SGSN Administration Guide, StarOS Release 21.17

First Published: 2019-12-19

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 NONINFRINGEMENT 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.

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: www.cisco.com go trademarks. 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)

© 2019 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

About this Guide xxxvii

Conventions Used xxxvii

Supported Documents and Resources xxxix

Related Common Documentation xxxix

Related Product Documentation xxxix

Obtaining Documentation xxxix

Contacting Customer Support xxxix

CHAPTER 1

1-in-N IMEI Check per SGSN Subscriber 1

Feature Summary and Revision History 1

Feature Description 2

Configuring IMEI Check to EIR for the First 1-N Events 2

Configuring IMEI Check Every N Events in MAP Service 2

Configuring IMEI Check Every N Events in EIR-Profile 2

CHAPTER 2

Serving GPRS Support Node (SGSN) Overview 5

Product Description 5

Qualified Platforms 6

Licenses 6

Network Deployments and Interfaces 6

SGSN and Dual Access SGSN Deployments 7

SGSN/GGSN Deployments 8

S4-SGSN Deployments 9

SGSN Logical Network Interfaces 10

SGSN Core Functionality 13

All-IP Network (AIPN) 13

SS7 Support 14
PDP Context Support 14
Mobility Management 15
GPRS Attach 15
GPRS Detach 15
Paging 16
Service Request 16
Authentication 16
P-TMSI Reallocation 16
P-TMSI Signature Reallocation 16
Identity Request 17
Location Management 17
Session Management 17
PDP Context Activation 17
PDP Context Modification 18
PDP Context Deactivation 18
PDP Context Preservation 18
Charging 18
SGSN in GPRS/UMTS Network 19
SGSN in LTE/SAE Network 20
Features and Functionality 20
3G-2G Location Change Reporting 20
Access Restriction Support on S6d Interface 20
Accounting Path Framework, New for 14.0 21
AAA Changes To Support Location Services (LCS) Feature 21
APN Aliasing 21
Default APN 22
APN Redirection per APN with Lowest Context-ID 22
APN Resolution with SCHAR or RNC-ID 22
APN Restriction 23
Automatic Protection Switching (APS) 23
Authentications and Reallocations -- Selective 24
Avoiding PDP Context Deactivations 24
Backup and Recovery of Key KPI Statistics 24

Bulk Statistics Support 25
Bypassing APN Remap for Specific IMEI Ranges 26
CAMEL Service Phase 3, Ge Interface 26
CAMEL Service 26
CAMEL Support 26
Ge Interface 27
CAMEL Configuration 27
Commandguard 27
Configurable RAB Asymmetry Indicator in RAB Assignment Request 28
Congestion Control 28
Different NRIs for Pooled and Non-pooled RNCs/BSCs 28
Direct Tunnel 29
Direct Tunnel Support on the S4-SGSN 29
Downlink Data Lockout Timer 29
DSCP Templates for Control and Data Packets - Iu or Gb over IP 30
Dual PDP Addresses for Gn/Gp 30
ECMP over ATM 30
EDR Enhancements 30
EIR Selection for Roaming Subscribers 31
Equivalent PLMN 32
Fallback on DNS Failure 32
First Vector Configurable Start for MS Authentication 32
Format Encoding of MNC and MCC in DNS Queries Enhanced 32
Gb Manager 33
GMM-SM Event Logging 33
Gn/Gp Delay Monitoring 33
GTP-C Path Failure Detection and Management 34
GTPv0 Fallback, Disabling to Reduce Signalling 34
Handling Multiple MS Attaches All with the Same Random TLLI 35
HSPA Fallback 35
Ignore Context-ID during 4G/3G Handovers 35
Interface Selection Based on UE Capability 36
Intra- or Inter-SGSN Serving Radio Network Subsystem (SRNS) Relocation (3G only) 36
Lawful Intercept 36

Link Aggregation - Horizontal 36
Local DNS 37
Local Mapping of MBR 37
Local QoS Capping 37
Location Change Reporting on the S4-SGSN 38
Location Services 38
Lock/Shutdown the BSC from the SGSN 39
Multiple PLMN Support 39
Network Sharing 39
Benefits of Network Sharing 39
GWCN Configuration 40
MOCN Configuration 40
Implementation 41
NRI-FQDN based DNS resolution for non-local RAIs (2G subscribers) 41
NRI Handling Enhancement 42
NRPCA - 3G 42
NRSPCA Support for S4-SGSN 42
Operator Policy 43
Some Features Managed by Operator Policies 43
Overcharging Protection 43
QoS Traffic Policing per Subscriber 43
QoS Classes 44
QoS Negotiation 44
DSCP Marking 44
Traffic Policing 44
VPC-DI platform support for SGSN 45
Reordering of SNDCP N-PDU Segments 45
RAN Information Management (RIM) 46
S4 Support on the SGSN 46
S3 and S4 Interface Support 46
S4-SGSN Support for "Higher Bit Rates than 16 Mbps"Flag 47
S6d and Gr Interface Support 48
Configurable Pacing of PDP Deactivations on the S4-SGSN 48
DNS SNAPTR Support 48

S4-SGSN Statistics Support 49
S13' Interface Support 49
Idle Mode Signaling Reduction 49
ISR with Circuit Switched Fallback 50
ISD / DSD Message Handling and HSS Initiated Bearer Modification 50
UMTS-GSM AKA Support on the S4-SGSN 51
3G and 2G SGSN Routing Area Update 51
IPv4 and IPv6 PDP Type Override 52
NAPTR-based Dynamic HSS Discovery 53
P-GW Initiated PDP Bearer Deactivation 53
S-GW and P-GW Tunnel and EPS Subscription Recovery 53
Local Configuration of S-GW and S4-SGSN per RAI 53
Configurable GUTI to RAI Conversion Mapping 54
S4-SGSN Support for Fallback to V1 Cause Code in GTPv2 Context Response 54
S4-SGSN Support for Mobility Management Procedures 54
QoS Mapping Support 54
MS Initiated Primary and Secondary Activation 55
Deactivation Procedure Support 55
MS, PGW and HSS Initiated PDP Modification Procedure Support 55
Fallback from the S4 Interface to the Gn Interface 57
Operator Policy Selection of S4 or Gn Interface 57
IDFT Support During Connected Mode Handovers 57
Disassociated DSR Support 58
SGSN Serving Radio Network Subsystem (SRNS) Relocation Support 58
E-UTRAN Service Handover Support 59
Support for Gn Handoff from S4-SGSN to 2G/3G Gn SGSN 59
Suspend/Resume Support on the S4-SGSN 59
Flex Pooling (Iu / Gb over S16) Support on the S4-SGSN 60
LORC Subscriber Overcharging Protection on S4-SGSN 60
Summary of Functional Differences between an S4-SGSN and an SGSN (Gn/Gp) 60
Session Recovery 69
SCTP Parameters for SGSN 70
SGSN Pooling and Iu-Flex / Gb-Flex 71
Gb/Iu Flex Offloading 71

SGSN Supports Enhanced IMSI Range 72
SGSN Support for RAI Based Query 72
SGSN Support For Sending Extended Bits Bi-directionally 72
SGSN support to Ignore PDP Data Inactivity 72
Short Message Service (SMS over Gd) 73
SMS Authentication Repetition Rate 73
SMSC Address Denial 73
Status Updates to RNC 74
Target Access Restricted for the Subscriber Cause Code 74
Topology-based Gateway (GW) Selection 74
Threshold Crossing Alerts (TCA) Support 75
Tracking Usage of GEA Encryption Algorithms 76
Validation of MCC/MNC Values in the Old RAI Field 76
VLR Pooling via the Gs Interface 76
Synchronization of Crash Events and Minicores between Management Cards 77
Zero Volume S-CDR Suppression 77
How the SGSN Works 78
First-Time GPRS Attach 78
PDP Context Activation Procedures 80
Network-Initiated PDP Context Activation Process 81
MS-Initiated Detach Procedure 82
Supported Standards 84
IETF Requests for Comments (RFCs) 84
3GPP Standards 84
ITU Standards 95
Object Management Group (OMG) Standards 95

CHAPTER 3 **SGSN in a 2.5G GPRS Network 97**
SGSN in a 2.5G GPRS Network 97
2.5G SGSN Configuration Components 98
The SGSN_Ctx 98
The Accounting_Ctx 99
How the 2.5G SGSN Works 100
For GPRS and/or IMSI Attach 100

For PDP Activation 101
Information Required for the 2.5G SGSN 102
Global Configuration 102
SGSN Context Configuration 104
Accounting Context Configuration 106

CHAPTER 4 SGSN 3G UMTS Configuration 107
SGSN 3G UMTS Configuration 107
3G SGSN Configuration Components 108
For GPRS and/or IMSI Attach 109
Information Required for 3G Configuration 109
Global Configuration 110
SGSN Context Configuration 113
Accounting Context Configuration 115

CHAPTER 5 SGSN Service Configuration Procedures 117
SGSN Service Configuration Procedures 118
2.5G SGSN Service Configuration 118
3G SGSN Service Configuration 119
Dual Access SGSN Service Configuration 120
Configuring the S4-SGSN 121
Configuring an SS7 Routing Domain 123
Configuring an SS7 Routing Domain to Support Broadband SS7 Signaling 123
Example Configuration 124
Configuring an SS7 Routing Domain to Support IP Signaling for SIGTRAN 124
Example Configuration 125
Configuring GTT 125
Example Configuration 126
Configuring an SCCP Network 126
Example Configuration 127
Configuring a MAP Service 127
Example Configuration 128
Configuring an IuPS Service (3G only) 128
Example Configuration 129

Configuring an SGTP Service 129
Example Configuration 129
Configuring a Gs Service 129
Example Configuration 130
Configuring an SGSN Service (3G only) 130
Example Configuration 131
Configuring a GPRS Service (2.5G only) 132
Example Configuration 132
Configuring a Network Service Entity 132
Configure a Network Service Entity for IP 132
Example Configuration for a Network Service Entity for IP 133
Configure a Network Service Entity for Frame Relay 133
Example Configuration for a Network Service Entity for IP 133
Configuring DNS Client 133
Example Configuration 134
Configuring GTPP Accounting Support 134
Creating GTPP Group 135
Configuring GTPP Group 135
Verifying GTPP Group Configuration 136
Configuring and Associating the EGTP Service (S4 Only) 136
Example Configuration 137
Configuring and Associating the GTPU Service (S4 Only) 138
Example Configuration 138
Configuring the DNS Client Context for APN and SGW Resolution (Optional) 139
Example Configuration 139
Configuring the S6d Diameter Interface (S4 Only) 140
Configuring the Diameter Endpoint for the S6d Interface 140
Example Configuration 141
Configuring the HSS Peer Service and Interface Association for the S6d Interface 141
Example Configuration 142
Associating the HSS Peer Service with the SGSN and GPRS Services for the S6d Interface 142
Example Configuration 142
Configuring Operator Policy-Based S6d Interface Selection (Optional) 142
Example Configuration 143

Configuring the Subscription Interface Preference for the S6d Interface (Optional) 143
Example Configuration 143
Configuring the S13' Interface (S4 Only, Optional) 143
Configuring a Diameter Endpoint for the S13' Interface 144
Example Configuration 144
Configuring the HSS Peer Service and Interface Association for the S13' Interface 145
Example Configuration 145
Associating the HSS Peer Service with the SGSN and GPRS Services for the S13' Interface 146
Example Configuration 146
Configuring S13' Interface Selection Based on an Operator Policy 146
Example Configuration 147
Configuring QoS Mapping for EPC-Capable UEs using the S4 Interface (S4 Only, Optional) 147
Example Configuration 148
Configuring the Peer SGSN Interface Type (S4 Only, Optional) 148
Example Configuration 148
Configuring Gn Interface Selection Based on an Operator Policy (S4 Only, Optional) 149
Example Configuration 149
Configuring a Custom MME Group ID (S4 Only, Optional) 149
Example Configuration 150
Configuring and Associating the Selection of an SGW for RAI (S4 Only, Optional) 150
Example Configuration 151
Configuring a Local PGW Address (S4 Only, Optional) 152
Example Configuration 152
Configuring the Peer MME Address (S4 Only, Optional) 152
Example Configuration 152
Configuring the ISR Feature (S4 Only, Optional) 153
Example Configuration 153
Configuring IDFT for Connected Mode Handover (S4 Only, Optional) 154
Example Configuration 155
Creating and Configuring ATM Interfaces and Ports (3G only) 155
Creating and Configuring Frame Relay Ports (2.5G only) 155
Configuring APS/MSP Redundancy 155
Example Configuration 156

CHAPTER 6 **3G-2G Location Change Reporting** 157

Feature Description 157

Relationships 157

License 158

Standards Compliance 158

How it Works 158

Call Flows 158

Configuring Location Change Reporting 160

Verifying the Location Change Reporting Configuration 160

CHAPTER 7 **5G NSA for SGSN** 163

Feature Summary and Revision History 163

Feature Description 164

How It Works 165

Limitations 165

Flows 165

Standards Compliance 167

Configuring 5G NSA for SGSN 168

Enabling DCNR in Call Control Profile 168

Configuring DCNR in SGSN Global Configuration 168

Monitoring and Troubleshooting 169

Show Commands and Outputs 169

Bulk Statistics 172

CHAPTER 8 **APN-OI-Replacement for Gn-SGSN** 177

Feature Description 177

How It Works 178

Monitoring and Troubleshooting 180

CHAPTER 9 **APN Restriction** 183

Feature Description 183

Relationships to Other Features 183

How it Works 184

Limitations 185
Standards Compliance 186
Configuring APN Restriction 186
Verifying the APN Restriction Configuration 186
Monitoring and Troubleshooting the APN Restriction 186

CHAPTER 10 **Attach Rate Throttling** 189
Feature Description 189
How it Works 190
Attach Rate Throttling Feature 190
Limitations 191
Configuring the Attach Rate Throttling Feature 191
Monitoring and Troubleshooting the Attach Rate Throttling Feature 192
Attach Rate Throttling Show Commands and Outputs 192

CHAPTER 11 **Backup and Recovery of Key KPI Statistics** 193
Feature Description 193
How It Works 193
Architecture 194
Limitations 195
Configuring Backup Statistics Feature 196
Configuration 196
Verifying the Backup Statistics Feature Configuration 197
Managing Backed-up Statistics 197

CHAPTER 12 **Cause Code #66** 199
Feature Description 199
How It Works 200
Standards Compliance 200
Configuring PDP Activation Restriction and Cause Code Values 200
Configuring PDP Activation Restriction 201
Configuring SM Cause Code Mapping for SGSN 201
Configuring ESM Cause Code Mapping for ESM Procedures (for MME) 201
Configuring EMM and ESM Cause Code Mapping for EMM Procedures (for MME) 202

Configuring ESM Cause Code Mapping for ESM Procedures (MME Service Configuration Mode) 202
Configuring EMM and ESM Cause Code Mapping for EMM Procedures (MME Service Configuration Mode) 203
Verifying the Feature Configuration 203
Monitoring and Troubleshooting the Cause Code Configuration 204
Show Command(s) and/or Outputs 205
show gmm-sm statistics verbose 205
Bulk Statistics 205

CHAPTER 13 Cause Code Mapping 207
Cause Code Mapping 207
Feature Description 207
Configuring Cause Code Mapping 208
Configuring GMM Cause Codes to Replace MAP Cause Codes 208
Verifying Configuration to Replace MAP Cause Codes 208
Configuring GMM Cause Code for RAU Reject due to Context Transfer Failure 209
Verifying Configuration for Context Transfer Failures 209
Configuring SM Cause Codes 209
Verifying Configuration for SM Cause Codes 209

CHAPTER 14 SGSN Controlling Peer Status Based on Heartbeat Message 211
Feature Summary and Revision History 211
Feature Description 211
Configuring SGSN Controlling Peer Status Based on Heartbeat Message 212
Configuring SCTP Peer Active Heartbeat Acknowledgment 212

CHAPTER 15 Default APN Selection Based on Context ID 213
Feature Summary and Revision History 213
Feature Description 213
Configuring Default APN Selection Based on Context ID 214
Configuring APN Selection Default 214

CHAPTER 16 Direct Tunnel for 3G Networks 215

Direct Tunnel Feature Overview 215
Direct Tunnel Configuration 219
Configuring Direct Tunnel Support on the SGSN 219
Enabling Setup of GTP-U Direct Tunnels 220
Enabling Direct Tunnel per APN 220
Enabling Direct Tunnel per IMEI 221
Enabling Direct Tunnel to Specific RNCs 221
Restricting Direct Tunnels 222
Verifying the SGSN Direct Tunnel Configuration 223

CHAPTER 17 **Direct Tunnel for 4G (LTE) Networks 225**
Direct Tunnel for 4G Networks - Feature Description 225
How It Works 228
DT Establishment Logic 228
Establishment of Direct Tunnel 229
Direct Tunnel Activation for Primary PDP Context 230
Direct Tunnel Activation for UE Initiated Secondary PDP Context 230
RAB Release with Direct Tunnel 231
Iu Release with Direct Tunnel 232
Service Request with Direct Tunnel 233
Downlink Data Notification with Direct Tunnel when UE in Connected State 234
Downlink Data Notification with Direct Tunnel when UE in Idle State 234
Intra SGSN Routing Area Update without SGW Change 235
Routing Area Update with S-GW Change 240
Intra SRNS with S-GW Change 245
Intra SRNS without S-GW Change 245
New SRNS with S-GW Change and Direct Data Transfer 248
New SRNS with S-GW Change and Indirect Data Transfer 248
Old SRNS with Direct Data Transfer 251
Old SRNS with Indirect Data Transfer 252
Network Initiated Secondary PDP Context Activation 255
PGW Init Modification when UE is Idle 255
Limitations 256
Standards Compliance 257

Configuring Support for Direct Tunnel 257
Configuring Direct Tunnel on an S4-SGSN 257
Enabling Setup of GTP-U Direct Tunnel 257
Enabling Direct Tunnel to RNCs 258
Restricting Direct Tunnels 258
Verifying the Call-Control Profile Configuration 259
Verifying the RNC Configuration 259
Configuring S12 Direct Tunnel Support on the S-GW 259
Monitoring and Troubleshooting Direct Tunnel 260
show subscribers sgsn-only 260
show gmm-sm statistics sm-only 261
Direct Tunnel Bulk Statistics 261

CHAPTER 18 EC-GSM Support on the SGSN 263
Feature Description 263
How It Works 264
Standards Compliance 264
Limitations and Restrictions 265
Configuring EC-GSM on the SGSN 265
Verifying EC-GSM for SGSN 265
Monitoring and Troublshooting EC-GSM on the SGSN 265

CHAPTER 19 Enhanced Whitelisting in SGSN 267
Feature Summary and Revision History 267
Feature Description 268
How it Works 268
Architecture 268
Configuring Enhanced Whitelisting in SGSN 269
Configuring Discrete IMSI Numbers 269
Configuring IMSI Range 269
Configuring Discrete MSISDN Numbers 270
Associating MSISDN Range with Operator Policy 270
Configuring MSISDN Range 271
Configuring Routing Area List 271

Configuring RAU-inter Restrict for SGSN 272
Configuring RAU-intra Allow for SGSN 272
Configuring SRNS Intra 273

CHAPTER 20 Exclude OPC in SCCP Calling-Party-Address on Gs Interface for Route-On-GT 275
Feature Description 275
Configuring the Feature 275
Verifying the Configuration 276

CHAPTER 21 GMM-SM Event Logging 277
Feature Description 277
Feature Overview 277
Events to be Logged 277
Event Record Fields 278
EDR Storage 283
Architecture 283
Limitations 283
Configuration 283

CHAPTER 22 Graceful Assert Handling 285
Feature Summary and Revision History 285
Feature Description 285
Configuring Graceful Assert Handling 286
Monitoring and Troubleshooting 287
Show Commands and/or Outputs 287
show session subsystem facility sessmgr instance <instance_num> debug-info verbose 287

CHAPTER 23 GTPU Error Indication Enhancement 289
Feature Description 289

CHAPTER 24 Identity Procedure on Authentication Failure 291
Feature Description 291
Authentication Failures 291
Identity Procedure 292

How It Works 292
GSM Authentication Unacceptable 293
MAC Failure in 2G 293
Configuring Performance of Identity Procedure 293
Verifying the Configuration 293
Monitoring and Troubleshooting the Performance of Identity Procedure for Authentication Failure 294
show gmm-sm statistics verbose 294
show gmm-sm statistics 294

CHAPTER 25 **Idle Mode Signaling Reduction on the S4-SGSN 295**
Feature Description 295
Relationships 296
How ISR Works 296
Limitations 297
Call Flows 298
2G ISR Activation by the S4-SGSN 298
Standards Compliance 301
Configuring Idle-Mode-Signaling Reduction 301
Configuring 2G ISR 301
Verifying the 2G ISR Configuration 302
Configuring 3G ISR 302
Verifying the 3G ISR Configuration 302
Monitoring and Troubleshooting the ISR Feature 303
ISR Show Command(s) and Outputs 303
show subscribers gprs-only full 303
show subscribers sgsn-only full 303
show s4-sgsn statistics (2G ISR) 303
show s4-sgsn statistics (3G ISR) 304
show gmm statistics (2G ISR) 304
show gmm statistics (3G ISR) 304

CHAPTER 26 **IMSI Manager Broadcast Control 305**

Feature Description 305
How It Works 306
Configuring IMSI Manager Broadcast Control 307
Monitoring and Troubleshooting IMSI Manager Broadcast Control 307
Show Command(s) and/or Outputs 308
show demuxmgr statistics imsimgr all 308

CHAPTER 27 IMSI Manager Overload Control 309
Feature Description 309
Monitoring and Troubleshooting IMSI Manager Overload Control 310
Show Command(s) and/or Outputs 310
show demuxmgr statistics imsimgr all 310

CHAPTER 28 ISR with Circuit Switched Fallback 311
ISR with CSFB - Feature Description 311
Call Flows 312
Relationships to Other Features 315
Relationships to Other Products 315
How it Works 315
ISR CSFB Procedures 316
Standards Compliance 319
Configuring ISR with Circuit Switched Fallback 320
Monitoring and trouble-shooting the CSFB feature 320

CHAPTER 29 Location Services 321
Location Services - Feature Description 321
How Location Services Works 321
Relationship to Other SGSN Functions 322
Architecture 322
Limitations 323
Flows 323
Flows 323
Standards Compliance 325
Configuring Location Services (LCS) on the SGSN 326

Enabling LCS 326
Identifying the GMLC 327
Configuring Exclusion of GMLC Address from Update-GPRS-Location Messages 327
Creating the Location Service Configuration 328
Fine-tuning the Location Service Configuration 328
Associating the Location Service Config with the SGSN 329
Associating the Location Service Config with an Operator Policy 329
Verifying the LCS Configuration for the SGSN 330
Monitoring and Troubleshooting the LCS on the SGSN 330

CHAPTER 30 **LORC Subscriber Overcharging Protection for S4-SGSN 331**
Feature Description 331
LORC Subscriber Overcharge Protection on the S4-SGSN 331
Release Access Bearer Requests 332
Relationships 332
How It Works 332
3G Iu-Release Procedure and Overcharge Protection over S4 333
2G Ready-to-Standby State Transition and Overcharge Protection over S4 333
Standards Compliance 334
Configuring Subscriber Overcharging Protection 335
Enabling Release Access Bearer Request 335
Configuring the Causes to Include ARRL in Release Access Bearer Request 335
Enabling Subscriber Overcharging Protection on S4 337

CHAPTER 31 **MOCN for 2G SGSN 339**
Feature Description 339
Gate Core Network (GWCN) Configuration 339
Multi Operator Core Network (MOCN) Configuration 340
Relationships to Other Features 341
How It Works 341
Automatic PLMN Selection in Idle Mode 341
MOCN Configuration with Non-supporting MS 341
Architecture 342
Redirection in GERAN with MOCN Configuration 342

Standards Compliance 345
Configuring 2G MOCN 345
GPRS MOCN Configuration 345
gprs-mocn 345
Verifying gprs-mocn Configuration 345
Common PLMN-Id and List of PLMN Ids Configuration 345
plmn id 345
Verifying plmn id Configuration 346
Network Sharing Configuration 346
network-sharing cs-ps-coordination 346
Verifying network-sharing Configuration 346
network-sharing failure-code 347
Verifying Failure Code Configuration 347
Monitoring and Troubleshooting 2G SGSN MOCN Support 347
show sgsn-mode 347
show gprs-service name 347
show gmm-sm statistics verbose 348

CHAPTER 32 **MTC Congestion Control** 349
Feature Description 349
Relationships 350
How It Works 350
SGSN Congestion Control 350
APN-level Congestion Control for MM 350
APN-level Congestion Control for SM 351
Support for the Extended T3312 Timer 352
Limitations 352
Flows for SGSN Congestion Control 352
Flows for APN-level Congestion Control for MM 353
Flows for APN-level Congestion Control for SM 354
Handling Value for Extended T3312 Timer 356
Standards Compliance 356
Configuring MTC Congestion Control 356
Enabling Global-level Congestion Control 357

Verifying the Global-level Congestion Control Configuration 357
Configuring System-detected Congestion Thresholds 358
Verifying System-detected Congestion Thresholds Configuration 358
Configuring SGSN Congestion Control 359
Verifying the SGSN Congestion Control Configuration 360
Configuring APN-based Congestion Control 360
Verifying the APN-based Congestion Control Configuration 361
Configuring Extended T3312 Timer 361
Verifying the Extended T3312 Configurations 363
Configuring Backoff Timers 363
Verifying the T3346 Configurations 364
Configuring O&M Triggered Congestion 364
Monitoring MTC Congestion Control 365
show session disconnect-reasons 365
show congestion-control statistics imsimgr all full 365

CHAPTER 33 **Network Requested Secondary PDP Context Activation** 367
Feature Description 367
Benefits 367
Relationships to Other Features 367
How It Works 368
Gn/Gp SGSN 368
Successful Activation for Gn/Gp SGSN 368
Unsuccessful Activation for Gn/Gp SGSN 369
S4-SGSN 371
Successful Activation for S4-SGSN 371
Limitations 374
Standards Compliance 374
Configuring NRSPCA 374
Sample NRSPCA Configuration 374
Verifying the NRSPCA Configuration 375
Monitoring and Troubleshooting the NRSPCA Feature 375
NRSPCA show Commands 376
show gmm-sm statistics sm-only 376

show sgtpc statistics 379

CHAPTER 34 **Operator Policy 381**

What Operator Policy Can Do 381

A Look at Operator Policy on an SGSN 381

A Look at Operator Policy on an S-GW 382

The Operator Policy Feature in Detail 382

Call Control Profile 382

APN Profile 383

IMEI-Profile (SGSN only) 384

APN Remap Table 384

Operator Policies 385

IMSI Ranges 386

How It Works 386

Operator Policy Configuration 386

Call Control Profile Configuration 387

Configuring the Call Control Profile for an SGSN 387

Configuring the Call Control Profile for an MME or S-GW 388

APN Profile Configuration 388

IMEI Profile Configuration - SGSN only 389

APN Remap Table Configuration 389

Operator Policy Configuration 390

IMSI Range Configuration 390

Configuring IMSI Ranges on the MME or S-GW 390

Configuring IMSI Ranges on the SGSN 391

Associating Operator Policy Components on the MME 391

Configuring Accounting Mode for S-GW 391

Verifying the Feature Configuration 392

CHAPTER 35 **Paging in Common Routing Area for 2G and 3G 393**

Feature Description 393

How it Works 393

Paging in Common Routing Area for 2G subscriber 393

Paging in Common Routing Area for 3G subscriber 394

Standards Compliance 395
Configuring Paging in Common Routing Area for 2G and 3G 395
Verifying the Paging in Common Routing Area for 2G and 3G Configuration 395
show sgsn-mode 395
Monitoring and Troubleshooting Paging in Common Routing Area for 2G and 3G feature 395
Paging in Common Routing Area for 2G and 3G Show Command(s) and/or Outputs 395
show gmm-sm statistics 395
Paging in Common Routing Area for 2G and 3G Bulk Statistics 396

CHAPTER 36 **Page Throttling 399**
Feature Description 399
Relationships to Other SGSN Features 399
How it Works 400
Page Throttling in a GPRS Scenario 400
Page Throttling in an UMTS Scenario 401
Limitations 403
Configuring Page Throttling 404
To map RNC Name to RNC Identifier 404
To associate a paging RLF template 404
Verifying the Page Throttling Configuration 405
Monitoring and Troubleshooting the Page Throttling feature 406
Page Throttling Show Command(s) and/or Outputs 406
show gmm-sm statistics verbose 406

CHAPTER 37 **PGW Restart Notification in S4-SGSN 409**
Feature Description 409
Overview 409
How it Works 410
Limitations 410
Standards Compliance 410
Configuring PGW Restart Notification in S4-SGSN 411
Configure Node IE For PRN Advertisement 411
Configure Default APN Restoration Priority 411
Verifying the PRN Configuration in S4-SGSN 411

Monitoring and Troubleshooting PRN support in S4-SGSN 412
PGW Restart Notification Show Command(s) and/or Outputs 412
show s4-sgsn statistics 412
show egtpc statistics 412
show session disconnect-reasons verbose 413

CHAPTER 38 **Quality of Service (QoS) Management for SGSN 415**
Quality of Service Management 415
SGSN Quality of Service Management 415
Quality of Service Attributes 415
Quality of Service Attributes in Release 97/98 416
Quality of Service Attributes in Release 99 416
Quality of Service Management in SGSN 417
QoS Features 420
Traffic Policing 420
QoS Management When UE is Using S4-interface for PDP Contexts 426
QoS Handling Scenarios 431
QoS Handling During Primary PDP Activation 437
QoS Handling When EPS Subscription is Available 437
QoS Handling When Only GPRS Subscription is Available 437
QoS Handling During Secondary PDP Activation 437
QoS Handling When EPS Subscription is Available 437
QoS Handling When Only GPRS Subscription is Available 438
MS Initiated QoS Modification 438
HSS Initiated PDP Context Modification 440
PGW Initiated QoS Modification 440
ARP Handling 441
Difference between Gn SGSN and S4 SGSN 441
ARP values in Gn SGSN 441
ARP values in S4 SGSN 442
Handling of ARP Values in Various Scenarios 444
Mapping EPC ARP to RANAP ARP 445
ARP configured in CC Profile 446
ARP-RP Mapping for Radio Priority in Messages 446

CHAPTER 39 **RAB Release for Attach on the Same IU Connection** 449

Feature Summary and Revision History 449

Feature Description 450

Configuring RAB Release for Attach on the Same IU Connection 450

Configuring RAB Assignment Request 450

Monitoring and Troubleshooting 450

Show Commands and Outputs 450

Verifying the RAB Release Extension configuration 451

CHAPTER 40 **RIM Message Transfer from BSC or RNC to eNodeB** 453

Feature Description 453

RAN Information Management (RIM) 453

Relationships to Other Feature or Products 454

How It Works 454

RIM Addressing 454

Call Flows - Transmitter of GTP RIM Msg 454

Call Flows - Receiver of GTP RIM Msg 455

RIM Application 455

Standards Compliance 456

Configuring RIM Msg Transfer to or from eNodeB 456

Configuring RIM Functionality 456

Associating Previously Configured SGTP and IuPS Services 457

Configuring the peer-MME's address - Locally 457

Configuring the peer-MME's address - for DNS Query 457

Monitoring and Troubleshooting RIM Msg Transfer 457

show gmm-sm statistics verbose 458

show gmm-sm statistics verbose | grep RIM 458

show sgtpc statistics verbose 458

show bssgp statistics verbose 458

CHAPTER 41 **RTLLI Management for 2G M2M Devices** 459

Feature Description 459

How It Works 459

Configuring RTLLI Management 459
Monitoring and Troubleshooting 460

CHAPTER 42 S4 interface Support For Non-EPC Devices 463
Feature Description 463
Overview 463
How it Works 464
Architecture 464
Limitations 465
Configuring S4 Interface Support for Non-EPC Capable Devices 465
Configuring selection of the S4 interface 465
Monitoring and Troubleshooting S4 Interface Support for Non-EPC Capable devices 466
S4 Interface Support for Non-EPC devices Show Command(s) and/or Outputs 466
show call-control-profile full name < > 466
show subscribers sgsn-only full imsi < > 467
show subscribers gprs-only full imsi < > 467

CHAPTER 43 S4-SGSN Suspend-Resume Feature 469
Feature Description 469
Suspension of GPRS Services 469
Relationships to Other Features 470
How it Works 470
S4-SGSN Suspend-Resume Feature 470
Limitations 470
Call Flows 471
Intra-SGSN Suspend Procedure with Resume as the Subsequent Procedure 471
Intra-SGSN Suspend with Resume Procedure with Intra-RAU as Subsequent Procedure 472
Inter-SGSN Suspend and Resume Procedure with Peer S4-SGSN/MME 473
New Inter-SGSN Suspend and Resume Procedure from BSS to 2G Gn-SGSN 474
New SGSN Suspend and Resume Procedure with Peer Gn-SGSN as Old SGSN 475
Interface Selection Logic for Inter-SGSN Suspend (New SGSN) Procedure 476
Intra-SGSN Inter-System Suspend and Resume Procedure 478
Inter-SGSN Inter-System Suspend and Resume Procedure 478
Standards Compliance 480

Configuring the S4-SGSN Suspend/Resume Feature 480
Monitoring and Troubleshooting the S4-SGSN Suspend/Resume Feature 480
S4-SGSN Suspend and Resume Feature Show Commands 480
show subscriber gprs-only full all 480
show subscriber sgsn-only full all 481
show bssgp statistics verbose 481
show egtpc statistics 482
show egtpc statistics verbose 483
show sgtpc statistics verbose 487
S4-SGSN Suspend and Resume Feature Bulk Statistics 488

CHAPTER 44 SGSN Clear Subscriber Enhancement 491
Feature Summary and Revision History 491
Feature Description 492
Configuring Clear Subscriber 492
Clear Subscribers Enhancement 492

CHAPTER 45 SGSN-MME Combo Optimization 493
Feature Description 493
Overview 493
How It Works 494
Architecture 495
Flows 495
Limitations 497
Configuring the Combo Optimization 497
Verifying Combo Optimization Configuration 498
show lte-policy sgsn-mme summary 498
Monitoring and Troubleshooting Combo Optimization 498
Monitoring Commands for the SGSN-MME Combo Node 498
show hss-peer-service statistics all 498
Monitoring Commands for the SGSN 499
show demux-mgr statistics imsimgr all sgsn 499
show subscribers sgsn-only summary 499
show subscribers gprs-only summary 499

show subscribers sgsn-only full all 499
show subscribers gprs-only full all 500
show session subsystem facility aaamgr instance 500
Monitoring Commands for the MME 500
show mme-service statistics handover 500
Bulk Statistics for Monitoring the MME in an SGSN-MME Combo Node 501

CHAPTER 46 SGSN Pooling 503
Feature Description 503
A Basic Pool Structure 504
Benefits of SGSN Pooling 504
Pooling Requirements 505
How it Works 505
P-TMSI - NRI and Coding 505
Non-Broadcast LAC and RAC 505
SGSN Address Resolution 505
Mobility Inside the Pool 506
Mobility Outside the Pool 507
MS Offloading 509
Iu/Gb Flex support over S16/S3 interface 510
Standards Compliance 511
Configuring the SGSN Pooling feature 512
2G-SGSN pool configuration 512
3G-SGSN pool configuration 512
Monitoring and Troubleshooting the SGSN Pooling feature 514
SGSN Pooling Show Command(s) and/or Outputs 514

CHAPTER 47 SGSN Processes Uplink Data Status IE in Service Request 515
Feature Description 515
Standards Compliance 515
Configuring Processing of Uplink Data Status IE in Service Request 515
Verifying the Configuration 516
Monitoring and Troubleshooting the Feature 516
Show Command(s) and/or Outputs 516

show gmm-sm statistics 516

CHAPTER 48 SGSN Serving Radio Network Subsystem Relocation 517

Feature Description 517

Relationships to Other Features 517

How it Works 518

SRNS Relocation on the SGSN (Gn/Gp) 518

SGSN (Gn/Gp) SRNS Relocation Call Flow Diagrams 519

SRNS Relocation on the S4-SGSN 525

IDFT Support During Connected Mode Handovers 528

S4-SGSN SRNS Relocation Call Flow Diagrams 530

Standards Compliance 553

Configuring SRNS Relocation on the SGSN 553

Configuring the SRNS Relocation Feature 553

Enabling IDFT (Optional, S4-SGSN Only) 554

Verifying the SRNS Feature Configuration 554

Monitoring and Troubleshooting SRNS Relocation 555

SRNS Bulk Statistics 555

Show Command Output Supporting the SRNS Relocation Feature 556

CHAPTER 49 SGSN Support for IMSI Manager Scaling 559

Feature Description 559

How it Works 559

Detailed Description 559

Relationships to Other Features 560

Configuring Support for Multiple IMSI Managers 560

Verifying the Configuration 561

Monitoring and Troubleshooting the Multiple IMSI Manager Support 561

Multiple IMSI Managers Show Command(s) and/or Outputs 561

show linkmgr all 561

show linkmgr instance parser statistics all 562

show gbmgr instance parser statistics all 562

show demuxmgr statistics imsimgr verbose 562

show demux-mgr statistics sgtpcmgr instance < id > 562

show session subsystem facility mmemgr instance < id > 563
show subscribers mme-only full all/ show mme-service session full all 563
show mme-service db record call-id <id> 563

CHAPTER 50 SGSN Support for Peer-Server Blocking 565
Feature Description 565
How it Works 566
Configuring Peer-Server Blocking 568
Verifying the Peer-Server Blocking Configuration 568
Monitoring and Troubleshooting the Peer-Server Blocking 569

CHAPTER 51 Support for EPC QoS Attributes on SGSN 571
Feature Description 571
Overview 571
How It Works 572
Standards Compliance 573
Configuring EPC QoS Support on SGSN 573
Configuring QoS Profile to Support EPS QoS Parameters in GTPv1 messages 573
Configure E-ARP values in the Quality of Service Profile 573
Configure Local Capping in the Quality of Service Profile 574
Configure Override of E-ARP Values Provided by GGSN 574
Verifying the Configuration 574
Monitoring and Troubleshooting EPC QoS Support on SGSN 574
Show Command(s) and/or Outputs 575
show subscriber sgsn-only full all 575
Troubleshooting EPC QoS Support on SGSN 575

CHAPTER 52 Support For QoS Upgrade From GGSN or PCRF 577
Feature Description 577
How it Works 577
Configuring Support for QoS upgrade from GGSN/PCRF 579
Verifying the QoS Upgrade Support Configuration 580

CHAPTER 53 Support for SGSN QoS based on PLMN, RAT Type 581

Feature Description 581
How it Works 581
Configuring SGSN Support for RAT Type based QoS Selection 582
Configuring APN Profile and QoS Profile Association 582
Configuring the Quality of Service Profile 583
Monitoring and Troubleshooting RAT Type Based QoS Selection 583
Show Command(s) and/or Outputs 583
show apn-profile full [all | name] 583
show quality-of-service-profile [all | full [all | name] | name] 584

CHAPTER 54 **Support for RAT/Frequency Selection Priority ID (RFSP-ID) 585**
Feature Description 585
How it Works 585
Encoding and De-coding of RFSP Ids in different scenarios 585
Standards Compliance 588
Configuring Support for RAT/Frequency Selection Priority ID 588
Monitoring and Troubleshooting the the Support for RFSP-ID 589
Show Command(s) and/or Outputs 589
show call-control profile 589
show subscribers sgsn-only full all 589
show subscribers gprs-only full all 589
show iups-service name 589
show sgsn-mode 590

CHAPTER 55 **Subscriber Overcharging Protection 591**
Feature Overview 591
Overcharging Protection - GGSN Configuration 593
GTP-C Private Extension Configuration 593
Verifying Your GGSN Configuration 594
Overcharging Protection - SGSN Configuration 594
Private Extension IE Configuration 595
RANAP Cause Trigger Configuration 595
RANAP RAB Release Configuration 596
Verifying the Feature Configuration 596

CHAPTER 56 **Topology-based Gateway Selection** 599

Feature Description 599

How It Works 600

First Primary Activation - Gn/Gp-SGSN 600

Primary Activation - S4-SGSN 600

Primary Activation for Subsequent PDN 601

Intra RAU, New SGSN RAU, Intra SRNS, New SRNS, IRAT 601

Limitations 601

Standards Compliance 601

Configuring Topology-based GW Selection 602

Configuring GW Selection 602

Verifying the GW Selection Configuration 602

Configuring DNS Queries for the Gn/Gp-SGSN 603

Verifying the DNS Queries Configuration for the Gn/Gp-SGSN 603

Configuring DNS Queries for the S4-SGSN 603

Verifying the DNS Queries Configuration for the S4-SGSN 604

Configuring the Canonical Node Name for the Gn/Gp-SGSN 604

Verifying the Canonical Node Name Configuration 604

Monitoring Topology-based GW Selection 604

show subscribers [gprs-only | sgsn-only] full 605

CHAPTER 57 **Triggering Iu Release Command Procedure** 607

Feature Summary and Revision History 607

Feature Description 608

Configuring RAB Messages with Cause 46 609

Configuring RAB Assignment Response 609

Configuring RAB Release Request 609

Monitoring and Troubleshooting 610

Show Commands and Outputs 610

show iups-service all 610

Bulk Statistics 610

CHAPTER 58 **UDPC2 Support for MME/SGSN** 611

Feature Description 611
How It Works 612
Configuring MME/SGSN Support on UDPC2 614
Configuring MME Managers per Session Card 614
Configuring MME Managers per Chassis 615
Verifying the Configuration 617

CHAPTER 59 UTRAN to E-UTRAN Handover 619
Feature Summary and Revision History 619
Feature Description 620
Configuring UTRAN to E-UTRAN Handover 620
Configuring eNodeB Data Forwarding 620
Monitoring and Troubleshooting 621
Show Commands and Outputs 621

CHAPTER 60 Monitoring, Troubleshooting and Recommendations 623
Monitoring, Troubleshooting and Recommendations 623
Monitoring 624
Daily - Standard Health Check 624
Monthly System Maintenance 627
Every 6 Months 628
Troubleshooting 628
Problems and Issues 628
Troubleshooting More Serious Problems 629
Causes for Attach Reject 629
Single Attach and Single Activate Failures 629
Mass Attach and Activate Problems 630
Single PDP Context Activation without Data 630
Mass PDP Context Activation but No Data 631
Recommendations 632

APPENDIX A Engineering Rules 635
Engineering Rules 635
Service Rules 635

SGSN Connection Rules 636
Operator Policy Rules 637
SS7 Rules 639
SS7 Routing 639
SIGTRAN 640
Broadband SS7 640
SCCP 641
GTT 641
SGSN Interface Rules 641
System-Level 641
3G Interface Limits 642
2G Interface Limits 642

About this Guide

This preface describes the *SGSN Administration Guide*, its organization, document conventions, related documents, and contact information for Cisco customer service.

The SGSN (Serving GPRS Support Node) is a StarOS application that runs on Cisco® ASR 5500 and virtualized platforms.

- Conventions Used, on page xxxvii
- Supported Documents and Resources, on page xxxix
- Contacting Customer Support , on page xxxix

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 **commands**	This typeface represents commands that you enter, for example: **show ip access-list** 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 **command** *variable*	This typeface represents a variable that is part of a command, for example: **show card** *slot_number* *slot_number* 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 **File** menu, then click **New**

Command Syntax Conventions	Description
{ keyword or *variable* **}**	Required keyword options and variables are those components that are required to be entered as part of the command syntax. Required keyword options and variables are surrounded by grouped braces { }. For example: **sctp-max-data-chunks { limit** *max_chunks* **| mtu-limit }** If a keyword or variable is not enclosed in braces or brackets, it is mandatory. For example: **snmp trap link-status**
[keyword or *variable* **]**	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by brackets.
|	Some commands support multiple options. These are documented within braces or brackets by separating each option with a vertical bar. These options can be used in conjunction with required or optional keywords or variables. For example: **action activate-flow-detection { intitiation | termination }** or **ip address [count** *number_of_packets* **| size** *number_of_bytes* **]**

Supported Documents and Resources

Related Common Documentation

The most up-to-date information for this product is available in the SGSN Release Notes provided with each product release.

The following common documents are available:

- *AAA Interface Administration and Reference*
- *Command Line Interface Reference*
- *GTPP Interface Administration and Reference*
- *Installation Guide* (platform dependent)
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *System Administration Guide* (platform dependent)
- *Thresholding Configuration Guide*
- *Cisco StarOS IP Security (IPSec) Reference*

Related Product Documentation

The following document(s) is/are also available for products that work in conjunction with the SGSN:

- *GGSN Administration Guide*
- *MME Administration Guide*
- *MURAL Software Installation Guide*

Obtaining Documentation

The most current Cisco documentation is available on the following website:

http://www.cisco.com/cisco/web/psa/default.html

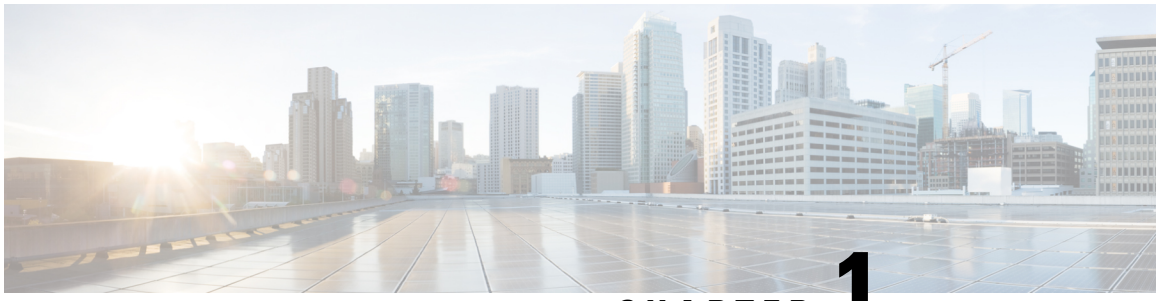
Use the following path selections to access the SGSN documentation:

Products > Wireless > Mobile Internet> Network Functions > Cisco SGSN Serving GPRS Support Node

Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.



CHAPTER 1

1-in-N IMEI Check per SGSN Subscriber

- Feature Summary and Revision History, on page 1
- Feature Description, on page 2
- Configuring IMEI Check to EIR for the First 1-N Events, on page 2

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *SGSN Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.10

Feature Description

The SGSN supports IMEI check for a configurable number of subscriber events ranging from 1 to 15 events. With this release, the SGSN skips sending IMEI check to EIR for the first "N-1" events where IMEI/IMEISV is received. The number of IMEI Check for each subscriber towards EIR is drastically reduced thereby reducing the EIR load. This also ensures that each subscriber is IMEI/IMEISV checked periodically.

Important Fresh IMEI check happens for requests with foreign PTMSI landed to different session managers other than the session manager where the subscriber was housed previously.

Configuring IMEI Check to EIR for the First 1-N Events

This section describes how to configure IMEI check to EIR for the first 1-N events.

