\_sscmode\_value***
  - **ssc-mode *sscmode\_value***: Specify the SSC mode. *sscmode\_value* must be an integer in the range of 1–3.
  - **allowed *allowed\_sscmode\_value***: Specify the allowed SSC mode. Up to two modes are allowed apart from the default SSC mode. *allowed\_sscmode\_value* must be an integer in the range of 1–3.
- **no ssc-mode**: Specify this command to remove the SSC mode from the SMF DNN profile.





# CHAPTER 41

## SMF Charging

- [Feature Summary and Revision History, on page 657](#)
- [Overview, on page 658](#)
- [Mapping of Charging Scenario on Various Interfaces, on page 675](#)
- [Error Handling Scenarios, on page 681](#)
- [Dynamic Configuration Change Support, on page 685](#)

## Feature Summary and Revision History

### Summary Data

*Table 188: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 189: Revision History*

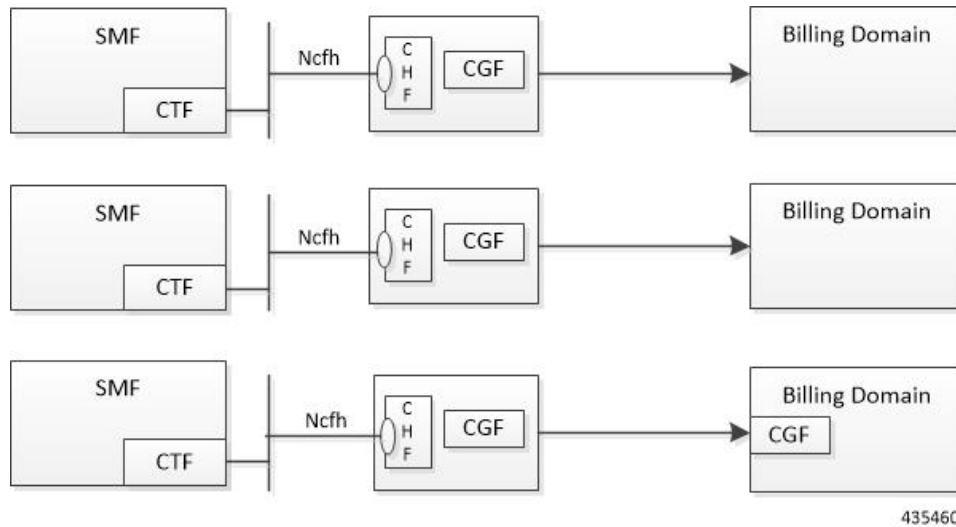
Revision Details	Release
Introduced support for the following: <ul style="list-style-type: none"><li>• Zero Usage Report Suppression</li><li>• Dynamic ACS Configuration Change</li></ul>	2021.01.0
First introduced.	Pre-2020.02.0

# Overview

The SMF acts as a Charging Transfer Function (CTF). The CTF generates charging events toward the Charging Function (CHF), which is responsible for generating Charging Data Records (CDRs).

This SMF interacts with various interfaces such as N40, N4, N7, and N10, facilitating charging in entirety. Currently, the Cisco SMF uses the Nchf/N40 interface to generate charging events.

**Figure 119: SMF as a Charging Transfer Function**



The SMF Charging feature supports the following functionality:

- Converged Online and Offline charging
- PDU session charging using the service-based interface.
- Network slice instance charging
- Charging information collection per PDU session for UEs served under 3GPP access.
- Unique identity number assignment per PDU session for billing purposes.
- Separate count of data volumes on both the uplink and downlink directions. The data volumes reflect the data as delivered to and forwarded from the user.
- Charging mechanism that provides the date and time information when the PDU session starts.
- Handling of Charging Characteristics specific to a subscription or a subscribed DNN.
- Identification of data volumes, elapsed time, or events for individual service data flows (flow-based charging). One PCC rule identifies one service data flow.
- Usage reporting of a service or a detected application per rating group or per combination of the rating group and service ID. This reporting level can be activated per PCC rule.
- Quota management per Rating Group (RG) per PDU session.
- Charging for IP-based PDU session types.



## Converged Charging

The 5G system supports converged charging for offline and online charging scenarios.

The SMF performs converged charging for each of the following:

- Charging data that is related to PDU session.
- Charging data that are related to service-data flows within a PDU session.

The scope of convergent charging in this implementation includes quota management and usage reporting. For convergent charging, the SMF interacts with the CHF for charging data related to PDU sessions. The Charging Data Request and the Charging Data Response messages are exchanged between the SMF and the CHF based on session-based charging (SCUR scenarios). The Charging Data Request is issued by the SMF only when conditions that are related to chargeable events are met.

## Chargeable Events

PCC rules can be activated, deactivated, and modified at any time during the PDU session lifetime.

The following attributes can be modified by the PCF in a dynamic PCC rule active in the SMF:

- Charging Key
- Service Identifier
- Measurement Method

Activities on PCC rules and QoS flows are not chargeable events. However, change of charging rule in PCC rules lead to chargeable events such as:

- Start of service data flow
- Termination of service data flow, for the last service data flow for the original PCC rule

The charging key (that is, rating group) is used to request online charging quota.

## Charging Identifier

The charging identifier correlates charging information between the SMF and CHF during the duration of a PDU session. The SMF generates and assigns a charging identifier when a PDU session is established. The charging identifier is unique for that PDU session and is used in all messages that are exchanged in that PDU session.

## Charging Information

The SMF collects the following charging information for converged online and offline charging:

- Usage of access and core network resources: Describes the amount of data that is delivered to and forwarded from the UE.
- Usage duration: Time interval from PDU Session Establishment to PDU Session Release.
- User: UE information used by the user for a PDU session.
- Data network: Data network address as determined by the DNN.
- Start time: PDU session start time.

- User location: HPLMN and VPLMN reporting area.

For service-data flows (flow-based charging), the SMF collects the following information:

- PDU session description.
- Data that are transmitted in uplink and downlink directions based on the rating-group information, or a combination of rating-group and service ID during volume-based charging.
- Duration of service data flow based on the rating group, or a combination of rating-group and service ID during event-based charging.
- Events and timestamps based on rating-group or based on a combination of the rating-group and service ID during event-based charging.

The SMF collects charging information for service data flows per UPF, within a PDU session, based on the rating-group or based on a combination of rating-group and service ID.

## How it Works

### Charging Session

The SMF supports converged session-based charging (SCUR) as specified in *3GPP TS 32.290, section 5.3.2.3*.

The SMF establishes charging session with the CHF with the Charging Data Request and Response (Initial) exchange. During the life of the PDU session, usage is reported with Charging Data Request/Response (Update) exchange. After the session is released, Charging Data Request/Response (Termination) messages are exchanged.

### Offline Charging and Online Charging

Charging is enabled for a session based on the input that is received from the PCF.

For offline charging, the SMF sends Charging Data Request Initial toward the Charging Function (CHF) based on the presence of charging descriptors and refChgData field set in the smPolicyDecision message from the PCF in SmPolicyControlCreate response.

On determining if charging is required during initial session establishment or post-session establishment, charging is enabled for the PDU session. Once charging is enabled, SMF sends the Charging Data Request (Initial) Message toward the CHF.

The SMF determines Volume/Time threshold value either locally or from Charging Data Response. These values are used to update Volume/Time threshold IE in URR and to set the reporting trigger accordingly. The measurement method that is used in URR is derived from charging data.

For online charging, the SMF receives the Volume/Time Threshold and Quota values from the CHF. These values are received in the Charging Data Response (Initial) or using a Charging Data Request (Update) during a PDU Session Establishment. The SMF relays these Volume/Time Threshold and quota values to the UPF in the corresponding URR.




---

**Note** The threshold values from CHF always override the locally configured values.

---

The following table maps the IEs that are shared with the UPF during Create or Update URR during online or offline charging scenarios:

**Table 190: IE Mapping for Online and Offline Charging Scenarios**

IE	Online	Offline	Derived From
Volume Limit	Yes	Yes	CHF Response or Local Configuration
Time Limit	Yes	Yes	CHF Response or Local Configuration
Volume Quota	Yes	No	CHF Response
Time Quota	Yes	No	CHF Response
Quota Holding Time	Yes	—	CHF Response
Monitoring Time	Yes	Yes	<ul style="list-style-type: none"> <li>• Local configuration for offline charging</li> <li>• CHF response for online charging</li> </ul>
Reporting Trigger	Yes	Yes	The respective triggers that are set as shown in the following table.

The following table lists the reporting triggers and their derived source:

**Table 191: Reporting Triggers and the Derived Source**

Reporting Trigger	Derived From
Volume Threshold Trigger	If Volume threshold is set
Time Threshold Trigger	If Time threshold is set
Volume Quota Trigger	If Quota Exhausted trigger is set from CHF
Time Quota Trigger	If Quota Exhausted trigger is set from CHF
LIUSA Trigger	If URR contains Linked URR

## Quota Management

The SMF requests quota from the CHF upon meeting any of the following conditions:

- The Rating Group (RG) is installed for the first time and the charging method is Online for the dynamic rule.
- The start of traffic trigger is initiated from the UPF for the RG in the case of static or predefined rules.
- A specific trigger type, as defined in the 3GPP specification 32.255, is received in the usage report for the online charging service from the UPF.

The SMF uses the **quota request always** CLI command to request the quota always. This CLI command is available in the Charging Profile configuration mode. Upon configuring this CLI command, the SMF always requests for quota when reporting the usage to the CHF for the online services. The quota requesting ends when the charging service stops.

Irrespective of the **quota request [ always | standard ]** CLI configuration, the quota request is disabled for the trigger type "qht" configured through the **quota suppress triggers** CLI command.

For command details, see the [Charging Profile Configuration, on page 672](#) section in the *SMF Charging* chapter of this guide.

## Service Units for Quota Management

The SMF sends Charging Data Request (CDR) to the Charging Function (CHF) for the service to be granted authorization to start, and to reserve the number of units. While triggering the CDR, the SMF requests volume (uplink, downlink, total) and time quota from CHF to support VoLTE and other use cases. The values of the requested units for static rules are obtained from the Diameter configuration under Active Charging Service. For the dynamic audio or video rules, the values for the requested service units are configured through the **requested-service-unit** CLI command in the Charging Profile Configuration mode. For command details, see the [Charging Profile Configuration, on page 672](#) section in the *SMF Charging* chapter of this guide.

## Support for Validity Time

The SMF uses time quota value and its corresponding trigger on N4 interface to arm the UPF about the time when the SMF needs the reporting of validity time.

The CHF arms the SMF to report the usage for the rating group when the timer associated with the validity\_time expires.

Based on the presence of Validity Quota and Time Quota, the SMF behaves as specified in the following ways:

- When the CHF sends only the Time Quota and not the Validity Quota, the SMF relays the CDR-U to the CHF and reports as Quota\_EXHAUSTED upon receiving the usage report from the UPF.
- When the CHF sends only the Validity Quota and not the Time Quota, the SMF relays the CDR-U to the CHF and reports as VALIDITY\_TIME upon receiving the usage report from the UPF.
- When the CHF sends both the Validity Quota and the Time Quota, the SMF determines the lower value of time\_quota and validity\_time, and then relays the CDR-U to the CHF accordingly. The SMF sends the "VALIDITY\_TIME" trigger when the validity\_time is lesser than the time\_quota value. Similarly, when the validity\_time is greater than the time\_quota value, the SMF sends the "Quota\_EXHAUSTED" trigger.

## CHF Selection

The CHF selection, that is, CHF address determination by the SMF is performed during PDU Session Establishment. This selection is based on the following in order of priority:

1. PCF provides one or more CHF addresses as part of the PCC rule.
2. UDM-provided charging characteristics.
3. NRF-based discovery.
4. SMF locally provisioned charging characteristics.




---

**Note** The local configuration is currently used to get CHF IP/port.

---

## Charging Activities at SMF

### URR Generation Toward N4

The SMF receives charging-data and usage-monitoring-data from the PCF. Based on this information, the SMF derives URR toward N4. In case the SMF is configured with volume/time limit at the session level, the SMF creates session-level URR.

### Handling of Initial Event in Charging Component

The session context of SMF is configured with trigger/threshold as per the default described in *3GPP TS 32.255*. It overrides the same based on configuration present in the charging profile. The same values can be further overridden by CHF Charging Data Response Initial. Currently, trigger/threshold cannot be overridden when in PDU Establishment state.

The charging profile is referenced from the charging-characteristic profile. The CC profile is taken from UDM subscription for PDU session. If the CC profile is not mentioned in the UDM response, it is taken from the DNN profile.

After trigger/threshold/quota are determined, the SMF N4 Setup Request with set of Create URRs are derived from charging-data with one session-level URR.

If the session-level reporting is determined, the session-level URR is associated to each SDF URR.

The following triggers are supported:

- Volume/Time trigger at session/RG level
- AMBR change
- QoS change
- Quota threshold and quota exhausted
- Quota handling time
- Tariff time change

### Obtaining Threshold Values at SMF

Threshold values, during online charging, are always obtained from the CHF. Whereas the threshold values, during offline charging, are obtained either from the CHF or from the charging profile configuration.

If charging profile is not determined during PDU establishment, the SMF refers to the charging profile from the DNN profile. Once the Charging Profile is determined, the SMF uses the determined Charging Profile to obtain the threshold values for Session/SDF URR.

The configuration has threshold values at a session level or rating-group level. The rating-group level threshold values are generic and not about a rating-group. These threshold values are overwritten by CHF response.

**Note**

The CHF response has various triggers. If some trigger is available at the session level or rating-group level, and if the volume or time threshold value is unavailable, then these values are assumed to be disabled at the corresponding level.

## Trigger Determination at SMF

The SMF has triggers enabled by default, as specified in 3GPP TS 32.255, section 5.2.1.4.

These triggers can be overwritten at a session level by trigger configurations present in the charging profile. Further, these triggers can also be overwritten by CHF responses.

Trigger configuration in charging profile is only applicable at a session level. It is not applicable for rating-groups.




---

**Note** The CHF response has various triggers. If some triggers exist at a session or rating-group level and other triggers do not exist, then these triggers are assumed to be disabled.

---

## Reporting Category

The charging trigger can be of two reporting categories—Immediate and Deferred. The usage report of the immediate category must be reported to the CHF immediately. For reporting events that must be deferred, the SMF stores the usage report locally, and publishes either when the next trigger of the immediate category is invoked, or when the storage limit is exhausted.

When reporting stored usage reports to the CHF, the usage report is triggered because of the trigger type in UsedUnitCategory and the message is triggered because of the trigger type in ChargingDataRequest.

Sometimes, a scenario can have two triggers hit at the same time. AMBR\_Change and QoS Change can happen at the same time. In which case, all the triggers as applicable at the RG level or session level will have multiple trigger values.

A trigger can be enabled at the RG level, and for some RG it can be immediate reporting and for others it can be deferred reporting. When a trigger event is hit, various usage reports will have a corresponding category filled respectively in usedUnitContainer.

Deferred CDR will be relayed in the following scenarios:

- An immediate category event happens.
- Maximum number of charging conditions are crossed.
- Configured number of maximum deferred reporting is crossed.

Maximum Charging Characteristics (CC) is reset whenever there are push CDRs. This could be because of maximum CC limits being crossed or because of immediate category reporting.




---

**Note** Currently, SMF does not support two charging descriptors with the same rating group.

---

## Handling Reporting Level

The reporting category is classified into the following:

- Rating Group (RG) level: The RG is mandatory at this level.
- Service ID level: The RG and service ID is mandatory at this level.
- Sponsor ID level: The RG and Sponsor ID is mandatory at this level.

The reporting level is communicated to the SMF from PCF in the Charging Data Request. If the reporting-level is RG, then RG is the primary key. If the reporting level is Service\_level or SponserLevl, then RG and Service ID or RG or Sponsor ID respectively become the primary key. The SMF drops the charging descriptors from the PCF if the above requirement is not satisfied.

**Re-Authorization**

The CHF triggers Reauthorization of charging descriptors using Charging Notify request. Reauthorization is implemented at the session-level or at a RG-level for both online and offline charging.

The SMF processes the reauthorization details (which contain an array of RG, ServiceId, QuotaMgmtIndicator) received in CHF Notify and retrieves the charging descriptors associated with the current PDU session. SMF ignores any unmatched reauthorization item.

For the charging descriptors identified for reauthorization, the SMF queries for usage reports from UPF and sends it to the CHF.

As part of the CHF response, the SMF detects any change in quota or threshold information and performs N4 Session Modification to update URRs.

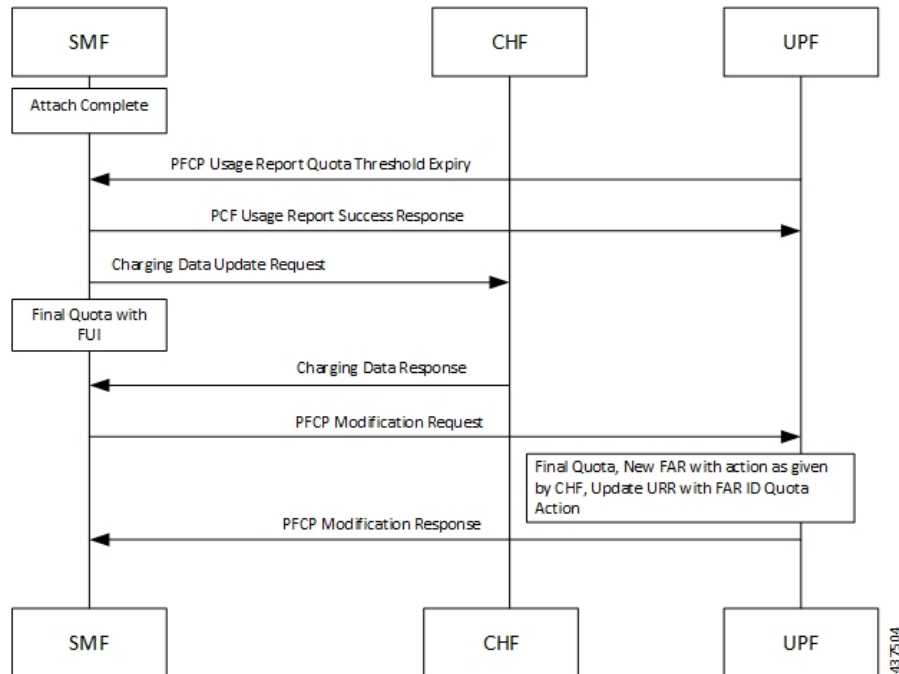
**Final Unit Indication Support**

The SMF supports Final Unit Indication (FUI) in the Charging Data Initial or Update Response from CHF as per 3GPP TS 32.291, section 6.1.6.2.1.12.

On receiving FUA, the SMF installs new FAR and associates its FAR-ID in the URR, in the FAR ID Quota Action IE. If a FAR with same parameters exists, the SMF uses its FAR-ID in the Create or Update URR. The UPF initiates appropriate actions set in FAR after quota exhaustion.

Currently, the SMF only supports Terminate and Redirect FU actions.

**Figure 120: FUI in the Charging Data Initial or Update Response from CHF**



**Note**

- At any instance, CHF provides granted unit (Quota) to the SMF along with FUI.
- When SMF receives the granted unit with FUI, the SMF creates FAR toward N4 and associates it to the corresponding URR which carries the Quota information.
- After UPF receives the FAR associated with the URR, the corresponding FAR action is implemented when the quota exhausts.

## Static and Predefined Rules for Charging

Configuration of static or predefined rules is similar to the procedures on SMF and UPF. The layout of configuration is as follows:

1. Rulebase: A one-to-many rulebase is configurable. For a single PDU session, you can activate a single rulebase any time. PCF can activate the rulebase at SMF by sending the rulebase name in the PCC rule.
2. Ruledef: Each rulebase can have one-to-many ruledef configurations. A ruledef can either be of static or predefined type. Each ruledef is assigned to a charging action.
3. Charging Action: Contains QoS and charging information.

The SMF derives charging data for each charging action in the rulebase. Charging action associated to static rules in the rulebase is immediately derived and updated in the PDU context. Charging action that is associated to predefined rules is derived and updated when PCF activates the specific predefined rule at SMF.

The charging action derived URR has the following behavior:

- Online charging is identified by the "**cca charging credit**" configuration under charging action.
- Offline charging is identified by the "**billing action egcdr**" configuration under charging action.
- Armed triggers for volume-limit and time-limit are under the gtp group configuration, under APN. The UPF automatically detects these values and sends the respective usage reports.
- The SMF, unlike the dynamic case, does not send the Create URR immediately for charging data that is derived from the configured rules.
- Using the online charging method, the UPF sends usage report with the "Start" trigger. The SMF uses CHF to derive the quota for the RG and relays the same information to the UPF in the Update URR message.
- You can configure the UPF threshold at a rulebase level. It creates a rulebase-level URR that is linked to all ruledef-level URR within the rulebase.

## Modification Scenarios in Charging

### PCF Update

The PCF performs the following actions during a modification scenario:

- Addition of PCC rules
- Modification of reference data



- Deletion of PCC rules
- Content update in charging data - using Measurement method

## CHF Response

The CHF response, during an exchange, sends updated volume and time thresholds and quota. The SMF relays the updated URR toward N4.

A change in threshold, trigger, or quota triggers an Update URR, which leads to the N4 relay.

SMF sends the Update URR based on the following triggers:

- Volume or time threshold
- Volume or time quota
- Tariff time change
- Quota holding time, and so on

## URR Linking

- If you have configured session-level volume or time value locally or have received them from the CHF, the SMF creates session-level URR and links it to all URR corresponding to offline charging descriptors.
- If PCF receives multiple charging descriptors that are of the same rating group, the SMF creates extra URR and links it to all URR derived from charging descriptors of the same rating group.

## URR Format

Following is the URR ID format:

- URR ID is 32-bit.
- MSB (32nd) bit for static or predefined URRs is configured to 1, and for dynamic URRs is configured to 0.
- First four LSB bits are configured for interface type.
  - 1 for offline
  - 7 for online
- Bit 4-31 is for URR ID number.

For example: Dynamic first URR if ID is 1:

0x00 00 01 01 Offline

0x00 00 01 07 Online

Static or Predefined first URR if ID is 1:

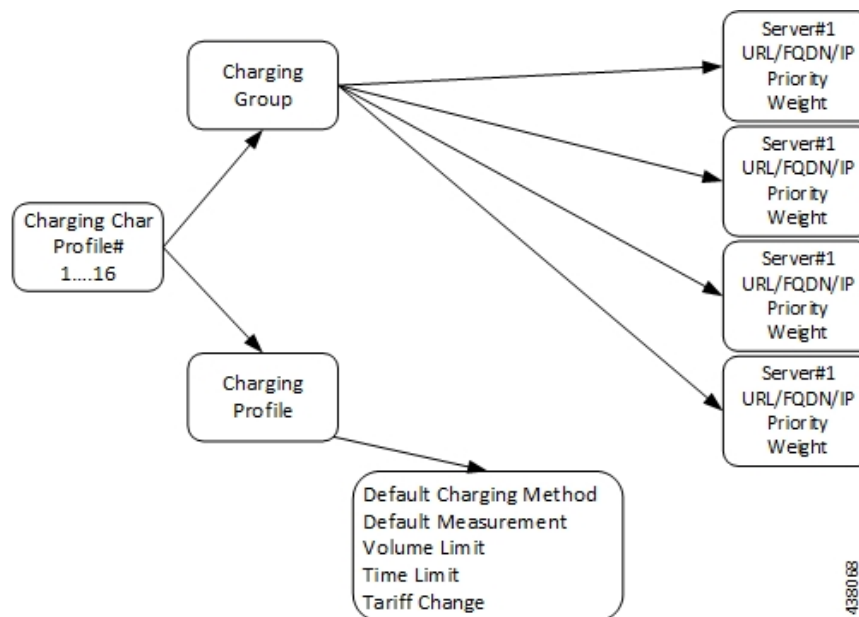
0x80 00 01 01 Offline

0x80 00 01 07 Online

## Local Configuration

The following figure illustrates how local configuration works.

**Figure 121: Local Configuration**



- Note**
1. The SMF supports up to 16 charging characteristic profiles.
  2. Each CC profile comprises of charging group and charging profile.
  3. The charging server group and charging profile are linked to the DNN profile. Currently, the charging profile supports configuration for trigger and thresholds.

## Zero Usage Report Suppression

The SMF relays the offline resource usage report from the UPF to the CHF if any of the following conditions is met:

- Reporting type is immediate.
- Reporting type is deferred and the maximum number of deferred reporting is crossed.

The usage report includes the charging records with zero value as well. These zero value records (UUC and CDR-U) occupy unnecessary disk space on the CHF. To avoid this issue, the SMF leverages new configuration to control the offline charging records with zero byte data count.

When you configure the **offline zero-usage** CLI command in the Charging Profile configuration mode, the SMF relays the usage to the CHF without any overload of UUC or CDR-U.

The users can select the UUC or CDRs they want to suppress based on the CLI configuration.



**Important**

The CDR release is never be suppressed even if the **offline zero-usage drop cdr** command is configured in the Charging Profile configuration mode.

For details on the configuration, see the [Configuring Zero Usage Report Suppression, on page 674](#) section.

## Call Flows

This section shows the following call flows:

### PDU Session Establishment

The following figure illustrates the call flow of PDU session establishment.

**Figure 122: PDU Session Establishment Call Flow**

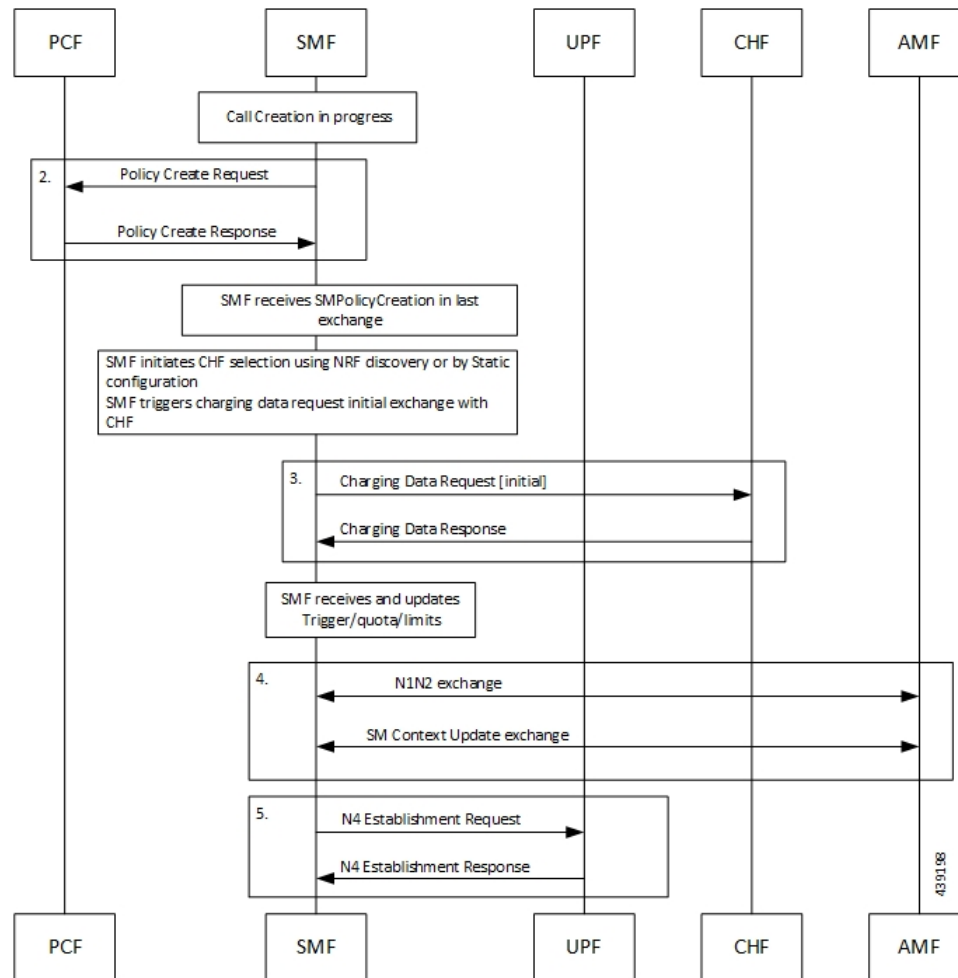


Table 192: PDU Session Establishment Call Flow Description

Step	Description
1.	Call creation starts at SMF.
2.	SMF performs a Policy Create exchange with PCF. In this exchange, the SMF can receive Charging Data that is associated to a PCC Rule. This Charging data indicates that charging is enabled for the session in progress.  PCF may enable Static or Predefined rules. These rules can be also enabled with charging, based on the configuration.
3.	After the charging is detected at SMF, SMF initiates a Charging Data Request Initial exchange with CHF. In this exchange SMF may receive the following information from CHF: <ul style="list-style-type: none"> <li>• CC triggers at session or RG level</li> <li>• Session level Time or Volume limits</li> <li>• Time or Volume limits at RG level</li> <li>• Quota at RG level</li> </ul>
4.	SMF sends the N1N2 Exchange and SM Context Update Exchange to AMF.
5.	SMF initiates N4 session establishment request exchange with UPF. In the same request, SMF relays the information related to charging in the Create URRs.

## Limitations

The SMF Charging feature has the following limitations on the N4 interface:

- If the session-level URR (CDR-i) is created once, it remains throughout the session. This URR is not deleted in the subsequent session (CDR-u).
- If the session-level URR is not created, then it is not created in the subsequent CDR-u even if session limits are available.

## Standards Compliance

The SMF Charging feature complies with the following standards:

- 3GPP TS 32.255
- 3GPP TS 32.290

## 3GPP June 2019 Compliance for Charging Interface

The SMF is compliant with the 3GPP June 2019 specification TS 32.290 version 15.3.0.

For the June release, the messages goes over the version "v2" as indicated in the following URI format:

```
nchf-convergedcharging/v2/chargingdata
```

The CLI command for compliance configuration is: **service nchf-convergedcharging**. If this CLI command or version is not configured, the default version from 3GPP December 2018 is applied.

With the 3GPP June 2019 compliance, the following information elements (IE) are added:

- Authorized QoS
- Subscribed QoS
- IEs in QoSData
- Serving Network Function ID

## Configuring SMF Charging

The SMF Charging involves the following configurations:

- DNN Profile Configuration
- Charging Characteristics Profile Configuration
- Charging Profile Configuration
- Zero Usage Report Suppression Configuration

### DNN Profile Configuration

Use the following configuration to configure a DNN profile for SMF Charging.

```
config
  profile dnn profile_name
    charging-profile profile_name
    network-element-profiles { amf | chf | pcf | udm } profile_name
  end
```

#### NOTES:

- **charging-profile**: Specifies the Charging Profile configuration.
- **network-element-profiles**: Specifies the network element profile. Network element profile can be one of the following:
  - **amf**: Specifies the AMF network element profile.
  - **chf**: Specifies the CHF network element profile.
  - **pcf**: Specifies the PCF network element profile.
  - **udm**: Specifies the UDM network element profile.
- *profile\_name*: Specifies the name of selected network element profile. After you select the network profile, enter a string.

### Charging Characteristics Profile Configuration

Use the following configuration to configure charging characteristics profile for SMF Charging.

```
config
  profile charging-characteristics cc_value
```

```
charging-profile profile_name
end
```

**NOTES:**

- *cc\_value*: Specifies the charging characteristics value, which is an integer from 1 to 16.

## Charging Profile Configuration

Use the following configuration to configure the charging profile parameters for SMF charging.

**config**

```
profile charging profile_name
  limit [ rating-group ] { duration duration_value | volume volume_value }
  max-charging-condition max_cc_value
  max-deferred-urr max_urr_value
  method { none | offline | online }

  quota request [ always | standard ]
  quota suppress triggers [ qht ]
  reporting-level { offline | online { [rating-group]
| rating-group | service-id }
  requested-service-unit time seconds volume downlink downlink_value
  uplink uplink_value total total_value
  tight-interworking-mode { false | true }
  triggers session session_level_triggers
end
```

**NOTES:**

- **limit**: Specifies the threshold limit.
- **duration**: Specifies the duration threshold for charging. The threshold value ranges from 0 through 2147483647.
- **volume**: Specifies the volume threshold for charging. The threshold value ranges from 0 through 9223372036854775807.
- **rating-group**: Specifies the volume and duration threshold for a Rating Group.
- **max-charging-condition** *max\_cc\_value*: Specifies the maximum number of changes to the charging condition. *max\_cc\_value* must be an integer ranging from 0 through 500. The default value is 20.
- **max-deferred-urr** *max\_urr\_value*: Specifies the maximum number of deferred USU containers. *max\_urr\_value* must be an integer ranging from 0 through 200. The default value is 50.
- **method**: Specifies the charging method. The default charging method is offline.
- **quota request** [ **always** | **standard** ]: Controls the requesting of quota from the CHF for online charging services based on the configuration. If the **quota request always** is configured, the SMF always requests for quota. If the **no quota request** or **quota request standard** CLI command is configured, then the SMF requests the quota for specific trigger types as defined in standard, which is the default behaviour.
- **quota suppress triggers** [ **qht** ]: Suppresses the quota from the CHF upon configuring the usage report trigger type "qht".
- **reporting-level**: Specifies the reporting level configuration to be used for offline and online charging.

The default value is [rating-group] level.

- **requested-service-unit**: Configures the value for the requested service units.
  - **time seconds**: Configures the time quota value in seconds from 1 through 4000000000.
  - **downlink downlink\_value**: Configures the downlink volume in bytes from 1 through 4000000000.
  - **uplink uplink\_value**: Configures the uplink volume in bytes from 1 through 4000000000.
  - **total total\_value**: Configures the total volume in bytes from 1 through 4000000000.
- **tight-interworking-mode**: Configuration to enable tight interworking mode for online or offline charging methods.
- **triggers**: Specifies the list of triggers to be configured.
- **session session\_level\_triggers**: Specifies the list for Session Level Triggers. The list of Session Level Triggers is as follows:
  - **repor3gpp-ps-change**
  - **ambr-change**
  - **max-number-of-changes-in-charging-conditions**
  - **plmn-change**
  - **qos-change**
  - **rat-change**
  - **serv-node-change**
  - **tarrif-time-change**
  - **ue-pra-change**
  - **ue-time-change**
  - **upf-add**
  - **upf-rem**
  - **user-loc-change**

The following is a sample configuration for SMF Charging:

```
config
  charging-server chl
    fqdn abc.com
    capacity 10 (default : 10)
    priority 1 (default: 1)
    ip-address 127.0.0.1
    port 1234
    !
  !
  dnn-profile dnn1
    charging-server-name [ chserv1 ]
    charging-profile chProf1
    !
  profile charging chl
```

```

limit volume tot 2000
limit duration 20
limit rating-group volume tot 4000
limit rating-group duration 40
triggers session [ ambr-change qos-change]
max-charging-condition 20
max-deferred-urr 100
reporting-level service-id
requested-service-unit time 20 volume downlink 8000 uplink 2000 total 10000
!
profile charging-characteristics 1
charging-profile chl
!
```

## Configuring Zero Usage Report Suppression

Use the following configuration to enable the zero usage report suppression feature.

```

config
  profile charging ChargingProfile_name
    offline zero-usage [ drop { cdr | uuc } | measurement { duration |
volume } | trigger { external | final | internal } ]
  end
```

### NOTES:

- **offline zero-usage**: The SMF suppresses the offline URR with zero volume and duration. By default, the zero usage drop configuration is disabled on SMF.
- **drop { cdr | uuc }**: The SMF suppresses the CDR or UUC with zero usage. If there are multiple reports, then the SMF drops only the reports with zero usage. Note that there is no impact on the online reporting. If the **drop** command is not configured, the SMF stops sending UUC for the offline usage report.
- **measurement { duration | volume }**: The SMF specifies the measurement method of the network usage for suppression. The measurement method is based on volume and duration. If the **measurement** command is not configured, the SMF suppresses the records with both zero volume and zero duration, or the records with zero volume or zero duration depending on the configuration.
- **trigger { external | final | internal }**: Specifies the list of triggers to be suppressed.
  - **external**: The SMF suppresses the usage reports that are generated due to external triggers such as QoS Change, RAT change, User Location change, and PLMN Change.
  - **final**: The SMF suppresses the usage reports that are generated at the end of a context.
  - **internal**: The SMF suppresses the usage reports that are generated due to internal triggers such as volume limit, time limit, and tariff change.

## Static PCC Rules Configuration

For information on Configuring Static PCC Rules for Charging, refer to *Configuring the Static PCC Rules Support on SMF* section in the *Policy and User Plane Management* chapter.

The following is an example Static PCC Rule configuration:

```

configure
```



```

active-charging service acs
  credit-control group 1
    diameter ignore-service-id true
    pending-traffic-treatment forced-reauth drop
    pending-traffic-treatment noquota pass
    quota holding-time 10
    usage-reporting quotas-to-report based-on-grant report-only-granted-volume
  exit
  urr-list urrlocal
    rating-group 320011 service-identifier 10 urr-id 1
  charging-action ca95
    billing-action egcdr
    cca charging credit
    content-id          320011
    service-identifier 10
  exit
  charging-action test
    cca charging credit preemptively-request //This is not in scope of current release
  exit
  rulebase rb1
    action priority 10 ruledef rd95 charging-action ca95
    action priority 11 dynamic-only ruledef rd93 charging-action ca93
  exit

gtp group group1
  gtp egcdr service-data-flow threshold interval 1234
  gtp egcdr service-data-flow threshold volume downlink 13000
  gtp egcdr service-data-flow threshold volume uplink 17000
  gtp egcdr service-data-flow threshold volume total 22222
  exit

```

# Mapping of Charging Scenario on Various Interfaces

## Feature Description

The SMF supports charging on the N7, N40, and N4 interfaces. Based on the charging data information that SMF receives, it provides reporting level support for online and offline charging. The behavior of SMF changes according to the messages received on the N7, N4, and N40 interfaces.

## How it Works

The SMF provides the different reporting levels for online and offline charging with the following rules:

- Configured rules are derived from the static or predefined charging actions.
- Session-level Usage Reporting Rule (URR) is derived from CHF trigger or local configuration.
- The SMF does not associate session-level URR for online and offline method charging description.
- The SMF does not associate session-level URR to the configured charging-action URRs.
- Rulebase URR is applicable only for the offline configured URR.
- For the configured online or online-offline charging method, if Ignore Service ID configuration exists, the URR list must contain "rg x urr-id y". Else, the SMF drops the charging actions as malformed.

**Important**

The SMF supports multiple charging methods within the same rating group.

**Charging Mapping**

The N7 interface uses Charging Data from PCC rules or local configuration, N4 interface uses URR or Packet Detection Rule (PDR), and N40 interface uses Used Unit Container (UUC).

The SMF charging mapping on N7, N4, and N40 interfaces with various charging methods is described as follows.

*Offline Method When Charging Data is Derived from One PCC Rule*

Reporting level: Rating Group level or Service ID level

N4 interface:

- First URR is derived from the first Charging Data. Charging data limits from rating group trigger or local configuration.
- Second URR is derived from Session Limit, which is CHF or local configuration.
- Second URR is linked to the first URR.
- First PDR is derived from the first PCC rule.
- First and second URRs are linked to the first PDR.

N40 interface:

- First UUC is derived from the usage report of the first URR.
- First UUC may or may not have a service identifier.

**Note**

- Session-level URR is not associated to the configured URRs.
- If configured, rulebase URR replaces session-level URR.
- If configured and rulebase URR exists, it is linked to the first URR.

*Online Method When Charging Data is Derived from One PCC Rule*

Reporting level: Service ID level or Rating Group level

N4 interface:

- First URR is derived from the first Charging Data, which is threshold or quota from rating group granted-unit.
- Second URR is derived from Session Limit, which is CHF or local configuration.
- Second URR is linked to the first URR.
- First PDR is derived from the first PCC rule.

- First and second URRs are linked to the first PDR.

N40 interface:

- First UUC is derived from the usage report of the first URR.
- First UUC may or may not have a service identifier.

**Note**

- Session-level URR is not associated to the configured URRs.

### *Offline Method When Charging Data is Derived from Two PCC Rules*

Reporting level: Service ID level

N4 interface:

- First URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA.
- Second URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA.
- Third URR is derived from rating group level, which limits from Rating-Group trigger or local configuration.
- Fourth URR is derived from Session Limit, which is CHF or local configuration.
- The third and fourth URRs are linked to the first and second URRs.
- First PDR is derived from first PCC rule.
- Second PDR is derived from second PCC rule.
- First, third, and fourth URRs are linked to the first PDR.
- Second, third, and fourth URRs are linked to the second PDR.

N40 interface:

- First UUC is derived from the usage report of the first URR.
- Second UUC is derived from the usage report of the second URR.
- Both the first and the second UUCs have a service identifier.

**Note**

- Session-level URR is not associated to the configured URRs.
- If configured, rulebase URR is linked to the first and second URRs.

### *Online Method When Charging Data is Derived from Two PCC Rules*

Reporting level: Service ID level

N4 interface:

- First URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA.
- Second URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA.
- Third URR is derived from rating group level, which is threshold or quota from the rating group granted unit.
- Fourth URR is derived from Session Limit, which is CHF or local configuration.
- Third and fourth URRs are linked to the second and fourth URRs.
- First PDR is derived from the first PCC rule.
- Second PDR is derived from the second PCC rule.
- First, third, and fourth URRs are linked to the first PDR.
- Second, third, and fourth URRs are linked to the second PDR.

N40 interface:

- First UUC is derived from usage report of the first URR.
- Second UUC is derived from the usage report of the second URR.
- Both the first and the second UUCs have a service identifier.




---

**Note**

- Session-level URR is not associated to the configured URRs.
  - If Ignore Service ID is configured, this method is not valid.
- 

### *Offline-Online Method When Charging Data is Derived from One PCC Rule*

Reporting level: Service ID level or Rating Group level

N4 interface:

- Offline URR is derived from the first Charging Data, which limits rating group trigger or local configuration.
- Online URR is derived from the first Charging Data, which limits from the granted unit.
- First PDR is derived from the first PCC rule.
- Offline and online URRs are linked to the first PDR.

N40 interface:

- First UUC is derived from the usage report of the offline URR.
- Second UUC is derived from the usage report of the online URR.

### *Offline-Online Method When Charging Data is Derived from Two PCC Rules*

Reporting level: Service ID level

N4 interface:

- First offline URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR\_Off3.
  - Second offline URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR\_Off3.
  - Third offline URR is the rating group level, which limits the rating group trigger or local configuration.
- First online URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR\_Online3.
- Second online URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR\_Online3.
- Third online URR is the rating group level, which limits from the granted unit.
- First PDR is derived from the first PCC rule.
- Second PDR is derived from the second PCC rule.
- First offline URR, first online URR, third offline URR, and third online URR are linked to the first PDR.
- Second offline URR, third online URR, third offline URR, and third online URR are linked to the second PDR.

N40 interface:

- First UUC is derived from the usage report of the first offline URR and has a service identifier.
- Second UUC is derived from the usage report of the second offline URR and has a service identifier.
- Third UUC is derived from the usage report of the first online URR and has a service identifier.
- Fourth UUC is derived from the usage report of the second online URR and has a service identifier.

### *Offline-Online Method When Charging Data is Derived from One PCC Rule with No Service Identifier*

The offline and online reporting levels are at Service ID and Rating Group levels respectively.

Prerequisite: No Reporting Level from PCF

- CLI:
  - Tight interworking mode
  - Ignore Service Identifier
  - Offline Reporting: Service Identifier
  - Online Reporting: Rating Group



- 
- Note**
- The SMF ignores the volume or time limit trigger from CHF at the rating group level.
  - Session-level URR is not associated to URRs that are derived from the first Charging Data.
- 

N4 interface:

- Offline URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR\_Online.
- Online URR is derived from the first Charging Data, which limits from the granted unit.
- First PDR is derived from the first PCC rule.
- Online URR and offline URR are linked to the first PDR.

N40 interface:

- First UUC is derived from the usage report of the offline URR and has a service identifier.
- Second UUC is derived from the usage report of the online URR and does not have a service identifier.



- 
- Note**
- Session-level URR is not associated to the configured URRs.
  - If URR is configured, URR rulebase is derived from egcdr and is linked to both the offline and the online URRs.
- 

#### *Offline-Online Method When Charging Data is Derived from Two PCC Rules with No Service Identifier*

The offline and online reporting levels are at Service ID and Rating Group levels respectively.

Prerequisite: No Reporting Level from PCF

- CLI:
  - Tight interworking mode
  - Ignore Service Identifier
  - Offline Reporting: Service Identifier
  - Online Reporting: Rating Group



- 
- Note**
- The SMF ignores the volume or time limit trigger from CHF at the rating group level.
  - Session-level URR is not associated to URRs that are derived from the first Charging Data.
- 

N4 interface:

- First offline URR is derived from the first Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR\_Online.
- Second online URR is derived from the second Charging Data. Charging data has no limit and the rating trigger must be LIUSA. Charging data has the linked URR ID as URR\_Online.
- URR\_Online is derived from the second Charging Data, which limits from the granted unit.
- First PDR is derived from the first PCC rule.
- Second PDR is derived from the second PCC rule.
- First offline URR and URR\_Online are linked to the first PDR.
- Second offline URR and URR\_Online are linked to the second PDR.

N40 interface:

- First UUC is derived from the usage report of the first offline URR and has a service identifier.
- Second UUC is derived from the usage report of the second offline URR and has a service identifier.
- Third UUC is derived from the usage report of the URR\_Online and does not have a service identifier.



**Note**

- Session-level URR is not associated to the configured URRs.
- If URR is configured, URR rulebase is derived from egcdr and is linked to both the first and second offline URRs along with URR\_Online.

## Limitations

This feature has the following limitations:

- Same rating group is not supported for multiple Charging-action of rulebase and Dynamic Charg-Desc.
- Tight interworking mode is not supported for the service which is at the rating group level.
- One service at the rating group level and another service at service ID level are not supported.

## Standards Compliance

The Different Reporting Level Support for Online and Offline Charging feature complies with the following standards:

- 3GPP TS 32.255
- 3GPP TS 32.290

## Error Handling Scenarios

This section describes the different handling scenarios associated with the errors that occur during SMF charging.

## Application Error and Result Code Handling

SMF supports the application error codes from CHF at command level as defined in 3GPP TS 32.291 specification, version 15.3.0, section 6.1.7.3. The SMF also supports RG-level result codes as defined in 3GPP 32.291 specification, version 15.3.0 section 6.1.6.3.14.

The following labels are defined in the "chf\_appl\_err\_stats" counter to indicate the CHF response failures at the application level.

- http2\_err\_code—Includes the following values:
  - 403
  - 400
  - 404
- appl\_err\_code—Includes the following values:
  - END\_USER\_REQUEST\_REJECTED
  - END\_USER\_SERVICE\_DENIED
  - QUOTA\_LIMIT\_REACHED
  - CHARGING\_NOT\_APPLICABLE
- appl\_err\_action—Includes the following values:
  - drop\_traffic
  - disable\_charging
  - terminate
- appl\_err\_exchg\_type—Includes the following values:
  - initial
  - update

### Application Error Codes

The following table provides details of the application error codes with the corresponding SMF action.

Application Error /Session Level	HTTP2 Code	SMF Action	CHF Expected Actions	Limitations
CHARGING_FAILED	400	Terminate	None	None
RE_AUTHORIZATION_FAILED	400	None	Take corrective action	-
CHARGING_NOT_APPLICABLE	403	Continue subscriber session without Charging (no offline charging as well)	None	None



Application Error /Session Level	HTTP2 Code	SMF Action	CHF Expected Actions	Limitations
USER_UNKNOWN	404	Terminate	None	None
END_USER REQUEST_DENIED	403	Terminate	None	None
QUOTA_LIMIT_REACHED	403	Drop traffic for the online services. Offline services are not impacted.	CHF sends notify (RAR) after this condition is recovered for the session	

**Note**

- The error code 403 is not configured in the failure handling template.
- CHARGING\_NOT\_APPLICABLE (Disable charging) for static and predefined rules, occurs when a proprietary IE “Charging Disabled” in subscriber params is sent in the N4 modification or establishment request. This request is sent to prevent UPF from generating Start of Traffic for the URRs pending for activation.

## RG-level Result Codes

The following table provides details of the result code with the corresponding SMF action.

RG-level Result code	HTTP Status Code	SMF Behaviour	CHF Expected Behaviour	Limitations
RATING_FAILED	200	Drop traffic corresponding to the rating group	None	None
QUOTA_MANAGEMENT_NOT_APPLICABLE	200	Convert to offline	None	None
USER_UNKNOWN	200	Ignored (supported only at session level)	Not expected from CHF	None
END_USER SERVICE_DENIED	200	Drop traffic corresponding to the rating group	CHF sends notify (RAR) after this condition is recovered for the rating group.	Traffic will be dropped for offline service as well for online or offline services.

RG-level Result code	HTTP Status Code	SMF Behaviour	CHF Expected Behaviour	Limitations
QUOTA_LIMIT_REACHED	200	Drop traffic corresponding to the rating group	CHF sends notify (RAR) after this condition is recovered for the session	None
END_USER SERVICE_REJECTED	200	Drop traffic corresponding to the rating group	CHF sends notify (RAR) after this condition is recovered for the session	None

## CHF Server Reconciliation

The SMF falls back to the first available offline CHF server when the NF selected by NRF discovery is unreachable. The CHF Reconciliation feature includes deleting the existing subscribers that are associated to a set of offline NFs, and the subscribers that are in offline fallback mode.

The CHF server reconciliation works when one of the following two conditions is met:

1. If the NRF detects that an offline CHF server is active.
2. If the RAR is received from the CHF server on an offline converted session.

For the second condition, the session gets deleted directly. With the NRF discovery, this feature involves the following steps:

1. SMF subscribes for the notification of NF instance IDs from NRF through NF\_LIB component of Rest-ep.
2. If the NF discovery query determines that all the NFs are down, the NF\_LIB component treats these set of NFs as offline. If any one of the NFs is available again, the NRF triggers notification for the same to the SMF.
3. The SMF performs NRF discovery after re-validation timer. If the NRF detects any new NF, the SMF receives the corresponding notification from the NRF.
4. When the SMF identifies that an NF is online with all the required NF discovery query parameters, then the SMF initiates the CHF server reconciliation.

The following labels are introduced as part of this feature:

- `disc_pdu_rel_chf_reconciliation`: This label is defined under `SMF_DISCONNECT_STATS` to show the reason of disconnection.
- `chf_reconl_pdu_sess_rel`: This label is defined under `smf_service_stats` metric to show the number of times the PDU session release procedure is initiated.

# Dynamic Configuration Change Support

## Feature Description

The Dynamic Configuration Change Support feature allows SMF to dynamically handle the configuration changes of the charging parameters while minimizing the configuration errors. The existing and new SMF Charging parameters allow implementation of the dynamic configuration updates. This feature supports the following charging configurations:

- Active Charging Service (ACS) Profile
  - Rulebase
  - Ruledef
  - Charging-Action
  - Credit-Control-group
- Charging Profile
- Charging Characteristics
- GTPP Group
- Upf-Apn Configuration Group

## How it Works

This section describes how dynamic change in configuration works for the supported Failure Handling Profile and Charging Profile configuration.