Configuring IMEI Check Every N Events in MAP Service

Use the following configuration to perform IMEI check every N events for each subscriber.

```
configure
  context context_name
    map-service map_service_name
       equipment-identity-register { isdn E.164_num | point code point_code
} check-imei-sub-every-n-events times
      no equipment-identity-register { isdn E.164_num | point code point_code
} [ include-imsi | map-include-imsi ]
       end
```

Notes:

- **check-imei-sub-every-n-events** *times*: Performs IMEI check every N events for each subscriber. *times* must be an integer ranging from 1 to 15.
- **no**: Disables the configuration to perform IMEI check every N events for each subscriber.

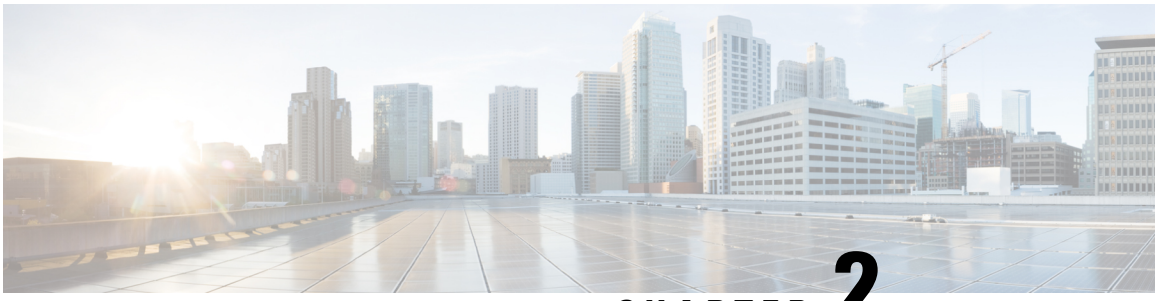
Configuring IMEI Check Every N Events in EIR-Profile

Use the following configuration to Perform IMEI check every N events for each subscriber.

```
configure
  sgsn-global
    eir-profile profile_name
       check-imei-sub-every-n-events check_frequency
       no check-imei-sub-every-n-events
       end
```

Notes:

- **eir-profile** *profile_name*: Configures EIR profile. Pointcode/ISDN should be configured for EIR Profile to be valid. *profile_name* Specifies the EIR profile name, must be a string of 1 to 64 characters.
- **check-imei-sub-every-n-events** *check_frequency*: Performs IMEI check every N events for each subscriber . *check_frequency* must be an integer from 1 to 15.
- **no**: Disables the configuration to Perform IMEI check every N events for each subscriber.



CHAPTER 2

Serving GPRS Support Node (SGSN) Overview

This section contains general overview information about the Serving GPRS Support Node (SGSN), including sections for:

- Product Description, on page 5
- Network Deployments and Interfaces, on page 6
- SGSN Core Functionality , on page 13
- Features and Functionality , on page 20
- How the SGSN Works, on page 78
- Supported Standards, on page 84

Product Description

StarOS provides a highly flexible and efficient Serving GPRS Support Node (SGSN) service to the wireless carriers. Functioning as an SGSN, the system readily handles wireless data services within 2.5G General Packet Radio Service (GPRS) and 3G Universal Mobile Telecommunications System (UMTS) data networks. The SGSN also can serve as an interface between GPRS and/or UMTS networks and the 4G Evolved Packet Core (EPC) network.

Important Throughout this section the designation for the subscriber equipment is referred to in various ways: UE for user equipment (common to 3G/4G scenarios), MS or mobile station (common to 2G/2.5G scenarios), and MN or mobile node (common to 2G/2.5G scenarios involving IP-level functions). Unless noted, these terms are equivalent and the term used usually complies with usage in the relevant standards.

In a GPRS/UMTS network, the SGSN works in conjunction with radio access networks (RANs) and Gateway GPRS Support Nodes (GGSNs) to:

- Communicate with home location registers (HLR) via a Gr interface and mobile visitor location registers (VLRs) via a Gs interface to register a subscriber's user equipment (UE), or to authenticate, retrieve or update subscriber profile information.
- Support Gd interface to provide short message service (SMS) and other text-based network services for attached subscribers.
- Activate and manage IPv4, IPv6, or point-to-point protocol (PPP) -type packet data protocol (PDP) contexts for a subscriber session.
- Setup and manage the data plane between the RAN and the GGSN providing high-speed data transfer with configurable GEA0-3 ciphering.

- Provide mobility management, location management, and session management for the duration of a call to ensure smooth handover.
- Provide various types of charging data records (CDRs) to attached accounting/billing storage mechanisms such as our SMC-based hard drive or a GTPP Storage Server (GSS) or a charging gateway function (CGF).
- Provide CALEA support for lawful intercepts.

The S4-SGSN is an SGSN configured with 2G and/or 3G services and then configured to interface with the 4G EPC network via the S4 interface. This enables the S4-SGSN to support handovers from UMTS/GPRS networks to the EPC network. The S4-SGSN works in conjunction with EPC network elements and gateways to:

- Interface with the EPC network S-GW (via the S4 interface) and MME (via the S3 interface) to enable handovers between 2G/3G networks and the EPC (4G) network.
- Interface with the Equipment Identity Registry via the S13' interface to perform the ME identity check.
- Interface with the HSS via the S6d interface to obtain subscription-related information.
- Communicate with S4-SGSNs via the S16 interface.
- Provide Idle Mode Signaling support for EPC-capable UEs.

This section catalogs many of the SGSN key components and features for data services within the GPRS/UMTS environment. Also, a range of SGSN operational and compliance information is summarized with pointers to other information sources.

Qualified Platforms

SGSN is a StarOS application that runs on Cisco® ASR 5500 and virtualized platforms. For additional platform information, refer to the appropriate *System Administration Guide* and/or contact your Cisco account representative.

Licenses

The SGSN is a licensed Cisco product and requires the purchase and installation of the SGSN Software License. Separate feature licenses may be required. Contact your Cisco account representative for detailed information on specific licensing requirements.

For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* section in the *System Administration Guide*.

Network Deployments and Interfaces

The following logical connection maps illustrate the SGSN's ability to connect to various radio access network types, core network types, and network components:

- GSM edge radio access network (GERAN) provides access to the 2.5G general packet radio service (GPRS) network
- UMTS terrestrial radio access network (UTRAN) provides access to the 3G universal mobile telecommunications system (UMTS) network
- Evolved UTRAN (E-UTRAN) provides access to the 4G mobile evolved packet core (EPC) of the long term evolution/system architecture evolution (LTE/SAE) network
- Another SGSN

- Standalone gateway GPRS support node (GGSN)
- Co-located P-GW/GGSN
- Mobile Service Center (MSC)
- Visitor Location Register (VLR)
- Home Location Register (HLR)
- Charging Gateway (CF - sometimes referred to as a charging gateway function (CGF))
- GTPP Storage Server (GSS)
- Equipment Identity Registry (EIR)
- Home Subscriber Server (HSS)
- Mobility Management Entity (MME)
- Serving Gateway (S-GW)
- CAMEL service's GSM service control function (gsmSCF)
- Short Message Service server Center (SMS-C)
- Network devices in another PLMN

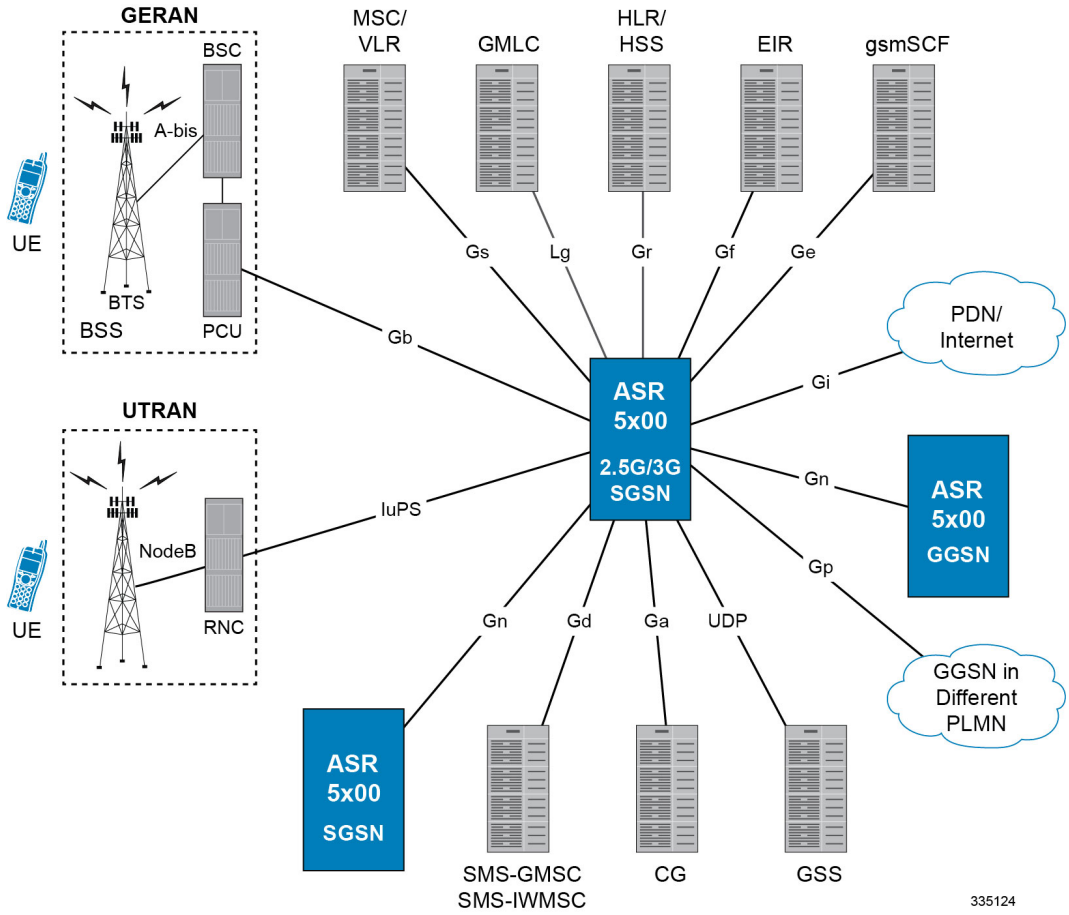
SGSN and Dual Access SGSN Deployments

SGSNs and GGSNs work in conjunction within the GPRS/UMTS network. As indicated earlier in the section on *System Configuration Options*, the flexible architecture of StarOS enables a single chassis to reduce hardware requirements by supporting integrated co-location of a variety of the SGSN services.

A chassis can be devoted solely to SGSN services or the SGSN system can include any co-location combination, such as multiple instances of 2.5G SGSNs (configured as GPRS services); or multiple instances of 3G SGSNs (configured as SGSN services); or a combination of 2.5G and 3G SGSN to comprise a dual access SGSN.

Important The following illustrates the GPRS/UMTS Dual Access architecture with a display of all the interfaces supported as of Release 14.0. The *SGSN Logical Network Interfaces* section below lists the interfaces available for the release applicable to the version of this manual.

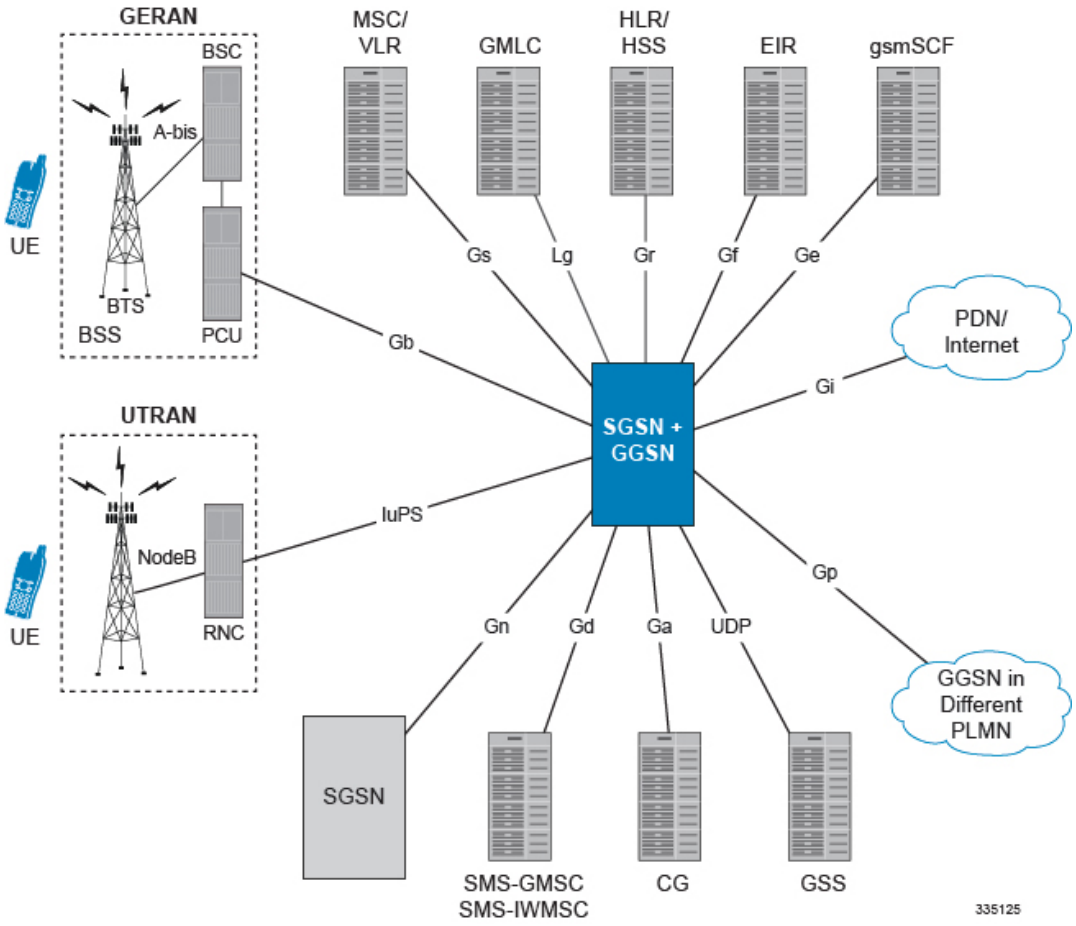
Figure 1: 2.5G and 3G Dual Access Architecture



SGSN/GGSN Deployments

The co-location of the SGSN and the GGSN in the same chassis facilitates handover. A variety of GSN combos is possible, 2.5G or 3G SGSN with the GGSN.

Figure 2: GSN Combo Architecture



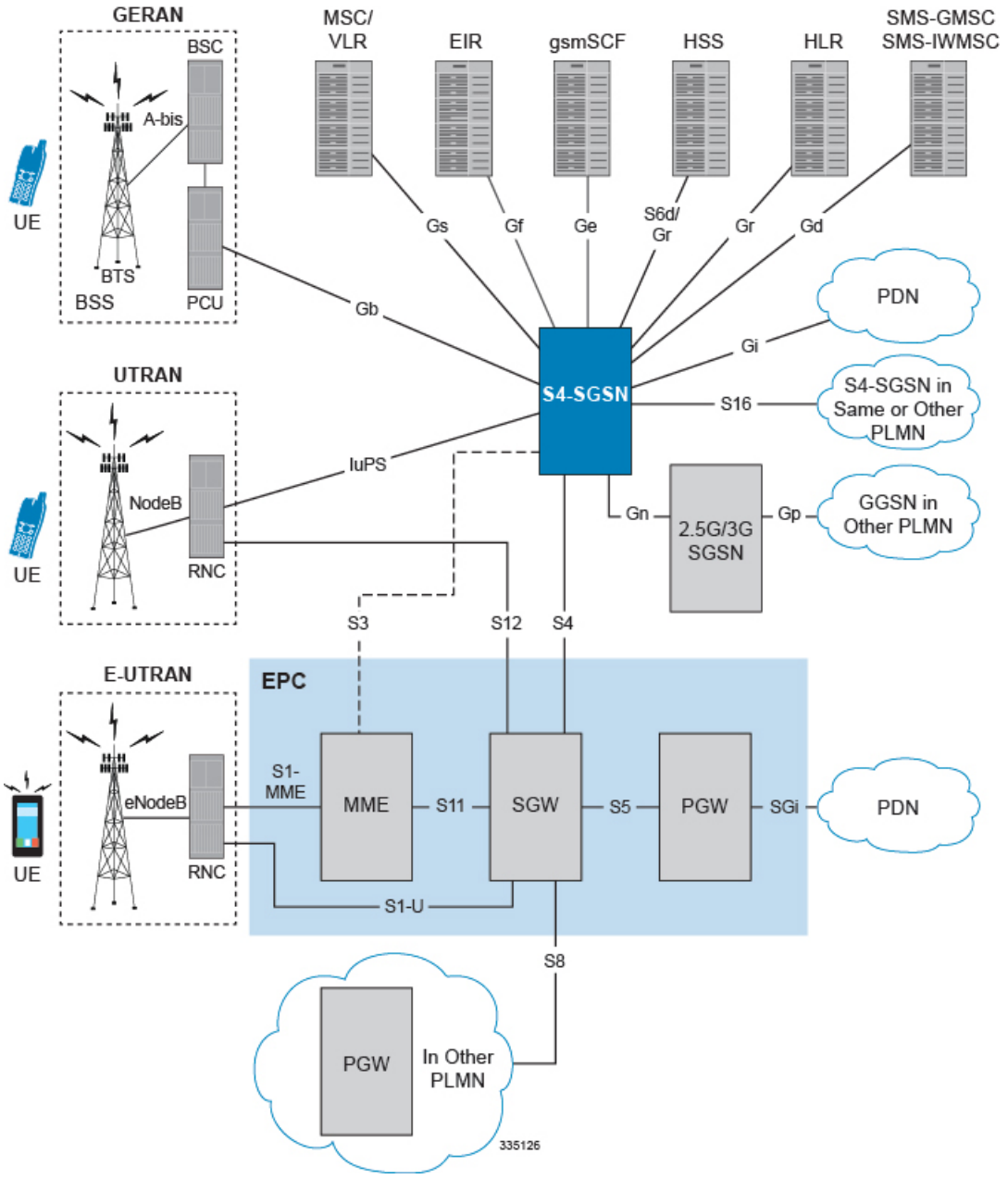
S4-SGSN Deployments

An S4-SGSN is an SGSN that is configured for S4 interface support to enable the soft handover of 2G and 3G subscribers to the EPC S-GW via the EPC S4 interface. Comprehensive S4-SGSN support includes interfaces to the following network elements and gateways:

- EPC serving gateway (S-GW) via the S4 interface
- Equipment identity registry (EIR) via the S13' interface
- Home subscriber server (HSS) via the S6d interface
- EPC mobility management entity (MME) via the S3 interface
- Peer S4-SGSN via the S16 interface

The S4, S13' and S6d interfaces are license-enabled features. Support for the S16 and S3 interfaces are included as part of the S4 license.

Figure 3: S4-SGSN Network Architecture



SGSN Logical Network Interfaces

The SGSN provides IP-based transport on all RAN and core network interfaces, in addition to the standard IP-based interfaces (Ga, Gn, Gp, Iu-PS). This means enhanced performance, future-proof scaling and reduction of inter-connectivity complexity. The all-IP functionality is key to facilitating evolution to the next generation technology requirements.

The SGSN provides the following functions over the logical network interfaces illustrated above:

- **Ga:** The SGSN uses the Ga interface with GPRS Transport Protocol Prime (GTPP) to communicate with the charging gateway (CG, also known as CGF) and/or the GTPP storage server (GSS). The interface transport layer is typically UDP over IP but can be configured as TCP over IP for:
  - One or more Ga interfaces per system context, and
  - An interface over Ethernet 10/100 or Ethernet 1000 interfaces

  The charging gateway handles buffering and pre-processing of billing records and the GSS provides storage for Charging Data Records (CDRs). For additional information regarding SGSN charging, refer to the Charging section.
- **IuPS:** The SGSN provides an IP over ATM (IP over AAL5 over ATM) interface between the SGSN and the RNCs in the 3G UMTS radio access network (UTRAN). RANAP is the control protocol that sets up the data plane (GTP-U) between these nodes. SIGTRAN (M3UA/SCTP) or QSAAL (MTP3B/QSAAL) handle IuPS-C (control) for the RNCs.

  Some of the procedures supported across this interface are:
  - Control plane based on M3UA/SCTP
  - Up to 128 Peer RNCs per virtual SGSN. Up to 256 peers per physical chassis
  - SCTP Multi-Homing supported to facilitate network resiliency
  - M3UA operates in and IPSP client/server and single/double-ended modes
  - Multiple load shared M3UA instances for high-performance and redundancy
  - Works over Ethernet and ATM (IPoA) interfaces
  - Facilitates SGSN Pooling
  - RAB (Radio Access Bearer) Assignment Request
  - RAB Release Request
  - Iu Release Procedure
  - SGSN-initiated Paging
  - Common ID
  - Security Mode Procedures
  - Initial MN Message
  - Direct Transfer
  - Reset Procedure
  - Error Indication
  - SRNS relocation
- **Gb:** This is the SGSN's interface to the base station system (BSS) in a 2G radio access network (RAN). It connects the SGSN via UDP/IP via an Ethernet interface. Gb-IP is the preferred interface as it improves control plane scaling as well as facilitates the deployment of SGSN Pools.

  Some of the procedures supported across this interface are:
  - BSS GSM at 900/1800/1900 MHz
  - BSS Edge
  - Frame Relay congestion handling
  - Traffic management per Frame Relay VC
  - NS load sharing
  - NS control procedures
  - BVC management procedures
  - Paging for circuit-switched services
  - Suspend/Resume

- Flow control
- Unacknowledged mode
- Acknowledged mode

- **Gn/Gp:** The Gn/Gp interfaces, comprised of GTP/UDP/IP-based protocol stacks, connect the SGSNs and GGSNs to other SGSNs and GGSNs within the same public land mobile network (PLMN) - the Gn - or to GGSNs in other PLMNs - the Gp.

  This implementation supports:

  - GTPv0 and GTPv1, with the capability to auto-negotiate the version to be used with any particular peer
  - GTP-C (control plane) and GTP-U (user plane)
  - One or more Gn/Gp interfaces configured per system context

  As well, the SGSN can support the following IEs from later version standards:

  - IMEI-SV
  - RAT TYPE
  - User Location Information
  - Extended PDP Type (Release 9)
  - Extended RNC ID (Release 9)

- **Ge:** This is the interface between the SGSN and the SCP that supports the CAMEL service. It supports both SS7 and SIGTRAN and uses the CAP protocol.
- **Gr:** This is the interface to the HLR. It supports SIGTRAN (M3UA/SCTP/IP) over Ethernet.

  Some of the procedures supported by the SGSN on this interface are:

  - Send Authentication Info
  - Update Location
  - Insert Subscriber Data
  - Delete Subscriber Data
  - Cancel Location
  - Purge
  - Reset
  - Ready for SM Notification
  - SIGTRAN based interfaces M3UA/SCTP
  - Peer connectivity can be through an intermediate SGP or directly depending on whether the peer (HLR, EIR, SMSC, GMLC) is SIGTRAN enabled or not
  - SCTP Multi-Homing supported to facilitate network resiliency
  - M3UA operates in IPSP client/server and single/double-ended modes
  - Multiple load shared M3UA instances for high-performance and redundancy
  - Works over Ethernet (IPoA) interface

- **Gs:** This is the interface used by the SGSN to communicate with the visitor location register (VLR) or mobile switching center (MSC) to support circuit switching (CS) paging initiated by the MSC. This interface uses Signaling Connection Control Part (SCCP) connectionless service and BSSAP+ application protocols.
- **Gd:** This is the interface between the SGSN and the SMS Gateway (SMS-GMSC / SMS-IWMSC) for both 2G and 3G technologies through multiple interface mediums. Implementation of the Gd interface requires purchase of an additional license.

- **Gf:** Interface is used by the SGSN to communicate with the equipment identity register (EIR) which keeps a listing of UE (specifically mobile phones) being monitored. The SGSN's Gf interface implementation supports functions such as:
  - International Mobile Equipment Identifier-Software Version (IMEI-SV) retrieval
  - IMEI-SV status confirmation
- **Lg:** This is a Mobile Application Part (MAP) interface, between the SGSN and the gateway mobile location center (GMLC), supports 3GPP standards-compliant LoCation Services (LCS) for both 2G and 3G technologies. Implementation of the Lg interface requires purchase of an additional license.
- **S3:**On the S4-SGSN, this interface provides a GTPv2-C signaling path connection between the EPC mobility management entity (MME) and the SGSN. This functionality is part of the S4 interface feature license.
- **S4:** On the S4-SGSN, this interface provides a data and signaling interface between the EPC S-GW and the S4-SGSN for bearer plane transport (GTPv1-U). The S4-SGSN communicates with the P-GW via the S-GW. A separate feature license is required for S4 interface support.
- **S6d:** On the SGSN, this is the S6d interface between the SGSN and the HSS. This enables the SGSN to get subscription details of a user from the HSS when a user tries to register with the SGSN. A separate feature license is required for S6d Diameter interface support.
- **S13':** The SGSN supports the S13' interface between the SGSN and the EIR. This enables the SGSN to communicate with an Equipment Identity Registry (EIR) via the Diameter protocol to perform the Mobile Equipment (ME) identity check procedure between the SGSN and EIR. Performing this procedure enables the SGSN to verify the equipment status of the Mobile Equipment. A separate feature license is required for S13' interface support.
- **S16:**On the S4-SGSN, this interface provides a GTPv2 path to a peer S4-SGSN. Support for this interface is provided as part of the S4 interface license.

SGSN Core Functionality

The SGSN core functionality is comprised of:

- All-IP Network (AIPN), on page 13
- SS7 Support
- PDP Context Support
- Mobility Management
- Location Management
- Session Management
- Charging

All-IP Network (AIPN)

AIPN provides enhanced performance, future-proof scaling and reduction of inter-connectivity complexity.

In accordance with 3GPP, the SGSN provides IP-based transport on all RAN and core network interfaces, in addition to the standard IP-based interfaces (Ga, Gn, Gp, Iu-Data). The all-IP functionality is key to facilitating Iu and Gb Flex (SGSN pooling) functionality as well as evolution to the next generation technology requirements.

The following IP-based protocols are supported on the SGSN:

- SCTP

- M3UA over SCTP
- GTPv0 over UDP
- GTPv1 over UDP
- GTPv2 over UDP (S4-SGSN only)
- GTP-U over UDP
- Diameter over TCP and SCTP (S4-SGSN only)

SS7 Support

StarOS SGSN implements SS7 functionality to communicate with the various SS7 network elements, such as HLRs and VLRs.

The SGSN employs standard Signaling System 7 (SS7) addressing (point codes) and global title translation. SS7 feature support includes:

- Transport layer support includes:
  - Broadband SS7 (MTP3B/SSCF/SSCOP/AAL5)
  - SIGTRAN (M3UA/SCTP/IP)
- SS7 variants supported:
  - ITU-T (International Telecommunication Union - Telecommunications - Europe)
  - ANSI (American National Standards Institute - U.S.)
  - B-ICI (B-ISDN Inter-Carrier Interface)
  - China
  - TTC (Telecommunication Technology Committee - Japan)
  - NTT (Japan)
- SS7 protocol stack components supported:
  - MTP2 (Message Transfer Part, Level 2)
  - MTP3 (Message Transfer Part, Level 3)
  - SCCP (Signaling Connection Control Part) with BSSAP+ (Base Station System Application Part Plus) and RANAP (Radio Access Network Application Part)
  - ISUP (ISDN User Part
  - TCAP (Transaction Capabilities Applications Part) and MAP (Mobile Application Part)

PDP Context Support

Support for subscriber primary and secondary Packet Data Protocol (PDP) contexts in compliance with 3GPP standards ensure complete end-to-end GPRS connectivity.

The SGSN supports a total of 11 PDP contexts per subscriber. Of the 11 PDP context, all can be primaries, or 1 primary and 10 secondaries or any combination of primary and secondary. Note that there must be at least one primary PDP context in order for secondaries to establish.

PDP context processing supports the following types and functions:

- Types: IPv4, IPv6, IPv4v6 (dual stack) and/or PPP
- GTPP accounting support
- PDP context timers

- Quality of Service (QoS)

Mobility Management

The SGSN supports mobility management (MM) in compliance with applicable 3GPP standards and procedures to deliver the full range of services to the mobile device. Some of the procedures are highlighted below:

GPRS Attach

The SGSN is designed to accommodate a very high rate of simultaneous attaches. The actual attach rate depends on the latencies introduced by the network and scaling of peers. In order to optimize the entire signaling chain, the SGSN eliminates or minimizes bottlenecks caused by large scale control signaling. For this purpose, the SGSN implements features such as an in-memory data-VLR and SuperCharger. Both IMSI and P-TMSI based attaches are supported.

The SGSN provides the following mechanisms to control MN attaches:

- **Attached Idle Timeout** - When enabled, if an MN has not attempted to setup a PDP context since attaching, this timer forces the MN to detach with a cause indicating that the MN need not re-attach. This timer is particularly useful for reducing the number of attached subscribers, especially those that automatically attach at power-on.
- **Detach Prohibit** - When enabled, this mechanism disables the Attached Idle Timeout functionality for selected MNs which aggressively re-attach when detached by the network.
- **Prohibit Reattach Timer** - When enabled, this timer mechanism prevents MNs, that were detached due to inactivity, from re-attaching for a configured period of time. Such MNs are remembered by the in-memory data-VLR until the record needs to be purged.
- **Attach Rate Throttle** - It is unlikely that the SGSN would become a bottleneck because of the SGSN's high signaling rates. However, other nodes in the network may not scale commensurately. To provide network overload protection, the SGSN provides a mechanism to control the number of attaches occurring through it on a per second basis.

Beside configuring the rate, it is possible to configure the action to be taken when the overload limit is reached. See the **network-overload-protection** command in the "Global Configuration Mode" section in the *Command Line Interface Reference*. Note, this is a soft control and the actual attach rate may not match exactly the configured value depending on the load conditions.

GPRS Detach

The SGSN is designed to accommodate a very high rate of simultaneous detaches. However, the actual detach rate is dependent on the latencies introduced by the network and scaling of peers. A GPRS detach results in the deactivation of all established PDP contexts.

There are a variety of detaches defined in the standards and the SGSN supports the following detaches:

- **MN Initiated Detach** - The MN requests to be detached.
- **SGSN Initiated Detach** - The SGSN requests the MN to detach due to expiry of a timer or due to administrative action.
- **HLR Initiated Detach** - The detach initiated by the receipt of a cancel location from the HLR.

Mass detaches triggered by administrative commands are paced in order to avoid flooding the network and peer nodes with control traffic.

Paging

CS-Paging is initiated by a peer node - such as the MSC - when there is data to be sent to an idle or unavailable UE. CS-paging requires the Gs interface. This type of paging is intended to trigger a service request from the UE. If necessary, the SGSN can use PS-Paging to notify the UE to switch channels. Once the UE reaches the connected state, the data is forwarded to it.

Paging frequency can be controlled by configuring a paging-timer.

Service Request

The Service Request procedure is used by the MN in the PMM Idle state to establish a secure connection to the SGSN as well as request resource reservation for active contexts.

The SGSN allows configuration of the following restrictions:

- Prohibition of services
- Enforce identity check
- PLMN restriction
- Roaming restrictions

Authentication

The SGSN authenticates the subscriber via the authentication procedure. This procedure is invoked on attaches, PDP activations, inter-SGSN routing Area Updates (RAUs), and optionally by configuration for periodic RAUs. The procedure requires the SGSN to retrieve authentication quintets/triplets from the HLR (AuC) and issuing an authentication and ciphering request to the MN. The SGSN implements an in-memory data-VLR functionality to pre-fetch and store authentication vectors from the HLR. This decreases latency of the control procedures.

Additional configuration at the SGSN allows for the following:

- Enforcing ciphering
- Retrieval of the IMEI-SV

P-TMSI Reallocation

The SGSN supports standard Packet-Temporary Mobile Identity (P-TMSI) Reallocation procedures to provide identity confidentiality for the subscriber.

The SGSN can be configured to allow or prohibit P-TMSI reallocation on the following events:

- Routing Area Updates
- Attaches
- Detaches
- Service Requests

The SGSN reallocates P-TMSI only when necessary.

P-TMSI Signature Reallocation

The SGSN supports operator definition of frequency and interval for Packet Temporary Mobile Subscriber Identity (P-TMSI) signature reallocation for all types of routing area update (RAU) events.

Identity Request

This procedure is used to retrieve IMSI and IMEI-SV from the MN. The SGSN executes this procedure only when the MN does not provide the IMSI and the MM context for the subscriber is not present in the SGSN's data-VLR.

Location Management

The SGSN's 3GPP compliance for location management ensures efficient call handling for mobile users.

The SGSN supports routing area updates (RAU) for location management. The SGSN implements standards based support for:

- Periodic RAUs
- Intra-SGSN RAUs
- Inter-SGSN RAUs.

The design of the SGSN allows for very high scalability of RAUs. In addition, the high capacity of the SGSN and Flex functionality provides a great opportunity to convert high impact Inter-SGSN RAUs to lower impact Intra-SGSN RAUs. The SGSN provides functionality to enforce the following RAU restrictions:

- Prohibition of GPRS services
- Enforce identity request
- Enforce IMEI check
- PLMN restriction
- Roaming restrictions

The SGSN also provides functionality to optionally supply the following information to the MN:

- P-TMSI Signature and Allocated P-TMSI
- List of received N-PDU numbers for loss less relocation
- Negotiated READY timer value
- Equivalent PLMNs
- PDP context status
- Network features supported

Session Management

Session management ensures proper PDP context setup and handling.

For session management, the SGSN supports four 3GPP-compliant procedures for processing PDP contexts:

- Activation
- Modification
- Deactivation
- Preservation

PDP Context Activation

The PDP context activation procedure establishes a PDP context with the required QoS from the MN to the GGSN. These can be either primary or secondary contexts. The SGSN supports a minimum of 1 PDP primary context per attached subscriber, and up to a maximum of 11 PDP contexts per attached subscriber.

The PDP context types supported are:

- PDP type IPv4
- PDP type IPv6
- PDP type IPv4v6
- PDP type PPP

Both dynamic and static addresses for the PDP contexts are supported.

The SGSN provides configuration to control the duration of active and inactive PDP contexts.

When activating a PDP context the SGSN can establish the GTP-U data plane from the RNC through the SGSN to the GGSN or directly between the RNC and the GGSN (one tunnel).

The SGSN is capable of interrogating the DNS infrastructure to resolve the specified APN to the appropriate GGSN. The SGSN also provides default and override configuration of QoS and APN.

PDP Context Modification

This procedure is used to update the MN and the GGSN. The SGSN is capable of initiating the context modification or negotiating a PDP context modification initiated by either the MN or the GGSN.

PDP Context Deactivation

This procedure is used to deactivate PDP contexts. The procedure can be initiated by the MN or the SGSN. The SGSN provides configurable timers to initiate PDP deactivation of idle contexts as well as active contexts.

PDP Context Preservation

The SGSN provides this functionality to facilitate efficient radio resource utilization. This functionality comes into play on the following triggers:

- **RAB (Radio Access Bearer) Release Request**

  This is issued by the RAN to request the release of RABs associated with specific PDP contexts. The SGSN responds with a RAB assignment request, waits for the RAB assignment response and marks the RAB as having been released. The retention of the PDP contexts is controlled by configuration at the SGSN. If the PDP contexts are retained the SGSN is capable of receiving downlink packets on them.

- **Iu Release Request**

  The RAN issues an Iu release request to release all RABs of an MN and the Iu connection. The retention of the PDP contexts is controlled by configuration at the SGSN. When PDP contexts are retained the SGSN is capable of receiving downlink packets on them.

  When PDP contexts are preserved, the RABs can be restored on a service request from the MN without having to go through the PDP context establishment process again. The service request is issued by the MN either when it has some data to send or in response to a paging request, on downlink data, from the SGSN.

Charging

Charging functionality for the SGSN varies depending upon the type of network in which it is deployed.

SGSN in GPRS/UMTS Network

The SGSN provides an efficient and accurate billing system for all calls and SMSs passing through the SGSN. The charging-specific interfaces and 3GPP standards supported by the SGSN deployments are listed below:

- Allows the configuration of multiple CGFs and a single GSS in a single GTPP group along with their relative priorities.
- Implements the standardized Ga interface.
- Fully supports the GPRS Tunneling Protocol Prime (GTPP) over UDP/TCP.
- Supports the relevant charging information as defined in:
  - **3GPP TS 29.060 v7.9.0 (2008-09):** Technical Specification; 3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 6)
  - **3GPP TS 32.215 v5.9.0 (2005-06):** 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging data description for the Packet Switched (PS) domain (Release 4)
  - **3GPP TS.32.251 V8.8.0 (2009-12):** 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Packet Switched (PS) domain charging (Release 8)
  - **3GPP TS 32.298 V8.7.0 (2009-12):** 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description (Release 8)

Charging Data Records (CDRs)

The SGSN generates CDRs with the charging information. The following sections outline the types of CDRs generated by the SGSN.

For full dictionary, CDR and field information, refer to the *GTPP Accounting Overview*, the *SGSN and Mobility Management Charging Detail Record Field Reference Tables*, and the *S-CDR Field Descriptions* sections in the *AAA and GTPP Interface Administration and Reference*

SGSN Call Detail Records (S-CDRs)

These charging records are generated for PDP contexts established by the SGSN. They contain attributes as defined in TS 32.251 v7.2.0.

Mobility Call Detail Records (M-CDRs)

These charging records are generated by the SGSN's mobility management (MM) component and correspond to the mobility states. They contain attributes as defined in 3GPP TS 32.251 v7.2.0.

Short Message Service CDRs

SGSN supports following CDRs for SMS related charging:

- SMS-Mobile Originated CDRs (SMS-MO-CDRs)
- SMS Mobile Terminated CDRs (SMS-MT-CDRs)

These charging records are generated by the SGSN's Short Message Service component. They contain attributes as defined in 3GPP TS 32.215 v5.9.0.

Location Request CDRs

SGSN supports the following Location Request CDRs:

- Mobile terminated location request CDRs (LCS-MT-CDRs)
- Mobile originated location request CDRs (LCS-MO-CDRs)

SGSN in LTE/SAE Network

Beginning in release 14.0, an SGSN can function in an LTE/SAE network using enhancements to support various other interfaces including an S4 interface. In these cases, the SGSN is referred to as an S4-SGSN.

Serving Gateway Call Detail Records (S-GW-CDRs)

The S4-SGSN does not support S-CDRs because the S4 interface is used, per PDP (or EPS bearer) and charging records are generated by the S-GW using the S-GW-CDR. The S-GW collects the charging information per user per IP-CAN bearer. The collected information is called as S-GW-CDR and sent to the Charging Gateway over the Gz interface.

Features and Functionality

It is impossible to list all of the features supported by the Gn/Gp SGSN (2.5G and 3G) or the S4-SGSN.

Those features listed below are only a few of the features that enable the operator to control the SGSN and their network. All of these features are either proprietary or comply with relevant 3GPP specifications.

Some of the proprietary features may require a separate license. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* section in the *System Administration Guide*.

3G-2G Location Change Reporting

With Location Change Reporting enabled, the SGSN facilitates location-based charging on the GGSN by providing the UE's geographical location information when the UE is in connected mode.

Location-based charging is a values-added function that ensures subscribers pay a premium for location-based services, such as service in a congested areas. With the required feature license installed, the operator uses the CLI to enable the reporting independently for each network access type: GPRS (2G) or UMTS (3G).

For more information about how the feature works and how to configure it, refer to the *3G-2G Location Change Reporting* feature section.

Important The "Location reporting in connected mode" license is required to enable this functionality.

Access Restriction Support on S6d Interface

The SGSN supports the below parameters added in the Update Location Request/Answer and Insert Subscriber Data Request/Answer messages on S6d interface:

- SGSN advertises the DCNR feature support by setting the 'NR as Secondary RAT feature bit' in Supported Features list 2 towards HSS if the DCNR feature is configured at SGSN and UE advertises DCNR capability in NAS
- SGSN also handles the new bit 'NR as Secondary RAT Not Allowed' in the Access-Restriction-Data bitmask sent by HSS to control if the subscriber is allowed to access NR via dual connectivity
- SGSN handles the Extended Bandwidth UL/DL parameters under AMBR sent by HSS

Gateway selection is improved to avoid SGSN from falling back and triggering an "A" query to get the normal GGSN information.

When no collocated PGW/GGSN with "+nc-nr" capability is found in DNS response, the SGSN will select the next collocated PGW/GGSN node. If “3gpp-pgw:x-gn+nc-nr/ x-3gpp-pgw:x-gp+nc-nr” is not present in DNS response, the SGSN will select “3gpp-pgw:x-gn / x-3gpp-pgw:x-gp” instead of triggering another to "A" query to get the GGSN information. "UP Function Selection Indication Flags" IE in Create PDP Context Request message will be set to "1" only when “+nc-nr” capable gateway is selected.

Accounting Path Framework, New for 14.0

As of Release 14.0, the SGSN uses a new accounting path framework to support PSC3 numbers of 8 million attached subs and 16 million PDP contexts. In the old accounting path framework, there was one AAA session per sub-session in the Session manager and one archive session per sub-session in AAA manager. As part of the new accounting path framework there is only one AAA session per call in the Session manager and one archive session per call in the AAA manager. Also, there is an additional accounting session in the Session manager and the AAA manager per sub-session. The new accounting path framework improves memory and CPU utilization and prevents tariff or time limit delay. There are no changes in the CLI syntax to support the new accounting path and the existing accounting behavior of SGSN is not modified.

AAA Changes To Support Location Services (LCS) Feature

The Location Services (LCS) feature in SGSN provides the mechanism to support mobile location services for operators, subscribers and third party service providers. AAA changes have been made to support the LCS feature. A new CDR type Mobile Originated Location Request CDRs (LCS-MO-CDR) is introduced. LCS-MO-CDRs support the standard dictionaries.

For detailed information on LCS-MO-CDRs, refer to the *GTPP Interface Administration and Reference*.

APN Aliasing

In many situations, the APN provided in the Activation Request is unacceptable perhaps it does not match with any of the subscribed APNs or it is misspelled and would result in the SGSN rejecting the Activation Request. The APN Aliasing feature enables the operator to override an incoming APN specified by a subscriber or provided during the APN selection procedure (TS 23.060) or replace a missing APN with an operator-preferred APN.

The APN Aliasing feature provides a set of override functions: Default APN, Blank APN, APN Remapping, and Wildcard APN to facilitate such actions as:

- overriding a mismatched APN with a default APN.
- overriding a missing APN (blank APN) with a default or preferred APN.
- overriding an APN on the basis of charging characteristics.

- overriding an APN by replacing part or all of the network or operator identifier with information defined by the operator, for example, MNC123.MCC456.GPRS could be replaced by MNC222.MCC333.GPRS.
- overriding an APN for specific subscribers (based on IMSI) or for specific devices (based on IMEI).

Default APN

Operators can configure a "default APN" for subscribers not provisioned in the HLR. The default APN feature will be used in error situations when the SGSN cannot select a valid APN via the normal APN selection process. Within an APN remap table, a default APN can be configured for the SGSN to:

- override a requested APN when the HLR does not have the requested APN in the subscription profile.
- provide a viable APN if APN selection fails because there was no "requested APN" and wildcard subscription was not an option.

In either of these instances, the SGSN can provide the default APN as an alternate behavior to ensure that PDP context activation is successful.

Recently, the SGSN's default APN functionality was enhanced so that if a required subscription APN is not present in the subscriber profile, then the SGSN will now continue the activation with another configured 'dummy' APN. The call will be redirected, via the GGSN, to a webpage informing the user of the error and prompting to subscribe for services.

Refer to the *APN Remap Table Configuration Mode* in the *Command Line Interface Reference* for the command to configure this feature.

APN Redirection per APN with Lowest Context-ID

The APN Redirection per APN with Lowest Context-ID feature adds the flexibility to select the subscription APN with the least context ID when the APN is not found in the subscription. SGSN already provides sophisticated APN replacement with support for first-in-subscription, default APN, blank APN, and wildcard APN. This latest feature works along similar lines providing further flexibility to the operator in allowing activations when the MS requested APN is incorrect, misspelled, or not present in the subscription.

The SGSN's APN selection procedure is based on 3GPP 23.060 Annex A, which this feature extends based on CLI controls under the APN Remap Table configuration mode.

APN Resolution with SCHAR or RNC-ID

It is now possible to append charging characteristic information to the DNS string. The SGSN includes the profile index value portion of the CC as binary/decimal/hexadecimal digits (type based on the configuration) after the APN network identification. The charging characteristic value is taken from the subscription record selected for the subscriber during APN selection. This enables the SGSN to select a GGSN based on the charging characteristics information.

After appending the charging characteristic the DNS string will take the following form: <apn_network_id>.<profile_index>.<apn_operator_id >. The profile index in the following example has a value 10: quicknet.com.uk.1010.mnc234.mcc027.gprs.

If the RNC_ID information is configured to be a part of the APN name, and if inclusion of the profile index of the charging characteristics information is enabled before the DNS query is sent, then the profile index is included after the included RNC_ID and the DNS APN name will appear in the following form: <apn_network_id>.<rnc_id>.<profile_index>.<apn_operator_id>. In the following example, the DNS query

for a subscriber using RNC 0321 with the profile index of value 8 would appear as: quicknet.com.uk.0321.1000.mnc234.mcc027.gprs.

APN Restriction

The reception, storage, and transfer of APN Restriction values is used to determine whether a UE is allowed to establish PDP Context or EPS bearers with other APNs. This feature is supported by both the Gn/Gp-SGSN and the S4-SGSN.

During default bearer activation, the SGSN sends the current maximum APN restriction value for the UE to the GGSN/P-GW in a Create Session Request (CSR). The GGSN/P-GW retains an APN restriction value for each APN. The UE's APN Restriction value determines the type of application data the subscriber is allowed to send. If the maximum APN restriction of the UE (received in the CSR) and the APN Restriction value of the APN (for which activation is being request) do not concur, then the GGSN/P-GW rejects activation. The maximum APN restriction for a UE is the most restrictive based on all already active default EPS bearers.

This feature provides the operator with increased control to restrict certain APNs to UEs based on the type of APN. This feature requires no special license.

APN Restriction for SGSN is enabled/disabled in the **call-control-profile** configuration mode using the **apn-restriction** command. Refer to the *Command Line Interface Reference* for usage details.

Automatic Protection Switching (APS)

Automatic protection switching (APS is now available on an inter-card basis for SONET configured CLC2 (Frame Relay) and OLC2 (ATM) optical line cards. Multiple switching protection (MSP) version of is also available for SDH configured for the CLC2 and OLC2 (ATM) line cards.

APS/MSP offers superior redundancy for SONET/SDH equipment and supports recovery from card failures and fiber cuts. APS allows an operator to configure a pair of SONET/SDH lines for line redundancy. In the event of a line problem, the active line switches automatically to the standby line within 60 milliseconds (10 millisecond initiation and 50 millisecond switchover).

At this time, the Gn/Gp-SGSN supports the following APS/MSP parameters:

- 1+1 - Each redundant line pair consists of a working line and a protection line.
- uni-directional - Protection on one end of the connection.
- non-revertive - Upon restoration of service, this parameter prevents the network from automatically reverting to the original working line.

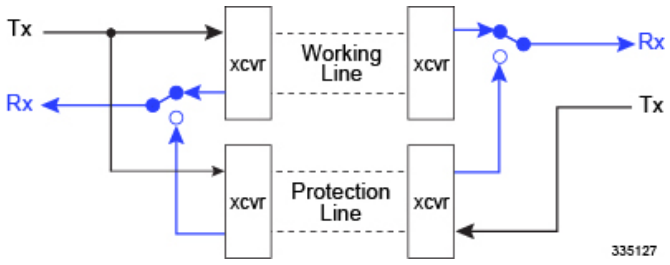
The protection mechanism used for the APS/MSP uses a linear 1+1 architecture, as described in the ITU-T G.841 standard and the Bellcore publication GR-253-CORE, SONET Transport Systems; Common Generic Criteria, Section 5.3. The connection is unidirectional.

With APS/MSP 1+1, each redundant line pair consists of a working line and a protection line. Once a signal fail condition or a signal degrade condition is detected, the hardware switches from the working line to the protection line.

With the non-revertive option, if a signal fail condition is detected, the hardware switches to the protection line and does not automatically revert back to the working line.

Since traffic is carried simultaneously by the working and protection lines, the receiver that terminates the APS/MSP 1+1 must select cells from either line and continue to forward one consistent traffic stream. The receiving ends can switch from working to protection line without coordinating at the transmit end since both lines transmit the same information.

Figure 4: SONET APS 1+1



Refer to the section on *Configuring APS/MSP Redundancy* in the *SGSN Service Configuration Procedures* section for configuration details.

Authentications and Reallocations -- Selective

Subscriber event authentication, P-TMSI reallocation, and P-TMSI signature reallocation are now selective rather than enabled by default.

The operator can enable and configure them to occur according to network requirements:

- every instance or every nth instance;
- on the basis of UMTS, GPRS or both;
- on the basis of elapsed time intervals between events.

There are situations in which authentication will be performed unconditionally:

- IMSI Attach all IMSI attaches will be authenticated
- When the subscriber has not been authenticated before and the SGSN does not have a vector
- When there is a P-TMSI signature mismatch
- When there is a CKSN mismatch

There are situation in which P-TMSI will be reallocated unconditionally:

- Inter SGSN Attach/RAU
- Inter-RAT Attach/RAU in 2G
- IMSI Attach

Avoiding PDP Context Deactivations

The SGSN can be configured to avoid increased network traffic resulting from bursts of service deactivations/activations resulting from erroneous restart counter change values in received messages (Create PDP Context Response or Update PDP Context Response or Update PDP Context Request). Be default, the SGSN has the responsibility to verify possible GTP-C path failure by issuing an Echo Request/Echo Response to the GGSN. Path failure will only be confirmed if the Echo Response contains a new restart counter value. Only after this confirmation of the path failure does the SGSN begin deactivation of PDP contexts.

Backup and Recovery of Key KPI Statistics

This feature allows the backup of a small set of KPI counters for recovery of the counter values after a session manager crash.

Using the feature-specific CLI **statistics-backup sgsn backup-interval** command, in the Global configuration mode, the operator can enable the feature and define the frequency of the backup; range 1-60 minutes.

In support of this functionality, four schemas (gprs-bk, iups-bk, map-bk, sgtp-bk) have been defined with stats, derived from the SGSN and SGTP schemas, that will be backed up for recovery of their counter values.

For more information about the schema, refer to the *Statistics and Counters Reference*. For more information about this functionality and configuration for this feature, refer to the *Backup and Recovery of Key KPI Statistics* feature chapter in this Guide.

Bulk Statistics Support

System support for bulk statistics allows operators to choose which statistics to view and to configure the format in which the statistics are presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

When used in conjunction with the Web Element Manager, the data can be parsed, archived, and graphed.

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema. The following is the list of schemas supported for use by the SGSN:

- **System**: Provides system-level statistics
- **Card**: Provides card-level statistics
- **Port**: Provides port-level statistics
- **DLCI-Util**: Provides statistics specific to DLCIs utilization for CLC-type line cards
- **EGTPC**: Provides statistics specific to the configured ETPC service on the S4-SGSN
- **GPRS**: Provides statistics for LLC, BSSGP, SNDCP, and NS layers
- **SCCP**: Provides SCCP network layer statistics
- **SGTP**: Provides SGSN-specific GPRS Tunneling Protocol (GTP) statistics
- **SGSN**: Provides statistics for: mobility management (MM) and session management (SM) procedures; as well, MAP, TCAP, and SMS counters are captured in this schema. SGSN Schema statistic availability is per service (one of: SGSN, GPRS, MAP) and per routing area (RA)
- **SS7Link**: Provides SS7 link and linkset statistics
- **SS7RD**: Provides statistics specific to the proprietary SS7 routing domains

The following four schema are used by the SGSN for backed up / recovered counters (for details, see the *Backup and Recovery of Key KPI Statistics* section in this guide) :

- **iups-bk**
- **gprs-bk**
- **map-bk**
- **sgtp-bk**

The system supports the configuration of up to 4 sets (primary/secondary) of receivers. Each set can be configured with to collect specific sets of statistics from the various schemas. Statistics can be pulled manually from the chassis or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

The format of the bulk statistic data files can be configured by the user. Users can specify the format of the file name, file headers, and/or footers to include information such as the date, chassis host name, chassis uptime, the IP address of the system generating the statistics (available for only for headers and footers), and/or the time that the file was generated.

When the Web Element Manager is used as the receiver, it is capable of further processing the statistics data through XML parsing, archiving, and graphing.

The Bulk Statistics Server component of the Web Element Manager parses collected statistics and stores the information in the PostgreSQL database. If XML file generation and transfer is required, this element generates the XML output and can send it to a Northbound NMS or an alternate bulk statistics server for further processing.

Additionally, if archiving of the collected statistics is desired, the Bulk Statistics server writes the files to an alternative directory on the server. A specific directory can be configured by the administrative user or the default directory can be used. Regardless, the directory can be on a local file system or on an NFS-mounted file system on the Web Element Manager server.

Bypassing APN Remap for Specific IMEI Ranges

Prior to Release 16, if a local default APN configured in an IMEI profile could not be used, then any default APN configured under an operator policy was used. Also, only the **apn-selection-default** CLI option, under the APN Remap Table configuration associated with an IMEI profile, was valid. Other CLI options such as **apn-remap** and **blank-apn** were not applicable when a remap table was associated with an IMEI profile.

With Release 16, an APN Remap Table associated with an IMEI profile overrides a remap table associated with an operator policy. This means activation will be rejected if a local default APN configured, in an APN Remap Table associated with an IMEI profile, cannot be used. This will occur even if a valid local default APN is available in an APN Remap Table associated with an operator policy.

Important To achieve the previous default behavior, customers already using an APN Remap Table that is associated with an IMEI profile *will have to change the existing configuration* to achieve the previous behavior. For details and sample configurations, see the Release 16 specific information for **apn-selection-default** in the *APN Remap Table Configuration Mode Commands* section of the *Command Line Interface Reference* for a Release 16 or higher.

CAMEL Service Phase 3, Ge Interface

The SGSN provides PDP session support as defined by Customized Applications for Mobile network Enhanced Logic (CAMEL) phase 3.

CAMEL Service

CAMEL service enables operators of 2.5G/3G networks to provide operator-specific services (such as prepaid GPRS service and prepaid SMS service) to subscribers, even when the subscribers are roaming outside their HPLMN.

CAMEL Support

SGSN support for CAMEL phase 3 services expands with each SGSN application release. Current support enables operators of 2.5G/3G networks to provide operator-specific services (such as prepaid GPRS service and prepaid SMS service) to subscribers, even when the subscribers are roaming outside their HPLMN.

For this release the SGSN has expanded its support for CAMEL Scenario 1 adding:

- Implementation of Scenario1 triggers (TDP-Attach, TDP-Attach-ChangeofPosition)

- Implementation of Scenario1 Dynamic triggers (DP-Detach, DP-ChangeofPosition)
- Expanded conformance to 3GPP spec 23.078 (Release 4)

The SGSN supports the following GPRS-related functionality in CAMEL phase 3:

- Control of GPRS PDP contexts

Functional support for CAMEL interaction includes:

- PDP Context procedures per 3GPP TS 29.002
  - GPRS TDP (trigger detection point) functions
  - Default handling codes, if no response received from SCP
  - GPRS EDP (event detection points) associated with SCP
  - Charging Procedures: Handle Apply Charging GPRS & Handle Apply Charging Report GPRS
- "GPRS Dialogue scenario 2" for CAMEL control with SCP
- CAMEL-related data items in an S-CDR:
  - SCF Address
  - Service Key
  - Default Transaction Handling
  - Level of CAMEL service (phase 3)
- Session Recovery for all calls have an ESTABLISHED CAMEL association.

Ge Interface

The SGSN's implementation of CAMEL uses standard CAP protocol over a Ge interface between the SGSN and the SCP. This interface can be deployed over SS7 or SIGTRAN.

The SGSN's Ge support includes use of the gprsSSF CAMEL component with the SGSN and the gsmSCF component with the SCP.

CAMEL Configuration

To provide the CAMEL interface on the SGSN, a new service configuration mode, called "CAMEL Service", has been introduced on the SGSN.

1. An SCCP Network configuration must be created or exist already.
2. A CAMEL Service instance must be created.
3. The CAMEL Service instance must be associated with either the SGSN Service configuration or the GPRS Service configuration in order to enable use of the CAMEL interface.
4. The CAMEL Service must be associated with the SCCP Network configuration.

Until a CAMEL Service is properly configured, the SGSN will not process any TDP for pdp-context or mo-sms.

For configuration details, refer to the *Serving GPRS Support Node Administration Guide* and the *Command Line Interface Reference.*

Commandguard

Operators can accidentally enter configuration mode via CLI or file replay. To protect against this, SGSN supports **commandguard** CLI command. Commandguard, which is disabled by default, can only be enabled

or disabled from the Global Configuration mode. When Commandguard is enabled it affects the **configure** and **autoconfirm** CLI commands by causing them to prompt (Y/N) for confirmation. When **autoconfirm** is enabled Commandguard has no affect. The commandguard state is preserved in the SCT and, when enabled, is output by the various variants of the **show config** CLI.

Configurable RAB Asymmetry Indicator in RAB Assignment Request

The SGSN sets the value for the RAB Asymmetry Indicator that is included in the RAB Assignment Request.

In releases prior to R12.0, the SGSN set the RAB asymmetry indicator to "Symmetric-Bidirectional" when downlink and uplink bit rates were equal. Now, the SGSN selects the value based on the symmetry of negotiated maximum bit rates as follows:

- If the uplink and downlink bit rates are equal then it is set to "Symmetric-Bidirectional",
- If uplink bit rate is set to 0 kbps, then it is set to "Asymmetric-Unidirectional-Downlink",
- If downlink bit rate is set to 0 kbps, then it is set to "Asymmetric-Unidirectional-Uplink",
- If the uplink and downlink bit rates are non-zero and different, then it is set to "Asymmetric-Bidirectional".

A change in CLI configuration allows the SGSN to override the above functionality and set the RAB Asymmetry Indicator to "Asymmetric-Bidirectional" when uplink and downlink bit rates are equal. As a result, two sets of bit rates - one for downlink and one for uplink - will be included in the RAB Assignment Requests as mandated in 3GPP TS 25.413.

Congestion Control

With Release 17, the SGSN supports several of the 3GPP TS23.060 R10 machine type communications (MTC) overload control mechanisms to be used in the handling of signaling bursts from machine-to-machine (M2M) devices:

- General congestion control applicable only for Mobility Management messages.
- APN-based congestion control for Mobility Management
- APN-based congestion control for Session Management
- Extended T3312 timer support
- MM (Mobility Management) T3346 - MM Back-off Timer and SM (Session Management) T3396 - SM Back-off Timer

For more information about the congestion control functionality and configuration, refer to the *MTC Congestion Control* section in this Guide.

Different NRIs for Pooled and Non-pooled RNCs/BSCs

The SGSN adds support for configuring different NRIs for pooled and non-pooled areas in order to load-balance subscribers coming from non-pooled RNCs to pooled RNCs.

Consider a scenario when two SGSNs support pooling and a RNC/BSC controlled by a SGSN is in pool but not the other, and both RNCs/BSCs are given same NRI(s), this leads to imbalance in subscriber distribution between the SGSNs. With this enhancement if an NRI is configured for both pooled and non-pooled, then the SGSN reuses the same NRI when moving from pooled to non-pooled areas and vice versa.

A new keyword **non-pooled-nri-value** is introduced in the NRI configuration for GPRS and SGSN services to configure set of NRI which should be used for non-pooled RNCs/BSCs. The NRIs configured under the existing keyword **nri-value** will be used for pooled RNCs/BSCs. If the new keyword **non-pooled-nri-value**

is not configured, then NRIs configured under the keyword **nri-value** will be used for both pooled and non-pooled RNCs/BSCs.

If the new keyword **non-pooled-nri-value** is configured without pooling enabled at SGSN(null-nri-value is not configured), then SGSN will use NRIs under **non-pooled-nri-value** irrespective of BSC/RNCs being pooled or non-pooled, till pooling is enabled at SGSN. After pooling is enabled, NRIs under keyword **nri-value** will be for pooled RNC/BSCs and **non-pooled-nri-value** will be for non-pooled RNC/BSCs. This is applicable for both SGSN and GPRS service.

Direct Tunnel

In accordance with standards, one tunnel functionality enables the SGSN to establish a direct tunnel at the user plane level - a GTP-U tunnel, directly between the RAN and the GGSN. Feature details and configuration procedures are provided in the *Direct Tunnel* feature section in this guide.

Direct Tunnel Support on the S4-SGSN

Direct tunnelling of user plane data between the RNC and the S-GW can be employed to scale UMTS system architecture to support higher traffic rates. The direct tunnel (DT) approach optimizes core architecture without impact to UEs and can be deployed independently of the LTE/SAE architecture.

Now, DT support is added to the S4-SGSN to enable the establishment of a direct tunnel over the S12 interface between an RNC and an S-GW in a PS domain under a range of scenarios, such as (but not limited to):

- Primary PDP activation
- Secondary PDP activation
- Service Request Procedure
- Intra SGSN Routing Area Update without SGW change
- Intra SGSN Routing Area Update with SGW change
- Intra SGSN SRNS relocation without SGW change
- Intra SGSN SRNS relocation with SGW change
- New SGSN SRNS relocation with SGW change
- New SGSN SRNS relocation without SGW relocation
- E-UTRAN to UTRAN Iu mode IRAT handover - with application of S12U FTEID for Indirect Data Forwarding Tunnels as well
- UTRAN to E-UTRAN Iu mode IRAT handover - with application of S12U FTEID for Indirect Data Forwarding Tunnels as well
- Network-Initiated PDP Activation

The Direct Tunnel Support on the S4-SGSN feature is license controlled. Contact your Cisco Account or Support representative for information on how to obtain a license.

For a complete description of this feature and its configuration requirements, refer to the *S4-SGSN Direct Tunnel Solution* session in the *Serving GPRS Support Node Administration Guide.*

Downlink Data Lockout Timer

The Downlink Data Lockout Timer is a new, configurable timer added for both GPRS and SGSN services to reduce the frequency of mobile-initiated keep alive messages. If enabled, this timer starts whenever the paging procedure fails after the maximum number of retransmissions and the Page Proceed Flag (PPF) is cleared. If there is any downlink activity when the lockout timer is running, the packets are dropped and the drop cause

is set as Page Failed. When the lockout timer expires, the PPF is set to true and further downlink packets are queued and paging is re-initiated. In order to avoid endless paging activity when there is no page response or uplink activity from the UE, an optional configurable *repeat* count value is used. If the repeat value is configured as 'y' then the lockout timer is started 'y' number of times after page failure. The implementation of the lockout timer is different for 2G/3G subscribers, but the behavior is the same.

DSCP Templates for Control and Data Packets - Iu or Gb over IP

The SGSN supports a mechanism for differentiated services code point (DSCP) marking of control packets and signaling messages for the SGSN's M3UA level on the Iu interface and for LLC messages for the Gb interface.

This DSCP marking feature enables the SGSN to perform classifying and managing of network traffic and to determine quality of service (QoS) for the interfaces to an IP network.

Implementation of this feature requires the use of several CLIs commands to create one or more reusable templates. These templates set DSCP parameter configuration for downlink control packets and data packets that can be associated with one or more configurations for at the GPRS service level, the peer-NSEI level, the IuPS service level, and the PSP instance level.

Dual PDP Addresses for Gn/Gp

In accordance with 3GPP Release 9.0 specifications, it is now possible to configure SGSN support for dual stack PDP type addressing (IPv4v6) for PDP context association with one IPv4 address and one IPv6 address/prefix when requested by the MS/UE.

ECMP over ATM

Iu Redundancy is the implementation of equal-cost multi-path routing (ECMP) over ATM.

Iu Redundancy is based on the standard ECMP multi-path principle of providing multiple next-hop-routes of equal cost to a single destination for packet transmission. ECMP works with most routing protocols and can provide increased bandwidth when traffic load-balancing is implemented over multiple paths.

ECMP over ATM will create an ATM ECMP group when multiple routes with different destination ATM interfaces are defined for the same destination IP address. When transmitting a packet with ECMP, the NPU performs a hash on the packet header being transmitted and uses the result of the hash to index into a table of next hops. The NPU looks up the ARP index in the ARP table (the ARP table contains the next-hop and egress interfaces) to determine the next-hop and interface for sending packets.

EDR Enhancements

A new event-logging handle has been introduced. In earlier releases the EDR module was used for event logging purpose, from this release onwards CDR_MODULE_EVENT_RECORD is used instead of CDR_MODULE_EDR. In Release 12.0, for generating event logs the SGSN re-used the existing 'EDR" module which is primarily used for charging records. But from Release 15.0 onwards, the session-event module will be used by SGSN for event logging. The CLI options present under the EDR Module are also present under the Session Event Module.

In Release 21.3, the following EDR enhancements are implemented:

- New fields for Activation EDR:

A new field - NSAPI, is added as a part of the Activation EDR. The location of this field is added at the end of the Activation EDR.

- New fields for ISRAU EDR:

  A new field - PDN-Info, which consists of nsapi, ggsn-address, ipv4-pdp-address, ipv6-pdp-address, is added as a part of the ISRAU EDR and the location of this field is added at the end of the ISRAU EDR.

  The PDN-Info field is optional and will be sent only if there are PDP contexts handled by the SGSN.

- EDR for Service Request parameter:

  An EDR is now generated for a Service Request parameter. This EDR has the following fields listed in order:

  - 1: Time-Stamp
  - 2: Event-ID
  - 3: Event-Result
  - 4: RAT
  - 5: Service-Request-Trigger
  - 6: Service-Type
  - 7: Paging-Attempts
  - 8: Request-Retries
  - Cause-Prot-Types
  - Cause-Code
  - Disconnect Reason
  - Location (MCC+MNC+LAC+RAC+SAC)
  - Subscriber's MSISDN, IMSI, PTMSI, IMEISV, HLR's MSISDN

EIR Selection for Roaming Subscribers

EIR selelction for roaming subscribers functionality makes it possible for the SGSN to select an EIR based on the PLMN into which the subscriber has roamed and reduce signalling back to home PLMNs for roamers.

The Equipment Identity Register (EIR), used for authentication and authorization during an Attach, is the carrier's IMEI(SV) database of the unique numbers allocated to each subscriber's mobile station equipment (IMEI) and the manufacturer's software version (SV). An IMEI(SV) can be in one of three lists in the EIR:

- white list - the subscriber equipment is permitted access
- black list - the subscriber equipment is not permitted access
- grey list - the subscriber equipment is being tracked for evaluation or other purposes

As part of this function, the operator can create and use an EIR profile to define the parameters to:

- use a single EIR address for multiple EIRs,
- achieve the Check-IMEI-Request, and

- associate the EIR profile with a call control profile.

Equivalent PLMN

This feature is useful when an operator deploys both GPRS and UMTS access in the same radio area and each radio system broadcasts different PLMN codes. It is also useful when operators have different PLMN codes in different geographical areas, and the operators' networks in the various geographical areas need to be treated as a single HPLMN.

This feature allows the operator to consider multiple PLMN codes for a single subscriber belonging to a single home PLMN (HPLMN). This feature also allows operators to share infrastructure and it enables a UE with a subscription with one operator to access the network of another operator.

Fallback on DNS Failure

In releases prior to 21.5, on failure of DNS query with APN name and LAC-RAC extension, no more DNS queries were sent.

In release 21.5, SGSN sends DNS query with only APN name on failure of DNS query with APN name and LAC-RAC extension. The **dns-extn lac-rac fallback** command in the APN Profile Configuration mode can be configured to enable or disable fallback on DNS failure.

Important This enhancement is applicable only for Gn-SGSN.

First Vector Configurable Start for MS Authentication

Previously, the SGSN would begin authentication towards the MS only after the SGSN received all requested vectors. This could result in a radio network traffic problem when the end devices timed out and needed to re-send attach requests.

Now, the SGSN can be configured to start MS authentication as soon as it receives the first vector from the AuC/HLR while the SAI continues in parallel. After an initial attach request, some end devices restart themselves after waiting for the PDP to be established. In such cases, the SGSN restarts and a large number of end devices repeat their attempts to attach. The attach requests flood the radio network, and if the devices timeout before the PDP is established then they continue to retry, thus even more traffic is generated. This feature reduces the time needed to retrieve vectors over the GR interface to avoid the high traffic levels during PDP establishment and to facilitate increased attach rates.

Format Encoding of MNC and MCC in DNS Queries Enhanced

In order to provide effective control on DNS queries for particular type of procedures, existing CLI commands in GPRS and SGSN services have been deprecated and replaced with new enhanced commands. The command **dns israu-mcc-mnc-encoding [hexadecimal | decimal]** has been deprecated and a new CLI command **dns mcc-mnc-encoding { rai-fqdn | apn-fqdn | rnc-fqdn| mmec-fqdn| tai-fqdn}* {a-query | snaptr-query }* { decimal | hexadecimal }**. New keyword options **snaptr-query** and **a-Query** are provided to control different types of queries.

To ensure backward compatibility:

1. If the command **dns israu-mcc-mnc-encoding decimal** is executed, it will be auto converted to d**ns mcc-mnc-encoding rai-fqdn a-query snaptr-query decimal**.
2. If the command **dns israu-mcc-mnc-encoding hexadecimal** is executed, it will be auto converted to **dns mcc-mnc-encoding rai-fqdn a-query snaptr-query hexadecimal**

For more information see, *Command Line Interface Reference*.

Gb Manager

A new SGSN proclet has been developed. Now, all the link level procedures related to Gb -

- protocol (GPRS-NS and BSSGP) hosting, handling, administration, message distribution,
- keeping the other managers informed about the link/remote-node status,
- handling functionality of the Gb interface (all 2G signaling)

are removed from the Link Manager and moved to the SGSN's new Gb Manager proclet.

The new Gb Manager provides increased flexibility in handling link level procedures for each access type independently and ensures scalability. The consequence of relieving the Link Manager, of a large amount of message handling, is to decrease delays in sending sscop STAT messages resulting in the detection of link failure at the remote end. Use of this separate new proclet to handle 2G signaling messages means there will not be any MTP link fluctuation towards the RNS, which is seen during the BSC restart or extension activity in the network. As well, this improves the fluctuation towards the 3G connectivity.

GMM-SM Event Logging

To facilitate troubleshooting, the SGSN will capture procedure-level information per 2G or 3G subscriber (IMSI-based) in CSV formatted event data records (EDRs) that are stored on an external server.

This feature logs the following events:

- Attaches
- Activation of PDP Context
- RAU
- ISRAU
- Deactivation of PDP Context
- Detaches
- Authentications
- PDP Modifications

The new SGSN event logging feature is enabled/disabled per service via CLI commands. For more information on this feature, refer to the section *GMM/SM Event Logging* in this guide.

Gn/Gp Delay Monitoring

The SGSN measures the control plane packet delay for GTP-C signaling messages on the SGSN's Gn/Gp interface towards the GGSN.

If the delay crosses a configurable threshold, an alarm will be generated to prompt the operator.

A delay trap is generated when the GGSN response to an ECHO message request is delayed more than a configured amount of time and for a configured number of consecutive responses. When this occurs, the GGSN will be flagged as experiencing delay.

A clear delay trap is generated when successive ECHO Response (number of successive responses to detect a delay clearance is configurable), are received from a GGSN previously flagged as experiencing delay.

This functionality can assist with network maintenance, troubleshooting, and early fault discovery.

GTP-C Path Failure Detection and Management

The SGSN now provides the ability to manage GTP-C path failures detected as a result of spurious restart counter change messages received from the GGSN.

Previous Behavior: The old default behavior was to have the Session Manager (SessMgr) detect GTP-C path failure based upon receiving restart counter changes in messages (Create PDP Context Response or Update PDP Context Response or Update PDP Context Request) from the GGSN and immediately inform the SGTPC Manager (SGTPCMgr) to pass the path failure detection to all other SessMgrs so that PDP deactivation would begin.

New Behavior: The new default behavior has the SessMgr inform the SGTPCMgr of the changed restart counter value. The SGTPCMgr now has the responsibility to verify a possible GTP-C path failure by issuing an Echo Request/Echo Response to the GGSN. Path failure will only be confirmed if the Echo Response contains a new restart counter value. Only after this confirmation of the path failure does the SGTPCMgr inform all SessMgrs so that deactivation of PDP contexts begins.

GTPv0 Fallback, Disabling to Reduce Signalling

GTPv0 fallback can cause unnecessary signaling on the Gn/Gp interface in networks where all the GGSNs support GTPv1.

By default, the SGSN supports GTPv0 fallback and uses either GTPv1 or GTPv0. After exhausting all configured retry attempts for GTPv1, the SGSN retries the GTP-C Request using GTPv0. This fallback is conditional and is done only when the GTP version of a GGSN is unknown during the first attempt at activating a PDP context with the GGSN.

It is possible for the operator to disable the GTPv0 fallback for requests to GGSNs of specific APNs. Disabling the fallback function is configured under the APN profile and is applicable for GGSNs corresponding to that APN. If GTPv1 only is enabled in the APN profile, then the SGSN does not attempt fallback to GTPv0 (towards GGSNs corresponding to that APN) after all GTPv1 retries have been attempted. If more than one GGSN address is returned by the DNS server during activation, then the SGSN attempts activation with the next GGSN after exhausting all the GTPv1 retry attempts. If only one GGSN address is returned, then the SGSN rejects the activation after exhausting all the configured GTPv1 retries.

This change enables the operator to prevent unnecessary signaling on the Gn/Gp interface in networks where all the GGSNs support GTPv1. For example, if all the home GGSNs in an operator's network support GTPv1, then the unnecessary GTPv0 fallabck can be avoided by enabling this feature for the APNs associated with home GGSNs.

Handling Multiple MS Attaches All with the Same Random TLLI

Some machine-to-machine (M2M) devices from the same manufacturer will all attempt PS Attaches using the same fixed random Temporary Logical Link Identifier (TLLI).

The SGSN cannot distinguish between multiple M2M devices trying to attach simultaneously using the same random TLLI and routing area ID (RAI). As a result, during the attach process of an M2M device, if a second device tries to attach with the same random TLLI, the SGSN interprets that as an indication that the original subscriber moved during the Attach process and the SGSN starts communicating with the second device and drops the first device.

The SGSN can be configured to allow only one subscriber at a time to attach using a fixed random TLLI. While an Attach procedure with a fixed random TLLI is ongoing (that is, until a new P-TMSI is accepted by the MS), all other attaches sent to the SGSN with the same random TLLI using a different IMSI will be dropped by the SGSN's Linkmgr.

To limit the wait-time functionality to only the fixed random TLLI subscribers, the TLLI list can be configured to control which subscribers will be provided this functionality.

HSPA Fallback

Besides enabling configurable support for either 3GPP Release 6 (HSPA) and 3GPP Release 7 (HSPA+) to match whatever the RNCs support, this feature enables configurable control of data rates on a per RNC basis. This means that operators can allow subscribers to roam in and out of coverages areas with different QoS levels.

The SGSN can now limit data rates (via QoS) on a per-RNC basis. Some RNCs support HSPA rates (up to 16 Mbps in the downlink and 8 Mbps in the uplink) and cannot support higher data rates - such as those enabled by HSPA+ (theoretically, up to 256 Mbps both downlink and uplink). Being able to specify the QoS individually for each RNC makes it possible for operators to allow their subscribers to move in-and-out of coverage areas with different QoS levels, such as those based on 3GPP Release 6 (HSPA) and 3GPP Release 7 (HSPA+).

For example, when a PDP context established from an RNC with 21 Mbps is handed off to an RNC supporting only 16 Mbps, the end-to-end QoS will be re-negotiated to 16 Mbps. Note that an MS/UE may choose to drop the PDP context during the QoS renegotiation to a lower value.

This data rate management per RNC functionality is enabled, in the radio network controller (RNC) configuration mode, by specifying the type of 3GPP release specific compliance, either release 7 for HSPA+ rates or pre-release 7 for HSPA rates. For configuration details, refer to the *RNC Configuration Mode* section in the *Command Line Interface Reference*.

Ignore Context-ID during 4G/3G Handovers

HSS and HLR, when operating as separate network nodes, are required to use the same context-ID for a given APN-configuration of a subscriber. During inter-RAT cell reselections and handovers between 2G/3G and 4G, if the SGSN does not find a matching APN-configuration for the given context-ID learnt from the peer node, then the PDP does not get established. This could result in SRNS relocation failures when none of the PDP's learnt from the SGSN has a matching context-ID in the HLR.

New commands have been added to enable the operator to configure the SGSN to ignore the context-ID provided by the peer and to use the PDP- type and address information to search through HLR subscription and to update the context-ID information within the PDP. For details, refer to the description for the **rau-inter**

command under the *Call-Control Profile Configuration Mode Commands* section of the *Command Line Interface Reference*.

Interface Selection Based on UE Capability

The SGSN selects S6d/Gr interface based on whether hss-peer-service or map service is associated with the SGSN or GPRS service. If both the services are associated, then the selection is made based on configuration of the CLI command **prefer subscription-interface** under the Call Control Profile mode. With this feature enhancement, the SGSN now allows selection of S6d/ Gr interface only if the UE is EPC capable. A new CLI option **epc-ue** is added to the command **prefer subscription-interface** under the Call Control Profile mode for this enhancement. If this keyword is configured the S6d/Gr interface is selected only if UE is EPC capable. If this keyword is not configured the SGSN selects the S6d/Gr interface based on whether hss-peer-service or map service is associated with the SGSN or GPRS service (this is also the default behavior). The interface selection based on UE capability is done only at the time of Attach / new SGSN RAU / SRNS. Interface selected during Attach / new SGSN RAU / SRNS may change while doing inter PLMN RAU (intra SGSN) procedures.

Intra- or Inter-SGSN Serving Radio Network Subsystem (SRNS) Relocation (3G only)

Implemented according to 3GPP standard, the SGSN supports both inter- and intra-SGSN RNS relocation (SRNS) to enable handover of an MS from one RNC to another RNC.

The relocation feature is triggered by subscribers (MS/UE) moving from one RNS to another. If the originating RNS and destination RNS are connected to the same SGSN but are in different routing areas, the behavior triggers an intra-SGSN Routing Area Update (RAU). If the RNS are connected to different SGSNs, the relocation is followed by an inter-SGSN RAU. This feature is configured through the Call-Control Profile Configuration Mode which is part of the feature set.

Lawful Intercept

The Cisco Lawful Intercept feature is supported on the SGSN. Lawful Intercept is a license-enabled, standards-based feature that provides telecommunications service providers with a mechanism to assist law enforcement agencies in monitoring suspicious individuals for potential illegal activity. SGSN supports use of IP Security (a separate license-enabled, standards-based feature) for the LI interface; for additional information on IPSec, refer to the *Cisco StarOS IP Security (IPSec) Reference*. For additional information and documentation on the Lawful Intercept feature, contact your Cisco account representative.

Link Aggregation - Horizontal

The SGSN supports enhanced link aggregation (LAG) within ports on different XGLCs. Ports can be from multiple XGLCs. LAG works by exchanging control packets (Link Aggregation Control Marker Protocol) over configured physical ports with peers to reach agreement on an aggregation of links. LAG sends and receives the control packets directly on physical ports attached to different XGLCs. The link aggregation feature provides higher aggregated bandwidth, auto-negotiation, and recovery when a member port link goes down.

Local DNS

Previously, the SGSN supported GGSN selection for an APN only through operator policy, and supported a single pool of up to 16 GGSN addresses which were selected in round robin fashion.

The SGSN now supports configuration of multiple pools of GGSNs; a primary pool and a secondary. As part of DNS resolution, the operator can use operator policies to prioritize local GGSNs versus remote ones. This function is built upon existing load balancing algorithms in which weight and priority are configured per GGSN, with the primary GGSN pool used first and the secondary used if no primary GGSNs are available.

The SGSN first selects a primary pool and then GGSNs within that primary pool; employing a round robin mechanism for selection. If none of the GGSNs in a pool are available for activation, then the SGSN proceeds with activation selecting a GGSN from a secondary pool on the basis of assigned weight. A GGSN is considered unavailable when it does not respond to GTP Requests after a configurable number of retries over a configurable time period. Path failure is detected via GTP-echo.

Local Mapping of MBR

The SGSN provides the ability to map a maximum bit rate (MBR) value (provided by the HLR) to an HSPA MBR value.

The mapped value is selected based on the matching MBR value obtained from the HLR subscription. QoS negotiation then occurs based on the converted value.

This feature is available within the operator policy framework. MBR mapping is configured via new keywords added to the **qos class** command in the APN Profile configuration mode. A maximum of four values can be mapped per QoS per APN.

Important To enable this feature the **qos prefer-as-cap**, also a command in the APN Profile configuration mode, must be set to either **both-hlr-and-local** or to **hlr subscription**.

Local QoS Capping

The operator can configure a cap or limit for the QoS bit rate.

The SGSN can now be configured to cap the QoS bit rate parameter when the subscribed QoS provided by the HLR is lower than the locally configured value.

Depending upon the keywords included in the command, the SGSN can:

- take the QoS parameter configuration from the HLR configuration.
- take the QoS parameter configuration from the local settings for use in the APN profile.
- during session establishment, apply the lower of either the HLR subscription or the locally configured values.

Refer to the *APN Profile Configuration Mode* section of the *Command Line Interface Reference* for the **qos** command.

Location Change Reporting on the S4-SGSN

3G/2G Location Change Reporting on the SGSN facilitates location-based charging on the P-GW by providing the UE's location information when the UE is in connected mode.

The Gn-SGSN supports 2G and 3G location change reporting via user location information (ULI) reporting to the GGSN. For details, see the feature section *3G-2G Location Change Reporting*.

With Release 16.0, the S4-SGSN also supports 2G and 3G location change reporting per 3GPP 29.274 release 11.b, if the P-GW requests it. With this feature enhancement configured, the S4-SGSN is ready to perform ULI reporting per PDN connection via GTPv2. Reporting only begins after the S4-SGSN receives a reporting request from the P-GW. The P-GW generates a request based on charging enforcement and policy enforcement from the policy and charging rules function PCRF. Location Change Reporting is configured and enabled/disabled per APN.

The S4-SGSN's version of Location Change Reporting has been further enhanced with a network sharing option. If the network sharing license is installed and if the network sharing feature is enabled, then the operator can configure which PLMN information the SGSN sends to the P-GW in the ULI or Serving Network IEs.

Important The S3/S4 license is required to enable S4 functionality. The new "Location-reporting in connected-mode" license is required to enable Location Change Reporting functionality for the S4-SGSN. This new license is now required for Location Change Reporting on the Gn-SGSN.

Location Services

Location Services (LCS) on the SGSN is a 3GPP standards-compliant feature that enables the SGSN to collect and use or share location (geographical position) information for connected UEs in support of a variety of location services, such as location-based charging and positioning services.

The SGSN uses the Lg interface to the gateway mobile location center (GMLC), which provides the mechanisms to support specialized mobile location services for operators, subscribers, and third party service providers. Use of this feature and the Lg interface is license controlled. This functionality is supported on the 2G and 3G SGSN.

For details about basic location services and its configuration, refer to the *Location Services* section of the *SGSN Administration Guide*.

With Release 15.0, supported functionality has expanded to include:

- Mobile terminating deferred location requests are now supported
- Mobile originating requests are now supported, both immediate and deferred
- Differences between 2G and 3G LCS call flows are eliminated

Important With this release, expanded functionality for this feature is qualified for lab and field trials only.

Lock/Shutdown the BSC from the SGSN

When the SGSN returns to Active state, after scenarios such as rebooting or reloading, all the BSCs that had been connected to the SGSN would attempt to re-establish connections. This could result in two serious problems for operators:

1. High CPU usage in the SGSN where too many BSC/RNCs were connected.
2. Network overload when other network nodes cannot match the SGSN's capacity.

The SGSN now supports a Lock/Shutdown feature that provides a two prong solution. CPU Usage Solution: Staggering the BSC auto-learning procedures when the SGSN re-loads will help to reduce the high CPU usage. This can be achieved by the operator locking the NSE/BSCs from the SGSN before reboot/reload and then unlocking them one-by-one to avoid high CPU usage.

Network Overload Solution: A new timer, SNS-GUARD, has been added to clean-up resources if the SNS procedure does not complete properly, whether or not the BSC is administratively locked. Now the SGSN starts this timer after sending SNS-SIZE-ACK and the BSC information will be removed, if the auto-learning clean-up procedure does not complete before the timer expires.

A series of new commands and keywords has been added to enable the operator to configure this new administrative Lock/Shutdown the BSC functionality as part of 'interface management' configuration. For details, refer to the *SGSN Global Interface Management* section of the *Command Line Interface Reference.*

Multiple PLMN Support

With this feature, the 2.5G and 3G SGSNs now support more than one PLMN ID per SGSN. Multiple PLMN support facilitates MS handover from one PLMN to another PLMN.

Multiple PLMN support also means an operator can 'hire out' their infrastructure to other operators who may wish to use their own PLMN IDs. As well, multiple PLMN support enables an operator to assign more than one PLMN ID to a cell-site or an operator can assign each cell-site a single PLMN ID in a multi-cell network (typically, there are no more than 3 or 4 PLMN IDs in a single network).

This feature is enabled by configuring, within a single context, multiple instances of either an IuPS service for a single 3G SGSN service or multiple GPRS services for a 2.G SGSN. Each IuPS service or GPRS service is configured with a unique PLMN ID. Each of the SGSN and/or GPRS services must use the same MAP, SGTPU and GS services so these only need to be defined one-time per context.

Network Sharing

In accordance with 3GPP TS 23.251, the 2G and 3G SGSN provides an operator the ability to share the RAN and/or the core network with other operators. Depending upon the resources to be shared, there are 2 network sharing modes of operation: the Gateway Core Network (GWCN) and the Multi-Operator Core Network (MOCN).

Benefits of Network Sharing

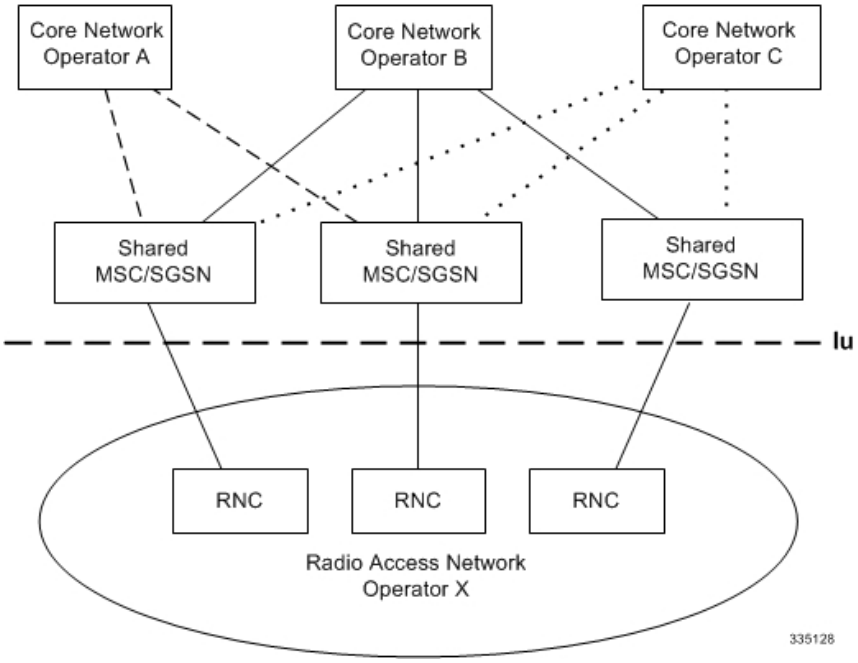
Network sharing provides operators with a range of logistical and operational benefits:

- Enables two or more network operators to share expensive common network infrastructure.
- A single operator with multiple MCC-MNC Ids can utilize a single physical access infrastructure and provide a single HPLMN view to the UEs.
- Facilitates implementation of MVNOs.

GWCN Configuration

For the 3G SGSN with a gateway core network configuration, the complete radio access network and part of the core network are shared (for example, MSC/SGSN) among different operators, while each operator maintains its own separate network nodes (for example, GGSN/HLR).

Figure 5: GWCN-type Network Sharing



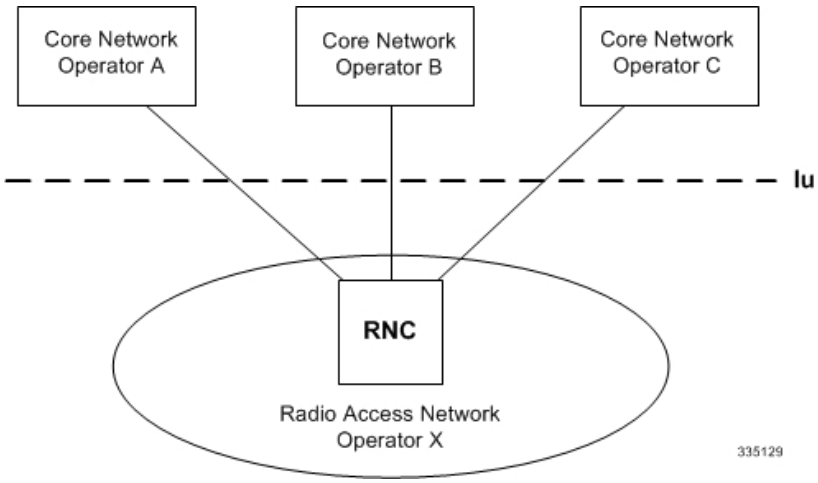
With the GWCN configuration, the SGSN supports two scenarios:

- GWCN with non-supporting UE
- GWCN with supporting UE

MOCN Configuration

In the multi-operator core network configuration, the complete radio network is shared among different operators, while each operators maintains its own separate core network. This functionality is available for both 2G and 3G SGSN.

Figure 6: MOCN-type Network Sharing



With the MOCN configuration, the SGSN supports the following scenarios:

- MOCN with non-supporting UE
- MOCN with supporting UE

Important The MOCN network sharing functionality now requires a separate feature license for both 2G and 3G scenarios. Contact your Cisco representative for licensing information.

Implementation

To facilitate network sharing, the SGSN implements the following key features:

- Multiple virtual SGSN services in a single physical node.
- Sharing operators can implement independent policies, such as roaming agreements.
- Equivalent PLMN configuration.
- RNC identity configuration allows RNC-ID + MCC-MNC instead of just RNC-ID.

Configuration for network sharing is accomplished by defining:

- NRI in the SGSN service configuration mode
- PLMN IDs and RNC IDs in the IuPS configuration mode
- Equivalent PLMN IDs and configured in the Call-Control Profile configuration mode.
- IMSI ranges are defined in the SGSN-Global configuration mode
- The Call-Control Profile and IMSI ranges are associated in the configuration mode.

For commands and information, refer to the *2G SGSN Multi-Operator Core Network* section in the *Serving GPRS Support Node Administration Guide* and the command details in the *Command Line Interface Reference*.

NRI-FQDN based DNS resolution for non-local RAIs (2G subscribers)

The SGSN now supports use of NRI-RAI based address resolution which includes both local lookup as well as DNS Query for non-local RAIs when selection of the call control profile is based on the old-RAI and the PLMN Id of the BSC where the subscriber originally attached. This feature was formerly supported only for

3G subscribers and is now extended to 2G subscribers. The command enables the SGSN to perform address resolution for peer SGSN with an NRI when an unknown PTMSI (Attach or RAU) comes from an SGSN outside the pool. The SGSN uses NRI-RAI based address resolution for the non-local RAIs for 2G subscribers in place of RAI based address resolution.

This functionality is applicable in situations for either inter- or intra-PLMN when the SGSN has not chosen a local NRI value (configured with SGSN Service commands) other than **local-pool-rai** or **nb-rai**. This means the RAI (outside pool but intra-PLMN) NRI length configured here will be applicable even for intra-PLMN with differently configured NRI lengths (different from the local pool). This functionality is not applicable to call control profiles with an associated MSIN range as ccprofile selection is not IMSI-based.

NRI Handling Enhancement

The SGSN's DNS lookup for SGSN pooling is supported in the call control profile. Previously, the SGSN's complete Gn DNS database had to be configured in the call control profile. If there was more than one SGSN in the local pool, then there would be multiple instances for every SGSN in the pool.

By using just the NRI value, this enhancement facilitates lookup for a peer SGSN in the local pool.

NRPCA - 3G

The SGSN supports the Network Requested Primary PDP Context Activation (NRPCA) procedure for 3G attachments.

There are no interface changes to support this feature. Support is configured with existing CLI commands (network-initiated-pdp-activation, location-area-list) in the call control profile configuration mode and timers (T3385-timeout and max-actv-retransmission) are set in the SGSN service configuration mode. For command details, see the *Command Line Interface Reference*

NRSPCA Support for S4-SGSN

The SGSN supports Secondary PDP context activation by the network. 3GPP TS 23.060 specifies two procedures for GGSN-initiated PDP Context Activation:

- Network Requested PDP Context Activation (NRPCA) - the SGSN already supports this but only for 3G access, and
- Network Requested Secondary PDP Context Activation (NRSPCA) Procedure.

NRSPCA allows the network to initiate Secondary PDP context activation if the network determines that the service requested by the user requires activation of an additional secondary PDP context. Network requested bearer control makes use of the NRSPCA procedure.

Network requested bearer control functionality is mandatory in EPC networks, requiring use of NRSPCA. The P-GW supports only the NRSPCA procedure. With this release, now the S4-SGSN supports network requested bearer control.