### ACS Profile

The SMF supports dynamic change in the ACS configuration during the run time. The ACS Profile configuration defines various parameters for the ACS profile.

The following table lists the SMF and UPF behavioral changes during the dynamic update of ACS configuration in different scenarios.

**Table 193: ACS Profile Configurations and its Impact during Dynamic Update**

Configuration	Config Applied on both SMF and UPF	Config Applied only on SMF	Config Applied only on UPF
Rulebase addition	<p><b>Existing Session:</b> Continue to use the current rulebase value</p> <p><b>New Session:</b> No impact for the new session</p>	<p><b>Existing Session:</b> Change in the rulebase gets rejected at UPF</p> <p><b>New Session:</b> Session creation fails at UPF for this rulebase</p>	<p><b>Existing Session:</b> Change in the rulebase gets rejected at SMF</p> <p><b>New Session:</b> Session creation fails at SMF for this rulebase</p>

Rulebase removal	<p><b>Existing Session:</b> Not allowed without node drain</p> <p><b>New Session:</b> No impact for the new session</p>	<p><b>Existing Session:</b> Not allowed without node drain</p> <p>After the configuration change, the rulebase configuration remains stale on SMF if the rulebase removal on UPF is missed</p> <p><b>New Session:</b> No impact for the new session</p>	<p><b>Existing Session:</b> Not allowed without node drain</p> <p>After the configuration change, the rulebase configuration remains stale on UPF if the rulebase removal on SMF is missed</p> <p><b>New Session:</b> No impact for the new session</p>
Ruledef addition	<p><b>Existing Session:</b> Activates the new rule successfully</p> <p><b>New Session:</b> No impact for the new session</p>	<p><b>Existing Session - Static Rule:</b> The UPF neither activates the rule nor sends the report for this rule.</p> <p><b>Existing Session - Predefined Rule:</b> Fails to activate the new rule until the UPF receives it.</p> <p><b>New Session:</b> Same as the existing session</p>	<p><b>Existing Session - Static Rule:</b> The UPF activates this rule and reports the usage. The SMF has the charging data for this RG+ServID. It creates dummy ChrgParam and associates URR to it.</p> <p><b>Existing Session - Predefined Rule:</b> Fails to activate the new rule until the SMF receives it</p> <p><b>New Session:</b> Same as the existing session</p>
Ruledef deletion	<p><b>Existing Session:</b> The current flows remain as is. If the flow is not created, it will never be created for this session. The SMF or UPF does not remove the associated charging.</p> <p><b>New Session:</b> No impact for the new session</p>	<p><b>Existing Session - Predefined rule :</b> The SMF rejects this rule creation.</p> <p><b>Static and Activated Predefined Rules:</b> Existing flows remain as is. The SMF or UPF does not remove the associated charging. The received usage is reported successfully.</p> <p>If the SMF has not received the first usage report and when the first report arrives, the SMF creates chrgParam/Urr context from RG+ServID.</p> <p><b>New Session:</b> Same as the existing session</p>	<p><b>Existing Session - Predefined rule:</b> The SMF continues to allow this rule creation but fails at the UPF.</p> <p><b>Static and Activated Predefined Rules:</b> The UPF continues with the created URR for these flows. The SMF reports the usage without any issue.</p> <p><b>New Session:</b> Same as the existing session</p>

Charging Action addition with new RG/Svc Id (With addition of new rules associated to that CA)	<p><b>Existing Session - Static Rule:</b> The SMF creates charging entry for this RG when the first URR is received.</p> <p><b>Existing Session - Predefined Rule:</b> The SMF activates the rule based on the PCF trigger.</p> <p><b>New Session:</b> No impact for the new session</p>	<p><b>Existing Session - Static Rule:</b> The UPF does not activate this flow. The SMF never receives the usage.</p> <p><b>Existing Session - Predefined Rule:</b> The UPF fails to install predefined rule due to the unavailability of ruledef info.</p> <p><b>New Session:</b> Same as the existing session</p>	<p><b>Existing Session - Static Rule:</b> The UPF activates this flow. The SMF creates the charging entry for this RG when the first URR is received.</p> <p>In this case, the SMF does not find Charging-action with this RG+ServID. It creates dummy ChrgParam with the received RG+ServID.</p> <p><b>Existing Session - Predefined Rule:</b> Same as mentioned for the static rule.</p> <p><b>New Session:</b> Same as the existing session</p>
Charging action (and associated rules) removal	<p><b>Existing Session - Static Rules:</b> The SMF and UPF continue with the current flow and report any URRs for this RG.</p> <p><b>Predefined Rules:</b></p> <p>The SMF and UPF continue with the current flow and report any URRs for this RG. Once the rule is deactivated, it will not be activated again.</p> <p><b>New Session:</b> No impact for the new session</p>	<p><b>Existing Session - Static Rules:</b> The SMF and UPF continue with the current flow and report any URRs for this RG.</p> <p><b>Predefined Rules:</b></p> <p>The SMF and UPF continue with the current flow and report any URRs for this RG. Once the rule is deactivated, it will not be activated again.</p> <p><b>New Session:</b> Same as the existing session</p>	<p><b>Existing Session - Static Rules:</b> The SMF and UPF continue with the current flow and report any URRs for this RG.</p> <p><b>Predefined Rules:</b></p> <p>The SMF and UPF continue with the current flow and report any URRs for this RG. Once the rule is deactivated, it will not be activated again.</p> <p><b>New Session:</b> Same as the existing session</p>
RG/Svc Id, Online/Offline Config changed within CA	<p><b>Static Rules and Already Active Predefined Rules:</b> The UPF creates new URRs and reports them. The SMF reconciles from URR ID table and creates charging data for these URRs as and when reported.</p> <p><b>Post config change activation of predefined rules:</b> No issues. Both SMF and UPF are in sync.</p> <p><b>New Session:</b> No impact for the new session</p>	<p><b>Static Rules and Already Active Predefined Rules:</b> The UPF continues reporting with old URR ID and the SMF continues to report it without any issue.</p> <p><b>Post config change activation of predefined rules:</b> Same as Static Rules</p> <p><b>New Session:</b> The UPF rejects the establishment request if the predefined rules are activated during session establishment.</p>	<p><b>Static Rules and Already Active Predefined Rules:</b> The UPF creates new URRs and reports them. The SMF reconciles from URR ID table and creates dummy chrgParam and associates URR to it.</p> <p><b>Post config change activation of predefined rules:</b> Same as Static Rules</p> <p><b>New Session:</b> The UPF rejects the establishment request if the predefined rules are activated during session establishment.</p>

URR Id table entry addition (New RG addition)	No action needed on SMF	No action needed on SMF	The UPF creates URR.
URR Id table entry removal	No impact	No impact	The UPF creates URR. The removal has no impact on the created URR.
URR Id table entry modification	No impact	No impact	The UPF creates URR. Removal has no impact on the created URR.  If the same URR-id is allocated to different RG+ServID, the removal impacts the URR. The UPF fails to create new URR for the new RG+ServId.

**NOTES:**

- If the online report includes service id and the ignore-service-id is not configured in credit control profile, the SMF drops the report.
- If the new online URR contains the same RG as an existing URR, then the SMF drops the usage report.
- If the new offline URR contains the same RG+service ID as an existing URR, the SMF drops the usage report.
- In the same usage report, if the next online URRs include the same RG and the next offline URRs include with the same RG + service ID, the SMF drops the usage report.

## Charging Profile

The Charging Profile supports dynamically updating the configuration based on the values that you pass during the runtime. The refresh operation of the values takes place considering the following scenarios:

- **Configuration reflects in the next encounter to access:** If the values are updated while an operation is in-progress, the SMF ignores the new values and continues to use the old values. For example, Limits in Charg-Profile and CC triggers.
- **Configuration reflects only on a new session:** If the configuration is specific to a session and the session has already considered the values, then the SMF does not consider the new values. For example, PduContext (DB entry). This case indicates that any update to the configuration does not impact the sessions that are already created. For instance, Charging Method in Profile or Charg-Profile in Charging Characteristics.
- **Configuration reflects instantly:** Configurations immediately consider the dynamic values whenever they are updated. If SMF has already used a configuration and it is later updated, then it uses the latest values.

If a session is created using a Charging Profile, which later gets deleted from the Ops Center, the session might attempt to access the configuration structure of the deleted profile. In such cases, the Smf-Service pod maintains a default profile mapped to the sessions whose profiles are missing.

The Charging Profile is responsible for handling the SMF charging parameters.

The following table lists the configuration parameters with the dynamic configuration change and its impact on the existing sessions.

**Table 194: Charging Profile Parameters**

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
limit rating-group duration	Allowed	New values are used during the new URR creation or the subsequent URR update for the existing sessions <b>Note</b> The dynamic configuration does not initiate a URR update.
max-charging-condition	Allowed	No impact
max-deferred-urr	Allowed	No impact
metering-method	Allowed	New values are used during the new URR creation for the existing sessions
method	Allowed	No impact
reporting-level	Allowed	No impact
requested-service-unit time	Allowed	No impact
tight-interworking-mode	Allowed	No impact <b>Note</b> In 2021.01.0 and later releases, the <b>tight-interworking-mode</b> CLI command is obsolete
triggers session	Allowed	No impact
Request Quota	Allowed	No impact

### Charging-Characteristics Profile

The Charging-Characteristics Profile configuration defines the various parameters for managing the charging characteristics for SMF Charging.

The following table illustrates if the configuration parameters allow dynamic configuration change.

**Table 195: Charging-Characteristics Profile Parameters**

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
charging-profile	Not Allowed	The configuration is used only once while setting up the session.

## Charging-Action Profile

The Charging-Action Profile configuration defines the QoS and charging related parameters associated with the rule definitions.

The following table illustrates if configuration parameters allow dynamic configuration change.

**Table 196: Charging-Action Profile Parameters**

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Rating group and Service ID	Allowed	No impact

## Credit-Control-Group Profile

The Credit-Control-Group configuration defines the parameters to be used for subscribers who use the mapped rulebase.

The following table illustrates if configuration parameters allow dynamic configuration change.

**Table 197: Credit-Control-Group Profile Parameters**

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Ignore Service ID	Allowed	No impact

## Rulebase Profile

The Rulebase configuration parameters define the protocol rules to match a flow and the associated actions to be taken for the matching flow.

The following table illustrates if configuration parameters allow dynamic configuration change.

**Table 198: Rulebase Profile Parameters**

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Ruledef association to Charging-action	Allowed	No impact
Credit-Control-Group	Allowed	The configuration is used only once while setting up the session

## GTPP Group Profile

The GTPP Group Profile configuration specifies the parameters for creating the GTPP group.

The following table illustrates if configuration parameters allow dynamic configuration change.

**Table 199: GTPP Group Profile Parameters**

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Limits for offline configured urrs	Allowed	New values are used during the new URR creation for the existing sessions.



### Upf-Apn Configuration Profile

The Upf-Apn Configuration Profile configuration defines the various parameters for the Upf-Apn profile. The following table illustrates if configuration parameters allow dynamic configuration change.

*Table 200: Upf-Apn Configuration Profile Parameters*

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Association of gtp Group	Allowed	The configuration is used only once while setting up the session.

### Network Profile for Peer CHF

The network profile for peer CHF configuration defines the various network configurations. The following table illustrates if configuration parameters allow dynamic configuration change.

*Table 201: Network Profile for Peer CHF Parameters*

Configuration Parameters	Dynamic Change	Impact on Existing Sessions
Set of CHFs configured	Allowed	No impact





## CHAPTER 42

# SMF Deregistration with NRF

- [Feature Summary and Revision History, on page 693](#)
- [Feature Description, on page 693](#)
- [How it Works, on page 694](#)

## Feature Summary and Revision History

### Summary Data

*Table 202: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 203: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

The SMF supports the deregistration of Network Function (NF) Repository Function (NRF), wherein the NF deregister service operation of the SMF removes the profile of a network function that is registered in the NRF.

The SMF starts the NF deregister service operation in the following scenarios:

- When the Service Based Interface (SBI) endpoint is not configured and all the rest endpoints stop functioning.
- When all the configured SBI endpoints VIP IP and N11 VIP IPs are offline.

## How it Works

The NF deregister service operation deletes the specific resource based on its NF instance ID. The NF deregistration starts when the Uniform Resource Identifier (URI) receives a request to delete a specific NF instance.

The recommended SMF shutdown process involves the following steps:

1. All N11 and SBI VIP IPs are marked as offline. After these endpoints appear offline, the NF deregistration request is sent to the NRF. The NRF notifies the peer NFs, such as AMF, about the SMF shutdown and its unavailability for traffic.
2. Wait for a grace period to allow convergence and perform a "system mode shutdown" to stop all the pods.

When the endpoint SBI is not configured, the system deletes the rest-ep pod immediately and avoids proper convergence. Implementing the system mode shutdown without taking the SBI and N11 VIP IPs offline also avoids convergence.

## Call Flows

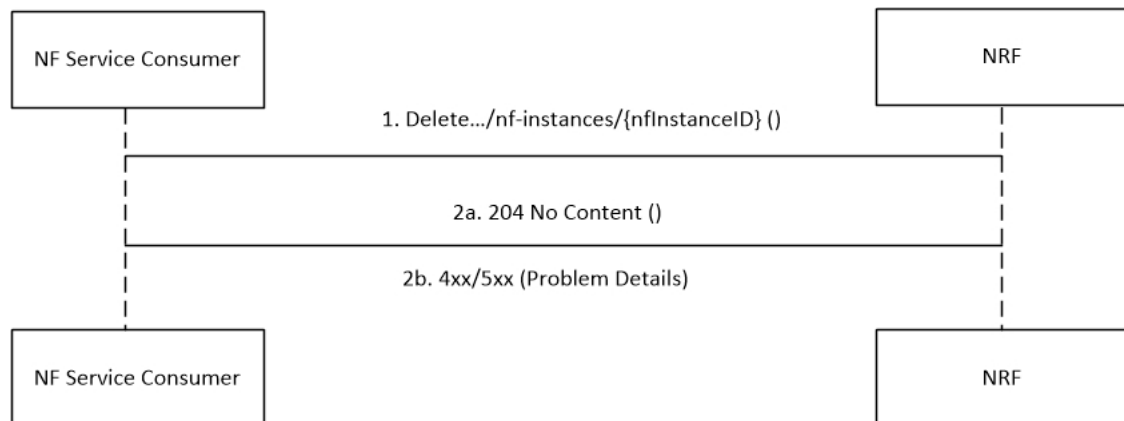
This section describes the following call flows:

- NRF deregistration call flow
- NRF deregistration trigger events call flow

### NF Deregistration Call Flow

This section describes the NF deregistration call flow.

**Figure 123: NRF Deregistration Call Flow**



440474

Table 204: NRF Deregistration Call Flow Description

Step	Description
1	The NF Service Consumer sends a Delete request to the resource URI that indicates the NF instance. The request body is empty.
2a	If the deletion of the specified resource is successful, the “204 No Content” message appears. The response body remains empty.
2b	If the NF instance, which is identified with the NF instance ID, does not exist in the list of registered NF instances in the NRF database, the NRF sends the “404 Not Found” status code with the problem details.

## NF Deregistration Trigger Events Call Flow

This section describes the NF deregistration trigger events call flow.

Figure 124: NF Deregistration Trigger Events Call Flow

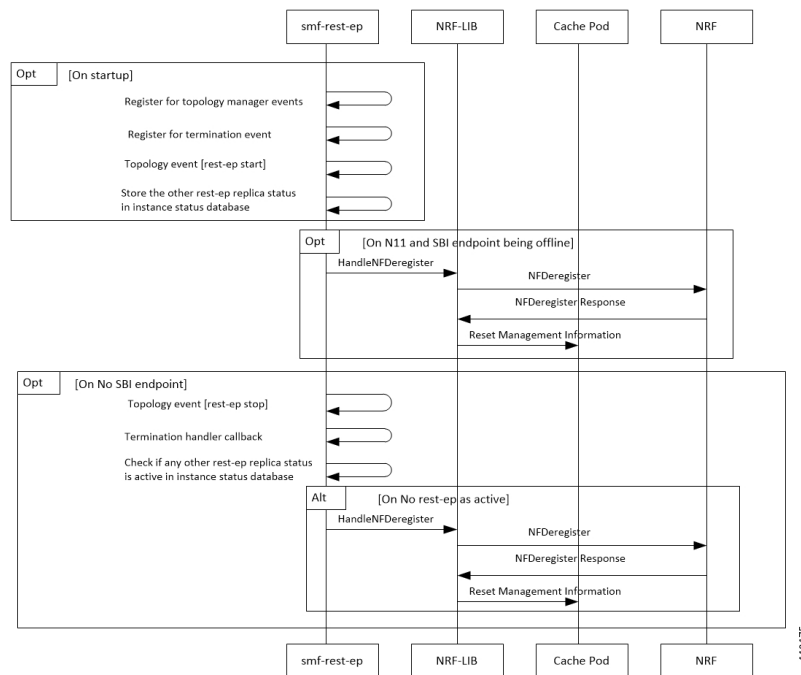


Table 205: NF Deregistration Trigger Events Call Flow Description

Step	Description
On startup	
1	The SMF rest-ep registers for topology manager events to identify the state of other rest-ep instances and keeps a track of these instances in an instance state database.
2	The SMF rest-ep registers for the termination handler with the application infrastructure for receiving notification when the application infrastructure stops functioning. As part of the termination handler, the SMF rest-ep monitors the instance state database for any other working rest-ep.

Step	Description
3	The SMF rest-ep starts the topology event.
4	The SMF rest-ep saves the status of other rest-ep replicas in the instance state database.
When the N11 and SBI endpoints are offline	
5	The SMF rest-ep sends the Handle NF deregister message to the NRF-Lib.
6	When all the SBI and N11 VIP IP endpoints are offline, the SMF rest-ep sends the deregistration request to the NRF.
7	The NRF sends the NF deregister response to the NRF-Lib.
8	The NRF-Lib resets all the management information that is configured in the cache pod.
When no SBI endpoint exists	
9	The SMF rest-ep starts the topology event to stop the other rest-ep.
10	The SMF rest-ep starts the termination handler callback.
11	The SMF rest-ep checks the instance status database for any other working rest-ep.
When no rest-ep is functional	
12	The SMF rest-ep sends the Handle NF deregister message to the NRF-Lib.
13	The SMF rest-ep sends the deregistration request to the NRF.
14	The NRF sends the NF deregistration response to the NRF-Lib.
15	The NRF-Lib resets all the management information that is configured in the cache pod.

## Standards Compliance

The SMF deregistration with NRF feature complies with the *3GPP TS 29.510 V15.2.0 (2018-12)*.

## Limitations

The SMF deregistration with NRF feature has the following limitation:

- When N11 and SBI VIP IPs are not marked offline, the NF deregistration is not sent for the system mode shutdown because there is no specific order for pod deletion. Also, no monitoring procedure exists to check if the rest-ep pods are working.



# CHAPTER 43

## SMF Overload Management

This chapter describes the SMF load and overload control functionality as defined by 3GPP load and overload specifications of the respective interfaces.

- [Feature Summary and Revision History, on page 697](#)
- [Feature Overview, on page 698](#)
- [SBA Interface Overload Control, on page 698](#)

### Feature Summary and Revision History

#### Summary Data

*Table 206: Summary Data*

Applicable Products or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 207: Revision History*

Revision Details	Release
Added support for message priority configuration.	2020.04.0
First introduced.	2020.03.0

# Feature Overview

The SMF provides mechanisms to manage the overload and congestion that occur on the SMF and Service-based Architecture (SBA). The SMF receives ingress messages at a rate higher than the engineered capacity. The internal queues on the SMF might experience higher utilization level than configured. The same might happen on the SBA servers, directly or indirectly resulting from the overloaded traffic from the network or from the SMF.

## SBA Interface Overload Control

### Feature Description

An interface can handle only a specified number of incoming requests. When the incoming requests exceed the specified numbers, the interface overloads. For instance, an interface is overloaded when:

- There is a network element failure causing large number of re-attaches
- Multiple users perform location update or transition from idle to active mode frequently

Overloading causes the interface to either drop the requests or delay processing the request. The overall network performance degrades because of overloading at the interface. This can lead to node congestion, failure or collapse which in turn causes load increase on the other nodes.

The SMF measures different resources and defines the load based on those measurements. Also, the SMF updates the NRF about the load. Currently, the SMF applies overload protection on inbound messages. The external nodes throttle towards the SMF to come out of a congestion when overload protection is applied on the inbound interface (SBA Interface).

**NOTE:** The scope of this feature is only on overload due to inbound requests on SBA interface.

### How it Works

The SMF protects inbound requests from overloading at Endpoint and Application levels.

- **Endpoint Level** – The protection is based on the HTTP request method without taking the message type into account.
- **Application Level** – The protection is based on the message type.

### Message Priority

The SMF applies the overload protection on the incoming request messages after evaluating the resources' availability to process the request and the message priority. The high priority messages get the lower preference to throttle, and low-priority messages get higher preference. An overloaded NF applies the message prioritization schemes on the incoming messages during an overloaded condition. In such conditions, the NF excludes the messages of the highest priority from the overload protection mechanism.



Once you configure message priority, SMF starts classifying the messages based on their priority. This configuration is optional. If you chose not to use this configuration, SMF applies the overload protection technique without considering the message priority.

## Overload Protection at Endpoint

For endpoints, the SMF offers overload protection at both the endpoint and client levels. The SMF defines the overload threshold limits for the inbound request messages. Based on the threshold range, the SMF can reject the inbound request messages. The SMF sends back an HTTP response with the configured status to the request initiator.

The following are the overload threshold limits defined in the SMF:

- **Low** – When this threshold is met, only the POST method (with generic URI contributing to resource allocation) is rejected.
- **High** – All messages are rejected with the configured (reject) statuses when this threshold is met.
- **Critical** – All messages are rejected with the configured (reject) statuses when this threshold is met.

## Configuring Overload Protection

This section describes the configuration procedures involved in configuring the overload protection for inbound request messages.

### Configuring Overload Protection at Endpoint Level

Use the following configuration to configure overload protection at endpoint level.

```
config
    endpoint sbi
        overload-control threshold threshold_limit threshold_range action
        action_status action_code range
    commit
end
```

#### NOTES:

- **overload-control**: Specify the overload control at endpoint level.
- **threshold** : Specify the threshold limit and range.
- **threshold\_limit**: Specify the threshold limit. *threshold\_limit* must be one of the following:
  - *low*: Specify the low threshold limit for overload protection.
  - *high*: Specify the high threshold limit for overload protection.
  - *critical*: Specify the critical threshold limit for overload protection.
- **threshold\_range**: Specify the threshold range. *threshold\_range* must be an integer in the range of 10 – 100000.
- **action** : Specify the action to be taken for the threshold limit.

- *action\_status*: Specify the action for the threshold limit. *action\_status* must be:
  - **reject**: Reject the inbound messages if the specified threshold range is met.
- *action\_code*: Specify the action status code. *action\_code* must be:
  - **reject-code**: Specify the reject status code.
- *range*: Specify the range of the action code. *range* must be an integer in the range of 100 – 600.

The following is an example configuration:

```
overload-control threshold low 500 action reject reject-code 501
overload-control threshold critical 10000 action reject reject-code 329
```

## Configuring Overload Protection at Client Level

Use the following sample configuration to configure overload protection at client level.

```
config
    endpoint sbi
        overload-control client threshold threshold_limit threshold_range action
        action_status action_code range
        commit
    end
```

### NOTES:

- **overload-control client**: Specify the overload control at client level.
- **threshold** : Specify the threshold limit and range.
- *threshold\_limit*: Specify the threshold limit. *threshold\_limit* must be one of the following:
  - *low*: Specify the low threshold limit for overload protection.
  - *high*: Specify the high threshold limit for overload protection.
  - *critical*: Specify the critical threshold limit for overload protection.
- *thershold\_range*: Specify the threshold range. *thershold\_range* must be an integer in the range of 10 – 100000.
- **action** : Specify the action to be taken for the threshold limit.
- *action\_status*: Specify the action for the threshold limit. *action\_status* must be:
  - **reject**: Reject the inbound messages if the specified threshold range is met.
- *action\_code*: Specify the action status code. *action\_code* must be:
  - **reject-code**: Specify the reject status code.
- *range*: Specify the range of the action code. *range* must be an integer in the range of 100 – 600.

The following is an example configuration:

```
overload-control client threshold low 50 action reject reject-code 329
overload-control client threshold critical 20000 action reject reject-code
501
```

## Verifying the Overload Protection Configuration

Use the **show running-config** command to view the overload protection configuration in the SMF Ops Center. The following is a sample output of the **show running-config** command.

```
[cluster1/data] example# show running-config

endpoint sbi
  overload-control threshold low 5000 action reject reject-code 555
  overload-control threshold high 7000 action reject reject-code 329
  overload-control threshold critical 10000 action reject reject-code 503
  overload-control client threshold low 750 action reject reject-code 329
  overload-control client threshold high 500 action reject reject-code 329
  overload-control client threshold critical 1000 action reject reject-code 503
interface n11
  overload-control threshold low 4000 action reject reject-code 555
  overload-control threshold high 6000 action reject reject-code 329
  overload-control threshold critical 7000 action reject reject-code 503
  overload-control client threshold low 500 action reject reject-code 329
  overload-control client threshold high 700 action reject reject-code 329
  overload-control client threshold critical 800 action reject reject-code 503
exit
```

## Configuring the Message Priority

Use the following configuration to configure message priority for the inbound request messages.

```
configure
  overload-control threshold threshold_limit threshold_range action reject
  reject-code range exclude message-priority priority_value
end
```

### NOTES:

- **overload-control** – Specify the overload control at endpoint level.
- **threshold** – Specify the threshold limit and range.
- **threshold\_limit** – Specify the threshold limit. *threshold\_limit* must be one of the following:
  - low – Specify the low threshold limit for overload protection.
  - high – Specify the high threshold limit for overload protection.
  - critical – Specify the critical threshold limit for overload protection.
- **threshold\_range** – Specify the threshold range. *threshold\_range* must be an integer in the range of 10–100000.
- **action** – Specify the action to be taken for the threshold limit.
- **action\_status** – Specify the action for the threshold limit. *action\_status* must be:

- **reject** – Rejects the inbound messages if the specified threshold range is met.
- **exclude message-priority** – Excludes the messages from the overload protection mechanism depending on the assigned priority.
- *priority\_value* – Specifies the priority value.

The following is an example configuration:

```
overload-control threshold low 1000 action reject reject-code 100 exclude
message-priority 8
```

```
overload-control threshold high 2000 action reject reject-code 100 exclude
message-priority 5
```

If the priority value is 8, then the messages received with priority 8 or higher are not throttled. This applies even when the system threshold is lower than the priority value. The 3GPP defined message priority is 0–31 as per *3GPP TS 29.500, section 6.8.4*.

## Monitoring and Troubleshooting

This section provides information regarding bulk statistics available to monitor and troubleshoot this feature.

### Statistics

The following statistics are available in support of Overload Control.

Bulk Statistics	Statistics Type	Description
endpoint_overload_status	Gauge	Contains Endpoint-Name, Interface-Name and Overload-Level as labels. Once any level(low/high/critical) is hit, the gauge value will be set to 1. In normal condition the value is set to 0.
endpoint_client_overload_status	Gauge	Contains Endpoint-Name, Interface-Name, peer-host name and Overload-Level as labels. Once any level(low/high/critical) is hit, the gauge value will be set to 1. In normal condition the value is set to 0.
endpoint_pending_request	Gauge	Display current outstanding request for an endpoint. It contains Endpoint name and Interface Name as label.

<b>Bulk Statistics</b>	<b>Statistics Type</b>	<b>Description</b>
endpoint_client_pending_request	Gauge	Display current outstanding request for a peer connected with an endpoint. It contains Endpoint name, Interface Name and peer host address connected to the endpoint as label.
endpoint_overload_exclude	Counter	Display the messages with their priority details that were excluded from the overload control mechanism. The metric is incremented for every message, which bypasses the overload control mechanism.





## CHAPTER 44

# Support for the Unsubscribe-To-Notifications Messages

- [Feature Summary and Revision History, on page 705](#)
- [Feature Description, on page 706](#)
- [How it Works, on page 706](#)
- [OAM Support for the Unsubscribe-To-Notifications Messages, on page 707](#)

## Feature Summary and Revision History

### Summary Data

*Table 208: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Product(s) or Functional Area	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 209: Revision History*

Revision Details	Release
First introduced.	2020.02.2

## Feature Description

The Unified Data Management (UDM) is responsible for primarily storing the subscriber data, which SMF accesses for managing the user sessions on the network. The SMF explicitly subscribes to receive the notifications about the events that occur in the subscriber data such session terminate. When the SMF wants to stop receiving the notifications, it initiates the Unsubscribe-to-Notification messages to UDM. Upon receiving these messages, the UDM cancels the subscription by removing the notification subscription for the subscribed session.

## How it Works

This section provides a brief of how the SMF and UDM interact over the Unsubscribe-to-Notifications message:

1. The NF such as SMF sends an Unsubscribe-to-Notifications request to the resource identified by the URI to the UDM. The SMF transacts the request to the UDM over the N10 interface. The Unsubscribe-to-Notifications request lets the SMF unsubscribe from notifications for a specific subscriber session. The SMF receives the URI details during the subscription creation process.

The Unsubscribe-to-Notifications request contains the 'SUPI' and 'subscriptionId' in the URI.

2. The UDM processes the request, and based on the response; it sends a response code to the SMF. For example, if the unsubscription is successful, then UDM sends 204 code. If the request is not processed, then the appropriate HTTP status code indicating the error is returned in the response body along with the additional error information.
3. The SMF is equipped to handle the timeout and failure that occurs when sending the Unsubscribe-to-Notifications messages to the UDM. In the event, the Unsubscribe-to-Notifications request fails, the SMF continues to process the corresponding sessions.

The Unsubscribe-to-Notification message is required for sessions that are hosted on the EUTRA network. They may not be a requirement for sessions that are released on the NR and WLAN network. For these access types, the SMF sends the UDM registration and deregistration messages that include subscription to notifications through implicit-unsubscribe during the deregistration.

## Standards Compliance

The Support for the Unsubscribe-To-Notifications Messages feature complies with the following standards:

- 3GPP TS 29.503 - 5G System; Unified Data Management Services

## Call Flows

This section describes the call flow for the Unsubscribe-To-Notifications message support.

### Unsubscribe-to-Notifications Call Flow

This section describes the call flow on how the SMF sends a request to the UDM to unsubscribe from notifications of data changes.



Figure 125: Unsubscribe-to-Notifications Interaction with UDM

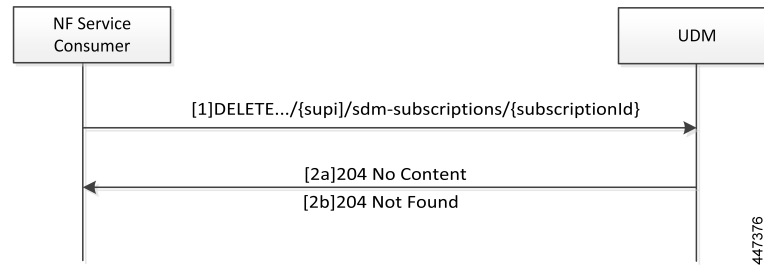


Table 210: Unsubscribe-to-Notifications Interaction Call Flow Description

Step	Description
1	<p>The NF service consumer such as SMF sends a request to the UDM to unsubscribe from notifications. By unsubscribing, the UDM no longer sends notifications to SMF when the data modifications occur in the respective subscriber session.</p> <p>The NF service consumer sends a DELETE request to the resource identified by the URI. The NF service consumer receives the URI when the subscription gets created.</p>
2a	If the deletion of request is successful, the UDM responds with "204 No Content".
2b	<p>If the subscription is invalid, which could be due to an unknown subscriptionId value, then the HTTP status code "404 Not Found" is returned along with the additional error information in the response body (as part of the "ProblemDetails" element).</p> <p>If the request is not processed, then the appropriate HTTP status code indicating the error is returned in the DELETE response body along with the additional error information.</p>

## OAM Support for the Unsubscribe-To-Notifications Messages

This section describes operations, administration, and maintenance information for this feature.

### Statistics Support

The SMF maintains the following labels on the smf-rest-ep pod for monitoring the number of unsubscribe-to-notifications messages that are initiated towards UDM:

- nfType – “udm”
- messageDirection – “outbound”
- apiName – “sdm\_unsubscription\_req”
- nfUri – “nf\_uri”
- respStatus – “response\_status”
- rspCause – “response\_cause”





## CHAPTER 45

# SMF Interface for Metrics

- [Feature Summary and Revision History, on page 709](#)
- [Feature Description, on page 709](#)

## Feature Summary and Revision History

### Summary Data

#### Feature Summary

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 211: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

SMF uses Prometheus for gathering statistics/counters from its microservices.

Grafana is used as the user interface to view metrics. It pulls the data from the Prometheus data store. Default graphs for KPI are available using Grafana for rendering a graphical view of the statistics with timelines.

For each microservice, counters and a set of labels are defined. Counters are incremented/decremented with the set of labels depending on the functionality.

The following snapshot is a sample of the Grafana dashboard.

**Figure 126: Grafana Dashboard**



## SMF Rest EP Microservice

This section describes the supported counters and set of labels for the SMF Rest EP microservice.

### Counters

The SMF REST EP microservice includes the following counters:

**Table 212: SMF REST EP Microservice Counters**

Number	Metric	Description
1	smf_restep_http_msg_total	This counter is incremented with every HTTP message received/sent at rest-ep microservice.
2	smf_restep_http_msg	This counter is incremented with every HTTP message received/sent at rest-ep microservice along with the time taken to serve the message.

### Labels

The SMF REST EP microservice includes the following labels for the counters:

Table 213: SMF REST EP Microservice Labels for Counters

Number	Label	Description
1	NF TYPE	This label can be any 5G Node that interacts with SMF. For example: AMF, PCF, NRF
2	MESSAGE DIRECTION	Displays the direction of the HTTP message with respect to the REST EP microservice. The possible values are: "inbound" "outbound"
3	API NAME	Displays the service name being served. It can be: "register_ue" "deregister_ue" "subscription_req" "nf_registration" "nf_discovery" "slice_selection" "amf_create_sm_context" "amf_update_sm_context" "amf_release_sm_context" "amf_n1_n2_transfer" "pcf_sm_policy_control_create" "pcf_sm_policy_control_update" "pcf_sm_policy_control_delete" "pcf_sm_policy_control_update_notify" "pcf_sm_policy_control_terminate_notify"
4	NF URI	Displays the rest-ep URI used in the HTTP message (can be FQDN).
5	RESPONSE STATUS	Displays the HTTP Response. It can be any 2xx, 4xx or 5xx response.

## SMF Service

This section describes the supported counters and set of labels for the SMF service.

### Labels

The SMF service includes the following labels for the counters:

Table 214: SMF Service Labels for Counters

Number	Label	Description
1	PROCEDURE TYPE	This label can take any value depending on the type of procedure queried for: <p>"pdu_sess_create"  "ue_req_pdu_sess_mod"  "smf_req_pdu_sess_mod"  "pcf_req_pdu_sess_mod"  "ue_req_pdu_sess_rel"  "smf_req_pdu_sess_rel"  "pcf_req_pdu_sess_rel"  "amf_req_pdu_sess_rel"</p>
2	STATUS	Displays the status type. The possible values are: <p>"attempted"  "success"  "failure"</p>
3	PDU CONNECTION TYPE	Displays the PDU connection type. The possible values are: <p>"ipv4"  "ipv6"  "ipv4v6"</p>
4	PDU STATE	Displays the PDU state. The possible values are: <p>"idle"  "connected"</p>

## SMF Protocol Microservice

This section describes the supported counters and set of labels for the SMF Protocol microservice.

### Counters

The SMF service includes the following counters:

Table 215: SMF Service Counters

Number	Metric	Description
1	smf_service_stats	This counter is incremented with every query made to the smf-service.

Number	Metric	Description
2	smf_service_counters	This is a gauge counter and can be incremented/decremented based on the functionality with every query made to the smf-service.

## Labels

The SMF Protocol service includes the following labels for the counters:

**Table 216: SMF Protocol Service Labels for Counters**

Number	Label	Description
1	MESSAGE NAME	This label can take any value depending on the procedure queried for: "session_establishment_req" "session_establishment_res" "session_modification_req" "session_modification_res" "session_report_req" "session_report_res" "session_deletion_req" "session_deletion_res" "association_setup_req" "association_setup_res" "association_update_req" "association_update_res" "association_release_req" "association_release_res" "prime_pfd_management_req" "prime_pfd_management_res" "heartbeat_req" "heartbeat_res" "node_report_req" "node_report_res"
2	MESSAGE DIRECTION	Displays the direction of the HTTP message with respect to the REST EP microservice. The possible values are: "inbound" "outbound"

Number	Label	Description
3	STATUS	Displays the status of the message. The possible values are: “accepted” “denied” “discarded”

## Converged Core Refactoring Changes

This section describes the changes related to converged core refactoring in this chapter.

For the SMF Protocol service, the "n4" prefix in the procedure names for the "Message Name" label is removed.





# CHAPTER 46

## System Logging Support Per SUPI

- [Feature Summary and Revision History, on page 715](#)
- [Feature Description, on page 715](#)
- [Configuration Support for Persistent Transaction Logs, on page 720](#)

### Feature Summary and Revision History

Table 217: Revision History

Revision Details	Release
First introduced.	Pre-2020.02.0

### Feature Description

Application infrastructure provide common way to log the log messages across applications. Each log has timestamp, log message, log level and log tag.

Log tag is made up of module name, component name and interface name. It is used as filter to enable/disable specific type of log messages. Log tag needs to be pre-created and is supposed to be pass while logging.

#### Creating log tag

```
common.LogTagN7RestEp = appCtx.RegisterLogTag("rest_ep", "app", "n7")
```

Log a message

```
appCtx.Info(common.LogTagN7RestEp, "Starting rest-ep app")
```

#### Log Level

App infra provides 6 log levels, which can be used as filter along with log tag to enable/disable specific logs. Each level represents the level of importance of log message, which can be used while troubleshooting.

Log Level	Usage
Error	Error is used when there is incorrectness which can lead to serious issues.

Log Level	Usage
Warn	Warn can used to notify something serious is about to happen if it continuous like this and not attended.
Info	Info can used for normal expected behavior like app started, stopped, etc.
Debug	Debug can used to provide more information which is require to debug problems.
Trace	Trace can used to provide very detailed information. It can also be used in monitor routines where same debug log is keep coming periodically.
Off	Meaning no loggin informatin, this can be configured in CLI to turn off/turn on logging.

### Log Level Order

Every time app infra is logging any log message, it matches the log level and log tag with configured log setting before logging.

Log Level (order)	Usage
Error (0)	Matches error logs.
Warn (1)	Matches warn and error logs.
Info (2)	Matches info, warn and error logs.
Debug (3)	Matches debug, info, warn and error logs.
Trace (4)	Matches trace, debug, info, warn and error logs.
Off (5)	Matches no log to disable errors.

### Logging Types

App infra provides three different types of logging, each logging type can be configured.

- Application logging
- Transaction logging
- Monitor Subscriber Logging
- Trace logging

### Application Logging

Application Logging is single line simple logging. It can be used by application from anywhere.

The application log includes the time stamp, service name, log level, file name with line no, log tag and log message.

To log application logs, logging API on application context is called.

```
appCtx.Warn(logTagConfig, "Found multiple config versions: %s hence can not notify listeners",
fileVersions)
```

Sample application log:

```
[time stamp] [service name] [log level] [file name : line no] [log tag] [log
message]
2019/12/31 12:16:52.589 rest-ep [DEBUG] [FileChangeMonitor.go:82] [infra.config.core] Found
multiple config versions: 10 hence can not notify listeners
```

### Transaction Logging

Transaction logging is a special type of logging which represents the transaction execution.

A transaction log is generated for the events that happen between the components such as NF, pods, services. The transaction logs are preserved in the file system residing within the OAM pod to ensure that they are persistent. You can view these logs through the OAM console. When storing the logs in the file system, you can compress the size of logs by truncating the logs. Further, you can also define the maximum amount of data that a file must contain which is useful for managing the disk space.

The multiline logs include:

- Transaction type, priority and status
- Session state
- Session and subscriber IDs (if available)
- Execution logs
  - Each execution log include timestamp, log level, log tag and log message
  - The log level and log tag can be used as filter to enable/disable specific logs

To log transaction logs, logging API on transaction is called.

```
txn.Debug(LogTagUdm, "Sending request to udm")
```

Sample Transaction log:

```
***** TRANSACTION: 00001 *****
TRANSACTION SUCCESS:
Txn Type           : MessageTypeExampleCreate(1)
Priority            : 100
Session State      : Create_Session
Subscriber Id      : sub_key:addtcp-123
Session Keys       : addtcp-123 (pk) uk1_addtcp-123 (uk) uk2_addtcp-123 (uk) nuk1 (nuk)
nuk2 (nuk)
LOG MESSAGES:
2019/12/31 13:05:20.585 [INFO] [service.processor.n7] Message Example_Create decoded
2019/12/31 13:05:20.586 [INFO] [service.processor.n7] Session state is Create_Session
2019/12/31 13:05:20.586 [DEBUG] [infra.transaction.core] Trying to load session
2019/12/31 13:05:20.586 [DEBUG] [infra.session_cache.core] Get session by pk addtcp-123

2019/12/31 13:05:20.586 [DEBUG] [infra.session_cache.core] Record not found by key
addtcp-123 in cache, loading from datastore
2019/12/31 13:05:20.586 [DEBUG] [infra.transaction.core] Session start triggered
2019/12/31 13:05:20.586 [DEBUG] [infra.transaction.core] Queuing new transaction for
processing
2019/12/31 13:05:20.586 [DEBUG] [service.udm_query.n7] Sending request to udm
2019/12/31 13:05:20.592 [DEBUG] [service.udm_query.n7] Received response from udm
response:"2"
```

```

2019/12/31 13:05:20.592 [DEBUG] [infra.transaction.core] Last stage ( init_done ) ->
Next stage ( udm_done )
2019/12/31 13:05:20.592 [DEBUG] [service.udm_query.n7] Sending udp request
2019/12/31 13:05:20.595 [INFO] [service.udm_query.n7] Received udp response
response:"Success"
2019/12/31 13:05:20.595 [DEBUG] [infra.transaction.core] Last stage ( udm_done ) ->
Next stage ( udp_done )
2019/12/31 13:05:20.595 [DEBUG] [service.udm_query.n7] Sending Tcp request
2019/12/31 13:05:20.603 [INFO] [service.udm_query.n7] Received tcp response
response:"Success"
2019/12/31 13:05:20.603 [DEBUG] [infra.transaction.core] Last stage ( udp_done ) ->
Next stage ( finished )
2019/12/31 13:05:20.603 [INFO] [service.processor.n7] Process end
2019/12/31 13:05:20.603 [DEBUG] [infra.transaction.core] Creating session
2019/12/31 13:05:20.603 [DEBUG] [infra.session_cache.core] Save session with key
addtcp-123 in cache
*****

```

### Transaction Logs Additional Settings

Transaction logging have following two additional settings which can be optionally enabled.

1. Message: Using CLI enable messages in transaction logging can be enabled, "logging transaction message enable". Incoming request and outgoing response messages associated with the transaction in transaction logs can also be enabled.

```

Transaction Log received from Instance: example.rest_ep.cluster1.example-data.1
***** TRANSACTION: 00046 *****

```

#### TRANSACTION SUCCESS:

```

Txn Type      : MessageTypeExampleDelete(5)
Priority      : 1
Session State : No_Session

```

#### INCOMING REQUEST:

```

Timestamp: 2020/03/23 06:23:27.146
Message: Example Delete Request
Description: Transaction REST Req Message
Source: 192.168.2.168:9001//session/123
Destination: example.rest_ep.cluster1.example-data.1
PAYLOAD:
  Key: 123

```

#### OUTGOING RESPONSE:

```

Timestamp: 2020/03/23 06:23:27.146
Message: Example Delete Response
Description: Transaction REST Rsp Message
Source: example.rest_ep.cluster1.example-data.1
Destination: 192.168.2.168:9001//session/123
PAYLOAD:
  PduSessionId: 5

```

#### LOG MESSAGES:

```

2020/03/23 06:23:27.146 [INFO] [rest_ep.app.n7] Process end
2020/03/23 06:23:27.146 [INFO] [rest_ep.app.n7] Prepare success response
2020/03/23 06:23:27.146 [INFO] [rest_ep.app.n7] Response: response:"Success"
delete_rsp:<pduSessionId:5 > udp_rsp:<udpSessionId:5555 >

```

2. Duplicate: Using CLI duplicate in transaction logging can be enabled"logging transaction duplicate enable". Transaction logs duplicated in application context logs can also be enabled.

### Monitor Subscriber Logging

This logging helps to control the logging level of transaction logs when monitor subscriber CLI is enabled. Monitor Subscriber CLI can be used to capture the transaction logs for a given supi. With Monitor Subscriber

Logger we can control the logging level specifically for the subscriber for which monitor subscriber CLI is triggered.

This logging is helpful in where transaction logs are set to error by default and capturing the debug level transaction logs for certain modules specific subscriber is useful. This can be achieved using the below two steps:

1. Enable the Monitor Subscriber logger at info level using command: Example: logging name infra.config.core level monitor-subscriber debug.
2. Enable the monitor subscriber for given subscriber using the following sample command:

```
monitor subscriber supi imsi-123456789 transaction-logs yes
```

### Sample Monitor Subscriber Log

```
[cluster1/data] example# monitor subscriber supi imsi-123456789 transaction-logs yes
supi: imsi-123456789
captureDuration: 300
enableInternalMsg: false
enableTxnLog: true
  % Total      % Received % Xferd  Average Speed   Time    Time       Time  Current
                               Dload  Upload   Total     Spent    Left     Speed
100  242  100    100  100    142  14285  20285  --:--:--  --:--:--  --:--:--  34571
Command: --header Content-type:application/json --request POST --data
{"commandname":"mon_sub","parameters":{"supi":"imsi-123456789",
"duration":300,"enableTxnLog":true,"enableInternalMsg":false,"action":"start"}}
http://oam-pod:8879/commands
Result start mon_sub, fileName
->monsublogs/imsi-123456789_WithTxnLogs_TS_2020-03-23T08:16:19.806104824.txt
Starting to tail the monsub messages from file:
monsublogs/imsi-123456789_WithTxnLogs_TS_2020-03-23T08:16:19.806104824.txt

Transaction Log received from Instance: example.rest_ep.cluster1.example-data.1
***** TRANSACTION: 00038 *****
TRANSACTION SUCCESS:
    Txn Type           : MessageTypeExampleRestQuery(6)
    Priority            : 1
    Session State      : No_Session

LOG MESSAGES:
2020/03/23 06:23:27.093 [INFO] [rest_ep.app.n7] Message Sample_Rest_Query decoded
2020/03/23 06:23:27.093 [INFO] [rest_ep.app.n7] Process init
2020/03/23 06:23:27.093 [INFO] [rest_ep.app.n7] Process continue
2020/03/23 06:23:27.093 [INFO] [infra.transaction.core] Calling RPC Udm on host Udm_v1
proc-name Udm proc-method: Register
2020/03/23 06:23:27.094 [INFO] [rest_ep.app.n7] Process end
2020/03/23 06:23:27.094 [INFO] [rest_ep.app.n7] Prepare success response
2020/03/23 06:23:27.094 [INFO] [rest_ep.app.n7] default Response: response:"123"
rest_rsp:<restSessionId:5678 >
*****
```

### Trace Logging

Similar to transaction logging, tracing is also special type logging. This logs are appended in traces. Refer tracing section to understand more about trac logging.

To log trace logs, logging trace API on transaction is called:

```
txn.DebugTrace(LogTagUdm, "Sending request to udm")
```

To differentiate trace APIs with transaction APIs, all trace logging apis are suffixed with Trace word.

```
txn.ErrorTrace()          txn.WarnTrace()  txn.InfoTrace()  txn.DebugTrace()  txn.TraceTrace()
```

# Configuration Support for Persistent Transaction Logs

This section describes how to configure support for the persistent transaction logging.

Configuration of persistent transaction logs involves the following steps:

- Configuring the persistent transaction logs
- Viewing the transaction logs

## Configuring the Persistent Transaction Logs

This section describes how to configure the persistent transaction log parameters.

The transaction logs are saved in the transaction log file which reside in the transaction logs directory of OAM pod.

```
config
  logging
    transaction
      persist [ disable | enable ]
      max-file-size max_filesize
      max-rotation max_rotation
    end
```

### NOTES:

- **logging**– Enters the logging configuration mode.
- **transaction**– Enters the transaction log configuration mode.
- **persist [ disable | enable ]**– Configures the ability to write the transaction logs to the transaction log file.
- **max-file-size *max\_filesize***– Specifies the maximum size (in MB) of the transaction logs that must be preserved in the file. The default size is 50 MB. The accepted range is 1–10000 MB.
- **max-rotation *max\_rotation***– Specifies the maximum number of files that must be stored in the folder. After the specified number is reached, the files are rotated, which means that the oldest file is deleted and the latest log file is added to the folder. For example, if the folder has files a1.txt–a.10.txt and when the a.11.txt is added, then a1.txt is deleted. The default number is 10. The accepted range is 2–1000.

## Viewing the Transaction Logs

This section describes how to view the transaction logs that are stored on the OAM pod.

To view the persistent transaction logs, use the following configuration through the SMF Ops Center:

```
transaction file dump filename file_path
```

You can use the **transaction log list** command to view the list of log files and their paths.

The following is a sample output of the transaction logs:

```
RELEASE_NAMESPACE: 'example-data'
Dumping file 'transactionlogs/transaction.log.20200907033433.4.gz'
```

```
InstanceInfo: example.example-rest-ep.cluster1.example-data.1
TimeStamp: 2020-09-09 00:25:18.379439773 +0000 UTC
***** TRANSACTION: 01371 *****
TRANSACTION SUCCESS:
  Txn Type           : MessageTypeExampleCreate(1)
  Priority            : 1
  Session Namespace  : none(0)
LOG MESSAGES:
  2020/09/09 00:25:18.339 [INFO] [rest_ep.app.n7] Message Example_Create decoded
  2020/09/09 00:25:18.339 [INFO] [rest_ep.app.n7] Process init
  2020/09/09 00:25:18.339 [DEBUG] [rest_ep.app.n7] Config from GetConfig is Version: 783da2fc038c6bc961a95e2bf3dd6d93f282e36b30e0362698alde369a2fd15c Services: [Name: restServer Type: Rest Endpoint: sbi Name: tcpServer Type: Tcp Endpoint: tcp-protocol Name: udpServer Type: Udp Endpoint: udp-protocol]
  2020/09/09 00:25:18.339 [INFO] [rest_ep.app.n7] Process continue
  2020/09/09 00:25:18.339 [DEBUG] [rest_ep.app.n7] DerivedConfig from GetConfig is DerivedNameToBeTested_cb3383b95927a434d42cd9d5687ccf1b13e2de4b2faf4543287a34afb32518fe
  2020/09/09 00:25:18.339 [DEBUG] [rest_ep.udp.n5] Sending message Example_Create to example-service
  2020/09/09 00:25:18.342 [INFO] [infra.transaction.core] Calling RPC example-service_ipc_stream on host example-service_1 proc-name example-service_ipc_stream
```







## CHAPTER 47

# TAI Selection from AMF

- [Feature Summary and Revision History, on page 723](#)
- [Feature Description, on page 723](#)
- [How it Works, on page 724](#)
- [Configuring TAI Selection from AMF, on page 740](#)

## Feature Summary and Revision History

### Summary Data

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 218: Revision History*

Revision Details	Release
First introduced.	2021.01.0

## Feature Description

SMF supports TAI selection from AMF with this release.

SMF is added with a new priority attribute in the SmfInfo data type. Which enables the discovery and the selection of SMF based on the relative priorities registered by candidate SMFs in different smfInfo entries with different TAI lists. New SmfInfoList map is supported.

## How it Works

### Architecture

New priority attribute added in the SmfInfo data type to enable the discovery and selection of SMF, this is based on the relative priorities registered by candidate SMFs in different smfInfo entries with different TAI lists.

- SmfInfo in NFProfile is sent if there's no change in configuration(All tai-groups data being sent without priority).
- SmfInfoList map is new element in NFprofile.
- Each SmfInfoList entry doesn't contain all tai-group-list data. Each element contains entries of the same priority tai-groups per NSSAI.



**Note** All tai-groups under a slice is expected to be of the same priority.

- If tai-group-list has tai-groups of different priority configured under a slice, tai-groups are logically grouped based on priority. SmfInfo has data of tai-group of one priority and subsequent priority tai-group(s) data in each of SmfInfoList entry.
- if no tai-group is associated with any slice, then old behaviour prevails. If there's tai-group association for few slices and few without, then the smfinfoList entries of slices without tai-group have no TAI details
- For any tai-group if priority isn't defined, it's grouped separately and sent as a SmfInfo entry or different SmfInfoList entry.
- Key for each SmfInfoList map element is Incremental counter string.

**Table 219: NFProfile**

Attribute Name	Data Type	P	Cardinality	Description
nfInstanceId	NfInstanceId	M	1	Unique identity of the NF Instance.
nfType	NFType	M	1	Type of Network Function
nfStatus	NFStatus	M	1	Status of the NF Instance.
nfInstanceName	String	O	0.1	Human readable name of the NF Instance

Attribute Name	Data Type	P	Cardinality	Description
heartBeatTimer	Integer	C	0..1	Time in seconds expected between 2 consecutive heart-beat messages from an NF Instance to the NRF. It may be included in the registration request. When present in the request it shall contain the heartbeat time proposed by the NF service consumer. It shall be included in responses from NRF to registration requests (PUT) or in NF profile updates (PUT or PATCH). If the proposed heartbeat time is acceptable by the NRF based on the local configuration, it shall use the same value as in the registration request; otherwise the NRF shall override the value using a preconfigured value.
plmnList	array(PlmnId)	C	1..N	PLMN(s) of the Network Function (NOTE 7). This IE shall be present if this information is available for the NF. If not provided, PLMN ID(s) of the PLMN of the NRF are assumed for the NF.
snpnList	array(PlmnIdNid)	C	1..N	SNPN(s) of the Network Function. This IE shall be present if the NF pertains to one or more SNPNs.
sNssais	array(Snssai)	O	1..N	S-NSSAIs of the Network Function. If not provided, the NF can serve any S-NSSAI. When present this IE represents the list of S-NSSAIs supported in all the PLMNs listed in the plmnList IE. If the sNssais attribute is provided in at least one NF Service, the S-NSSAIs supported by the NF Profile shall be the set or a superset of the S-NSSAIs of the NFService(s).

Attribute Name	Data Type	P	Cardinality	Description
perPlmnSnsaiList	array(PlmnSnsai)	O	1..N	This IE may be included when the list of S-NSSAIs supported by the NF for each PLMN it's supporting is different. When present, this IE shall include the S-NSSAIs supported by the Network Function for each PLMN supported by the Network Function. When present, this IE shall override sNssais IE. (NOTE 9) If the perPlmnSnsaiList attribute is provided in at least one NF Service, the S-NSSAIs supported per PLMN in the NF Profile shall be the set or a superset of the perPlmnSnsaiList of the NFService(s).
nsiList	array(string)	O	1..N	NSI identities of the Network Function. If not provided, the NF can serve any NSI.
fqdn	Fqdn	C	0..1	FQDN of the Network Function (NOTE 1) (NOTE 2). For AMF, the FQDN registered with the NRF shall be that of the AMF Name (see 3GPP 23.003 [12] clause 28.3.2.5).
interPlmnFqdn	Fqdn	C	0..1	If the NF needs to be discoverable by other NFs in a different PLMN, then an FQDN that is used for inter-PLMN routing as specified in 3GPP 23.003 [12] shall be registered with the NRF (NOTE 8).  A change of this attribute shall result in triggering a "NF_PROFILE_CHANGED" notification from NRF towards subscribing NFs located in a different PLMN, but the new value shall be notified as a change of the "fqdn" attribute.

Attribute Name	Data Type	P	Cardinality	Description
ipv4Addresses	array(Ipv4Addr)	C	1..N	IPv4 address(es) of the Network Function (NOTE 1) (NOTE 2)
ipv6Addresses	array(Ipv6Addr)	C	1..N	IPv6 address(es) of the Network Function.
allowedPlmns	array(PlmnId)	O	1..N	<p>PLMNs allowed to access the NF instance. If not provided, any PLMN is allowed to access the NF.</p> <p>A change of this attribute shall not trigger a "NF_PROFILE_CHANGED" notification from NRF, and this attribute shall not be included in profile change notifications to subscribed NFs.</p>
allowedSnpons	array(PlmnIdNid)	O	1..N	<p>SNPNs allowed to access the NF instance.</p> <p>If this attribute is present in the NFService and in the NF profile, the attribute from the NFService shall prevail.</p> <p>The absence of this attribute in both the NFService and in the NF profile indicates that no SNPN, other than the SNPN(s) registered in the snpnList attribute of the NF Profile, is allowed to access the service instance.</p> <p>A change of this attribute won't trigger a "NF_PROFILE_CHANGED" notification from NRF, and this attribute won't be included in profile change notifications to subscribed NFs.</p>

Attribute Name	Data Type	P	Cardinality	Description
allowedNfTypes	array(NFType)	O	1..N	<p>Type of the NFs allowed to access the NF instance.</p> <p>If not provided, any NF type is allowed to access the NF.</p> <p>A change of this attribute won't trigger a "NF_PROFILE_CHANGED" notification from NRF, and this attribute won't be included in profile change notifications to subscribed NFs.</p>
allowedNfDomains	array(string)	O	1..N	<p>Pattern (regular expression according to the ECMA-262 dialect [8]) representing the NF domain names allowed to access the NF instance.</p> <p>If not provided, any NF domain is allowed to access the NF.</p> <p>A change of this attribute won't trigger a "NF_PROFILE_CHANGED" notification from NRF, and this attribute won't be included in profile change notifications to subscribed NFs.</p>
allowedNssais	array(Snssai)	O	1..N	<p>S-NSSAI of the allowed slices to access the NF instance.</p> <p>If not provided, any slice is allowed to access the NF.</p> <p>A change of this attribute won't trigger a "NF_PROFILE_CHANGED" notification from NRF, and this attribute won't be included in profile change notifications to subscribed NFs.</p>

Attribute Name	Data Type	P	Cardinality	Description
priority	Integer	O	0..1	<p>Priority (relative to other NFs of the same type) within the range 0 to 65535, to be used for NF selection; lower values indicate a higher priority. Priority may or may not be present in the nfServiceList parameters, xxxInfo parameters and in this attribute. Priority in the nfServiceList has precedence over the priority in this attribute, which has precedence over the priority in xxxInfo parameter. (NOTE 4).</p> <p>The NRF may overwrite the received priority value when exposing an NFProfile with the Nnrf_NFDiscovery service.</p>
capacity	Integer	O	0..1	<p>Static capacity information within the range 0 to 65535, expressed as a weight relative to other NF instances of the same type; if capacity is also present in the nfServiceList parameters, those will have precedence over this value. (NOTE 4).</p>
load	Integer	O	0..1	<p>Dynamic load information, within the range 0 to 100, indicates the current load percentage of the NF.</p>
oadTimeStamp	DateTime	O	0..1	<p>It indicates the point in time in which the latest load information (sent by the NF in the "load" attribute of the NF Profile) was generated at the NF Instance.</p> <p>If the NF did not provide a timestamp, the NRF should set it to the instant when the NRF received the message where the NF provided the latest load information.</p>

Attribute Name	Data Type	P	Cardinality	Description
locality	string	O	0..1	Operator defined information about the location of the NF instance (e.g. geographic location, data center) (NOTE 3)
udrInfo	UdrInfo	O	0..1	Specific data for the UDR (ranges of SUPI, group ID ...)
udrInfo	map(UdrInfo)	O	1..N	Multiple entries of UdrInfo. This attribute provides additional information to the udrInfo. udrInfoList may be present even if the udrInfo is absent.  The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters.
udmInfo	UdmInfo	O	0..1	Specific data for the UDM (ranges of SUPI, group ID...)
udmInfoList	map(UdmInfo)	O	1..N	Multiple entries of UdmInfo. This attribute provides additional information to the udmInfo. udmInfoList may be present even if the udmInfo is absent.  The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters
ausfInfo	AusfInfo	O	0..1	Specific data for the AUSF (ranges of SUPI, group ID...)



Attribute Name	Data Type	P	Cardinality	Description
ausfInfoList	map(AusfInfo)	O	1..N	<p>Multiple entries of AusfInfo. This attribute provides additional information to the ausfInfo. ausfInfoList may be present even if the ausfInfo is absent.</p> <p>The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters.</p>
amfInfo	AmfInfo	O	0..1	Specific data for the AMF (AMF Set ID, ...)
amfInfoList	map(AmfInfo)	O	1..N	<p>Multiple entries of AmfInfo. This attribute provides additional information to the amfInfo. amfInfoList may be present even if the amfInfo is absent.</p> <p>The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters.</p>
smfInfo	SmfInfo	O	0..1	Specific data for the SMF (DNN's, ...).
smfInfoList	map(SmfInfo)	O	1..N	<p>Multiple entries of SmfInfo. This attribute provides additional information to the smfInfo. smfInfoList may be present even if the smfInfo is absent.</p> <p>The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters.</p>
upfInfo	UpfInfo	O	0..1	Specific data for the UPF (S-NSSAI, DNN, SMF serving area, interface...)

Attribute Name	Data Type	P	Cardinality	Description
upfInfoList	map(UpfInfo)	O	1..N	<p>Multiple entries of UpfInfo. This attribute provides additional information to the upfInfo. upfInfoList may be present even if the upfInfo is absent.</p> <p>The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters.</p>
pcfInfo	PcfInfo	O	0..1	Specific data for the PCF
pcfInfoList	map(PcfInfo)	O	1..N	<p>Multiple entries of PcfInfo. This attribute provides additional information to the pcfInfo. pcfInfoList may be present even if the pcfInfo is absent.</p> <p>The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters.</p>
bsfInfo	BsfInfo	O	0..1	Specific data for the BSF.
bsfInfoList	map(BsfInfo)	O	1..N	<p>Multiple entries of BsfInfo. This attribute provides additional information to the bsfInfo. bsfInfoList may be present even if the bsfInfo is absent.</p> <p>The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters.</p>
chfInfo	ChfInfo	O	0..1	Specific data for the CHF.

Attribute Name	Data Type	P	Cardinality	Description
chfInfoList	map(ChfInfo)	O	1..N	Multiple entries of ChfInfo. This attribute provides additional information to the chfInfo. chfInfoList may be present even if the chfInfo is absent.  The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters.
nefInfo	NefInfo	O	0..1	Specific data for the NEF.
nrfInfo	NrfInfo	O	0..1	Specific data for the NRF.
udsfInfo	UdsfInfo	O	0..1	Specific data for the UDSF.
udsfInfoList	map(UdsfInfo)	O	1..N	Multiple entries of udsfInfo. This attribute provides additional information to the udsfInfo. udsfInfoList may be present even if the udsfInfo is absent.  The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters
nwdafInfo	NwdafInfo	O	0..1	Specific data for the NWDAF.
pcscfInfoList	map(PcscfInfo)	O	1..N	Specific data for the P-CSCF.  The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters. (NOTE 11)
hssInfoList	map(HssInfo)	O	1..N	Specific data for the HSS.  The key of the map will be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters.
customInfo	object	O	0..1	Specific data for custom Network Functions.

Attribute Name	Data Type	P	Cardinality	Description
recoveryTime	DateTime		0..1	Timestamp when the NF was (re)started.
nfServicePersistence	boolean	O	0..1	<p>True: If present, and set to true, it indicates that the different service instances of a same NF Service in this NF instance, supporting a same API version, are capable to persist their resource state in shared storage and therefore these resources are available after a new NF service instance supporting the same API version is selected by a NF Service Consumer (see 3GPP 23.527 [27]).</p> <p>False (default): Otherwise, it indicates that the NF Service Instances of a same NF Service are not capable to share resource state inside the NF Instance.</p>
nfServices	array(NFService)	O	1..N	List of NF Service Instances. It will include the services produced by the NF that can be discovered by other NFs, if any.
nfProfileChangesSupportInd	boolean	O	0..1	<p>NF Profile Changes Support Indicator.</p> <p>See Annex B.</p> <p>This IE may be present in the NFRegister or NFUpdate (NF Profile Complete Replacement) request and must be absent in the response.</p> <p>True: the NF Service Consumer supports receiving NF Profile Changes in the response.</p> <p>False (default): the NF Service Consumer does not support receiving NF Profile Changes in the response.</p> <p>Write-Only: true</p>

Attribute Name	Data Type	P	Cardinality	Description
nfProfileChangesInd	boolean	O	0..1	<p>NF Profile Changes Indicator. See Annex B.</p> <p>This IE must be absent in the request to the NRF and may be included by the NRF in NFRegister or NFUpdate (NF Profile Complete Replacement) response.</p> <p>True: the NF Profile contains NF Profile changes.</p> <p>False (default): complete NF Profile.</p> <p>Read-Only: true</p>
defaultNotificationSubscriptions	array(DefaultNotificationSubscription)	O	1..N	<p>Notification endpoints for different notification types. (NOTE 10)</p>
gmlcInfo	GmlcInfo	O	0..1	Specific data for the GMLC
nfSetIdList	array(NfSetId)	O	1..N	<p>NF Set ID defined in clause 28.12 of 3GPP TS 23.003 [12].</p> <p>At most one NF Set ID must be indicated per PLMN of the NF.</p>
servingScope	array(string)	O	1..N	<p>The served area(s) of the NF instance.</p> <p>The absence of this attribute does not imply that the NF instance can serve every area in the PLMN.</p>
lcHSupportInd	boolean	O	0..1	<p>This IE indicates whether the NF supports Load Control based on LCI Header (see clause 6.3 of 3GPP TS 29.500 [4]).</p> <p>True: the NF supports the feature.</p> <p>False (default): the NF does not support the feature.</p>

Attribute Name	Data Type	P	Cardinality	Description
olcHSupportInd	boolean	O	0..1	<p>This IE indicates whether the NF supports Overload Control based on OCI Header (see clause 6.4 of 3GPP TS 29.500 [4]).</p> <p>True: the NF supports the feature.</p> <p>False (default): the NF does not support the feature.</p>

Attribute Name	Data Type	P	Cardinality	Description
----------------	-----------	---	-------------	-------------

Attribute Name	Data Type	P	Cardinality	Description
<b>Note</b>				At least one of the addressing parameters (FQDN, IPv4address or IPv6address) is included in the NF Profile. If the NF supports the NF services with "https" URI scheme (i.e use of TLS is mandatory), then the FQDN provided in the NF Profile or the NF Service profile (see clause 6.1.6.2.3). See NOTE 1 of Table 6.1.6.2.3-1 for the use of these parameters. If multiple ipv4 addresses and/or ipv6 addresses are included in the NF Profile, the NF Service Consumer of the discovery service must select one of these addresses randomly, unless operator defined local policy of IP address selection, in order to avoid overload for a specific ipv4 address and/or ipv6 address.
<b>Note</b>				If the type of Network Function is UPF, the addressing information is for the UPF N4 interface.
<b>Note</b>				A requester NF may use this information to select a NF instance (e.g. a NF instance preferably located in the same data center).
<b>Note</b>				The capacity and priority parameters, if present, are used for NF selection and load balancing. The priority and capacity attributes must be used for NF selection in the same way that priority and weight are used for server selection as defined in IETF RFC 2782 [23].
<b>Note</b>				The NRF must notify NFs subscribed to receiving notifications of changes of the NF profile, if the NF recoveryTime or the nfStatus is changed. See clause 6.2 of 3GPP 23.527 [27].
<b>Note</b>				A requester NF may consider that all the resources created in the NF before the NF recovery time have been lost. This may be used to detect a restart of a NF and to trigger appropriate actions, e.g. release local resources. See clause 6.2 of 3GPP 23.527 [27].
<b>Note</b>				A NF may register multiple PLMN IDs in its profile within a PLMN comprising multiple PLMN IDs. If so, all the attributes of the NF Profile must apply to each PLMN ID registered in the plmnList. As an exception, attributes including a PLMN ID, e.g. IMSI-based SUPI ranges, TAIs and GUAMIs, are specific to one PLMN ID and the NF may register in its profile multiple occurrences of such attributes for different PLMN IDs (e.g. the UDM may register in its profile SUPI ranges for different PLMN IDs).
<b>Note</b>				Other NFs are in a different PLMN if they belong to none of the PLMN ID(s) configured for the PLMN of the NRF.
<b>Note</b>				This is for the use case where an NF (e.g. AMF) supports multiple PLMNs and the slices supported in each PLMN are different. See clause 9.2.6.2 of 3GPP TS 38.413 [29].
<b>Note</b>				If notification endpoints are present both in the profile of the NF instance (NFProfile) and in some of its NF Services (NFService) for a same notification type, the notification endpoint(s) of the NF Services must be used for this notification type.
<b>Note</b>				The absence of the pscfInfoList attribute in a P-CSCF profile indicates that the P-CSCF can be selected for any DNN and Access Type.
<b>Note</b>				The absence of both the smfInfo and smfInfoList attributes in an SMF profile indicates that the SMF can be selected for any S-NSSAI, DNN, TAI and access type.
<b>Note</b>				The servingScope attribute may indicate geographical areas, It may be used e.g. to discover and



Attribute Name	Data Type	P	Cardinality	Description
				select NFs in centralized Data Centers that are expected to serve users located in specific region(s) or province(s). It may also be used to reduce the large configuration of TAIs in the NF instances.

Table 220: SMFInfo

Attribute name	Data Type	P	Cardinality	Description
sNssaiSmfInfoList	array(sNssaiSmfInfoItem)	M	1..N	List of parameters supported by the SMF per S-NSSAI.
taiList	array(Tai)	O	1..N	The list of TAIs the SMF can serve. It may contain the non-3GPP access TAI. The absence of this attribute and the taiRangeList attribute indicate that the SMF can be selected for any TAI in the serving network.
taiRangeList				
taiRangeList	array(TaiRange)	O	1..N	The range of TAIs the SMF can serve. It may contain the non-3GPP access' TAI. The absence of this attribute and the taiList attribute indicate that the SMF can be selected for any TAI in the serving network.
pgwFqdn	Fqdn	O	0..1	The FQDN of the PGW if the SMF is a combined SMF/PGW-C.
accessType	array(AccessType)	C	1..2	If included, this IE must contain the access type (3GPP_ACCESS and/or NON_3GPP_ACCESS) supported by the SMF.  If not included, it must be assumed the both access types are supported.

Attribute name	Data Type	P	Cardinality	Description
priority	integer	O	0..1	<p>Priority (relative to other NFs of the same type) in the range of 0-65535, to be used for NF selection for a service request matching the attributes of the SmfInfo; lower values indicate a higher priority.</p> <p>See the precedence rules in the description of the priority attribute in NFProfile, if Priority is also present in the nfServiceList parameters or in NFProfile.</p> <p>The NRF may overwrite the received priority value when exposing an NFProfile with the Nnrf_NFDiscovery service.</p>
<p><b>Note</b> An SMF profile may contain multiple SmfInfo entries, with each entry containing a different list of TAIs and a different priority, to differentiate the priority to select the SMF based on the user location. The priority in SmfInfo has the least precedence, i.e. it applies between SMFs or SMF Services with the same priority.</p>				

## Configuring TAI Selection from AMF

### Configuring TAI Group List

Use the following configuration to configure TAI Group List.

```

configure
nssai name nssai_name
  sst sst ssd ssd
  dnn dnn
  tai-group-list tai_group_list
end

```

#### NOTES:

- **tai-group-list** *tai\_group\_list* : Configures TAI group list.

## Verifying TAI Group List

Use the following show command to verify TAI Group List:

```
show running-config nssai

nssai name slice1
sst 02
sdt Abf123
dnn [ dnn1 intershat intershat1 intershat2 ]
tai-group-list [ tai-group-1 tai-group-2 tai-group-3 ]
exit
nssai name slice2
sst 02
sdt abc456
dnn [ dnn1 intershat ]
tai-group-list [ tai-group-4 tai-group-5 tai-group-6 ]
exit
```

## Configuring Priority in SMF Info

Use the following configuration to configure Priority SMF Info.

```
configure
profile tai-group tai_group_name
  mcc mcc mnc mnc
  tac list list_name
  tac range tac_range
  Priority priority
end
```

NOTES:

- **priority** *priority* : Configures priority SMF information.

## Verifying Priority in SMF Info

Use the following show command to verify Priority in SMF info:

```
show running-config profile tai-group

profile tai-group t1
mcc 123 mnc 456
priority 1
tac list [ 1234 789123 ]
tac range start 1234 end 1980
exit
exit
exit
profile tai-group t2
priority 1
mcc 456 mnc 123
tac list [ 0000 123456 ]
tac range start 3456 end 9000
exit
exit
exit
```





# CHAPTER 48

## Timers Support

- [Feature Summary and Revision History, on page 743](#)
- [Feature Description, on page 743](#)
- [3GPP-compliant Timers, on page 744](#)
- [Custom-driven Timers, on page 746](#)

## Feature Summary and Revision History

### Summary Data

*Table 221: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 222: Revision History*

Revision Details	Release
First introduced.	2020.02.0

## Feature Description

The SMF supports configurable timers that are either 3GPP compliant or custom-driven.

This chapter provides detailed information about the function, operation, and configuration of the timers. This chapter covers the following topics:

- 3GPP-compliant timers
  - GTP timer
  - N11 timer
- Custom-driven timers
  - Absolute timer
  - Control plane inactive timer
  - User plane inactive timer

## 3GPP-compliant Timers

### GTP and N11 Timers Support

#### Feature Description

The SMF supports retransmission through the GTP and N11 timers. With this provision, when the peer does not respond with the timer value, the SMF retransmits the GTP and N11 requests. The SMF lets you configure the maximum number of retransmissions.



---

**Note** The SMF provides configuration support for GTP timer and N11 timers.

---

#### How it Works

The SMF supports the following 3GPP timers:

- **GTP retransmission timer:**

The SMF/PGW-C starts the timer denoted in the T3-RESPONSE. The timer is invoked when a signalling message (for which a reply is expected) is sent. A signalling message or the triggered message might get lost if a response is not received before the T3-RESPONSE timer expires.

Once the T3-RESPONSE timer expires, the message corresponding to the T3-RESPONSE timer is then retransmitted if the total number of retry attempts is less than N3REQUESTS.

- **5G N1N2 reattempt timer:**

If AMF rejects the N1N2 MessageTransfer with cause code as "Temporary reject registration ongoing" or "Temporary reject handover ongoing", then the SMF starts the timer for reattempting N1N2 MessageTransfer.

Once the timer expires, the message corresponding to N1N2 MessageTransfer is reattempted based on the configured retry attempts.

## Standards Compliance

The 3GPP timers support feature complies with the following standards:

- 3GPP TS 29.510 V15.2.0 (2018-12)

## Configuring the GTP and N11 Timers

This section describes how to configure the 3GPP-compliant timers—GTP and N11 timers.

### Configuring the N11 Timers

This section describes how to configure the N11 timers.

The N11 timer configuration is invoked when AMF rejects the N1N2 message transfer with the cause code as "Temporary reject registration ongoing" or "Temporary reject handover ongoing", then SMF considers the timer and reattempts the message transfer. When the timer expires, the transfer is reattempted based on the configured retry count.

#### configure

```

profile failure-handling failure_handling_name
  interface [ gtpc | N11 ] message message_type
    cause-code [ temp-reject-register | temp-reject-handover ]
    action [ retry { timeout timeout_duration |
      max-retry retry_count } | clear | terminate ]
  end

```

#### NOTES:

- **profile failure-handling** *failure\_handling\_name*— Enter the name of the profile for failure handling.
- **interface [ gtpc | N11 ]**— Configures the interface over which the message transfer must happen.
- **message** *message\_type*— Configures the message type that must be transferred over the interface. The N11 interface supports the message type as n1n2transfer.
- **cause-code [ temp-reject-register | temp-reject-handover ]**— Configures the HTTP cause code. You can configure multiple cause code values for a message.
- **action [ retry | clear | terminate ]**— Configures the action that must be performed when the message transfer is not successful.




---

**Note** Clear and terminate are not supported for the N11 interface.

---

- **action [ retry { max-retry retry\_count | timeout timeout\_duration } ]**— Specifies the number of times the message transfer must be reattempted and the time interval between the consecutive attempts.

### Example Configuration

Following is an example of N11 timer configuration.

```

show running-config
profile failure-handling n11-fht
  interface n11 message n1n2transfer
    cause-code temp-reject-register

```

```

action retry
  timeout 1000
  max-retry 2

```

## Configuring the GTP Timers

This section describes how to configure the GTP timers.

The GTP timer configuration is implemented when a signaling message or triggered message (for which a reply is expected) is lost as it did not get a response before the T3-RESPONSE timer expired. After the T3-RESPONSE timer expires, the message corresponding to the T3-RESPONSE timer is retransmitted if the total number of retry attempts is less than the N3-REQUESTS times.

**config**

```

endpoint gtp
  retransmission { max-retry retry_count | timeout timeout_duration }
end

```

**NOTES:**

- **endpoint gtp**: Enters the GTP retransmission configuration.
- **max-retry retry\_count**: Specifies the number of times the signalling message request to SMF must be reattempted. The accepted range is 0–5. Default range is 3. When the *retry\_count* is set to "0", the retransmission feature is disabled.
- **timeout timeout\_duration**: Configures the interval of time (in milliseconds) after which the GTP retransmission request is reattempted. The accepted range is 0–10. Default range is 2. When the *timeout\_duration* is set to "0", the retransmission feature is disabled.

### Example Configuration

Following is an example of GTP timer configuration.

```

show running-config

endpoint gtp
  retransmission max-retry 2 timeout 5

```

# Custom-driven Timers

## Absolute Timer Support

### Feature Description

The SMF supports Absolute Session Timeout for each PDU session. With this support, the SMF can retain the PDU session resources until the absolute session timer expires.

You can configure the absolute session timeout value under the DNN profile. If you have not configured the timeout value, the session timeout feature appears disabled and no timer is initiated.

Based on the configured value under the DNN profile, the absolute session timer is triggered during the session creation. You cannot modify the timer value during interim handling of any access and mobility procedures



for that session. After the timer expires, the SMF performs SMF-initiated release by informing all SBI interfaces and N4 Interfaces, that is, toward UE, UDM, PCF, CHF, and UPF interfaces.

## Configuring Absolute Session Timeout

To configure Absolute Session Timeout parameter under the DNN profile:

```
configure
  profile dnn dnnprofile_name
    timeout absolute absolutetimer_value
  end
```

### NOTES:

- **profile dnn** *dnnprofile\_name*: Specifies the name of the DNN profile. *dnnprofile\_name* must be an alphanumeric string.
- **timeout**: Specifies the timeout option.
- **absolute** *absolutetimer\_value*: Specifies the maximum duration of the session (in seconds), before the system automatically terminates the session. The default value is 0, which indicates that the function is disabled.

*absolutetimer\_value* must be an integer in the range of 0-2147483647.

The following is a sample configuration.

```
smf(config)# profile dnn intershat timeout absolute 900
```

## Inactivity Timer Support

### Feature Description

The SMF supports the following timers to handle the user plane (UP) and control plane (CP) inactive requests:

- UP inactivity timer
- UP idle timer
- CP idle timer

### Configuring UP Inactivity Timer

To configure the UP inactivity timer under DNN profile, use the following commands:

```
configure
  profile dnn dnnprofile_name
    userplane-inactivity-timer timer_value
  end
```

### NOTES:

- **userplane-inactivity-timer** *timer\_value*: Specifies the timer value in seconds. *timer\_value* must be an integer in the range of 0-86400. The default value of the timer is 0, which means the function is disabled.

- The SMF sends the configured inactivity timer to the UPF through the N4 PDU Session Establishment request. After the session establishment, if the configured value changes, the SMF reports the changes to the UPF through N4 modification request.
- The UPF starts the inactivity timer when there is no uplink or downlink data transmission over the N3 tunnel. The UPF stops the timer when the data transmission over N3 tunnel is resumed. On expiry of the timer, the UPF sends session report to the SMF with the user plane inactivity request (UPIR) flag set. After receiving the report indication for a session, the SMF clears the session if it is a 4G session and initiates idle mode entry if it is a 5G session.

## Configuring CP and UP Session Idle Timer

To configure the CP and UP idle timers under DNN profile, use the following commands:

```
configure
  profile dnn dnnprofile_name
    timeout { cp-idle timer_value | up-idle timer_value }
  end
```

### NOTES:

- **cp-idle** *timer\_value*: Specifies the maximum duration of the 5G session after the migration to CP idle state and before the automatic termination. The default value is 0, which indicates the function is disabled. *timer\_value* must be an integer in the range of 0-2147483647.
- **up-idle** *timer\_value*: Specifies the maximum duration of the 5G session after the migration to UP idle state and before the automatic termination. The default value is 0, which indicates the function is disabled. *timer\_value* must be an integer in the range of 0-2147483647.
- The up-idle timer starts when an AN-initiated or Network-initiated 5G session enters the idle mode. This timer stops when the session exits the idle mode. On expiry of the timer, the SMF clears the 5G sessions.
- The cp-idle timer starts when any 4G or 5G procedure ends, and stops when any new procedure starts. If the timer expires, the SMF clears the session.



# CHAPTER 49

## UDP Proxy for SMF

- [Feature Summary and Revision History, on page 749](#)
- [Feature Description, on page 749](#)

### Feature Summary and Revision History

#### Summary Data

*Table 223: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 224: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

#### Feature Description

The SMF has UDP interfaces toward the UPF (N3) and SGW (s5/s8 for EPS interworking). With the help of the protocol layer pods (smf-protocol and gtp-ep), the messages are encoded and decoded and exchanged on these UDP interfaces. For achieving the functionalities mentioned on the 3GPP specifications:

- It is mandatory for the protocol layer pods to receive the original source and destination IP address and port number. But the original IP and UDP header is not preserved when the incoming packets arrive at the UDP service in the Kubernetes (K8s) cluster.
- Similarly, for the outgoing messages, the source IP set to the external IP address of the UDP service (published to the peer node) is mandatory. But the source IP is selected as per the egress interface, when different instances of protocol layer pods send outgoing messages from different nodes of the K8s cluster.

The protocol layer POD spawns on the node, which has the physical interface configured with the external IP address to achieve the conditions mentioned earlier. However, spawning the protocol layer pods has the following consequences:

- It is not possible to achieve the node level HA (High Availability) because the protocol pods are spawned on the same node of the K8s cluster. Any failure to that node may result in loss of service.
- The protocol pods (smf-protocol, gtp-ep, and radius-ep) must include their own UDP client and server functionalities. In addition, each protocol layer pod may require labeling of the K8s nodes with the affinity rules. This restricts the scaling requirements of the protocol layer pods.

The SMF addresses these issues with the introduction of a new K8s POD called "smf-udp-proxy." The primary objectives of this POD are:

- The "smf-udp-proxy" POD acts as a proxy for all kinds of UDP messages. It also owns the UDP client and server functionalities.
- The protocol pods perform the individual protocol (PFCP, GTP, Radius) encoding and decoding and provide the UDP payload to the "smf-udp-proxy" POD. The "smf-udp-proxy" POD sends the UDP payload out after it receives the payload from the protocol pods.
- The "smf-udp-proxy" POD opens the UDP sockets on a virtual IP (VIP) instead of a physical IP. This ensures that the "smf-udp-proxy" POD does not have any strict affinity to a specific K8s node (VM). Thus, enabling node level HA for the UDP proxy.




---

**Note** One instance of the "smf-udp-proxy" POD is spawned by default in all the worker nodes in the K8s cluster. There are no changes to the configurations in this release.

---

## Relationships

The UDP Proxy for SMF feature has functional relationship with the Virtual IP Address feature.

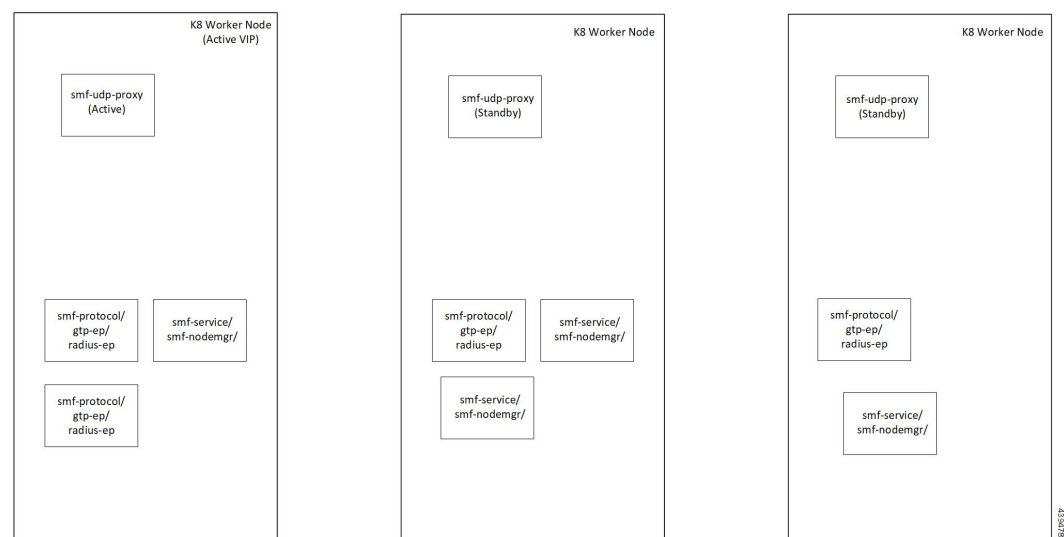
## Architecture

The "smf-udp-proxy" POD is placed in the worker nodes in the K8s cluster.

1. Each of the K8s worker node contains one instance of the "smf-udp-proxy" POD. However, only one of the K8s worker node owns the virtual IP at any time. The worker node that owns the virtual IP remains in the active mode while all the other worker nodes remain in the standby mode.
2. The active "smf-udp-proxy" POD binds to the virtual IP and the designated ports for listening to the UDP messages from the peer nodes (UPF and SGW).

3. The UDP payload received from the peer nodes are forwarded to one instance of the smf-protocol, gtp-ep, or radius-ep pods. The payload is forwarded either on the same node or different node for further processing.
4. The response message from the smf-protocol, gtp-ep, or radius-ep pods is forwarded back to the active instance of the "smf-udp-proxy" POD. The "smf-udp-proxy" POD sends the response message back to the corresponding peer nodes.
5. The SMF-initiated messages are encoded at the smf-protocol, gtp-ep, or radius-ep pods. In addition, the UDP payload is sent to the "smf-udp-proxy" POD. Eventually, the "smf-udp-proxy" POD comprises of the complete IP payload and sends the message to the peer. When the response from the peer is received, the UDP payload is sent back to the same smf-protocol, gtp-ep, or radius-ep POD from which the message originated.

**Figure 127: UDP Proxy Architecture**



## How it Works

The following sections describe the UDP proxy working principles.

### Port and Sequence Number Selection

The duplicate messages are detected based on the source IP, source address, and sequence number for all UDP-based protocols. Each message from the peer includes a unique combination of these three parameters (source IP, source address, and sequence number).

In this release, only the sequence number changes for each new SMF initiated message. The SMF initiated messages use the same source IP (Virtual IP) and same port (fixed to 8809) number.

The sequence number (PFCP) is a 24-bit value. The 8 MSBs (Most Significant Bit) specify the smf-protocol pod's instance number. The 16 LSBs (Least Significant Bit) are incrementing counters, which generate a unique number for each instance of the smf-protocol POD.

**Note**

- The UDP proxy uses the smf-protocol POD instance sequence number to determine the smf-protocol instance to which the response message must be forwarded to.
- Message retransmission and duplicate detection are not supported in this release.

## Protocol POD Selection for Peer Initiated Messages

When the "smf-udp-proxy" POD receives the peer node (for instance UPF) initiated messages, it is load balanced across the smf-protocol instances to select any instance of the smf-protocol POD. An entry of this instance number is stored along with the source IP and source port number of the peer node. This ensures that the messages from the same source IP and source port are sent to the same instance that was selected earlier.

**Note**

This release does not support the landing of retransmitted messages (from the peer nodes) on the same instance of the smf-protocol where duplicate messages are detected.

## High Availability for the UDP Proxy

The UDP proxy's HA model is based on the keepalived virtual IP concepts. A VIP is designated to the N4 interface during deployment. Also, a keepalived instance manages the VIP and ensures that the IP address of the VIP is created as the secondary address of an interface in one of the worker nodes of the K8s cluster.

The "smf-udp-proxy" instance on this worker node binds to the VIP and assumes the role of the active "smf-udp-proxy" POD. All "smf-udp-proxy" instances in other worker nodes remain in the standby mode.

When the worker node hosting the VIP fails, the keepalived instance moves the VIP to another worker node in the K8s cluster. The "smf-udp-proxy" instance in that worker node assumes the active role now.

**Note**

In this release, the VIP support for the "smf-udp-proxy" is enabled with single instance of "smf-udp-proxy." The failover scenario is not supported in this release.

## Call Flows

This section describes the call flow defined for the UDP proxy feature.

### UDP Proxy for SMF Call Flow

The following call flow describes the flow of messages for the SMF initiated messages (applicable to messages initiated by peer nodes as well).

Figure 128: UDP Proxy for SMF Call Flow

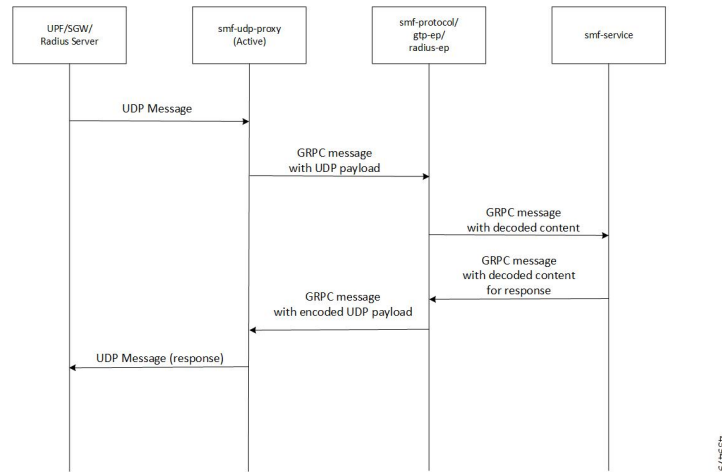


Table 225: UDP Proxy for SMF Call Flow

Step	Description
1	The peer nodes send the UDP messages to the VIP address. The active instance of “smf-udp-proxy” receives the UDP messages.
2	The UDP message’s IP and the UDP header is stripped and the UDP payload is sent to the selected smf-protocol, gtp-ep, or radius-ep POD. The meta-data contains the source IP and source port number. With the help of the internal GRPC based IPC, the message is forwarded to the smf-protocol, gtp-ep, or radius-ep POD.
3	Based on the protocol, the smf-protocol, gtp-ep, or radius-ep POD decodes the message and loads the contents in proto-encoded buffer. The smf-protocol, gtp-ep, or radius-ep POD forwards the message to the smf-service POD for further processing over GRPC.
4	The smf-service POD generates the response message and sends it back to the smf-protocol, gtp-ep, or radius-ep POD in proto-encoded buffer.
5	The smf-protocol, gtp-ep, or radius-ep POD encodes the message and creates the UDP payload. The UDP payload is sent to the active “smf-udp-proxy” in a GRPC message.
6	The active “smf-udp-proxy” sends the message to the peer nodes on the UDP socket.







# CHAPTER 50

## UPF Path Management and Restoration

- [Feature Summary and Revision History, on page 755](#)
- [Feature Description, on page 756](#)
- [How it Works, on page 756](#)
- [Configuration Support for UPF Path Management and Restoration, on page 757](#)
- [OAM Support, on page 760](#)

### Feature Summary and Revision History

#### Summary Data

*Table 226: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 227: Revision History*

Revision Details	Release
First introduced.	2020.02.0

## Feature Description

A heartbeat is used to monitor the status of a UPF node in terms of its responsiveness. The heartbeat initiates a bilateral flow of request and response between the SMF and UPF.

The SMF periodically sends a signal in the form of a heartbeat request to the registered UPF node to determine if it is active. If the SMF does not receive a response from UPF after the retransmission attempts are exhausted, then SMF recognizes that a failure has occurred and purges the subscribers that are mapped to that UPF node.

You can control the number of heartbeat requests that SMF sends to UPF, the interval between the consecutive requests, and the duration until which SMF waits for a response.

## Standards Compliance

The heartbeat transmission between SMF and UPF complies with the following standards:

- 3GPP TS 23.527
- 3GPP TS 23.007

## Converged Core Refactoring Changes

This section describes the changes related to converged core refactoring in this chapter.

The existing PFCP endpoint configuration is extended to support the "sxa" interface at the interface-level.

## How it Works

You can configure the heartbeat capability at the interface-level, UPF profile group-level, or both. The interface-level configuration is mandatory. If the interface-level configuration is unavailable, then the heartbeat parameters get configured with the default values. The profile-level configuration overrides the interface-level configuration.

The heartbeat feature is also extended to achieve high-availability for the Node Manager.

### Interface and profile-level heartbeat

The SMF-UPF interaction to detect the UPF path failure using the heartbeat messages involves the following steps:

1. The SMF sends a heartbeat request message to the discovered UPF instances or profile groups based on the configured schedule.
2. If the UPF instance or profile is alive, it sends a heartbeat response to the SMF indicating that it is operational. In case the UPF does not send a heartbeat response, then SMF retransmits the heartbeat request based on the configured interval and the number of permitted attempts.
3. After the configured count of heartbeat message reattempts is exhausted and the SMF does not receive a response from UPF, then SMF starts 'Network requested PDU Session Release' procedure for the subscribers that are associated with that UPF.

### Heartbeat and high-availability in Node Manager

Each UPF instance is associated with a primary and secondary Node Manager. The secondary Node Manager acts as a standby system on which the primary manager fails over. The primary Node Manager is responsible for the IP allocation and managing the association-specific messages such as association create, update, or delete request. To achieve uninterrupted access to the UPF and ensure a high-availability environment, the following interactions occur:

- When the Node Manager goes down or reinstated, it updates its status to all the mapped UPFs.
- In case the primary Node Manager is down, the secondary manager is notified. The secondary manager sends a heartbeat request to the UPF node to determine if the node is alive.
- When the secondary Node Manager is informed that the primary Node Manager is available, the secondary manager suspends the heartbeat timers and retransmission for the UPF node that is managed by the primary Node Manager.

## Configuration Support for UPF Path Management and Restoration

This section describes how to configure the support for monitoring the UPF status.

Configuring the support for detecting the UPF status using the heartbeat feature involves the following steps:

- Configuring the Heartbeat Parameters for UPF
- Configuring the Heartbeat Parameters for UPF Profile
- Associating UPF Group to Individual UPF Network Configuration

### Configuring the Heartbeat Parameters for UPF

This section describes how to configure the heartbeat feature for UPF.

To configure the heartbeat feature for UPF at the interface-level, use the following configuration:

**config**

```

endpoint pfcf
  interface { n4 | sxa }
    heartbeat
      interval interval
      max-retransmissions max_retry_count
      retransmission-timeout retry_interval
    end

```

**NOTES:**

- **endpoint pfcf**: Enters the endpoint configuration mode.
- **interface**: Configures the N4 or Sxa interface over which the heartbeat messages are exchanged between SMF and UPF.
- **heartbeat**: Enters the heartbeat configuration.

- **interval** *interval*: Specify the heartbeat interval in seconds. The accepted range is 60–360. The default value is 60 seconds.

Setting the *interval* to "0" disables the heartbeat feature.

- **max-retransmissions** *max\_retry\_count*: Specify the maximum retries for the Packet Forwarding Control Protocol (PFCP) heartbeat request. The accepted range is 0–10. The default value is 3.
- **retransmission-timeout** *retry\_interval*: Specify the heartbeat retransmission timeout in seconds. The accepted range is 1–20. The default value is 5.

## Verifying the Heartbeat Configuration for UPF

This section describes how to verify the heartbeat configuration for UPF.

To view the configuration, use the **show running-config endpoint pfc** command.

The following is a sample output of the **show running-config endpoint pfc** command.

```
show running-config endpoint pfc

endpoint pfc
interface n4
  heartbeat
    interval          61
    retransmission-timeout 3
    max-retransmissions 5
  exit
exit

interface sxa
  heartbeat
    interval          300
    retransmission-timeout 15
    max-retransmissions 0
  exit
exit
exit
```

## Configuring the Heartbeat Parameters for the UPF Profile

This section describes how to configure the heartbeat feature for the UPF profile.

To configure the heartbeat parameters for the UPF profile, use the following configuration:

```
configure
  profile upf-group group_name
    heartbeat
      interval interval
      retransmission-timeout max_retry
      max-retransmissions retry_count
    end
```

### NOTES:

- **profile upf-group** *group\_name*— Specifies the UPF group for which the heartbeat feature must be enabled.

- **interface**— Configures the N4 interface over which the heartbeat messages are exchanged between SMF and UPF.
- **heartbeat** — Enters the heartbeat configuration.
- **interval** *interval*— Specifies the heartbeat interval in seconds. The accepted range is 60–360. The default value is 60 seconds.  
Setting the *interval* to "0", disables the heartbeat feature.
- **max-retransmissions** *max\_retry*— Specifies the maximum retries for the Packet Forwarding Control Protocol (PFCP) heartbeat request. The accepted range is 0–10. The default value is 3.
- **retransmission-timeout** *retry\_count*— Specifies the heartbeat retransmission timeout in seconds. The accepted range is 1–20. The default value is 5.

## Verifying the Heartbeat Configuration for UPF Group

This section describes how to verify the heartbeat configuration for the UPF group.

To view the configuration, use the **show running-config profile upf-group** command.

The following is a sample output of the **show running-config profile upf-group** command.

```
show running-config profile upf-group
profile upf-group upfGroup1
heartbeat
  interval                62
  retransmission-timeout  3
  max-retransmissions     2
exit
exit
```

## Associating UPF Group to Individual UPF Network Configuration

This section describes how to associate a UPF group with a UPF configuration.

Each UPF network configuration includes the UPF profile that associates each UPF instance with a UPF profile.

To associate an UPF group profile with a network configuration, use the following sample configuration:

```
config
  profile network-element upf upf_profile_name
    upf-group-profile upf_group
  end
```

### NOTES:

- **profile network-element upf** *upf\_profile\_name*: Configure the UPF network configuration.
- **upf-group-profile** *upf\_group*: Configures the UPF group name that must be associated to the specified UPF network configuration.

## Verifying the Association of the UPF Group with the Individual UPF

This section describes how to verify the association of the UPF group with the individual UPF.

To view the association, use the **show running-config profile network-element upf** command.

The following is a sample output of the **show running-config profile network-element upf** command.

```
profile network-element upf upf1
n4-peer-address ipv4 10.80.70.229
n4-peer-port      8805
upf-group-profile upfGroup1
dnn-list          [ intershat intershat1 intershat2 ]
capacity          65535
priority          65535
```

## OAM Support

This section describes the operations, administration, and maintenance information for this feature.

### Bulk Statistics

The SMF maintains the following bulk statistics triggered during the heartbeat request and response procedure.

- `nodemgr_upf_heartbeat_fail_stats`— Counter that gets updated per UPF when it fails to respond to a heartbeat request.
- `nodemgr_upf_hb_msg_stats`— Counter for all the heartbeat messages for the specified UPF.

The `nodemgr_upf_heartbeat_fail_stats` counter supports the following labels:

- `upf_heartbeat_req_tx`— Label for the heartbeat request that the SMF sends.
- `upf_heartbeat_req_retx`— Label for the retransmitted heartbeat request.
- `upf_heartbeat_rsp_rx`— Label for the heartbeat response that the SMF receives.



# CHAPTER 51

## Voice over New Radio

- [Feature Summary and Revision History, on page 761](#)
- [Feature Description, on page 762](#)
- [VoNR P-CSCF Address Support, on page 762](#)
- [VoNR MO and MT Call Support, on page 770](#)
- [Paging Policy Differentiation Support, on page 779](#)
- [P-CSCF FQDN, on page 783](#)

## Feature Summary and Revision History

### Summary Data

*Table 228: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 229: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

New Radio (NR) is the 5G radio access technology, and Voice over NR (VoNR) is the voice or video over the 5G network. VoNR is the target voice or video communication solution for 5G networks.

Voice services in 5GS over NG-RAN continue to be based on IP Multimedia Subsystem (IMS), such as Voice over LTE (VoLTE). VoNR is supported only when 5GS is connected to the IMS core.

## Standards Compliance

The VoNR feature complies with the following standards:

- 3GPP TS 23.228, Release 15.3.0
- 3GPP TS 23.501, Release 15.4.0
- 3GPP TS 23.502, Release 15.4.0

## VoNR P-CSCF Address Support

### Feature Description

The SMF supports IMS Protocol Data Unit (PDU) Session Creation and fetches the P-CSCF addresses to be sent to the UE during initial attach over NR.

### How it Works

The serving PLMN AMF sends an indication toward the UE during the registration procedure to indicate whether an IMS voice over PS session is supported in the 3GPP access network. A UE with "IMS voice over PS" voice capability over 3GPP access takes this indication into account when performing voice domain selection. The UE includes extended Protocol Configuration Options (ePCO) IE in "PDU Session Establishment Request" by setting P-CSCF container options in the AMF. Further, the AMF forwards these ePCO IE options in smContextCreate Request towards the SMF. The SMF fetches the P-CSCF addresses based on DNN profile, which maintains IMS-related data. The SMF includes P-CSCF IPv4 and IPv6 address in N1N2Message Transfer towards the AMF as per PDN-Types and requested P-CSCF container values.



#### Important

The SMF does not include the P-CSCF address if the UE does not set the P-CSCF container options in the ePCO IE.

### Call Flows

This section describes the call flow that is associated with this feature.