For a complete description of this feature and its configuration requirements, refer to the *Network Requested Secondary PDP Context Activation* chapter in the *Serving GPRS Support Node Administration Guide*

Operator Policy

This non-standard feature is unique to the StarOS. This feature empowers the carrier with unusual and flexible control to manage functions that are not typically used in all applications and to determine the granularity of the implementation of any: to groups of incoming calls or to simply one single incoming call. For details about the feature, its components, and how to configure it, refer to the *Operator Policy* section in this guide.

Important **SGSN configurations created prior to Release 11.0 are not forward compatible.** All configurations for SGSNs, with -related configurations that were generated with software releases prior to Release 11.0, must be converted to enable them to operate with an SGSN running Release 11.0 or higher. Your Cisco Representative can accomplish this conversion for you.

Some Features Managed by Operator Policies

The following is a list of some of the features and functions that can be controlled via configuration of Operator Policies:

- APN Aliasing
- Authentication
- Direct Tunnel - for feature description and configuration details, refer to the *Direct Tunnel* section in this guide
- Equivalent PLMN
- IMEI Override
- Intra- or Inter-SGSN Serving Radio Network Subsystem (SRNS) Relocation (3G only)
- Network Sharing
- QoS Traffic Policing per Subscriber
- SGSN Pooling - Gb/Iu Flex
- SuperCharger
- Subscriber Overcharging Protection - for feature description and configuration details for Gn-SGSN, refer to the *Subscriber Overcharging Protection* section in this guide.

Overcharging Protection

Overcharging Protection enables the Gn-SGSN to avoid overcharging the subscriber if/when a loss of radio coverage (LORC) occurs in a UMTS network. For details and configuration information, refer to the *Subscriber Overcharging Protection* section in this book.

QoS Traffic Policing per Subscriber

Traffic policing enables the operator to configure and enforce bandwidth limitations on individual PDP contexts for a particular traffic class.

Traffic policing typically deals with eliminating bursts of traffic and managing traffic flows in order to comply with a traffic contract.

The SGSN conforms to the DiffServ model for QoS by handling the 3GPP defined classes of traffic, QoS negotiation, DSCP marking, traffic policing, and support for HSDPA/HSUPA.

QoS Classes

The 3GPP QoS classes supported by the SGSN are:

- Conversational
- Streaming
- Interactive
- Background

The SGSN is capable of translating between R99 and R97/98 QoS attributes.

QoS Negotiation

On PDP context activation, the SGSN calculates the QoS allowed, based upon:

- **Subscribed QoS -** This is a per-APN configuration, obtained from the HLR on an Attach. It specifies the highest QoS allowed to the subscriber for that APN.
- **Configured QoS -** The SGSN can be configured with default and highest QoS profiles in the configuration.
- **MS requested QoS -** The QoS requested by the UE on pdp-context activation.

DSCP Marking

The SGSN performs diffserv code point (DSCP) marking of the GTP-U packets according to allowed-QoS to PHB mapping. The default mapping matches that of the UMTS to IP QoS mapping defined in 3GPP TS 29.208.

The SGSN also supports DSCP marking of the GTP control plane messages on the Gn/Gp interface. This allows QoS to be set on GTP-C messages, and is useful if Gn/Gp is on a less than ideal link. DSCP marking is configurable via the CLI, with default = Best Effort Forwarding.

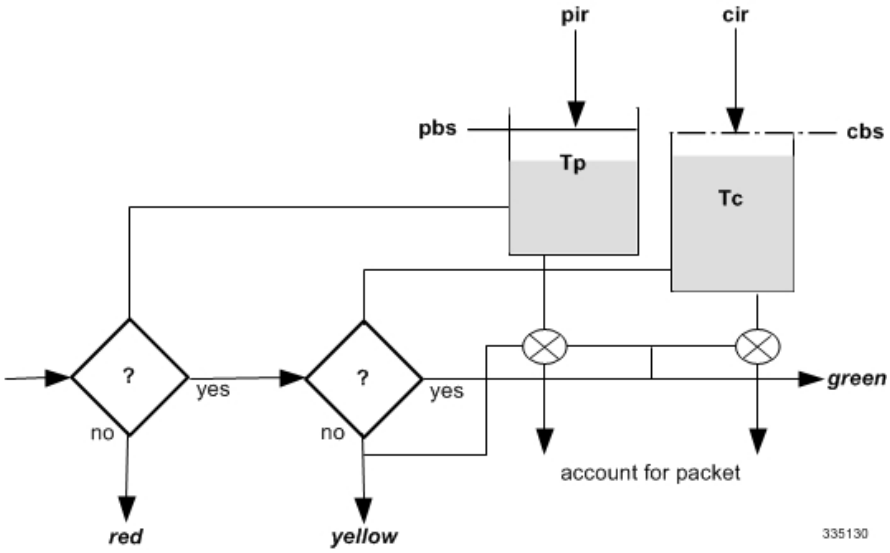
Traffic Policing

The SGSN can police uplink and downlink traffic according to predefined QoS negotiated limits fixed on the basis of individual contexts - either primary or secondary. The SGSN employs the Two Rate Three Color Marker (RFC2698) algorithm for traffic policing. The algorithm meters an IP packet stream and marks its packets either green, yellow, or red depending upon the following variables:

- **PIR -** Peak Information Rate (measured in bytes/second)
- **CIR -** Committed Information Rate (measured in bytes/second)
- **PBS -** Peak Burst Size (measured in bytes)
- **CBS -** Committed Burst Size (measured in bytes)

The following figure depicts the working of the TCM algorithm:

Figure 7: TCM Algorithm Logic for Traffic Policing



For commands and more information on traffic policing configuration, refer to the *Command Line Interface Reference*.

VPC-DI platform support for SGSN

The traditional proprietary Cisco ASR 5500 hardware platform provides carrier class hardware redundancy and have limited scalability. The VPC-SI model separates the StarOS from the proprietary hardware. It consists of the StarOS software running within a single VM. This provides the end user with low entry cost (software licenses and commodity hardware), simplified setup, and well-defined interfaces. The VPC-SI is ideally suited for small carriers, remote locations, lab testing, trials, demos, and other models where full functionality is needed. The Cisco VPC-Distributed Instance (VPC-DI) platform allows multiple VMs to act as a single StarOS instance with shared interfaces, shared service addresses, load balancing, redundancy, and a single point of management. The VPC-DI offers enhanced hardware capabilities and the SGSN is enhanced to support the VPC-DI platform.

Important For more information on the VPC-DI platform, see the *VPC-DI System Administration Guide*.

Reordering of SNDCP N-PDU Segments

The SGSN fully supports reordering of out-of-order segments coming from the same SNDCP N-PDU. The SGSN waits the configured amount of time for all segments of the N-PDU to arrive. If all the segments are not received before the timer expiries, then all queued segments are dropped.

RAN Information Management (RIM)

RAN information is transferred from a source RAN node to a destination RAN node in a RIM container. This is a mechanism for the exchange of information between applications belonging to RAN nodes, for example two BSCs. The RIM container is transparent to the SGSN.

Support for RIM procedures is optional for both the SGSN and other RAN nodes (e.g., RNC). When the SGSN supports RIM procedures, the SGSN provides addressing, routing and relay functions. All RIM messages are routed independently by the SGSN. The SGSN performs relaying of RIM messages between BSSGP, RANAP, and GTP in accordance with 3GPP TS 48.018, TS25.413, and TS29.060 respectively.

On the Gb (BSSGP) interface, RIM procedures are negotiated at the start/restart of a Gb link as part of the signaling BVC reset procedure. On the Iu (RANAP) interface, there is no negotiation for using RIM procedures. Support for RIM procedures enhances the subscriber's user experience by minimizing the service outage during cell re-selection.

S4 Support on the SGSN

The SGSN can provide an interface between UMTS (3G) and/or GPRS (2.5G) networks and the evolved packet core (EPC) network. This functionality requires a special S4 feature license. Throughout the documentation the SGSN with this additional functionality is referred to as an S4-SGSN.

To facilitate communication with GPRS, UMTS, and EPC networks, the SGSN is configured with standard 2.5G SGSN, 3G SGSN or dual access SGSN services, and then configured with additional enhancements to enable communication with the EPC network.

The S4-SGSN communicates with other UMTS and GPRS core networks elements via the GTPv1 protocol, and communicates with EPC network elements and peer S4-SGSNs via the GTPv2 protocol. The S4-SGSN communicates with the UMTS (3G) / GPRS (2.5G) radio access network elements in the same manner as an SGSN.

Depending on the configured SGSN service type, the S4-SGSN can interface with some or all of the following UMTS/GPRS and EPC network elements:

- Serving Gateway (S-GW)
- Mobility Management Entity (MME)
- Peer S4-SGSN (2.5G or 3G with S4 support)
- Peer dual access S4-SGSN
- Peer SGSN (2.5G or 3G)
- Peer dual access SGSN
- GGSN

S3 and S4 Interface Support

S3 and S4 interface support is a license-enabled feature that enables 2G and 3G networks to interface with the 4G evolved packet core (EPC) network. The S3/S4 functionality ensures session continuity on handovers between 2G/3G subscribers and 4G LTE subscribers. S3/S4 functionality simplifies core network operations the following ways:

- Replaces the GGSN in the network with the P-GW
- Replaces the need for an HLR by providing connectivity to the HSS
- Optimized idle mode signaling during 3G/2G to 4G handovers (when the ISR feature is enabled)

The S3 and S4 interfaces provide control and bearer separation, and offload the backward compatibility requirement from the mobility management entity (MME) and serving gateway (S-GW) EPC elements to the UMTS core.

- **S3 Interface**: Provides a GTPv2-C signaling path connection between the MME and the SGSN (MPC). The S4-SGSN to MME RAU/TAU context handovers are supported via the S3 interface.
- **S4 Interface**: Provides a data and signaling interface between the S-GW and the S4-SGSN (MPC) for bearer plane transport (GTPv2-U). The S4-SGSN communicates with the P-GW via the S-GW.

With support for S3/S4 interface, soft-handoffs between 2G/3G and the EPC networks are possible for multi-mode UEs. Without this functionality, the Gn/Gp SGSN can still inter-work with the EPC core using GTPv1, but soft-handoffs cannot be achieved. Note that GTPv2 to GTPv1 conversions (for QoS and Context IDs) are lossy data conversions, so a subscriber doesn't encounter a similar type of network behavior while in 2G/3G and 4G networks.

S4-SGSN Support for "Higher Bit Rates than 16 Mbps"Flag

As per 3GPP R9 specifications, the SGSN can now be aware if the UE is capable of supporting extended R7 bit rates. The "higher bit rates than 16 Mbps" flag is used for this purpose. This flag is sent by the RNC in the Initial UE message or Re-location Complete message or by Peer S4-SGSN / MME in Forward Relocation Request / Context Response message. The SGSN also supports sending "higher Bit Rates than 16 Mbps flag" as part of MM Context in Context response/Forward Relocation request/Identification request during Old ISRAU/SRNS handover procedures.The SGSN stores the UE capability in the MM-context. During PDP context activation, the per bearer bit rate or APN-AMBR is capped based on the flag's value. If the RNC is not 3GPP R9 compliant, the SGSN does not receive this flag. A new CLI keyword **sm ue-3gpp-compliance-unknown restrict-16mbps** is introduced under the sgsn-service to support this functionality. When the CLI is configured, the SGSN caps the APN-AMBR for non-GBR bearers to "16" Mbps and rejects activation of GBR bearers with GBR higher than "16" Mbps. If not, APN-AMBR and GBR higher than "16" Mbps are allowed.

Consider the scenarios where UE 3GPP compliance is not known and the CLI is configured to restrict bitrate to 16 Mbps or it is known that UE is not capable of supporting bitrates higher than 16Mbps; the Session Manager uses the flag to perform the following actions:

1. The APN-AMBR is restricted to "16" Mbps during PDP activation of non-GBR bearers, particularly the default bearer.
2. If the PGW upgrades the APN-AMBR in Create Session Response during non-GBR bearer activation, then the APN-AMBR is retained as "16" Mbps and same is indicated to the UE in an Activate Accept.
3. If the PGW upgrades APN-AMBR in Update Bearer Request for non-GBR bearer, then the APN-AMBR is restricted to "16" Mbps and only if the APN-AMBR changes, the PGW init bearer modification procedure is continued. In case APN-AMBR does not change, then Update Bearer Response is sent immediately.
4. For GBR bearers, Update Bearer Request with GBR/MBR higher than "16" Mbps is rejected with "No resources available".
5. Activation of GBR bearers with MBR/GBR higher than "16" Mbps in Create Bearer Request is rejected with cause "No resources available".
6. After S3 SRNS, Modify Bearer Command is initiated to modify the APN-AMBR to "16" Mbps for Non-GBR bearers having bitrates higher than 16 Mbps.
7. After S3 SRNS, GBR bearers having bitrates higher than "16" Mbps are de-activated.

For more information on the CLI command see, Command Line Interface Reference.

S6d and Gr Interface Support

The S4-SGSN supports the Diameter based S6d interface to the HSS, in addition to the legacy Gr interface to the HLR (used by an SGSN configured to use the Gn/Gp interfaces). This is a license-enabled feature.

The S6d / Gr interface enhancements allow operators to consolidate the HLR/HSS functions into a single node, which improves operational efficiency and other overhead. With the deployment of the EPC core, many operators may consolidate the HLR/HSS functions into a single node. Until then, the S4-SGSN still supports the MAP-based Gr and the Diameter based S6d interfaces.

The SGSN selects the Gr interface / S6d interface based on the MAP or HSS service associated with the configured SGSN and/or GPRS services. If both the services are associated, then SGSN will use the following order of selection:

1. Select the appropriate interface based on any operator policy preference for S6d / Gr.
2. If no operator policy is present, then by use the Gr interface by default.

The S4-SGSN sets the following initiate UGL messages on a change of HSS service:

- Initial attach indicator bit in Update GPRS Location message, ISR information IE, if the UGL is sent for an initial attach or for a inbound routing area update without ISR activation and the selected interface is Gr.
- Initial attach indicator bit in Update Location Request message, ULR flags, if the ULR is sent for an initial attach or for a inbound routing area update without ISR activation and the selected interface is S6d.

Configurable Pacing of PDP Deactivations on the S4-SGSN

The S4-SGSN now supports configurable pacing of PDP de-activations towards UEs due to path failures. Previously in the S4-SGSN, the pacing of path failure delivery was started by the EGTP application and it used the generic session manager pacing mechanism. The generic pacing mechanism performed 1000 path failure initiated PDP de-activations per second per session manager. Since this may not be desirable for many operators based on their RAN's capability, the S4-SGSN now supports the configurable pacing of PDP deactivations via the SGSN application (the same mechanism used in the Gn/Gp SGSN).

The existing **pdp-activation-rate command** in *SGSN Global Configuration Mode* can be used to configure the pacing of PDP de-activations for both the connected-ready state and the idle-standby state.

This feature is included with the SGSN S3/S4 license. No additional feature license is required.

DNS SNAPTR Support

By default, the S4-SGSN supports the initiation of a DNS query after APN selection using a S-NAPTR query. The SGSN resolves a P-GW by sending an APN-FQDN query to the DNS client. Similarly, the SGSN resolves the S-GW by sending a RAI-FQDN query to the DNS client. The DNS Client then sends a query to the DNS server to retrieve NAPTR/SRV/A records and return the S-GW or P-GW IP address to the SGSN.

On the S4-SGSN, an additional configurable is available that identifies the context where DNS lookup for EPC-capable UEs must occur. This is accomplished by creating a call control profile that directs the system's DNS client to perform the lookup in the context where the SGSN's DNS client is configured.

If the CLI configurable is not used, or removed, the S4-SGSN chooses the DNS client from the context where the EGTP service is configured for performing P-GW DNS resolution, if the EGTP service is associated for a EPC capable UE.

If the EGTP service is not present and the UE is EPC-capable, and if **apn-resolve-dns-query snaptr** is configured in an APN profile, then the S4-SGSN uses the DNS client in the context where the SGTP service is present for resolving a co-located P-GW/GGSN and selects the Gn interface.

S4-SGSN Statistics Support

Statistics have been added to provide information on S4-SGSN functionality.

The statistics added track information related to:

- SGW Relocations
- ISR Deactivations
- Number of active PDPs using the S4 interface in 3G
- S3 Interface Selection Statistics
- Procedure Abort Statistics
- GTPU Statistics
- IDFT Statistics

In addition, support for EGTPC schema bulk statistics is implemented to provide information on communication between the S4-SGSN and the EPC S-GW over the S4 interface.

S13' Interface Support

In addition to the MAP-based Gf interface, the S4-SGSN supports the Diameter-based S13' (S13 prime) interface towards the equipment identify registry. The S13' interface support enables operators to consolidate the EIR functions into a single node, which increases operational efficiency. S13' interface support is a license-enabled feature.

The S13' interface enables the S4-SGSN to perform the ME Identity Check procedure to validate the IMEI with the EIR. The S4-SGSN selects Gf or S13' interface based on which interface is configured and the type of service (MAP or HSS) is associated with the SGSN and/or the GPRS service. If both services are associated, then the S4-SGSN will select the appropriate interface based on the following sequence:

1. An operator policy preference is configured for Gf or S13'
2. If no operator policy preference is set, then by default the S4-SGSN uses the Gf interface

By default, the IMSI is sent to the EIR as part of the IMEI Check procedure over the S13' interface.

Idle Mode Signaling Reduction

The Idle mode signaling reduction (ISR) feature on the S4-SGSN provides a mechanism to optimize and/or reduce signaling load during inter-RAT cell-reselection in idle mode (that is, in the ECM-IDLE, PMM-IDLE, and GPRS-STANDBY states). It is a mechanism that allows the UE to remain simultaneously registered in a UTRAN/GERAN Routing Area (RA) and an E-UTRAN Tracking Area (TA) list. This allows the UE to make cell reselections between E-UTRAN and UTRAN/GERAN without having to send any TAU or RAU requests, as long as the UE remains within the registered RA and TA list.

ISR is a feature that reduces the mobility signalling and improves the battery life of UEs. Also reduces the unnecessary signalling with the core network nodes and air interface. This is important especially in initial deployments when E-UTRAN coverage will be limited and inter-RAT changes will be frequent.

The benefit of the ISR functionality comes at the cost of more complex paging procedures for UEs, which must be paged on both the registered RA and all registered TAs. The HSS also must maintain two PS registrations (one from the MME and another from the SGSN).

ISR support for 3G subscribers was introduced in release 14.0. ISR support for 2G subscribers is available in 15.0 and later releases.

ISR is not supported on the Gn/Gp SGSN.

For a detailed description of this feature, refer to the *Idle Mode Signaling Reduction on the S4-SGSN* chapter in this guide.

Important ISR is a license enabled feature. Contact your Cisco representative for details on licensing information.

ISR with Circuit Switched Fallback

Circuit-Switched Fallback (CSFB) is an alternative solution to using IMS and SRVCC to provide voice services to users of LTE. The IMS is not part of the solution, and voice calls are never served over LTE. Instead, the CSFB relies on a temporary inter-system that switches between LTE and a system where circuit-switched voice calls can be served.

The LTE terminals 'register' in the circuit switched domain when powered and attaching to LTE. This is handled through an interaction between the MME and the MSC-Server in the circuit-switched network domain over the SGs interface.

Consider the following scenarios:

- Voice calls initiated by the mobile user: If the user makes a voice call, the terminal switches from a LTE system to a system with circuit-switched voice support. Depending on where the UE latches on after completion of the voice call:
  - The packet-based services that are active on the end-user device at this time are handed over and continue to run in a system with circuit-switched voice support but with lower data speeds.

  OR

  - The packet-based services that are active on the end-user device at this time are suspended until the voice call is terminated and the terminal switches back to LTE again and the packet services are resumed.
- Voice calls received by the mobile user: If there is an incoming voice call to an end-user that is currently attached to the LTE system, the MSC-Server requests a paging in the LTE system for the specific user. This is done through the SGs interface between the MSC Server and the MME. The terminal receives the page, and temporarily switches from the LTE system to the system with circuit-switched voice support, where the voice call is received. Once the voice call is terminated, the terminal switches back to the LTE system.

For a detailed feature description of this feature refer to the chapter "ISR with Circuit Switched Fallback" in this document.

ISD / DSD Message Handling and HSS Initiated Bearer Modification

The Home Subscriber Server (HSS) / Home Location Register (HLR) maintains the subscriber database. Insert Subscriber Data (ISD) and Delete Subscriber Data (DSD) messages are generated by the HSS/HLR. These messages are used to communicate the subscribers current subscription data to the S4-SGSN. The subscription data for a subscriber can include one of the following:

- GPRS subscription data.
- EPS subscription data.

- Both GPRS and EPS subscription data.

The PDP is either modified or deleted based on the subscription data received by the S4-SGSN.

The S4-SGSN deletes the PDP context if any form of barring is detected or if the APN-name or PDP-type of the PDP address is changed. The S4-SGSN modifies the PDP if QoS is changed or APN-AMBR is changed (in case of EPS subscription).

If a PDP modification is required based on the subscription data received but the associated UE is disconnected or in an inactive state, such PDP contexts are deleted by the S4-SGSN.

Important The S4-SGSN does not delete the PDP contexts if Idle Mode Signalling Reduction (ISR) is activated or PDP is preserved. In such cases the S4-SGSN initiates a PDP modify only after UE activity is detected.

If the UE is connected or in a ready state, the S4-SGSN sends an updated bearer command (with subscribed QoS) to the S-SGW or P-GW and the P-GW initiates a PDP modify procedure.

HSS initiated bearer modification

The Modify bearer command is a notification sent to the S-GW/P-GW which notifies a change in the subscribed QoS. The message is sent to S-GW/P-GW if the UE is in ready or connected state. Modify Bearer command is not sent when the PDP is in preserved state and when ISR is active, in such cases the S4-SGSN initiated modify request using Modify Bearer Request updates the QoS to the S-GW/P-GW after the PDP is active or UE activity is detected on S4-SGSN respectively.

UMTS-GSM AKA Support on the S4-SGSN

The S4-SGSN provides support for the following UMTS/GSM Authentication and Key Agreement (AKA) procedures:

- SRNS relocation
- Attach
- PTMSI attach (foreign/local)
- Service Request
- Inter SGSN RAU
- Timers Handling
- Re-use of Vectors
- Using the Peer SGSN/MME vectors (ISRAU/PTMSI attach) in the same or different PLMN

3G and 2G SGSN Routing Area Update

The S4-SGSN supports outbound Routing Area Update (RAU) procedures for a subscriber already attached on that SGSN (that have PDP contexts anchored through S4 interface) and inbound RAU procedures for an EPC capable UE. The RAU procedures are required to enable mobility across the UMTS and EPC core network coverage areas using the S3 interface for context transfers.

The S4-SGSN determines if the old peer node is an MME or SGSN based on the most significant bit of the LAC. If the most significant bit of the LAC is set then the old peer node is an MME (and the RAI is mapped from GUTI). If the bit is not set then the old RAI represents an SGSN.

However, some operators have already used LAC values greater than 32768 (most significant bit set) for their existing UMTS / GPRS networks. For such operators identification of a peer node through MSB bit of LAC

will not work. In these cases, operators can use the Configurable GUTI to RAI Conversion Mapping, on page 54 feature.

The following RAU procedures are supported for both 2G and 3G services:

- 2G and 3G Intra-SGSN RAU with and without S-GW relocation
- 2G and 3G Inter-SGSN/SGSN-MME RAU with and without S-GW relocation across S16 and S3 interfaces
- Intra-SGSN Inter-RAT RAU with and without S-GW relocation

2G and 3G Intra RAU with and without S-GW Relocation

The S4-SGSN supports the intra-SGSN routing area update (ISRAU), which can occur in the following scenarios:

- The MS changes its routing area
- The periodic RAU timer expires for the MS
- The MS changes its network capability

The S4-SGSN also supports intra SGSN, inter PLMN RAU requests. However, if the new PLMN's operator policy is configured to use the Gn interface, the PDP contexts are not transferred from the S4 interface to the Gn interface.

Important The S4-SGSN currently does not support the association of a different EGTP service for each PLMN.

2G and 3G Inter-SGSN and Inter SGSN-MME RAU with and without S-GW Relocation Across S16 and S3 Interfaces

The S4-SGSN supports both Inter-SGSN RAU and SGSN-MME RAU, which will be triggered when a UE sends Routing Area Update (RAU) request to a new SGSN in the following scenarios:

- The serving RAI changes from one SGSN coverage area to another SGSN coverage area
- During a handover from a E-UTRAN coverage area to a UMTS coverage area

Intra-SGSN Inter-RAT RAU with and without S-GW Relocation

The S4-SGSN supports intra-SGSN 3G to 2G routing area updates (RAU) and supports the handover of MM and PDP contexts from the SGSN service to the GPRS service. Similarly, it supports intra-SGSN 2G to 3G RAUs and supports the handover of MM and PDP contexts from the GPRS service to the SGSN service.

Important Currently, the S4-SGSN expects that both the SGSN and GPRS services will be associated with the same EGTP service for successful intra-SGSN inter-RAT handovers.

IPv4 and IPv6 PDP Type Override

The S4-SGSN supports the override of the IPv4/IPv6 PDP type by either IPv4 or IPv6 when the dual PDP feature is enabled. This is controlled via a call control profile, and is configured independently for 2G GPRS and 3G UMTS access.

Statistics are maintained to track successes and failures for IPv4 and IPv6 PDP activations with override.

NAPTR-based Dynamic HSS Discovery

In releases prior to R15.0, the SGSN could contact a HSS only through static configuration of the HSS peer end point through the HSS service. From Release R15.0 onwards, dynamic peer discovery is supported. The HSS address will be resolved using NAPTR based DNS request-response method. The following commands have to be enabled for dynamic peer discovery:

- In the Context Configuration Mode, the command **diameter endpoint** < *endpoint_name* > has to be enabled.
- In the Diameter Endpoint Configuration Mode, the command **dynamic-peer-discovery [protocol { sctp | tcp }]** has to be enabled.
- In the Diameter Endpoint Configuration Mode, the command **dynamic-peer-realm** < *realm_name* > has to be enabled.
- In the Diameter Endpoint Configuration Mode, the command **dynamic-peer-failure-retry-count** < *no_of_retries* > has to be enabled.

The "realm name" is used for dynamic peer discovery. The "dynamic-peer-failure-retry-count" is used to configure the number of re-tries in peer discovery.

P-GW Initiated PDP Bearer Deactivation

The S4-SGSN supports the P-GW initiated PDP deactivation procedure in addition to the legacy MS initiated deactivation procedure.

The S4-SGSN processes Delete Bearer Requests received from the S-GW (sent by the P-GW) and deactivates the requested bearers (PDP contexts) by sending a Deactivate PDP Context Request to the UE and then deactivates the PDP context. If the S4-SGSN receives a Delete Bearer Request from the S-GW and the subscriber is in the PMM-IDLE / GPRS-STANDBY state, it pages the UE before deactivating the PDP context request.

In the case of 3G, the S4-SGSN will initiate RAB release procedures for the deactivated bearers. For 2G there is no RAB release procedure.

S-GW and P-GW Tunnel and EPS Subscription Recovery

The S4-SGSN supports session recovery procedures and recovers the S4 tunnel created for each subscriber assigned PDP contexts through S4 interface. This functionality is part of session recovery procedures and allows sessions to be reconstructed when the system recovers from a card-level software fault.

The SGSN side TEID and the S-GW side TEID for the S4 tunnel are check-pointed and recovered during session recovery. The S4-SGSN also recovers every PDN connection and their corresponding P-GW-side TEID.

The S4-SGSN session recovery procedures have been enhanced to support recovery of EPS subscription data received from the HLR / HSS. The EPS subscription information may contain a maximum of 50 APN profiles and each APN profile contains an APN name string and a PDN GW FQDN string, which is check-pointed and recovered as part of the enhanced session recovery procedures.

Local Configuration of S-GW and S4-SGSN per RAI

The SGSN already supports selection of the S-GW using DNS SNAPTR queries for the RAI FQDN. The S4-SGSN now provides the option to configure a local S-GW address for a RAI (LAC, RAC MCC and MNC). This functionality enhances the S-GW selection logic to allow the call to continue even if DNS lookup fails for any reason.

The S4-SGSN will select this local S-GW address based on the configured local policy. The local policy also can be configured to allow the selection of the locally configured S-GW address when the DNS lookup fails.

Local selection of the S-GW address applies in the following scenarios:

- First PDP context activation for a subscriber
- Intra SGSN routing area update
- New SGSN routing area update
- Intra SGSN inter RAT handover

Configurable GUTI to RAI Conversion Mapping

The S4-SGSN allows operators to configure mapping to an EPC MME for networks that already use LAC ranges between 32768 and 65535.

LAC ranges between 32768 to 65535 are currently being used in some UMTS/GPRS deployments although 3GPP TS 23.003 indicates that a UMTS / GPRS network should not use LACs in that range. This range is reserved for the MME group code.

In an LTE network, the MME group code is mapped to the LAC and therefore the LAC and MME group code should be separate. The S4-SGSN provides a customized solution for this problem by identifying the valid MME group codes, which it uses to identify whether the received LAC is a native LAC or a LAC mapped from GUTI (i.e., an MME group code part of GUTI).

S4-SGSN Support for Fallback to V1 Cause Code in GTPv2 Context Response

As per revised 3GPP TS 29.274 v8.6.0, the Context Response message received from a peer SGSN can have a cause code "Fallback to GTP-V1", if the peer SGSN had provided a Gn interface for a subscriber due to local policy. When a new SGSN receives a Context Response with cause code as "Fallback to GTP-v1" it performs a GTP-v1 SGSN Context Request, Context Response and Context Ack with the peer SGSN to obtain the subscribers MM and PDP contexts.

S4-SGSN Support for Mobility Management Procedures

To support the S6d/Gr interface, the S4-SGSN supports the following mobility management procedures over the those (HSS/HLR) interfaces:

- Attach
- Service request
- Detach
- Iu-Release procedures
- Operator policy override for the Gn/S4 interface for EPC subscribers
- Zone code
- ARD
- ADD
- Operator policy-based Mobility Management context handling

QoS Mapping Support

The S4-SGSN supports the configuration of QoS parameters to ensure proper QoS parameter mapping between the S4-SGSN and EPC S-GWs, P-GWs, and UEs.

The S4-SGSN communicates QoS parameters towards the S-GW and P-GW in EPC QoS. However, it sends QoS towards the UE in the QoS format defined in the GMM/SM specification (TS 24.008). 3GPP defines a

mapping for EPS QoS to pre-release 8 QoS in TS 23.401, Annex E. On the S4-SGSN, operators can configure the quality of service (QoS) parameters as call-control-profiles that will ensure proper QoS mapping between the S4-SGSN and the EPC gateways (P-GW and S-GW) and UEs.

The configured call-control-profiles will be used if the S4 interface is chosen for PDP activation, but the subscription does not have an EPS subscription. Therefore, GPRS subscription data (which uses QoS in pre-release 8 format), will be mapped to EPS QoS behavior. The Allocation and Retention policy will be mapped to EPS ARP using the configured call control profiles.

If the QoS mapping configuration is not used, the following default mappings are used:

- Default ARP high-priority value = 5
- Default ARP medium-priority value = 10
- Default pre-emption capability = shall-not-trigger-pre-emption
- Default pre-emption vulnerability = not pre-emptable

MS Initiated Primary and Secondary Activation

The S4-SGSN supports default and dedicated bearer activation for:

- Default and dedicated activation - secondary PDP procedure trigger from MS).
- Lawful Intercept for activation rejects and failures
- Dual stack PDP handling
- APN-selection as per annex A.2/Spec 23.060 rel-9

Deactivation Procedure Support

The S4-SGSN supports the following deactivation procedures:

- 3G / 2G MS initiated bundle deactivation
- 3G / 2G MS initiated dedicated bearer deactivation
- 3G / 2G P-GW initiated dedicated bearer deactivation
- 3G / 2G P-GW initiated PDN deactivation

MS, PGW and HSS Initiated PDP Modification Procedure Support

The S4-SGSN supports the following packet data protocol (PDP) modification procedures:

- 2G and 3G MS initiated PDP modification procedures
- 2G and 3G P-GW Initiated PDP modification procedures
- 2G and 3G HSS initiated PDP modification procedures

The PDP context modification procedures are invoked by the network or by the MS to modify the parameters that were negotiated under the following conditions:

- During the PDP context activation procedure
- During the secondary PDP context activation procedure
- At a previously performed PDP context modification procedure

Depending on the selected Bearer Control Mode, the MS or the network may also create and delete a traffic flow template (TFT) in an active PDP context. The procedure can be initiated by the network or the MS at any time when a PDP context is active. Only the network may modify or delete a TFT packet filter that the network has created. Conversely, only the MS may modify or delete a TFT packet filter that the MS has created.

MS-Initiated PDP Context Modification

The Mobile Station (MS) initiated PDP context modification procedure MS allows for a change in negotiated QoS, the radio priority level, or the TFT negotiated during the PDP context activation procedure.

E-UTRAN capable MSs will not modify the QoS of the first PDP context that was established within the PDN connection.

The MS initiates the Modification procedure by sending a MODIFY PDP CONTEXT REQUEST message to the SGSN. The SGSN validates the received message and sends out a BEARER RESOURCE COMMAND message to the S-GW with a valid PTI value which is then sent to the PGW. On accepting the modification, the P-GW sends out an Update Bearer Request with the PTI copied from the received BEARER RESOURCE COMMAND message. Upon successful completion of the modification, the SGSN replies with the MODIFY PDP CONTEXT ACCEPT message.

P-GW-Initiated PDP Context Modification

The Packet Data Node Gateway (P-GW) initiated PDP context modification procedure is used in cases when:

- One or several of the EPS Bearer QoS parameters are to be modified
- To add/modify/delete the TFT related to the PDP Context or BCM-Mode change
- To modify the APN-AMBR

The P-GW can request the modification procedure by sending an UPDATE BEARER REQUEST message without a PTI field to the S-GW, and the S-GW will forward the request to SGSN. The SGSN validates the request and initiates a MODIFY PDP CONTEXT REQUEST message to the MS. On successful completion of the procedure, the SGSN will send an UPDATE BEARER RESPONSE with an appropriate cause value.

HSS Initiated PDP Context Modification

The Home Subscriber Server (HSS) initiated PDP context modification procedure is used when the HSS decides to modify the subscribed QoS, where typically QoS related parameters are changed. The parameters that may be modified are UE-AMBR, APN-AMBR QCI and Allocation/Retention Policy.

The HSS initiates the modification by sending an Insert Subscriber Data (IMSI, Subscription Data) message to the SGSN. The Subscription Data includes EPS subscribed QoS (QCI, ARP) and the subscribed UE-AMBR and APN AMBR.

The S4-SGSN then updates the stored Subscription Data and acknowledges the Insert Subscriber Data message by returning an Insert Subscriber Data Ack (IMSI) message to the HSS and sends the Modify Bearer Command (EPS Bearer Identity, EPS Bearer QoS, APN AMBR) message to the S-GW. The S-GW forwards the Modify Bearer Command (EPS Bearer Identity, EPS Bearer QoS, APN AMBR) message to the P-GW. Note that the EPS Bearer QoS sent in the Modify Bearer Command does not modify the per bearer bit-rate. It is sent to carry only a change in the ARP / QCI received from subscription. Also, the Modify Bearer Command can be sent only for the default bearer (primary PDP) in a PDN connection.

The P-GW modifies the default bearer of each PDN connection corresponding to the APN for which subscribed QoS has been modified. If the subscribed ARP parameter has been changed, the P-GW shall also modify all dedicated EPS bearers having the previously subscribed ARP value unless superseded by PCRF decision. The P-GW then sends the Update Bearer Request (EPS Bearer Identity, EPS Bearer QoS [if QoS is changed], TFT, APN AMBR) message to the S-GW.

The S-GW sends the Update Bearer Request (EPS Bearer Identity, EPS Bearer QoS [if QoS is changed] APN-AMBR, TFT) message to the SGSN. On completion of modification S4-SGSN acknowledges the bearer modification by sending the "Update Bearer Response (EPS Bearer Identity)" message to P-GW via S-GW. If the bearer modification fails, the P-GW deletes the concerned EPS Bearer.

Fallback from the S4 Interface to the Gn Interface

The S4-SGSN supports fallback the S4 interface and selects the Gn interface for the 1st PDP context activation if the APN DNS-SNAPTR resolution returns only a Gn address. This functionality allows the PDP context request to be completed when DNS resolution returns a GGSN address instead of a P-GW address.

This mechanism is applicable in the following cases:

- The UE is EPC-capable
- The UE's subscription has a GPRS subscription only (and not an EPS subscription)

If the subscription has an EPS subscription for an APN, then it is assumed that the P-GW addresses are configured in the DNS for that APN.

Operator Policy Selection of S4 or Gn Interface

The S4-SGSN supports Operator Policy selection of either the S4 or the Gn interface for PDP context operations. This feature allows flexible operator control over interface selection for operational or administrative reasons.

This functionality overrides any other criteria for selection of the P-GW or the GGSN for PDP contexts. This feature is applicable only for EPC-capable UEs.

IDFT Support During Connected Mode Handovers

The S4-SGSN supports the setup of indirect data forwarding tunnels (IDFT) between the eNodeB and the RNC via the SGW during connected mode handovers. This allows the S4-SGSN to support connected mode handovers between the UTRAN and E-UTRAN networks across the S3 interface.

Once enabled, IDFT is employed under the following conditions:

- **If the SGSN is the old node participating in the connected mode handover, then indirect data forwarding tunnels is used if**:
  - The target node to which the connected mode handover is initiated should be an eNodeB (i.e., the SGSN performs the handover to the MME).
  - The **enb-direct-data-forward** CLI setting is not configured as the source RNC configuration (in RNC Configuration Mode).
- **If the SGSN is the new node participating in the connected mode handover, then indirect data forwarding tunnels is employed if**:
  - The source node from which connected mode handover is initiated is an eNodeB (i.e., the MME is performing a handover to the SGSN).
  - The **enb-direct-data-forward** setting is not configured in the source RNC configuration (in RNC Configuration Mode).
  - The source MME indicated that it does not support direct forwarding via a Forward Relocation Request.

Important If the target SGSN did **not** relocate to a new SGW, IDFT does not apply. The target SGSN sets up an indirect data forwarding tunnel with SGW only if the SGW is relocated. If the SGW is not relocated, then it is the source MME that sets up the indirect data forwarding tunnel between source the eNodeB and target RNC through the SGW.

Disassociated DSR Support

The S4-SGSN supports the disassociation of the SGSN and EGTP applications for a Delete Session Request in a certain scenario. In this scenario, the SGSN application instructs the EGTP facility to send the Delete Session Request to the SGW and not respond back to the SGSN application to confirm the action. In effect, the SGSN application disassociates itself from the EGTP facility. Since the SGSN application is no longer waiting for a response from the EGTP facility, there will be reduced internal communication between the SGSN and EGTP. The the EGTP facility will handle retransmissions of the DSR request, thereby eliminating the possibility of hanging sessions at the SGSN.

The behavior of the disassociated DSR feature for each of the applicable scenarios follows:

1. The SGSN / MME wants to send a DSR with OI=0 and SI=1 to an old SGW during SGW relocation.
2. The SGSN application instructs the EGTP facility to inform the old SGW of the DSR and the SGSN doesn't expect any response from EGTP.
3. The EGTP facility handles retransmissions of this DSR request.

SGSN Serving Radio Network Subsystem (SRNS) Relocation Support

SRNS relocation is the method defined in 3GPP TS 23.401 for connected mode inter-RAT handovers from E-UTRAN to UTRAN or UTRAN to E-UTRAN networks. The SGSN already supports SRNS relocation across the Gn interface. The SGSN now also supports SRNS relocation with the following cases across the S3 (S4-SGSN to MME) and S16 (S4-SGSN to S4-SGSN) interfaces:

- Intra-SGSN SRNS relocation
- Inter-SGSN SRNS relocation over the S16 interface
- UTRAN-to-E-UTRAN connected mode Inter-RAT handover over the S3 interface
- UTRAN-to-E-UTRAN connected mode Inter-RAT handover over the S3 interface

The relocation feature is triggered by subscribers (MS/UE) moving between an eNodeB and an RNC. If the originating and destination nodes are connected to the same S4-SGSN but are in different routing areas, the behavior triggers an intra-SGSN Routing Area Update (RAU). If the nodes are connected to different S4-SGSNs, the relocation is followed by an inter-SGSN RAU.

As part of the SRNS relocation feature implementation on the S4-SGSN, the SGSN application also supports the gtpv2 (egtp) protocol for:

- Inter-SGSN SRNS relocations over the S16 interface
- MME - SGSN SRNS relocations over the S3 interface

A command is available to enable the SGSN to support SRNS relocation when the source RNC is behaving as the target RNC.

Configuration and Maintenance

The existing **srns-inter** and **srns-intra** commands in *Call Control Profile Configuration Mode* are used to enable this feature.

In addition, the **enb-direct-data forward** command in *RNC Configuration Mode* can be used to enable the S4-SGSN to apply direct forwarding tunnels or indirect data forwarding tunnels (IDFT) between a particular eNodeB and RNC.

Statistics are also available with the **show s4-sgsn statistics all** command that enable operators to track SGW relocations and SRNS procedure aborts.

E-UTRAN Service Handover Support

The SGSN supports configuration-based enabling of the E-UTRAN Service Handover Information Element, which is optional in the following RANAP messages used during SRNS relocation:

- RAB Assignment Request
- Relocation Request

This feature is useful in the following scenarios:

1. A UE is E-UTRAN capable, the PLMN is E-UTRAN capable, but the UE has not subscribed to EPS services (no 4G subscription available).
2. The VPLMN is E-UTRAN-capable, and the UE of an inbound roamer is E-UTRAN capable, but the UE has only a UTRAN/GERAN roaming agreement in place.

The feature ensures that an SRNS relocation handover to E-UTRAN is not allowed for E-UTRAN capable UEs that have only a UTRAN/GERAN roaming agreement. This results in an elimination of potential service denial or disruption issues, and unnecessary signaling.

To implement this feature, CLI commands have been implemented so that the SGSN can be configured to:

- Override the "eutran-not-allowed" flag received from the HLR/HSS in the ISD/ULA request for the Access Restriction Data (ARD) parameter (for scenario 2 above).
- Enable the inclusion of the E-UTRAN Service Handover IE in RAB Assignment Request and Relocation Request RANAP messages for scenarios 1 and 2 above).

Important SRNS relocation must be configured via the **srns-inter** and/or **srns-intra** commands in *Call Control Profile Configuration Mode* before configuring E-UTRAN Service Handover Support.

Support for Gn Handoff from S4-SGSN to 2G/3G Gn SGSN

The S4-SGSN supports handoffs from the S4-SGSN to a 2G/3G peer Gn/Gp SGSN as follows:

- An EPC capable UE is attached to an S4-SGSN and has PDP contexts towards the EPC core using the S4 interface.
- When the UE hands off to a Gn/Gp SGSN, the S4-SGSN transfers the PDP contexts to the peer SGSN using the GTPv1 protocol.

No CLI commands are require to implement this functionality.

Suspend/Resume Support on the S4-SGSN

The S4-SGSN Suspend/Resume feature provides support for suspend/resume procedures from the BSS and a peer S4-SGSN.

When a UE is in a 2G coverage area wants to make a circuit switched voice call but the Class A mode of operation is not supported by the network, then the packet switched data session (PDP contexts) must be suspended before the voice call can be made. In this case, the BSS sends a Suspend Request to the SGSN. If the UE is already attached at that SGSN then the suspend request is handled via an intra-SGSN suspend/resume procedure. If the UE is not attached at the SGSN then the Suspend Request is forwarded to a peer SGSN/MME through GTPv2 and an inter-SGSN/SGSN-MME suspend procedure occurs. Once the UE completes the voice call, either the BSS sends a resume request to resume the suspended PDPs or the UE directly sends a Routing Area Update Request (RAU) in 2G which will be treated as an implicit resume.

The ability for a GPRS user to access circuit-switched services depends on the subscription held, the network capabilities, and the MS capabilities.

For detailed information on this feature, refer to the *S4-SGSN Suspend/Resume Feature* chapter in this guide.

Flex Pooling (Iu / Gb over S16) Support on the S4-SGSN

This feature adds the SGSN Pooling functionality across S16 (peer S4-SGSN) interface, so that the default SGSN can forward the received Context Requests from the non-Pooled SGSN to the right pooled SGSN, based on the NRI in P-TMSI. Flex pooling provides better scalability and load balancing. A new CLI command for pooling has been provided under eGTP Service Configuration to enable S4-SGSN pooling across the S16 interface. For more information on the command, refer to the *Command Line Interface Reference Manual*.

This feature requires the SGSN S3/S4 license and Flex feature license - no additional feature licenses are required.

LORC Subscriber Overcharging Protection on S4-SGSN

With Release 17.0, the S4-SGSN now supports Subscriber Overcharging Protection to prevent both 2G and 3G subscribers from being overcharged when a loss of radio coverage (LORC) occurs over the S4 interface.

As a part of this functionality, the operator must configure all cause codes on the SGSN. If the SGSN receives a cause code via Iu/Gb interfaces that matches one of the cause codes configured on the SGSN, then the SGSN includes the ARRL (Abnormal Release of Radio Link) bit in the Release Access Bearer Request.

This feature ensures more accurate billing by protecting the subscriber from overcharging in instances where abnormal radio resource release occurs. For more information about this feature, refer to the feature chapter *LORC Subscriber Overcharging Protection on S4-SGSN* in this Guide.

Summary of Functional Differences between an S4-SGSN and an SGSN (Gn/Gp)

Since the S4-SGSN is configured with 2G, 3G, and/or dual access SGSN services before being configured with enhancements to enable communication with the EPC network, it shares similarities with a Gn/Gp SGSN. But, the S4-SGSN also contains a number of functional differences. The following table summarizes these differences.

Table 1: Summary of Functional Differences between SGSN and S4-SGSN

Procedure	Gn/Gp SGSN	S4-SGSN
MS Initiated First Primary PDP Context Activation	1. The requested QoS is negotiated with the subscribed QoS. The negotiated QoS is sent in the Create PDP Context Request.	1. The requested QoS is ignored if UE has EPS subscription. If EPS subscription is available SGSN always uses the subscribed EPS QoS to send in the Create Session Request. If there is no EPS subscription but the UE is still granted access to the S4 interface, then the system negotiates the requested QoS with the subscribed GPRS QoS. The S4-SGSN maps the negotiated QoS to EPS QoS as per as per the mapping table given in TS 23.203 Table 6.1.7 and TS 23.401 Annex E. and sends the Create Session Request. If the requested traffic class is conversational / streaming, then the system maps it to the interactive class as a primary PDP context. In S4-SGSN if QoS is downgraded by RNC during RAB establishment, then by default the PDP activation is rejected. This is as per section 9.2.2.1A of 23.060 step A below figure 64b. But S4-SGSN provides a CLI to locally accept the RAB negotiated QoS to override this spec defined behavior. 2. Two primary PDP contexts are for the same APN must be selected for the same P-GW.
MS Initiated Secondary PDP Context Activation	1. Secondary PDP context's requested QoS will be capped to the subscribed QoS. 2. Since the Create PDP Context is the message also used for creating the Secondary PDP context, ARP also is sent for secondary PDP context.	1. ARP is not sent in the Bearer Resource command. But it is sent by the P-GW in the Create Bearer Request.