#### *VoNR PDU Session Creation Call Flow*

This section describes the VoNR PDU Session Creation call flow.



Figure 129: VoNR PDU Session Creation Call Flow

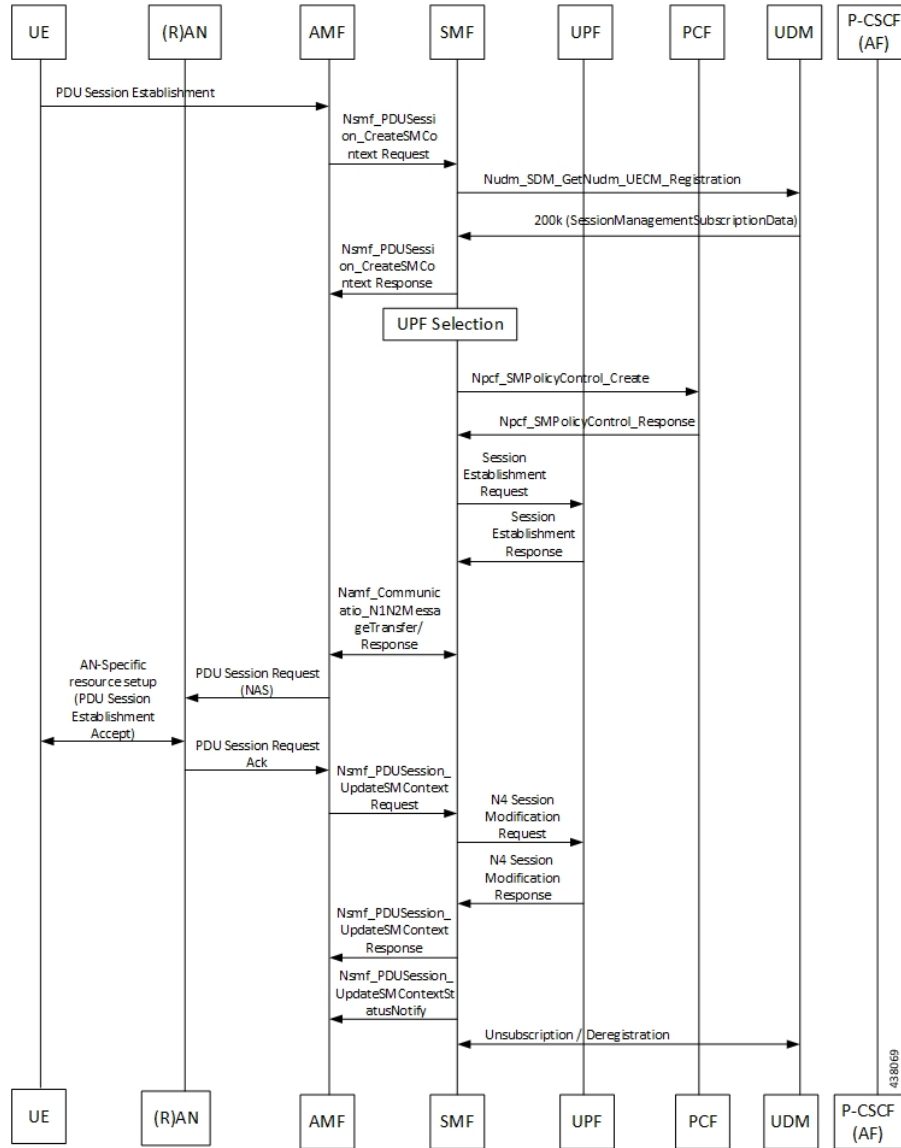


Table 230: VoNR PDU Session Creation Call Flow Description

Step	Description
1	Based on the UE registration with the RAN and the AMF, the UE set to "voice centric" for 5GS ensures that the voice service is always available. The UE selects the respective DNN for IMS. The UE initiates N1-Message with "PDU Session Establishment Request" by including container identifier "P-CSCF IPv4/IPv6 Request" in ePCO IE. <b>Note</b> The DNN can be common for both the "voice" and "data" centric services.
2	The AMF performs the SMF selection as described in 3GPP TS 23.501.

Step	Description
3	The AMF sends Nsmf_PDUSession_CreateSMContext Request to the SMF by including N1 and N2 Message as Multipart along with ePCO IE if it is received from the UE in “PDU Session Establishment Request”.
4	<p>The SMF fetches the session management subscription data for the corresponding SUPI, DNN, and S-NSSAI. If it is not available locally, the SMF retrieves the subscription data using Nudm_SDM_Get and subscribes for the subscription data change notification using Nudm_SDM_Subscribe. The UDM retrieves this information from UDR using Nudr_DM_Query and subscribes to the notifications from the UDR for the same data by Nudr_DM_subscribe. The S-NSSAI used with the UDM is the S-NSSAI with value for the HPLMN.</p> <p>The SMF uses the DNN Selection Mode to decide the retrieval of session management subscription data. If the SMF is not subscribed for subscription data (DNN, S-NSSAI), then the SMF uses local configuration instead of session management subscription data.</p>
5	The UDM provides the subscription details to the SMF. Based on the local configuration or session management subscription data from UDM for the respective DNN, the “IMS Voice over PS” is supported.
6	The SMF sends Nsmf_PDUSession_CreateSMContext Response (Cause, SM Context ID, or N1 SM container (PDU Session Reject (Cause))) by processing the PDU Session Establishment Request. The SMF creates an SM context and responds to the AMF by providing an SM Context Identifier.
7	The SMF also selects one or more UPFs based on SSC mode, PDU Session-Type, and voice or data-centric services based on DNN capabilities.
8	The SMF initiates “Npcf_SMPolicyControl_Create” Request by including “SmPolicyContextData”, which contains Supi, pduSessionId, ratType, servingNetwork, userLocationInfo, ueTimezone, Pei, Online/Offline charging, chargingcharacteristics, PDU Session-Type, allocated UE IP address/prefix(es), subsDefQos, and information.
9	<p>The PCF responds back with “Npcf_SMPolicyControl_CreateResponse (200 OK)” by including “SmPolicyDecision” in the message to the SMF. “SmPolicyDecision” contains the sessionRules, pccRules, qosDecs, chgDecs, chargingInfo, traffConDecs, umDecs, qosChars, and so on as defined in the <i>3GPP TS 29.512, section 5.6.2.4</i>. All these parameters are only applicable for “IMS Voice over PS session”. This section does not cover Data and Voice PDU sessions.</p> <p><b>Note</b> When a UE initiates a Resource Modification Request, and if the SMF includes the "qosFlowUsage" attribute containing "IMS_SIG" within SmPolicyUpdateContextData data structure and the PCF accepts that a QoS flow dedicated to IMS signaling can be used, the PCF returns the "qosFlowUsage" containing "IMS_SIG" value within the SmPolicyDecision data structure. The PCC rules provided have the 5QI applicable for IMS signaling.</p>
10	The SMF initiates “N4 Session Establishment Request” to the UPF and provides packet detection, enforcement, and reporting rules to be installed on the UPF for this PDU session.
11	The UPF acknowledges by sending an N4 Session Establishment Response. If CN Tunnel Info is allocated by the UPF, the CN Tunnel Info is provided to SMF in this step.

Step	Description
12	<p>The SMF sends Namf_Communication_N1N2MessageTransfer to the SMF. This transfer message includes the PDU Session ID, N2 SM information (PDU Session ID, QFI(s), QoS Profile(s), CN Tunnel Info, S-NSSAI from the Allowed NSSAI, Session-AMBR, PDU Session Type, User Plane Security Enforcement information, UE Integrity Protection Maximum Data Rate), N1 SM container (PDU Session Establishment Accept (QoS Rule(s) and QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with the QoS rule(s), selected SSC mode, S-NSSAI(s), DNN, allocated IPv4 address, interface identifier, Session-AMBR, selected PDU Session Type, Reflective QoS Timer (if available), P-CSCF address(es), and [Always-on PDU Session])).</p> <p>The N1 SM container contains the PDU Session Establishment Accept that the AMF provides to the UE. If the UE requested P-CSCF discovery, then the message also includes the P-CSCF IP addresses as determined by the SMF.</p> <p>The SMF fetches these P-CSCF addresses from DNN configuration, which are locally provisioned under DNN with IMS-Support and list of P-CSCF addresses or P-CSCF FQDN.</p>
13	The AMF sends N2 PDU Session Request (N2 SM information, NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept))) to (R)AN.
14	<p>The (R)AN issues AN-specific signaling exchange to the UE that is related with the information received from the SMF. The (R)AN also allocates (R)AN N3 Tunnel Info for the PDU session.</p> <p>The (R)AN forwards the NAS message (PDU Session ID, N1 SM container (PDU Session Establishment Accept)) that was provided in Step 12 to the UE. The (R)AN provides the NAS message only if the necessary (R)AN resources are established and the allocation of (R)AN Tunnel Info is successful.</p>
15	<p>The (R)AN sends N2 PDU Session Response (PDU Session ID, Cause, N2 SM information (PDU Session ID, AN Tunnel Info, List of accepted/rejected QFI(s), User Plane Enforcement Policy Notification)) to the AMF. The AN Tunnel Info corresponds to the Access Network address of the N3 tunnel corresponding to the PDU session.</p> <p>If the (R)AN rejects QFI(s) the SMF is responsible of updating the QoS rules and QoS flow-level QoS parameters if needed for the QoS flow associated with the QoS rule(s) in the UE accordingly.</p> <p>The NG-RAN rejects the establishment of UP resources for the PDU session when it cannot fulfill User Plane Security Enforcement information with a value of Required. The SMF releases the PDU session and the NG-RAN sends notification to the SMF when it cannot fulfill a User Plane Security Enforcement with a value of Preferred.</p>
16	<p>The AMF sends Nsmf_PDUSession_UpdateSMContext Request (N2 SM information, Request Type) to the SMF. The AMF forwards the N2 SM information received from (R)AN to the SMF. If the list of rejected QFI(s) is included in N2 SM information, the SMF releases the rejected QFI(s) associated QoS profiles.</p> <p>If the User Plane Enforcement Policy Notification in the N2 SM information indicates that no user plane resources can be established, and the User Plane Enforcement Policy indicated "required" as described in <i>3GPP TS 23.501, section 5.10.3</i>, the SMF releases the PDU session.</p>
17	The SMF initiates an N4 Session Modification procedure with the UPF. The SMF provides AN Tunnel Info to the UPF and the corresponding forwarding rules.
18	The UPF provides an N4 Session Modification Response to the SMF.

Step	Description
19	The SMF sends Nsmf_PDUSession_UpdateSMContext Response (Cause) to the AMF.
20	(Conditional) The SMF sends Nsmf_PDUSession_SMContextStatusNotify (Release) to the AMF.
21	If during the procedure, any time after Step 5, the PDU Session Establishment is not successful, the SMF informs the AMF by invoking Nsmf_PDUSession_SMContextStatusNotify (Release). The SMF also releases any N4 session(s) created, any PDU session address if allocated (for example, IP address) and releases the association with PCF, if any.

## Limitations

Currently, only up to 64 address lists can be configured for both P-CSCF IPv4 and IPv6 addresses.

## Configuring the VoNR P-CSCF Address Support

This section describes how to configure VoNR P-CSCF Address Support.

Configuring VoNR P-CSCF Address Support involves the following steps:

1. Creating P-CSCF Profile
2. Configuring P-CSCF Server Selection Method
3. Configuring P-CSCF Server Parameters
4. Defining P-CSCF Profile in DNN Profile Configuration

### Creating P-CSCF Profile

Use the following configuration to create a P-CSCF profile instance:

```
configure
  profile pcscf pcscf_profile_name
end
```

#### NOTES:

- **pcscf** *pcscf\_profile\_name*: Specifies the P-CSCF profile. This command creates a P-CSCF profile and provides access to the P-CSCF Profile Configuration mode. For details on the commands supported in this mode, see the *pcscf-profile* section in this document. *pcscf\_profile\_name* must be an alphanumeric string.

### Configuring P-CSCF Server Selection

Use the following configuration to configure the P-CSCF server selection method:

```
configure
  profile pcscf pcscf_profile_name
    pcscf-selection round-robin
  end
```

#### NOTES:

- **pcscf-selection round-robin**: Configures the P-CSCF server selection method. Currently, round-robin is the only supported algorithm for the server selection.
- This command performs the round-robin selection of P-CSCF server based on the configured precedence value.

## Configuring P-CSCF IPv4 Server

Use the following configuration to configure the P-CSCF IPv4 server:

```
configure
  profile pcscf pcscf_profile_name
    v4-list
  end
```

### NOTES:

- **v4-list**: Prompts you to configure the P-CSCF IPv4 server details.
- Entering the **v4-list** command takes you to the P-CSCF IPv4 Server Configuration mode. For details on the commands supported in this mode, see the *CLI Reference Content*.

## Configuring P-CSCF Server IPv4 Addresses

Use the following sample configuration to configure the IPv4 address of the primary, secondary, and tertiary P-CSCF servers.

```
config
  profile pcscf pcscf_profile_name
    v4-list
      precedence precedence_value
      primary server_ipv4_address
      secondary server_ipv4_address
      tertiary server_ipv4_address
    end
```

### NOTES:

- **precedence precedence\_value**: Specify the precedence value. *precedence\_value* must be an integer in the range of 1-64. This precedence value is used for the round-robin selection of P-CSCF server. The lower the precedence, the higher the priority.
- **primary server\_ipv4\_address**: Specify the IPv4 address of the primary P-CSCF server in dotted-decimal notation.
- **secondary server\_ipv4\_address**: Specify the IPv4 address of the secondary P-CSCF server in dotted-decimal notation.
- **tertiary server\_ipv4\_address**: Specify the IPv4 address of the tertiary P-CSCF server in dotted-decimal notation.

## Configuring P-CSCF IPv6 Server

Use the following configuration to configure the P-CSCF IPv6 server:

```

configure
  profile pcscf pcscf_profile_name
    v6-list
  end

```

**NOTES:**

- **v6-list:** Prompts you to configure the P-CSCF IPv6 server details.
- Entering the **v6-list** command prompts you to the P-CSCF IPv6 Server Configuration mode. For details on the commands supported in this mode, see the *CLI Reference* section.

**Configuring P-CSCF Server IPv6 Addresses**

Use the following sample configuration to configure the IPv6 address of the primary, secondary, and tertiary P-CSCF servers.

```

config
  profile pcscf pcscf_profile_name
    v6-list
      precedence precedence_value
      primary server_ipv6_address
      secondary server_ipv6_address
      tertiary server_ipv6_address
    end

```

**NOTES:**

- **precedence precedence\_value:** Specify the precedence value. *precedence\_value* must be an integer in the range of 1-64. This precedence value is used for the round-robin selection of P-CSCF server. The lower the precedence, the higher the priority.
- **primary server\_ipv6\_address:** Specify the IPv6 address of the primary P-CSCF server in colon-separated hexadecimal notation.
- **secondary server\_ipv6\_address:** Specify the IPv6 address of the secondary P-CSCF server in colon-separated hexadecimal notation.
- **tertiary server\_ipv6\_address:** Specify the IPv6 address of the tertiary P-CSCF server in colon-separated hexadecimal notation.

**Configuring P-CSCF IPv4v6 Server**

Use the following configuration to configure the P-CSCF IPv4v6 server:

```

configure
  profile pcscf pcscf_profile_name
    v4v6-list
  end

```

**NOTES:**

- **v4v6-list:** Prompts you to configure the P-CSCF IPv4v6 server details.
- Entering the **v4v6-list** command takes you to the P-CSCF IPv4v6 Server Configuration mode. For details on the commands supported in this mode, see the *CLI Reference* section.

## Configuring P-CSCF Server IPv4v6 Addresses

Use the following sample configuration to configure the IPv4v6 address of the primary, secondary, and tertiary P-CSCF servers.

```

config
  profile pcscf pcscf_profile_name
    v4v6-list
      precedence precedence_value
        primary ipv4 server_ipv4_address ipv6 server_ipv6_address
        secondary { [ ipv4 server_ipv4_address ] [ ipv6 server_ipv6_address ] }
      }
      tertiary { [ ipv4 server_ipv4_address ] [ ipv6 server_ipv6_address ] }
    }
  end

```

### NOTES:

- **precedence** *precedence\_value*: Specify the precedence value. *precedence\_value* must be an integer in the range of 1-64. This precedence value is used for the round-robin selection of P-CSCF server. The lower the precedence, the higher the priority.
- **primary ipv4** *server\_ipv4\_address* **ipv6** *server\_ipv6\_address*: Specify the IPv4 and IPv6 address of the primary P-CSCF server in dotted-decimal notation and colon-separated hexadecimal notation respectively.
- **secondary** { [ **ipv4** *server\_ipv4\_address* ] [ **ipv6** *server\_ipv6\_address* ] }: Specify the IPv4 and IPv6 address of the secondary P-CSCF server in dotted-decimal notation and colon-separated hexadecimal notation respectively.
- **tertiary** { [ **ipv4** *server\_ipv4\_address* ] [ **ipv6** *server\_ipv6\_address* ] }: Specify the IPv4 and IPv6 address of the tertiary P-CSCF server in dotted-decimal notation and colon-separated hexadecimal notation respectively.

## Defining P-CSCF Profile in DNN Profile Configuration

Use the following configuration to configure the P-CSCF profile in the existing DNN profile configuration:

```

configure
  profile dnn dnn_profile_name
    pcscf-profile pcscf_profile_name
  end

```

### NOTES:

- **pcscf-profile** *pcscf\_profile\_name*: This command defines the P-CSCF profile to be associated with the DNN profile. *pcscf\_profile\_name* must be the name of the configured P-CSCF profile.

## Verifying the Feature Configuration

Use the following show command to verify the P-CSCF FQDN feature configuration.

```
show running-config
```

The following is an example of the output of this show command:

```

profile pcscf pcscf1
fqdn cisco.com
v4-list

```

```
precedence 3
primary 3.3.3.1
secondary 3.3.3.2
exit
precedence 5
primary 5.5.5.1
secondary 5.5.5.2
exit
```

# VoNR MO and MT Call Support

## Feature Description

The SMF supports Mobile Originated (MO) and Mobile Terminated (MT) VoNR with 5G QoS Identifier (5QI) as Guaranteed Bit Rate (GBR) flow for UE after the IMS PDU Session Creation. The SMF further supports VoNR calls for the following mobility (inter gNB, inter AMF) scenarios:

- MO and MT calls for idle mode UE
- MO and MT calls when the UE is handing over

During the mobility scenario of VoNR MO and MT calls, make sure to consider the following points:

- VoNR GBR flows are supported during UE and network service request procedures, Xn and N2 based handover.
- QoS failures at N1 and N2 interface, which are rejected by UE and gNB, are not handled by SMF.
- Charging features are not integrated with VoNR MO and MT, and mobility features.

## Call Flows

This section describes the call flows associated with this feature.

### VoNR MO Call Handling Procedure

This section describes the VoNR MO call handling procedure.



Figure 130: VoNR MO Call Handling Flow

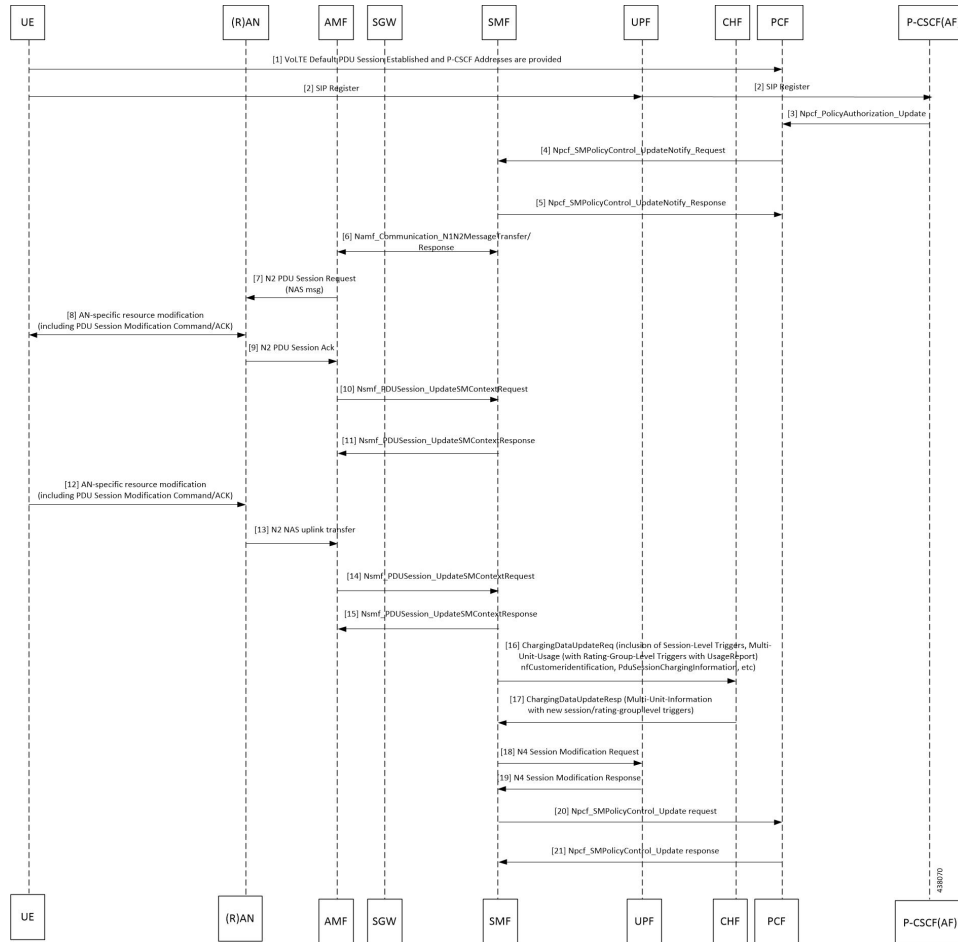


Table 231: VoNR MO Call Handling Flow Description

Step	Description
1	The SMF performs the PDU Session Establishment as described in the <a href="#">VoNR PDU Session Creation Call Flow, on page 762</a> section.
2	The UE initiates SIP Registration towards the called-party via UPF, P-CSCF through the backed IMS core network.
3	P-CSCF sends “Npcf_PolicyAuthorization_Update” to PCF to enforce policies, modify service information, gate control, modify subscription to SDF notification/deactivation, updating of traffic routing information, and so on (as defined in <i>3GPP TS 29.514</i> ). This service allows the NF consumer to subscribe and unsubscribe the notification of events (for example, change of Access Type, RAT type, or changes of the PLMN identifier).
4	The PCF sends Npcf_SMPolicyControl_UpdateNotify request to update and/or delete the PCC rule(s) PDU session-related policy context at the SMF and Policy Control Request Trigger information. This enforces PCC rules, policy control request triggers, SDF, and charging related information.

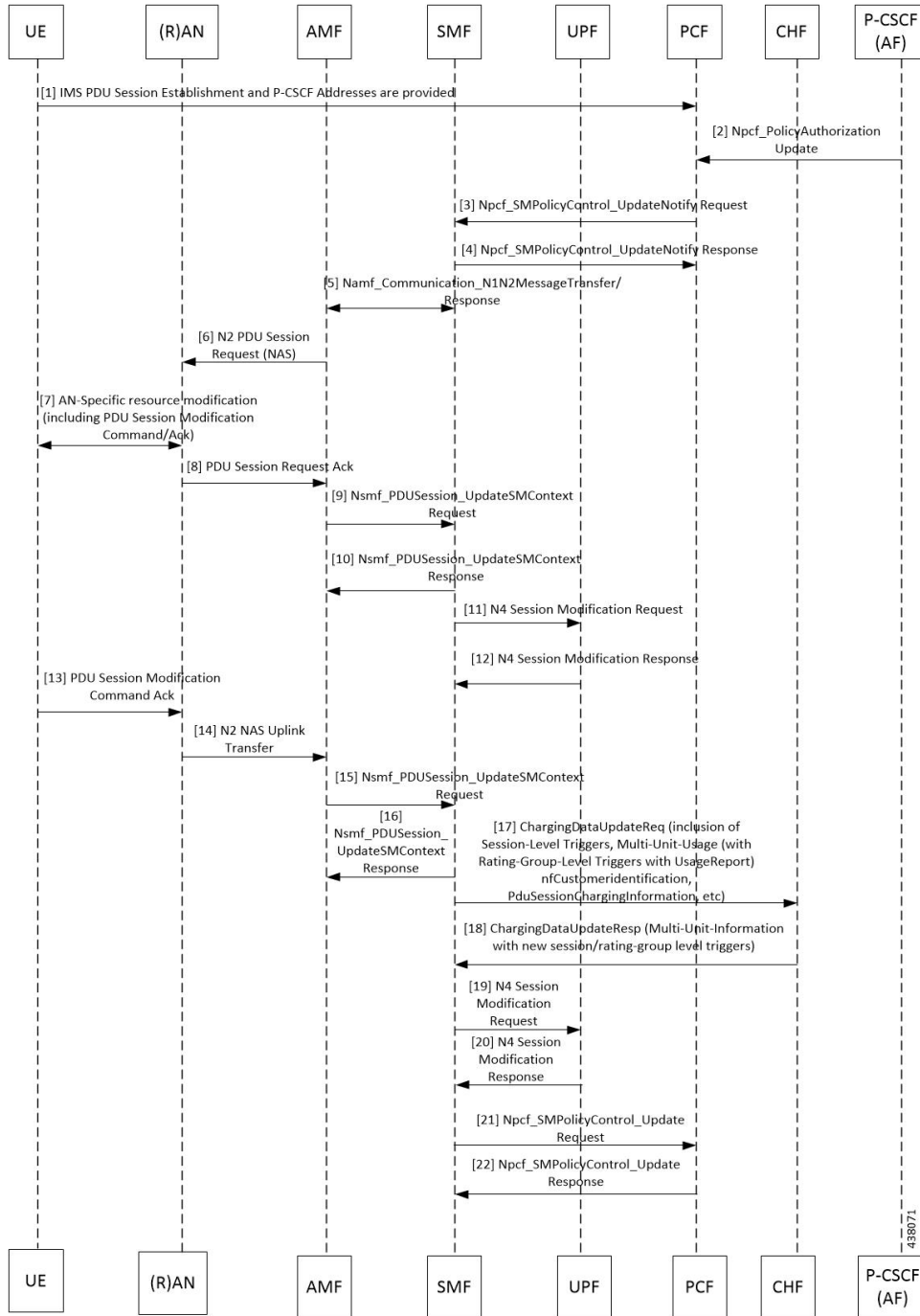
Step	Description
5	The SMF processes the received PCC rules and sends 200 OK message for a successful scenario. When the processing of any content fails, the SMF includes "400 Bad Request" in "Npcf_SMPolicyControl_UpdateNotify request" and sends it along with appropriate cause value as defined in <i>3GPP TS 29.512</i> .
6	The SMF sends Namf_Communication_nN1N2MessageTransfer/Response (PDU Session ID, QFIs, QoS Profile(s), Session-AMBR), N1 SM container (PDU Session Modification Command (PDU Session ID, QoS rule(s), QoS Flow level parameters if needed for the QoS Flow(s) associated with the QoS rule(s), QoS rule operation, and QoS Flow level QoS parameters operation, Session-AMBR))).  If the UE is in CM-IDLE state or Mobility handover (HO) state, see the procedure in <a href="#">VoNR MO Call Flow for UE in Idle Mode, on page 774</a> .
7	The AMF sends N2 PDU Session Request (N2 SM information received from SMF, NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command))) message to the (R)AN.
8	The (R)AN issues AN specific signalling exchange with the UE that is related with the information received from SMF. For example, in an NG-RAN, an RRC Connection Reconfiguration takes place with the UE modifying the necessary (R)AN resources related to the PDU session.
9	The (R)AN acknowledges N2 PDU Session Request by sending a N2 PDU Session ACK (N2 SM information (List of accepted/rejected QFIs, AN Tunnel Info, PDU Session ID, Secondary RAT usage data), User Location Information) message to the AMF. In case of Dual Connectivity, if one or more QFIs were added to the PDU session, the master RAN node assigns one or more of these QFIs to an NG-RAN node which was not involved in the PDU session earlier. In this case, the AN Tunnel Info includes a new N3 tunnel endpoint for QFIs assigned to the new NG-RAN node. Correspondingly, if one or more QFIs were removed from the PDU session, a (R)AN node may no longer be involved in the PDU session anymore, and the corresponding tunnel endpoint is removed from the AN Tunnel Info. The NG-RAN rejects QFIs if it cannot fulfill the User Plane Security Enforcement information for a corresponding QoS Profile, for example, due to the UE Integrity Protection Maximum Data Rate being exceeded.
10	The AMF forwards the N2 SM information and the User Location Information received from the (R)AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation.  If the (R)AN rejects QFIs, the SMF updates the QoS rules and QoS parameters if needed for the QoS flow(s) associated with the QoS rule(s) in the UE accordingly.
11	The SMF sends an Nsmf_PDUSession_UpdateSMContext Response. N2 SM information includes Secondary RAT Usage Data.
12	The UE acknowledges the PDU Session Modification Command by sending a NAS message (PDU Session ID, N1 SM container (PDU Session Modification Command ACK)) message.
13	The (R)AN forwards the NAS message to the AMF.
14	The AMF forwards the N1 SM container (PDU Session Modification Command ACK) and User Location Information received from the (R)AN to the SMF via Nsmf_PDUSession_UpdateSMContext service operation.

Step	Description
15	The SMF sends an Nsmf_PDUSession_UpdateSMContext Response.  If the SMF-initiated modification is to delete QoS Flows (for example, triggered by PCF) which do not include QoS Flow associated with the default QoS rule and the SMF does not receive response from the UE, the SMF marks that the status of those QoS Flows is to be synchronized with the UE.
16	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
17	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides parameter changes for Session-Level and Rating-Group values.
18	The SMF updates N4 session of the UPF(s) that are involved in the PDU Session Modification by sending N4 Session Modification Request (N4 Session ID) message to the PCF. For a PDU Session of Ethernet PDU Session Type, the SMF notifies the PCF to add or remove Ethernet Packet Filter Set(s) and forwarding rule(s).  The UPFs that are impacted in the PDU Session Modification procedure depend on the modified QoS parameters and the deployment. For example, in case of the session AMBR of a PDU Session with UL flow classifier (CL) changes, only the UL CL is involved.
19	The PCF sends an N4 session modification response message containing any information that the PCF has to provide to the SMF in response to the control information received.
20	For PCF-initiated policy modification case, the SMF notifies the PCF whether the PCC decision could be enforced or not by performing an SMF-initiated SM Policy Association Modification procedure as defined in <i>3GPP TS 23.502, section 4.16.5.1</i> . The SMF notifies any entity that has subscribed to User Location Information related with PDU Session change.
21	The PCF sends an Npcf_SMPolicyControl_Update response with updated policy information about the PDU session.

### VoNR MT Call Handling Procedure

This section describes the VoNR MT call handling procedure.

Figure 131: VoNR MT Call Handling Flow

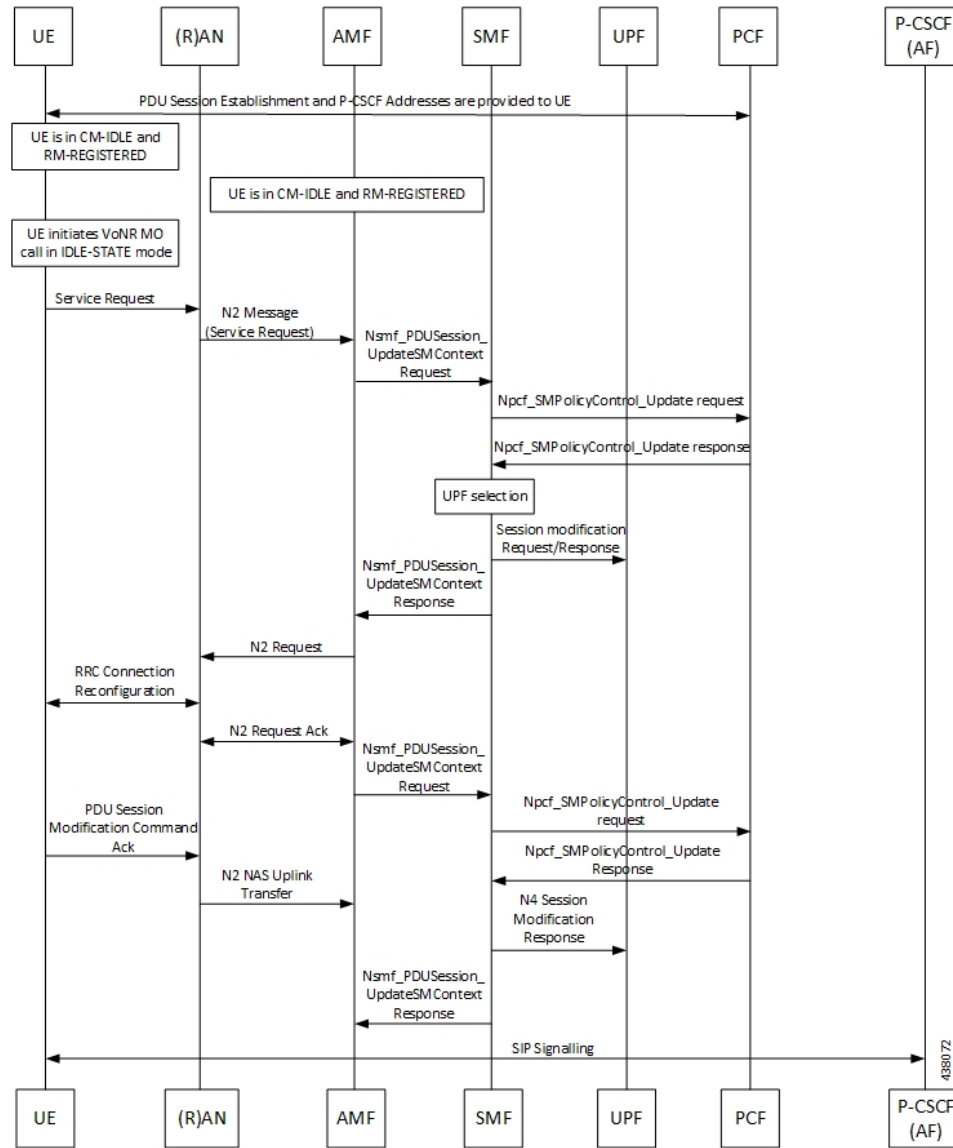


The VoNR MT call handling procedure remains the same as the VoNR MO call handling procedure except for the SIP Registration Request initiated from UE to P-CSCF(AF) through the UPF.

VoNR MO Call Flow for UE in Idle Mode

This section describes the VoNR MO call handling procedure when the UE is in idle mode.

Figure 132: VoNR MO Call Handling Flow for UE in Idle Mode



Step	Description
1	The SMF performs the PDU session establishment as described in <a href="#">VoNR PDU Session Creation Call Flow, on page 762</a> section, and fetches the P-CSCF addresses for sending it to the UE. The SMF programs UPF with Paging Policy Differentiation (PPD) for the respective PDU session as part of N4 interface by provisioning flows, and traffic detection information for every PDR.
2	The UE maintains its state in CM-IDLE and RM-REGISTERED.
3	The UPF maintains the UE in CM-IDLE and RM-REGISTERED state.
4	The UE initiates the VoNR call in CM-IDLE state.
5	The UE performs Service-Request procedures as defined in <i>3GPP TS 23.502</i> .

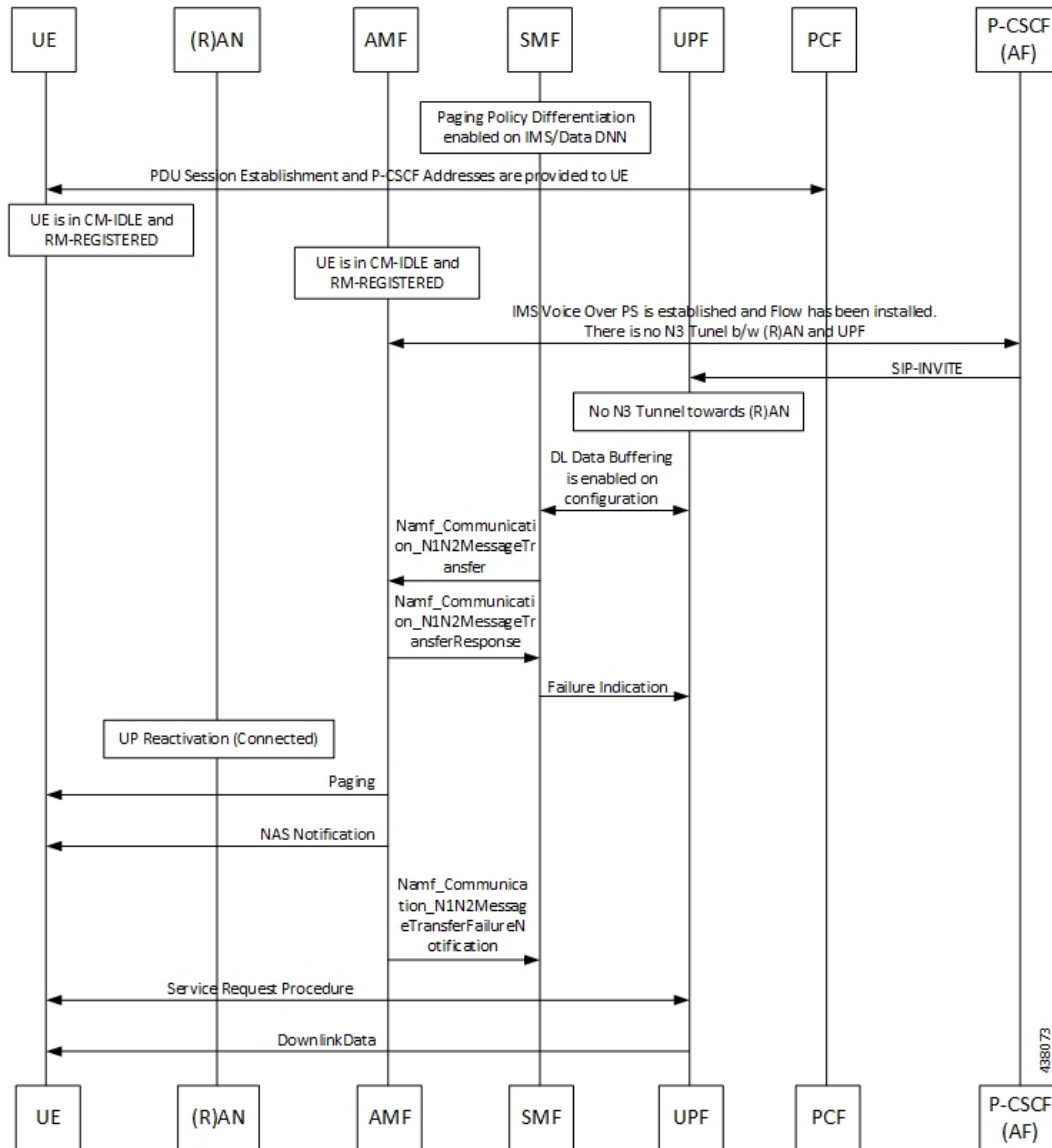
Step	Description
6	The RAN sends N2 message (service request) to the AMF.
7	The AMF sends Nsmf_PDUSession_UpdateSMContext Request (PDU Session ID(s), Operation Type, UE Location information, Access Type, RAT Type, UE presence in LADN service area, Indication of Access Type can be changed) to the SMF.
8	If the AMF notifies the SMF that the access type of the PDU session can be changed, and if the PCC is deployed, the SMF performs an SMF-initiated SM Policy Association Modification procedure as defined in <i>3GPP TS 23.502</i> , Section 4.16.5.1.
9	The PCF provides the updated PCC Rule(s) to the SMF.
10	The SMF performs the UPF selection. <b>Note</b> Selection of multiple or other UPFs is currently not supported.
11	The SMF initiates an N4 Session Modification request to the UPF. The SMF provides (R)AN Tunnel Info and the corresponding forwarding rules to the UPF. The UPF provides an N4 Session Modification Response to the SMF.
12	The SMF sends Nsmf_PDUSession_UpdateSMContext Response (N2 SM information (PDU Session ID, QFI(s), QoS profile(s), CN N3 Tunnel Info, S-NSSAI, User Plane Security Enforcement, UE Integrity Protection Maximum Data Rate), N1 SM Container, Cause) to the AMF. The SMF sends N1 SM Container and/or N2 SM Information to the AMF when applicable.
13	The AMF sends N2 Request (N2 SM information received from SMF, security context, Mobility Restriction List, Subscribed UE-AMBR, MM NAS Service Accept, list of recommended cells, TAs, NG-RAN node identifiers, UE Radio Capability, Core Network Assistance Information, Tracing Requirements) to the (R)AN.
14	The NG-RAN performs RRC Connection Reconfiguration with the UE depending on the QoS Information for all the QoS Flows of the PDU sessions whose UP connections are activated, and Data Radio Bearers.
15	The (R)AN sends N2 Request Acknowledgement message (N2 SM information (AN Tunnel Info, List of accepted QoS Flows for the PDU Sessions whose UP connections are activated, List of rejected QoS Flows for the PDU Sessions whose UP connections are activated), PDU Session ID) to the AMF.  The N2 Request ACK message includes N2 SM information, for example, AN Tunnel Info. NG-RAN responds N2 SM information with separate N2 message (for example, N2 tunnel setup response) if the AMF sends separate N2 message.
16	The AMF sends Nsmf_PDUSession_UpdateSMContext Request (N2 SM information, RAT Type, Access Type) per PDU Session to the SMF. The AMF determines Access Type and RAT Type based on the Global RAN Node ID associated with the N2 interface. If the AMF received N2 SM information (one or multiple), then the AMF forwards the N2 SM information to the relevant SMF per PDU Session ID. If the UE Time Zone has changed compared to the last reported UE Time Zone, then the AMF includes the UE Time Zone IE in this message.

Step	Description
17	The SMF notifies the PCF whether the PCC decision could be enforced or not by performing an SMF-initiated SM Policy Association Modification procedure as defined in <i>3GPP TS 23.502</i> , Section 4.16.5.1. The SMF notifies any entity that has subscribed to User Location Information related with PDU Session change.
18	The PCF sends an Npcf_SMPolicyControl_Update response with updated policy information about the PDU session.
19	<p>The SMF updates N4 session of the UPF(s) that are involved in the PDU session modification by sending N4 Session Modification Request (N4 Session ID) message to the UPF. For a PDU session of Ethernet PDU Session Type, the SMF notifies the UPF to add or remove Ethernet Packet Filter Set(s) and forwarding rule(s).</p> <p>The UPFs that are impacted in the PDU Session Modification procedure depend on the modified QoS parameters and the deployment. For example, in case of the session AMBR of a PDU session with UL CL changes, only the UL CL is involved.</p> <p>The UPF sends an N4 session modification response message containing any information that the UPF has to provide to the SMF in response to the control information received.</p>
20	The SMF sends a Nsmf_PDUSession_UpdateSMContext Response. The N2 SM information includes Secondary RAT Usage Data.

### VoNR MT Call Flow for UE in Idle Mode

This section describes the VoNR MT call handling procedure when the UE is in idle mode.

Figure 133: VoNR MT Call Flow for UE in Idle Mode



The VoNR MT call flow remains the same as the VoNR MO call flow for service request when the UE is in CM-IDLE state except the following:

- The SIP-INVITE received by P-CSCF
- The PCC rule enforcements triggered from PCF towards SMF.



**Note**

The PCC rules, QoS, PDR, and traffic detection rule enforcements remain the same as the VoNR MT Call Handling procedure as defined in [VoNR MT Call Handling Procedure, on page 773](#) VoNR MT Call Handling Procedure.



When the AMF receives Namf\_Communication\_N1N2MessageTransfer Request (N2 SM information (PDU Session ID, QFI(s), QoS Profile(s), Session-AMBR), N1 SM container (PDU Session Modification Command (PDU Session ID, QoS rule(s), QoS Flow level parameters if needed for the QoS Flow(s) associated with the QoS rule(s), QoS rule operation, and QoS Flow level parameters operation, Session-AMBR))) when the UE is in CM-IDLE state. If the UE is in CM-IDLE state and an Asynchronous type communication (ATC) is activated, the AMF updates and stores the UE context based on the Namf\_Communication\_N1N2MessageTransfer.

The AMF performs paging operations to the UE, and the UE triggers service request procedure. Once the paging is established, the AMF decides QoS Flows, QoS rules, and Session-AMBR that need to be accepted, which are received in Namf\_Communication\_N1N2MessageTransfer Request and the AMF performs Nsmf\_PDUSession\_UpdateSMContext operation with SMF to notify on accepting the QoS Flows, QoS rules, session-AMBR, and so on.

# Paging Policy Differentiation Support

## Feature Description

The SMF supports Paging Policy Differentiation feature by providing a configuration at PLMN, DNN, and 5QI level for data and IMS DNN sessions of the UE. The SMF provides Paging Policy Indicator based on UPF data. The SMF also supports QoS flow (PPI, ARP, and 5QI) towards the AMF over N11 interface.

## Call Flows

This section describes the call flows associated with this feature.

### VoNR Paging Policy Differentiation Procedure

This section describes the VoNR Paging Policy Differentiation procedure.

Figure 134: VoNR Paging Policy Differentiation Call Flow

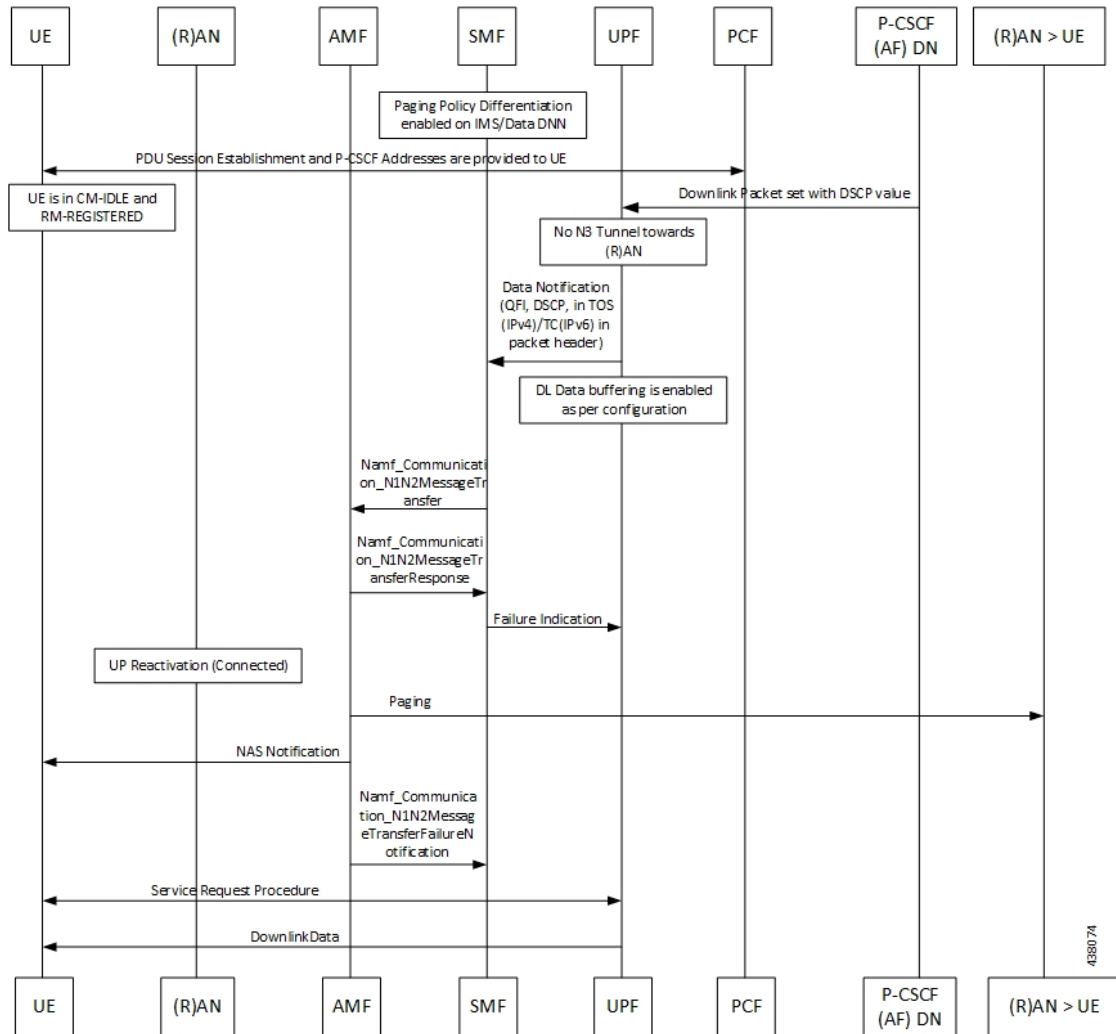


Table 232: VoNR Paging Policy Differentiation Call Flow Description

Step	Description
1	The SMF enables Paging Policy Differentiation (PPD) under DNN profile based on DNN, 5QI, and PLMN.
2	The SMF performs the PDU session establishment as described in <a href="#">VoNR PDU Session Creation Call Flow</a> section, and fetches the P-CSCF addresses for sending it to the UE. The SMF programs UPF with PPD for the respective PDU session as part of N4 interface by provisioning flows, and traffic detection information for every PDR.
3	The UPF detects if any Downlink (DL) Packet is set with DSCP value (TOS in IPv4 / TC in IPv6) when PPD is enabled for the PDU session.
4	The UPF detects that there is no forwarding path as there is no N3 Tunnel for the DSCP marked DL packets.

Step	Description
5	The UPF sends Data-Notification (QFI, DSCP in TOS (IPv4) / TC (IPv6) in packet header).
6	<p>The UPF enables DL Data buffering based on the buffering configuration. The UPF sends Data Notification (N4 Session ID, Information to identify the QoS Flow for the DL data packet, DSCP) message to the SMF.</p> <ol style="list-style-type: none"> <li>1. On arrival of the first DL data packet for any QoS Flow, the UPF sends Data Notification message to the SMF, if the SMF has not previously notified the UPF (in which case the next steps are skipped).</li> <li>2. If the UPF receives DL data packets for another QoS Flow in the same PDU session, the UPF sends another Data Notification message to the SMF.</li> <li>3. If the Paging Policy Differentiation feature (as specified in <i>3GPP TS 23.501, section 5.4.3</i>) is supported by the UPF and if the PDU Session type is IP, the UPF includes the DSCP in TOS (IPv4) / TC (IPv6) value from the IP header of the DL data packet and the information to identify the QoS Flow for the DL data packet.</li> <li>4. The SMF sends the Data Notification Acknowledgement message to the UPF.</li> <li>5. The UPF forwards the DL data packets towards the SMF on request. The SMF buffers the data packets.</li> </ol>
7	<p>The SMF determines the AMF and invokes the Namf_Communication_N1N2MessageTransfer to the AMF including the PDU Session ID based on N4 Session ID. The SMF, while waiting for the User Plane Connection to be activated, receives additional Data Notification message.</p> <p>The SMF derives a different Paging Policy Indicator according to the additional Data Notification or the DSCP of the data packet. The SMF invokes a new Namf_Communication_N1N2MessageTransfer indicating the higher priority or different Paging Policy Indicator to the AMF.</p> <p>When supporting Paging Policy Differentiation, the SMF determines the Paging Policy Indicator related to the downlink data that has been received from the UPF or triggered the Data Notification message, based on the DSCP as described in <i>3GPP TS 23.501, section 5.4.3</i>. The SMF indicates the Paging Policy Indicator in the Namf_Communication_N1N2MessageTransfer.</p>
8	The AMF sends Namf_Communication_N1N2MessageTransfer response to the SMF with a cause "Attempting to reach UE" if the UE is in CM_IDLE State. If the UE is in CM-CONNECTED state, then the AMF sends a Namf_Communication_N1N2MessageTransfer response to the SMF immediately with a cause "N1/N2 transfer success".
9	The SMF sends Failure Indication to the UPF on receiving a negative response from AMF.
10	The AMF initiates paging towards the UE through the (R)AN.
11	The AMF initiates NAS Notification towards the UE.
12	The AMF notifies the SMF by sending Namf_Communications_N1N2MessageTransfer Failure Notification to the Notification Target Address provided by the SMF if the UE does not respond to paging. The AMF is unaware of an ongoing Mobility Management (MM) procedure that prevents the UE from responding. The AMF receives an N14 Context Request message indicating that the UE performs Registration procedure with another AMF.