Procedure	Gn/Gp SGSN	S4-SGSN
MS Initiated PDP Context Deactivation	1. Both single and bundle deactivation is allowed.	1. If a primary PDP context must be deactivated, only bundle deactivation is allowed.
GGSN/P-GW Initiated PDP Context Deactivation	1. The GGSN can deactivate the primary PDP context alone without initiating a bundle deactivation.	1. If the P-GW deactivates the primary PDP context (default bearer), it is treated as a bundle deactivation.
PDP Context Preservation for conversational/streaming class.	1. The SGSN sends the Update PDP Context Request to the GGSN with 0kbps as the Maximum Bit Rate value.	
PDP Context Preservation for interactive/background class.	1. The SGSN preserves the PDP context as it is.	1. The S4-SGSN preserves the PDP context as it is. 2. If a direct tunnel was established, or if ISR is active, then the S4-SGSN sends a Release Access Bearer Request to the S-GW.
RNC Initiated QoS Modification	1. The SGSN initiates the PDP Context Modification procedure.	1. The S4-SGSN ignores the RAB Modify Request received from the RNC.
Intra-SGSN Routing Area Update in PMM-Idle Mode	1. The SGSN sends the Update PDP Context Request to the GGSN if the PLMN changes.	1. An intra-SGSN RAU may involve a change of S-GW. 2. An S4-SGSN sends a Modify Bearer Request to the S-GW/P-GW if the RAU involves a change of PLMN and if the S-GW doesn't change.

Procedure	Gn/Gp SGSN	S4-SGSN
Intra SGSN RAU in PMM-CONNECTED Mode	1. The SGSN sends the Update PDP Context Request to the GGSN if the PLMN changes or if QoS changed due to an RNC release change.	1. An intra-SGSN RAU may involve a change of the S-GW. In 16.0 if QoS is changed during inter RNC handover (due to new RNC supporting a lower QoS range), then S4-SGSN internally caps the QoS towards RNC for non GBR bearers alone (interactive / background class). The changed QoS is not signalled to SGW / PGW. If there are GBR bearers (conversational / streaming class) that have a higher guaranteed bit rate than that can be supported by the target RNC, then such GBR bearers are deactivated. 2. However, in an S4-SGSN, the SGSN initiated modification procedure is defined only for changing of APN-AMBR. A change of RNC release will initiate a per bearer QoS change. There is no way to communicate this to the S-GW / P-GW.

Procedure	Gn/Gp SGSN	S4-SGSN
Old - Inter-SGSN RAU with no change in interface type across SGSNs.	Where both "old" and "new" refer to SGSNs (Gn/Gp): 1. The old SGSN orders the PDP contexts as per priority in the SGSN Context Response message. If the UE is PMM-CONNECTED in the old SGSN, then the old SGSN initiates an SRNS Context Transfer before sending the SGSN context response. In addition, the old SGSN initiates an SRNS Data Forward Command to the SRNS to transfer the unsent data from the old SRNS to the old SGSN.	Where both "old" and "new" refer to S4-SGSNs. 1. If the new S4-SGSN indicated that the S-GW has changed in the Context Ack message, then the old S4-SGSN has to initiate a Delete Session Request to the old S-GW with Scope Indication bit set. This Delete Session Request is locally consumed at old SGW and will not be forwarded to PGW. 2. The S4-SGSN does not support lossless PDCP for inter-SGSN handovers. If the UE was PMM-CONNECTED in the old S4-SGSN, then it will not initiate an SRNS Context Transfer before sending the Context Response. The assumption is that the SRNS relocation procedure had occurred prior to the inter-SGSN RAU for CONNECTED subscribers. 3. For inter S4-SGSN context transfers the Context Ack message doesn't carry any data TEID. That is, the GTPv2 protocol doesn't define any inter-SGSN data tunnel. Therefore, during connected mode, a RAU between two S4-SGSN without an SRNS relocation will result in packet losses. It is assumed that SRNS relocation is enabled in the UTRAN.

Procedure	Gn/Gp SGSN	S4-SGSN
Old - Inter SGSN RAU with change in interface across SGSN	Where "old" is SGSN (Gn/Gp) and "new" is S4-SGSN: 1. The old SGSN sends a SGSN context response with PDP contexts in prioritized order. 2. If the MS is in PMM-CONNECTED state in the old SGSN, it will initiate an SRNS Context Transfer towards the old SRNS and will initiate SRNS Data Forward Command to transfer unsent packets from old SRNS back to old SGSN. In the new SGSN, the PDPs will continue to use Gn interface. Promotion of PDPs to S4 post handover from a Gn SGSN is not yet supported.	Where "old" is S4-SGSN and "new" is SGSN (Gn/Gp): 1. The old S4-SGSN receives a GTPv1 SGSN Context Request and it converts the EPS bearer information to PDP contexts and responds with a SGSN Context Response towards the new SGSN. 2. The old S4-SGSN prioritizes the PDP contexts as per ARP. PDP prioritization for EPS bearers is not supported.
New Inter SGSN RAU for a PMM-IDLE subscriber without a change of interface	1. Uses the PDP context prioritized order in the SGSN Context Response to select high priority PDP contexts in the case of resource limitations at the new SGSN. 2. The SGSN ends the UPCQ to GGSN.	1. Performs the S-GW selection procedure. 2. Uses ARP to prioritize EPS bearers. In GTPv1 the PDP contexts sent in SGSN context response will be in prioritized order. But such an order is not defined for sending EPS bearers in Context Response. The idea is to use to ARP for prioritization. PDP prioritization for EPS bearers is not supported. 3. The new S4-SGSN alerts of any change in S-GW through the Context Ack to the old S4-SGSN. The PMM module will wait until the S-GW selection procedure is complete at the new S4-SGSN to alert of the context ack.

Procedure	Gn/Gp SGSN	S4-SGSN
New Inter SGSN RAU for a PMM-CONNECTED subscriber	Where "old" is S4-SGSN and "new" is SGSN (Gn/Gp): 1. The new SGSN receives PDP contexts in the SGSN Context Response in prioritized order. 2. RABs will be established at the new SGSN based on the ASI bit value for each PDP.	Where "new" is S4-SGSN and "old" is SGSN (Gn/Gp): 1. The new S4-SGSN receives PDP contexts in the Context Response. There is no prioritized order. ARP is used to prioritize. PDP prioritization for EPS bearers is not supported. 2. New S4-SGSN performs S-GW selection. 3. The new S4-SGSN cannot establish RAB as there is no ASI bit in the GTPv2 Context Response. The assumption is that the Context Req / Response is used only for IDLE mode handover, and that for connected mode handover, the SRNS relocation procedure should be used.
New SGSN PMM-CONNECTED / PMM-IDLE subscriber handover with interface change	Where "old" is S4-SGSN and "new" is SGSN (Gn/Gp): 1. The new S4-SGSN sends a GTPv1 SGSN Context Request and receives the PDP contexts mapped from EPS bearers in the SGSN context response. 2. The old SGSN will establish an inter-SGSN tunnel for transferring queued packets.	Where "old" is SGSN (Gn/Gp) and "new" is S4-SGSN: 1. The new S4-SGSN sends a GTPv1 SGSN context request, after learning that the old SGSN is an SGSN (Gn/Gp) based on a DNS S-NAPTR response. 2. The new S4-SGSN will continue to use the Gn interface for the PDPs. Conversion of PDPs to S4-SGSN is not supported at this time.
APN Selection Logic	1. No concept of subscribed default APN.	1. One among the subscribed APN will be indicated as a default APN by the HSS. That APN will be used under the following cases: 1) No requested APN, 2) The requested APN is not in the subscription but the requested PDP type matches with default APN's PDP type.

Procedure	Gn/Gp SGSN	S4-SGSN
DNS Queries	1. APN FQDN, RAI FQDN and RNC-ID FQDN are formed with a .gprs extension. 2. DNS A/AAAA records are queried. 3. Optionally, also uses S-NAPTR queries for EPC-capable UEs to select a co-located P-GW/GGSN	1. APN FQDN, RAI FQDN, RNC-ID FQDN are formed with a .3gppnetwork.org extension. 2. DNS S-NAPTR records are queried 3. If DNS SNAPTR response returns only Gn address, S4-SGSN will use Gn interface for selecting a PGW/GGSN.
Path Failure Detection	1. Can be echo-based or non-echo-based.	1. Echo-based only.
Charging	1. Applicable.	1. Charging for PDP contexts applicable only if CAMEL is used. However, the S4-SGSN will continue to generate M-CDRs. Also CAMEL is not supported in S4-SGSN now. Hence S4-SGSN only generates M-CDRs. PDP related CDRs are generated by SGW.

Procedure	Gn/Gp SGSN	S4-SGSN
Intra-SGSN Inter System Handover (2G to 3G or 3G to 2G Inter RAT handovers)	1. For 2G to 3G handovers, the RABs are not established in 3G after handover. It is the function of the UE to initiate Service Request procedure to setup RAB. 2. For 3G to 2G handovers, the QoS is capped to 472 Kbps in 2G and the Update PDP Context Request initiated from 2G will carry the capped QoS to GGSN.	1. For 2G to 3G handovers, the RABs are not established in 3G after the handover. The S4-SGSN preserves the PDP without deactivation. For 3G to 2G handover, the QoS is not capped to 472 Kbps in 2G. The reason is that in GTPv2 the Modify Bearer Request initiated from S4-SGSN upon 3G to 2G RAU is defined only for informing S-GW / P-GW of a switch in tunnel IDs and change in RAT type. This message doesn't carry QoS. The S4-SGSN relies on the P-GW + PCRF to decide the best QoS for the informed RAT type and lets the P-GW initiate a separate modification procedure to set the right QoS. In 16.0, during 3G to 2G handover, SGSN internally caps the APN-AMBR to 472 kbps and post handover, it initiates a Modify Bearer Command message to SGW/PGW. If there are any GBR bearers (conversational / streaming class) with bit rate greater than 472 kbps then those GBR bearer PDPs will be deactivated.
Direct Tunnel (DT) Activation	Configuration enabling DT is accomplished at various levels - the Call Control Profile level, the RNC level, and at the APN Profile level for DT per APN/GGSN. For a given UE, it is possible that one PDN connection to an APN to a GGSN uses DT while another PDN connection to a different APN to a different GGSN does not use DT. It all depends upon whether or not the target GGSN supports DT.	Configuration for DT is only available at Call Control Profile and RNC levels as the S4-SGSN's DT is between an SGW and an RNC. In an S4-SGSN, either all PDPs of a given UE use DT or none of them use DT. So, combinations of some PDPs using DT and some PDPs not using DT is not possible.

Procedure	Gn/Gp SGSN	S4-SGSN
Handling Suspend from BSS / peer SGSN	PDPs are suspended at SGSN. Any downlink data received at this point will be queued by the SGSN.	PDPs are suspended at SGSN. Downlink data buffering happens at the PGW and not the SGSN because the PDP suspension is carried via a GTPv2 Suspend Notification message from the SGSN to the SGW to the PGW.

Session Recovery

Session recovery provides a seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault that prevents a fully attached user session from having the PDP contexts removed or the attachments torn down.

Session recovery is performed by mirroring key software processes (e.g., session manager and AAA manager) within the system. These mirrored processes remain in an idle state (in standby-mode) until they may be needed in the case of a software failure (e.g., a session manager task aborts). The system spawns new instances of "standby mode" session and AAA managers for each active control processor (CP) being used.

As well, other key system-level software tasks, such as VPN manager, are performed on a physically separate packet processing card to ensure that a double software fault (e.g., session manager and VPN manager fail at the same time on the same card) cannot occur. The packet processing card used to host the VPN manager process is in active mode and is reserved by the operating system for this sole use when session recovery is enabled.

The additional hardware resources required for session recovery include a standby System Management Card and a standby packet processing card.

There are two modes for Session Recovery.

- **Task recovery mode:** One or more session manager failures occur and are recovered without the need to use resources on a standby packet processor card. In this mode, recovery is performed by using the mirrored "standby-mode" session manager task(s) running on active packet processor cards. The "standby-mode" task is renamed, made active, and is then populated using information from other tasks such as AAA manager.
- **Full packet processing card recovery mode:** Used when a packet processing card hardware failure occurs, or when a packet processor card migration failure happens. In this mode, the standby packet processor card is made active and the "standby-mode" session manager and AAA manager tasks on the newly activated packet processor card perform session recovery.

Session/Call state information is saved in the peer AAA manager task because each AAA manager and session manager task is paired together. These pairs are started on physically different packet processor cards to ensure task recovery.

When session recovery occurs, the system reconstructs the following subscriber information:

- Data and control state information required to maintain correct call behavior
- Subscriber data statistics that are required to ensure that accounting information is maintained
- A best-effort attempt to recover various timer values such as call duration, absolute time, and others

For more information on session recovery use and session recovery configuration, refer to the *Session Recovery* section in the *System Administration Guide*.

SCTP Parameters for SGSN

The details on the configurable values for SCTP parameters are provided in the table given below:

Parameter	Minimum value	Maximum value	Granularity
RTO.min	10ms	5s	10ms
RTO.max	500ms	120s	10ms
RTO.initial	RTO.min	RTO.max	10ms
RTO.alpha	1/8	1/8	-
RTO.beta	1/4	1/4	-
Valid.Cookie.Life	5s	120s	1s
HB.interval	1s	300s	1s
SACK period	0ms	500ms	10ms
SACK frequency	1	5	1
MTU size	508 bytes	65535 bytes	1 byte

The details on the default values for SCTP parameters are provided in the table given below:

Parameter	Default Value
RTO Alpha	5
RTO Beta	10
Valid Cookie Life	600
Max. associate retransmission value	10
Max. number of outgoing streams	16
Max. number of incoming streams	16
Max. retransmission initiations	5
Max. MTU size	1500
Min. MTU size	508
Start MTU	1500
Max. path retransmission	5
RTO Initital	30
RTO Max	600

Parameter	Default Value
RTO Min	10
HB interval	30
HB enable	True
SACK period	2
SACK frequency	2
Bundle valid	True
Bundle enable	False

SGSN Pooling and Iu-Flex / Gb-Flex

This implementation allows carriers to load balance sessions among pooled SGSNs, to improve reliability and efficiency of call handling, and to use Iu-Flex / Gb-Flex to provide carriers with deterministic failure recovery.

The SGSN, with its high capacity, signaling performance, and peering capabilities, combined with its level of fault tolerance, delivers many of the benefits of Flex functionality even without deploying SGSN pooling.

As defined by 3GPP TS 23.236, the SGSN implements Iu-Flex and Gb-Flex functionality to facilitate network sharing and to ensure SGSN pooling for 2.5G and 3G accesses as both separate pools and as dual-access pools.

SGSN pooling enables the following:

- Eliminates the single point of failure between an RNC and an SGSN or between a BSS and an SGSN.
- Ensures geographical redundancy, as a pool can be distributed across sites.
- Minimizes subscriber impact during service, maintenance, or node additions or replacements.
- Increases overall capacity via load sharing across the SGSNs in a pool.
- Reduces the need/frequency for inter-SGSN RAUs. This substantially reduces signaling load and data transfer delays.
- Supports load redistribution with the SGSN offloading procedure.

The SGSN Pooling and Iu-Flex / Gb-Flex feature is license controlled. Contact your Cisco Account or Support representative for information on how to obtain a license.

Gb/Iu Flex Offloading

The SGSN supports Gb/Iu Flex subscriber offloading from one SGSN to another specific SGSN in a 2G/3G pool.

In addition, the operator can configure the offloading Target NRI in P-TMSI, and the quantity to offload to the Target. This can be used to provide load balancing, or to offload a single node in pool, take it out of service for whatever reason (e.g., maintenance).

SGSN Supports Enhanced IMSI Range

From release 19.0 onwards, the IMSI range supported has been enhanced to "2500" from "1000". The IMSI ranges configured must be unique; the SGSN selects the appropriate operator policy based on the IMSI range of the UE. The operator can verify the configured IMSI ranges and the associated operator policy by issuing the command "show config". The length of the description field in the imsi-range command under the SGSN Global Configuration mode has been reduced from a maximum of "100" alphanumeric characters to "50" alphanumeric characters. Reduction of the supported string size results in improvement of the boot up time.

SGSN Support for RAI Based Query

The SGSN now supports a RAI based query when NRI based query fails. A new CLI option **rai-fqdn-fallback** is provided in the **peer-nri-length** CLI under the Call Control Profile Configuration, which allows the operator to configure the SGSN's support to fallback on RAI based query when NRI based query fails.

This feature is not supported in the following scenarios:

- 2G Context Request and Identification Request messages are not supported.
- S4 support of this extensions for all applicable scenarios is not supported.

SGSN Support For Sending Extended Bits Bi-directionally

The SGSN now supports sending extended bitrates in both uplink and downlink directions. Extended bitrates are included in both uplink and downlink direction when the negotiated birate indicates that extended birates should be included in one direction. A new CLI **ranap bidirectional-always ext-mbr-ie** is added under the RNC Configuration mode to enable sending extended bitrates bi-directionally.

SGSN support to Ignore PDP Data Inactivity

The SGSN supports options to configure PDP Data Inactivity detection duration and actions to be performed on timeout under the APN-Profile. The following configurable actions are supported under APN-Profile in case of PDP Data Inactivity detection in the PDP context:

1. De-activate all PDPs of the subscriber
2. De-activate all PDPs of the bundle (all linked PDPs)
3. Detach the subscriber. This action is triggered when:
    - Data in-activity is detected for all PDPs
    - Data in-activity is detected for any of the PDPs

On the Detection of the PDP Data Inactivity, depending on the configuration option the SGSN either de-activates the PDP or detaches the subscriber.

A new CLI **ignore-pdp-data-inactivity** is added to provide an option under the IMEI-Profile to ignore PDP Data Inactivity configuration for one or more IMEIs. On configuring this CLI, the SGSN ignores the application of in-activity configuration (configured in the APN-Profile) for a specified set of IMEI's.

Important The IMEI range or set of IMEI's are mapped to specific IMEI-Profile using the CLI configuration option under Operator-policy.

For more information on the command see. Command Line Interface Reference.

Short Message Service (SMS over Gd)

The SGSN implements a configurable Short Message Service (SMS) to support sending and receiving text messages up to 140 octets in length. The SGSN handles multiple, simultaneous messages of both types: those sent from the MS/UE (SMS-MO: mobile originating) and those sent to the MS/UE (SMS-MT: mobile terminating). Short Message Service is disabled by default.

After verifying a subscription for the PLMN's SMS service, the SGSN connects with the SMSC (short message service center), via a Gd interface, to relay received messages (from a mobile) using MAP-MO-FORWARD-REQUESTs for store-and-forward.

In the reverse, the SGSN awaits messages from the SMSC via MAP-MT-FORWARD-REQUESTs and checks the subscriber state before relaying them to the target MS/UE.

The SGSN will employ both the Page procedure and MNRG (mobile not reachable for GPRS) flags in an attempt to deliver messages to subscribers that are absent.

The SGSN supports

- charging for SMS messages, and
- lawful intercept of SMS messages

For information on configuring and managing the SMS, refer to the *SMS Service Configuration Mode* section in the *Command Line Interface Reference*.

SMS Authentication Repetition Rate

The SGSN provides an authentication procedures for standard GMM events like Attach, Detach, RAU, and Service-Request, and SMS events such as Activate, all with support for 1-in-N Authenticate functionality. The SGSN did not provide the capability to authenticate MO/MT SMS events.

Now, the authentication functionality has been expanded to the Gs interface where the SGSN now supports configuration of the authentication repetition rate for SMS-MO and SMS-MT, for every nth event. This functionality is built on existing SMS CLI, with configurable MO and/or MT. The default is not to authenticate.

SMSC Address Denial

Previously, the SGSN supported restricting MO-SMS and MT-SMS only through SGSN operator policy configuration.

Now, the SGSN can restrict forwarding of SMS messages to specific SMSC addresses, in order to allow operators to block SMS traffic that cannot be charged for. This functionality supports multiple SMSCs and is configurable per SMSC address with a maximum of 10 addresses. It is also configurable for MO-SMS and/or MT-SMS messages.

Status Updates to RNC

During MMGR recovery due to memory overload or demux migration leads to missing status updates for RNC.As the result RNC status remains unavailable even when links towards RNC are up. The Session Controller allows the Standby Session Managers along with Active Session Managers to fetch the status updates.

Target Access Restricted for the Subscriber Cause Code

This enhancement is a 3GPP TS (29.274 and 29.060) release compliance enhancement. As per 3GPP TS 29.274 and TS 29.060,the source-serving node (MME/SGSN) is allowed to reject SGSN Context Request (GTPv1) and Context Request (GTPv2) mobility management messages with "Target Access Restricted for the subscriber" cause if target access is restricted for the subscriber based on the Access-Restriction-Data in the subscription profile. The target node (MME/SGSN) is allowed to reject RAU/TAU with anyone one of the following NAS Causes:

- 15 "No suitable cells in tracking area", or
- 13 "Roaming not allowed in this tracking area", or
- 12 "Tracking area not allowed"

New statistics have been introduced under "show egtpc statistics verbose" and "show sgtpc statistics verbose" to reflect the context response sent and received with the new reject cause "Target Access Restricted for the subscriber".

Rejecting RAU/TAU much early in call cycle results in reduced signaling.

Important No new CLI is provided for GTP cause code mapping to EMM/NAS cause. RAU Reject will always be sent with NAS cause "No suitable cells in location area" and TAU Reject will always be sent with EMM cause "No suitable cells in Tracking Area".

Important The MME and SGSN revert to the old behavior as per earlier releases if the peer node is not capable of sending the RAT-TYPE IE in CONTEXT-REQ message.

For more information refer to the 3GPP TS 29.274 (section 7.3.6), TS 29.060 (section 7.5.4), TS 29.060 Annex B (Table B.5: Mapping from Gn/Gp to NAS Cause values Rejection indication from SGSN) and TS 29.274 Annex C (Table C.5: Mapping from S3/S16 to NAS Cause values Rejection indication from MME/S4-SGSN)

Topology-based Gateway (GW) Selection

Topology-based gateway selection is a mechanism defined by 3GPP to choose a gateway based on the geographical (topological) proximity of the GGSN to the SGSN or the P-GW to the S-GW. The two being co-located would have the highest priority. Topology-based selection is not allowed for roamers connected to HPLMN access points (Home Routed Scenario).

DNS S-NAPTR returns a candidate list of GW nodes for each of the DNS queries. 3GPP TS 29.303 provides an algorithm to feed these candidate lists and choose the topologically closer nodes among them. S-NAPTR DNS query is supported by default on the S4-SGSN and, with Release 16, can be enabled for the Gn/Gp-SGSN.

The SGSN's Topology-based GW Selection feature supports two levels of sorting, first level is degree and second level is order/priority, where order is for NAPTR records and priority is for SRV Records. Degree has the highest preference.

For details on the use and configuration of this feature, refer to the *Topology-based Gateway Selection* section in the *SGSN Administration Guide*.

Threshold Crossing Alerts (TCA) Support

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

The system supports Threshold Crossing Alerts for certain key resources such as CPU, memory, number of sessions etc. With this capability, the operator can configure threshold on these resources whereby, should the resource depletion cross the configured threshold, a SNMP Trap would be sent.

The following thresholding models are supported by the system:

- **Alert**: A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.
- **Alarm**: Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values.

Generation of specific traps can be enabled or disabled on the chassis. Ensuring that only important faults get displayed. SNMP traps are supported in both Alert and Alarm modes.

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

Logs are supported in both the Alert and the Alarm models.

- **Alarm System**: High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists or a condition clear alarm is generated. "Outstanding" alarms are reported to the system's alarm subsystem and are viewable through the Alarm Management menu in the Web Element Manager.

The Alarm System is used only in conjunction with the Alarm model.

Important For more information on threshold crossing alert configuration, refer to the *Thresholding Configuration Guide*.

Tracking Usage of GEA Encryption Algorithms

GPRS encryption algorithm (GEA) significantly affects the SGSN processing capacity based on the GEAx level used - GEA1, GEA2, or GEA3.

Operators would like to be able to identify the percentages of their customer base that are using the various GEA encryption algorithms. The same tool can also track the migration trend from GEA2 to GEA3 and allow an operator to forecast the need for additional SGSN capacity.

New fields and counters have been added to the output generated by the **show subscribers gprs-only|sgsn-only summary** command. This new information enables the operator to track the number of subscribers capable of GEA0-GEO3 and to easily see the number of subscribers with negotiated GEAx levels.

Validation of MCC/MNC Values in the Old RAI Field

This feature is developed to comply with 3GPP TS 24.008. As per 3GPP TS 24.008, in some abnormal instances the MCC stored in the Mobile Station (MS) contains elements which do not belong to the set {0, 1 ... 9}. In such cases the Mobile Station should transmit the stored values using full hexadecimal encoding. When receiving such an MCC, the network should treat the RAI as deleted. In some instances it is possible that the MNC stored in the Mobile Station has the following:

- Digit 1 or 2 not in the set {0, 1 ... 9}
- Digit 3 not in the set {0, 1 ... 9, F} hex

In such cases the MS should transmit the stored values using full hexadecimal encoding. When receiving such an MNC, the network should treat the RAI as deleted. The same handling is applicable for a network where a 3-digit MNC is sent by the mobile station to a network using only a 2-digit MNC.

A validation check has been introduced to verify the MCC and MNC fields received in the old RAI IE in Attach/RAU requests. When the MCC and MNC fields received in the RAU request (inter-SGSN) and are invalid, the RAU request is rejected by SGSN. When the MCC and MNC fields received in the Attach Request and are invalid, the identity of the MS is retrieved directly from the MS instead of sending identity request to the peer node where peer SGSN identity is derived from the old-RAI.

Important These feature is applicable for both 2G and 3G networks.

A new CLI command **[no] rai-skip-validation** has been introduced under both IuPS service and GPRS service configuration modes. This new command enables/disables rejection of RAU requests with invalid MCC/MNC values in the old RAI field. By default the old RAI MCC/MNC fields are validated. This command also impacts the PTMSI attaches where the old RAI field is invalid. If the OLD RAI field is invalid and if the validation is enabled through the new CLI command, the identity of the MS is requested directly from the MS instead of the peer SGSN.

VLR Pooling via the Gs Interface

VLR Pooling, also known as Gs Pooling, helps to reduce call delays and call dropping, when the MS/UE is in motion, by routing a service request to a core network (CN) node with available resources.

VLR pools are configured in the Gs Service, which supports the Gs interface configuration for communication with VLRs and MSCs.

A *pool area* is a geographical area within which an MS/UE can roam without the need to change the serving CN node. A pool area is served by one or more CN nodes in parallel. All the cells, controlled by an RNC or a BSC belong to the same one (or more) pool area(s).

VLR hash is used when a pool of VLRs is serving a particular LAC (or list of LACs). The selection of VLR from this pool is based on the IMSI digits. From the IMSI, the SGSN derives a hash value (V) using the algorithm: [(IMSI div 10) modulo 1000]. Every hash value (V) from the range 0 to 999 corresponds to a single MSC/VLR node. Typically many values of (V) may point to the same MSC/VLR node.

For commands to configure the VLR and pooling, refer to the "Gs Service Configuration Mode" section in the *Command Line Interface Reference*.

Synchronization of Crash Events and Minicores between Management Cards

The crash log is unique to each of the management cards, so if a crash occurs when card the "8" is active it will be logged on card "8". A subsequent switch-over would no longer display the crash in the log. To retrieve this crash, a switch back over to card "8" has to be done. The crash event log and dumps are unique to active and standby management cards, so if a crash occurs on an active card then the crash event log and related dumps will be stored on an active card only. This crash information is not available on the standby card. Whenever the cards switchover due to a crash in the active card, and crash information is no longer displayed on the card which takes over. Crash information can be retrieved only from the current active card. To retrieve the crash list of the other card a switch-over is required again. To avoid this switch-over and to obtain the crash information from the standby card, synchronization between two management cards and maintaining latest crash information is required.

The arriving crash event will be sent over to the standby SMC/MMIO and saved in the standby's crashlog file in the similar manner. Minicore, NPU or kernel dumps on flash of active SMC/MMIO needs to be synchronized to standby SMC/MMIO using the 'rsync' command. When a crash log entry or the whole list is deleted through the CLI command, it should be erased on both active and standby SMCs/MMIOs. There is no impact on memory. All the crash related synchronization activity will be done by the evlogd of standby SMC/MIO card, as the standby evlogd is less loaded and the standby card has enough room for synchronization activity. Therefore the performance of the system will not be affected.

Zero Volume S-CDR Suppression

This feature is developed to suppress the CDRs with zero byte data count, so that the OCG node is not overloaded with a flood of CDRs. The CDRs can be categorized as follows:

- Final-cdrs: These CDRs are generated at the end of a context.
- Internal-trigger-cdrs: These CDRs are generated due to internal triggers such as volume limit, time limit, tariff change or user generated interims through the CLI commands.
- External-trigger-cdrs: These CDRs are generated due to external triggers such as QoS Change, RAT change and so on. All triggers which are not considered as final-cdrs or internal-trigger-cdrs are considered as external-trigger-cdrs.

The customers can select the CDRs they want to suppress. A new CLI command **[no] [default] gtpp suppress-cdrs zero-volume { external-trigger-cdr | final-cdr | internal-trigger-cdr }**is developed to enable this feature. This feature is disabled by default to ensure backward compatibility. For more information see, *Command Line Interface Reference* and *Statistics and Counters Reference*.

Important This is a license controlled feature.

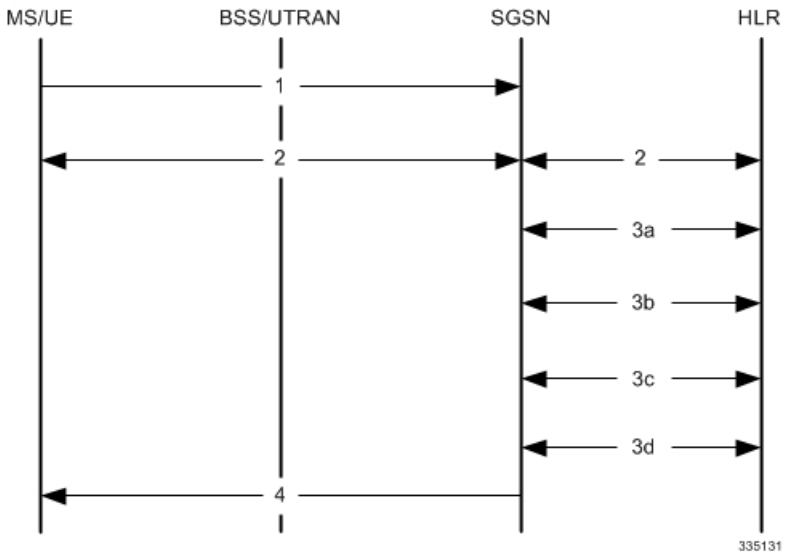
How the SGSN Works

This section illustrates some of the GPRS mobility management (GMM) and session management (SM) procedures the SGSN implements as part of the call handling process. All SGSN call flows are compliant with those defined by 3GPP TS 23.060.

First-Time GPRS Attach

The following outlines the setup procedure for a UE that is making an initial attach.

Figure 8: Simple First-Time GPRS Attach



This simple attach procedure can connect an MS via a BSS through the Gb interface (2.5G setup) or it can connect a UE via a UTRAN through the Iu interface in a 3G network with the following process:

Table 2: First-Time GPRS Attach Procedure

Step	Description
1	The MS/UE sends an Attach Request message to the SGSN. Included in the message is information, such as: • Routing area and location area information • Mobile network identity • Attach type

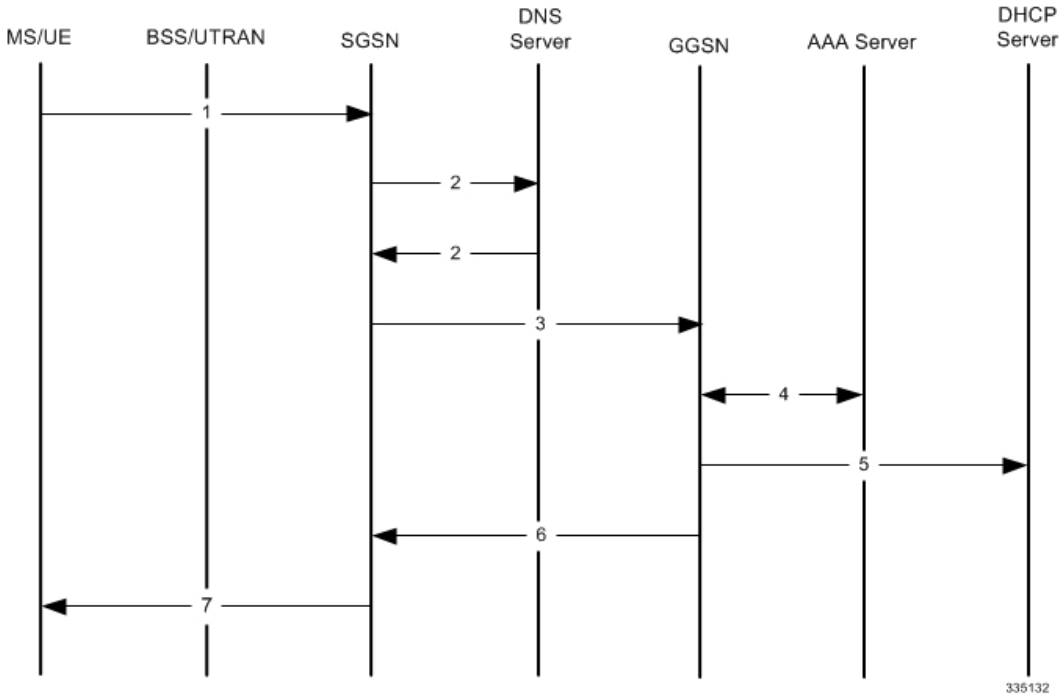
Step	Description
2	Authentication is mandatory if no MM context exists for the MS/UE: • The SGSN gets a random value (RAND) from the HLR to use as a challenge to the MS/UE. • The SGSN sends a Authentication Request message to the UE containing the random RAND. • The MS/UE contains a SIM that contains a secret key (Ki) shared between it and the HLR called a Individual Subscriber Key. The UE uses an algorithm to process the RAND and Ki to get the session key (Kc) and the signed response (SRES). • The MS/UE sends a Authentication Response to the SGSN containing the SRES.
3	The SGSN updates location information for the MS/UE: a) The SGSN sends an Update Location message, to the HLR, containing the SGSN number, SGSN address, and IMSI. b) The HLR sends an Insert Subscriber Data message to the "new" SGSN. It contains subscriber information such as IMSI and GPRS subscription data. c) The "New" SGSN validates the MS/UE in new routing area: If invalid: The SGSN rejects the Attach Request with the appropriate cause code. If valid: The SGSN creates a new MM context for the MS/UE and sends a Insert Subscriber Data Ack back to the HLR. d) The HLR sends a Update Location Ack to the SGSN after it successfully clears the old MM context and creates new one
4	The SGSN sends an Attach Accept message to the MS/UE containing the P-TMSI (included if it is new), VLR TMSI, P-TMSI Signature, and Radio Priority SMS. At this point the GPRS Attach is complete and the SGSN begins generating M-CDRs.

If the MS/UE initiates a second call, the procedure is more complex and involves information exchanges and validations between "old" and "new" SGSNs and "old" and "new" MSC/VLRs. The details of this combined GPRS/IMSI attach procedure can be found in 3GPP TS23.060.

PDP Context Activation Procedures

The following figure provides a high-level view of the PDP Context Activation procedure performed by the SGSN to establish PDP contexts for the MS with a BSS-Gb interface connection or a UE with a UTRAN-Iu interface connection.

Figure 9: Call Flow for PDP Context Activation



The following table provides detailed explanations for each step indicated in the figure above.

Table 3: PDP Context Activation Procedure

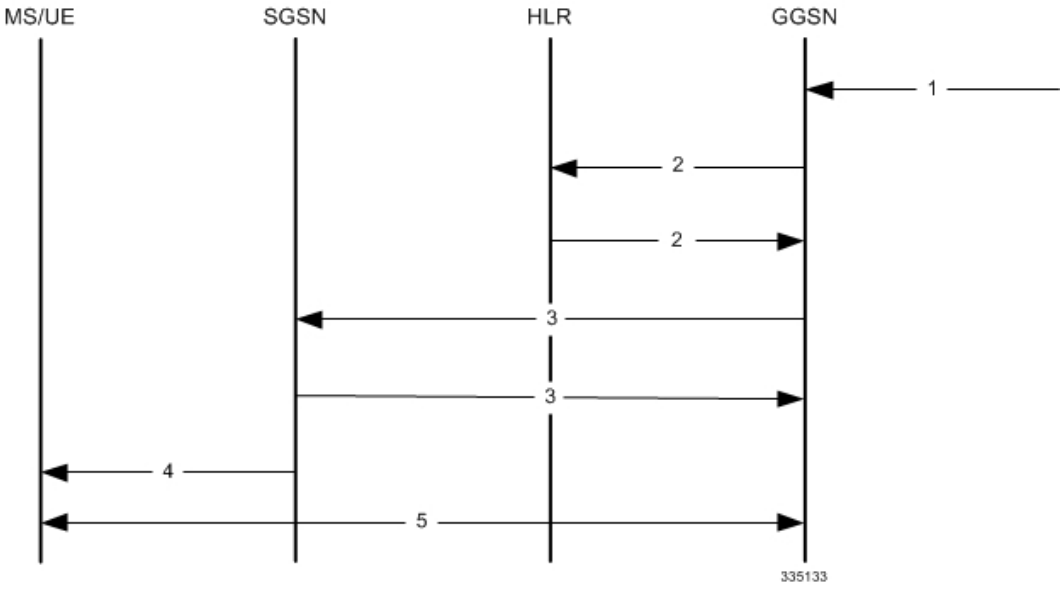
Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).
2	The SGSN sends a DNS query to resolve the APN provided by the MS/UE to a GGSN address. The DNS server provides a response containing the IP address of a GGSN.
3	The SGSN sends a Create PDP Context Request message to the GGSN containing the information needed to authenticate the subscriber and establish a PDP context.
4	If required, the GGSN performs authentication of the subscriber.

Step	Description
5	If the MS/UE requires an IP address, the GGSN may allocate one dynamically via DHCP.
6	The GGSN sends a Create PDP Context Response message back to the SGSN containing the IP Address assigned to the MS/UE.
7	The SGSN sends a Activate PDP Context Accept message to the MS/UE along with the IP Address. Upon PDP Context Activation, the SGSN begins generating S-CDRs. The S-CDRs are updated periodically based on Charging Characteristics and trigger conditions. A GTP-U tunnel is now established and the MS/UE can send and receive data.

Network-Initiated PDP Context Activation Process

In some cases, the GGSN receives information that requires it to request the MS/UE to activate a PDP context. The network, or the GGSN in this case, is not actually initiating the PDP context activation -- it is requesting the MS/UE to activate the PDP context in the following procedure:

Figure 10: Network-Initiated PDP Context Activation



The table below provides details describing the steps indicated in the graphic above.

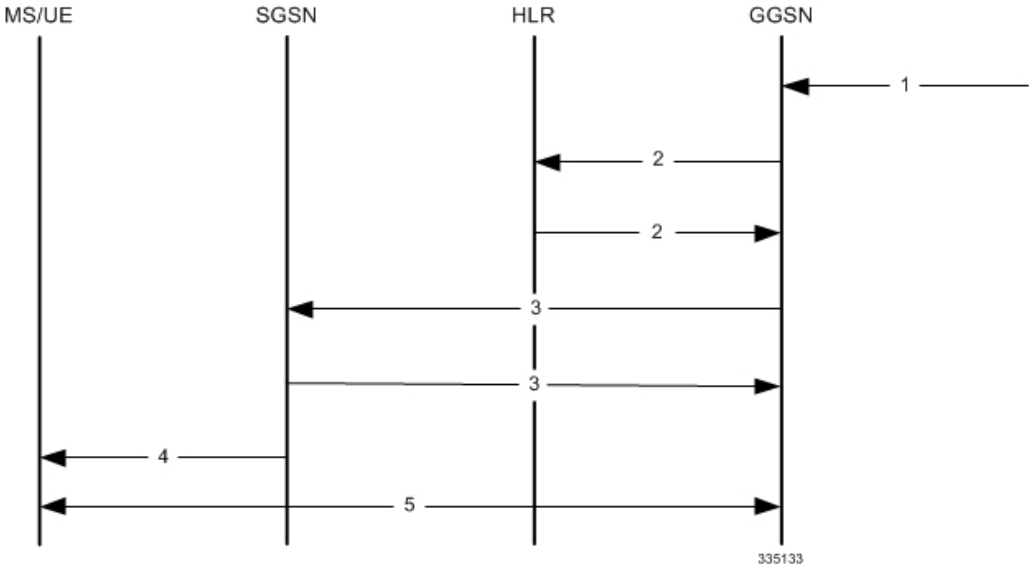
Table 4: Network Invites MS/UE to Activate PDP Context

Step	Description
1	The GGSN receives a PDU with a static PDP address that the GGSN 'knows' is for an MS/UE in its PLMN.
2	The GGSN uses the IMSI in place of the PDP address and sends an SRI (send routing information for GPRS) to the HLR. The HLR sends an SRI response back to the GGSN. The response may include the access of the target SGSN and it may also indicate it the MS/UE is not reachable, in which case it will include the reason in the response message.
3	The GGSN sends a PDU Notification Request to the SGSN (if the address was received). If the address was not received or if the MS/UE continues to be unreachable, the GGSN sets a flag marking that the MS/UE was unreachable. The notified SGSN sends a PDU Notification Response to the GGSN.
4	The SGSN determines the MS UE's location and sets up a NAS connection with the MS/UE. The SGSN then sends a Request PDP Context Activation message to the MS/UE.
5	If the MS/UE accepts the invitation to setup a PDP context, the MS/UE then begins the PDP context activation process indicated in the preceding procedure.

MS-Initiated Detach Procedure

This process is initiated by the MS/UE for a range of reasons and results in the MS/UE becoming inactive as far as the network is concerned.

Figure 11: MS-Initiated Combined GPRS/IMSI Detach



The following table provides details for the activity involved in each step noted in the diagram above.

Table 5: MS-Initiated Combined GPRS/IMSI Detach Procedure

Step	Description
1	The UE sends a Detach Request message to the SGSN containing the Detach Type, P-TMSI, P-TMSI Signature, and Switch off indicator (i.e. if UE is detaching because of a power off).
2	The SGSN sends Delete PDP Context Request message to the GGSN containing the TEID. The GGSN sends a Delete PDP Context Response back to the SGSN. The SGSN stops generating S-CDR info at the end of the PDP context.
3	The SGSN sends a IMSI Detach Indication message to the MSC/VLR.
4	The SGSN sends a GPRS Detach Indication message to the MSC/VLR. The SGSN stops generating M-CDR upon GPRS Detach.
5	If the detach is not due to a UE switch off, the SGSN sends a Detach Accept message to the UE.
6	Since the UE GPRS Detached, the SGSN releases the Packet Switched Signaling Connection.

Supported Standards

The SGSN services comply with the following standards for GPRS/UMTS and EPC wireless data services.