Step	Description
13	If the UE is in CM-IDLE state, upon receiving a paging request for a PDU session associated to 3GPP access, the UE initiates the UE Triggered Service Request procedure as defined in <i>3GPP TS 23.502, section 4.2.3.2</i> .

## Configuring the VoNR Paging Profile Differentiation

This section describes how to configure VoNR Paging Profile Differentiation feature.

Configuring VoNR Paging Profile Differentiation feature involves the following steps:

1. Creating PPD Profile
2. Configuring PPD Profile Parameters
3. Enabling PPD in DNN Profile Configuration

### Creating PPD Profile

Use the following configuration to create an instance of PPD profile:

```
configure
  profile ppd ppd_profile_name
end
```

#### NOTES:

- **ppd** *ppd\_profile\_name*: Specifies the PPD profile. This command creates a PPD profile and provides access to the PPD Profile Configuration mode. For details on the commands supported in this mode, see the *ppd-profile* section in this document. *ppd\_profile\_name* must be an alphanumeric string.

### Configuring PPD Profile Parameters

Use the following configuration to define the PPD profile parameters:

```
configure
  profile ppd ppd_profile_name
    5qi 5qi_value
    dscp dscp_value { ppi ppi_value }
  end
```

#### NOTES:

- **5qi**: Specifies the list of 5QI Priority Level. *5qi\_value* must be an integer in the range of 0-127. To list the different priority levels, use comma and hyphen as needed. For example, 5QI 3,10-15,65.
- **dscp** *dscp\_value*: Specifies the DSCP value. *dscp\_value* must be an integer in the range of 0-63.
- **ppi** *ppi\_value*: Specifies the paging policy indicator value. *ppi\_value* must be an integer in the range of 0-7.

### Enabling PPD in DNN Profile Configuration

Use the following configuration to enable the PPD feature in the existing DNN profile configuration:

```
configure
  profile dnn dnn_profile_name
    ppd-profile ppd_profile_name
  end
```

**NOTES:**

- **ppd-profile** *ppd\_profile\_name*: This command defines the PPD profile to be associated with the DNN profile. *ppd\_profile\_name* must be the name of the configured PPD profile.
- This command enables the PPD feature in the DNN profile based on the configured values of DNN, 5QI, and PLMN.

## Verifying the Feature Configuration

Use the following show command to verify the feature configuration details.

**show running-config**

The following is an example of the output of this show command:

```
product smf# show running-config
profile dnn dnntst1
pcscf-profile pcscf1
!
```

## P-CSCF FQDN

### Feature Description

The SMF sends the DNS queries to the DNS server through the DNS proxy server to fetch a maximum of two P-CSCF IP addresses. This operation helps in resolving the Fully Qualified Domain Name (FQDN) of the P-CSCF. This release provides the configuration support for the P-CSCF FQDN within the SMF profile.

For more information on the configuration commands, see the [Configuring the P-CSCF FQDN, on page 783](#) section.

### Relationships

The P-CSCF FQDN feature works only when the DNS proxy is configured. For more information on the DNS proxy configuration, see the *DNS Proxy Integration in SMF* chapter.

## Configuring the P-CSCF FQDN

Use the following configuration to define the FQDN of the P-CSCF.

```
configure
  profile pcscf pcscf_profile_name
    fqdn domain_name
  end
```

**NOTES:**

- **pcscf-profile** *pcscf\_profile\_name*: Specifies the P-CSCF profile name, and enters into the P-CSCF Profile Configuration mode. *pcscf\_profile\_name* must be an alphanumeric string.
- **fqdn** *domain\_name*: Specifies the FQDN of the P-CSCF server. *domain\_name* must be an alphanumeric string.

## Verifying the Feature Configuration

Use the following show command to verify the feature configuration details.

### **show running-config**

The following is an example of the output of this show command:

```
profile ppd ppdtemp
5QI 3,10-15,65
dscp 15 ppi 2
dscp 20 ppi 3
!
profile dnn ims
ppd-profile ppdtemp
!
```



# CHAPTER 52

## VoLTE Support

- [Feature Summary and Revision History, on page 785](#)
- [Feature Description, on page 785](#)

### Feature Summary and Revision History

#### Summary Data

*Table 233: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 234: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

### Feature Description

The SMF supports Voice over Long-Term Evolution or LTE (VoLTE). The VoLTE technology utilizes IP Multimedia Subsystem (IMS) to allow you to make cellular calls over the LTE access network.

## How it Works

A 5G mobile device with LTE access requests voice services to communicate with PGW-C over S-GW and MME resulting in the establishment of a PDU session. The P-GW supports a non-GBR bearer with QCI flows as 5 for VoLTE sessions. This support allows IMS signaling along with P-CSCF, DNS IPv4, or DNS IPv6 addresses for end users. For mobile-originated (MO) or mobile-terminated (MT) calls, the Application Function (AF) provides policy authorization details to the PCF. The PCF then converts these details to GBR flows and PCC rules and sends them to PGW-C. The PGW-C then converts the GBR-flows to dedicated bearers by establishing the dedicated bearer creation procedure with UE. The PGW-C provisions the GBR with the QCI flow as 1 to UPF. By this provisioning, the UPF supports voice communication between the calling and called devices over IMS network elements.

As per the E-UTRAN Attach procedure, the MME triggers the GTPv2 Create Session Request to PGW-C over S-GW. This request includes the EPS Bearer Identity (EBI) value, ePCO options for P-CSCF and DNS IPv4 or DNS IPv6 containers, PDN-Type, and PAA options for IPv4 or IPv6 allocated address for end users. The P-GW then processes the received Create Session Request and communicates with various SBI interfaces to receive the following information:

- Subscription data from UDM by including PGW-C FQDN in the subscription request.
- Policy information from PCF by sending SM policy create request. Policy information includes details, such as PCC rules and Session-AMBR.
- Online and offline charging information from CHF by sending the charging create data request.

After communication with SBI interfaces, which are based on the local SMF profile configuration, the P-GW sends the GTPv2 Create Session Response to the end user over S-GW and MME. This response includes:

- PAA with IPv4 or IPv6 addresses that PGW-C IPAM module allocates
- ePCO option with P-CSCF
- DNS IPv4 or DNS IPv6 address based on DNN-Profile configuration
- Non-GRB with the QCI flow as 5 for IMS signaling

For an MO or MT call, if the PCF is provisioned for GBR with the QCI flow as 1 for end users, the P-GW converts these GBR flows to the dedicated bearer creation. The GBR flows include the flow information and the PCC rules in the SM Policy Update Notify Request. The dedicated bearer is created by sending GTPv2 Create Bearer Request to UE over S-GW or MME. Another S5-U tunnel is created between S-GW and P-GW to allow GBE flow packets for the voice communication between the calling and called devices.

## Call Flows

This section describes the following call flows:

- VoLTE PDU Session Creation Call Flow
- VoLTE Mobile-Originated (MO) Call Creation Call Flow
- VoLTE Mobile-Terminated (MT) Call Creation Call Flow

### VoLTE PDU Session Creation Call Flow

To enable the connectivity through a 5G core, the initial attach on the E-UTRAN or EPS deviates from the defined 3GPP procedures in the following ways:



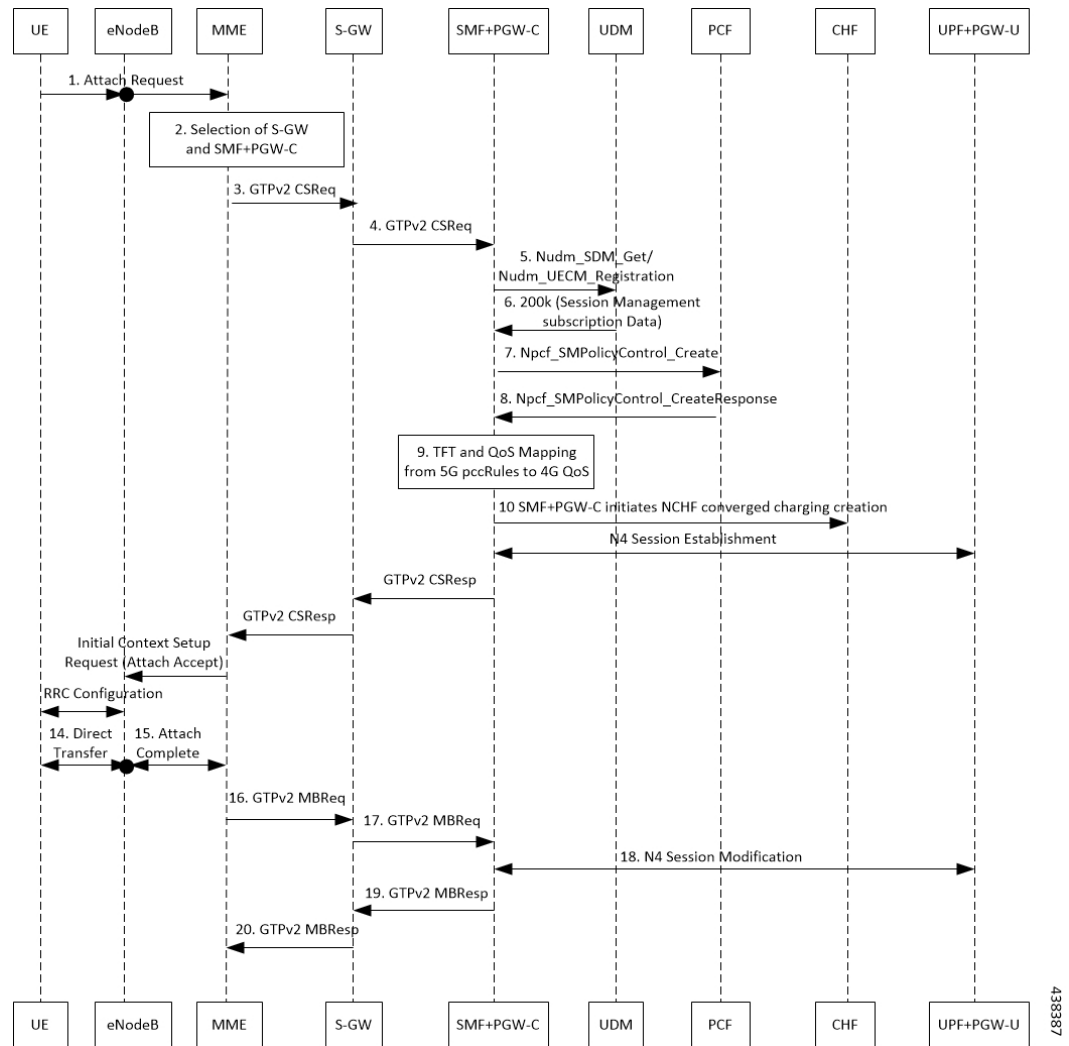
- An SMF+P-GW replaces the P-GW in the procedure.
- The SM Policy Association Establishment procedure replaces the IP-CAN Session Establishment and modification.
- The integrated charging over the NCHF interface with CHF replaces the online and offline charging functionality by using the Gy and Gz interfaces.
- Communication with the User Plane node happens over the N4 interface instead of the Sxb interface.



**Note** Depending on the mapped PCC rules, the SMF+PGW-C can initiate the dedicated bearer creation.

The following call flow depicts the creation of a VoLTE PDU session.

**Figure 135: VoLTE PDU Session Creation Call Flow**



438387

Table 235: VoLTE PDU Session Creation Call Flow Description

Step	Description
1	UE sends the attach request to MME through eNodeB.
2	MME determines if the UE is active and subscribed for the handoff to NR. Then, MME selects a SMF+PGW-C node as the P-GW for the PDU session.
3	MME sends the create session request to the selected S-GW and includes the selected SMF+PGW-C address in the request.
4	S-GW initiates the create session request toward SMF+PGW-C by including the “P-CSCF IPv4 or IPv6 request” container identifier in the extended PCO IE options.  SMF+PGW-C extracts and saves the PDU session ID that UE sends in the PCO option. Then, SMF+PGW-C performs a UDM registration and sends both the N11 and S5 or S8 interface ID to UDM. Based on the local configuration or the session management subscription data, which is received from UDM for respective DNN, SMF+PGW-C determines to support “IMS Voice over PS”.
5	SMF+PGW-C sends the NPCF SM policy control creation request to PCF to initiate the SM policy association establishment procedure. In this procedure, PGW-C+SMF includes the information elements that are received in the create session request message into the Npcf_SMPolicyControl_Create service. These elements comprise the following information: <ul style="list-style-type: none"> <li>• SUPI contains the IMSI.</li> <li>• DNN contains the APN.</li> <li>• PEI contains the IMEI-SV.</li> <li>• Session AMBR contains the APN-AMBR.</li> <li>• Default QoS information that contains the default EPS bearer QoS. The QCI values are mapped into 5QI values.</li> </ul>
6	PGW-C+SMF receives the PCC rules, PDU session policy information, and 5G QoS information. The PCC rules are mapped into EPS QoS information. The SMF+PGW-C creates TFT from the SDF filters that are received in the PCC rules. Then, SMF+PGW-C associates them with the corresponding default and dedicated bearers.
7	Based on the charging policies received from the PCF, the SMF+PGW-C initiates the NCHF converged charging creation procedure toward CHF. This procedure is based on the charging rules that are received from the PCF.
8	The SMF+PGW-C starts the UPF+PGW-U selection and N4 session establishment procedure. As this session is a 4G session that connects to the SMF+PGW-C, a separate CN tunnel is created for each bearer. Also, the QoS Flow Identifier (QFI) is not sent in the QoS Enforcement Rule (QER) and Packet Detection Rule (PDR).
9	The SMF+PGW-C sends create session response to the S-GW. This response includes the bearer information and the TEID for the default bearer. The SMF+PGW-C also includes the 5G QoS parameters in PCO options 001CH (QoS rules), 001DH (Session-AMBR), 001EH (PDU session address lifetime), and 001FH (QoS flow descriptions) to the UE.

Step	Description
10	Based on the charging policies received from PCF, the SMF+PGW-C initiates NCHF converged charging creation procedure toward CHF. This procedure is based on the charging rules that are received from PCF.
11	S-GW sends create session response to MME.
12	MME sends the Initial Context Setup Request to eNodeB with the N1 Attach Accept message.
13	eNodeB and UE perform the RRC configuration.
14	UE sends the direct transfer message to eNodeB.
15	eNodeB sends the attach completion message in the Initial Context Setup Response and the TEID of eNodeB to MME.
16	MME sends a modify bearer request to S-GW with eNodeB TEID.
17	S-GW sends the modify bearer request to SMF+PGW-C with eNodeB TEID.
18	SMF+PGW-C performs the N4 session modification to update the eNodeB TEID on the data path to the UPF+PGW-U.
19	SMF+PGW-C sends the modify bearer response to the S-GW.
20	S-GW sends the modify bearer response to MME.

### VoLTE Mobile-Originated (MO) Call Creation Call Flow

This section describes the VoLTE MO call creation call flow.

Figure 136: VoLTE MO Call Creation Call Flow

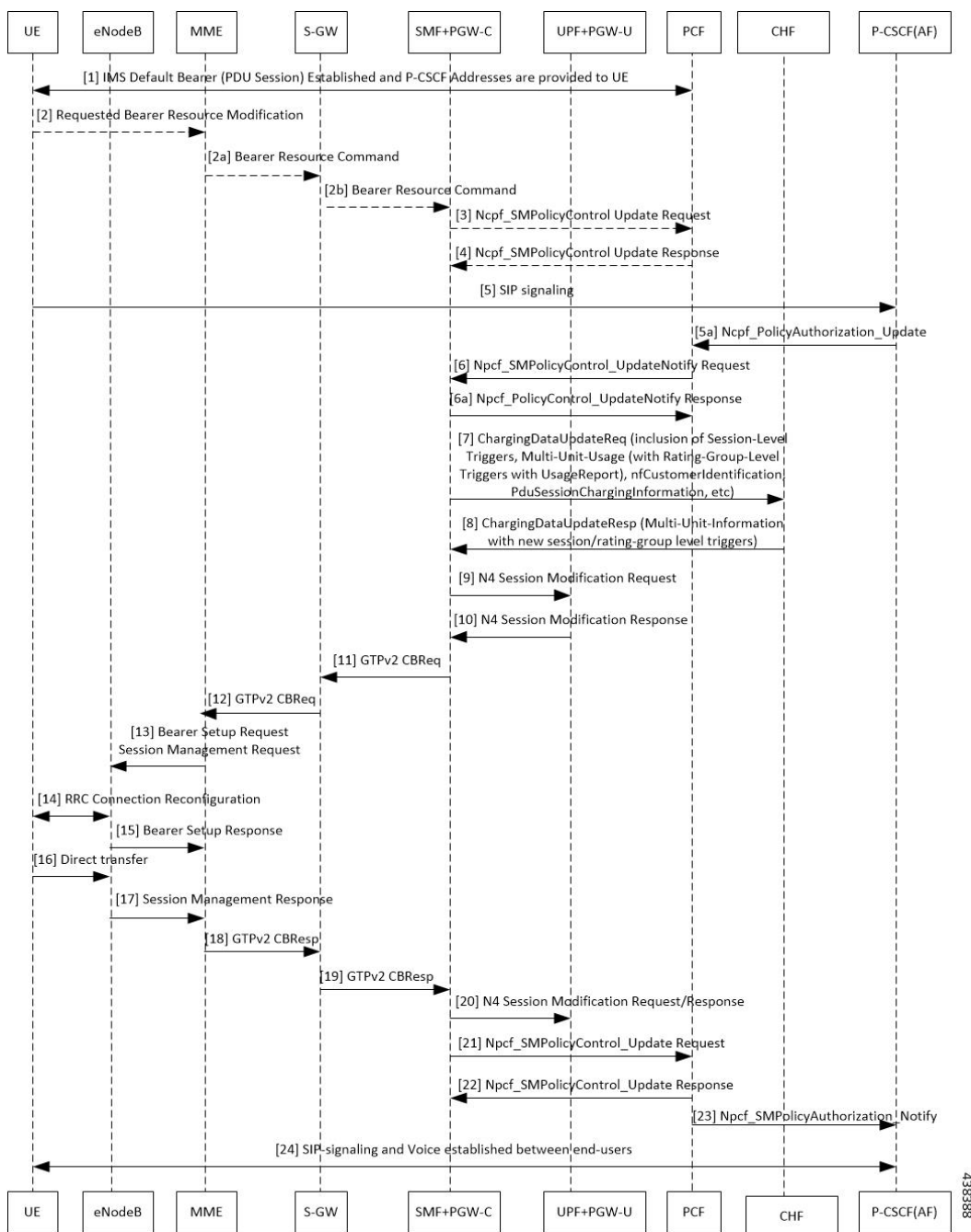


Table 236: VoLTE MO Call Creation Call Flow Description

Step	Description
1	UE requests for establishment of the IMS default bearer, PDU session, through PCF. After establishing the session, the UE receives the P-CSCF addresses from PCF.
2	UE sends the requested bearer resource modification information to MME.

Step	Description
2a	MME sends the bearer resource command to S-GW.
2b	S-GW sends the bearer resource command to SMF+PGW-C.
3	SMF+PGW-C sends the NPCF SM policy control update request to PCF.
4	PCF sends the NPCF SM Policy control update response back to SMF+PGW-C.
5	UE initiates SIP signaling toward P-CSCF (AF).
5a	P-CSCF sends NPCF Policy Authorization Update message to PCF through CHF.
6	PCF sends the NPCF SM policy control update notify request to SMF+PGW-C.
6a	SMF+PGW-C sends the NPCF SM Policy control update notify response back to PCF.
7	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
8	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides params changes for Session-Level and Rating-Group values.
9	SMF sends N4 Session Modification Request to the UPF by including Create ULPDRs and Create ULFARs. Create ULPDRs include SDFs and QER Info which are received as part of PCC Rule Installation.
10	UPF responds back with N4 Session Modification Response to SMF by including Created ULPDR and Created ULFAR. Create ULFAR contains UL Tunnel Information of UPF for the dedicated bearer creation.
11	SMF+PGW-C sends the GTPv2 create bearer request to S-GW.
12	S-GW sends the GTPv2 create bearer request to MME.
13	MME sends the bearer setup request and session management request to eNodeB.
14	RRC connection reconfiguration starts between UE and eNodeB.
15	The eNodeB sends the bearer setup response to MME.
16	UE initiates a direct transfer toward eNodeB.
17	eNodeB sends the session management response to MME.
18	MME sends the GTPv2 create bearer response to S-GW.
19	S-GW sends the GTPv2 create bearer response to SMF+PGW-C.
20	SMF+PGW-C sends the N4 session modification request or response to UPF+PGW-U.
21	SMF+PGW-C sends the NPCF SM policy control update request to PCF.
22	PCF sends the NPCF SM policy control update response back to SMF+PGW-C.
23	PCF sends the NPCF policy authorization notify request to P-CSCF (AF).
24	Establishes SIP-signaling and voice call between end-users through UE and P-CSCF (AF).

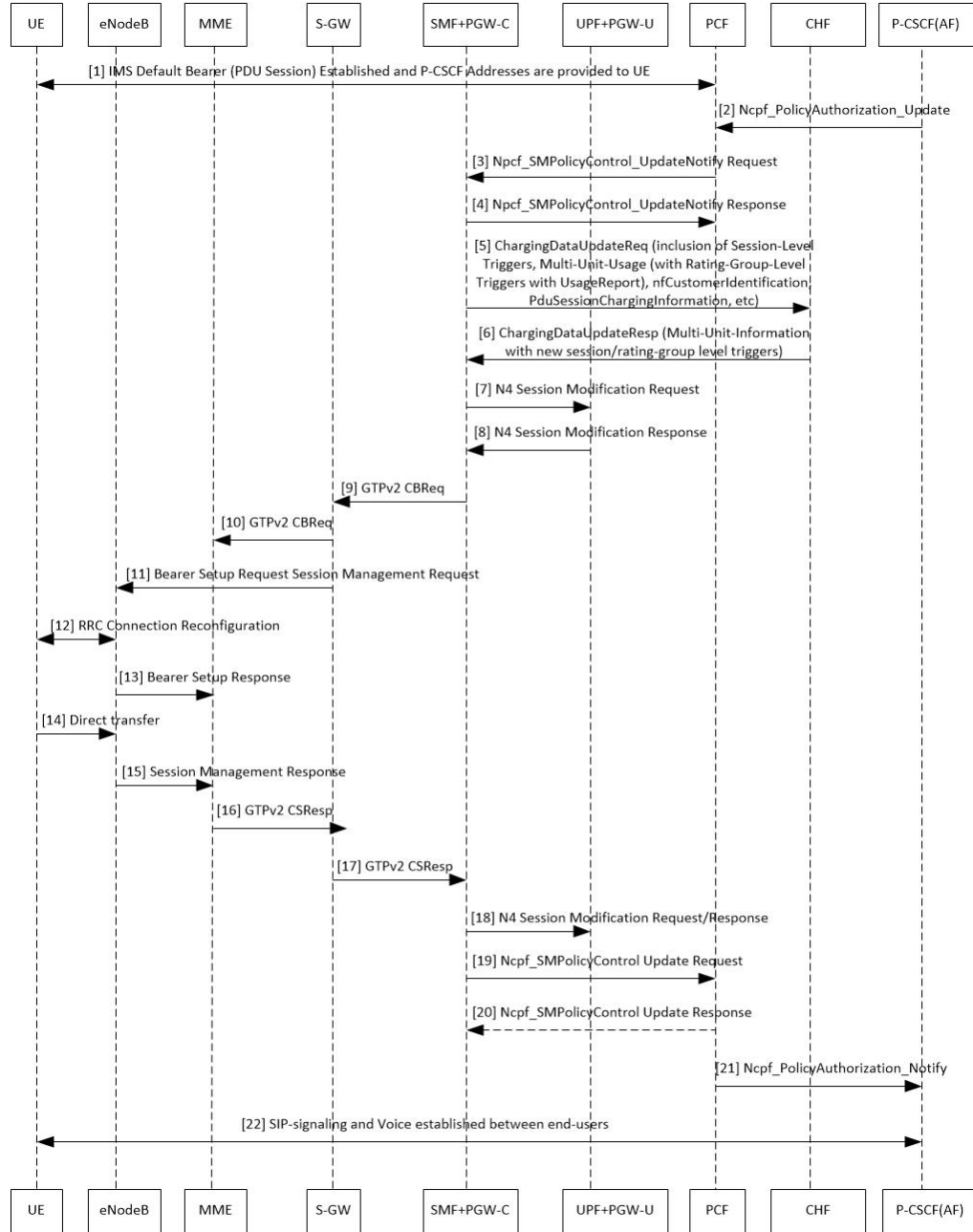
**Note**

- 
- The PCC rules that the PCF provides are mapped to TFTs for the new dedicated bearer. The associated QoS is mapped to 4G QoS.
  - The NCHF Converged Charging Update service procedures replace all the Gy and Gz interface messages.
  - The User Plane resources for dedicated bearers are added through the N4 Session Modification procedure towards the UPF. PDRs, QERs, and FARs are added for the SDF filters for the new dedicated bearer.
  - SMF+PGW-C saves the EBI for the dedicated bearer that is received in the create bearer response.
- 

**VoLTE Mobile-Terminated (MT) Call Creation Call Flow**

This section describes the VoLTE MT call creation call flow.

Figure 137: VoLTE MT Call Creation Call Flow



438389

Table 237: VoLTE MT Call Creation Call Flow Description

Step	Description
1	UE requests for establishment of the IMS default bearer, PDU session, through PCF. After establishing the session, the UE receives the P-CSCF addresses from PCF.
2	P-CSCF (AF) sends the NPCF policy authorization update to PCF.
3	PCF sends the NPCF SM Policy control update notify request to SMF+PGW-C.

Step	Description
4	SMF+PGW-C sends the NPCF SM Policy control update notify response to PCF.
5	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
6	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides params changes for Session-Level and Rating-Group values.
7	SMF sends N4 Session Modification Request to the UPF by including Create ULPDRs and Create ULFARs. Create ULPDRs include SDFs and QER Info which are received as part of PCC Rule Installation.
8	UPF responds back with N4 Session Modification Response to SMF by including Created ULPDR and Created ULFAR. Create ULFAR contains UL Tunnel Information of UPF for the dedicated bearer creation.
9	SMF+PGW-C sends the GTPv2 create bearer request to S-GW.
10	S-GW sends the GTPv2 create bearer request to MME.
11	MME sends the bearer setup request and session management request to eNodeB.
12	RRC connection reconfiguration starts between UE and eNodeB.
13	eNodeB sends the bearer setup response to MME.
14	UE initiates a direct transfer toward eNodeB.
15	eNodeB sends the session management response to MME.
16	MME sends the GTPv2 create bearer response to S-GW.
17	S-GW sends the GTPv2 create bearer response to SMF+PGW-C.
18	SMF+PGW-C sends the N4 session modification request or response to UPF+PGW-U.
19	SMF+PGW-C sends the NPCF SM policy control update request to PCF.
20	PCF sends the NPCF SM policy control update response back to SMF+PGW-C.
21	PCF sends the NPCF policy authorization notify request to P-CSCF (AF).
22	Establishes SIP-signaling and voice call between end-users through UE and P-CSCF (AF).

## Standards Compliance

The VoLTE support feature complies with the following standard:

- *3GPP TS 23.502 V15.2.0 (2018-09)*

## Limitations

The VoLTE support feature has the following limitations:

- The UE-initiated dedicated bearer creation is not supported.



- VoLTE is not integrated with charging.
- PCF-initiated modification is not supported to change the GBR flows and PCC rules. However, the addition and deletion of GBR flows are supported.





# CHAPTER 53

## VoWiFi Support

- [Feature Summary and Revision History, on page 797](#)
- [Feature Description, on page 797](#)

### Feature Summary and Revision History

#### Summary Data

*Table 238: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 239: Revision History*

Revision Details	Release
First introduced.	Pre-2020.02.0

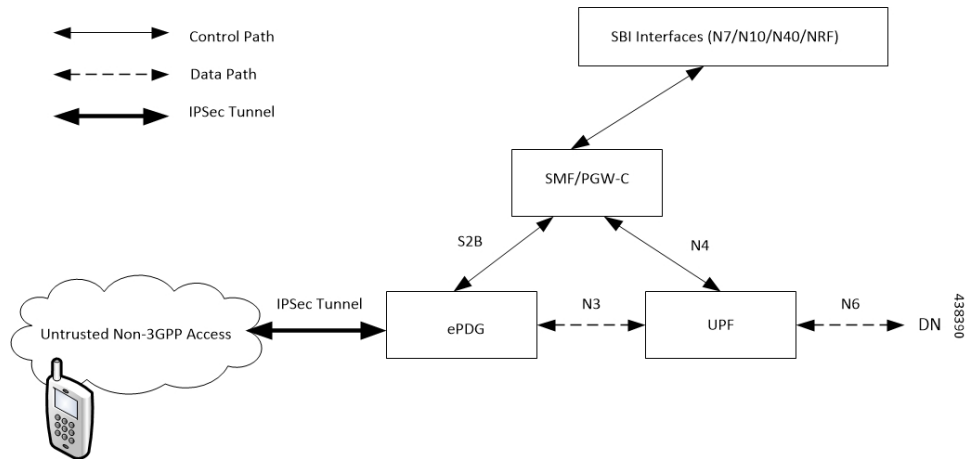
### Feature Description

The SMF supports Voice over Wi-Fi (VoWiFi). The VoWiFi technology provides the telephony services using Voice over IP (VoIP) from the mobile devices that are connected across a Wi-Fi network.

## Architecture

This section describes the VoWiFi architecture.

**Figure 138: VoWiFi Architecture**



## How it Works

A 5G mobile device connects through an untrusted Wi-Fi network for voice services to establish a PDN connection with PGW-C. This connection is established through Internet Key Exchange Protocol version 2 (IKEv2) protocol between the UE and enhanced Packet Data Gateway (ePDG). The P-GW receives the GTPv2 Create Session Request from an untrusted Wi-Fi ePDG over the S2b interface. The PGW-C then communicates with the SBI interfaces for creating the default and dedicated bearers. The SBI interfaces can be an N7, N10, N40, or an NRF interface.

## Call Flows

This section describes the following call flows:

- VoWiFi PDU Session Creation Call Flow
- VoWiFi Mobile-Originated (MO) Call Creation Call Flow
- VoWiFi Mobile-Terminated (MT) Call Creation Call Flow

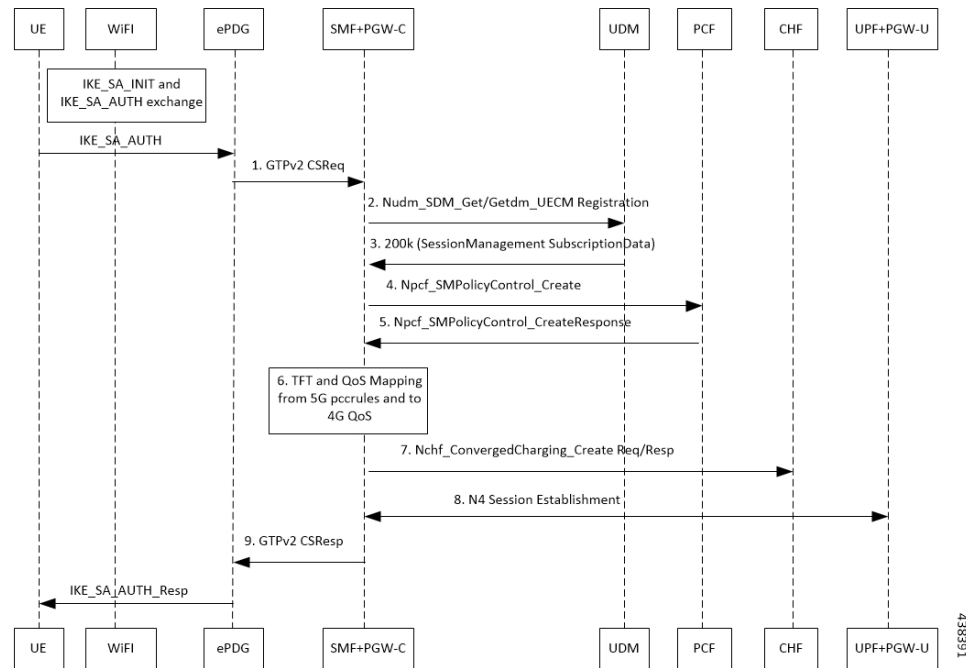
### VoWiFi PDU Session Creation Call Flow

To enable connectivity through a 5G core, the initial attach on the ePDG or EPS deviates from the defined 3GPP procedures in the following ways:

- An SMF+P-GW replaces the P-GW in the procedure.
- The SM Policy Association Establishment procedure replaces the IP-CAN Session Establishment and modification.
- The integrated charging over the NCHF interface with CHF replaces the online and offline charging functionality by using the Gy and Gz interfaces.
- Communication with the User Plane node happens over the N4 interface instead of the Sxb interface.

The following call flow depicts the creation of a VoWiFi PDU session.

**Figure 139: VoWiFi PDU Session Creation Call Flow**



**Table 240: VoWiFi PDU Session Creation Call Flow Description**

Step	Description
1	The UE initiates the IKE_SA_INIT and IKE_SA_AUTH exchange. The UE then sends the IKE_SA_AUTH exchange message to ePDG to create the IPsec tunnel.
2	The UE sends the IKE_SA_AUTH exchange message to the SMF+PGW-C as a GTP Create Session Request by including the "P-CSCF IPv4 or IPv6 request and DNS IPv4 or IPv6" container identifier in APCO IE Options.
3	The SMF+PGW-C extracts and saves the PDU Session ID that the UE sent in the APCO IE option. The SMF+PGW-C then performs a UDM registration and sends both the N11 and S2b interface IDs to UDM. Based on the local configuration or session management subscription data that is received from UDM for respective DNN, SMF+PGW-C determines to support "IMS Voice over PS".

Step	Description
4	<p>The SMF+PGW-C sends the NPCF SM Policy Control Creation Request to the PCF to initiate the SM Policy Association Establishment procedure. In this procedure, the PGW-C+SMF includes the information elements that are received in the Create Session Request message into the Npcf_SMPolicyControl_Create service. These elements comprise the following information:</p> <ul style="list-style-type: none"> <li>• SUPI contains the IMSI.</li> <li>• DNN contains the APN.</li> <li>• PEI contains the IMEI-SV.</li> <li>• Session AMBR contains the APN-AMBR.</li> <li>• Default QoS information that contains the default EPS bearer QoS. The QCI values are mapped into 5QI values.</li> </ul>
5	<p>The PGW-C+SMF receives the PCC rules, PDU session policy information, and 5G QoS information. The PCC rules are mapped into EPS QoS information. The SMF+PGW-C creates TFT from the SDF filters that are received in the PCC rules. The SMF+PGW-C then associates them with the corresponding default and dedicated bearers.</p>
6	<p>Based on the charging policies received from the PCF, the SMF+PGW-C initiates Nchf_ConvergedCharging_Create procedure toward CHF. This procedure is based on the charging rules that are received from the PCF.</p>
7	<p>The SMF+PGW-C starts the UPF+PGW-U selection and N4 Session Establishment procedure. As this session is a 4G session that connects to the SMF+PGW-C, a separate CN tunnel is created for each bearer. Also, the QoS Flow Identifier (QFI) is not sent in the QoS Enforcement Rule (QER) and Packet Detection Rule (PDR).</p>
8	<p>The eSMF+PGW-C sends Create Session Response to the ePDG. This response includes the bearer information and the TEID for the default bearer. The SMF+PGW-C also includes the 5G QoS parameters in APCO options 001CH (QoS rules), 001DH (Session-AMBR), 001EH (PDU session address lifetime), and 001FH (QoS flow descriptions) to the UE.</p>
9	<p>The ePDG sends IKE_SA_AUTH Response to the UE.</p> <p>Then, depending on the mapped PCC rules, the SMF+PGW-C initiates the dedicated bearer creation.</p>

### VoWiFi Mobile-Originated (MO) Call Creation Call Flow

This section describes the VoWiFi MO call creation call flow.

Figure 140: VoWiFi MO Call Creation Call Flow

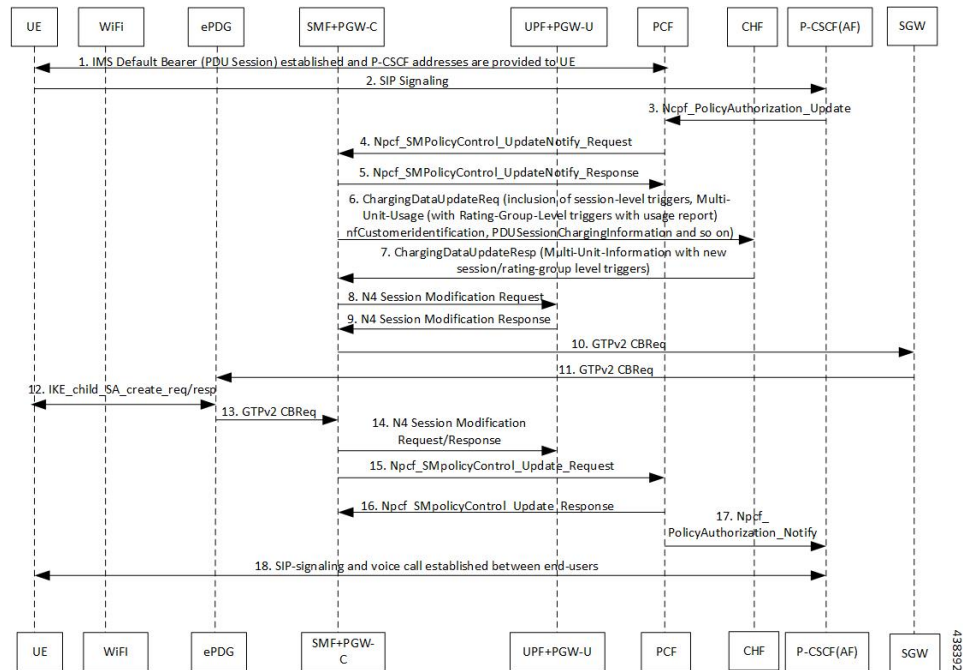


Table 241: VoWiFi MO Call Creation Call Flow Description

Step	Description
1	UE requests for establishment of the IMS default bearer, PDU session, through PCF. After establishing the session, the UE receives the P-CSCF addresses from PCF.
2	The UE initiates the SIP signaling toward P-CSCF (AF).
3	The P-CSCF (AF) sends the NPCF Policy Authorization Update message to the PCF.
4	The PCF sends the NPCF SM Policy Control Update Notify Request to the SMF+PGW-C.
5	The SMF+PGW-C sends the NPCF SM Policy Control Update Notify Response back to the PCF.
6	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
7	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides params changes for Session-Level and Rating-Group values.
8	SMF sends N4 Session Modification Request to the UPF by including Create UL PDRs and Create UL FARs. Create UL PDRs include SDFs and QER Info which are received as part of PCC Rule Installation.
9	UPF responds back with N4 Session Modification Response to SMF by including Created UL PDR and Created UL FAR. Create UL FAR contains UL Tunnel Information of UPF for the dedicated bearer creation.
10	The SMF+PGW-C sends the GTPv2 Create Bearer Request to the S-GW.

Step	Description
11	The S-GW sends the GTPv2 Create Bearer Request to the ePDG.
12	IKE_CHILD_SA exchange happens between the UE and ePDG.
13	The ePDG sends the GTPv2 Create Bearer Response back to the SMF+PGW-C.
14	The established N4 session is modified between SMF+PGW-C and UPF+PGW-C.
15	The SMF+PGW-C sends the NPCF SM Policy Control Update Request to the PCF.
16	The PCF sends the NPCF SM Policy Control Update Response back to the SMF+PGW-C.
17	PCF sends the NPCF policy authorization notify request to P-CSCF (AF).
18	Establishes SIP-signaling and voice call between end-users through UE and P-CSCF (AF).

**Note**

- The PCC rules that the PCF provides are mapped to TFTs for the new dedicated bearer. The associated QoS is mapped to 4G QoS.
- The NCHF Converged Charging Update Service procedures replace all the Gy and Gz interface messages.
- The User Plane resources for dedicated bearers are added through the N4 Session Modification procedure towards the UPF. PDRs, QERs, and FARs are added for the SDF filters for the new dedicated bearer.
- The SMF+PGW-C saves the EBI for the dedicated bearer that is received in the Create Bearer Response.

**VoWiFi Mobile-Terminated (MT) Call Creation Call Flow**

This section describes the Mobile-Terminated (MT) call flow.



Figure 141: VoWiFi MT Call Creation Call Flow

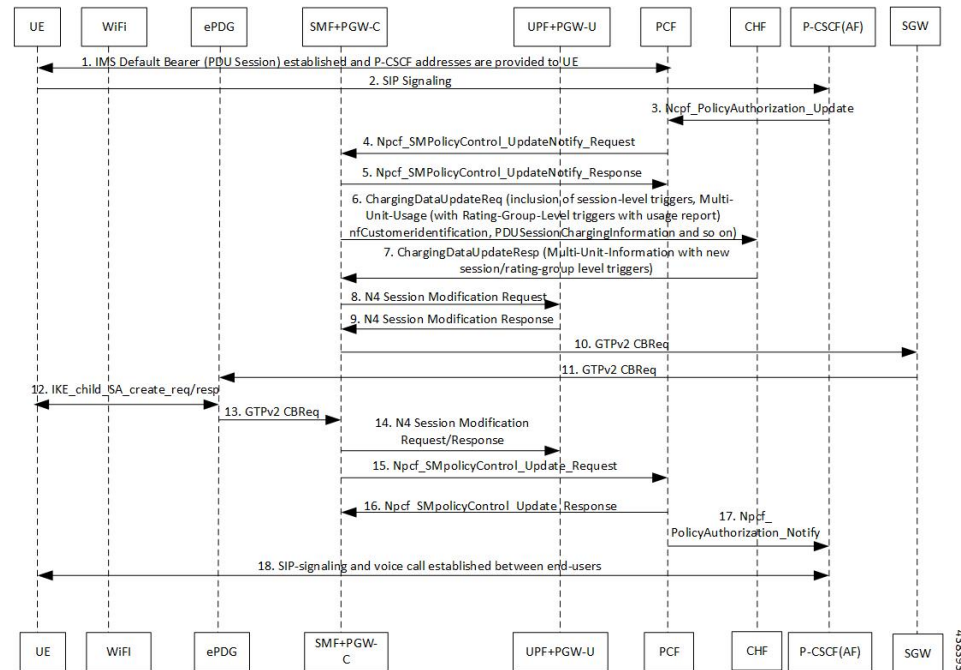


Table 242: VoWiFi MT Call Creation Call Flow Description

Step	Description
1	UE requests for establishment of the IMS default bearer, PDU session, through PCF. After establishing the session, the UE receives the P-CSCF addresses from PCF.
2	The UE-initiates the SIP signaling towards the P-CSCF (AF).
3	The P-CSCF (AF) sends the NPCF Policy Authorization Update message to the PCF.
4	The PCF sends the NPCF SM Policy Control Update Notify Request to the SMF+PGW-C.
5	The SMF+PGW-C sends the NPCF SM Policy Control Update Notify Response back to the PCF.
6	SMF sends ChargingDataUpdateReq by including Multi-Unit-Usage with Rating-Group-Id that are received as part of Charging_Description of Sm_PolicyControl_UpdateNotify_Request to install PCC Rules.
7	CHF provides ChargingDataUpdateResp with Multi-Unit-Information for received Rating-Group values in requested message. CHF also provides params changes for Session-Level and Rating-Group values.
8	SMF sends N4 Session Modification Request to the UPF by including Create UL PDRs and Create UL FARs. Create UL PDRs include SDFs and QER Info which are received as part of PCC Rule Installation.
9	UPF responds back with N4 Session Modification Response to SMF by including Created UL PDR and Created UL FAR. Create UL FAR contains UL Tunnel Information of UPF for the dedicated bearer creation.
10	The SMF+PGW-C sends the GTPv2 Create Bearer Request to the S-GW.

Step	Description
11	The S-GW sends the GTPv2 Create Bearer Request to the ePDG.
12	IKE_CHILD_SA exchange happens between the UE and ePDG.
13	The ePDG sends the GTPv2 Create Bearer Response back to the SMF+PGW-C.
14	The established N4 session is modified between SMF+PGW-C and UPF+PGW-C.
15	The SMF+PGW-C sends the NPCF SM Policy Control Update Request to the PCF.
16	The PCF sends the NPCF SM Policy Control Update Response back to the SMF+PGW-C.
17	PCF sends the NPCF policy authorization notify request to P-CSCF (AF).
18	Establishes SIP-signaling and voice call between end-users through UE and P-CSCF (AF).

## Standards Compliance

The VoWiFi support feature complies with the following standard:

- *3GPP TS 23.502 V15.2.0 (2018-09)*

## Limitations

In this release, the VoWiFi support feature has the following limitations:

- UE-initiated Dedicated Bearer Creation is not supported.
- VoWiFi is not integrated with charging.
- PCF-initiated modification is not supported to change the GBR flows and PCC rules. However, the addition and deletion of GBR flows are supported.
- Integration of charging is not supported.



# CHAPTER 54

## Wi-Fi Handovers

- [Feature Summary and Revision History, on page 805](#)
- [Feature Description, on page 806](#)
- [How it Works, on page 810](#)
- [Configuring the WiFi Handovers Feature, on page 825](#)

## Feature Summary and Revision History

### Summary Data

*Table 243: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 244: Revision History*

Revision Details	Release
TFT Handling for WiFi Handovers is supported.	2021.01.0
The Wi-Fi to 5GS Handover with EPS Fallback feature is fully qualified in this release.	2020.02.2
The Wi-Fi to 5GS Handover with EPS Fallback feature is not fully qualified in this release. For more information, contact your Cisco Account representative.	2020.02.1

Revision Details	Release
First introduced.	Pre-2020.02.0

## Feature Description

The SMF+PGW-C product supports Wi-Fi handovers. The cloud-based architecture supports the following Wi-Fi handovers in 5GS or EPS and non-3GPP untrusted access.

- EPC to non-3GPP untrusted Wi-Fi handover
- Non-3GPP untrusted Wi-Fi to EPC handover
- Non-3GPP untrusted Wi-Fi to 5GS handover with EPS fallback
- Non-3GPP untrusted Wi-Fi to 5GS handover
- 5GS to non-3GPP untrusted Wi-Fi handover

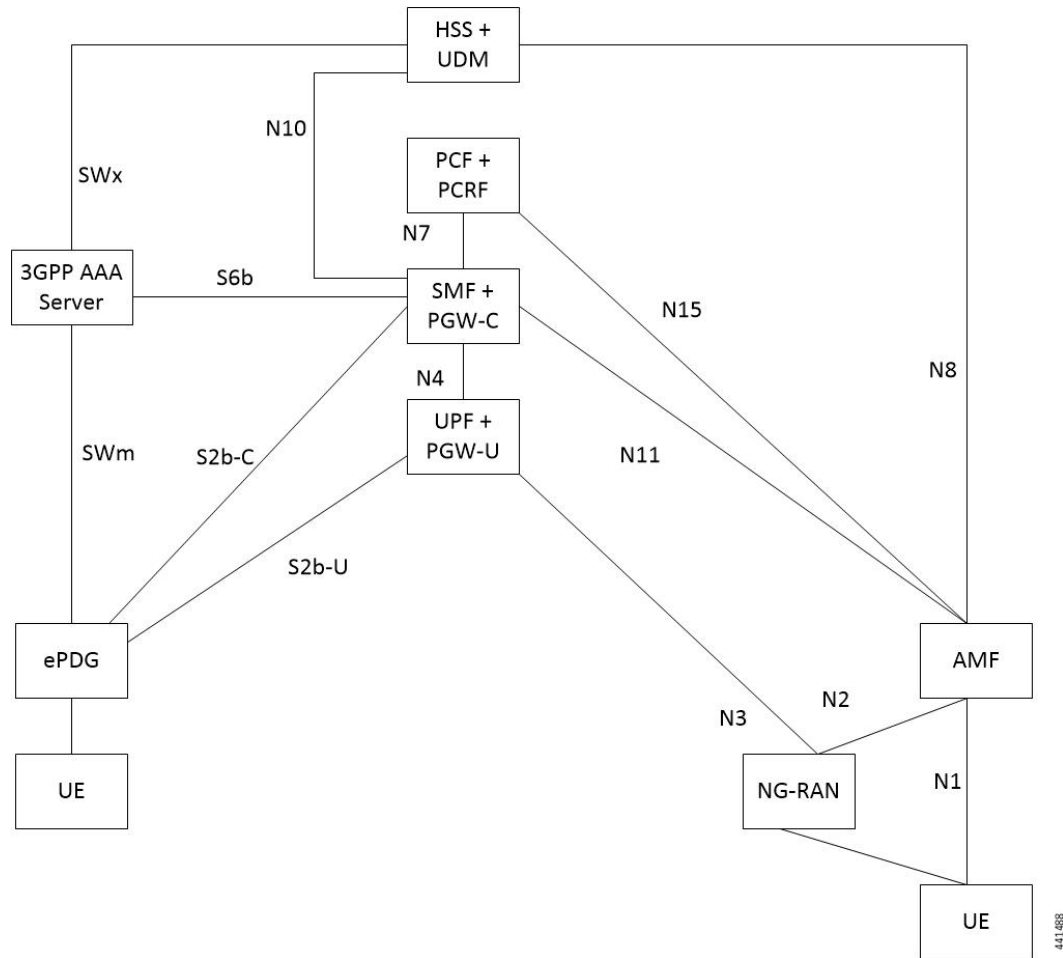
## Architecture

The following sections describe the architecture for interworking between the ePDG or EPC and 5GS and the nonroaming architecture within the EPS using S5 and S2b interfaces.

### ePDG and 5GS Interworking for Handover

The following figure illustrates the non-roaming architecture for interworking between the ePDG or EPC and 5GS.

Figure 142: Non-roaming Architecture for Interworking between ePDG or EPC and 5GS



The interworking between the ePDG and 5GS is similar to the interworking between the EPC and 5GS without the N26 interface. In this interworking, the IP address preservation occurs on the UEs on inter-system mobility. Fetching and saving the PGW-C and SMF and the corresponding APN and DNN information through the HSS and UDM makes interworking possible. In such networks, the AMF also supports interworking with UEs without the N26 interface during the initial registration in 5GC. The AMF may support interworking with UEs without N26 in the Attach procedure in 5GS. In case of a non-3GPP untrusted Wi-Fi access, the ePDG does not communicate with the AMF because the N26 interface does not exist.

A 5GS supports network slicing and can interwork with the EPS in its PLMN or in other PLMNs. The SMF+PGW-C performs UDM registration for each UE with PGW-C FQDN and NSSAI values. With this registration, the AMF or ePDG identify the PGW-C IP-address from the UDM or HSS as part of the subscription information after the UE authorization is completed.

The mobility between 5GC to EPC does not ensure that all the active PDU sessions can be transferred to the EPC. During PDN connection establishment in the EPC, the UE allocates the PDU session ID and sends it to the PGW-C+SMF through the PCO.

An S-NSSAI that is associated with the PDN connection is determined based on the operator policy by the PGW-C+SMF. For example, the combination of PGW-C+SMF address and APN is sent to the UE in the PCO along with a PLMN ID to which the S-NSSAI relates. If the PGW-C+SMF supports multiple S-NSSAI and

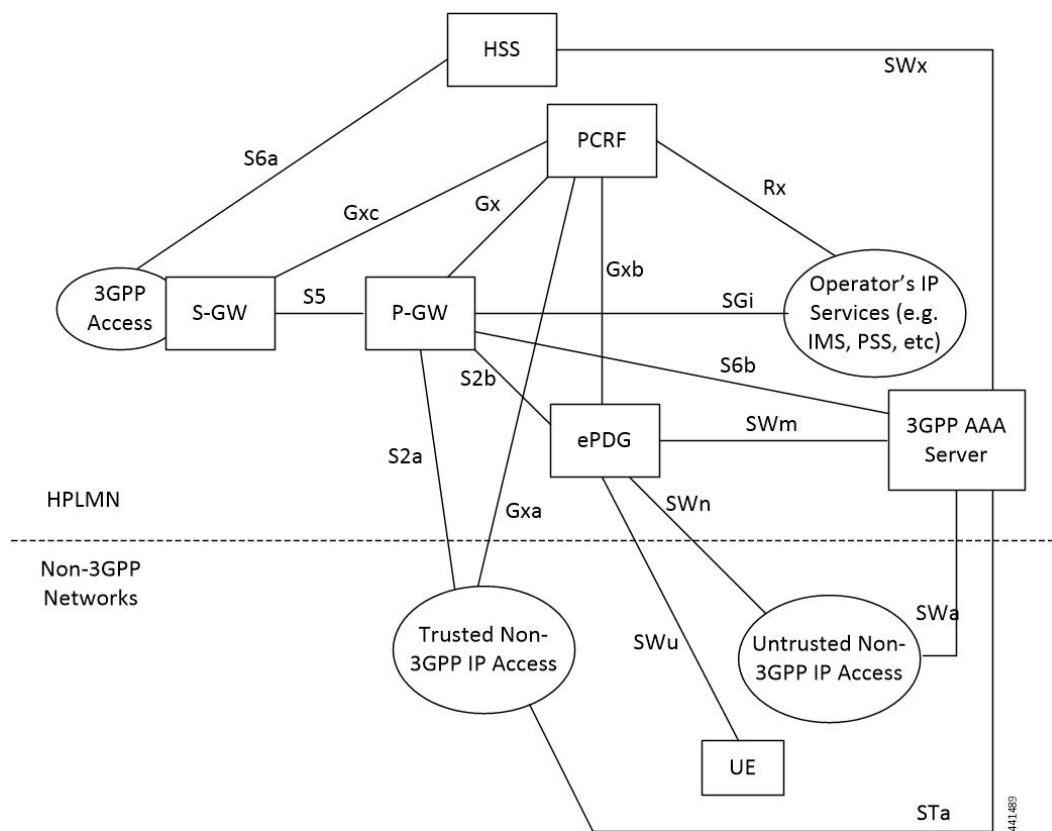
the APN is valid for multiple S-NSSAIs, the PGW-C+SMF selects only the S-NSSAI that is mapped to the subscribed S-NSSAIs of the UE.

The UE saves the S-NSSAI and the PLMN ID that is associated with the PDN connection. The UE derives the requested NSSAI through the received PLMN ID. The NAS registration request message includes the requested NSSAI. The RRC carries the registration request when the UE registers in 5GC. This scenario is applicable if the UE is non-roaming or the UE has configured NSSAI for the VPLMN in roaming case.

## EPS and ePDG Interworking for Handover

The following figure illustrates the non-roaming architecture within the EPS using S5 and S2b interfaces.

**Figure 143: Non-roaming Architecture Within EPS using S5, S2a, and S2b Interfaces**



For 3GPP access to non-3GPP access untrusted Wi-Fi handover and for non-3GPP access untrusted Wi-Fi to 3GPP access handover, if a UE has multiple PDN connections to different APNs in the source access and the UE can route different simultaneously active PDN connections through different access networks, the UE can transfer from the source to the target access all the PDN connections that were active in source access before handover or only a subset of them. This transfer can have the restriction that multiple PDN connections to the same APN have one access.

The transfer process can occur in the following scenarios:

- 3GPP access to non-3GPP access untrusted Wi-Fi handover
- Non-3GPP access untrusted Wi-Fi to 3GPP access handover

The UE can transfer from the source to the target access all the PDN connections that were active in source access before handover or only a subset of them if the following conditions are met:

- The UE has multiple PDN connections to different APNs in the source access
- The UE can route different, but simultaneously active, PDN connections through different access networks."

The SMF supports untrusted Wi-Fi access for end-users over S2b interface with ePDG after establishment of IPSec connection between the end-user and ePDG.

For untrusted Wi-Fi to EPC handover, the SMF provides a PGW-C FQDN during UDM registration and fetches the subscription information.

During UE handover, the MME fetches PGW-C FQDN from the HSS. After authentication, the MME initiates GTPv2 create session request indicating handover. The SMF+PGW-C does not perform the UDM registration and subscription procedures while processing handover request. SMF+PGW-C ensures that GTPv2 MB request indicating handover is sent to perform data path switching from untrusted Wi-Fi to EPC.

For EPC to untrusted Wi-Fi handover, the HSS provides SMF+PGW-C FQDN after the subscriber authentication. When UE performs handover, after authentication HSS provides SMF+PGW-C FQDN. The ePDG initiates GTPv2 create session request indicating handover toward PGW after IPSec tunnel establishment. SMF+PGW-C performs the UDM registration and no subscription procedures exist while processing the handover request.

## TFT Handling for WiFi Handovers

In 4G and 5G deployment, the three-way audio or video multiparty call conference, and RCS message use cases, PGW-C ends up having more than four filters (it can go upto max 16 filters) for both UL and DL direction. SMF includes “EPS Bearer Level Traffic Flow Template (Bearer TFT)” is included in the GTPv2 CBReq/UBReq of BearerContextList. CBReq/UBReq carry maximum of 4 TFTs per bearer.

In case of three-way Audio/Video and multiparty call-conference, PCF tries to push the pccRules by adding different subscriber TFTs in multiple “N7 Policy Notify Req” messages. PGW-C handles the received “N7 Update Notify Req” in dedicated bearer establishment or update towards WiFi or LTE by initiating GTPv2 CBReq or UBReq messages. SMF accommodates the received SDF Filters in TFT as it never crosses more than 256 Bytes (4 TFTs).



**Note** PGW-C don't support more than 4TFTs received from PCF “N7 Policy Notify Req”.

PCF keeps pushing multiple pccRules for same bearer by sending “N7 Policy Notify Req” and over the period SMF ends up having 12-16 filters for case of multiparty call.

When subscriber moves from LTE to WiFi or WiFi to LTE or NR to WiFi Handover call-model cases, SMF first establishes default bearer creation as part of HO. SMF then tries to send out CBReq for Dedicated bearer establishment by accommodating all 16 filters in “EPS Bearer Level Traffic Flow Template (Bearer TFT)” of bearer context list of the subscriber and if it fails to encode because of these restrictions. The SMF sends out CBReq without “EPS Bearer Level Traffic Flow Template (Bearer TFT)” IE based on HO type, SGW/MME/ePDG rejects GTPv2 CBResp with Mandatory IE Incorrect with “TFT Semantic Errors”.

After receiving CBResp from SGW/ePDG, SMF doesn't free up policy/charging resources for respective failed bearers and that leads to further stale entries on SMF and UPF which leads to system inconsistency for that subscriber with “EBI Mismatch – 408 Error Voice Call Failure WiFi HOs”.

# Standards Compliance

The Wi-Fi handovers feature complies with the following standards:

- 3GPP TS 23.502 V15.2.0 (2018-09)
- 3GPP TS 23.402 V15.3.0 (2018-03)
- 3GPP TS 29.214 V15.5.0 (2018-03)

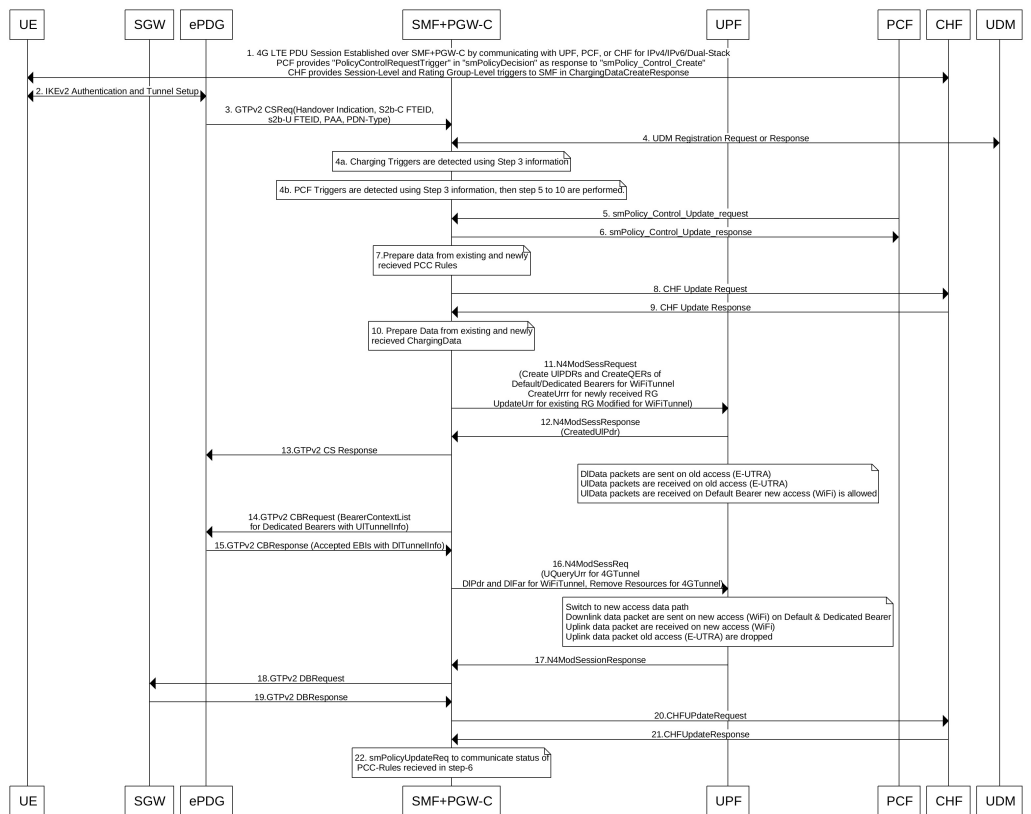
# How it Works

This section describes the Wi-Fi to LTE handover, Wi-Fi handover with EPS fallback, and Wi-Fi to 5GS handover.

## EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow

This section describes the EPC to non-3GPP untrusted Wi-Fi handover call flow.

Figure 144: EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow



442340



Table 245: EPC to Non-3GPP Untrusted Wi-Fi Handover Call Flow Description

Step	Description
1	<p>The UE is attached to the 3GPP access network.</p> <p>The SMF+PGW-C communicates with UPF, PCF, and CHF for IPv4, IPv6, or dual-stack to establish 4G LTE PDU session. The PCF sends the Policy Control Request trigger, which is the SM policy decision, in response to SM policy control create. The CHF provides session-level or rating-group-level triggers to the SMF in Charging Data Create response.</p>
2	<p>The UE connects to an untrusted non-3GPP access and an ePDG is selected through the ePDG selection process. Then, the UE initiates the handover attach procedure as defined in <i>3GPP TS 23.402, section 8.6.2.1</i>. After the IKE tunnel is established between the UE and ePDG and after the UE is authenticated over SWm interface with AAA server, the UE initiates IKE authentication (IKE_AUTH). The IKE_AUTH includes configuration parameters of the earlier assigned IPv4 or IPv6 addresses in the EPC and P-CSCF and the DNS options.</p>
3	<p>The ePDG sends a Create Session Request to the P-GW. This request includes the following details:</p> <ul style="list-style-type: none"> <li>• IMSI</li> <li>• APN</li> <li>• Handover indication</li> <li>• RAT type</li> <li>• ePDG TEID of the Control Plane</li> <li>• ePDG address for the User Plane</li> <li>• ePDG TEID of the User Plane</li> <li>• EPS bearer identity</li> <li>• User location</li> </ul> <p>The RAT type indicates the non-3GPP access technology type. If the UE supports the IP address preservation and is included in the port analyzer adapter (PAA), then the ePDG configures the handover indication in the Create Session Request to allow the PDN gateway to reallocate the same IP address or the prefix assigned to the UE. This IP address or prefix is assigned while UE is connected to the 3GPP IP access and initiates the policy modification procedure with PCF.</p>
4a	<p>The SMF performs UDM registration by updating the PGW-C FQDN with UDM.</p> <p>The UDM registration does not occur during the session establishment with EPC.</p>
4b	<p>The SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during EPC session establishment.</p>
4c	<p>The SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the communication with PCF during EPC session establishment.</p>
5	<p>Based on the detected armed Policy Control Triggers that are received in Step 4b, the SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to the PCF.</p>

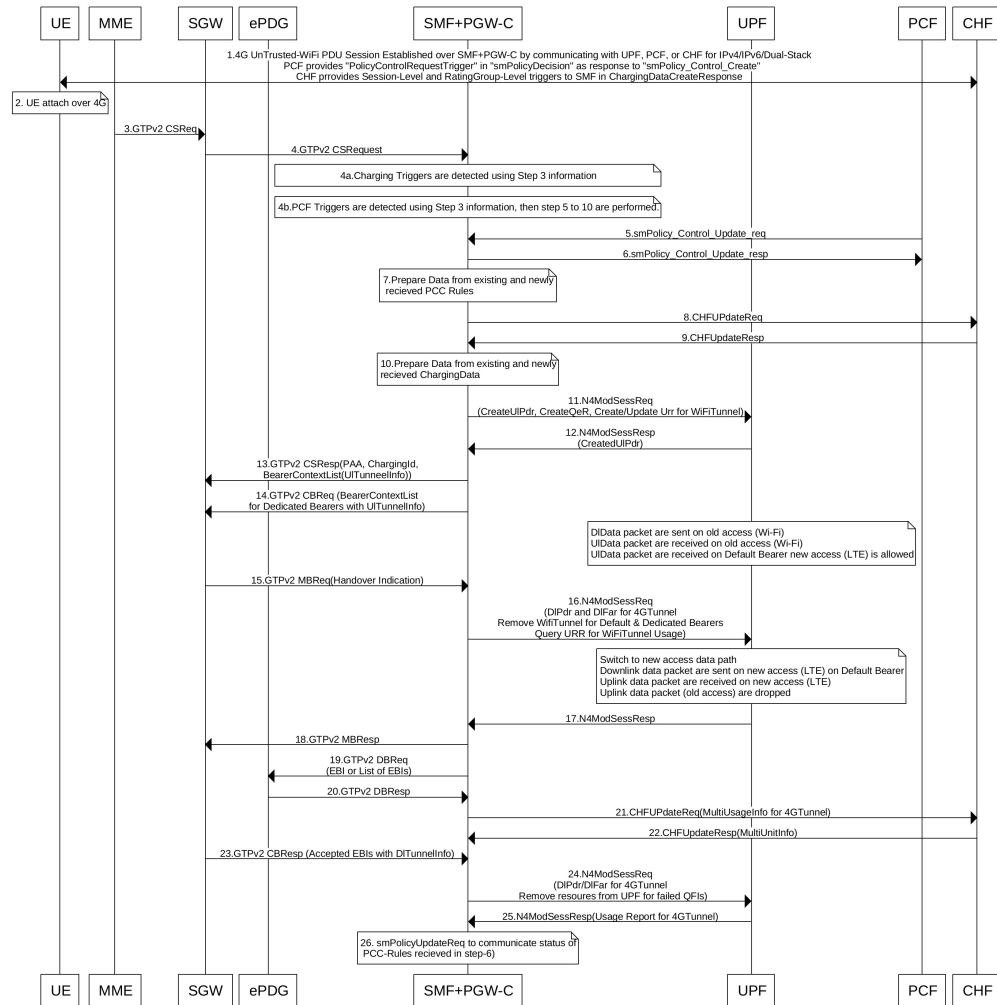
Step	Description
6	The PCF includes new or updated PCC rules and sends the SM Policy Control Update response. The Update response includes information on the SM policy decision.
7	Based on the information received in Step 6 and existing policy data of EPC session, SMF prepares the information for the new or updated PCC rules.
8	If new PCC rules are received in Step 6 with new Rating Group that requires quota information, SMF sends the Charging Update request to CHF. SMF also includes new access parameters for the PDU session information.
9	CHF sends the Charging Update Response with multi-unit information that contains quota information for the requested rating-group in Step 8 to SMF. CHF may also send the new quota information for the existing rating-group of EPC session.
10	SMF processes the information that is received as Charging Update response from CHF.
11	SMF sends the N4 session modification request to UPF for Wi-Fi tunnel. This request includes details on creation of uplink PDR, creation of QER, creation of URR for received new rating-group quota information, and update on URR for modified quota information.
12	UPF sends the UL tunnel information that is in created PDR as the N4 session modification response to SMF.
13	SMF sends the GTPv2 Create Session response to S-GW. This response details on request accepted or request accepted partially, P-GW S2b F-TEID, PAA, APN-AMBR, bearer context creation, charging gateway address, and APCO.
14	SMF sends the GTPv2 Create Bearer request to S-GW. This request includes information on bearer context list, which contains DL tunnel information to end-user, to be created.
15	S-GW sends the GTPv2 Create Bearer response to SMF. The response includes details on request accepted or request accepted partially and bearer contexts.
16	SMF processes the Create Bearer response and derives the DL tunnel Information for the established bearer and the the failed EBI list, if any. SMF sends the N4 session modification request to UPF for Wi-Fi tunnel. This request is to create the DL PDR and DL FAR with DL tunnel information for each bearer, RAT modification information, and to delete resources for the 4G tunnel. SMF also deletes the N4 resources of Wi-Fi tunnel for the received failed EBI list or the failed QFI list.
17	UPF sends the usage report as N4 Session Modification response to SMF.
18	SMF+PGW-C sends the GTPv2 DB request to S-GW. This request includes EBI or list of EBIs.
19	S-GW sends the GTPv2 DB response to SMF+PGW-C.
20	SMF sends the Charging Update request to CHF. This request includes the PDU session information with the new access params and multi-usage report containing details on the access params and usage report that is received in Step 8
21	CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information may include new quota information for the existing rating-groups.

Step	Description
22	SMF sends the SM Policy Control Update request to UPF. This request includes the new access params and rule report for failed QFI list that is received from AMF as part of Create Bearer response.  PCF sends the SM policy decision as SM Policy Control Update response.  SMF processes the SM policy decision and handles it as PCF Initiation Modify procedure as defined in 3GPP 23.502, section 4.3.3.2.

## Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow

This section describes the non-3GPP untrusted Wi-Fi to EPC handover call flow.

Figure 145: Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow



442341

Table 246: Non-3GPP Untrusted Wi-Fi to EPC Handover Call Flow Description

Step	Description
1	One or more PDU sessions are established between UE and ePDG through untrusted non-3GPP access. With the 5G NAS capability of UE, ePDG selects a combined PGW+SMF. UE sends the PDU session ID to the PGW+SMF.
2	<p>UE discovers the E-UTRAN access and hands over the sessions from the currently used non-3GPP access system to E-UTRAN. For details on UE discovery of the 3GPP access system, see <i>3GPP TS 23.401</i>, section 4.8.</p> <p>UE sends an Attach request to MME for the Handover Attach request type. E-UTRAN routes the messages received from UE to MME as defined in <i>3GPP TS 23.401</i>. UE includes the one of the APNs which are corresponding to the PDN connections in the source non-3GPP access. The APN is provided as defined in <i>3GPP TS 23.401</i>.</p>
3	<p>MME and HSS perform authentication, which is followed by location update procedure and subscriber data retrieval to receive the APN information.</p> <p>The MME selects an APN, an SGW and PDN gateway as defined in <i>3GPP TS 23.401</i>. MME sends a Create Session Request message to SGW. This request includes information on IMSI, MME context ID, PDN-GW address, handover indication for the “handover” request type, and APN.</p>
4	<p>SGW sends a Create Session Request, which is handover indication, message to PDN-GW in the HPLMN as described in <i>3GPP TS 23.401</i>. As the MME includes the handover indication information in the Create Session Request message, the SGW sends the GTPv2 Create Session Request message to PDN GW. This message includes details on IMSI, APN, handover indication, RAT type, S5-C TEID, S5-U TEID of the user plane, EBI, and user location information. The RAT type indicates the 3GPP IP access E-UTRAN technology type. If the UE supports IP address preservation and is included in PAA, the SGW configures the handover indication in the Creation Session Request. With this configuration, the PDN GW re-allocates the same IP address or prefix that was assigned to the UE while it was connected to the 3GPP IP access. With this configuration, SGW initiates the Policy Modification Procedure to the PCF.</p> <p>As the handover indication is included, the PDN GW does not switch the tunnel from non-3GPP IP access to 3GPP access system at this point.</p> <p>SMF does not perform the UDM Registration as the registration happens during the Wi-Fi session establishment.</p>
4a	SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during EPC session establishment.
4b	SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the communication with PCF during EPC session establishment.
5	Based on the detected armed Policy Control Triggers that are received in Step 4b, SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to PCF.
6	PCF sends the SM Policy Control Update response, which is the SM policy decision, by including new or updated PCC rules.
7	Based on the information received in Step 6 and existing policy data of EPC session, SMF prepares the information for the new or updated PCC rules.

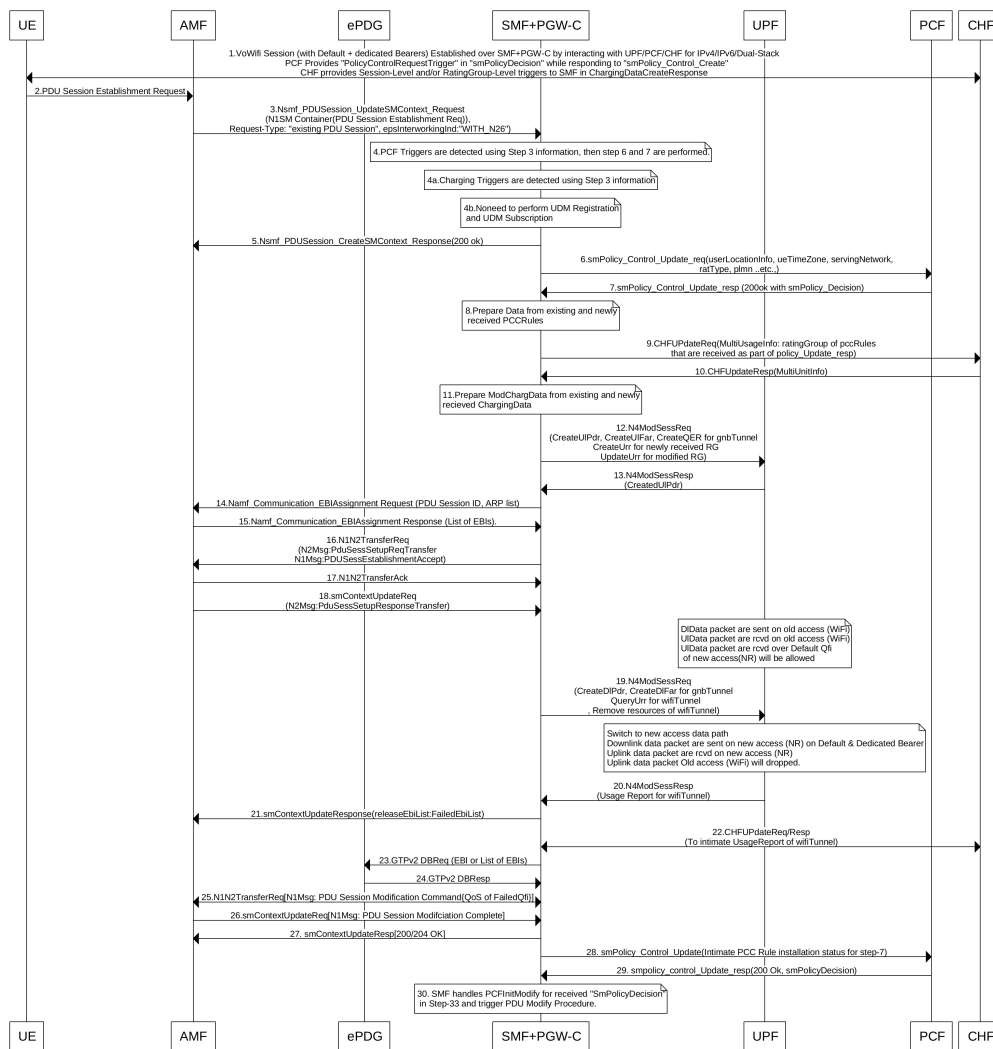
Step	Description
8	If SMF receives new PCC rules in Step 6, the SMF sends the Charging Update request, with the new rating-group having quota information, to CHF. This request includes the PDU session information with the new access params.
9	CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information includes new quota information for the rating-group and the existing rating-group of EPC session, if any.
10	SMF prepares the charging data of the received Charging Update Response that CHF sent.
11	SMF sends the N4 Session Modification Request to UPF. This request includes the details on creation of UL and DL PDR, creation of QER, creation of URR for received new rating-group quota information, updated URR for modified quota information, and creation of FAR.
12	UPF sends the UL tunnel information in the created PDR as N4 Session Modification response to SMF.
13	SMF sends the GTPv2 Create Session response to S-GW. This response details on request accepted or request accepted partially, P-GW S2b F-TEID, PAA, APN-AMBR, bearer context creation, charging gateway address, and APCO.
14	SGW sends the Modification Bearer request with handover indication to PGW for data path switching from Wi-Fi tunnel to 4G tunnel.
15	PGW sends the N4 Session Modification request to delete the Wi-Fi tunnel and to configure DL tunnel information that is received in GTPv2 Create Session request for 4G tunnel in Step 4.
16	UPF sends the N4 Session Modification response to SMF.
17	SMF sends the GTPv2 Create Session request, which includes the bearer context list, to SGW. This list includes the DL Tunnel information for the end-user.
18	SGW sends the GTPv2 Create Session response to SMF. This response includes details on request accepted or request accepted partially and bearer contexts.
19	ePDG sends the GTPv2 Create Bearer resp (accepted EBIs with DL tunnel info to SMF
20	SMF processes the Create Bearer response and derives the DL tunnel Information for the established bearer and the failed EBI list, if any. SMF sends the N4 session modification request to UPF for Wi-Fi tunnel. This request is to update the DL FAR with the DL tunnel information, RAT modification information, and to delete resources for the 4G tunnel. SMF also deletes the N4 resources of Wi-Fi tunnel for the received failed EBI list or the failed QFI list.
21	UPF sends the N4 Session Modification Response with usage report to SMF.
22	SMF sends the Charging Update request to CHF. This request includes the PDU session information with new access params and multi-usage report consisting of access-params and usage report that is received in Step 8.
23	CHF sends the Charging Update Response with multi-unit information that contains quota information for the existing rating-groups to SMF.
24	SMF+PGW-C initiates the GTPv2 DB Request toward SGW by including EBI or EBI list.
25	SGW sends the GTPv2 DB Response toward SMF+PGW-C.

Step	Description
26	<p>SMF sends the SM Policy Control Update request to UPF. This request includes the new access params and rule report for failed QFI list that is received from AMF as part of Create Bearer response.</p> <p>PCF sends the SM policy decision as SM Policy Control Update response.</p> <p>SMF processes the SM policy decision and handles it as PCF Initiation Modify procedure as defined in 3GPP 23.502 section 4.3.3.2.</p>

## Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow

This section describes the non-3GPP untrusted Wi-Fi to 5GS handover call flow.

Figure 146: Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow



442343

Table 247: Non-3GPP Untrusted Wi-Fi to 5GS Handover Call Flow Description

Step	Description
1	One or more PDU sessions are established between UE and ePDG through untrusted non-3GPP access. With the 5G NAS capability of UE, ePDG selects a combined PGW+SMF. UE sends the PDU session ID to the PGW+SMF.
2	<p>UE sends the PDU Session Establishment request through 3GPP access to AMF. This request includes details on PDU session ID, requested PDU session type, requested SSC mode, 5GSM capability PCO, SM PDU DN request container, number of packet filters, and an optional requested always-on PDU session.</p> <p>The request type with an existing PDU session indicates switching between 3GPP access and non-3GPP access or to a PDU session handover from an existing PDN connection in EPC.</p>
3	<p>If the request type is “Existing PDU Session”, the AMF selects the SMF based on SMF-ID that is received from UDM. For this request type, if AMF does not identify the PDU Session ID or the subscription context that the AMF received from UDM during the Registration or if the subscription profile update notification procedure contains no SMF ID corresponding to the PDU Session ID, an error occurs. Then, AMF updates the Access Type stored for the PDU session.</p> <p>If the request type with an existing PDU session refers to a PDU session that moved between 3GPP access and non-3GPP access and if the S-NSSAI of the PDU session is available in the Allowed NSSAI of the target access type, the PDU Session Establishment procedure is performed when the SMF ID corresponding to the PDU Session ID and the AMF are part of the same PLMN.</p> <p>AMF sends the NSMF PDU Session Create SM Context Request with the request type “Existing PDU Session” to SMF. This request includes information on SUPI, DNN, S-NSSAIs, PDU Session ID, AMF ID, Request Type, PCF ID, Priority Access, N1 SM container including the PDU Session Establishment Request, User location information, Access Type, PEI, GPSI, Subscription For PDU Session Status Notification, DNN Selection Mode.</p> <p>SMF analyzes the existing PDU session from the PDU Session Establishment request using SUPI+PDU-Session-ID. SMF also compare the IPv4 or IPv6 addresses of the received UE against the retrieved PDU session IPv4 or IPv6 addresses. SMF reject the request if the session is not retrieved or IPv4 or IPv6 addresses do not match.</p>
4	SMF detects the PCF triggers with the information available in Step 3 against the Request Policy Control triggers that are received in the earlier communication with PCF during Wi-Fi session.
4a	SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during Wi-Fi session.
4b	SMF does not perform the UDM registration as happens during Wi-Fi Session Establishment.
5	SMF sends the NSMF PDU Session Create SM Context response to AMF. This response includes the cause, SM Context ID or N1 SM container with PDU session rejection cause.
6	Based on the detected armed Policy Control Triggers that are received in Step 4a, SMF sends the SM Policy Control Update request with the detected access parameters in Step 3 to PCF.
7	PCF sends the SM Policy Control Update response, which is the SM policy decision, by including new or updated PCC rules.

Step	Description
8	Based on the information received in Step 7 and existing policy data of Wi-Fi session, SMF prepares the information.
9	If SMF receives new PCC rules in Step 7, the SMF sends the Charging Update request to CHF with new rating-group for quota information. This request includes the PDU session information with the new access params.
10	CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information includes quota information for the rating-groups received in Step 9 and for the existing rating-group of Wi-Fi session.
11	SMF processes the data that is received Charging Update response from CHF.
12	SMF sends the N4 session modification request to UPF for gnb tunnel. This request includes details on creation of uplink PDR, creation of QER, creation of URR for received new rating-group quota information, update on URR for modified quota information, and creation of FAR.
13	UPF sends the UL tunnel information that is in created PDR as the N4 session modification response to SMF.
14	SMF sends the EBI assignment request to AMF. This request includes the ARP list for the PDU session ID.
15	AMF sends the list of EBIs as response to SMF.
16	SMF sends the N1 N2 Transfer Request toward AMF. This request includes the N2 message as “PDU Session Resource Setup Request Transfer” with supported QFI list and UL Tunnel Information of gnb Tunnel. This request also includes the N1 message as “PDU Session Establishment Accept” with authorized QoS rule, authorized QoS flow description, EPCO, PDN addresses, and session AMBR values.
17	AMF sends the N1 N2 Transfer acknowledgement to SMF.
18	AMF sends the SM Context Update request to SMF with “PDU Session Resource Setup Response Transfer” containing the failed QFI list and the DL tunnel information.
19	SMF sends the N4 session modification request to UPF for the gnb tunnel resources. This request is to create the DL PDR, to create DL FAR with DL tunnel information, include details on RAT-change and delete resources for Wi-Fi tunnel. SMF also deletes the N4 resources of gnb tunnel for received failed QFI list.
20	UPF sends the N4 Session Modification Response with the usage report to SMF.
21	SMF sends the SM Context Update response to AMF.
22	SMF sends the Charging Update request to PCF. This request includes the PDU session information with new access params and multi-usage report with old access-params and usage report that is received in Step 18.  SMF receives the Charging Update response that includes new quota information for existing rating-groups.
23	SMF+PGW-C initiates the GTPv2 DB request, which includes EBIs, to ePDG.

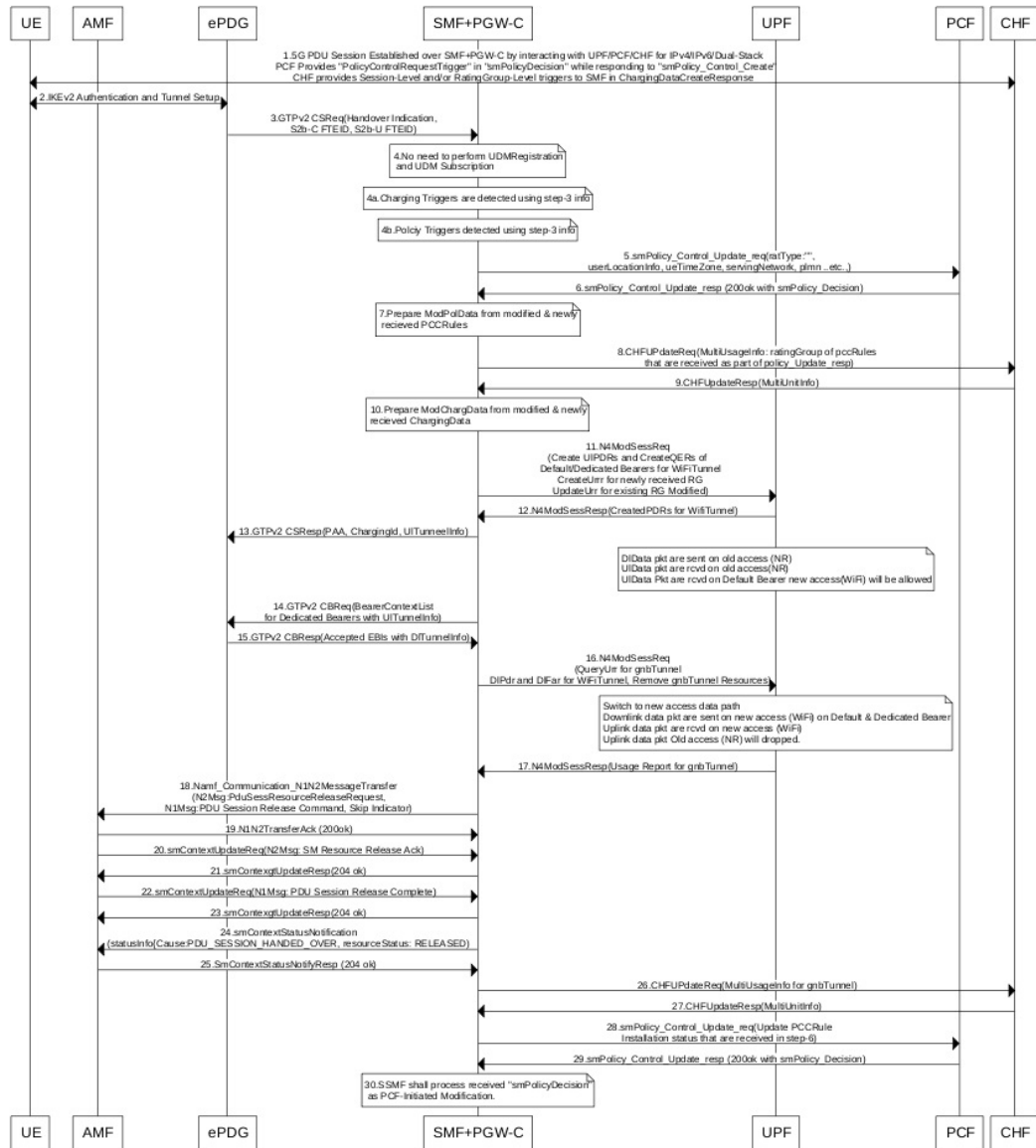


Step	Description
24	ePDG sends the GTPv2 DB response to SMF+PGW-C.
25	SMF receives the SM Context Update request with N1 message for PDU session modification completion from AMF.
26	SMF sends 200/204 OK as SM Context Update response to AMF.
27	SMF sends the SM policy decision as SM Policy Control Update response to AMF.
28	SMF sends the SM Policy Control Update request to PCF. This request includes the new access params and rule report for failed QFI list that is received from AMF as part of N2 message.
29	PCF sends the SM policy decision as SM Policy Control Update response to SMF.
30	SMF processes the SM policy decision and handles it as PCF Initiation Modify procedure as defined in 3GPP 23.502 section 4.3.3.2.

## 5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow

This section describes the 5GS to non-3GPP untrusted Wi-Fi handover call flow.

Figure 147: 5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow



442344

Table 248: 5GS to Non-3GPP Untrusted Wi-Fi Handover Call Flow Description

Step	Description
1	The UE and the SMF or the UPF interact through the NG-RAN to establish one or more PDU sessions.

Step	Description
2	The UE connects to an untrusted non-3GPP access and selects an ePDG. Then, the UE initiates the handover attach procedure, as defined in <i>3GPP TS 23.402, section 8.6.2.1</i> . After establishing the IKE tunnel between the UE and the ePDG, and authenticating the UE over SWm interface with the AAA server, the UE initiates IKE_AUH. The IKE_AUH includes cfg_params of the earlier assigned IPv4 or IPv6 addresses in 5GS and P-CSCF and DNS options.
3	<p>The ePDG sends a Create Session request to the P-GW. This request includes the following details:</p> <ul style="list-style-type: none"> <li>• IMSI</li> <li>• APN</li> <li>• handover indication</li> <li>• RAT type</li> <li>• ePDG TEID of the control plane</li> <li>• ePDG address for the user plane</li> <li>• ePDG TEID of the user plane</li> <li>• EPS bearer identity</li> <li>• user location</li> </ul> <p>The RAT type indicates the non-3GPP access technology type. If the UE supports the IP address preservation and includes it in the port analyzer adapter (PAA), then the ePDG configures the handover indication in the Create Session request. This configuration allows the P-GW to reallocate the same IP address or the prefix assigned to the UE. The IP address or prefix assignment occurs while the UE is connected to the 3GPP IP access. The policy modification procedure begins with the PCF.</p>
4	The SMF does not perform the UDM registration as it has already been registered with UDM during the 5GS session establishment.
4a	The SMF detects the charging triggers with the information available in Step 3 against the charging triggers that are received during the Wi-Fi session.
4b	The SMF detects the policy triggers with the information available in Step 3 against the requested policy control triggers that are received while communicating with PCF during the Wi-Fi session establishment.
5	Based on the detected armed Policy Control Triggers that are received in Step 4b, the SMF sends the SM Policy Control Update request with the detected access parameters to the PCF.
6	The PCF sends the SM policy decision in the SM Policy Control Update response by including new or updated PCC rules.
7	Based on the information received in Step 6 and the existing policy data of 5GS session, the SMF prepares the “ModPolData” information.

Step	Description
8	If the SMF receives new PCC rules in Step 6, the SMF sends the Charging Update request to the CHF with new rating-group for quota information. This request includes the PDU session information with the new access parameters.
9	The CHF sends the multi-unit information as Charging Update response to the SMF. The multi-unit information includes quota information for the rating-groups received in Step 8 and for the existing rating-group of 5GS session.
10	The SMF processes the ModChargingData in the Charging Update response received from the CHF.
11	The SMF sends the N4 session modification request to the UPF for Wi-Fi tunnels. This request includes details on creation of uplink FAR, creation of QER, creation of URR for the received new rating-group quota information, and update on URR for the modified quota information.
12	The UPF sends the N4 session modification response to the SMF with the UL tunnel information in the created PDR.
13	The SMF sends the GTPv2 Create Session response to the S-GW. The response includes details on accepted request or partially accepted request, P-GW S2b F-TEID, PAA, APN-AMBR, creation of bearer context, charging gateway address, and APCO.
14	The SMF sends the GTPv2 Create Bearer request to the S-GW. This request includes information on bearer context list, which contains UL tunnel information for each dedicated bearer to end-user.
15	The S-GW sends the GTPv2 Create Bearer response to the SMF. The response includes details on accepted request or partially accepted request and bearer contexts.
16	The SMF processes the Create Bearer response and derives the DL tunnel information for the established bearer and the failed EBI list, if any. The SMF sends the N4 session modification request to the UPF for Wi-Fi tunnel. This request is to create DL PDR and DL FAR with the DL tunnel information or list of charging description IDs for the detected charging triggers.  The SMF deletes the gnb tunnel resources and the N4 resources of the Wi-Fi tunnel for the failed bearer context list.
17	The UPF sends the usage report in the N4 Session Modification response to the SMF.
18	The SMF initiates the NAMF communication N1 N2 message transfer, to the S-GW. This transfer message includes the PDU Session Resource Release Request N2 message.
19	The AMF sends N1 N2 Transfer Acknowledgement to the SMF.
20	The AMF sends the SM Context Update request to the SMF. This request includes the SM Resource Release Acknowledgement N2 message.
21	The SMF sends the 200/204 OK as SM Context Update response to the AMF.
22	The AMF sends the SM Context Update request to the SMF. This request includes the PDU Session Release Complete N1 message.
23	The SMF sends the 200/204 OK as SM Context Update response to the AMF.

Step	Description
24	<p>If the SMF supports the June 2019 compliance version of 3GPP specification 23.502, the SMF indicates the release details to the AMF. The SMF achieves this functionality by sending the SM Context Status Notification message (statusInfo {Cause: PDU_SESSION_HANDED_OVER, resourceStatus: RELEASED}). The SMF sends this notification after a successful handover of 5GS to Non-3GPP Untrusted WiFi session.</p> <p>The SMF processes the message as per the compliance profile configured for the corresponding service. For information on the compliance profile configuration, see the <a href="#">Configuring Compliance Profile, on page 825</a> section.</p> <p><b>Important</b> If the SMF supports the December 2018 compliance version of 3GPP specification, the Step 24 and Step 25 are not applicable.</p>
25	<p>The AMF sends the 204 OK as SM Context Status Notify response to the SMF.</p> <p><b>Important</b> If the SMF supports the December 2018 compliance version of 3GPP specification, the Step 24 and Step 25 are not applicable.</p>
26	<p>The SMF sends the Charging Update request to the CHF. This request includes the PDU session information with the new access parameters and multi-usage report containing details on the old access parameters and the usage report that is received in Step 17.</p>
27	<p>The CHF sends the multi-unit information as Charging Update response to SMF. The multi-unit information includes new quota information for the existing rating-groups.</p>
28	<p>The SMF sends the SM Policy Control Update to PCF. This update includes the new access parameters and rule report for failed QFI list that are received from the AMF as part of Create Bearer response.</p>
29	<p>The PCF sends the SM policy decision through the SM Policy Control Update response to the SMF.</p>
30	<p>The SMF processes the SM policy decision and handles it as PCF-initiated modification procedure as defined in <i>3GPP TS 23.502, section 4.3.3.2</i>.</p>

## Non 3GPP Untrusted LTE to WiFi Handover

This section describes the non-3GPP untrusted LTE to WiFi handover call flow.

Figure 148: Non-3GPP Untrusted LTE to WiFi Handover with TFTs more than 4 for a Dedicated Bearer

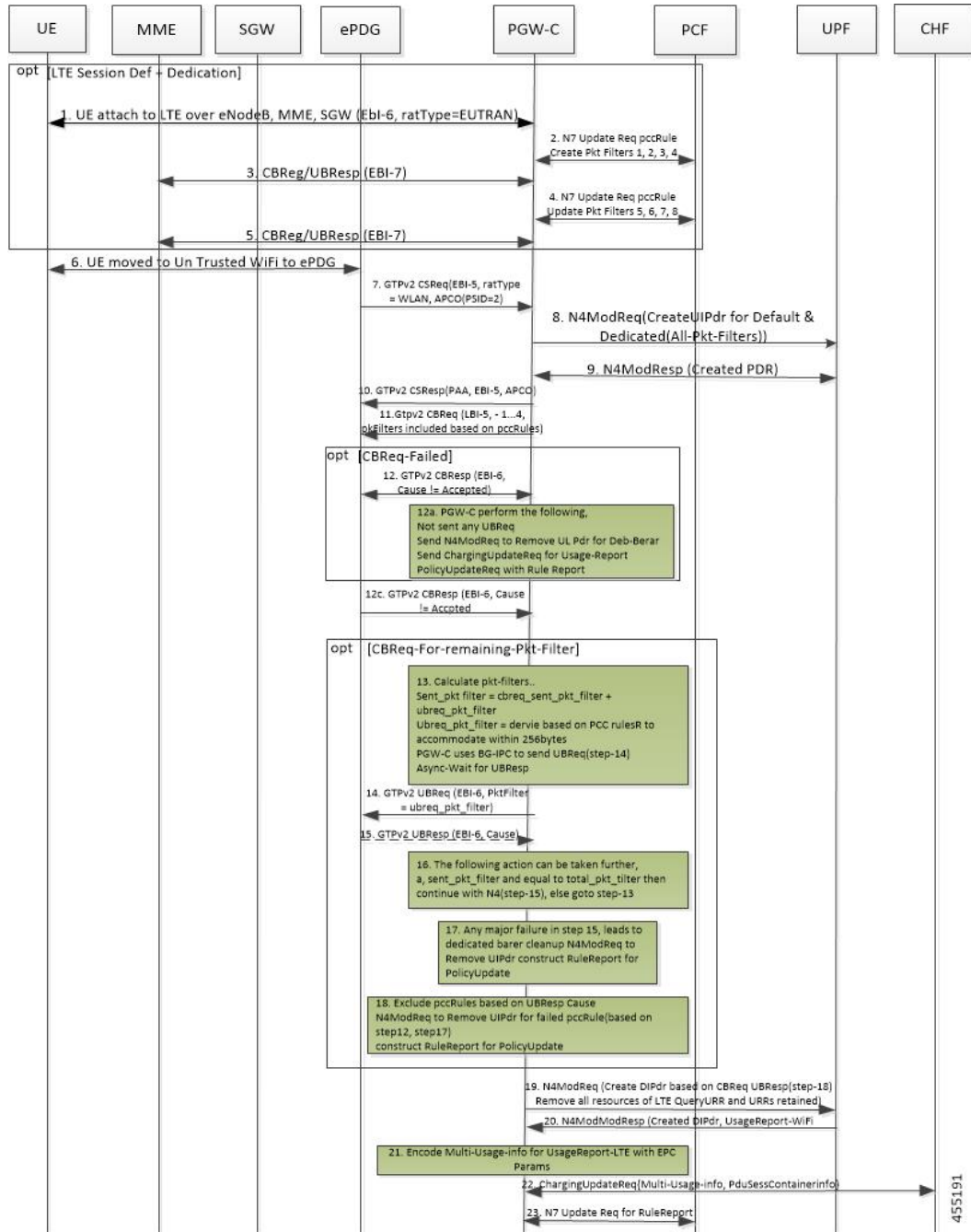


Table 249: Non-3GPP Untrusted LTE to WiFi Handover Call Flow Description

Step	Description
1	Session established in LTE with a default bearer and dedicate bearer with 8 TFTs.
2	LTE->Wifi Handover triggered, when CSReq is received with hi flag set from ePDG.

Step	Description
3	After successfully handling CSReq, CSResp is sent back to ePDG, indicating default bearer successfully handed over.
4	For the dedicated bearer which has 8 TFT, since all TFTs cannot be sent in CBReq, CBReq message is triggered with only 4 TFTs toward ePDG.
5	After successful CBResponse from ePDG, SMF shall send remaining TFTs in the UBRReq message.
6	After successful UBRResponse from ePDG, SMF continues with completion of establishing the bearer towards UPF.
7	At step 5. or step 6., if there is failure in CBResponse or failure in UBRResponse, SMF deletes that bearer and if armed, sends rule report to PCF mentioning the corresponding rules as Inactive.

**Important**

Steps 4-7 are applicable for LTE → WiFi and NR → WiFi if a dedicate bearer has more than 4 TFTs.

## Configuring the WiFi Handovers Feature

This section describes the configurations related to the Wi-Fi Handovers feature.

### Configuring Compliance Profile

The SMF provides the compliance profile support for the 3GPP specification 23.502 through the CLI configuration. This compliance profile is in use during the 5GS to non-3GPP untrusted WiFi handover procedure.

Use the following configuration to configure the SMF in compliance with the 3GPP specification.

**configure**

```

profile compliance profile_name
  service threegpp23502 version spec spec_version full version_format
  uri_version uri_version
  range
  !
  !

```

**NOTES:**

- **full**: Specifies the full version in the format — `<Major-version>.<Minor-version>.<patch-version>.[alpha-<draft-number>]`
- **spec**: Specifies the 3GPP specification version number. It can be one of the following values:
  - 15.4.0
  - 15.6.0

To support 3GPP December 2018 specification compliance, configure the specification version as 15.4.0. The default version is 15.4.0.

To support 3GPP June 2019 specification compliance, configure the specification version as 15.6.0.

- **uri**: Specifies the URI version in the format — "v" concatenated with a number. It can be both v1 and v2, or either v1 or v2.