IETF Requests for Comments (RFCs)

- **RFC-1034,** Domain Names - Concepts and Facilities, November 1987; 3GPP TS 24.008 v7.8.0 (2007-06)
- **RFC-1035,** Domain Names - Implementation and Specification, November 1987; 3GPP TS 23.003 v7.4.0 (2007-06)
- **RFC-2960,** Stream Control Transmission Protocol (SCTP), October 2000; 3GPP TS 29.202 v6.0.0 (2004-12)
- **RFC-3332,** MTP3 User Adaptation Layer (M3UA), September 2002; 3GPP TS 29.202 v6.0.0 (2004-12)
- **RFC-4187,** Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), January 2006
- **RFC-4666,** Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) - User Adaptation Layer (M3UA), September 2006; 3GPP TS 29.202 v6.0.0 (2004-12)

3GPP Standards

Table 6: 3GPP Standards Supported

3GPP Standard	R21.2	R21.3	R21.4
3GPP TS 9.60, 3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface (R98).	v7.10.0 (2002-12)	v7.10.0 (2002-12)	v7.10.0 (2002-12)
3GPP TS 22.041, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Operator Determined Barring (ODB)	v9.0.0 (2009-12)	v9.0.0 (2009-12)	v9.0.0 (2009-12)

3GPP Standard	R21.2	R21.3	R21.4
3GPP TS 22.042, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Identity and Timezone (NITZ); Service description, Stage 1	v9.0.0 (2009-12)	v9.0.0 (2009-12)	v9.0.0 (2009-12)
3GPP TS 23.003, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification	v10.5.0 (2012-03)	v10.5.0 (2012-03)	v10.5.0 (2012-03)
3GPP TS 23.007, 3rd Generation Partnership Project; Technical Specification Group Core Network; Restoration procedures	v11.8.0 (2014-03)	v11.8.0 (2014-03)	v11.8.0 (2014-03)
3GPP TS 23.015, 3rd Generation Partnership Project; Technical Specification Group Core Network; Technical realization of Operator Determined Barring (ODB)	v9.0.0 (2009-12)	v9.0.0 (2009-12)	v9.0.0 (2009-12)
3GPP TS 23.016, 3rd Generation Partnership Project; Technical Specification Group Core Network; Subscriber data management; Stage 2	v9.1.0 (2010-03)	v9.1.0 (2010-03)	v9.1.0 (2010-03)
3GPP TS 23.040, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Technical realization of the Short Message Service (SMS)	v9.3.0 (2010-09)	v9.3.2 (2010-09)	v9.3.2 (2010-09)

3GPP Standard	R21.2	R21.3	R21.4
3GPP TS 23.060, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2	v11.9.0 (2014-03)	v11.9.0 (2014-03)	v11.9.0 (2014-03)
3GPP TS 23.078, 3rd Generation Partnership Project; Technical Specification Group Core Network; Customized Applications for Mobile network Enhanced Logic (CAMEL) Phase 3 - Stage 2 (Release 4)	v4.11.1 (2004-04)	v4.11.1 (2004-04)	v4.11.1 (2004-04)
3GPP TS 23.107, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture	v9.3.0 (2011-12)	v12.0.0 (2011-12)	v12.0.0 (2011-12)
3GPP TS 23.236, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Intra-domain connection of Radio Access Network (RAN) nodes to multiple Core Network (CN) nodes	v11.0.0(2012-09)	v11.0.0(2012-09)	v11.0.0(2012-09)
3GPP TS 23.251, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Sharing; Architecture and functional description	v10.5.0 (2012-12)	v10.5.0 (2012-12)	v10.5.0 (2012-12)

3GPP Standard	R21.2	R21.3	R21.4
3GPP TS 23.271, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Functional stage 2 description of Location Services (LCS) (Release 9)	v9.6.0 (2011-03)	v9.6.0 (2011-03)	v9.6.0 (2011-03)
3GPP TS 23.401, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 9)	v11.9.0 (2014-03-10)	v10.8.0 (2014-03-10)	v10.8.0 (2014-03-10)
3GPP TS 24.007, 3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile radio interface signalling layer 3; General aspects	v10.0.0 (2011-03)	v10.0.0 (2011-03)	v10.0.0 (2011-03)
3GPP TS 24.008, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3	v11.8.0 (2013-09)	v11.8.0 (2013-09)	v11.8.0 (2013-09)
3GPP TS 24.011, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface (Release 7)	v7.1.0 (2009-2006)	v7.1.0 (2009-2006)	v7.1.0 (2009-2006)

3GPP Standard	R21.2	R21.3	R21.4
3GPP TS 24.030, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 9)	v10.0.0 (2011-04)	v10.0.0 (2011-04)	v10.0.0 (2011-04)
3GPP TS 24.080, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile radio interface layer 3 supplementary services specification; Formats and coding (Release 9)	v9.2.0 (2010-06)	v9.2.0 (2010-06)	v9.2.0 (2010-06)
3GPP TS 25.410, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu Interface: general aspects and principles	v9.0.1 (2011-03)	v9.0.1 (2011-03)	v9.0.1 (2011-03)
3GPP TS 25.411, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface layer 1	v9.0.1 (2011-03)	v9.1.0 (2011-03)	v9.1.0 (2011-03)
3GPP TS 25.412, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface signaling transport	v9.0.1 (2011-03)	v9.0.1 (2011-03)	v9.0.1 (2011-03)

3GPP Standard	R21.2	R21.3	R21.4
3GPP TS 25.413, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface RANAP signalling (Release 9)	12.0.0 (2013-12)	12.0.0 (2013-12)	12.0.0 (2013-12)
3GPP TS 25.414, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface data transport and transport signaling	v9.0.1 (2011-03)	v9.1.0 (2011-03)	v9.1.0 (2011-03)
3GPP TS 25.415, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface user plane protocols	v9.0.1 (2011-03)	v9.0.1 (2011-03)	v9.0.1 (2011-03)
3GPP TS 29.002, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile Application Part (MAP) specification	v12.0.0 (2013-03)	v12.0.0 (2013-03)	v12.0.0 (2013-03)
3GPP TS 29.016, 3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); Serving GPRS Support Node (SGSN) - Visitors Location Register (VLR); Gs interface network service specification	v8.0.0 (2008-12)	v8.0.0 (2008-12)	v8.0.0 (2008-12)

3GPP Standard	R21.2	R21.3	R21.4
3GPP TS 29.018, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); Serving GPRS Support Node (SGSN) - Visitors Location Register (VLR) Gs interface layer 3 specification	v10.7.0 (2012-09)	v10.7.0 (2012-09)	v10.7.0 (2012-09)
3GPP TS 29.060,3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface	v12.0.0 (2013-03)	v12.0.0 (2013-03)	v12.0.0 (2013-03)
3GPP TS 29.078, 3rd Generation Partnership Project; Technical Specification Group Core Network; Customized Applications for Mobile network Enhanced Logic (CAMEL) Phase 3; CAMEL Application Part (CAP) specification (Release 4)	v4.9.0 (2009-2009)	v4.9.0 (2009-2009)	v4.9.0 (2009-2009)
3GPP TS 29.202, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; SS7 Signalling Transport in Core Network; Stage 3	v8.0.0 (2007-06)	v8.0.0 (2007-06)	v8.0.0 (2007-06)

3GPP Standard	R21.2	R21.3	R21.4
3GPP TS 29.272, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol (Release 9)	v12.0.0 (2013-03)	v12.0.0 (2013-03)	v12.0.0 (2013-03)
3GPP TS 29.274, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3 (Release 9)	v11.9.0 (2013-12)	v11.9.0 (2013-12)	v11.9.0 (2013-12)
3GPP TS 29.303, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Domain Name System Procedures; Stage 3 (Release 9)	v10.4.0 (2012-09)	v10.4.0 (2012-09)	v10.4.0 (2012-09)
3GPP TS 32.215, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging data description for the Packet Switched (PS) domain	v5.9.0 (2007-10)	v5.9.0 (2007-10)	v5.9.0 (2007-10)

3GPP Standard	R21.2	R21.3	R21.4
3GPP TS 32.251, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Packet Switched (PS) domain charging	v9.8.0	v9.8.0	v9.8.0
3GPP TS 32.298, 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description	v8.7.0 (2009-2012)- Fully compliant v9.6.0 (2010-2012) - Partially complaint (IMSI unAuth and CSG Information not supported)	v8.7.0 (2009-2012)- Fully compliant v9.6.0 (2010-2012) - Partially complaint (IMSI unAuth and CSG Information not supported)	v8.7.0 (2009-2012)- Fully compliant v9.6.0 (2010-2012) - Partially complaint (IMSI unAuth and CSG Information not supported)
3GPP TS 32.406, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Performance Management (PM); Performance measurements Core Network (CN) Packet Switched (PS) domain	v9.0.0 (2009-12)	v9.0.0 (2009-12)	v9.0.0 (2009-12)
3GPP TS 32.410, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Key Performance Indicators (KPI) for UMTS and GSM	v9.0.0 (2009-09)	v9.0.0 (2009-09)	v9.0.0 (2009-09)

3GPP Standard	R21.2	R21.3	R21.4
3GPP TS 33.102, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture	v9.4.0 (2010-12)	v9.4.0 (2010-12)	v9.4.0 (2010-12)
3GPP TS 33.106, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful Interception requirements	v9.0.0 (2009-12)	v9.0.0 (2009-12)	v9.0.0 (2009-12)
3GPP TS 33.107, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions	v9.4.0 (2011-03)	v9.4.0 (2011-03)	v9.4.0 (2011-03)
3GPP TS 33.108, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Handover interface for Lawful Interception (LI) (Release 7)	v7.10.0 (2010-2012)	v7.10.0 (2010-2012)	v7.10.0 (2010-2012)
3GPP TS 44.064, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile Station - Serving GPRS Support Node (MS-SGSN); Logical Link Control (LLC) layer specification	v9.1.0 (2011-12)	v9.1.0 (2011-12)	v9.1.0 (2011-12)

3GPP Standard	R21.2	R21.3	R21.4
3GPP TS 44.065, 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile Station (MS) - Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCP)	v9.0.0 (2009-12)	v9.0.0 (2009-12)	v9.0.0 (2009-12)
3GPP TS 48.014, 3rd Generation Partnership Project; Technical Specification Group GSM EDGE Radio Access Network; General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) interface; Gb interface Layer 1	v9.0.0 (2009-12)	v9.0.0 (2009-12)	v9.0.0 (2009-12)
3GPP TS 48.016, 3rd Generation Partnership Project; Technical Specification Group GSM EDGE Radio Access Network; General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN) interface; Network Service	v9.0.0 (2009-12)	v9.0.0 (2009-12)	v9.0.0 (2009-12)

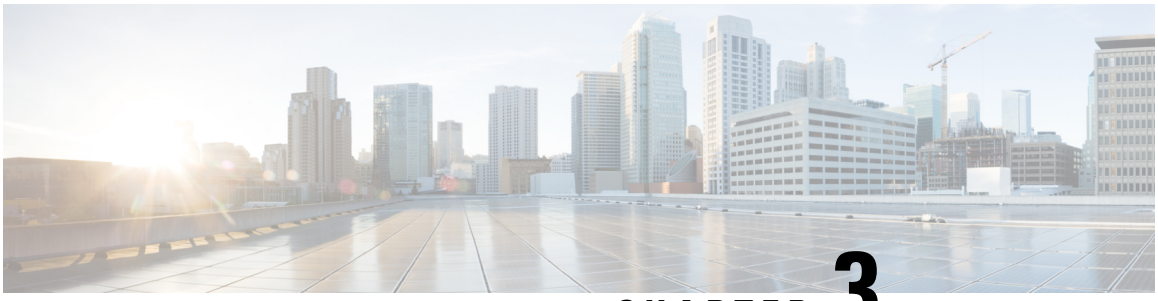
3GPP Standard	R21.2	R21.3	R21.4
3GPP TS 48.018, 3rd Generation Partnership Project; Technical Specification Group GSM/EDGE Radio Access Network; General Packet Radio Service (GPRS); Base Station System (BSS) - Serving GPRS Support Node (SGSN); BSS GPRS Protocol (BSSGP) (Release 7)	v11.5.0 (2013-11)	v13.1.0 (2016-04)	v13.1.0 (2016-04)

ITU Standards

- **Q711**; 3GPP TS 29.002 v7.15.0 (2006-2010), 3GPP TS 29.016 v7.0.0 (2007-08), and 3GPP TS 25.410 v7.0.0 (2006-03)
- **Q712**; 3GPP TS 29.002 v7.15.0 (2006-2010), 3GPP TS 29.016 v7.0.0 (2007-08), and 3GPP TS 25.410 v7.0.0 (2006-03)
- **Q713**; 3GPP TS 29.002 v7.15.0 (2006-2010), 3GPP TS 29.016 v7.0.0 (2007-08), and 3GPP TS 25.410 v7.0.0 (2006-03)
- **Q714**; 3GPP TS 29.002 v7.15.0 (2006-2010), 3GPP TS 29.016 v7.0.0 (2007-08), and 3GPP TS 25.410 v7.0.0 (2006-03)
- **Q715**; 3GPP TS 29.002 v7.15.0 (2006-2010), 3GPP TS 29.016 v7.0.0 (2007-08), and 3GPP TS 25.410 v7.0.0 (2006-03)
- **Q716**; 3GPP TS 29.002 v7.15.0 (2006-2010), 3GPP TS 29.016 v7.0.0 (2007-08), and 3GPP TS 25.410 v7.0.0 (2006-03)
- **Q771**; 3GPP TS 29.002 v7.15.0 (2006-2010)
- **Q772**; 3GPP TS 29.002 v7.15.0 (2006-2010)
- **Q773**; 3GPP TS 29.002 v7.15.0 (2006-2010)
- **Q774**; 3GPP TS 29.002 v7.15.0 (2006-2010)
- **Q775**; 3GPP TS 29.002 v7.15.0 (2006-2010)

Object Management Group (OMG) Standards

- CORBA 2.6 Specification 01-09-35, Object Management Group



CHAPTER 3

SGSN in a 2.5G GPRS Network

- SGSN in a 2.5G GPRS Network, on page 97
- 2.5G SGSN Configuration Components, on page 98
- How the 2.5G SGSN Works , on page 100
- Information Required for the 2.5G SGSN, on page 102

SGSN in a 2.5G GPRS Network

This chapter outlines the basic configuration and operation of the Serving GPRS Support Node (SGSN) in 2.5G GPRS wireless data networks.

The simplest configuration that can be implemented on the system to support SGSN functionality in a 2.5G network requires one context but we recommend a minimum of two: one for the SGSN service (required) and another for the charging context.

The service context organizes the following:

- GPRS service configuration
- MAP (Mobile Application Part) configuration
- DNS (Domain Naming System) configuration for resolution of APN (Access Point Name) domain names
- SGTP (SGSN GPRS Tunneling Protocol) configuration

The charging context facilitates the following:

- Configuration of connectivity to the CGF (Charging Gateway Function)

The following functionality is configured at the global or system level in the local management context:

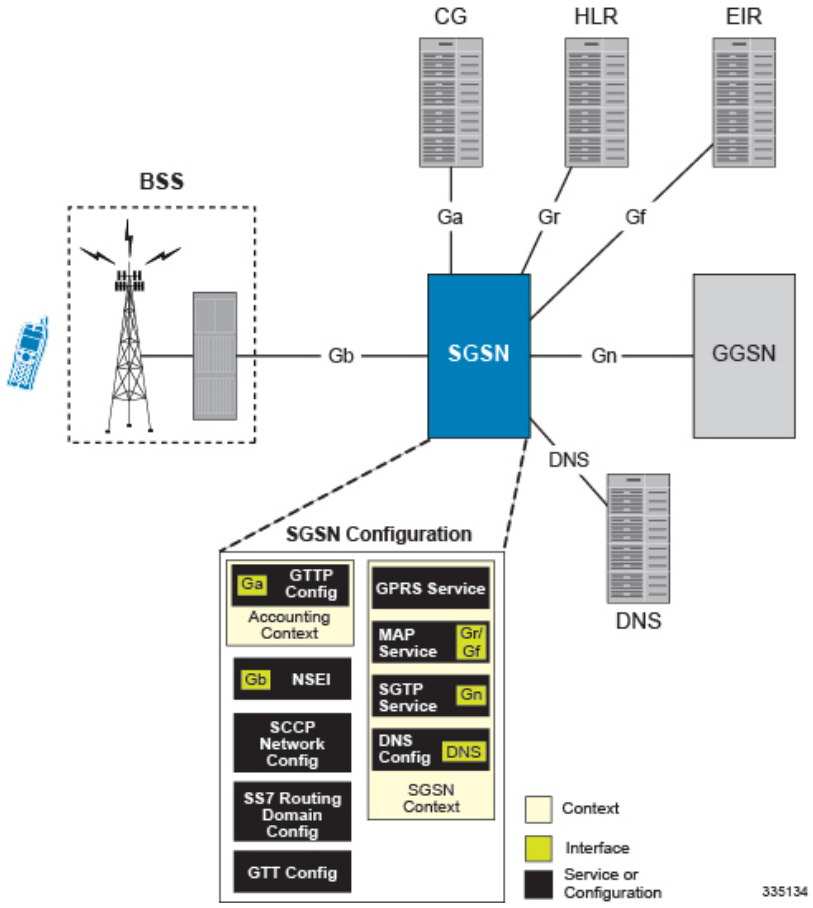
- NSEI (Network Service Entity Identity) configuration
- SCCP (Signalling Connection Control Part) network configuration
- SS7 (Signaling System 7) connectivity configuration
- GTT (Global Title Translation) configuration

To simplify configuration management, more contexts can be created to categorize the service configuration. Each context can be named as needed. The contexts listed above can be configured as illustrated in the figure on the next page.

2.5G SGSN Configuration Components

In order to support 2.5G SGSN functionality, the system must be configured with at least one context for the GPRS service (2.5G SGSN service). In the example below, the required context has been named "SGSN_Ctx".

Figure 12: Sample 2.5G SGSN Configuration



The SGSN_Ctx

As indicated, there must be at least one context to contain the service and routing configurations.

Although multiple context can be created, our example configuration uses only one context, named "SGSN_Ctx", to contain all of the following configurations:

- **SS7 Routing Domain** - SS7 routing is facilitated through the configuration and use of SS7 routing domains. SS7 routing domains group SS7-related configuration parameters. Depending on the SS7 signalling method, an SS7 routing domain may be configured with one of the following:
  - **Linksets** - Used for broadband SS7 signalling, linksets are comprised of link ids that specify point codes for SCCP endpoints. It is important to note that SCCP endpoints are further defined through the configuration of SCCP Networks which are associated with the SS7 routing domain in which the linkset is configured.

  - **Application Server Processes (ASPs) / Peer Server Processes (PSPs)** - Used for IP (SIGTRAN), M3UA ASPs and PSPs dictate the IP address and port information used to facilitate communication between network endpoints. ASPs refer to the local endpoints.

- **GTT** - Global Title Translation (GTT) configuration consists of defining GTT associations, defining GTT address maps, and referring to these in an SCCP network configuration.The GTT Associations define GTT rules. The GTT Address Maps define a GTT database. These are configured in the Global Configuration mode and are available to all SCCP networks configured in the system.
- **SCCP Network** - SCCP (Signalling Connection Control Part) networks are a concept specific to this platform. SCCP networks apply only to SS7 applications using SCCP. The purpose of an SCCP network is to isolate the higher protocol layers above SCCP and the application itself from SS7 connectivity issues, as well as, to provide a place for global SCCP configuration specific to SGSN services. Use the following example configuration to specify a global SCCP configuration specific to SGSN services.
- **MAP Service** - The Mobile Application Part (MAP) is an SS7 protocol which provides an application layer for the various nodes in GSM and UMTS mobile core networks and GPRS core networks to communicate with each other in order to provide services to mobile phone users. MAP is the application-layer protocol used to access the Home Location Register (HLR), Visitor Location Register (VLR), Mobile Switching Center (MSC), Equipment Identity Register (EIR), Authentication Center (AUC), Short Message Service Center (SMSC) and Serving GPRS Support Node (SGSN).

  The primary facilities provided by MAP are:

  - Mobility Services: location management (when subscribers move within or between networks), authentication, managing service subscription information, fault recovery.
  - Operation and Maintenance: subscriber tracing, retrieving a subscriber's IMSI.
  - Call Handling: routing, managing calls while roaming, checking that a subscriber is available to receive calls.
  - Supplementary Services.
  - SMS
  - Packet Data Protocol (PDP) services for GPRS: providing routing information for GPRS connections.
  - Location Service Management Services: obtaining the location of subscribers.

- **SGTP Service**- The SGSN GPRS Tunneling Protocol (GTP) service specifies the GTP settings for the SGSN. At a bare minimum, an address to use for GTP-C (Control signaling) and an address for GTP-U (User data) must be configured.
- **GPRS Service**- All of the parameters needed for the system to perform as a an SGSN in a GPRS network are configured in the GPRS service. The GPRS service uses other configurations such as SGTP and MAP to communicate with other network entities and setup communications between the BSS and the GGSN.
- **NSEI** (Network Service Entity Instance)- This identifies the NSEI to use and associates it with a Network Service Virtual Connection Identifier.
- **DNS**- DNS Client configurations provide DNS configuration in a context to resolve APN domain names.

The Accounting_Ctx

If no context is defined for GTPP configuration, the SGSN automatically generates an accounting context with default GTPP configurations. The context, from our example, contains the following configuration:

- **GTPP Configuration** - This configuration specifies how to connect to the GTPP charging servers.
- **Ga Interface** - This is an IP interface.

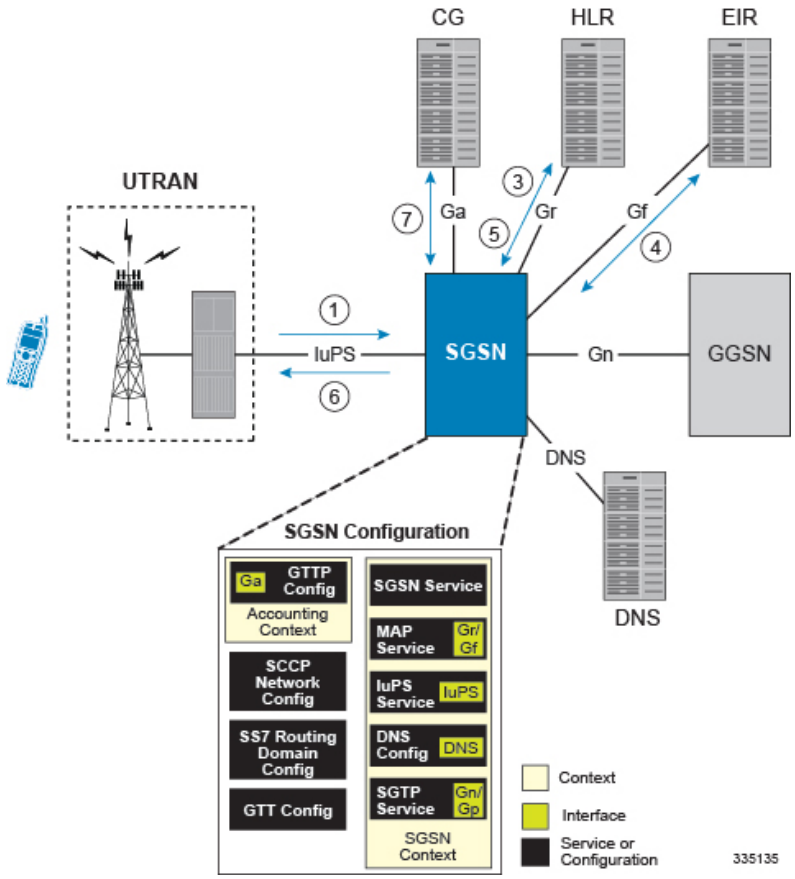
How the 2.5G SGSN Works

In compliance with 3GPP specifications, the 2.5G SGSN supports standard operational procedures such as: attach, detach, PDP activation.

For GPRS and/or IMSI Attach

The following illustrates the step-by-step call flow indicating how the 2.5G SGSN handles a GPRS/IMSI attach procedure.

Figure 13: GPRS/IMSI Attach Procedure



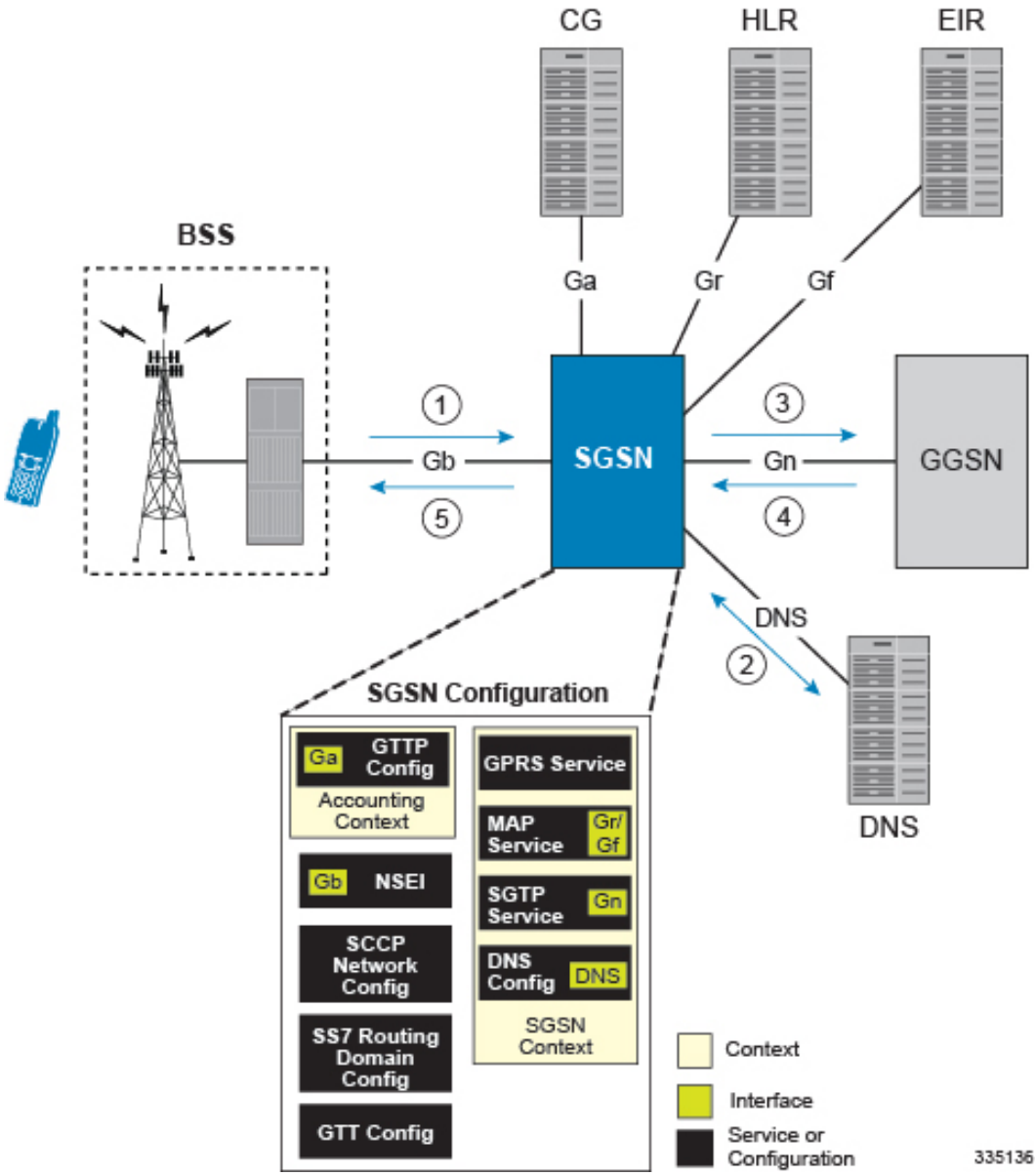
1. An Attach Request message is sent from the UE to the SGSN by the BSS over the Gb interface. This is Typically a Frame Relay connection.
2. The SGSN identifies UE and determines IMSI. Depending on whether or not the UE is already attached, this could be a simple database lookup or it could require the SGSN to communicate with an SGSN that may have been previously handling the call.
3. The SGSN communicates with the HLR to authenticate the UE.
4. Once the UE has been authenticated, the SGSN communicates with the EIR to verify that the equipment is not stolen.

5. Once equipment check is complete, the SGSN communicates with the HLR to update UE location information.
6. The SGSN then sends an Attach Complete message to UE.
7. SGSN begins sending M-CDR data to the CG.

For PDP Activation

The following provides a step-by-step illustration indicating how the 2.5G SGSN handles a PDP activation procedure.

Figure 14: PDP Activation Procedure



1. A PDP Activation Request message is sent from the UE to the SGSN by the BSS over the Gb interface. This request includes the Access Point Name (APN) the UE is attempting to connect to. This is typically a Frame relay connection.
2. The SGSN queries the DNS server to resolve the APN to the IP address of the GGSN to use to establish the PDP context.
3. The SGSN sends a Create PDP Context Request message to the GGSN. This message identifies the APN the UE is attempting to connect to and other information about the subscriber.
4. The GGSN performs its processes for establishing the PDP context. This may include subscriber authentication, service provisioning, etc. The GGSN eventually sends an affirmative create PDP context response to the SGSN containing the IP address assigned to the UE.
5. The SGSN sends an Activate PDP Context Accept message back to the UE. The subscriber can now begin sending/receiving data.
6. The SGSN begins generating S-CDR data that will be sent to the CG.

Information Required for the 2.5G SGSN

This section describes the minimum amount of information required to configure the SGSN to be operational in a 2.5G GPRS network. To make the process more efficient, we recommend that this information be collected and available prior to configuring the system.

There are additional configuration parameters that deal with fine-tuning the operation of the SGSN in the network. Information on these parameters is not provided here but can be found in the appropriate configuration command chapters in the *Command Line Interface Reference*.

Global Configuration

Table 7: Required Information for Global Configuration

Required Information	Description
NSEI (Network Service Entity)	
NSVL Instance ID	A unique ID number to identify the NSVL instance
Peer Network Service Entity	The name or NSEI index number of a peer NSE.
SS7 Routing Domain For Broadband SS7 Signaling	
SS7 Routing Domain ID	A unique ID number from 1 through 12 to identify the SS7 Routing Domain.
SS7 Routing Domain Variant	The network variant for the SS7 Routing Domain.
Sub Service Field	The Sub Service Field selector that this SS7 Routing Domain should use.
Linkset ID	A unique ID number from 1 through 49 to identify the linkset.
Linkset Self Point Code	A point code for the specified network variant that will identify the system when using this linkset.

Required Information	Description
Adjacent Point Code	The pointcode of the entity that the system will use to communicate for SS7 signaling when this linkset is used.
Link ID	A unique ID number from 1 through 16 that identitfies the MTP3 link.
Priority	An MTP3 priority number from 0 through 15 for the link.
Signaling Link Code	A number from 0 through 15 that is unique from all other SLCs in the linkset.
Arbitration	Whether the link will use passive or active arbitration.
SS7 Routing Domain to Support IP SS7 Signaling for SIGTRAN	
SS7 Routing Domain ID	A unique ID number from 1 through 12 to identify the SS7 Routing Domain.
SS7 Routing Domain Variant	The network variant for the SS7 Routing Domain.
Sub Service Field	The Sub Service Field selector that this SS7 Routing Domain should use.
ASP Instance ID	A unique ID number from 1 through 4 to use for the M3UA ASP instance.
ASP Instance Endpoint	The IP address and Port if needed of an interface that will be used as this ASP instance end point. If the interface was created in a context other than the current context, that context name is also needed.
Peer Server ID	A unique ID number from 1 through 49 to use for the M3UA peer server configuration.
Peer Server Name	A name for the Peer Server configuration. Usually this is the name of the SS7 network entity that this instance is configured to communicate with. HLR, VLR, or EIR for example.
Routing Context ID	The ID of the M3UA routing context used to reach this peer server.
Peer Server Process ID	A unique number from 1 through 4 used to identify each PSP process for the current peer server.
Peer server self-point-code	The point code to identify the peer server process being configured.
PSP Mode	Specify whether this peer server process will be used to communicate with the peer server in client or server mode.
Exchange Mode	Specify whether this peer server process will use double or single-ended mode for exchanges with the peer server.

Required Information	Description
SCTP End Point Address	A local SCTP end point address configured in an ASP instance that this peer server process will use.
ASP Association	The ID of a configured ASP instance that this peer server process will be associated with.
GTT	
GTT Association	There are many different ways to configure a GTT Association and the needs of every network are different. Please refer to the Global Title Translation Association Configuration Mode chapter in the Command Line Interface Reference for the commands available.
GTT Address Map	There are many different ways to configure a GTT Address Map and the needs of every network are different. Please refer to the Global Title Translation Address Map Configuration Mode chapter in the Command Line Interface Reference for the commands available.
SCCP Network	
SCCP Network ID	A unique number from 1 through 12 with which to identify the SCCP configuration.
SCCP Variant	The network variant for the SCCP network configuration.
Self Point Code	The point code that the system will use to identify itself when using this SCCP configuration.
SS7 Routing Domain Association	The ID number of the SS7 routing Domain with which to associate this SCCP network configuration.
GTT Association	The ID number of the GTT Association to use with this SCCP network configuration.
GTT Address Map	The ID number of the GTT Address Map to use with this SCCP network configuration.
SCCP Destination	The point code, version, and susbsystem number of the SCCP entity with which to communicate.

SGSN Context Configuration

Table 8: Required Information for SGSN Context Configuration

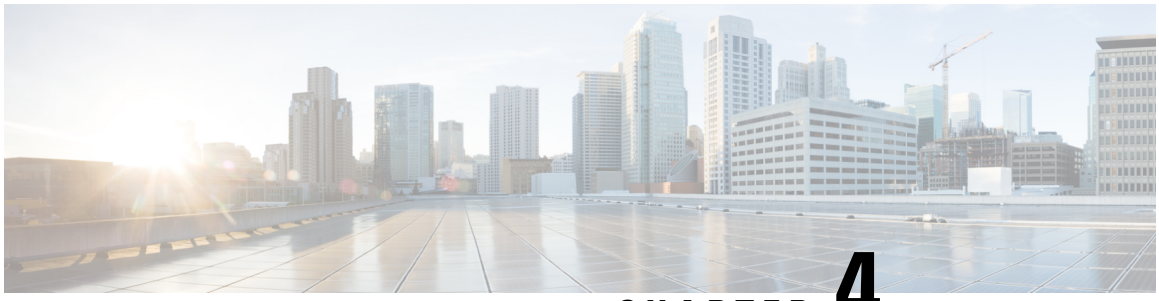
Required Information	Description
SGSN context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the SGSN context will be recognized by the system.

Required Information	Description
MAP service Configuration	
MAP Service name	A unique name with which to identify an individual MAP service.
SCCP Network ID	The ID of the SCCP network configuration to use for SS7 connectivity for SCCP applications.
EIR Address	The ISDN or point code of the EIR.
HLR Mapping	The IMSI prefixes and associated HLR point codes and the point code for the default HLR.
SGTP Service	
SGTP Service Name	A unique alpha and /or numeric name for the SGTP service configuration.
GTPC Address	An IP address that is associated with an interface in the current context. This is used for GTP-C.
GTPU Address	An IP address that is associated with an interface in the current context. This is used for GTP-U.
GPRS Service	
GPRS Service Name	a unique name to identify this GPRS service.
PLMN ID	The MCC and MNC for the SGSN service to use to identify itself in the PLMN.
Core Network ID	The core Network ID for this SGSN service to use to identify itself on the core network.
SGSN Number	The E.164 number to use to identify this SGSN.
MAP Service Name	The name of a MAP service that this SGSN service will use for MAP. If the MAP service is not in the same context, the context name of the MAP service must also be specified.
Network Service Entity Identifier	The ID of a configured Network Service Entity Identifier (NSEI) and the RAC and LAC that this SGSN should use.
DNS Client	
Name Server Addresses	The IP addressees of Domain Naming Servers i n the network.
DNS CLient Name	A unique name for the DNS client.
DNS Client Address	The IP address of an Interface in the current context that the DNS is bound to.

Accounting Context Configuration

Table 9: Required Information for Accounting Context Configuration

Required Information	Description
Context name	An identification string from 1 to 79 alphanumeric characters by which the SGSN context will be recognized by the system. Our example uses the name Accounting_Ctx.
GTPP Charging	
GTTP Group Name	If you are going to configure GTTP accounting server groups, you will need to name them.
Charging Agent Address	The IP address of an interface in the current context that to use for the Ga interface to communicate with the CGFs.
GTTP Server	The IP address and priority to use to contact the GTTP server.
GTTP Dictionary Name	The name of the GTTP dictionary to use.



CHAPTER 4

SGSN 3G UMTS Configuration

- SGSN 3G UMTS Configuration , on page 107
- 3G SGSN Configuration Components, on page 108
- Information Required for 3G Configuration, on page 109

SGSN 3G UMTS Configuration

This chapter outlines the basic deployment, configuration, and operation of the system to function as a Serving GPRS Support Node (SGSN) in 3G UMTS wireless data networks.

The simplest configuration that can be implemented on the system to support SGSN functionality in a 3G network requires one context but we recommend a minimum of two: one for the SGSN service (required) and another for the charging context.

The SGSN context facilitates the following:

- SGSN service configuration
- Mobile Application Part (MAP) configuration
- IuPS (Iu Packet Switched) interface configuration for communication with the RAN (Radio Access Network)
- DNS (Domain Naming System) Client configuration for resolution of APN domain names
- SGTP (SGSN GPRS Tunneling Protocol) configuration

The charging context facilitates the following:

- Configuration of connectivity to the CGF (Charging Gateway Function)

The following functionality is configured at the global system level:

- SCCP (Signalling Connection Control Part) network configuration
- SS7 (Signaling System 7) connectivity configuration
- GTT (Global Title Translation) configuration

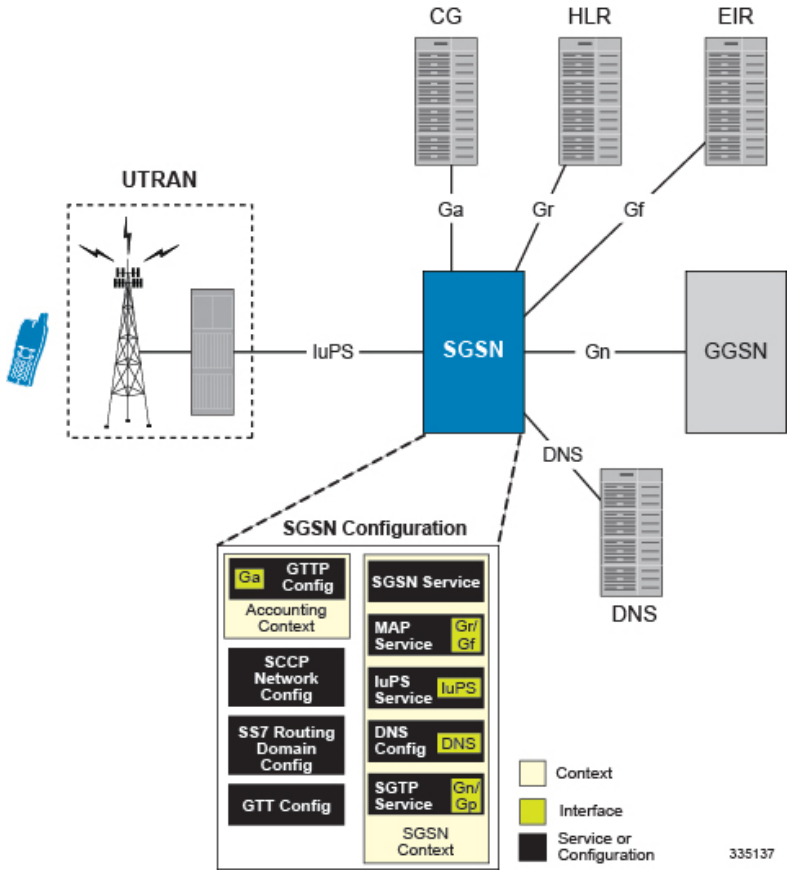
To simply configuration management, more contexts can be created and used and all context can be named as needed. The contexts listed above can be configured as illustrated in the figure on the next page.

Note With the SGSN, all configuration and created contexts, reside within the "local" or management context which is described in the *System Administration Guide*.

3G SGSN Configuration Components

In order to support 3G SGSN functionality, the system must be configured with at least one context for the SGSN (UMTS) service . In the example below, the required context has been named "SGSN_Ctx".

Figure 15: Sample 3G Network Configuration

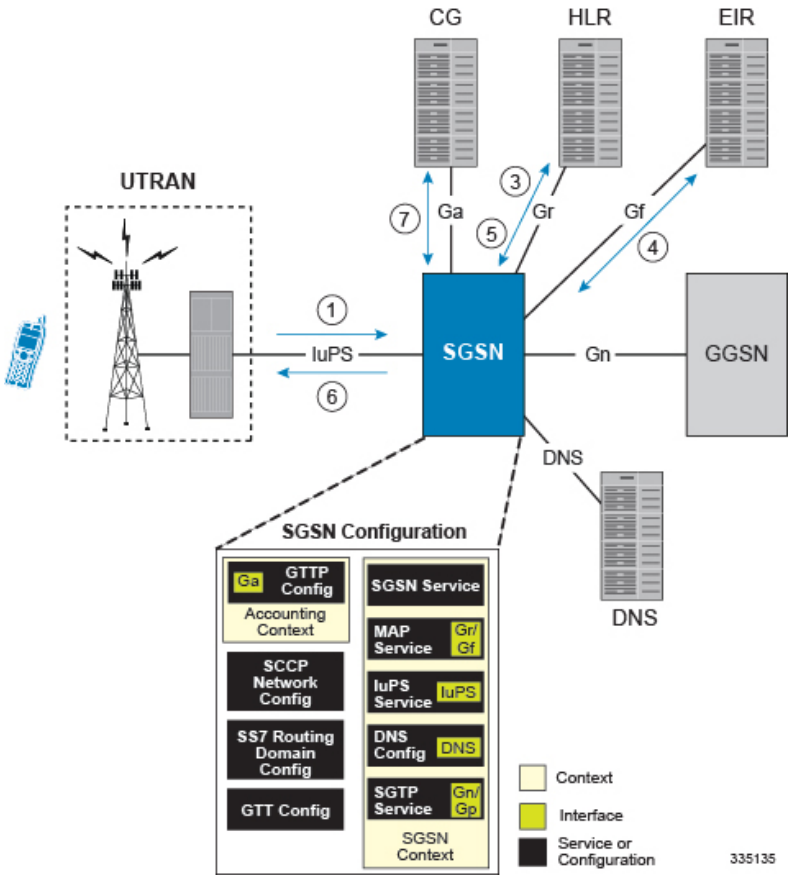


This configuration uses two contexts:

- SGSN Context containing:
  - Contains SGSN and related services
  - DNS Configuration
- Accounting Context containing:
  - GTPP configuration

For GPRS and/or IMSI Attach

Figure 16: GPRS/IMSI Attach Procedure



1. An Attach Request message is sent from the UE to the SGSN by the RNC over the IuPS interface.
2. The SGSN identifies UE and determines IMSI. Depending on whether or not the UE is already attached, this could be a simple database lookup or it could require the SGSN to communicate with an SGSN that may have been previously handling the call.
3. The SGSN communicates with the HLR to authenticate the UE.
4. Once the UE has been authenticated, the SGSN communicates with the EIR to verify that the equipment is not stolen.
5. Once equipment check is complete, the SGSN communicates with the HLR to update UE location information.
6. The SGSN then sends an Attach Complete message to UE.
7. SGSN begins sending M-CDR data to the CG.

Information Required for 3G Configuration

The following sections describe the minimum amount of information required to configure and make the SGSN operational on the network. To make the process more efficient, it is recommended that this information be available prior to configuring the system.

There are additional configuration parameters that are not described in this section. These parameters deal mostly with fine-tuning the operation of the SGSN in the network. Information on these parameters can be found in the appropriate sections of the Command Line Interface Reference.

Global Configuration

Table 10: Required Information for Global Configuration

Required Information	Description
SS7 Routing Domain to Support IP SS7 Signaling for SIGTRAN for the IuPS Interface	
SS7 Routing Domain ID	A unique ID number from 1 through 12 to identify the SS7 Routing Domain.
SS7 Routing Domain Variant	The network variant for the SS7 Routing Domain.
Sub Service Field	The Sub Service Field selector that this SS7 Routing Domain should use.
ASP Instance ID	A unique ID number from 1 through 4 to use for the M3UA ASP instance.
ASP Instance Endpoint	The IP address and port (if needed) of an interface that will be used as this ASP instance end point.
ASP Instance Endpoint Context	The name of the context in which the interface associated with this routing domain is configured
Peer Server ID	A unique ID number from 1 through 49 to use for the M3UA peer server configuration.
Peer Server Name	A name for the Peer Server configuration. Usually this is the name of the SS7 network entity that this instance is configured to communicate with. HLR, VLR, or EIR for example.
Peer Server Mode	The mode of operation for the peer server.
Routing Context ID	The ID of the M3UA routing context used to reach this peer server.
Self Point Code	The point code that the peer server will be routed to for its destination.
Peer Server Process (PSP) ID	A unique number from 1 through 4 used to identify each PSP process for the current peer server.
PSP Mode	Specify whether this peer server process will be used to communicate with the peer server in client or server mode.
Exchange Mode	Specify whether this peer server process will use double or single-ended mode for exchanges with the peer server.

Required Information	Description
SCTP End Point Address	A local SCTP end point address configured in an ASP instance that this peer server process will use. For the IuPS service, this is the address of the RNC.
ASP Association	The ID of a configured ASP instance that this peer server process will be associated with.
SS7 Routing Domain to Support IP SS7 Signaling for SIGTRAN for the Gr Interface	
SS7 Routing Domain ID	A unique ID number from 1 through 12 to identify the SS7 Routing Domain.
SS7 Routing Domain Variant	The network variant for the SS7 Routing Domain.
Sub Service Field	The Sub Service Field selector that this SS7 Routing Domain should use.
ASP Instance ID	A unique ID number from 1 through 4 to use for the M3UA ASP instance.
ASP Instance Endpoint	The IP address and Port (if needed) of an interface that will be used as this ASP instance end point.
ASP Instance Endpoint Context	The name of the context in which the interface associated with this routing domain is configured
Peer Server ID	A unique ID number from 1 through 49 to use for the M3UA peer server configuration.
Peer Server Name	A name for the Peer Server configuration. Usually this is the name of the SS7 network entity that this instance is configured to communicate with. HLR, VLR, or EIR for example.
Peer Server Mode	The mode of operation for the peer server.
Routing Context ID	The ID of the M3UA routing context used to reach this peer server.
Self Point Code	The point code that the peer server will be routed to for its destination.
Peer Server Process ID	A unique number from 1 through 4 used to identify each PSP process for the current peer server.
PSP Mode	Specify whether this peer server process will be used to communicate with the peer server in client or server mode.
Exchange Mode	Specify whether this peer server process will use double or single-ended mode for exchanges with the peer server.
SCTP End Point Address	A local SCTP end point address configured in an ASP instance that this peer server process will use. For the IuPS service, this is the address of the HLR.

Required Information	Description
ASP Association	The ID of a configured ASP instance that this peer server process will be associated with.
SCCP Network for the IuPS Interface	
SCCP Network ID	A unique number from 1 through 12 with which to identify the SCCP configuration.
SCCP Variant	The network variant for the SCCP network configuration.
Self Point Code	The point code that the system will use to identify itself when using this SCCP configuration.
SS7 Routing Domain Association	The ID number of the SS7 routing Domain with which to associate this SCCP network configuration.
SCCP Destination Point Code	The point code for the SCCP destination entity. For the IuPS interface, this is the RNC's point code
SCCP Destination Name	The name by which the SCCP destination will be known by the system
SCCP Destination Version	The SCCP variant.
SCCP Destination Subsystem Number	The subsystem number (SSN) of the SCCP destination.
SCCP Network for the Gr Interface	
SCCP Network ID	A unique number from 1 through 12 with which to identify the SCCP configuration.
SCCP Variant	The network variant for the SCCP network configuration.
Self Point Code	The point code that the system will use to identify itself when using this SCCP configuration.
SS7 Routing Domain Association	The ID number of the SS7 routing Domain with which to associate this SCCP network configuration.
SCCP Destination Point Code	The point code for the SCCP destination entity. For the IuPS interface, this is the RNC's point code
SCCP Destination Name	The name by which the SCCP destination will be known by the system
SCCP Destination Version	The SCCP variant.
SCCP Destination Subsystem Number	The subsystem number (SSN) of the SCCP destination.
Port Configuration	
Bind-to Interface Name	The name of the logical interface to bind the port to.
Bind-to Interface Context Name	The name of the context in which the logical interface is configured.