# CHAPTER 55

## Wireless Priority Services

- [Feature Summary and Revision History, on page 827](#)
- [Feature Description, on page 828](#)
- [How it Works, on page 835](#)
- [Configuring Wireless Priority Services, on page 836](#)

### Feature Summary and Revision History

#### Summary Data

*Table 250: Summary Data*

Applicable Product(s) or Functional Area	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Disabled – Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 251: Revision History*

Revision Details	Release
SBI Message Priority Mechanism and Message-Prioritization based on Procedures are introduced.	2021.01.0
The Wireless Priority Services feature is fully qualified in this release.	2020.03.0

Revision Details	Release
<p>First introduced.</p> <p>This feature is not fully qualified in this release. For more information, contact your Cisco Account representative.</p>	2020.02.0

## Feature Description

The Wireless Priority Services (WPS) feature is supported on the SMF+PGW-C over 5GC. The SMF+PGW-C validates prioritization of WPS services for Session Creation/Modification and various handover scenarios. It also evaluates the WPS services for Paging-Policy Differentiation for Network Triggered Service Request procedures.

## Use Cases

The WPS feature implements the 3GPP recommendations for wireless priority support for the following use cases in 5GS and EPS. The use cases are defined as per *3GPP TS 23.501 (sections 5.16.3, 5.16.4, 5.16.5, 5.16.6, 5.19, and 5.21)*.

WPS supports the following use cases:

- [Multimedia Priority Services](#) , on page 828
- [Mission Critical Services](#), on page 834
- [Expanded Prioritization for VoLTE/VoNR/Emergency Calls](#), on page 834
- [DSCP Marking for N3/S5-U/S2-B over PFCP](#), on page 835

## Multimedia Priority Services

The Multimedia Priority Service (MPS) allows priority access to system resources to Service Users, creating the ability to deliver or complete sessions of a high priority nature. Service Users are government-authorized personnel, emergency management officials and/or other authorized users. MPS supports priority sessions on an "end-to-end" priority basis. MPS includes signalling priority and media priority.

MPS provides the ability to invoke, modify, maintain and release sessions with priority, and deliver the priority media packets under network congestion conditions.

All MPS-subscribed UEs get priority for QoS Flows (for example, used for IMS signalling) when established to the DN that is configured to have priority for a given Service User by setting MPS-appropriate values in the QoS profile in the UDM. Service Users are treated as On Demand MPS subscribers and not On Demand MPS subscribers, based on regional/national regulatory requirements. On Demand service is based on Service User invocation/revocation explicitly and applied to the media QoS Flows being established. Not On Demand MPS service does not require invocation and provides priority treatment for all QoS Flows only to the DN that is configured to have priority for a given Service User after attachment to the 5G network.

Priority treatment for MPS includes priority message handling for Mobility Management procedures. Priority treatment for MPS session requires appropriate ARP and 5QI setting for QoS Flows according to the operator's policy.

MPS priority mechanisms can be classified as subscription-related and invocation-related. Subscription related mechanisms are divided into - always applied and conditionally applied. Invocation-related mechanisms are divided into - for mobile originated SIP call/sessions, for mobile terminated SIP call/sessions and for Priority PDU connectivity services.

Subscription-related mechanisms that are conditionally applied include:

**UDM:** One or more ARP priority levels are assigned for prioritized or critical services. The ARP of the prioritized QoS Flows for each DN is set to an appropriate ARP priority level.

**PCF:** The "IMS Signalling Priority" information is set for the subscriber in the UDM, and the PCF modifies the ARP of the QoS Flow used for IMS signalling.

## On-Demand MPS Service

The invocation-related priority mechanisms for prioritized services are based on interaction with an Application Server and between the Application Server and the PCF over Rx/N5 interface (as described in *3GPP TS 23.228, clause 5.21* in the case of MPS using IMS).

Invocation-related mechanisms for Mobile Originations (for example, via SIP/IMS) are explained below:

- PCF:
  - When an indication for a session arrives over the Rx/N5 interface and the UE does not have priority for the signaling QoS Flow, the PCF derives the ARP and 5QI parameters plus associated QoS characteristics as appropriate, as per the Service Provider policy (specified in *clause 6.1.3.11* of *3GPP TS 23.503*).
  - For MPS sessions, when establishing or modifying a QoS Flow as part of the session origination procedure, the PCF selects the ARP and 5QI parameters plus associated QoS characteristics as appropriate, to provide priority treatment to the QoS Flows.
  - When all active sessions to a particular DN are released and the UE is not configured for priority treatment to that particular PDU session, the PCF downgrades the IMS Signaling QoS Flows from appropriate settings of the ARP and 5QI parameters plus associated QoS characteristics as appropriate, to those entitled by the UE based on subscription.

Invocation-related mechanisms for Mobile Terminations (for example, via SIP/IMS) are explained below:

- PCF: When an indication for a session arrives over the Rx/N5 interface, the mechanisms as described above for Mobile Originations are applied.
- UPF: If an IP packet arrives at the UPF for a UE that is CM-IDLE, the UPF sends a "Data Notification" including the information to identify the QoS Flow for the DL data packet to the SMF (specified in *clause 4.2.3.3* of *3GPP TS 23.502*).
- SMF: If a "Data Notification" message arrives at the SMF for a QoS Flow associated with an ARP priority level value for priority use, delivery of priority indication during the Paging procedure is provided by inclusion of the ARP in the N11 interface "N1N2MessageTransfer" message (specified in *clause 4.2.3.3* of *3GPP TS 23.502*).
- AMF: If an "N1N2MessageTransfer" message arrives at the AMF containing an ARP priority level value for priority use, the AMF handles the request with priority and includes the "Paging Priority" IE in the N2 "Paging" message set to a value assigned to indicate that there is an IP packet at the UPF entitled to priority treatment (specified in *clause 4.2.3.3* of *3GPP TS 23.502*).

- SMF: For a UE that is not configured for priority treatment, upon receiving the "N7 Session Management Policy Modification" message from the PCF with an ARP priority level for priority use, the SMF sends an "N1N2MessageTransfer" to update the ARP for the Signaling QoS Flows (specified in *clause 4.3.3.2 of 3GPP TS 23.502*).
- AMF: Upon receiving the "N1N2MessageTransfer" message from the SMF with an ARP priority level for priority use, the AMF updates the ARP for the Signaling QoS Flows (specified in *clause 4.3.3.2 of 3GPP TS 23.502*).
- (R)AN: Inclusion of the "Paging Priority" in the N2 "Paging" message triggers priority handling of paging in times of congestion at the (R)AN (specified in *clause 4.2.3.3 of 3GPP TS 23.502*).

Invocation-related mechanisms for the Priority PDU connectivity services:

- PCF:
  - If the state of the Priority PDU connectivity services is modified from disabled to enabled, the QoS Flows controlled by the Priority PDU connectivity services are established/modified to have the service appropriate settings of the ARP and 5QI parameters plus associated QoS characteristics as appropriate, using the PDU Session Modification procedure (specified in *clause 4.3.3 of 3GPP TS 23.502*).
  - If the state of Priority PDU connectivity services is modified from enabled to disabled, the QoS Flows controlled by the Priority PDU connectivity services are modified from service appropriate settings of the ARP and 5QI parameters plus associated QoS characteristics as appropriate, to those entitled by the UE as per subscription, using the PDU Session Modification procedure (specified in *clause 4.3.3 of 3GPP TS 23.502*).

## SBI Message Priority Mechanism

The primary usage of SBI Message Priority (SMP) is to provide guidance to 5GC NF acting as HTTP/2 clients or servers while making throttling decisions related to overload control. The priority information may also be used for routing in the proxies. Eventually a server may use the priority information to process higher-priority requests before lower-priority requests. The SMP mechanism uses the "3gpp-Sbi-Message-Priority" custom HTTP header to set and carry the message priority between the client and the server. The custom HTTP header enforces the message priority end to end between the client and the server through one or more proxies.

The SMP mechanism uses the stream priority mechanism specified in IETF RFC 7540 [7] clause 5.3. The stream priority enforces the message priority at the HTTP/2 connection level not end to end. HTTP/2 clients, servers implementing SBIs must support the custom HTTP header and stream priority.

**The header contains the HTTP/2 message priority value:** The encoding of the header follows the ABNF as defined in IETF RFC 7230 [12].

```
3gpp-Sbi-Message-Priority = "3gpp-Sbi-Message-Priority" ":" (DIGIT / %x31-32 DIGIT / "3" %x30-31)
```

A message with

```
3gpp-Sbi-Message-Priority "0"
```

has the highest priority.

Example:

```
3gpp-Sbi-Message-Priority: 10
```

A client, proxy, and a server uses the "3gpp-Sbi-Message-Priority" value when setting or evaluating the priority of a message. The client assigns the request priority by adding the "3gpp-Sbi-Message-Priority" custom HTTP header to the message and setting its value. If the "3gpp-Sbi-Message-Priority" custom HTTP header isn't present in a response message, then the HTTP nodes use the priority indicated in the "3gpp-Sbi-Message-Priority" of the associated request message. If the server wants to assign a different priority to the response message than the server assigns the response priority by adding the "3gpp-Sbi-Message-Priority" custom HTTP header to the message and setting its value.

### Message-Priority Indication over GTP-C

An overloaded node performs message prioritization when handling incoming messages during an overloaded condition based on the relative GTP-C message priority signaled in the GTP-C header.

When message throttling is performed:

- GTP requests related to priority traffic (eMPS as described in *3GPP TS 22.153*) and emergency have the highest priority. Depending on regional/national requirements and network operator policy, these GTP requests are the last to be throttled when applying traffic reduction. The priority traffic is exempted from throttling due to GTP overload control up to the point where the requested traffic reduction cannot be achieved without throttling the priority traffic.
- For other types of sessions, message throttling considers the relative priority of the messages so that low priority messages are considered for throttling before the other messages. The relative priority of the messages is derived from the relative priority of the procedure for which the message is being sent (as specified in clause 12.3.9.3.2) or derived from the session parameters such as APN and ARP.

The high priority messages are given lower preference to throttle and low priority messages are given higher preference to throttle. An overloaded node also applies these message prioritization schemes when handling incoming initial messages during an overloaded condition, as part of the self-protection mechanism.

A sending GTP-C entity determines the relative message priority to signal in the message according to either procedure based or session parameters. If the message affects multiple bearers (for example, Modify Bearer Request), the relative message priority considers the highest priority ARP among all the bearers.

A GTP-C entity sets the same message priority in a Triggered message or Triggered Reply message as received in the corresponding Initial message or Triggered message respectively. For incoming GTP-C messages that do not have a message priority in the GTP-C header, the receiving GTP-C entity:

- Applies a default priority if the incoming message is an Initial message.
- Applies the message priority sent in the Initial message or Triggered message if the incoming message is a Triggered or Triggered Reply message respectively.

The nodes in the network homogenously support this feature; otherwise an overloaded node processes initial messages received from the non-supporting nodes according to the default priority and processes initial messages received from the supporting nodes according to the message priority signaled in the GTP-C message.

### Message-Prioritization based on Session Parameters

Message prioritization is also performed based on the session parameters such as APN and ARP. The procedures and messages associated with the higher priority sessions are given lesser preference while throttling, as compared to the procedures and messages associated with the lower priority sessions. Within each group of sessions, the messages are further prioritized based on the category of the procedure for which the message is being sent.

## Message Prioritization Based on Procedures

Message prioritization is performed based on the relative priority of the procedure for which the message is being sent. Procedures are grouped into various categories and each of these categories are assigned a priority. Also, within a given category of procedures, messages could be further prioritized based on session parameters such as APN, QCI, ARP and/or LAPI.

Messages with a high priority are given lower preference to throttle and messages with low priority are given higher preference to throttle. The grouping of the procedures isn't performed based on an individual GTP-C entity but while considering all the procedures in general. A GTP-C entity considers the procedures applicable to it and prioritizes message throttling based on the category of the procedure. The categories are listed in decreasing order of priority with category 1 having the highest priority. For each category, a nonexhaustive list of messages is provided. Any existing or newly defined message in future is considered based on the category (as specified below) of the procedure for which the message is sent.

- 1. UE session mobility within and across 3GPP or non-3GPP access:** Procedures involving active or idle mode UE mobility, such that GTP-C signalling involved are classified under this category. Some examples are X2/S1 based handover with/without an SGW change, TAU/RAU with a change of MME/SGSN with/without an SGW change, 3GPP access to trusted non-3GPP access handover, etc. Throttling of these messages during the procedures related to UE session mobility results in the failure of the corresponding procedures, this could result potentially in the loss of the PDN connection and/or the interruption of the services. As a result, the messages, as identified below, when sent during the procedures belonging to this category, must be considered with the highest priority and hence, must be given the lowest preference to throttle.
  - Create Session Request.
  - Create Session Request with "handover" indication bit set.
  - Modify Bearer Request.
  - Modify Bearer Request with "handover" indication bit set.
  - Modify Access Bearer Request.
- 2. Release of PDN connection or bearer resources:** Procedures resulting in the deactivation of an existing PDN connection, the deactivation of bearer(s) or of data forwarding tunnel of an UE leads to freeing up of the resources at the overloaded node. This can potentially ease the overload situation, since the freed up resources can be used for serving the remaining of the UEs. Thus, the messages belonging to this category resulting in the deactivation of PDN connection or bearer(s) or data forwarding tunnel(s), as identified below, must be treated with the next lower level of priority and given the corresponding preference whilst throttling:
  - Delete Session Request.
  - Delete Bearer Request.
  - Delete Bearer Command.
  - Delete Indirect Data Forwarding Tunnel Request.
- 3. Miscellaneous session management procedures:** This category consists of the session management procedures, except PDN connection creation and bearer creation/modification procedures. Some examples are location reporting, when it isn't combined with other mobility procedures, Service request and S1 release procedure. These procedures do not severely impact the on-going service of the UE. Hence, the messages, as identified below, when sent during the procedures identified under this category, must be

treated with the next lower level of priority and hence, shall be given the corresponding preference whilst throttling.

- Release Access Bearer Request
- Modify Bearer Request.
- Change Notification
- Suspend Notification
- Resume Notification

**4. Request for new PDN Connection/bearer resources/modification of existing bearer resources:**

Procedures requesting the creation of PDN connection, creation or modification of bearer(s) or creation of data forwarding tunnel are be classified in this category. Throttling of the messages belonging to this category result in denial of new services while continuing with the existing services. This is the natural outcome of an overload condition, an overloaded node, due to lack of resources, isn't able to provide new services while trying to maintain the existing services. When the messages identified below are sent during the procedures belonging to this category are considered with the lowest level of priority and given highest preference to throttle:

- Create Session Request during PDN connection request
- Create Bearer Request.
- Update Bearer Request.
- Bearer Resource Command.
- Modify Bearer Command.
- Create Indirect Data Forwarding Tunnel Request.
- Downgrade the DSCP marking of the data packets for the session when quota exhausts.

### Message-Priority Header for PFCP

When the message throttling is performed:

- PFCP requests related to priority traffic (that is, eMPS as described in *3GPP TS 22.153*) and emergency have the highest priority. Depending on regional/national requirements and network operator policy, these PFCP requests are the last to be throttled when applying traffic reduction. Throttling exempts the priority traffic 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, the message throttling considers the relative priority of the messages so that the messages with low priority are first considered for the throttling. The relative priority of the messages is derived from the relative priority of the procedure for which the message is being sent or derived from the session parameters such as APN and ARP.

An overloaded node (UPF, SMF) may apply these message prioritization schemes when handling incoming initial messages during an overloaded condition, as part of a self-protection mechanism. Incoming messages are handled during an overloaded condition based on the relative PFCP message priority signaled in the PFCP header.

A PFCP entity determines whether to set and use the message priority in PFCP signalling, based on operator policy. A sending PFCP entity determines the relative message priority to signal in the message which are derived from the session parameters such as APN and ARP. If the message affects multiple bearers, the relative message priority is determined considering the highest priority ARP among all the bearers. A PFCP entity must 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:

- Applies a default priority if the incoming message is a Request message.
- Applies the message priority sent in the Request message if the incoming message is a Response message.

The SMF and UPF functions in the network homogeneously support this feature; otherwise an overloaded node will process the Request messages received from the non-supporting nodes according to the default priority and Request messages received from supporting nodes will be processed according to the message priority signalled in the PFCP message.

## Mission Critical Services

A Mission Critical Service (MCX Service) is a communication service that enables capabilities of Mission Critical Applications. The MCX service is provided to end users from Mission Critical Organizations and mission critical applications for businesses and organizations. An MCX Service is either Mission Critical Push To Talk (MCPTT), Mission Critical Video (MCVideo), or Mission Critical Data (MCData) and represents a set of requirements between two or more MCX Service types.

MCX Services are based on the ability to invoke, modify, maintain, and release sessions with priority, and deliver the priority media packets under network congestion conditions. These services are supported in a roaming environment when roaming agreements are in place and where regulatory requirements apply.

An MCX subscription allows users to receive priority services if the network supports MCX. MCX Users require the 5GS functionality for real-time, dynamic, secure and limited interaction with the QoS and policy framework for modification of the QoS and policy framework by authorized users.

## Expanded Prioritization for VoLTE/VoNR/Emergency Calls

The SMF+PGW-C supports Expanded Prioritization for VoLTE/VoNR/Emergency calls. The National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services (NGN-PS) (formerly called NGN Government Emergency Telecommunications Service (GETS)) is a set of voice, video and data services that are based on services available from public packet-switched Service Providers. The NS/EP NGN-PS provides priority treatment for a Service User's NS/EP communications and is particularly needed when the Service Providers' networks are impaired due to congestion and/or damage from natural disasters (such as floods, earthquakes and hurricanes) and man-made disasters (such as physical, cyber or other forms of terrorist attacks).

As part of this feature, the PGW-C control message is marked with DSCP marking and also for control message belonging to the eMPS session or containing Allocation and Retention Priority (ARP) associated with the eMPS profile.



## DSCP Marking for N3/S5-U/S2-B over PFCP

### Transport Level Marking

Transport level marking is 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 EPC, the S-GW and P-GW perform transport level marking on a per EPS bearer basis. For 5GC, the S-GW and P-GW perform transport level marking on a per QoS flow basis.

The UPF performs transport level marking with a DSCP value based on the mapping from the 5QI, the Priority Level (if explicitly signaled), and optionally the ARP priority level configured at the SMF. The CP function controls transport level marking by providing the DSCP in the ToS or Traffic Class within the Transport Level Marking IE in the FAR (associated to the PDR matching the traffic to be marked).

The UP function performs transport level marking for the detected traffic and sends the marked packet to the peer entity. The CP function changes transport level marking by changing the Transport Level Marking IE in the related FAR.

### WPS Profile Support

The SMF+PGW-C supports the WPS profile defined with ARP and DSCP marking value to be set for GTP-C and PFCP Protocol IP-headers. The WPS profile sets the message priority in the GTP-C and PFCP protocols.

The SMF+PGW-C allows a maximum of 64 WPS profiles and each WPS profile will be associated under the DNN profile. See the [Configuring Wireless Priority Services, on page 836](#) section for more information.

## Converged Core Refactoring Changes

This section describes the changes related to converged core refactoring in this chapter.

- The "N4" or "n4" prefix in the message and statistic names are removed.
- The "SMF" or "smf" prefix in the message and statistic names are removed.
- A new label is added for interface type in the Grafana query.

## How it Works

### License Information

The WPS feature requires a license to be enabled on the SMF+PGW-C to support the related features - MPS, MCX, Prioritization for VoLTE/VoNR/Emergency Service. Contact your Cisco account representative for more information on how to obtain a license.

### Standards Compliance

The Wireless Priority Services feature complies with the following standards:

- *3GPP TS 22.153*
- *3GPP TS 23.228*

- 3GPP TS 23.282
- 3GPP TS 23.379
- 3GPP TS 23.501
- 3GPP TS 23.502
- 3GPP TS 23.503
- 3GPP TS 24.301

## Configuring Wireless Priority Services

This section describes how to configure the Wireless Priority Services feature.

### Configuring the WPS Profile

Use the following sample configuration to configure the WPS profile.

```
config
  profile wps wps_profile_name
    arp arp_value
    dscp n3 n3_value
    message-priority [ gtpc pfcpc ]
  end
```

#### NOTES:

- **profile wps wps\_profile\_name**: Accesses the Wireless Priority Services Profile configuration. *wps\_profile\_name* must be an alphanumeric string of 1 to 63 characters.
- **arp arp\_value**: Specifies the range of ARP levels. *arp\_value* must be an integer from 1 to 15 separated either by "," or "-".
- **dscp n3 n3\_value**: Specifies the DSCP marking value for N3. *n3\_value* specifies the UP DSCP marking value within the range 0 to 0x3F.
- **message-priority { gtpc pfcpc }**: Specifies the message priority for GTP-C and PFCPC.

#### Verifying the WPS Profile Configuration

This section describes how to verify the WPS Profile configuration.

Execute the **show running-config** command to view the configuration.

The following is an example of the **show running-config** command output.

```
show running-config profile wps wps1
  profile wps wps1
  arp 1,4-6,9
  dscp n3 10
  message-priority [ pfcpc gtpc ]
  exit
```

## Associating WPS Profile under DNN Profile

Use the following sample configuration to associate the WPS profile with the configured DNN profile.

```
config
  profile dnn intershat
    wps-profile wps_profile_name
  end
```

### NOTES:

- **wps-profile** *wps\_profile\_name*: Enables the Wireless Priority Services Profile configuration. This profile is configured under the existing DNN profile configuration.

### Verifying WPS Profile under DNN Profile

This section describes how to verify the WPS profile configuration under the DNN profile.

Execute the **show running-config** command to view the configuration.

The following is an example of the **show running-config** command output.

```
show running-config profile dnn intershat
profile dnn intershat
network-element-profiles chf chf1
network-element-profiles amf amf1
network-element-profiles pcf pcfl
network-element-profiles udm udml
charging-profile chgprfl
virtual-mac b6:6d:47:47:47:47
wps-profile wps1
ssc-mode 2 allowed [ 3 ]
session type IPV4 allowed [ IPV6 IPV4V6 ]
upf apn intershat
exit
```

## WPS OAM Support

### SMF Session Gauge Counters

The "wps" label is introduced at the SMF service to account for session-level gauge counters that support WPS and non-WPS functionality.

For example:

```
smf_session_counters{always_on="disable",app_name="smf",cluster="smf",data_center="unknown",dnn="intershat",
instance_id="0",pdu_type="ipv4",rat_type="NR",service_name="smf-service",ssc_mode="ssc_mode_1",wps="non_wps"}
  10
smf_session_counters{always_on="disable",app_name="smf",cluster="smf",data_center="unknown",dnn="intershat",
instance_id="0",pdu_type="ipv4",rat_type="NR",service_name="smf-service",ssc_mode="ssc_mode_1",wps="wps"}
  20
```

### N4 Interface Metrics

The N4 interface counters related to message priority include:

- SESSION\_DELETION\_REQUEST
- SESSION\_ESTABLISHMENT\_REQUEST

- SESSION\_MODIFICATION\_REQUEST

An example of the N4 interface metrics:

```
proto_pfcfp_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="SESSION_DELETION_REQUEST",msgpriority=true,
service_name="protocol",status="accepted",transport_type="origin"} 4
proto_pfcfp_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="SESSION_ESTABLISHMENT_REQUEST",msgpriority=true,
service_name="protocol",status="accepted",transport_type="origin"} 6
proto_pfcfp_msg_total{app_name="SMF",cluster="Local",data_center="DC",instance_id="0",
message_direction="outbound",message_name="SESSION_MODIFICATION_REQUEST",msgpriority=true,
service_name="protocol",status="accepted",transport_type="origin"} 20
```

### GTPv2 Metrics

The GTPv2 counters related to message priority include:

- NumCreateBearerSuccess
- NumRxCreateBearerRes
- NumTxCreateSessionReq

An example of the GTPv2 metrics:

```
gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumCreateBearerSuccess",instance_id="0",interface_type="S5",priority_msg="true",service_name="gtpc-ep"}
2
gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumRxCreateBearerRes",instance_id="0",interface_type="S5",priority_msg="true",service_name="gtpc-ep"}
2
gtpc_app_priority_events{app_name="SMF",cluster="Local",data_center="DC",
event_type="NumTxCreateSessionReq",instance_id="0",interface_type="S5",priority_msg="true",service_name="gtpc-ep"}
2
```

### KPIs

Following KPIs are supported for this feature:

```
sum(policy_dynamic_pcc_rules_total{pccrule_change_type="binding_param_change",event="attempted"})
```

```
sum(policy_dynamic_pcc_rules_total{pccrule_change_type="binding_param_change",event="success"})
```

```
sum(policy_dynamic_pcc_rules_total{pccrule_change_type="binding_param_change",event="failure"})
```

**Table 252: Statistics to track number of times qci/arp modified**

KPI Name	Type	Description/Formula	Label
policy_dynamic_pcc_rules_total	counter	Total number of dynamic pcc rules added/modified/deleted as part of different procedures.	pccrule_change_type,status



# CHAPTER 56

## SMF Serviceability Support

- [Feature Summary and Revision History, on page 839](#)
- [Feature Description, on page 840](#)
- [show subscriber pei, on page 840](#)
- [show subscriber gpsi, on page 841](#)
- [show endpoint info, on page 842](#)

### Feature Summary and Revision History

#### Summary Data

*Table 253: Summary Data*

Applicable Product(s) or FunctionalArea	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Enabled – Always-on
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

#### Revision History

*Table 254: Revision History*

Revision Details	Release
The 5G SMF Serviceability CLI Enhancements are fully qualified in this release.	2020.03.0

Revision Details	Release
<p>First introduced.</p> <p>This feature is not fully qualified in this release. For more information, contact your Cisco Account representative.</p>	2020.02.0

## Feature Description

This chapter describes serviceability CLI enhancements to display the information about the deployed pods.

### show subscriber pei

*Table 255: show subscriber pei*

Field	Description
policy	Displays the policy information.
ipv4-addr	Displays the IPv4 pool name.
dnn	Displays the DNN value.
pcf	Displays the PCF Address.
rat	Displays the RAT Type—nr/e-utran/wlan information.
connectivity	Displays the connectivity—4G or 5G.
ipv4-range	Displays the IPv4 address range.
chf	Displays the CHF address.
pei	Displays the Permanent Equipment Identifier (PEI).
udm	Displays the UDM address.
upfEpKey	Displays the UPF address EP key information.
ipv6-pfx	Displays the IPv6 prefix information.
ipv6-pool	Displays the IPv6 Pool name.
chfGroupId	Displays the CHF address group ID information.
gpsi	Displays the Generic Public Subscription Identifier (GPSI).
pcfGroupId	Displays the PCF address group ID.
upf	Displays the UPF address.

Field	Description
ipv4-pool	Displays the IPv4 pool name.
ipv6-range	Displays the IPv4 address range.
amf	Displays the AMF address.
supi	Displays the SUPI value.
access	Displays the access information.

## show subscriber gpsi

*Table 256: show subscriber gpsi*

Field	Description
policy	Displays the policy information.
ipv4-addr	Displays the IPv4 pool name.
dnn	Displays the DNN value.
pcf	Displays the PCF Address.
rat	Displays the RAT Type—nr/e-utran/wlan information.
connectivity	Displays the connectivity—4G or 5G.
ipv4-range	Displays the IPv4 address range.
chf	Displays the CHF address.
pei	Displays the Permanent Equipment Identifier (PEI).
udm	Displays the UDM address.
upfEpKey	Displays the UPF address EP key information.
ipv6-pfx	Displays the IPv6 prefix information.
ipv6-pool	Displays the IPv6 pool name.
chfGroupId	Displays the CHF address group ID information.
gpsi	Displays the Generic Public Subscription Identifier (GPSI).
pcfGroupId	Specifies PCF Address group ID.
upf	Displays the UPF address.
ipv4-pool	Displays the IPv4 pool name.

Field	Description
ipv6-range	Displays the IPv4 address range.
amf	Displays the AMF address.
supi	Displays the SUPI value.
access	Displays the access information.

## show endpoint info

*Table 257: show endpoint info*

Field	Description
endpoint	Specifies the name of the endpoint.
address	Specifies the host and port of endpoint.
type	Specifies the type of endpoint.
status	Specifies current Status of endpoint.
interface	Specifies the interface name of endpoint.
internal	Specifies the type of endpoint (Internal/External).
startTime	Specifies the start time of endpoint.
stoppedTime	Specifies the end time of endpoint.





# CHAPTER 57

## Troubleshooting Information

- [Feature Summary and Revision History, on page 843](#)
- [clear Commands, on page 844](#)
- [show Commands, on page 845](#)
- [SMF Monitoring, on page 849](#)

## Feature Summary and Revision History

### Summary Data

*Table 258: Summary Data*

Applicable Product(s) or FunctionalArea	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 259: Revision History*

Revision Details	Release
Added Troubleshooting information for RADIUS, Roaming, and Option-3x features.	2021.01.0
First introduced.	Pre-2020.02.0

# clear Commands

## clear subscriber

*Table 260: clear subscriber Command Output Description*

Field	Description
all	Clears all the sessions.
amf	Clears subscriber based on AMF address.
chf	Clears subscriber based on CHF address.
dnn	Clears subscriber based on DNN value.
gtp-peer	Clears subscriber based on GTP-PEER address.
ipv4-pool	Clears subscriber based on IPv4 pool name.
ipv4-range	Clears subscriber based on IPv4 address-range.
ipv6-pool	Clears subscriber based on IPv6 pool name.
ipv4-range	Clears subscriber based on IPv6 prefix-range.
ipv6-range	Clears subscriber based on IPv6 prefix-range.
namespace	Clears subscriber based on the respective namespace. Default: none.
pcf	Clears subscriber based on PCF address.
policy	Clears subscriber based on policy information.
purge	Clears true, if purged locally.
sgw	Clears subscriber based on the S-GW address.
smf	Clears subscriber based on the SMF address.
supi	Clears subscriber based on the SUPI value.
	The output modifiers.

## clear subscriber supi imsi <imsi\_value>

*Table 261: clear subscriber supi imsi <imsi\_value> Command Output Description*

Field	Description
ebi	Clears subscriber based on EPS bearer ID.

Field	Description
imsi	Clears subscriber based on IMSI.
purge	Clears true, if purged locally.
	Output modifier.

## clear subscriber supi imsi <imsi\_value> psid <psid\_value>

Table 262: clear subscriber supi imsi <imsi\_value> psid <psid\_value> Command Output Description

Field	Description
ebi	Clears subscriber based on EPS bearer ID.
imsi	Clears subscriber based on IMSI.
psid	Clears subscriber based on Service ID.
purge	Clears true, if purged locally.
	Output modifier.

## show Commands

### show helm

The **show helm** command displays the version information for the SMF system image.

### show peers all

This command displays the list of external inbound and outbound connections established by SMF.

Table 263: show peers all Command Output Description

Field	Description
additionalDetails	Displays the additional details.
connectedTime	Displays the connected time.
direction	Displays the direction.
podInstance	Displays the pod instance.
rpc	Displays the interface RPC.
type	Displays the interface type.

Field	Description
	Displays the output modifiers.

## show subscriber

This commands displays the existing show subscriber CLI output with the newly added CLI output.

**Table 264: show subscriber Command Output Description**

Field	Description
all	Displays the information for all SUPIs or IMEIs.
amf	Displays the AMF address.
chf	Displays the CHF address.
count	Displays the number of sessions.
debug	Displays the debugging information.
dnn	Displays the DNN value.
gtp-peer	Displays the GTP-peer address.
namespace	Displays the product namespace under which to search. Default: none.
pcf	Displays the PCF address.
rat	Displays the RAT type as 4G or 5G.
supi	Displays the SUPI value.
udm	Displays the UDM address.
upf	Displays the UPF address.
	The output modifiers.

## show subscriber count

This command displays the CLI options for the count CLI command.

**Table 265: show subscriber count Command Output Description**

Field	Description
all	Displays all the SUPIs.
amf	Displays the AMF address.
chf	Displays the CHF address.

Field	Description
dnn	Displays the DNN value.
gtp-peer	Displays the GTP-peer address.
pcf	Displays the PCF address.
rat	Displays the RAT type as 4G or 5G.
supi	Displays the specific SUPI value.
udm	Displays the UDM address.
upf	Displays the UPF address.
	Displays the output modifiers.

## show subscriber count all

This command displays the total number of sessions for all the SUPIs.

**Table 266: show subscriber count all Command Output Description**

Field	Description
	Displays the output modifiers.

## show subscriber count chf <chf\_address>

This command displays the total number of sessions for the specified parameters.

**Table 267: show subscriber count chf <chf\_address> Command Output Description**

Field	Description
amf	Displays the AMF address.
dnn	Displays the DNN value.
gtp-peer	Displays the GTP-peer address.
pcf	Displays the PCF address.
rat	Displays the RAT type as 4G or 5G.
udm	Displays the UDM address.
upf	Displays the UPF address.
	Displays the output modifiers.

```
show subscriber count chf <chf_address> dnn <dnn_value>
```

## show subscriber count chf <chf\_address> dnn <dnn\_value>

This command displays the total number of sessions for the specified parameters.

*Table 268: show subscriber count chf <chf\_address> dnn <dnn\_value> Command Output Description*

Field	Description
amf	Displays the AMF address.
gtp-peer	Displays the GTP-peer address.
pcf	Displays the PCF address.
rat	Displays the RAT type as 4G or 5G.
udm	Displays the UDM address.
upf	Displays the UPF address.
	Displays the output modifiers.

## show subscriber count supi <supi\_value>

This command displays the total number of sessions for the specific SUPI value.

*Table 269: show subscriber count supi <supi\_value> Command Output Description*

Field	Description
	Displays the output modifiers.

## show subscriber debug-info supi <supi\_value>

This command displays the debug information for the specific SUPI value where the PSID value is optional.

*Table 270: show subscriber debug-info supi <supi\_value> Command Output Description*

Field	Description
psid	Displays the Provider Service Identifier.

## show subscriber debug-info supi <supi\_value> psid <psid\_value>

This command displays the debug information for the specific SUPI and PSID combination.

*Table 271: show subscriber debug-info supi <supi\_value> psid <psid\_value> Command Output Description*

Field	Description
	Displays the output modifiers.



**Note** Currently, the SMF does not validate the serving PLMN received on N11 interface. Also, the SMF does not validate the UE PLMN when the N11 smContextCreate or GTP createSessionRequest is received.

The PLMN value received in the NSSAI included in the PCO request remain the same as the PLMN configured on the SMF.

## show subscriber supi <supi\_value> psid <psid\_value> full

This command displays detailed subscriber information.

*Table 272: show subscriber supi <supi\_value> psid <psid\_value> full Command Output Description*

Field	Description
sessTimeStamp	Connected time of the session.
callDuration	Call duration.
commonId	Call ID equivalent for the session (common ID).
ipPool, ipv6Pool	IP pool from which the address has been allocated.
linkedEbi	Linked EBI for a session.
snssai	sNssai details.
smfIwkEpsInd	SMF EPS IWK decision based on AMF and UDM data.
TotalNumberOfPdrs	Number of associated PDRs.
TotalNumberOfFars	Number of associated FARs.
TotalNumberOfQers	Number of associated QERs.
TotalNumberOfUrrs	Number of associated URRs.
upfSeid	Remote SEID for a particular UPF session.
epsInterworking Indication	EPS interworking indication status of AMF.
ebi	ERAB ID allocated for each flow.
revalidationTime	Revalidation timer information for a session.

## SMF Monitoring

This section provides information on CLI commands for monitoring the health of 5G SMF.

## SMF Data Collection Method

The SMF application CLI data is collected at the following levels:

- SMF Application CLI:
  - SMF Ops-Center CLI
  - CEE Ops-Center CLI

### Application CLI

The following table lists the CLI commands to be executed on the SMF Ops-Center for RADIUS.

CLI Command	Description	Comments
<b>show subscriber supi</b> <i>supi_id</i> <b>full</b>	Displays detailed subscriber information.	Additional information for accounting, authentication, and RADIUS URR is added.
<b>show ipam dp</b> <i>dp-name</i> <b>ipv4-addr</b>	Displays IPAM data plane allocation for a specific UPF.	Additional information added to display VRF tag and static pool.
<b>show ipam dp</b> <i>dp-name</i> <b>ipv6-prefix</b>	Displays range of IPv6 pool allocated to the UPF.	Additional information added to display VRF tag and static pool.
<b>show radius</b>	Displays RADIUS endpoint accounting and authentication statistics.	
<b>show radius dyn-auth</b>	Displays statistics for RADIUS Disconnect/COA from RADIUS endpoint.	CoA is not supported in the SMF releases 2020.04 and 2021.01.
<b>show radius acct-server</b>	Displays RADIUS endpoint accounting statistics.	Per server details can also be fetched.
<b>show radius auth-server</b>	Displays RADIUS endpoint authentication statistics.	Per server details can also be fetched.
<b>show endpoint</b>	Displays internal and external connections.	Additional RADIUS-specific endpoint information is added.
<b>show peers</b>	Displays the list of external inbound and outbound connections established by the SMF.	Additional information for RADIUS Authentication and Accounting server is added.

### CEE Ops-Center CLI

The following table lists the CLI commands to be executed on the CEE Ops-Center.

CLI Command	Description	Comments
<b>show alerts active</b>	Displays active alerts.	New alerts are added for RADIUS.



CLI Command	Description	Comments
<b>show bulk-stats current</b>	Displays bulk statistics.	New bulk statistics are added for RADIUS.

## SMF Data Collection - CLI Output

### SMF Ops-Center CLI Commands

The CLI execution fails due to various reasons. In such cases, the output of the CLI contains the word "Error". The Validation Criteria looks for "Error" in a case-insensitive search.

The following are examples.

```
***** LASMF006 - show sessions commit-pending *****
Error: 'sessions commit-pending': Error in callback: java.lang.IllegalStateException:
Expected BEGIN_OBJECT but was STRING at line 1 column 1 path $

***** LASMF006 - show running-status *****
Error: application timeout
```

### Subscriber Details for RADIUS-specific Information

The **show subscriber supi *supi\_id* full** CLI command displays the subscriber details for RADIUS-specific use cases.

```
[unknown] smf# show subscriber supi imsi-123456789012345 full
subscriber-details
{
...
"alwaysOn": "None",
  "dcnr": "None",
  "wps": "Wps Session",
  "ratType": "NR",
  "idleTimeout": 600,      << can be overwritten from Radius in Auth Resp
  "sessTimeout": 1200,   << can be overwritten from Radius in Auth Resp

  "radiusEpInfo": "198.18.1.20:1812",
  "authAlg": "pap-default",
  "authStatus": "Authenticated"
...
...
  "accountingEnabled": "true",
  "n40ChargingEnabled": "true",
  "acctSessId": "198.15.1.40016777221"
...
...
"upfServData": {
  "numberOfTunnels": 2,
  "smfSeid": 72057615828912656,
  "UPState": "Activated",
  "urrInfo": [
    {
      "id": 2147483657,
      "chgName": "radiusurr",
      "method": {
        "duration": "false",
```

```

    "volume": "true",
    "event": "false"
  },

```

## Subscriber Details for Roaming-specific Information

The **show subscriber supi *supi\_id* nf-service smf full** CLI command displays the roaming status of a UE.

```

[unknown-smf] smf# show subscriber supi imsi-123456789012345 nf-service smf full
subscriber-details
{
...
  "authStatus": "Unauthenticated",
  "roamingStatus": "Vistor LBO",    <<< In-Roamer UE Roaming Status
  "uePlmnId": {
    "mcc": "123",
    "mnc": "456"
  }
...
  "authStatus": "Unauthenticated",
  "roamingStatus": "Roamer",      <<< Out-Roamer UE Roaming Status
  "uePlmnId": {
    "mcc": "123",
    "mnc": "456"
  }
...
  "authStatus": "Unauthenticated",
  "roamingStatus": "Homer",
  "uePlmnId": {
    "mcc": "123",
    "mnc": "456"
  }
}

```

## Subscriber Details with DCNR and Presence Reporting Enabled

The **show subscriber nf-service smf supi *supi\_id* full** CLI command displays the DCNR active session with presence reporting enabled for the Option-3x feature.

```

[unknown] smf# show subscriber nf-service smf supi imsi-310260789012345 full
subscriber-details
{
  "subResponses": [
    {
      "status": true,
      "genericInfo": {
        "supi": "imsi-310260789012345",
        "pei": "imei-123456786666660",
        "pduSessionId": 5,
        "pduSesstype": "Ipv4PduSession",
        "accessType": "3GPP_ACCESS",
        "dnn": "fast.t-mobile.com",
        "plmnId": {
          "mcc": "123",
          "mnc": "456"
        }
      },
...
      "alwaysOn": "None",
      "dcnr": "Enabled",
      "wps": "Non-Wps Session",
      "ratType": "EUTRA",
      "ueType": "NR Capable UE",
      "iwkEpsInd": true,
    }
  ]
}

```

```

        "sessTimeStamp": "2021-01-12 12:40:39.931012285 +0000 UTC",
        "callDuration": "4m25.36784895s",
        "ipPool": "poolv4",
        "commonId": 16777223,
        "linkedEbi": 5,
        "smfIwkEpsInd": true,
        "snssai": {
            "sd": "Abf123",
            "sst": 1
        },
        "authStatus": "Unauthenticated",
        "roamingStatus": "Roamer",
        "uePlmnId": {
            "mcc": "310",
            "mnc": "260"
        }
    },
    "policySubData": {
        "TotalDynamicRules": 2,
        "TotalFlowCount": 2,
        "TotalNonGBRFlows": 1,
        "TotalGBRFlows": 1,
        ...
        "presenceReporting": "Enabled",
        "praList": [
            {
                "praId": "0x80000b",
                "presenceState": "Inactive"
            },
            {
                "praId": "0x800000",
                "presenceState": "InArea"
            },
            {
                "praId": "0x80000a",
                "presenceState": "OutOfArea"
            }
        ]
    },
    ...
}
]
}

```

### Range of IPv4 Allocated to UPF

The **show ipam dp *dp\_name* ipv4-addr** CLI command displays the IP pool chunks allocated to UPF. This includes the VRF tag information and details such as whether the pool defined is a static or dynamic pool.

**[unknown] smf# show ipam dp 198.18.1.3 ipv4-addr**

```

=====
Flag Indication: S(Static) O(Offline)
N/P Indication: N(Native InstId) P(Peer InstId)
=====

```

StartAddress	EndAddress	AllocContext	Route	N/P	Utilization	Flag
16.0.0.0	16.0.0.31	v4pool3(vrf3@ISP)	16.0.0.0/27	-		S
16.0.0.0	16.0.0.31	v4pool4(vrf4@ISP)	16.0.0.0/27	-		S

Range of IPv6 Allocated to UPF

```

16.0.0.32          16.0.0.63          v4pool3(vrf3@ISP) 16.0.0.32/27    -
S
16.0.0.32          16.0.0.63          v4pool4(vrf4@ISP) 16.0.0.32/27    -
S
16.0.0.64          16.0.0.95          v4pool3(vrf3@ISP) 16.0.0.64/27    -
S
16.0.0.64          16.0.0.95          v4pool4(vrf4@ISP) 16.0.0.64/27    -
S
16.0.0.96          16.0.0.127         v4pool3(vrf3@ISP) 16.0.0.96/27    -
S
16.0.0.96          16.0.0.127         v4pool4(vrf4@ISP) 16.0.0.96/27    -
S
16.0.0.128         16.0.0.159         v4pool4(vrf4@ISP) 16.0.0.128/27   -
S
16.0.0.160         16.0.0.191         v4pool4(vrf4@ISP) 16.0.0.160/27   -
S
16.0.0.192         16.0.0.223         v4pool4(vrf4@ISP) 16.0.0.192/27   -
S
16.0.0.224         16.0.0.255         v4pool4(vrf4@ISP) 16.0.0.224/27   -
S
=====

```

Range of IPv6 Allocated to UPF

The **show ipam dp dp\_name ipv6-prefix** CLI command displays the IP pool chunks allocated to UPF. This includes the VRF tag information and details such as whether the pool defined is a static or dynamic pool.

**[unknown] smf# show ipam dp 198.18.1.3 ipv6-prefix**

```

=====
Flag Indication: S(Static) O(Offline)
N/P Indication: N(Native InstId) P(Peer InstId)
=====
StartAddress      EndAddress        AllocContext      Route
N/P  Utilization    Flag
=====
3001:db0::        3001:db0:0:3fff:: v6pool4(vrf4@ISP) 3001:db0::/50    -
S
3001:db0::        3001:db0:0:3fff:: v6pool3(vrf3@ISP) 3001:db0::/50    -
S
3001:db0:0:4000:: 3001:db0:0:7fff:: v6pool4(vrf4@ISP) 3001:db0:0:4000::/50 -
S
3001:db0:0:4000:: 3001:db0:0:7fff:: v6pool3(vrf3@ISP) 3001:db0:0:4000::/50 -
S
=====
[unknown] smf#

```

RADIUS Endpoint Authentication and Accounting Statistics

The **show radius** CLI command displays statistics for RADIUS Authentication and Accounting from RADIUS endpoint.

**[unknown] smf# show radius**

```

radius
-----
Server: 198.18.1.20, port: 1812, status: up, port-type: Auth
3 requests, 0 pending, 0 retransmits
2 accepts, 0 rejects, 1 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 1 ms latest rtt
-----
Server: 10.84.115.45, port: 1813, status: up, port-type: Acct

```

```

3 requests, 0 pending, 6 retransmits
0 responses, 3 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt
-----
Server: 198.18.1.20, port: 1813, status: up, port-type: Acct
5 requests, 0 pending, 3 retransmits
3 responses, 2 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 6 ms latest rtt
-----
[unknown] smf#

```

**[unknown] smf# show radius acct-server**

```

-----
Server: 10.84.115.45, port: 1813, status: up, port-type: Acct
3 requests, 0 pending, 6 retransmits
0 responses, 3 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 0 ms latest rtt
-----
Server: 198.18.1.20, port: 1813, status: up, port-type: Acct
5 requests, 0 pending, 3 retransmits
3 responses, 2 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 6 ms latest rtt
-----
[unknown] smf#

```

**[unknown] smf# show radius auth-server**

```

-----
Server: 198.18.1.20, port: 1812, status: up, port-type: Auth
3 requests, 0 pending, 0 retransmits
2 accepts, 0 rejects, 1 timeouts
0 bad responses, 0 bad authenticators
0 unknown types, 0 dropped, 1 ms latest rtt
-----
[unknown] smf#

```

**RADIUS Endpoint Disconnect Message and CoA Statistics**

The **show radius-dyn-auth** CLI command displays statistics for RADIUS Disconnect Message and CoA from RADIUS endpoint.

```

[unknown] smf# show radius-dyn-auth
radius-dyn-auth
-----
IP: 198.18.1.20
-----
COA:
0 total-requests      0 inprocess-requests
  0 retry-request-drops  0 invalid-requests
  0 bad-authenticators  0 internal-errors
0 ack-sent            0 nak-sent
-----
DISCONNECT:
2 total-requests      0 inprocess-requests
  0 retry-request-drops  0 invalid-requests
  0 bad-authenticators  0 internal-errors
1 ack-sent            1 nak-sent
-----
UnknownTypesRcvd: 0
-----
[unknown] smf#

```

## External Inbound and Outbound Connections

The **show peers all** CLI command fetches the list of external inbound and outbound connections established by the SMF.

```
[unknown] smf# show peers all | include Radius
RadiusServer -      10.84.115.45:1813  Outbound  radius-ep-0  Udp  18 hours  Radius
  Status: Active,Type: Acct  1
RadiusServer -      198.18.1.20:1812  Outbound  radius-ep-0  Udp  17 hours  Radius
  Status: Active,Type: Auth  1
RadiusServer -      198.18.1.20:1813  Outbound  radius-ep-0  Udp  17 hours  Radius
  Status: Active,Type: Acct  1
[unknown] smf#
```

## Internal and External Connections

The **show endpoint info** CLI command fetches the list of internal and external connections established by the SMF.

```
[unknown] smf# show endpoint all | include Radius
Radius:198.18.1.4:  198.18.1.4:3799  Udp  Started  RADIUS  false  18 hours
<none>  1
[unknown] smf#
```

## Status of Pods

The **show running-status** CLI command fetches the current status of pods. This is analogous to the K8 **kubectl get pods -n <>** CLI command.

```
[unknown] smf# show running-status | include radius
radius-ep-0      Started      19 hours
[unknown] smf#
```

## Configuration Errors

The **show config-error** CLI command displays the validation criteria — Pass (if there are no entries) or Failed.

```
[unknown] smf# show config-error | include radius
[unknown] smf#
```

## CEE Ops-Center CLI Commands

### RADIUS Alerts

The RADIUS endpoint for MVNO/PAPN flow supports new alerts. Some basic alerts are listed below. The same alerts can be enhanced based on RAT or as required by the users.

#### RADIUS EP Down Alert

Use the following example to configure alerts related to RADIUS EP Down.

```
alerts rules group RadiusEP
rule Radius_Server_Down
  expression "sum by (namespace, radSvrIP, radSvrPort)
(Radius_Server_Status{radSvrPortType=~\"Auth|Acct\"} < 1)"
  duration 15m
  severity major
  type "Processing Error Alarm"
  annotation summary
  value "\"Radius Server: {{ $labels.radSvrIP }}, Port: {{ $labels.radSvrPort }} in namespace:
{{ $labels.namespace }} is DOWN for more than 15min.\""
```

```
exit
exit
```

### *RADIUS Accounting Establishment Failure Threshold Alert*

Use the following example to configure alerts related to RADIUS Accounting Establishment Failure threshold.

```
alerts rules group RadiusEP
rule Radius_Acct_Establish_SR
  expression "sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
Establishment\", radPacketType=\"Rx\", radResult=\"Success\"}[5m])) / sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
Establishment\", radPacketType=\"Tx\"}[5m])) < 0.80"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of successful Radius Accounting Establish
responses received is lesser than threshold"
  exit
exit
```

### *RADIUS Accounting Release Failure Threshold Alert*

Use the following example to configure alerts related to RADIUS Accounting Release Failure threshold.

```
rule Radius_Acct_Release_SR
  expression "sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
Release\", radPacketType=\"Rx\", radResult=\"Success\"}[5m])) / sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"RadiusAcctReq\", procType=\"PDU Session
Release\", radPacketType=\"Tx\"}[5m])) < 0.80"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of successful Radius Accounting Release
responses received is lesser than threshold"
  exit
exit
```

### *RADIUS Authentication Failure Threshold Alert*

Use the following example to configure alerts related to RADIUS Authentication Failure threshold.

```
rule Radius_Auth_SR
  expression "sum by (namespace)
(increase(Radius_Requests_Statistics{radMsgCode=\"SecondaryAuthenReq\", procType=\"PDU
Session Establishment\", radPacketType=\"Rx\", radResult=\"Success\"}[5m])) / sum by
(namespace) (increase(Radius_Requests_Statistics{radMsgCode=\"SecondaryAuthenReq\",
procType=\"PDU Session Establishment\", radPacketType=\"Tx\"}[5m])) < 0.80"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of successful Radius Authentication
Request responses received is lesser than threshold"
  exit
exit
```

### *RADIUS Disconnect Message Failure Threshold Alert*

Use the following example to configure alerts related to RADIUS Disconnect Message Failure threshold.

```

rule Radius_Disconnect_Message_SR
  expression "sum by (namespace)
  (increase(Radius_CoaDM_Requests_Statistics{radMsgCode=\"DisconnectACK\", radPacketType=\"Tx\",
  radResult=\"Success\"}[5m])) / sum by
  (namespace) (increase(Radius_CoaDM_Requests_Statistics{radMsgCode=\"DisconnectRequest\",
  radPacketType=\"Rx\"}[5m])) < 0.80"
  severity major
  type "Communications Alarm"
  annotation summary
  value "This alert is fired when the percentage of successful Disconnect Message (DM)
  responses sent is lesser than threshold"
  exit
  exit
  exit

```

### *RADIUS Server RTT Alert*

Use the following example to configure alerts related to RADIUS server RTT.

```

rule Radius_Server_RTT
  expression "sum by (namespace, radSvrIP, radSvrPort)
  (Radius_Server_Rtt_ms{radSvrPortType=~\"Auth|Acct\"} > 5)"
  duration 15m
  severity warning
  type "Communications Alarm"
  annotation summary
  value "\"RTT for Radius Server: {{ $labels.radSvrIP }}, Port: {{ $labels.radSvrPort }}
  in namespace: {{ $labels.namespace }} is more than 5 ms.\""
  exit
  exit

```

### *RADIUS Accounting Start Initial Message Failure Threshold Alert*

Use the following example to configure alerts related to RADIUS Accounting Start Initial Message Failure threshold.

```

rule Radius_Acct_Start_SR
  expression "sum by (namespace)
  (increase(radius_accounting_message_stats{procedure_type=\"radius_initial\",
  status=\"success\"}[5m])) / sum by (namespace)
  (increase(radius_accounting_message_stats{procedure_type=\"radius_initial\",
  status=\"attempted\"}[5m])) < 0.80"
  severity major
  type "Processing Error Alarm"
  annotation summary
  value "This service based alert is fired when the percentage of successful Radius
  Accounting Start successful response received is lesser than threshold"
  exit
  exit

```

### *RADIUS Accounting Interim/Update Message Failure Threshold Alert*

Use the following example to configure alerts related to RADIUS Accounting Interim/Update Message Failure threshold.

```

rule Radius_Acct_Interim_SR
  expression "sum by (namespace)
  (increase(radius_accounting_message_stats{procedure_type=\"radius_update\",
  status=\"success\"}[5m])) / sum by (namespace)
  (increase(radius_accounting_message_stats{procedure_type=\"radius_update\",
  status=\"attempted\"}[5m])) < 0.80"
  severity major
  type "Processing Error Alarm"

```



```

        annotation summary
        value "This service based alert is fired when the percentage of successful Radius
Accounting Interim Update successful response received is lesser than threshold"
    exit
exit

```

### *RADIUS Accounting Stop/Terminate Message Failure Threshold Alert*

Use the following example to configure alerts related to RADIUS Accounting Stop/Terminate Message Failure threshold.

```

rule Radius_Acct_Stop_SR
    expression "sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_terminate\",
status=\"success\"}[5m])) / sum by (namespace)
(increase(radius_accounting_message_stats{procedure_type=\"radius_terminate\",
status=\"attempted\"}[5m])) < 0.80"
    severity major
    type "Processing Error Alarm"
    annotation summary
        value "This service based alert is fired when the percentage of successful Radius
Accounting Stop successful response received is lesser than threshold"
    exit
exit

```

### *RADIUS Authentication Type Message Failure Threshold Alert*

Use the following example to configure alerts related to RADIUS Authentication Type Message Failure threshold.

```

rule Radius_Auth_Type_SR
    expression "sum by (namespace, radius_auth_algorithm)
(increase(radius_authentication_message_stats{radius_auth_algorithm=\"radius_auth_algorithm.*\",
status=\"success\"}[1m])) / sum by (namespace)
(increase(radius_authentication_message_stats{radius_auth_algorithm=\"radius_auth_algorithm.*\",
status=\"attempted\"}[1m])) < 0.80"
    severity major
    type "Processing Error Alarm"
    annotation summary
        value "This alert is fired when the percentage of successful Radius Auth Type response
received is lesser than threshold"
    exit
exit

```

## **Roamer UE Alerts**

This section describes the alerts supported for roamer UEs. These alerts can be enhanced per RAT based or as per the intent of the end user.

### *In-roamer UE Failure Threshold Alert*

Use the following example to configure alerts related to In-roamer UE Failure Threshold.

```

alerts rules group RoamerUEs
rule In-Roamer_SR
    expression "sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
roaming_status=\"visitor-lbo\", rat_type!=\"\", status=\"Success\"}[5m])) / sum by (namespace)
(increase(smf_service_stats{app_name=\"smf\", roaming_status=\"visitor-lbo\", rat_type!=\"\",
status=\"attempted\"}[5m])) < 0.10"
    severity major
    type "Communications Alarm"
    annotation summary
        value "This alert is fired when the percentage of successful InRoamer is lesser than

```

```

threshold"
  exit
exit

```

### Out-roamer UE Failure Threshold Alert

Use the following example to configure alerts related to Out-roamer UE Failure Threshold.

```

rule Radius_Acct_Release_SR
  rule Out-Roamer_SR
    expression "sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
roaming_status=\"roamer\", rat_type!=\"\", status=\"Success\"}[5m])) / sum by (namespace)
(increase(smf_service_stats{app_name=\"smf\", roaming_status=\"roamer\", rat_type!=\"\",
status=\"attempted\"}[5m])) < 0.10"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when the percentage of successful InRoamer is lesser than
threshold"
    exit
exit

```

### Option-3x: DCNR Enabled UE Alerts

This section describes the alerts supported for DCNR enabled UEs with presence-reporting enabled. These alerts can be enhanced per 4G procedure based or as per the intent of the end user.

Examples of DCNR statistics/gauges: pdn\_sess\_create, pdn\_inter\_sgw\_handover, pdn\_mbr, pcfr\_req\_ded\_brr\_mod, pcfr\_req\_ded\_brr\_create, pcfr\_req\_ded\_brr\_delete, delete\_session\_request, smf\_initiated\_pdn\_detach, ue\_req\_pdn\_sess\_rel, and so on.

### DCNR UE Attach Failure Threshold Alert

Use the following example to configure alerts related to DCNR UE Attach Failure Threshold.

```

alerts rules group DCNRUES
  rule DCNR_UE_SR
    expression "sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
dcnr=\"enable\", rat_type!=\"EUTRA\", status=\"success\",
procedure_type=\"pdn_sess_create\"}[5m])) / sum by (namespace)
(increase(smf_service_stats{app_name=\"smf\", dcnr =\"enable\", rat_type!=\"EUTRA\",
status=\"attempted\", procedure_type=\"pdn_sess_create\"}[5m])) < 0.10"
    severity major
    type "Communications Alarm"
    annotation summary
    value "This alert is fired when attach success rate of DCNR enabled UE lesser than
threshold"
    exit
exit

```

### DCNR UE Attach Failure Threshold Alert with Presence Reporting

Use the following example to configure alerts related to DCNR UE Attach Failure Threshold with presence reporting enabled.

```

rule DCNR_UE_PRA_ENABLE_SR
  expression "sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
dcnr=\"enable\", rat_type!=\"EUTRA\", status=\"success\", procedure_type=\"pdn_sess_create\",
pra=\"enable\"}[5m])) / sum by (namespace) (increase(smf_service_stats{app_name=\"smf\",
dcnr =\"enable\", rat_type!=\"EUTRA\", status=\"attempted\",
procedure_type=\"pdn_sess_create\", pra=\"enable\"}[5m])) < 0.10"
  severity major
  type "Communications Alarm"

```

```

    annotation summary
      value "This alert is fired when attach success rate of DCNR enabled UE and presence
reporting enabled lesser than threshold "
    exit
  exit

```

## show alerts

This section provides the sample output for different variants of the **show alerts** CLI command.

### show alerts | include radius

```

alerts history radius_test cfb253587397
alerts history radius_test 911f84aff47c
alerts history radius_test 3ed7a5112905
alerts history radius_test 292af807b299
  source      radius-ep-n0-0
  labels      [ "namespace: smf" "pod: radius-ep-n0-0" ]
  annotations [ "summary: Container:  of pod: radius-ep-n0-0 in namespace: smf has been
restarted." ]
  source      radius-ep-n0-0
  labels      [ "name: k8s_radius-radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0"
"namespace: smf" "pod: radius-ep-n0-0" ]
  annotations [ "summary: Container:
k8s_radius-ep_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
in namespace: smf has been restarted." ]
  source      radius-ep-n0-0
  labels      [ "name: k8s_POD_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0"
"namespace: smf" "pod: radius-ep-n0-0" ]
  annotations [ "summary: Container:
k8s_POD_radius-ep-n0-0_smf_7f9e968a-39dc-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
in namespace: smf has been restarted." ]
alerts history radius_test 1c17e31c13f9
alerts history radius_test ffaabf0929
  source      radius-ep-n0-0
  labels      [ "name: k8s_POD_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0"
"namespace: smf" "pod: radius-ep-n0-0" ]
  annotations [ "summary: Container:
k8s_POD_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
in namespace: smf has been restarted." ]
  source      radius-ep-n0-0
  labels      [ "namespace: smf" "pod: radius-ep-n0-0" ]
  annotations [ "summary: Container:  of pod: radius-ep-n0-0 in namespace: smf has been
restarted." ]
  source      radius-ep-n0-0
  labels      [ "name: k8s_radius-ep_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0"
"namespace: smf" "pod: radius-ep-n0-0" ]
  annotations [ "summary: Container:
k8s_radius-ep_radius-ep-n0-0_smf_cd16807a-2f0b-11eb-ba84-0050569cb367_0 of pod: radius-ep-n0-0
in namespace: smf has been restarted." ]
[unknown] cee#

```

### show alerts active detail | include Radius

```

alerts active detail Radius_Server_Down 0fe030aba3ce
  summary "Radius Server: 198.18.1.20, Port: 1813 in namespace: smf is DOWN for more than
15min."
alerts active detail Radius_Server_Down 6f41c340311c
  summary "Radius Server: 10.84.115.45, Port: 1813 in namespace: smf is DOWN for more than
15min."
alerts active detail Radius_Server_Down 8a290c5ed1de
  summary "Radius Server: 198.18.1.20, Port: 1812 in namespace: smf is DOWN for more than
15min."

```

```
[unknown] cee#
[unknown] cee#
alerts active detail Radius_Server_Down 0fe030aba3ce
severity major
type "Processing Error Alarm"
startsAt 2020-12-11T13:30:16.874Z
source System
summary "Radius Server: 198.18.1.20, Port: 1813 in namespace: smf is DOWN for more than
15min."
labels [ "namespace: smf" "radSvrIP: 198.18.1.20" "radSvrPort: 1813" ]
alerts active detail Radius_Server_Down 6f41c340311c
severity major
type "Processing Error Alarm"
startsAt 2020-12-11T13:30:16.874Z
source System
summary "Radius Server: 10.84.115.45, Port: 1813 in namespace: smf is DOWN for more than
15min."
labels [ "namespace: smf" "radSvrIP: 10.84.115.45" "radSvrPort: 1813" ]
alerts active detail Radius_Server_Down 8a290c5ed1de
severity major
type "Processing Error Alarm"
startsAt 2020-12-11T13:30:16.874Z
source System
summary "Radius Server: 198.18.1.20, Port: 1812 in namespace: smf is DOWN for more than
15min."
labels [ "namespace: smf" "radSvrIP: 198.18.1.20" "radSvrPort: 1812" ]

[unknown] cee# show alerts active summary | include RTT
Radius_Server_RTT 1d0353b3db82 major 12-11T15:10:16 System RTT
for Radius Server: 198.18.1.20, Port: 1812 in namespace: smf is more than 5 ms.

[unknown] cee#
```

**show alerts active summary | include RTT**

```
Radius_Server_RTT 1d0353b3db82 major 12-11T15:10:16 System RTT
for Radius Server: 198.18.1.20, Port: 1812 in namespace: smf is more than 5 ms.
```

[unknown] cee#

**show alerts active summary | include Radius**

```
Radius_Server_RTT 1d0353b3db82 major 12-11T15:10:16 System RTT
for Radius Server: 198.18.1.20, Port: 1812 in namespace: smf is more than 5 ms.

Radius_Acct_Establish 520d9943d53f major 12-11T15:05:16 System This
alert is fired when the percentage of successful Radius Accounting Establish responses
received is lesser than threshold
Radius_Server_Down 0fe030aba3ce major 12-11T13:30:16 System Radius
Server: 198.18.1.20, Port: 1813 in namespace: smf is DOWN for more than 15min.

Radius_Server_Down 6f41c340311c major 12-11T13:30:16 System Radius
Server: 10.84.115.45, Port: 1813 in namespace: smf is DOWN for more than 15min.

Radius_Server_Down 8a290c5ed1de major 12-11T13:30:16 System Radius
Server: 198.18.1.20, Port: 1812 in namespace: smf is DOWN for more than 15min.
```

**DCNR UE Bulk Statistics**

Use the following SMF service bulk statistics to monitor the failures or issues associated with DCNR UEs.

Table 273: DCNR UE

Bulk Statistics Name	Query	Description
4G_DCNRUE_Attempted	bulk-stats query 4G_DCNRUE_Attempted expression "sum(smf_service_stats {dcnr='enable',status='attempted', rat_type='EUTRA'}) by (namespace)" exit	
4G_DCNRUE_Success	bulk-stats query 4G_DCNRUE_Success expression "sum(smf_service_stats {dcnr='enable',status='success', rat_type='EUTRA'}) by (namespace)" exit	
4G_PRA_ENABLE_Attempted	bulk-stats query 4G_PRA_ENABLE_Attempted expression "sum(smf_service_stats {pra='enable',status='attempted', rat_type='EUTRA', procedure_type!='create_session_request'}) by (namespace)" exit	
4G_PRA_ENABLE_Success	bulk-stats query 4G_PRA_ENABLE_Success expression "sum(smf_service_stats {pra='enable',status='success', rat_type='EUTRA', procedure_type!='create_session_request'}) by (namespace)" exit	

**RADIUS Bulk Statistics**

Use the following bulk statistics to monitor the failures or issues associated with RADIUS authentication, RADIUS accounting, and Disconnect Message requests.

Table 274: RADIUS Accounting Message (Per endpoint)

Bulk Statistics Name	Query	Description
Radius_EP_Acct_Establish_Attempt	bulk-stats query Radius_EP_Acct_Establish_Attempt expression "sum(Radius_Requests_Statistics {radMsgCode='RadiusAcctReq', procType=~'PDN Connect PDU Session Establishment', radPacketType='Tx'}) by (namespace,dnn)"  label dnn  exit	Total number of Accounting Requests attempted by MVNO subscribers during session establishment.
Radius_EP_Acct_Establish_Success	bulk-stats query Radius_EP_Acct_Establish_Success expression "sum(Radius_Requests_Statistics {radMsgCode='RadiusAcctReq', procType=~'PDN Connect PDU Session Establishment', radPacketType='Rx', radResult='Success',dnn!=""}) by (namespace,dnn)"  label dnn  exit	Total number of successful Accounting Requests from MVNO subscribers during session establishment.
Radius_EP_Acct_Establish_Failure	bulk-stats query Radius_EP_Acct_Establish_Failure expression "sum(Radius_Requests_Statistics {radMsgCode='RadiusAcctReq', procType=~'PDN Connect PDU Session Establishment', radPacketType='Rx', radResult!='Success'}) by (namespace,dnn)"  label dnn  exit	Total number of failed Accounting Requests from MVNO subscribers during session establishment.

Bulk Statistics Name	Query	Description
Radius_EP_Acct_Release_Attempt	<pre>bulk-stats query Radius_EP_Acct_Release_Attempt expression "sum (Radius_Requests_Statistics {radMsgCode='RadiusAcctReq', procType=~'PDU Session Release.* PDN Disconnect', radPacketType='Tx'}) by (namespace,dnn)"  label dnn  exit</pre>	Total number of Accounting Requests attempted by MVNO subscribers during session release.
Radius_EP_Acct_Release_Success	<pre>bulk-stats query Radius_EP_Acct_Release_Success expression "sum(Radius_Requests_Statistics {radMsgCode='RadiusAcctReq', procType=~'PDU Session Release.* PDN Disconnect', radPacketType='Rx', radResult='Success'}) by (namespace,dnn)"  label dnn  exit</pre>	Total number of successful Accounting Requests from MVNO subscribers during session release.
Radius_EP_Acct_Release_Failure	<pre>bulk-stats query Radius_EP_Acct_Release_Failure expression "sum(Radius_Requests_Statistics {radMsgCode='RadiusAcctReq', procType=~'PDU Session Release.* PDN Disconnect', radPacketType='Rx', radResult!='Success'}) by (namespace,dnn)"  label dnn  exit</pre>	Total number of failed Accounting Requests from MVNO subscribers during session release.

Bulk Statistics Name	Query	Description
Radius_EP_Acct_Release_Type_Attempt	<pre>bulk-stats query Radius_EP_Acct_Release_Type_Attempt expression "sum(Radius_Requests_Statistics {radMsgCode='RadiusAcctReq', procType=~'PDU Session Release.* PDN Disconnect', radPacketType='Tx'}) by (namespace, procType)"  label procType  exit</pre>	Total number of Accounting Requests attempted by MVNO subscribers for a particular release type.
Radius_EP_Acct_Release_Type_Success	<pre>bulk-stats query Radius_EP_Acct_Release_Type_Success expression "sum(Radius_Requests_Statistics {radMsgCode='RadiusAcctReq', procType=~'PDU Session Release.* PDN Disconnect', radPacketType='Rx', radResult!='Success'}) by (namespace, procType)"  label procType  exit</pre>	Total number of successful Accounting Requests from MVNO subscribers for a particular release type.
Radius_EP_Acct_Release_Type_Failure	<pre>bulk-stats query Radius_EP_Acct_Release_Type_Failure expression "sum(Radius_Requests_Statistics {radMsgCode='RadiusAcctReq', procType=~'PDU Session Release.* PDN Disconnect', radPacketType='Rx', radResult!='Success'}) by (namespace, procType)"  label procType  exit</pre>	Total number of failed Accounting Requests from MVNO subscribers for a particular release type.



Bulk Statistics Name	Query	Description
Radius_EP_Acct_Establish_Retry_Attempt	<pre>bulk-stats query Radius_EP_Acct_Establish _Retry_Attempt expression "sum(Radius_Requests_Statistics {radMsgCode='RadiusAcctReq', procType=~'PDN Connect PDU Session Establishment', radPacketType='Retry_Tx'}) by (namespace,dnn)"  label dnn  exit</pre>	Total number of Accounting Retry Requests attempted by MVNO subscribers during session establishment.
Radius_EP_Acct_Release_Retry_Attempt	<pre>bulk-stats query Radius_EP_Acct_Release _Retry_Attempt expression "sum(Radius_Requests_Statistics {radMsgCode='RadiusAcctReq', procType=~'PDU Session Release.* PDN Disconnect', radPacketType='Retry_Tx'}) by (namespace,dnn)"  label dnn  exit</pre>	Total number of Accounting Retry Requests attempted by MVNO subscribers during session release.

Table 275: RADIUS Accounting Message (Per SMF service)

Bulk Statistics Name	Query	Description
Radius_Acct_Initial_Attempt_Svc	<pre>bulk-stats query Radius_Acct_Initial_Attempt_Svc expression "sum (radius_accounting_message_stats {procedure_type='radius_initial', status='attempted'}) by (namespace)"  exit</pre>	Total number of subscribers with RADIUS Accounting Initial/Start Attempt from service endpoint.
Radius_Acct_Initial_Success_Svc	<pre>bulk-stats query Radius_Acct_Initial_Success_Svc expression "sum (radius_accounting_message_stats {procedure_type='radius_initial', status='success'}) by (namespace)"  exit</pre>	Total number of subscribers with RADIUS Accounting Initial/Start Success from service endpoint.

Bulk Statistics Name	Query	Description
Radius_Acct_Initial_Failure_Svc	bulk-stats query Radius_Acct_Initial_Failure_Svc expression "sum (radius_accounting_message_stats {procedure_type='radius_initial', status!~'success attempted'}) by (namespace)"  exit	Total number of subscribers with RADIUS Accounting Initial/Start Failure from service endpoint.
Radius_Acct_Terminate_Attempt_Svc	bulk-stats query Radius_Acct_Terminate_Attempt_Svc expression "sum (radius_accounting_message_stats {procedure_type='radius_terminate', status='attempted'}) by (namespace)"  exit	Total number of subscribers with RADIUS Accounting Terminate/Stop Attempt from service endpoint.
Radius_Acct_Terminate_Success_Svc	bulk-stats query Radius_Acct_Terminate_Success_Svc expression "sum (radius_accounting_message_stats {procedure_type='radius_terminate', status='success'}) by (namespace)"  exit	Total number of subscribers with RADIUS Accounting Terminate/Stop Success from service endpoint.
Radius_Acct_Terminate_Failure_Svc	bulk-stats query Radius_Acct_Terminate_Failure_Svc expression "sum (radius_accounting_message_stats {procedure_type='radius_terminate', status!~'success attempted'}) by (namespace)"  exit	Total number of subscribers with RADIUS Accounting Terminate/Stop Failure from service endpoint.
Radius_Acct_Update_Attempt_Svc	bulk-stats query Radius_Acct_Update_Attempt_Svc expression "sum (radius_accounting_message_stats {procedure_type='radius_update', status='attempted'}) by (namespace)"  exit	Total number of subscribers with RADIUS Accounting Update/Interim Attempt from service endpoint.

Bulk Statistics Name	Query	Description
Radius_Acct_Update_Success_Svc	bulk-stats query Radius_Acct_Update_Success_Svc expression "sum (radius_accounting_message_stats {procedure_type='radius_update', status='success'}) by (namespace)" exit	Total number of subscribers with RADIUS Accounting Update/Interim Success from service endpoint.
Radius_Acct_Update_Failure_Svc	bulk-stats query Radius_Acct_Update_Failure_Svc expression "sum (radius_accounting_message_stats {procedure_type='radius_update', status!~'success attempted'}) by (namespace)" exit	Total number of subscribers with RADIUS Accounting Update/Interim Failure from service endpoint.

Table 276: Disconnect Message

Bulk Statistics Name	Query	Description
Radius_EP_DM_Attempt	bulk-stats query Radius_EP_DM_Attempt expression "sum (Radius_CoaDM_Requests_Statistics {radMsgCode='DisconnectRequest', radPacketType='Rx'}) by (namespace,radSvrIP)" label radSvrIP exit	Total number of RADIUS Disconnect Message Attempts
Radius_EP_DM_Success	bulk-stats query Radius_EP_DM_Attempt expression "sum (Radius_CoaDM_Requests_Statistics {radMsgCode='DisconnectRequest', radPacketType='Rx'}) by (namespace,radSvrIP)" label radSvrIP exit	Total number of successful RADIUS Disconnect Messages

Bulk Statistics Name	Query	Description
Radius_EP_DM_Failure	<pre>bulk-stats query Radius_EP_DM_Failure expression "sum (Radius_CoaDM_Requests_Statistics {radMsgCode='DisconnectNAK', radPacketType='Tx', radResult='Success'}) by (namespace,radSvrIP)"  label radSvrIP  exit</pre>	Total number of failed RADIUS Disconnect Messages

Table 277: RADIUS Access Request (Secondary Authentication)

Bulk Statistics Name	Query	Description
Radius_EP_AccessReq_Attempt	<pre>bulk-stats query Radius_EP_AccessReq_Attempt expression "sum(Radius_Requests_Statistics {radMsgCode='SecondaryAuthenReq', procType!=", radPacketType='Tx', radResult='Success'}) by (namespace,dnn)"  label dnn  exit</pre>	Total number of MVNO subscribers with Access Request (secondary authentication) Attempts
Radius_EP_AccessReq_Success	<pre>bulk-stats query Radius_EP_AccessReq_Success expression "sum(Radius_Requests_Statistics {radMsgCode='SecondaryAuthenReq', procType!=", radPacketType='Rx', radResult='Success'}) by (namespace,dnn)"  label dnn  exit</pre>	Total number of MVNO subscribers with successful Access Requests (secondary authentication)

Bulk Statistics Name	Query	Description
Radius_EP_AccessReq_Failure	<pre>bulk-stats query Radius_EP_AccessReq_Failure expression "sum(Radius_Requests_Statistics {radMsgCode='SecondaryAuthenReq', radPacketType='Rx', radResult!='Success'}) by (namespace,dnn)"  label dnn  exit</pre>	Total number of MVNO subscribers with failed Access Requests (secondary authentication)

### Roamer UE Bulk Statistics

Use the following SMF service bulk statistics to monitor the failures or issues associated with Roamer UEs.

**Table 278: Roamer UE**

Bulk Statistics Name	Query	Description
4G_In-Roamers_Attempted	<pre>bulk-stats query 4G_In-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='attempted',rat_type='EUTRA'}) by (namespace)" exit</pre>	
4G_In-Roamers_Success	<pre>bulk-stats query 4G_In-Roamers_Success expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='success',rat_type='EUTRA'}) by (namespace)" exit</pre>	
4G_Out-Roamers_Attempted	<pre>bulk-stats query 4G_Out-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='roamer', status='attempted',rat_type='EUTRA'}) by (namespace)" exit</pre>	
4G_Out-Roamers_Success	<pre>bulk-stats query 4G_Out-Roamers_Success expression "sum(smf_service_stats {roaming_status='roamer', status='success',rat_type='EUTRA'}) by (namespace)" exit</pre>	

Bulk Statistics Name	Query	Description
5G_In-Roamers_Attempted	bulk-stats query 5G_In-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='attempted',rat_type='NR'}) by (namespace)" exit	
5G_In-Roamers_Success	bulk-stats query 5G_In-Roamers_Success expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='success',rat_type='NR'}) by (namespace)" exit	
5G_Out-Roamers_Attempted	bulk-stats query 5G_Out-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='roamer', status='attempted',rat_type='NR'}) by (namespace)" exit	
5G_Out-Roamers_Success	bulk-stats query 5G_Out-Roamers_Success expression "sum(smf_service_stats {roaming_status='roamer', status='success',rat_type='NR'}) by (namespace)" exit	
WiFi_In-Roamers_Attempted	bulk-stats query WiFi_In-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='attempted',rat_type='WLAN'}) by (namespace)" exit	
WiFi_In-Roamers_Success	bulk-stats query WiFi_In-Roamers_Success expression "sum(smf_service_stats {roaming_status='visitor-lbo', status='success',rat_type='WLAN'}) by (namespace)" exit	
WiFi_Out-Roamers_Attempted	bulk-stats query WiFi_Out-Roamers_Attempted expression "sum(smf_service_stats {roaming_status='roamer', status='attempted',rat_type='WLAN'}) by (namespace)" exit	

Bulk Statistics Name	Query	Description
WiFi_Out-Roamers_Success	bulk-stats query WiFi_Out-Roamers_Success expression "sum(smf_service_stats {roaming_status='roamer', status='success',rat_type='WLAN'}) by (namespace)" exit	

### Show Bulk Statistics

Use the **show bulk-stats** command to view the list of all configured bulk statistics.

### RADIUS Bulk Statistics

The following is a sample output of the bulk stats related to the RADIUS feature.

```
[unknown] cee# show bulk-stats | include Radius
smf      Radius_EP_Acct_Establish_Attempt      System  19.0
smf      Radius_EP_Acct_Establish_Failure      System   9.0
smf      Radius_EP_Acct_Establish_Retry_Attempt System  11.0
smf      Radius_EP_Acct_Establish_Success      System  10.0
smf      Radius_EP_Acct_Release_Attempt      System  19.0
smf      Radius_EP_Acct_Release_Failure      System  18.0
smf      Radius_EP_Acct_Release_Retry_Attempt System  37.0
smf      Radius_EP_Acct_Release_Success      System   1.0
smf      Radius_EP_Acct_Release_Type_Attempt System  19.0
smf      Radius_EP_Acct_Release_Type_Failure System  18.0
smf      Radius_EP_Acct_Release_Type_Success System   1.0
smf      Radius_EP_DM_Attempt              System  14.0
smf      Radius_EP_DM_Failure              System   9.0
smf      Radius_EP_DM_Success              System   5.0
smf      Radius_EP_SecondaryAuth_Attempt   System  16.0
smf      Radius_EP_SecondaryAuth_Success   System  16.0

[unknown] cee# show bulk-stats current | include Radius | exclude smf-data | exclude smf-ims

smf      Radius_Acct_Initial_Attempt_Svc      System   3.0
smf      Radius_Acct_Initial_Success_Svc     System   3.0
smf      Radius_Acct_Terminate_Attempt_Svc   System   3.0
smf      Radius_Acct_Terminate_Success_Svc   System   3.0
smf      Radius_EP_Acct_Establish_Attempt   System   3.0
smf      Radius_EP_Acct_Establish_Failure   System   1.0
smf      Radius_EP_Acct_Establish_Retry_Attempt System   3.0
smf      Radius_EP_Acct_Establish_Success   System   2.0
smf      Radius_EP_Acct_Release_Attempt     System   3.0
smf      Radius_EP_Acct_Release_Failure     System   2.0
smf      Radius_EP_Acct_Release_Retry_Attempt System   6.0
smf      Radius_EP_Acct_Release_Success     System   1.0
smf      Radius_EP_Acct_Release_Type_Attempt PDU Session Release - AMF initiated
1.0
smf      Radius_EP_Acct_Release_Type_Attempt PDU Session Release - RADIUS initiated
1.0
smf      Radius_EP_Acct_Release_Type_Attempt PDU Session Release - Admin initiated
1.0
smf      Radius_EP_Acct_Release_Type_Failure PDU Session Release - AMF initiated
1.0
smf      Radius_EP_Acct_Release_Type_Failure PDU Session Release - Admin initiated
1.0
```

```

smf      Radius_EP_Acct_Release_Type_Success      PDU Session Release - AMF initiated
1.0
smf      Radius_EP_Acct_Release_Type_Success      PDU Session Release - Admin initiated
1.0
smf      Radius_EP_DM_Attempt                    System 2.0
smf      Radius_EP_DM_Failure                    System 1.0
smf      Radius_EP_DM_Success                    System 1.0
smf      Radius_EP_SecondaryAuth_Attempt         System 2.0
smf      Radius_EP_SecondaryAuth_Success         System 2.0
    
```

### Roaming Bulk Statistics

The following is a sample output for the config based bulkstats related to the Roaming feature.

```

[unknown] cee# show bulk-stats | include Roam | include cmsgw
cmsgw     4G_In-Roamers_Attempted      System 0.0
cmsgw     4G_In-Roamers_Success        System 0.0
cmsgw     4G_Out-Roamers_Attempted     System 0.0
cmsgw     5G_In-Roamers_Attempted     System 0.0
cmsgw     5G_In-Roamers_Success        System 0.0
cmsgw     5G_Out-Roamers_Attempted     System 0.0
cmsgw     5G_Out-Roamers_Success        System 0.0
cmsgw     WiFi_In-Roamers_Attempted    System 0.0
cmsgw     WiFi_In-Roamers_Success      System 0.0
cmsgw     WiFi_Out-Roamers_Attempted   System 3.0
cmsgw     WiFi_Out-Roamers_Success     System 4.0
[unknown] cee#
    
```

### Option-3x Bulk Statistics

The following is a sample output for the config based bulkstats related to the Option-3x feature.

```

[unknown] cee# show bulk-stats | include DCNR
smf      4G_DCNRUE_Attempted           System 147.0
smf      4G_DCNRUE_Success             System 130.0
[unknown] cee#
[unknown] cee# show bulk-stats | include PRA
smf      4G_PRA_ENABLE_Attempted       System 107.0
smf      4G_PRA_ENABLE_Success         System 107.0
[unknown] cee#
    
```

## Grafana Charts

The Grafana charts can be used for monitoring based on the RADIUS endpoint or Service endpoint.

- RADIUS endpoint for call flows involving RADIUS Authentication, Accounting, and Disconnect Message.
- Service endpoint for accounting flows specific to Accounting Initial/Interim/Terminate packets.

## Error Logs

This section explains the basic error conditions and the related logs to debug the failures.

### Option-3x Feature

This section provides the basic error conditions and logs that are captured to debug the failures for the roaming feature.



### DCNR Disabled UE or 4G capable UE only

The following example displays the error log for DCNR disabled UE or 4G capable UE only.

```
2021/01/24 10:11:22.648 smf-service [ERROR] [GenericGtpMsg.go:1811] [smf-service.smf-app.sgw]
secRatUsageRpt recvd wrongly for DNCR disbled UE, ignoring report

2020/12/19 13:17:17.834 smf-service [ERROR] [GenericGtpMsg.go:1834] [smf-service.smf-app.sgw]
secRatUsageRpt recvd wrongly for 4gOnly UE, ignoring report
```

### Secondary RAT Usage with invalid EBI

The following example displays the error log for secondary RAT usage with invalid EBI.

```
2021/01/24 11:38:18.917 smf-service [DEBUG] [GenericGtpMsg.go:1824] [smf-service.smf-app.sgw]
Secondary Rat Data Usage Report Recvd
2021/01/24 11:38:18.917 smf-service [WARN] [IntMethods.go:137] [smf-service.Policy.gen] Qos
Flow not found with EBI [8]
2021/01/24 11:38:18.917 smf-service [ERROR] [GenericGtpMsg.go:1853] [smf-service.smf-app.sgw]
Qfi invalid in secRatUsageRpt
```

### Secondary RAT Usage invalid RAT Type

The following example displays the error log for secondary RAT usage with invalid RAT type.

```
2021/01/24 11:42:21.474 smf-service [DEBUG] [GenericGtpMsg.go:1824] [smf-service.smf-app.sgw]
Secondary Rat Data Usage Report Recvd
2021/01/24 11:42:21.474 smf-service [ERROR] [GenericGtpMsg.go:1861] [smf-service.smf-app.sgw]
Rat type invalid in secRatUsageRpt
```

### Secondary RAT Usage with intended PGW set to zero

The following example displays the error log for secondary RAT usage with intended P-GW set to zero (IRPGW:0).

```
2021/01/24 11:33:10.390 smf-service [DEBUG] [GenericGtpMsg.go:1824] [smf-service.smf-app.sgw]
Secondary Rat Data Usage Report Recvd
2021/01/24 11:33:10.390 smf-service [ERROR] [GenericGtpMsg.go:1865] [smf-service.smf-app.sgw]
secRatUsageRpt.IRPGW is false
```

### PRA ID received greater than four

The following example displays the error log when PRA ID received is greater than four.

```
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_types.go:659] [smf-service.Policy.gen]
praConfig:true for dnn:fast.t-mobile.com
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_pcf.go:1939] [smf-service.Policy.gen]
Added PRA ID: 9388618
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_pcf.go:1939] [smf-service.Policy.gen]
Added PRA ID: 9388608
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_pcf.go:1939] [smf-service.Policy.gen]
Added PRA ID: 8388618
2021/01/24 14:48:26.085 smf-service [DEBUG] [policy_pcf.go:1939] [smf-service.Policy.gen]
Added PRA ID: 9388619
2021/01/24 14:48:26.085 smf-service [WARN] [policy_pcf.go:1934] [smf-service.Policy.gen]
Max 4 PRAs allowed, ignoring the PRA-ID (8388608) from PCF
2021/01/24 14:48:26.085 smf-service [WARN] [policy_pcf.go:1934] [smf-service.Policy.gen]
Max 4 PRAs allowed, ignoring the PRA-ID (8388619) from PCF
```

## RADIUS Authentication

### Authentication Request Not Responded by Server

The following is an error log for RADIUS Authentication Request not responded by the RADIUS server.

```
[smf-service-n0-0] 2020/09/17 07:14:52.921 smf-service [ERROR] [GenericAAA.go:786]
[smf-service0.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [16] Secondary
Authentication Failed: TIMEOUT
[smf-service-n0-0] *errors.errorString Secondary Authentication Failed: TIMEOUT
[smf-service-n0-0] /opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:621 (0xd89cae)
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/procedures/generic/GenericAAA.go:786 (0x144fa52)
```

### Call Failure at Authentication Stage

The following is a sample error log for call failure at the RADIUS authentication stage.

```
[smf-service-n0-0]
[smf-service-n0-0] 2020/09/17 07:14:52.921 smf-service [ERROR] [idlestate.go:504]
[smf-service0.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [16]
USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED
[smf-service-n0-0] *errors.errorString USER_AUTHENTICATION_OR_AUTHORIZATION_FAILED
[smf-service-n0-0] /opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:621 (0xd89cae)
[smf-service-n0-0] /opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:580 (0x15d7ddc)
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/procedures/4g/pdnsetup/idlestate.go:537 (0x15bc4f5)
```

### Authentication Request Rejected by RADIUS Server

The following is an error log for RADIUS Authentication Request rejected by RADIUS server.

```
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [INFO] [idlestate.go:649]
[smf-service.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [1] Processing
Secondary Authentication Response
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [ERROR] [GenericAAA.go:1173]
[smf-service.smf-app.aaa] [imsi-123456789012345:5] [imsi-123456789012345:5] [1] Secondary
Authentication Failed: REJECT
[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [DEBUG] [Genericutil.go:681]
[smf-service.smf-app.gen] Internal Transaction Submit with BP for MessageType: 118, SLA: 0

[smf-service-n0-0] 2020/12/09 09:20:14.047 smf-service [DEBUG] [idlestate.go:169]
[smf-service.smf-app.gen] inCallStatus:9
```

```
*****
Transaction Log received from Instance: smf.radius-ep.ajay-smf1.smf.0
***** TRANSACTION: 00004 *****
TRANSACTION SUCCESS:
Txn Type           : SecondaryAuthenReq(2004)
Priority           : 1
Session State      : No_Session
LOG MESSAGES:
2020/12/09 09:20:13.756 [TRACE] [infra.message_log.core] >>>>>>>

2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Starting smf AccessRequest
2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Starting smf AccessRequest for User
[msisdn-9884886688]
2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Created new Radius Message for smf
AccessRequest
```

```

2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Selected server: 198.18.1.20:1812 ,
nasIP: 198.18.1.4 PID: 4194304
2020/12/09 09:20:13.757 [DEBUG] [Radius.smf.AAA] Sending an IPC Message to UDP proxy
[198.18.1.4]
2020/12/09 09:20:13.763 [DEBUG] [Radius.smf.AAA] PID: 4194304 - Response received on
channel
2020/12/09 09:20:13.763 [DEBUG] [Radius.smf.AAA] Authentication Result for user
[8899776655] = [REJECT]
2020/12/09 09:20:13.764 [TRACE] [infra.message_log.core] <<<<<<<<

*****

```

### Authentication Response with Incorrect Authenticator

The following is an error log for RADIUS Authentication Response with incorrect authenticator.

```

[radius-ep-n0-0] ***** TRANSACTION: 00044 *****
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0] Txn Type           : RadiusUdpProxyMsg(2002)
[radius-ep-n0-0] Priority            : 1
[radius-ep-n0-0] Session State       : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0] 2020/12/09 13:20:38.874 [TRACE] [infra.message_log.core] >>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0] 2020/12/09 13:20:38.874 [DEBUG] [Radius.smf.AAA] Response received
from udp proxy
[radius-ep-n0-0] 2020/12/09 13:20:38.874 [DEBUG] [Radius.smf.AAA] SrcIp: 198.18.1.20
SrcPort: 1812 DestIp: 198.18.1.4 DestPort: 16384
[radius-ep-n0-0] 2020/12/09 13:20:38.874 [ERROR] [Radius.smf.AAA] PID: 4194310 - Packet
dropped due to invalid authenticator
[radius-ep-n0-0] 2020/12/09 13:20:38.874 [TRACE] [infra.message_log.core] <<<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] *****

```

## RADIUS Accounting

### Accounting Request Timeout

The following is an error log for RADIUS Accounting Request timeout.

```

[radius-ep-n0-0] ***** TRANSACTION: 00027 *****
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0] Txn Type           : IntSmfAcctReqMsg(3)
[radius-ep-n0-0] Priority            : 1
[radius-ep-n0-0] Session State       : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0] 2020/12/09 13:09:10.247 [TRACE] [infra.message_log.core] >>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0] 2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Starting smf
AccountingRequest
[radius-ep-n0-0] 2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Starting smf
AccountingRequest for User [msisdn-9884886688]
[radius-ep-n0-0] 2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Created new Radius
Message for smf AccountingRequest
[radius-ep-n0-0] 2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Selected server:
198.18.1.20:1813 , nasIP: 198.18.1.4 PID: 4194304
[radius-ep-n0-0] 2020/12/09 13:09:10.247 [DEBUG] [Radius.smf.AAA] Sending an IPC Message
to UDP proxy [198.18.1.4]
[radius-ep-n0-0] 2020/12/09 13:09:15.091 [DEBUG] [Radius.smf.AAA] PID: 4194304 - Response
received on channel
[radius-ep-n0-0] 2020/12/09 13:09:15.091 [ERROR] [Radius.smf.AAA] Retried MaxNumber of
times without success
[radius-ep-n0-0] 2020/12/09 13:09:15.092 [DEBUG] [Radius.smf.AAA] Int-txn Accounting
Result for user [9884886688] = [TIMEOUT]

```

```
[radius-ep-n0-0]      2020/12/09 13:09:15.092 [TRACE] [infra.message_log.core] <<<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] *****
```

## Roaming Feature

This section provides the basic error conditions and logs that are captured to debug the failures for the roaming feature.

### PLMN Validation Failure

The following example displays the error log for PLMN validation failure resulting into setting the roaming status as "none".

```
2021/01/06 15:25:18.630 smf-service [DEBUG] [genericinfo.go:1597]
[smf-service.smf-app.subscriber] Set roaming status to 0
2021/01/06 15:25:18.630 smf-service [DEBUG] [genericinfo.go:2317]
[smf-service.smf-app.subscriber] Subscriber is %!s(uint32=0)
2021/01/06 15:25:18.630 smf-service [ERROR] [genericinfo.go:1082]
[smf-service.smf-app.subscriber] PLMN validation failed
2021/01/06 15:25:18.630 smf-service [DEBUG] [subscriber_policy_config.go:187]
[misc-lib.config.subscriber-policy] LookupParameters - {imsi-123456789012345
msisdn-22331010101010101 imei-123456786666660 0 123 456 intershat}
```

### Homer UE Status (Homer)

The following is an example of the generic logs for UE Roaming Status.

```
2021/01/06 15:04:39.146 smf-service [DEBUG] [genericinfo.go:1597]
[smf-service.smf-app.subscriber] Set roaming status to 1
2021/01/06 15:04:39.146 smf-service [DEBUG] [genericinfo.go:2317]
[smf-service.smf-app.subscriber] Subscriber is %!s(uint32=1)
2021/01/06 15:04:39.146 smf-service [DEBUG] [subscriber_policy_config.go:187]
[misc-lib.config.subscriber-policy] LookupParameters - {imsi-123456789012345 msisdn-9999988888
imei-352099001761480 Abf123 2 310 310 intershat}
```

### Out-roamer UE Status (Roamer)

The following is an example of the generic logs for out-roamer UE status.

```
2021/01/06 16:11:02.710 smf-service [DEBUG] [genericinfo.go:1597]
[smf-service.smf-app.subscriber] Set roaming status to 4
2021/01/06 16:11:02.710 smf-service [DEBUG] [genericinfo.go:2317]
[smf-service.smf-app.subscriber] Subscriber is %!s(uint32=4)
2021/01/06 16:11:02.710 smf-service [DEBUG] [subscriber_policy_config.go:187]
[misc-lib.config.subscriber-policy] LookupParameters - {imsi-123456789012345
```

### In-roamer UE Status (Visitor LBO)

The following is an example of the generic logs for in-roamer UE status.

```
2021/01/06 15:54:32.323 smf-service [DEBUG] [genericinfo.go:1597]
[smf-service.smf-app.subscriber] Set roaming status to 2
2021/01/06 15:54:32.323 smf-service [DEBUG] [genericinfo.go:2317]
[smf-service.smf-app.subscriber] Subscriber is %!s(uint32=2)
2021/01/06 15:54:32.323 smf-service [DEBUG] [subscriber_policy_config.go:187]
[misc-lib.config.subscriber-policy] LookupParameters - {imsi-123456789012345
msisdn-22331010101010101 imei-123456786666660 0 310 310 intershat}
```

## Generic MVNO Call Flow Error Logs

### *Incorrect Static IP to Pool Mapping*

The following is a sample error log for incorrect static IP to pool mapping or if static IP received from RADIUS is not found with any UPF.

```
[smf-service-n0-0] 2020/09/23 07:42:25.969 smf-service [DEBUG] [rmgrutil.go:501]
[smf-service.smf-app.resource] [imsi-123456789012345:5] [imsi-123456789012345:5] [16]
response received for message NmgrRersourceMgmtResponse
[smf-service-n0-0] 2020/09/23 07:42:25.969 smf-service [INFO] [upmgrCacheApi.go:450]
[misc-lib.upmgrcache.gen] Cache doesnot have entry for UpfEpKey:
[smf-service-n0-0] 2020/09/23 07:42:25.969 smf-service [ERROR] [rmgrutil.go:73]
[smf-service.smf-app.resource] [imsi-123456789012345:5] [imsi-123456789012345:5] [16] Both
the associated nodemgr instances for upfEpKey: is down
[smf-service-n0-0] *errors.errorString Both the associated nodemgr instances for upfEpKey:
is down
[smf-service-n0-0] /opt/workspace/smf-service/src/smf-service/vendor/wwwin-github.cisco.com/
mobile-cnat-golang-lib/app-infra.git/src/app-infra/infra/Transaction.go:621 (0xd8b29e)
[smf-service-n0-0]
/opt/workspace/smf-service/src/smf-service/procedures/generic/rmgrutil.go:73 (0x14dbd61)
```

### *Idle Timeout-based Release*

#### Idle Timeout Received from RADIUS

The following is a sample error log for idle timeout received from RADIUS.

```
[smf-service-n0-0] 2020/09/23 16:10:11.965 smf-service [DEBUG]
[Genericutil.go:7158] [smf-service.smf-app.gen] Idle timeout value received from Radius:
10
[smf-service-n0-0] 2020/09/23 16:10:11.965 smf-service [DEBUG]
[Genericutil.go:7168] [smf-service.smf-app.gen] Starting cp idle timer with timeout value:
10
```

#### Absolute Session Timeout Received from RADIUS

The following is a sample error log for absolute session timeout received from RADIUS.

```
[smf-service-n0-0] 2020/09/23 16:10:11.964 smf-service [DEBUG]
[Genericutil.go:7200] [smf-service.smf-app.gen] Session absolute timeout value
received from Radius: 200
```

#### Session Cleanup

The following is a sample error log for session cleanup.

```
[smf-service-n0-0] 2020/09/23 16:10:21.966 smf-service [WARN] [stateHandler.go:187]
[smf-service.smf-app.gen] [imsi-123456789012345:5] [imsi-123456789012345:5] [21]
TIMEOUT -- Cp Idle Session Timer Expired, Triggering release
```

## Disconnect Message

### *Disconnect Message Received from Unknown Client*

The following is a sample error log when disconnect message is received from an unknown client.

```
[radius-ep-n0-0]
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [INFO] [processor.go:157] [Radius.smf.Ipc]
Process continue - 2003
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [DEBUG] [coa.go:23] [Radius.smf.AAA] []
[] [11] Coa/Disconnect Req received from udp proxy
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [DEBUG] [coa.go:43] [Radius.smf.AAA] []
```

## Disconnect Message Received with Invalid Session ID Key

```

[] [11] SrcIp: 198.18.1.20 SrcPort: 3799 DestIp: 198.18.1.4 DestPort: 3799
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [ERROR] [coa.go:253] [Radius.smf.Ipc]
Bng Coa/Disconnect req failed - Invalid Coa Client 198.18.1.20
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [ERROR] [coa.go:48] [Radius.smf.AAA] []
[] [11] Unable to process Coa/Disconnect request - Error during init of Radius Message
Invalid Coa Client 198.18.1.20
[radius-ep-n0-0] 2020/11/25 10:30:02.960 radius-ep [DEBUG] [MasterBlueprint.go:345]
[infra.transaction.core] Last stage ( init_done ) -> Next stage ( finished )
[radius-ep-n0-0] ***** TRANSACTION: 00011 *****
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0] Txn Type : RadiusUdpProxyCoaMsg(2003)
[radius-ep-n0-0] Priority : 1
[radius-ep-n0-0] Session State : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [TRACE] [infra.message_log.core] >>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [DEBUG] [Radius.smf.AAA] Coa/Disconnect Req
received from udp proxy
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [DEBUG] [Radius.smf.AAA] SrcIp: 198.18.1.20
SrcPort: 3799 DestIp: 198.18.1.4 DestPort: 3799
[radius-ep-n0-0] 2020/11/25 10:30:02.960 [ERROR] [Radius.smf.AAA] Unable to process
Coa/Disconnect request - Error during init of Radius Message Invalid Coa Client 198.18.1.20

[radius-ep-n0-0] 2020/11/25 10:30:02.960 [TRACE] [infra.message_log.core] <<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] *****
[radius-ep-n0-0]

```

*Disconnect Message Received with Invalid Session ID Key*

The following is a sample error log when disconnect message is received with invalid session ID key.

```

[radius-ep-n0-0] ***** TRANSACTION: 00009 *****
[radius-ep-n0-0] TRANSACTION SUCCESS:
[radius-ep-n0-0] Txn Type : RadiusUdpProxyCoaMsg(2003)
[radius-ep-n0-0] Priority : 1
[radius-ep-n0-0] Session State : No_Session
[radius-ep-n0-0] LOG MESSAGES:
[radius-ep-n0-0] 2020/11/25 10:49:43.942 [TRACE] [infra.message_log.core] >>>>>>>
[radius-ep-n0-0]
[radius-ep-n0-0] 2020/11/25 10:49:43.942 [DEBUG] [Radius.smf.AAA] Coa/Disconnect Req
received from udp proxy
[radius-ep-n0-0] 2020/11/25 10:49:43.942 [DEBUG] [Radius.smf.AAA] SrcIp: 198.18.1.20
SrcPort: 3799 DestIp: 198.18.1.4 DestPort: 3799
[radius-ep-n0-0] 2020/11/25 10:49:43.942 [DEBUG] [Radius.smf.AAA] Decoded coa message
type is DisconnectRequest
[radius-ep-n0-0] 2020/11/25 10:49:43.942 [ERROR] [Radius.smf.AAA] Unable to process
DisconnectRequest - Error during construct Invalid DNN/IPv4Addr/IPv6Pfx value
[radius-ep-n0-0] 2020/11/25 10:49:43.942 [TRACE] [infra.message_log.core] <<<<<<<
[radius-ep-n0-0]
[radius-ep-n0-0] *****

```



## CHAPTER 58

# Sample SMF Configuration

- [Feature Summary and Revision History](#), on page 881
- [Sample Configuration](#), on page 881

## Feature Summary and Revision History

### Summary Data

*Table 279: Summary Data*

Applicable Product(s) or FunctionalArea	SMF
Applicable Platform(s)	SMI
Feature Default Setting	Not Applicable
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

### Revision History

*Table 280: Revision History*

Revision Details	Release
Updated the Sample SMF Configuration information for this release.	Pre-2020.02.0

## Sample Configuration

The following is only a sample configuration file provided solely for your reference. You must create and modify your own configuration file according to the specific needs of your deployment.