SGSN Context Configuration

Table 11: Required Information for SGSN Context Configuration

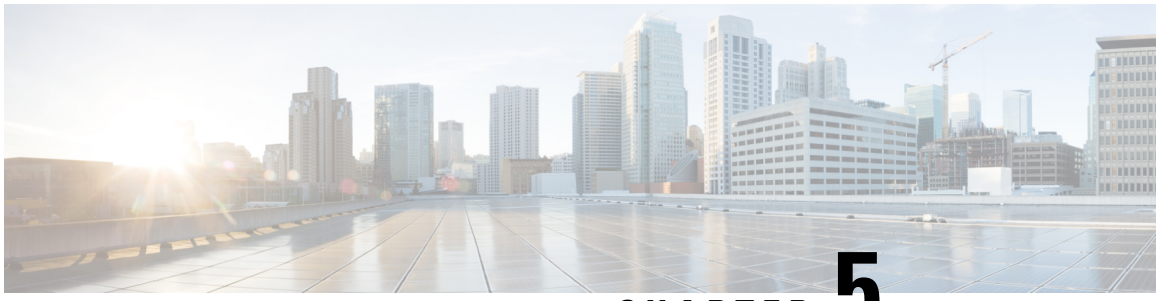
Required Information	Description
SGSN context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the SGSN context will be recognized by the system.
Logical Interface Name	The name by which the logical interface will be known by the system.
Logical Interface Addresses	IP addresses and subnets are assigned to the logical interface(s) which are then associated with physical ports.
MAP service Configuration	
MAP Service name	A unique name with which to identify an individual MAP service.
SCCP Network ID	The ID of the SCCP network configuration to use for SS7 connectivity for SCCP applications.
HLR IMSI Mapping	The IMSI prefixes for the HLR associated with this service.
HLR Point Code	The point code of the HLR to map to the IMSIs
Iu-PS Service	
IuPS Service Name	A unique name to identify the IuPS service.
SCCP Network ID	The ID of the SCCP network configuration to use for SS7 connectivity for SCCP applications.
GTPU Address	The address of an IP interface defined in the current context to use for GTPU connections to the RNC.
RNC ID	A unique ID number from 0 through 4095 for this RNC configuration and the MCC and MNC associated with the RNC.
RNC MCC	The mobile country code (MCC) associated with the RNC.
RNC MNC	The mobile network code (MNC) associated with RNC.
RNC Point Code	The SS7 point code for the specified RNC.
LAC ID	The location area code (LAC) ID associated with the RNC.
RAC ID	The routing area code (RAC) ID associated with the RNC.
SGTP Service	

Required Information	Description
SGTP Service Name	A unique alpha and /or numeric name for the SGTP service configuration.
GTP-C Address	An IP address that is associated with an interface in the current context. This is used for GTP-C over the Gn and/or Gp interface.
GTP-U Address	An IP address that is associated with an interface in the current context. This is used for GTP-U over the Gn and/or Gp interface.
SGSN Service	
SGSN Service Name	a unique name to identify this SGSN service.
Core Network ID	The core Network ID for this SGSN service to use to identify itself on the core network.
SGSN Number	The E.164 number to use to identify this SGSN.
MAP Service Name	The name of a MAP service that this SGSN service will use for MAP.
MAP Service Context	The context in which the MAP service is configured.
Maximum PDP Contexts	The maximum number of contexts each UE can establish at one time.
IuPS Service Name	The name of a configured IuPS service to use with the SGSN configuration. If the IuPS service is not in the same context, the context name of the IuPS service must also be specified.
IuPS Service Context	The context in which the IuPS service is configured.
SGTP Service Name	The name of the SGTP service that this SGSN service will use to for GTP.
SGTP Service Context	The context in which the SGTP service is configured.
Accounting Context Name	By default, the SGSN service looks for the GTPP accounting configuration in the same context as the SGSN service. If GTPP accounting is configured in a different context the context name must be specified.
DNS Client Configuration	
Name Server Addresses	The IP addresses of Domain Name Service (DNS) servers in the network.
DNS CLient Name	A unique name for the DNS client configured on the system.
DNS Client Address	The IP address of an Interface in the current context that the DNS is bound to.
DNS Client Port	The UDP port to use for DNS communications.

Accounting Context Configuration

Table 12: Required Information for Accounting Context Configuration

Required Information	Description
Accounting Context Name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the context will be recognized by the system.
Ga Interface Name	The name by which the logical interface used as the Ga interface will be known by the system.
Ga Interface Address	The IP address and subnet for the Ga interface.
GTPP Charging	
GTTP Group Name	If you are going to configure GTTP accounting Server groups, you will need to name them.
Charging Agent Address	The IP address of an interface in the current context that to use for the Ga interface to communicate with the CGFs.
GTTP Server	The IP address and priority to use to contact the GTTP server.
GTTP Dictionary Name	The name of the GTTP dictionary to use.



CHAPTER 5

SGSN Service Configuration Procedures

- SGSN Service Configuration Procedures, on page 118
- 2.5G SGSN Service Configuration, on page 118
- 3G SGSN Service Configuration, on page 119
- Dual Access SGSN Service Configuration , on page 120
- Configuring the S4-SGSN, on page 121
- Configuring an SS7 Routing Domain, on page 123
- Configuring GTT, on page 125
- Configuring an SCCP Network, on page 126
- Configuring a MAP Service, on page 127
- Configuring an IuPS Service (3G only), on page 128
- Configuring an SGTP Service, on page 129
- Configuring a Gs Service, on page 129
- Configuring an SGSN Service (3G only), on page 130
- Configuring a GPRS Service (2.5G only), on page 132
- Configuring a Network Service Entity, on page 132
- Configuring DNS Client, on page 133
- Configuring GTPP Accounting Support, on page 134
- Configuring and Associating the EGTP Service (S4 Only), on page 136
- Configuring and Associating the GTPU Service (S4 Only), on page 138
- Configuring the DNS Client Context for APN and SGW Resolution (Optional), on page 139
- Configuring the S6d Diameter Interface (S4 Only), on page 140
- Configuring the S13' Interface (S4 Only, Optional), on page 143
- Configuring QoS Mapping for EPC-Capable UEs using the S4 Interface (S4 Only, Optional), on page 147
- Configuring the Peer SGSN Interface Type (S4 Only, Optional), on page 148
- Configuring Gn Interface Selection Based on an Operator Policy (S4 Only, Optional), on page 149
- Configuring a Custom MME Group ID (S4 Only, Optional), on page 149
- Configuring and Associating the Selection of an SGW for RAI (S4 Only, Optional), on page 150
- Configuring a Local PGW Address (S4 Only, Optional), on page 152
- Configuring the Peer MME Address (S4 Only, Optional), on page 152
- Configuring the ISR Feature (S4 Only, Optional), on page 153
- Configuring IDFT for Connected Mode Handover (S4 Only, Optional), on page 154
- Creating and Configuring ATM Interfaces and Ports (3G only), on page 155

• Creating and Configuring Frame Relay Ports (2.5G only), on page 155
• Configuring APS/MSP Redundancy, on page 155

SGSN Service Configuration Procedures

This chapter provides configuration instructions to enable the SGSN to function in GPRS (2.5G), UMTS (3G), or LTE (4G) networks. The *System Administration Guide* provides interface and system-level configuration details and the *Command Line Interface Reference* provides additional command information.

Important Please note that LTE (4G) support is only available in releases 14.0 an higher.

Important At least one packet processing card must be activated prior to configuring the first service. Procedures for configuring the packet processing card can be found in the *System Administration Guide*.

High level step-by-step service configuration procedures are provided for the following:

2.5G SGSN Service Configuration

The following configuration steps must be completed to allow the system to operate in a 2.5G GPRS network.

The service handling the GPRS or 2.5G functions in the SGSN is called the "gprs-service".

Step 1 Create all the contexts you will use in your configuration. Refer to the "System Element Configuration Procedures" chapter in the *System Administration Guide.*

Step 2 Create and configure the Frame Relay interface(s) and Ethernet interface(s). Refer to the "System Element Configuration Procedures" chapter in the *System Administration Guide.*

Step 3 Configure SS7 routing domains. Use the procedure in Configuring an SS7 Routing Domain, on page 123. The concept of an SS7 routing domain is not a standard SS7 concept. It is a concept specific to this platform which groups a set of SS7 feature configuration together to facilitate the management of the SS7 connectivity resources for an SGSN service.

Step 4 Configure GTT. The GTT configuration is used to set rules for GTT and define the GTT databases. Follow the procedure in Configuring GTT, on page 125

Step 5 Configure SCCP-Networks. The purpose of an SCCP network is to isolate the higher protocol layers above SCCP and the application itself from SS7 connectivity issues, as well as, to provide a place for global SCCP configuration specific to SGSN services. Use the procedure in Configuring an SCCP Network, on page 126

Step 6 Configure MAP services. The MAP service configuration is used by the SGSN service to communicate with many of the nodes on the narrow band-SS7 network part of the network such as HLR, EIR, GSM-SCF, GMLC and SMS-GMSC/SMS-IWMSC. The purpose of having an isolated map configuration is to enable different application services to use the map service to communicate with other map entities in the network. Use the procedure in Configuring a MAP Service, on page 127

Step 7 Configure SGTP. The SGTP service configures the parameters used for GTP Tunneling. At the minimum, interfaces for GTP-C and GTP-U must be configured. Use the procedure in Configuring an SGTP Service, on page 129

Step 8 Configure the SGSN service. All the parameters specific to the operation of an SGSN are configured in the SGSN service configuration mode. SGSN services use other configurations like MAP and IuPS to communicate with other elements in the network. The system can support multiple gprs-services.

Step 9 Configure the GPRS service. All of the parameters needed for the system to perform as a an SGSN in a GPRS network are configured in the GPRS service. The GPRS service uses other configurations such as SGTP and MAP to communicate with other network entities and setup communications between the BSS and the GGSN. Use the procedure in Configuring a GPRS Service (2.5G only), on page 132

Step 10 Configure the Network Service Entity Instance. This identifies the NSEI to use and associates it with a Network Service Virtual Connection Identifier. Use the procedure in Configure a Network Service Entity for IP, on page 132

Step 11 Configure DNS. This configuration enables domain name resolution and specifies the DNSs to use for lookup. Use the procedure in Configuring DNS Client, on page 133

Step 12 Configure GTPP Accounting. This configures GTPP-based accounting for subscriber PDP contexts. Use the procedure in Configuring GTPP Accounting Support, on page 134

Step 13 Configure Frame Relay DLCI paths and bind them to NSEI links as needed. Refer to *Creating and Configuring Frame Relay Interfaces and Ports* in the *System Administration Guide.*

Step 14 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

3G SGSN Service Configuration

The following configuration steps must be completed to allow the system to operate in a 3G network.

Step 1 Create the contexts needed. Refer to the *System Element Configuration Procedures* chapter in the *System Administration Guide.*

Step 2 Create any interfaces needed in the appropriate context. Refer to the *System Element Configuration Procedures* chapter in the *System Administration Guide* for IP (broadcast Ethernet) interfaces and for ATM interfaces.

Step 3 Configure SS7 routing domains. The SS7 routing domain is proprietary concept to provide a combined configuration for the SS7 links, linksets, and related parameters. SS7 routing domain configurations are common to both SIGTRAN and MTP3-B networks. Use the procedure in Configuring an SS7 Routing Domain, on page 123

Step 4 Configure global title translations (GTT). The GTT configuration is used to set rules for GTT and to define the GTT databases. Follow the procedure in Configuring GTT, on page 125

Step 5 Configure SCCP networks. The SCCP network (layer) provides services to protocol layers higher in the SS7 protocol stack, for example RANAP and TCAP. The SCCP layer is also responsible for GTT. As well, all the SS7 routing domains (created in step 3) will be associated with an SCCP network. Use the procedure in Configuring an SCCP Network, on page 126

Step 6 Configure MAP services. The MAP service configuration is used by the SGSN service to communicate with many of the nodes in the SS7 network, such as the HLR, EIR, GSM-SCF, GMLC and SMS-GMSC/SMS-IWMSC. Having an isolated MAP configuration enables different application services to use the MAP service to communicate with other MAP entities in the network. Use the procedure in Configuring a MAP Service, on page 127

Step 7 Configure IuPS services. A set of parameters define the communication path between the SGSN service and radio network controllers (RNCs) in a UMTS IuPS service. Use the procedure in Configuring an IuPS Service (3G only), on page 128

Step 8 Configure SGTP services. The SGTP service configures the parameters used for GTP Tunneling. At a minimum, interfaces for GTP-C and GTP-U must be configured. Use the procedure in Configuring an SGTP Service, on page 129

Step 9 Configure the SGSN service. All the parameters specific to the operation of an SGSN are configured in the SGSN service configuration mode. SGSN services use other service configurations like MAP (map-service) and IuPS (iups-service) to communicate with other elements in the network.

Step 10 Configure DNS clients. This configuration enables domain name resolution and specifies the DNSs to use for lookup. Use the procedure in Configuring DNS Client, on page 133

Step 11 *Optional*: Configure operator policies. Operator policies are not required for SGSN operation, however, they provide the operator with a powerful method for determining call handling. SGSN operator policies specify rules governing the services, facilities and privileges available to a single subscriber or groups of subscribers. Use the procedure in *Configuring SGSN Operator Policies.*

Step 12 Configure GTPP Accounting. This configures GTPP-based accounting for subscriber PDP contexts. Use the procedure in Configuring GTPP Accounting Support, on page 134

Step 13 Configure ATM PVCs and bind them to interfaces or SS7 links as needed. Refer to *Creating and Configuring ATM Interfaces and Ports* in the *System Administration Guide.*

Step 14 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Dual Access SGSN Service Configuration

The following configuration steps must be completed to allow the SGSN to operate in both GPRS (2.5G) and UMTS (3G) networks. This type of co-location is referred to as dual access.

To configure dual access requires a combination of steps from both the 2.5G and 3G configuration procedures:

Step 1 Create the contexts needed. Refer to the *System Element Configuration Procedures* chapter in the *System Administration Guide.*

Step 2 Create any interfaces needed in the appropriate context refer to the *System Element Configuration Procedures* chapter in the *System Administration Guide.*

a) For IP (broadcast Ethernet) interfaces, refer to *Creating and Configuring Ethernet Interfaces and Ports* in the *System Administration Guide*.

b) For ATM interfaces (3G) refer to *Creating and Configuring ATM Interfaces and Ports* in the *System Administration Guide.*

c) For Frame Relay interfaces (2.5G) refer to *Creating and Configuring Frame Relay Interfaces and Ports* in the *System Administration Guide.*

Step 3 Configure SS7 routing domains. The SS7 routing domain is a non-standard, proprietary SS7 concept specific to this platform. SS7 routing domains provide a combined configuration for the SS7 links, linksets, and related parameters for SS7 connectivity resources for an SGSN service. SS7 routing domain configurations are common to both SIGTRAN and MTP3-B networks. Use the procedure in Configuring an SS7 Routing Domain, on page 123

Step 4 Configure global title translations (GTT). The GTT configuration is used to set rules for GTT and to define the GTT databases. Follow the procedure in Configuring GTT, on page 125

Step 5 Configure SCCP networks. The SCCP network (layer) provides services to protocol layers higher in the SS7 protocol stack, for example RANAP and TCAP. The SCCP layer is also responsible for GTT (step 4) and every SS7 routing domain (step 3) will be associated with an SCCP network. Use the procedure in Configuring an SCCP Network, on page 126

Step 6 Configure MAP services. The MAP service configuration is used by the SGSN service to communicate with many of the nodes in the SS7 network, such as the HLR, EIR, GSM-SCF, GMLC and SMS-GMSC/SMS-IWMSC. Having an isolated MAP configuration enables different application services to use the MAP service to communicate with other MAP entities in the network. Use the procedure in Configuring a MAP Service, on page 127

Step 7 Configure IuPS services. A set of parameters define the communication path between the SGSN service and radio network controllers (RNCs) in a UMTS IuPS service. Use the procedure in Configuring an IuPS Service (3G only), on page 128

Step 8 Configure SGTP services. The SGTP service configures the parameters used for GTP Tunneling. At a minimum, interfaces for GTP-C and GTP-U must be configured. Use the procedure in Configuring an SGTP Service, on page 129

Step 9 Configure the GPRS service. All of the parameters needed for the system to perform as a an SGSN in a GPRS network are configured in the GPRS service. The GPRS service uses other service configurations, such as SGTP (sgtp-service) and MAP (map-service) to communicate with other network entities and setup communications between the BSS and the GGSN. Use the procedure in Configuring a GPRS Service (2.5G only), on page 132

Step 10 Configure the Network Service Entity Instance. This identifies the NSEI to use and associates it with a Network Service Virtual Connection Identifier. Use the procedure in Configuring a Network Service Entity, on page 132

Step 11 Configure DNS. This configuration enables domain name resolution and specifies the DNSs to use for lookup. Use the procedure in Configuring DNS Client, on page 133

Step 12 Configure GTPP Accounting. This configures GTPP-based accounting for subscriber PDP contexts. Use the procedure in Configuring GTPP Accounting Support, on page 134

Step 13 Configure ATM PVCs and bind them to interfaces or SS7 links as needed. Refer to *Creating and Configuring ATM Interfaces and Ports* in the *System Administration Guide.*

Step 14 Configure Frame Relay DLCI paths and bind them to NSEI links as needed. Refer to *Creating and Configuring Frame Relay Interfaces and Ports* in the *System Administration Guide*.

Step 15 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring the S4-SGSN

The following configuration steps comprise the required and optional tasks for configuring the S4-SGSN to provide an interface between GPRS (2.5G) / UMTS (3G) networks and EPC (4G) networks via the EPC S4 interface. This is referred to as an S4-SGSN.

Important The S4-SGSN cannot operate until after 2G, 3G, or dual access SGSN service is configured. Do not begin S4-SGSN configuration until one of those services is configured and operational. Refer to the 2.5G SGSN Service Configuration, on page 118, Configuring an SGSN Service (3G only), on page 130 , or Dual Access SGSN Service Configuration , on page 120 sections in this chapter for details on configuring those services.

Before you begin the configuration procedure, note the following:

- Configuration steps 1 through 5 are **mandatory** for the S4-SGSN to operate properly.
- Configuration steps 6 through 15 are **optional**. They can be used to configure or enable various optional functionality and features, including:
  - Bypass DNS resolution for various network elements
  - Configure GUTI-to-RAI mapping
  - Configure operator-specific QoS mapping values
  - Configure the S13' interface for the Mobile Equipment Identity (MEI) check
  - Configure the license-enabled Idle Mode Signaling Reduction feature
  - Configure the Indirect Data Forwarding Tunnel feature

Step 1 Configure, 2G, 3G or Dual Access SGSN service support. Refer to the Configuring a GPRS Service (2.5G only), on page 132, 3G SGSN Service Configuration, on page 119, or Dual Access SGSN Service Configuration , on page 120 sections in this chapter for the configuration

Step 2 Configure and associate the EGTP service. The EGTP service is required to support communication between the SGSN and the EPC SGW over the S4 interface using the GTPv2 protocol. Refer to the Configuring and Associating the EGTP Service (S4 Only), on page 136 procedure.

Step 3 Configure and associate the GTPU service. The GTPU service supports the configured EGTP service by enabling the sending and receiving of GTP bearer packets from the EPC SGW over the S4 intereface. Refer to the Configuring and Associating the GTPU Service (S4 Only), on page 138 procedure.

Step 4 Configure DNS for APN resolution. Configurables must be set to enable the default DNS client on the SGSN to resolve EPC PGW and SGW addresses. Refer to the Configuring the DNS Client Context for APN and SGW Resolution (Optional), on page 139 procedure.

Step 5 Configure the S6d Diameter Interface. The S6d interface is used by the SGSN to communicate with the HSS. The HSS is a master user database that contains all subscription related information, Refer to the Configuring the S6d Diameter Interface (S4 Only), on page 140 procedure.

Step 6 *Optional*. Configure the S13' (S13 prime) interface. This interface is used to perform Mobile Equipment (ME) identity check procedure between the SGSN and Equipment Identity Registry. Refer to the Configuring the S13' Interface (S4 Only, Optional), on page 143 procedure.

Step 7 *Optional*. Configure operator-specific QoS mapping between EPC elements and the SGSN. The S4-SGSN communicates QoS parameters towards the SGW/ PGW and EPC UEs in different formats. Operators must configure the SGSN quality of service (QoS) parameters as a call-control-profile that will ensure proper QoS mapping between the S4-SGSN, SGW/PGW and UEs. Refer to the Configuring QoS Mapping for EPC-Capable UEs using the S4 Interface (S4 Only, Optional), on page 147 procedure.

Step 8 *Optional*. Configure the interface type used by the S4-SGSN to communicate with the peer SGSN. Refer to the Configuring the Peer SGSN Interface Type (S4 Only, Optional), on page 148 procedure.

Step 9 *Optional*. Configure Gn interface selection for EPC-capable UEs based on an operator policy. When the EGTP service is configured, the SGSN, by default, selects the S4 interface for 1) EPC capable UEs and 2) non-EPC capable UEs that have an EPS subscription only. However, operators have the option to forcefully select the Gn interface for both types of UEs. Refer to the Configuring Gn Interface Selection Based on an Operator Policy (S4 Only, Optional), on page 149 procedure.

Step 10 *Optional*. Configure a custom MME group ID. For operators who are using LAC ranges between 32768 and 65535 in UMTS/GPRS deployments, rather than for MMEs in LTE deployments, the SGSN provides a workaround to ensure backward compatibility. Refer to the Configuring a Custom MME Group ID (S4 Only, Optional), on page 149 procedure.

Step 11 *Optional*. Configure the S-GW for a RAI. If operators wish to bypass DNS resolution for obtaining the EPC S-GW address, the S4-SGSN can select a locally configured S-GW by performing a local look-up for the current RAI. Refer to the Configuring and Associating the Selection of an SGW for RAI (S4 Only, Optional), on page 150 procedure.

Step 12 *Optional*. Configure a Local PGW Address. For operators who wish to bypass DNS resolving an EPC P-GW address, the SGSN can be configured with a local P-GW address as part of an APN profile. Refer to the Configuring a Local PGW Address (S4 Only, Optional), on page 152 procedure.

Step 13 *Optional*. Configure the peer MME address. If operators wish to bypass DNS to resolve the peer MME address, the SGSN supports the local configuration of a peer MME address for a given MME group (LAC) and MME code (RAC). Refer to Configuring the Peer MME Address (S4 Only, Optional), on page 152 procedure.

Step 14 *Optional*. Configure the Idle Mode Signaling Reduction (ISR) feature. The ISR is a license-enabled feature allows the UE to roam between LTE and 2G/3G networks while reducing the frequency of TAU and RAU procedures due to the UE selecting E-UTRAN or UTRAN networks. Refer to the Configuring the ISR Feature (S4 Only, Optional), on page 153 procedure.

Step 15 *Optional*. Enable the setup of indirect data forwarding tunnels (IDFT) between the eNodeB and the RNC via the SGW during connected mode handovers. This allows for connected mode handovers between the UTRAN and E-UTRAN networks across the S3 (S4-SGSN-to-MME) interface. Refer to Configuring IDFT for Connected Mode Handover (S4 Only, Optional), on page 154.

Configuring an SS7 Routing Domain

The SGSN supports both SS7- and IP-based routing. IP-based routing is provided through the use of contexts. SS7 routing is facilitated through the configuration and use of SS7 routing domains. SS7 routing domains group SS7-related configuration parameters. Depending on the SS7 signaling method, an SS7 routing domain may be configured with one of the following:

- **Linksets**: Used for broadband SS7 signaling, linksets are comprised of link ids that specify point codes for SCCP endpoints. It is important to note that SCCP endpoints are further defined through the configuration of SCCP Networks (refer to *Configuring an SCCP Network*) which are associated with the SS7 routing domain in which the linkset is configured.
- **Application Server Processes** (ASPs) / **Peer Server Processes** (PSPs): Used for IP (SIGTRAN), M3UA ASPs and PSPs dictate the IP address and port information used to facilitate communication between network endpoints. ASPs refer to the local endpoints.

Configuring an SS7 Routing Domain to Support Broadband SS7 Signaling

Step 1 In global configuration mode, create a new SS7 routing domain, give it a unique ID and specify the network variant that SS7 communications through this routing domain use.

Step 2 In SS7 routing domain configuration mode, configure the MTP-3 sub-service field (SSF).

Step 3 Create an SS7 linkset with a unique ID.

Step 4 In linkset configuration mode, specify the self point code - this is the point code of the SGSN.

Step 5 Specify the adjacent point code to communicate with another SS7 node, e.g., an RNC.

Step 6 Configure individual links, identified with link IDs.

Step 7 In link configuration mode, specify the MTP3 link priority.

Step 8 Specify the Signaling Link Code (SLC) for this link. This must be unique to this link within the current linkset. Note that SLCs must match, one-to-one, with those defined for the peer nodes.

Step 9 Configure this link to use either passive or active arbitration.

Step 10 In SS7 routing domain configuration mode, configure SS7 routes by specifying destination point codes and associated linkset IDs.

Example Configuration

```
configure
   ss7-routing-domain id variant variant
      ssf subsvc
      linkset id id
      self-point-code  #.#.#
      adjacent-point-code #.#.#
      link id id
        priority pri
        signaling-link-code code
        arbitration arbitration
        exit
      exit
   route destination-point-code dpc linkset-id id
   end
```

Configuring an SS7 Routing Domain to Support IP Signaling for SIGTRAN

To configure IP, the SS7 routing domain must be configured in a specific way as described below:

Step 1 In Global configuration mode, create a new SS7 routing domain, give it a unique ID and specify the network variant that SS7 communications through this routing domain use.

Step 2 In SS7 Routing Domain configuration mode, configure the MTP-3 subservice field.

Step 3 Create an ASP (Application Service Part) instance for M3UA ASP configuration and give it a unique ID.

Step 4 Specify the local SCTP (Stream Control Transmission Protocol) end-point IP address and the name of the context where the IP interface associated with the address is configured.

Important At least one address needs to be configured before the end-point can be activated.

Step 5 Specify the end-point SCTP port address to be used. Default port address is 2905.

Step 6 Bind the end-point to the application server process (ASP) instance to activate it.

Step 7 In SS7 routing domain configuration mode, create a peer server configuration with a unique ID.

Step 8 Name the peer server configuration. Usually this is the name of the SS7 network entity that this instance is configured to communicate with, for example an HLR, an STP, or an RNC.

Step 9 Specify the M3UA routing context ID.

Step 10 Create a PSP instance and give it a unique ID.

Step 11 In PSP configuration mode, specify the PSP mode in which this PSP instance should operate.

Step 12 Specify the communication mode this PSP instance should use as client or server.

Step 13 Configure the exchange mode this PSP instance should use. Generally this is not configured for IPSP-SG configuration, e.g., SGSN and STP.

Step 14 Configure the IP address of the peer node SCTP end-point for this PSP instance. At least one address needs to be configured before the end-point can be activated. Up to two addresses can be configured.

Step 15 Specify the ID of the ASP instance with which to associate this PSP instance.

Step 16 Configure SS7 routes, in SS7 routing domain configuration mode, by specifying destination point codes and peer server IDs. Routes are configured if the destination point code (DPC) is at least a hop away from the SGSN or when the DPC is not the same as the peer server. For example, the route is configured between the SGSN and the HLR which communicates through STPs or signaling gateways. In this case, the signaling gateways are configured as the peer server on the SGSN.

Example Configuration

```
configure
   ss7-routing-domain id variant variant
     ssf subsvc
        asp instance instance_id
           end-point address address context ctxt_name
           end-point bind
           exit
     peer-server id id
        name name
        routing-context ctxt_id
        psp instance id
           psp-mode mode
           exchange-mode mode
           end-point address address
           associate asp instance id
           exit
     exit
   route destination-point-code dpc peer-server-id id
end
```

Configuring GTT

Global Title Translation (GTT) configuration consists of defining GTT associations, defining GTT address maps, and referring to these in an SCCP network configuration. The GTT Associations define GTT rules applicable to a specific GT format. The GTT Address Maps define a global title address to be routed to using a specific routing indicator. These are configured in the global configuration mode and are available to all SCCP networks configured in the system.

Step 1 In global configuration mode, create a GTT association with a unique name.

Step 2 In GTT association configuration mode, define the type of digit analysis to be used; "fixed" is the generally used digit analysis and if specified, also define the length of the digits to be analyzed. This is represented using action IDs.

Step 3 In GTT association configuration mode, define the GT format (1 to 4) for which the analysis needs to be applied.

Step 4 In the GT format configuration mode, specify the numbering plan and the nature of address to be used. Note that a separate GTT association needs to be created for a combination of numbering plan, nature of address, and GT format.

Important There are many different ways to configure a GTT association and the needs of every network are different. Please refer to the *Global Title Translation Association Configuration Mode* chapter in the Command Line Interface Reference for the commands available.

Step 5 In global configuration mode, create a GTT address map, with a unique name, for a specific global title address.

Step 6 In GTT address map configuration mode, associate a specific GTT association and the action ID.

Step 7 In GTT address map configuration mode, define the routing indicator to be included in the Called-party Address in the out-going SCCP message along with the destination of the message using the option out-address.

Important There are many different ways to configure a GTT Address Map and the needs of every network are different. Please refer to the *GTT Address Map Configuration Mode* chapter in the Command Line Interface Reference for the commands available.

Example Configuration

```
configure
   global-title-translation association instance <inst#>
      action id <id> type <action_type> start-digit <num> end-digit <num>
      gt-format <format_num>
      exit
   global-title-translation address-map instance <inst#>
      associate gtt-association <assoc#> action id <id>
      gt-address <gt_addr_prefix>
      out-address <name>
         ssf <sub_svc_fld>
         routing-indicator <route_ind>
         ni-indicator <addr_ind>
         ssn <sub_sys_num>
         point-code <pt_code>
         end
```

Configuring an SCCP Network

SCCP (Signaling Connection Control Part) networks are a concept specific to this platform. The SCCP network provides services to protocol layers higher in the SS7 protocol stack, e.g., RANAP and TCAP. This layer is also responsible for GTT. Every SS7 routing domain will be associated with an SCCP network. Use the following example configuration to specify a global SCCP configuration specific to SGSN services.

Important A total of 12 SCCP networks can be configured.

To configure an SCCP network:

Step 1 In global configuration mode, specify an identification number for this SCCP network configuration and the signaling variant.

Step 2 Specify the self point code of the SGSN.

Step 3 Specify the SS7 routing domain with which to associate this SCCP network configuration.

Step 4 If using GTT (Global Title Translation), specify the name of a GTT address map to use.

Step 5 Configure a destination point code and give it a name.

Step 6 Configure the destination point code version.

Step 7 Configure the destination point code subsystem number.

Example Configuration

```
configure
   sccp-network <id_number> variant <v_type>
      self-pointcode <sp_code>
      associate ss7-routing-domain <rd_id>
      global-title-translation address-map <map_name>
      destination dpc <dp_code> name <name>
      destination dpc <dp_code> version <ver_type>
      destination dpc <dp_code> ssn <ss_number>
      end
```

Configuring a MAP Service

The Mobile Application Part (MAP) is an SS7 protocol which provides an application layer for the various nodes in GSM and UMTS mobile core networks and GPRS core networks to communicate with each other in order to provide services to mobile phone users. MAP is the application-layer protocol used to access the Home Location Register (HLR), Visitor Location Register (VLR), Mobile Switching Center (MSC), Equipment Identity Register (EIR), Authentication Center (AUC), Short Message Service Center (SMSC) and Serving GPRS Support Node (SGSN).

The primary facilities provided by MAP are:

- Mobility Services: location management (when subscribers move within or between networks), authentication, managing service subscription information, fault recovery.
- Operation and Maintenance: subscriber tracing, retrieving a subscriber's IMSI.
- Call Handling: routing, managing calls while roaming, checking that a subscriber is available to receive calls.
- Supplementary Services.
- Short Message Service (SMS)
- Packet Data Protocol (PDP) services for GPRS: providing routing information for GPRS connections.
- Location Service Management Services: obtaining the location of subscribers.

Important A maximum of 12 MAP services can be configured on the system.

To configure MAP services:

Step 1 In the context config mode, create a MAP service and give it a name.

Step 2 In MAP Service configuration mode, configure the SCCP network that defines SS7 connectivity for SCCP applications.

Step 3 Configure the parameters to contact the HLR.

Step 4 In HLR configuration mode, specify the HLR pointcodes that should be associated with specific IMSI prefixes.

Step 5 Configure the HLR pointcode to use as the default.

Step 6 *Optional*: Enable the Short Message Service functionality.

Step 7 *Optional*: Configure the SMS routing.

Example Configuration

```
configure
   context context_name
    map-service map_name
      access-protocol sccp-network sccp_network_id
      equipment-identity-register point-code pnt_code
    hlr
      imsi any point-code
      default policy routing
      exit
    short-message-service
      smsc-routing  imsi-starts-with prefix point-code sms_pc
      end
```

Configuring an IuPS Service (3G only)

A set of parameters, in the IuPS service configuration mode, define the communication path between the SGSN service and the RNC. These configured parameters pertain to the RANAP layer of the protocol stack. IuPS services must be configured in the same context as the SGSN service that will use them.

To configure an IuPS service:

Step 1 In context configuration mode for the SGSN service, create an IuPS service and give it a unique name.

Step 2 In IuPS service configuration mode, specify the ID of the SCCP network to use for access protocol parameters.

Step 3 Bind an address of an IP interface defined in the current context to use for GTPU connections to the RNC.

Step 4 Specify an RNC to configure with a unique ID and the MCC and MNC associated with the RNC.

Step 5 In RNC configuration mode, specify the RNCs point code.

Step 6 Specify the LAC ID and RAC ID associated with the RNC.

Important Appropriate interfaces (i.e., physical, loopback, secondary) must be defined prior to configuring the IuPS service or the GTP-U IP address will decline to bind to the service.

Example Configuration

```
configure
   context context_name
     iups-service iups_name
        access-protocol sccp-network sccp_network_id
        gtpu bind address ip_address
        rnc id rnc_id mcc mcc_num mnc mnc_num
          pointcode rnc_pc
          lac lac_id rac rac_id
end
```

Configuring an SGTP Service

This section provides instructions for configuring GPRS Tunneling Protocol (GTP) settings for the SGSN. At a bare minimum, an address to use for GTP-C (Control signaling) and an address for GTP-U (User data) must be configured.

To configure the SGTP service:

Step 1 Create an SGTP service and give it a unique name, in context configuration mode.

Step 2 Specify the IP address of an interface in the current context to use for GTP-C.

Step 3 Specify the IP address of an interface in the current context to use for GTP-U.

Important Appropriate interfaces (i.e., physical, loopback, secondary) must be defined prior to configuring the SGTP service or the GTP-U IP address will decline to bind to the service.

Example Configuration

```
configure
   context name
     sgtp-service name
       gtpc bind address address
       gtpu bind address address
       end
```

Configuring a Gs Service

This section provides instructions for creating and configuring a Gs interface used by the SGSN to communication with an MSC or VLR. The Gs interface is defined as a Gs service which handles the configuration for the MSC/VLR.

The Gs interface parameters are configured within a Gs service in a context. Then the Gs service is referred to in a GPRS service, an SGSN service, or an Call-Control Profile. The Gs service does not need to be in the same context as the SGSN service, GPRS service, or a Call-Control Profile.

To configure the Gs service:

Step 1 In context configuration mode, create a Gs service and give it a unique name. Usually Gs service is defined in the same context in which MAP service is defined because the MSC/VLR, HLR, EIR, and SMS-C are reachable via the STP or SGW connected to the SGSN.

Step 2 Specify the name of the SCCP network that identifies the SS7 access protocols.

Step 3 Specify the target SS7 sub-system number (SSN), of the Base Station System Application Part (BSSAP), for communication. Without this bit of configuration, the Gs service can not start.

Step 4 Identify a location area code, in either a pooled or non-pooled configuration, relevant to the MSC/VLR. This step can be repeated as needed.

Step 5 Define the MSC/VLR by identifying its ISDN number, its SS7 point code, and the BSSAP SSN used to communicate with it. Repeat this step to define multiple MSC/VLRs. (Note: SSN only needs to be defined if the routing defined is to the MSC/VLR is PC+SSN.)

Example Configuration

```
configure
   context name
     gs-service name
       associate-sccp-network id
       bssap+ ssn ssn
       non-pool-area id use-vlr vlr_id lac lac_id
       vlr vlr_id isdn-number isdn_number bssap+ ssn ssn point-code vlr_pt_code
       end
```

Configuring an SGSN Service (3G only)

All the parameters specific to the operation of an SGSN in a UMTS network are configured in an SGSN service configuration. SGSN services use other service configurations like MAP (map-service) and IuPS (iups-service) to communicate with other elements in the network.

To configure an SGSN service:

Step 1 In Context configuration mode, create an SGSN service and give it a unique name.

Step 2 Specify the Core Network (CN) ID that will identify this SGSN service on the CN.

Step 3 Specify the E.164 number to identify this SGSN service.

Step 4 Configure the maximum number of PDP contexts that a UE can establish.

Step 5 Specify the MAP service and the context in which it is configured that this SGSN service should use.

Step 6 Specify the IuPS service name and the context in which it is configured for the SGSN service to use for RAN protocol settings.

Important If a direct tunnel is to be established, GTP-U direct tunneling must be enabled in both the IuPs service and in the call-control-profile. For the IuPS service, the DT must be enabled per RNC; DT is enabled by default on RNCs.

Step 7 Specify the SGTP service and the context in which it is configured for this SGSN service to use for GTP configuration.

Step 8 Specify the CDR types that the SGSN service should generate.

Step 9 Specify the context in which GTPP accounting is configured. If the accounting context is not specified the current context is assumed.

Step 10 Configure the charging characteristics profile. (Number of buckets for the max change condition, volume limit, time limit, and tariff time switch values should be defined individually according to requirements for each of the charging characteristics profiles.

Step 11 *Optional*: Specify the Gs service name and the context in which it is configured.

Important Session Management (SM) and GPRS Mobility Management (GMM) settings can be configured as needed using the SGSN configuration mode commands;sm <*keyword*> andgmm <*keyword*>. Refer to the *SGSN Service Configuration Mode* chapter in the *GPRS/UMTS Command Line Interface Reference*.

Example Configuration

```
configure
   context context_name
     sgsn-service svc_name
       core-network id cn_id
       sgsn-number sgsn_number
       max-pdp-contexts per-ms max_number
       { mobile-application-part-service | associate map-service } map_name
 context map_context
       ran-protocol iups-service iups_svc_name context iups_context
       { sgtp-service | associate sgtp-service } svc_name context name
       accounting cdr-types [ mcdr | scdr ]
       accounting context acct_context
       cc profile profile_number interval seconds
       { gs-service context  | associate gs-service } ctxt service
gs_service_name
       end
```

Notes:

- For releases 12.2 and earlier, use **mobile-application-part-service** *map_name* **context** *map_context* command. For releases 14.0 and later, use the **associate map-service** *map_name* **context** *map_context* command.
- For releases 12.2 and earlier, use the **sgtp-service** *svc_name* **context** *name* command. For releases 14.0 and later, use **associate sgtp-service** *svc_name* **context** *name* command.
- For releases 12.2 and earlier, use the **gs-service context** *ctxt* **service** *gs_service_name* command. For releases 14.0 and later, use the **associate gs-service context** *ctxt* **service** *gs_service_name* command.

Configuring a GPRS Service (2.5G only)

All the parameters specific to the operation of an SGSN in a GPRS network are configured in a GPRS service configuration. GPRS services use other configurations like MAP and SGTP to communicate with other elements in the network. The system can support multiple GPRS services.

To configure a GPRS service:

Step 1 In Context configuration mode, create a GPRS service instance and give it a unique name.

Step 2 Specify the context in which the accounting parameters have been configured.

Step 3 Create a PLMN definition for the GPRS service to include the identity of the mobile country code (MCC) and the mobile network code (MNC).

Step 4 Associate other services (such as a MAP or Gs or SGTP service) and their configurations with this GPRS service. This command should be repeated to associate multiple service types and/or multiple instances.

Step 5 Define the network service entity identifier (NSEI) of one or more remote SGSNs with their location area code (LAC) and routing area code (RAC). This step can be repeated to associate multiple peer-NSEIs.

Step 6 Specify the E.164 number to identify this SGSN.

Step 7 Configure the charging characteristic(s).

Step 8 Specify the types of CDRs to generate.

Example Configuration

```
configure
   context context_name
     gprs-service gprs_service_name
       accounting ctxt
       plmn id mcc mcc_num mnc mnc_num
       { service | associate service | }service_type service_name context
service_ctxt
       peer-nsei peer_nsei_id lac lac_id rac rac_id
       sgsn-number sgsn_isdn_number
       cc profile id buckets value
       cc profile id interval value
       accounting cdr-types cdr_type
       end
```

Configuring a Network Service Entity

Configure a Network Service Entity for IP

Prior to implementing this configuration, the IP interfaces should have been defined in the same context as the GPRS service.

Step 1 In Global configuration mode, create a network service entity (NSE) for IP. The resulting prompt will appear as:

```
[local]<hostname>(nse-ip-local)#
```

Step 2 In the Network Service Entity - IP local configuration mode, create up to four virtual links (NSVLs) for this entity - each with a unique NSVL Id. The resulting prompt will appear as:

```
[local]<hostname>(nse-ip-local-nsvl-<id>)#
```

Step 3 Configure the link access information: IP address, context name, and port number.

Step 4 Configure the links signaling characteristics.

Example Configuration for a Network Service Entity for IP

```
config
   network-service-entity ip-local -n
     nsvl instance id
       nsvl-address ip-address ip_addr context ctxt port num
         signaling-weight num data-weight num
         end
```

Configure a Network Service Entity for Frame Relay

Step 1 In Global configuration mode, create a network service entity (NSE) for Frame Relay. The resulting prompt will appear as:

```
[local]<hostname>(nse-fr-peer-nsei-id)#
```

Step 2 In the Peer NSEI configuration mode, create a virtual connection instance for this entity. The resulting prompt will appear as:

```
[local]<hostname>(nse-fr-peer-nsei-<id>-nsvci-<id>)#
```

Example Configuration for a Network Service Entity for IP

```
config
   network-service-entity peer-nsei id frame-relay
     ns-vc id id -n
     end
```

Configuring DNS Client

DNS client services can be configured for a context.

Step 1 In context configuration mode, enable DNS lookup.

Step 2 Specify the DNS to use for lookups; maximum of two DNS addresses can be used.

Step 3 Create a DNS client with a unique name.

Step 4 In DNS Client configuration mode, bind the DNS client to the IP address of an interface in the current context.

Example Configuration

```
configure
   context context_name
     ip domain-lookup
     ip name-servers ip_address
     dns-client name
        bind address ip_address
       end
```

Configuring GTPP Accounting Support

This section provides instructions for configuring GTPP-based accounting which allows the SGSN to send M-CDR and/or S-CDR accounting data to the Charging Gateways (CGs) over the Ga interface.

The Ga interface and GTPP functionality are typically configured within a separate charging context.

The SGSN begins to generate M-CDR data upon GPRS/IMSI attach. S-CDR data generation begins upon PDP context activation.

Accounting servers can be configured individually or as GTPP accounting server groups. GTPP accounting server groups can each have completely different GTPP settings configured. Although a GTTP server can be included in multiple GTPP groups.

Any GTPP accounting servers configured at the context level that are not specifically configured as part of a GTPP group, are automatically assigned to be part of the GTPP server group called default that is part of every context.

A maximum of 8 GTPP named server groups can be configured across all contexts. A maximum of 4 CGFs can be configured in each GTPP server group. A total of total 32 CGFs can be configured across all server groups, including the server group called default, in one context. Each GTPP group must have unique GTPP charging agents (CGFs) configured.

Important The system supports the specification of the UDP port number for the charging agent function on the system and for the CG. The default charging agent port is 49999. The default CG Server port is (3386). If an SGSN service and a GGSN service are both configured on this system be sure that the UDP ports are unique for each type of service. Refer to the Command Line Interface Reference for information on changing the ports used.

To configure the GTPP accounting support for a SGSN service:

Step 1 Create the GTPP group in accounting context by applying the example configuration in the *Creating GTPP Group* section.

Step 2 Configure the charging agent and GTPP server (CGF) related parameters for the GTPP accounting support by applying the example configuration in the *Configuring GTPP Group* section.

Step 3 Verify your GTPP group and accounting configuration by following the steps in the *Verifying GTPP Group Configuration* section.

Step 4 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Creating GTPP Group

Use the following example to create the GTPP group to support GTPP accounting:

```
configure
 context <vpn_ctxt_name>
 gtpp group <gtpp_group_name> -noconfirm
 end
```

Notes:

- In addition to one default GTPP group "default" a maximum of 8 GTPP groups can be configured with this command in a context.
- In case no GTPP group is configured in this context, system creates a default GTPP group named "default" and all the CGF servers and their parameters configured in this context are applicable to this "default" GTPP group.

Configuring GTPP Group

Use the following example to configure the GTPP server parameters, GTPP dictionary, and optionally CGF to support GTPP accounting:

```
configure
 context <vpn_ctxt_name>
 gtpp group <gtpp_group_name>
 gtpp charging-agent address <ip_address> [ port <port> ]
 gtpp server <ip_address> [ max <msgs >] [ priority <priority>]
 gtpp dictionary <dictionaries>
 gtpp max-cdrs <number_cdrs> [ wait-time <dur_sec> ]
 gtpp transport-layer { tcp | udp }
 end
```

Notes:

- In addition to one default GTPP group "default" a maximum of 8 GTPP groups can be configured with this command in a context.
- In case no GTPP group is configured in this context, system creates a default GTPP group named "default" and all the CGF servers and their parameters configured in this context are applicable to this "default" GTPP group.
- Command for CGF **gtpp charging-agent** is optional and configuring gtpp charging-agent on port 3386 may interfere with ggsn-service configured with the same ip address. Multiple interfaces can be configured within a single context if needed.
- For more information on GTPP dictionary encoding, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *GTPP Interface Administration and Reference*.

- For better performance, it is recommended to configure maximum number of CDRs as 255 with **gtpp max-cdrs** command.
- You can select transport layer protocol as TCP or UDP for Ga interface with **gtpp transport-layer** command. By default it is UDP.
- Multiple GTPP server can be configured using multiple instances of this command subject to following limits:
  - Total 4 GTPP server in one GTPP group
  - Total 32 GTPP server in one context
  - Total 9 GTPP groups (1 default and 8 user defined GTPP groups) can be configured in one context. Number of CGFs in 1 GTPP group is limited to 4 and a total of 32 CGF servers across all GTPP groups in one context are configurable.

Verifying GTPP Group Configuration

Verify that your CGFs were configured properly by entering the following command in *Exec Mode*:

```
show gtpp accounting servers
```

This command produces an output similar to that displayed below:

```
context: source
Preference      IP                                Port      Priority          State
  Group
----------    ---------------        ----      --------        -------              ------
Primary          192.168.32.135          3386                    1          Active
default
Primary          192.168.89.9              3386                100          Active
default
```

Configuring and Associating the EGTP Service (S4 Only)

This section describes how to configure and associate the EGTP service to support S4-SGSN functionality.

The SGSN communicates with the EPC network SGW via the GTPv2 protocol over the S4 interface. GTPv2 is configured on the chassis as part of an EGTP service. Once configured, the EGTP service then must be associated with the configured UMTS (3G) and/or GPRS (2G) service configured on the system to provide access to the EPC network.

Once the EGTP service is associated with the UTRAN and/or GERAN service, then the S4-SGSN will be chosen for PDP context activation in the following cases:

- If the last known capability of the UE indicates that it is EPC-capable.
- If the last known capability of the UE indicates it is non-EPC capable but has an EPS subscription only.
- If a PDP context is already activated for the UE, and the S4 interface is already selected for the UE.

Important The S4 feature license must be enabled on the S4-SGSN to configure the EGTP service.

Important S4 support for the SGSN requires the presence of an SGTP service, even though S4 support is being configured for the SGSN to use the S4 interface. The SGTP service is required to interface with non-EPC capable roaming partners via the Gn interface. SGTP is also required for subscribers using mobile phones that are not EPC-capable in an EPC network.

Important Currently, the S4-SGSN does not support the transfer of PDP contexts from the S4 interface to the Gn interface within the same S4-SGSN.

Use the following procedure to configure and associate the EGTP service to for S4 functionality on the SGSN:

Step 1 Access *Context Configuration Mode*.

Step 2 Create and configure the EGTP service in the desired context.

Step 3 Configure the interface type for the EGTP service.

Step 4 Configure the validation mode for the EGTP service. The default and recommened setting is **standard**.

Step 5 Associate the EGTP service with the configured 2.5G service (if configured).

Step 6 Associate the EGTP service with the configured 3G service (if configured).

Example Configuration

```
config
    context context_name
      egtp-service service_name
        gtpc  bind ipv4-address  ipv4_address
        interface-type interface-sgsn
        validation-mode standard
        end
config
   context context_name
      gprs-service gprs_service_name
        associate egtp-service egtp_service_name context context_name
        end
config
   context context_name
     sgsn-service sgsn_service_name
        associate egtp-service egtp_service_name context context_name
        end
```

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Important If you modify the **interface-type** command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

Configuring and Associating the GTPU Service (S4 Only)

This section describes how to configure and associate the GTPU service on the S4-SGSN.

The GTPU service is required to support the EGTP service for the sending and receiving of GTP bearer packets to and from the EPC SGW.

Use the following procedure to configure and associate the GTPU service:

Step 1 Access *Context Configuration Mode*.

Step 2 Create the GTPU service in the same context where the **egtp-service** is configured.

Step 3 Bind the GTPU service to the IP address to be used for GTP-U (the S4-SGSN side IP address for GTP-U packets).

Step 4 Associate the GTPU service with the configured **egtp-service**.

Example Configuration

```
config
   context context_name
     gtpu-service service_name
       bind ipv4-address ipv4_address
       end
config
   context egtp-service_context_name
     egtp-service egtp-service_name
       associate gtpu-service egtp_service_name
       end
```

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Configuring the DNS Client Context for APN and SGW Resolution (Optional)

This section describes how to configure the context from which DNS client has to be selected for performing an APN FQDN query for resolving a PGW address (S4-SGSN) or a co-located PGW / GGSN address (Gn SGSN), and the context from which DNS client has to be selected for performing an RAI FQDN query for resolving an SGW address (S4-SGSN).

By default, the S4-SGSN supports the initiation of a DNS query after APN selection using a S-NAPTR query for EPC-capable subscribers. The S4-SGSN resolves a PGW/GGSN by sending an APN-FQDN query to the DNS client. Similarly, the S4-SGSN resolves the SGW by sending a RAI-FQDN query to the DNS client. The DNS Client then sends a query to the DNS server to retrieve NAPTR/SRV/A records and return the SGW or PGW IP address to the SGSN.

Important For non-EPC capable subsribers, the S4-SGSN initiates only a DNS A query.

The Gn SGSN supports selecting a co-located PGW/GGSN node for EPC capable UEs by performing a DNS SNAPTR lookup for APN FQDN for the service parameter**"x-3gpp-pgw:x-gn" / "x-3gpp-pgw:x-gp"**. Note that in addition to these parameters, the service parameters In addition to these interfaces **"x-3gpp-ggsn:x-gn" & "x-3gpp-ggsn:x-gp"** are used for selecting standalone GGSNs.

For performing a DNS SNAPTR query, the SGSN requires an additional, optional, configuration that identifies the context where DNS lookup for EPC-capable UEs must occur. This is accomplished by creating a call-control-profile that specifies the context from which the DNS client should be used for resolving a co-located PGW/GGSN address on a Gn SGSN as well.

Use the following procedure to configure and associate the configure DNS for APN resolution to support S4 functionality:

Step 1 Access *Call Control Profile Configuration Mode* and create a call control profile.

Step 2 Configure the DNS client context to resolve PGW UEs via the context the DNS client is configured.

Step 3 Configure the DNS client context to resolve SGW UEs via the context where the DNS client is configured.

Example Configuration

```
config
   call-control-profile name
     dns-pgw context dns_client_context_name
     dns-sgw context dns_client_context_name
     end
```

Notes:

- **dns-pgw context** is valid for selecting a PGW (in an S4-SGSN) as well as a co-located PGW/GGSN (in a Gn/GP- SGSN). If the interface selected for a UE is S4 and if there is no **dns-pgw context** configured under the Call Control Profile, then by default it will look for the DNS client in the context where the

EGTP service is defined. If the interface selected for a UE is Gn/Gp, and if there is no **dns-pgw context** configured under the Call Control Profile, then by default the system will look for the DNS client in the context where the SGTP service is configured for selecting co-located PGW/GGSNs if:

- The UE is EPC capable and,
- **apn-resolve-dns-query snaptr** is configured under an APN Profile.

- **dns-sgw context** specifies the name of the context where the DNS client is configured and that will be used for DNS resolution of SGWs. If **dns-sgw** is not configured, the S4-SGSN uses the DNS client configured in the context where EGTP service is configured to query the SGW DNS address.

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Configuring the S6d Diameter Interface (S4 Only)

This section describes how to configure the S6d Diameter interface to support S4 functionality.

The S6d interface is a Diameter-based interface used to support S4 functionality by enabling the S4-SGSN to communicate with the HSS. The HSS is a master user database that contains all subscription related information, and performs the following functions:

- Authentication and authorization of the user
- Provides the subscribers location information
- Provides the subscribers IP information

To support the S6d interface, an HSS Peer Service must be configured and associated with a Diameter endpoint. This HSS Peer Service is then associated with the configured SGSN and/or GPRS services to enable communication with the HSS via the S6d interface. Optionally, operators can configure an operator policy-based interface selection.

Configuring the S6d interface consists of the following procedures:

1. Configuring a Diameter Endpoint for the S6d interface
2. Configuring the HSS Peer Service and Interface Association for the S6d interface
3. Associating the HSS Peer Service with the SGSN and GPRS Services for the S6d interface.
4. Optional. Configuring operator policy-based interface selection for the S6d interface.

Configuring the Diameter Endpoint for the S6d Interface

Use the following procedure to configure the Diameter endpoint for the S6d interface:

Step 1 Configure a port that will be bound to an interface (at step 3) to be used as the S6d interface.

Step 2 Configure an Ethernet interface to be used as a diameter endpoint.

Step 3 Configure a Diameter endpoint to be used as the S6d interface.

Step 4 Specify the origin host address and the IP address of the Ethernet interface to be used as the S6d interface.

Step 5 Specify the origin realm. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service provider's name.

Step 6 Specify the peer name, peer realm name, peer IP address and port number. The peer IP address and port number are the IP address and port number of the HSS.

Step 7 Specify the route entry peer. This parameter is optional. The route entry peer parameter is required if multiple HSS peers are configured under a Diameter point and operators want to associate a routing weight to each HSS peer so that the S4-SGSN contacts each HSS based on the weight distribution.

Step 8 Optional. Enable or disable the **watchdog-timeout** parameter.

Step 9 The **use-proxy** keyword can be specified in the **diameter-endpoint** command to enable the proxy mode. The usage of proxy mode depends on the operator's HSS capabilities.

Example Configuration

```
config
  port ethernet slot number/port number
    no shutdown
    bind interface s6d_interface_name context_name
    end
config
  context context_name
    interface s6d_interface_name
      ip address s6d_interface_ip_address subnet_mask
      exit
    diameter endpoint endpoint_name
      origin host host_name address s6d_interface_ip_address
      origin realm realm_name
      peer peer_name realm realm_name address hss_ip_address
      route-entry peer route_entry_name
      use-proxy
      no watchdog-timeout
      end
```

Configuring the HSS Peer Service and Interface Association for the S6d Interface

Use the following procedure to configure the HSS Peer Service and interface association for the S6d interface:

Step 1 Configure a Diameter endpoint. If not already configured, refer to the Configuring the Diameter Endpoint for the S6d Interface, on page 140 Then specify the IP address of the Ethernet interface configured in Step 1 as the Diameter endpoint address.

Step 2 Associate the Diameter endpoint with an HSS peer service.

Step 3 Specify the Diameter dictionary to be used for the HSS Peer Service. The **standard-r9** dictionary must be used for the S6d interface.

Example Configuration

```
config
   context sgsn_context_name
     hss-peer-service hss_peer_service_name
       diameter hss-endpoint hss_endpoint_name
       diameter hss-dictionary standard_r9
       end
```

Associating the HSS Peer Service with the SGSN and GPRS Services for the S6d Interface

Use this procedure to association the HSS Peer Service with the SGSN and GPRS Services:

Step 1 Access *Context Configuration Mode* and create an SGSN service.

Step 2 Associate the HSS peer service name with the SGSN service.

Step 3 Access *Context Configuration Mode* and create a GPRS service.

Step 4 Associate the HSS peer service name with the GPRS service.

Example Configuration

```
config
   context context name
     sgsn-service sgsn-service-name
       associate hss-peer-service hss-peer-service-name
       end
config
   context context name
     gprs-service gprs-service-name
       associate hss-peer-service hss-peer-service-name
       end
```

Configuring Operator Policy-Based S6d Interface Selection (Optional)

It is mandatory for the SGSN and GPRS services to have either a MAP service association or an HSS-Peer-Service association.

- If no MAP service is associated with the SGSN or GPRS services, and only the HSS service is associated with the SGSN or GPRS services, then the S6d interface is selected.
- If both the MAP service and the HSS-Peer-Service are associated with the SGSN or GPRS service, by default the Gr interface is selected. To override the default use of the Gr interface, configure the operator policy to select the **s6d-interface**.
- Once the interface selection is configured, the call-control-profile is first checked to determine whether to select the MAP-interface or HSS-interface. If neither the MAP nor HSS is configured under the call control profile, then the system checks the configured SGSN or GPRS-services.

Step 1 Access *Call Control Profile Configuration Mode* and create a call-control-profile.

Step 2 Associate the configured HSS peer service with the S6d interface. The **s6d-interface** option must be selected.

Example Configuration

```
config
   call-control-profile name
    associate hss-peer-service name s6d-interface
    end
```

Configuring the Subscription Interface Preference for the S6d Interface (Optional)

The S4-SGSN provides a mechanism to associate a MAP service with call-control-profile. In some situations, it is possible that both the MAP service and the HSS peer service are associated with the Call Control Profile. In these cases, operators can configure the preferred subscription interface.

Step 1 Access *Call Control Profile Configuration Mode* and create a call-control-profile.

Step 2 Specify the preference of the subscription-interface. Selecting the **hlr** option will cause the MAP protocol to be used to exchange messages with the HLR. The **hss** option causes the Diameter-protocol to be used to exchange messages with the HSS.

Example Configuration

```
config
   call-control-profile name
    prefer subscription-interface { hlr | hss }
    end
```

Configuring the S13' Interface (S4 Only, Optional)

The S13' (S13 prime) interface is a Diameter-based interface that is used to perform the Mobile Equipment (ME) identity check procedure between the SGSN and EIR. Configuring the S13' interface is optional.

The SGSN performs ME identity check to verify the Mobile Equipment's identity status.

The S13'interface uses the Diameter protocol. An HSS Peer Service must be configured and associated with a Diameter endpoint. It is not mandatory to configure the HSS Peer Service under the SGSN or the GPRS service. By configuring the HSS Peer Service in *Call Control Profile Configuration Mode*, the S13'interface can be used.

In the absence of an operator policy, the HSS Peer Service must be associated with the configured SGSN or GPRS service to be able to utilize the S13'interface. In the presence of an operator policy, the operator policy configured overrides the service configured in the SGSN or GPRS service.

Important The S13' interface can only be configured after the S6d interface has been configured. Refer to Configuring the S6d Diameter Interface (S4 Only), on page 140 procedure for information on configuring the S6d interface.

Configuring the S13' interface consists of the following procedures;

Step 1 Configure a Diameter Endpoint for the S13' interface.

Step 2 Configure the HSS Peer Service and Interface association for the S13' interface.

Step 3 Associate the HSS Peer Service with the SGSN and GPRS services for the S13' interface.

Step 4 Optional. Configure an operator policy S13-based interface selection call control profile for the S13' interface.

Configuring a Diameter Endpoint for the S13' Interface

Use this procedure to configure a Diameter endpoint for the S13' interface:

Step 1 Access *Context Configuration Mode* and create a Diameter endpoint.

Step 2 Specify the origin host address and the IP address of the S13'interface.

Step 3 Specify the origin realm. The realm is the Diameter identity. The originator's realm is present in all Diameter messages and is typically the company or service name.

Step 4 Specify the peer name, peer realm name, peer IP address and port number. The peer IP address and port number are the IP address and port number of the HSS.

Step 5 Specify the route entry peer (optional). The route entry peer parameter is required if multiple HSS or EIR peers are configured under a Diameter point and operators wish to associate a routing weight to each HSS or EIR peer so that SGSN contacts each HSS or EIR based on the weight distribution.

Step 6 The user can optionally enable or disable the parameter watchdog-timeout.

Step 7 The **use-proxy** keyword can be specified in the diameter-endpoint command to enable the proxy mode. The usage of proxy mode depends on the operator's EIR capabilities.

Example Configuration

```
config
  port ethernet s13'_interface_name
    no shutdown
    bind interface s13'_interface_name sgsn_context_name
    end
config
  context context_name
    interface s13'_interface_ip subnet_mask
    exit
    diameter endpoint s13'_endpoint_name
      origin host host_name address host_address
      origin realm realm_address
```

```
  peer peer_name realm realm_name  address hss_ip_address
  route-entry peer route_entry_name
  use-proxy
  no watchdog-timeout
  exit
 hss-peer-service hss_peer_service_name
  diameter hss-endpoint s6d_endpoint_name eir-endpoint s13'_endpoint_name
  end
```

Configuring the HSS Peer Service and Interface Association for the S13' Interface

Use the following procedure to configure the HSS Peer Service and Interface association:

Step 1 Configure an Ethernet interface to be used as a Diameter endpoint.

Step 2 Configure a Diameter endpoint and specify the IP address of the Ethernet interface configured in Step 1 as the Diameter endpoint address.

Step 3 Configure an HSS peer service and associate it with the Diameter endpoint configured for the S6d and S13' interfaces.

Step 4 Specify the Diameter dictionary to be used for the HSS-Peer-Service. The **standard-r9** option must be selected for the SGSN.

Example Configuration

```
config
   port ethernet slot_number/port_number
     no shutdown
     bind interface s6d_interface_name  sgsn_context_name
     end
config
   context sgsn_context_name
     interface s6d_interface_name
       ip address s6d_interface_ip_address subnetmask
       exit
     diameter endpoint s6d-endpoint_name
       origin realm realm_name
       origin host  name address s6d_interface_address
       peer peer_name realm realm_name address hss_ip_address
       exit
     diameter endpoint s13'_endpoint_name
       origin realm realm_name
       origin host name address s13'_interface_address
       peer peer_name realm realm_name  address eir_ip_address
       exit
     hss-peer-service hss_peer_service_name
       diameter hss-endpoint hss_endpoint_name  eir-endpoint  eir_endpoint_name
       diameter hss-dictionary standard-r9
       end
```

Associating the HSS Peer Service with the SGSN and GPRS Services for the S13' Interface

Use this procedure to associate the HSS Peer Service with the SGSN and GPRS services.

Step 1 In *Context Configuration Mode* create a SGSN service.

Step 2 Associate the HSS peer service with SGSN service, if configured, and provide the HSS peer service name and context name.

Step 3 Associate the HSS peer service with GPRS service, if configured, and provide the HSS peer service name and context name.

Example Configuration

```
config
   context context_name
     sgsn-service sgsn_service_name
       associate hss-peer-service hss-peer-service-name
       end
config
   context context_name
     gprs-service gprs_service_name
       associate hss-peer-service hss-peer-service-name
       end
```

Configuring S13' Interface Selection Based on an Operator Policy

It is mandatory for the SGSN and GPRS service to have either a MAP service association or an HSS Peer Service association.

- In the absence of a MAP service association with SGSN or GPRS service, and if the HSS service is associated with the SGSN or GPRS service then the S13' interface is selected.
- If both the MAP service and the HSS-Peer-Service are associated with the SGSN or GPRS service, by default the Gf interface is selected. To override this default, operators can configure an operator policy to configure behavior for the S13' interface selection.
- Once configured, the behavior is as follows:
  - First, the call control profile is checked to determine on whether a MAP or HSS interface is configured.
  - If neither A MAP or HSS is configured under the call control profile, then the system uses the configuration in the SGSN or GPRS service.

Use this procedure to configure an operator policy used for S13' interface selection.

Step 1 Access *Call Control Configuration Mode* and configure a call-control-profile.

Step 2 Associate the HSS Peer Service with the **s13-prime-interface**.

Example Configuration

```
config
   call-control-profile name
     associate hss-peer-service name s13-prime-interface
     end
```

Configuring QoS Mapping for EPC-Capable UEs using the S4 Interface (S4 Only, Optional)

An S4-SGSN communicates QoS parameters towards the SGW and PGW in EPC QoS. However, it sends QoS towards the UE in the QoS format defined in the GMM/SM specification (TS 24.008). 3GPP defines a mapping for EPS QoS to pre-release 8 QoS in TS 23.401, Annex E. On the S4-SGSN, operators can configure the quality of service (QoS) parameters as Call Control Profiles that will ensure proper QoS mapping between the S4-SGSN and the EPC gateways (PGW and SGW) and UEs. However, such configurations are optional. If no mapping is configured, then the S4-SGSN uses the default mapping.

The configured Call Control Profiles also will be used if the S4 interface is chosen for PDP activation, but the subscription does not have an EPS subscription. Therefore, GPRS subscription data (which uses QoS in pre-release 8 format), will be mapped to EPS QoS behavior. The allocation and retention policy will be mapped to EPS ARP using the configured Call Control Profiles. Specifically, the configuration provided in this section enables the S4-SGSN to:

- Map EPC ARP (allocation and retention priority) parameters to pre-release 8 ARP (Gn/Gp ARP) parameters during S4-SGSN to Gn SGSN call handovers.
- Map ARP parameters received in a GPRS subscription from the HLR to EPC ARP parameters if the S4 interface is selected for an EPC capable UE that has only a GPRS subscription (but no EPS subscription) in the HLR / HSS.

If the QoS mapping configuration is not used, the following default mappings are used:

- Default ARP **high-priority** value = 5
- Default ARP **medium-priority** value = 10
- Default **pre-emption capability** = **shall-not-trigger-pre-emption**
- Default **pre-emption vulnerability** = **pre-emptable**

Use this procedure to configure QoS mapping for EPC Gateways and UEs:

Step 1 Access *Call Control Profile Configuration Mode* and create a call-control-profile.

Step 2 Configure the QoS ARP settings.

Step 3 Exit back to the Local prompt.

Step 4 Access the call-control profile you just configured.

Step 5 Configure the QoS pre-emption or vulnerability capabilities.

Example Configuration

```
config
   call-control-profile cc_profile_name
    qos gn-gp arp high-priority hi_prior_value medium-priority med_prior_value

    end
config
   call-control-profile cc-profile-name
    qos gn-gp  pre-emption { capability { may-trigger-pre-emption |
shall-not-trigger-pre-emption } | vulnerability { not-pre-emptable |
pre-emptable } }
    end
```

Configuring the Peer SGSN Interface Type (S4 Only, Optional)

Operators can specify the type of interface the S4-SGSN will use to communicate with the peer SGSN in a call control profile.

Use the following procedure to configure the peer SGSN interface type:

Step 1 Access the Call Control Profile configuration for the peer SGSN.

Step 2 Configure the interface type to be used for communication between the S4-SGSN and the peer SGSN. **s16** must be specified if the peer SGSN is an S4-SGSN.

Example Configuration

```
config
   call-control-profile cc_profile_name
    sgsn-address { rac rac value lac lac value  | rnc_id rnc_id } prefer {
local | fallback-for-dns }  address ipv4 ipv4 address interface { gn | s16
}
    end
```

Notes:

- The **rnc_id** parameter can be used instead of the **rac** and **lac** values if operators wish to configure the target RNC ID that maps to the address of the peer SGSN via the S16 interface. The RNC ID is used by the S4-SGSN for inter-SGSN SRNS relocation. Configuration of the **rnc_id** is optional, and valid only if SRNS relocation first has been configured in *Call Control Profile Configuration Mode* using the **srns-inter** and/or **srns-intra** commands.
- The **fallback-for-dns option** is under development for future use, and is not currently supported on the S4-SGSN.
- NRI-based validation is not supported on the S4-SGSN.

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Configuring Gn Interface Selection Based on an Operator Policy (S4 Only, Optional)

The S4-SGSN uses the S4 interface to communicate with EPC-capable UEs. However, operators have the to option to create a call-control-profile that enables the S4-SGSN to forcefully select the Gn interface for EPC-capable UEs.

Use this procedure to forcefully select the Gn interface for EPC-capable UEs:

Step 1 Access *Call Control Profile Configuration Mode*.

Step 2 Create a call-control-profile.

Step 3 Configure the SGSN to forcefully select the Gn interface.

Example Configuration

```
config
   call-control-profile cc_profile_name
     sgsn-core-nw-interface { gn | s4 }
     end
```

Notes:

- **sgsn-core-nw-interface** specifies the interface that EPC-capable UEs will use to communicate with the packet core gateways (GGSN/SGW). The default setting for EPC-capable UEs is **s4**.

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Configuring a Custom MME Group ID (S4 Only, Optional)

3GPP specifications define how a GUTI allocated by an MME is translated into an old P-TMSI and old RAI when a UE hands over to an SGSN. 3GPP specifications state that when a GUTI is mapped to an old RAI, the MME group ID portion of the GUTI will be mapped to a Location Area Code (LAC). MME group IDs are 16-bit numbers which always have their most significant bit set. As a result, their range is 32768 - 65535.

However, some operators may have already configured their networks with LACs for UTRAN and GERAN coverage in the 32768 - 65535 range. To provide backward compatibility for such deployments, a custom list of MME group IDs must be configured for use by both the S4-SGSN and MME products for UTRAN/GERAN and E-UTRAN handovers.

Once the custom MME Group IDs have been configured, operators then can configure the S4-SGSN to use the available custom MME Group IDs configured for both GPRS (2G) and UTRAN (3G) network services.

Use the following procedure to configure the SGSN to use the custom MME Group IDs:

Step 1 Access *LTE Network Global MME ID Management Database Configuration Mode*.

Step 2 Specify the PLMN MCC and MNC values.

Step 3 Configure the low and high end values of the LAC range to be used.

Step 4 Access the context in which the SGSN (3G) service is configured.

Step 5 Associate the 3G service (if configured), with the MME's Network Global MME ID Management Database that contains the custom list of MME Group IDs.

Step 6 Access the context in which the 2G GPRS service is configured.

Step 7 Associate the 2G service, if configured, with the MME's Network Global MME ID Management Database that contains the custom list of MME Group IDs.

Example Configuration

```
config
   lte-policy
     network-global-mme-id-mgmt-db
      plmn mcc mcc_value mnc mnc_value mme-group-id-range first  low_end_of_range
 last high_end_of_range
       exit
     exit
 context context_name
   sgsn-service sgsn_service_name
     associate network-global-mme-id-mgmt-db
     end
config
   context context_name
     gprs-service gprs_service_name
     associate network-global-mme-id-mgmt-db
     end
```

Configuring and Associating the Selection of an SGW for RAI (S4 Only, Optional)

If operators wish to bypass DNS resolution of RAI FQDN for obtaining the S-GW address, the SGSN can select an S-GW by performing a local configuration look-up for the current Routing Area Instance (RAI). This is accomplished by configuring the TAI Management Database (tai-mgmt-db) of the SGSN to select an

S-GW address and its associated RAI. In addition, the TAI Management Database must be associated with the 2G and/or 3G services configured on the SGSN. The TAI Management Database can also be associated with a call-control-profile for RAI-to-SGW address mapping.

Use the following procedure to configure the selection of an SGW for RAI:

Step 1 Access *Global Configuration Mode*.

Step 2 Access *LTE Policy Configuration Mode*.

Step 3 Create a TAI Management Database and enter *TAI Management Database Configuration Mode*.

Step 4 Create a TAI Management Object and enter *TAI Management Object Configuration Mode*.

Step 5 Configure the RAI. Specify the RAI MCC, MNC, LAC and RAC values.

Step 6 Configure the SGW address serving the RAI. Specify the IPv4 address, the S5-to-S8 protocol as GTP, and the load balancing Weight for this SGW. On the S4-SGSN, only GTP is supported as the protocol option.

Step 7 Access *SGSN Service Configuration Mode* and associate the configured UTRAN (3G) service with the S-GW addresses and their associated RAIs.

Step 8 Access *GPRS Service Configuration Mode* and associate the configured GERAN (2G) and service with the S-GW addresses and their associated RAIs.

Step 9 *Optional*. Associate the SGW address-to-RAI mapping with a call-control-profile.

Example Configuration

```
config
   lte-policy
     tai-mgmt-db tai_mgmt_db_name
       tai-mgmt-ojb obj_name
         rai mcc mcc_value mnc mnc_value lac lac_value rac rac_value
         sgw-address ipv4_addr | ipv6_addr s5-s8-protocol gtp weight number
         end
config
   context context_name
     sgsn-service sgsn_service_name
       associate tai-mgmt-db tai_mgmt_db_name
       end
config
   context context_name
     gprs-service gprs_service_name
       associate tai-mgmt-db tai_mgmt_db_name
       end
config
   call-control-profile cc_profile_name
     associate tai-mgmt-db tai_mgmt_db_name
     end
```

Configuring a Local PGW Address (S4 Only, Optional)

If operators wish to bypass DNS resolution of APN FQDN on the S4-SGSN for obtaining a PGW address, the S4-SGSN can be configured to use a locally configured PGW IPv4 address in an APN profile.

Use the following procedure to configure the local PGW address:

Step 1 Access *APN Profile Configuration Mode* and create an APN profile.
Step 2 Specify the address resolution mode for the PGW as **local**.
Step 3 Configure the P-GW address.
Step 4 Configure the load balancing **weight** preference for the P-GW.

Example Configuration

```
config
   apn-profile apn_profile_name
     address-resolution-mode local
     pgw-address ipv4_address | ipv6_address weight weight_preference
     end
```

Configuring the Peer MME Address (S4 Only, Optional)

For operators wishing to bypass DNS resolution to obtain the peer EPC MME address, the SGSN supports the local configuration of a peer MME address for a given MME group (LAC) and MME code (RAC).

Use the following procedure to configure the peer MME address:

Step 1 Access *Call Control Configuration Mode* and create a call-control-profile.
Step 2 Configure the peer MME Group ID LAC and RAC values or the TAC.
Step 3 Specify a **local** preference for selection of the peer MME address.
Step 4 Specify the local MME address to use for lookup instead of a DNS query.
Step 5 Specify the interface type to use when communicating with the peer MME. The interface must be **s3**.

Example Configuration

```
config
   call-control-profile cc-profile-name
     peer-mme { mme-groupid  lac_value mme-code  rac_code | tac tac } prefer
local address ipv4_address | ipv6_address interface { gn [ s3 ] | s3 [ gn ] }

     end
```

Notes:

- The **tac** keyword can be used instead of the **mme-groupid** and **mme-code** parameters to configure the Tracking Area Code (TAC) of the target eNodeB that maps to the peer MME address. The TAC is used by the S4-SGSN for UTRAN to E-UTRAN (SGSN to MME) SRNS relocation across the S3 interface. Configuration of the **tac** is valid only if SRNS relocation first has been configured in *Call Control Profile Configuration Mode* via the **srns-inter** and/or **srns-intra** commands.

Configuring the ISR Feature (S4 Only, Optional)

Idle Mode Signaling Reduction (ISR) is a license-enabled feature that allows the UE to roam between LTE and 2G/3G networks while reducing the frequency of TAU and RAU procedures due to the UE selecting E-UTRAN or UTRAN networks. ISR reduces the signaling between the UE and the network, and also reduces the signaling between the E-UTRAN and UTRAN networks.

Use the following procedure to configure the ISR feature:

Step 1 Access *Call Control Configuration Mode*.

Step 2 Create a call-control-profile.

Step 3 Enable the Idle Mode Signaling Reduction feature for 3G (UMTS) network access

Step 4 Set the T3323 timeout value that the configured SGSN service will send to the UE in Attach Accept and RAU Accept messages.

Step 5 Enable the ISR feature for 2G network access

Step 6 Configure the implicit detach timer for 2G subscribers.

Example Configuration

```
config
   call-control-profile cc-profile-name
     idle-mode-signaling-reduction access-type umts
     end
config
   context context_name
     sgsn-service sgsn_service_name
     gmm T3323-timeout dur_mins
     end

config
   call-control-profile name
     idle-mode-signaling-reduction access-type gprs
     end
config
   context plmn_name
     gprs-service gprs_service_name
     gmm implicit-detach-timeout secs
     end
```

Notes:

- **idle-mode-signaling-reduction access-type umts** enables ISR for 3G network access.
- **gmm T3323-timeout** *dur_mins* is the amount of time, in minutes, the UE should wait after the Periodic RAU timer (T3312 timer) expiry before deactivating ISR for the 3G subscriber. Valid entries are from 1 to 186. The default is 54.
- **idle-mode-signaling-reduction access-type umts** enables ISR for 2G network access.
- **gmm implicit-detach-timeout** *secs* specifies the implicit detach timeout value to use for 2G ISR. Valid entries are from 240 to 86400 seconds. The default value is 3600 seconds.

Configuring IDFT for Connected Mode Handover (S4 Only, Optional)

The S4-SGSN supports the setup of indirect data forwarding tunnels (IDFT) between the eNodeB and the RNC via the SGW during connected mode handovers. This allows the S4-SGSN to support connected mode handovers between the UTRAN and E-UTRAN networks across the S3 interface.

Once enabled, IDFT is employed under the following conditions:

- **If the SGSN is the old node participating in the connected mode handover**:
  - The target node to which the connected mode handover is initiated should be an eNodeB (i.e., the SGSN performs the handover to the MME.
  - The **enb-direct-data-forward** CLI setting is not configured in the target RNC configuration (in RNC Configuration Mode).
- **If the SGSN is the new node participating in the connected mode handover**:
  - The source node from which connected mode handover is initiated is an eNodeB (i.e., the MME is performing a handover to the SGSN).
  - The **enb-direct-data-forward** CLI setting is not configured in the target RNC configuration (in RNC Configuration Mode).
  - The source MME indicated that it does not support direct forwarding via a Forward Relocation Request.

Important If the target SGSN did **not** relocate to a new SGW, then IDFT does not apply. The target SGSN sets up an indirect data forwarding tunnel with the SGW only if the SGW is relocated. If the SGW is not relocated, then the source MME sets up the indirect data forwarding tunnel between the source eNodeB and the target RNC through the SGW.

Important By default, indirect data forwarding is enabled, and direct forwarding is disabled.

To configure IDFT for connected mode inter RAT handovers:

Step 1 Enter the context where the IuPS service is configured.

Step 2 Enter IuPS Service Configuration Mode and enter the configured IuPS service.

Step 3 Enter the RNC ID of the IuPS service for which you want to enable IDFT.

Step 4 Disable direct data forwarding for connected mode inter RAT handovers.

Example Configuration

```
config
   context context_name
     iups-service iups_service_name
       rnc id rnc_id
          no enb-direct-data-forward
          end
```

Where:

- **no enb-direct-data-forward** enables the setup of IDFT between the eNodeB and the RNC via the SGW for connected mode inter RAT handovers. If IDFT is enabled, the SGSN/MME will send the IDFT request towards the SGW. Once enabled, the SGSN/MME will send IDFT requests towards the SGW.
- To disable IDFT, enter the **enb-direct-data-forward** command.

Creating and Configuring ATM Interfaces and Ports (3G only)

ATM ports and their associated PVCs can be configured for use with point-to-point interfaces and defined in a context or they can be bound to link IDs defined in SS7 routing domains.

Refer to the chapter titled *System Element Configuration Procedures* in the *System Administration Guide* for information on configuring ATM interfaces.

Creating and Configuring Frame Relay Ports (2.5G only)

Frame Relay ports and their associated DLCIs can be configured for communication with 2G Base Station subsystem (BSS) for an SGSN implementation.

Refer to the chapter titled *System Element Configuration Procedure*s in the *System Administration Guide* for information on configuring Frame Relay ports.

Configuring APS/MSP Redundancy

ASP/MSP redundancy is only available for the OLC2 and CLC2 line cards. It is setup per linecard -- all ports share the same setup.

APS is enabled with the **redundancy** command in the Card configuration mode.

Important At this time the **aps** command in the *Card Configuration Mode* chapter is still in development and should not be used. The parameters are all set by default and cannot be changed or disabled.

- Related configuration for signal degrade and signal failure bit error rate thresholds for high path, low path, and transport overhead - use the commands in the Port Channelized configuration mode.

For command details, refer to the *Card Configuration Mode Commands* chapter and the *Port Configuration Mode Commands* chapter in the ***Cisco UMTS Command Line Interface Reference.***

Step 1 Configure a line card for either SONET or SDH.

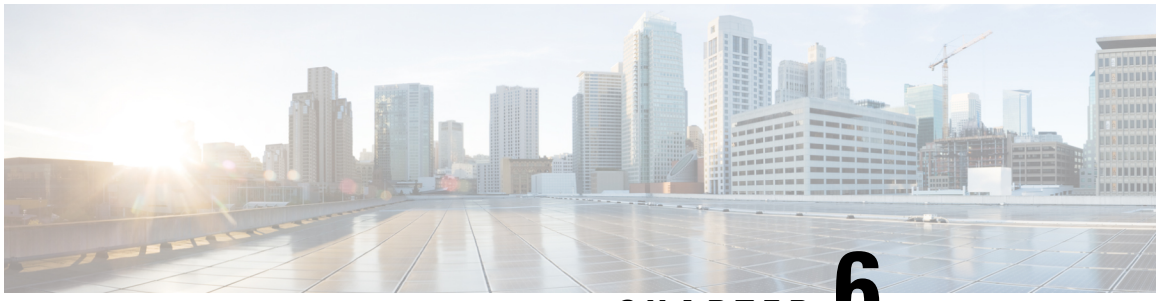
Step 2 Configure APS for a SONET line card or MPS for an SDH line card.

Use the configuration example below:

Example Configuration

Use the following example (replacing specific values) to setup a CLC2 (Frame Relay) line card:

```
config
      card 27
            framing sdh e1
            header-type 4-byte
            initial-e1-framing standard
            redundancy aps-mode
            service-type frame-relay
            no shutdown
            end
```



CHAPTER 6

3G-2G Location Change Reporting

3G/2G Location Change Reporting on the SGSN facilitates location-based charging on the GGSN by providing the UE's location information when it is in connected mode.

The SGSN notifies the GGSN whenever one of the following changes:

- The serving Cell Global Identity (CGI), or
- The Service Area Identity (SAI), or
- The Routing Area Identity (RAI).

Important With Release 16, the new "Location-reporting in connected-mode" license is required to enable Location Change Reporting functionality. For details, contact your Cisco Account Representative.

- Feature Description, on page 157
- How it Works, on page 158
- Configuring Location Change Reporting, on page 160

Feature Description

The 3G/2G Location Change Reporting feature enables the operator to charge the user for location-based services. Location-based charging is a values-added function that ensures subscribers pay a premium for operator-determined location-based services, such as service in a congested area.

This optional feature functions in accordance with 3GPP TS 23.060, Release 9, sections 12.7.5 and 15.1.3 and requires an additional license - the Location Reporting License. With the license, the operator uses the CLI to enable the feature independently for each access type: GPRS (2G) or UMTS (3G).

Relationships

The SGSN works with the GGSN for this feature. The GGSN must send subscription information to the SGSN for the 3G/2G Location Change Reporting feature to work.

This feature is independent of user location information (ULI) configuration, which allows GTP-C messages to be used for carrying user location information to the GGSN.

License

A feature-specific license is required. Please consult your Cisco Account Representative for information about the specific license. For information on installing and verifying licenses, refer to the "Managing License Keys" section of the *Software Management Operations* chapter in the *System Administration Guide*.

Standards Compliance

The SGSN 3G/2G Location Change Reporting feature complies with the following standards:

- 3GPP TS 23.060 Release 9
- 3GPP TS 29.060 Release 9.7.0

How it Works

When the Location Change Reporting feature is enabled, the SGSN advertizes support for location change reporting to the GGSN by including an extension header - MS-Info-Change-Reporting indication - in the Create-PDP-Context-Request (CPCQ) or the Update-PDP-Context-Request (UPCQ) GTP-C messages (as specified in section 6.1.5 of TS 23.060, R9).

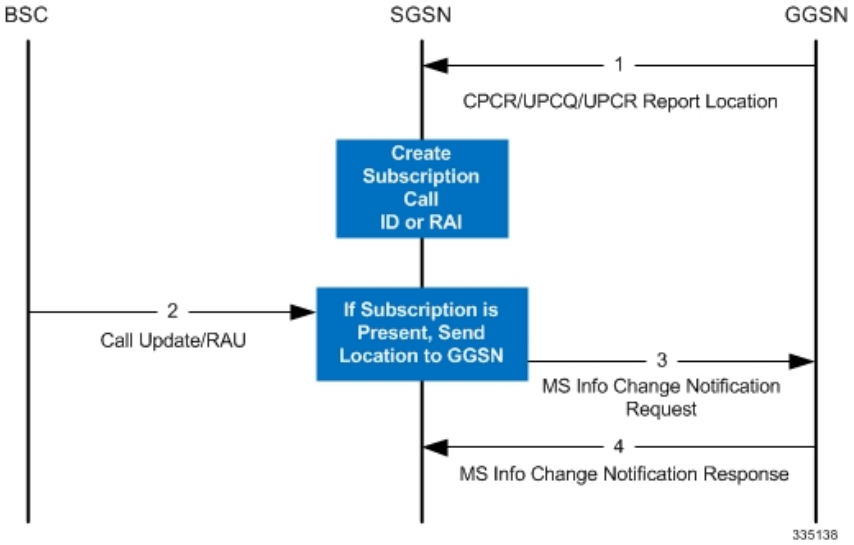
The SGSN initiates the process to report the UE location when subscription information is received from the GGSN. The SGSN decodes the MS-Info-Change-Reporting-Action IE in the CPCR, the UPCQ, and the UPCUPCR messages received from the GGSN that request the SGSN to check user locations.

The SGSN uses cell update procedures, location reporting procedures, and routing area update (RAU) procedures to identify changes in the serving cell (2G), or in the service area (3G), or in the routing area respectively to identify location changes. In a 2G network, the SGSN sends location information to the GGSN when it receives a cell update from a BSC. In a 3G network, the SGSN sends information to the GGSN when it receives location reports from the RNC. If the GGSN subscribes to the RAI changes and the UE performs an RAU, then the SGSN informs the GGSN of the new RAI.

Call Flows

The following call flows illustrate system behavior when the feature is enabled.

Figure 17: 2G Subscription



1. Subscription is created.
2. Determines if subscription is present.
3. Location is sent to all GGSNs to which the UE subscribes.

Figure 18: 3G Subscription

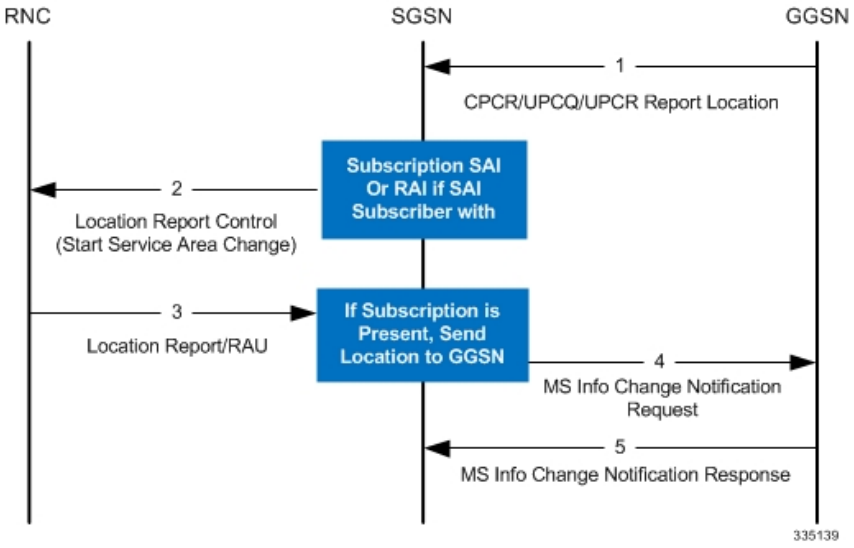
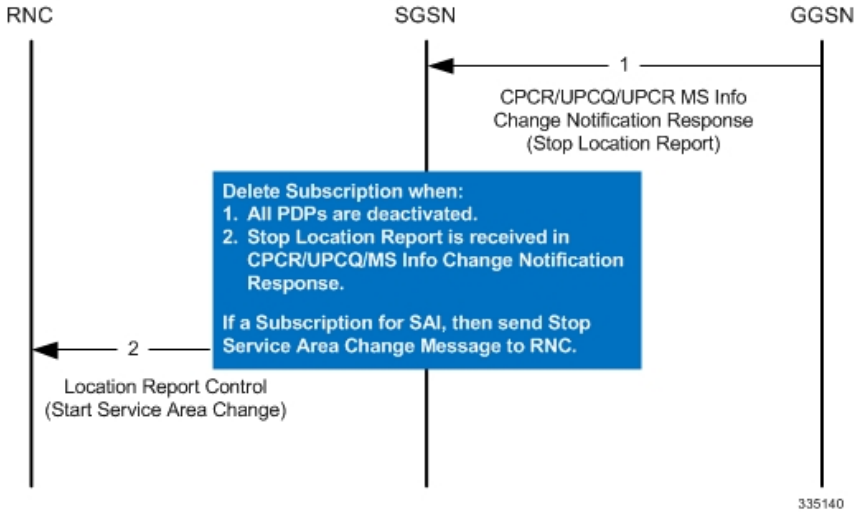


Figure 19: Delete Subscription



Configuring Location Change Reporting

By default, Location Change Reporting is disabled. Reporting to the GGSN is easily enabled in the Call Control Profile configuration mode.

The following configuration enables this feature:

```
config
     call-control-profile <cc_profile_name>
          location-reporting { gprs | umts }
          exit
```

Notes:

- The command can be repeated to enable location change reporting for GPRS (2G) and UMTS (3G).

The following configuration disables this feature:

```
config
     call-control-profile <cc_profile_name>
          remove location-reporting { gprs | umts }
          exit
```

Notes:

- Using the **remove** keyword with the command disables the feature.

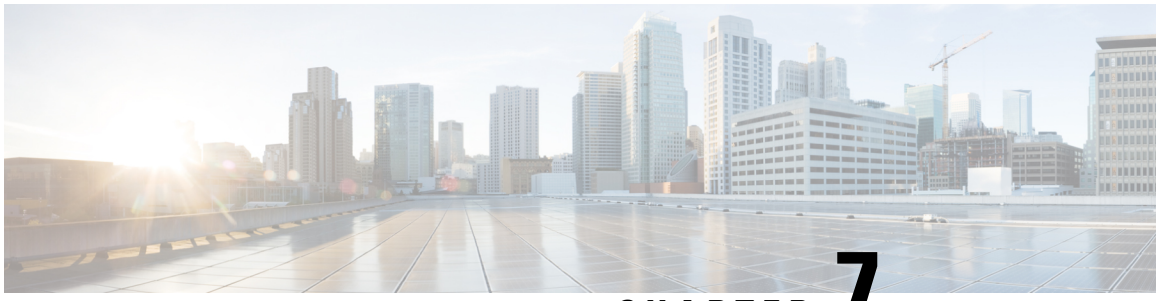
Verifying the Location Change Reporting Configuration

This section explains how to display the configuration after saving it in the .cfg file as described in the *System Administration Guide*.

Verification for the call control profile configuration is accomplished via the corresponding show command in Exec Mode:

show call-control-profile

```
[local]S4SGSN_Sim show call-control-profile full name ccprof1

Call Control Profile Name = ccprof1
Accounting Mode (SGW)                    : None
GPRS Attach All                          : Allow
GPRS Attach All Failure Code             : 14
UMTS Attach All                          : Allow
UMTS Attach All Failure Code             : 14
  .  .  .
  .  .  .
Location Reporting for UMTS                        : Enabled
Location Reporting for GPRS                        : Enabled
 EPS Attach Restrict
   Voice Unsupported                     : FALSE
IMSI Attach Fail                         : FALSE
CSFB Restrictions
```



CHAPTER 7

5G NSA for SGSN

- Feature Summary and Revision History, on page 163
- Feature Description, on page 164
- How It Works, on page 165
- Configuring 5G NSA for SGSN, on page 168
- Monitoring and Troubleshooting, on page 169

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	ASR 5000
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *5G Non Standalone Solution Guide* • *AAA Interface Administration and Reference* • *Command Line Interface Reference* • *SGSN Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.5

Feature Description

The 5G NSA solution for SGSN supports the following functionalities:

- **Dual Connectivity with New Radio (DCNR):**

  The UE supporting dual connectivity with New Radio (NR) sets the DCNR bit to "dual connectivity with NR supported" in the MS network capability IE of the "Attach Request" or "Routing Area Update Request" message.

  If the MS supports dual connectivity of E-UTRA with New Radio (NR), then the MS sets the Dual connectivity of E-UTRA with NR capability bit to "Mobile station supports dual connectivity of E-UTRA with NR" in the MS network capability IE of the "Attach Request" or "Routing Area Update Request" message.

  SGSN informs DCNR support to GGSN by setting the DCNR bit in the UP Function Selection Indication Flags IE of the Create PDP Context Request message.

  If all the conditions (UE DCNR capable, SGSN 5G-NSA support) are met, SGSN sends the GPRS Location Update Request with “nrAsSecondaryRAT” bit set in the Supported Features IE in MAP Interface Gr.

- **Dynamic Gateway Selection:**

  When DCNR capable UE attempts to register in SGSN and all DCNR validations are successful (for example, DCNR feature configuration on SGSN, HLR not sending "access-restriction" for NR, and so on) for dynamic gateway selection, SGSN uses the following service parameters received from DNS server (in NAPTR response) over other service parameters to select NR capable gateway:

  - x-3gpp-pgw:x-gn+nc-nr
  - x-3gpp-pgw:x-gp+nc-nr

  In order to select a network node with a particular network capability, the character string "+nc-<network capability>" must be appended to the "app-protocol" name where "nc" indicates "network capability", "nr" indicates "new radio", "x-gn" is "app protocol" and "x-3gpp-ggsn/pgw" are app services.

  For a DCNR capable UE, when the service parameters are received without network capability and new radio character string "+nc-nr", SGSN uses other service parameters to perform dynamic gateway selection.

  When the dynamic selection of gateway fails for any other reasons, SGSN fallbacks and selects the locally configured gateway.

- **DCNR Support to GGSN:**

  SGSN advertises the DCNR feature support by sending "NR as Secondary RAT" feature bit in "Supported Features" towards HLR, if DCNR feature is configured at SGSN and UE advertises DCNR capability in NAS.

  When DCNR capable UE attempts to register in SGSN and when all DCNR validations are successful (for example, DCNR feature configuration on SGSN, HLR not sending access-restriction for NR, and so on), the SGSN sets the UP Function Selection Indication Flags IE with DCNR flag set to 1 in the Create PDP Context Request message. This flag enables the selection of a PGW-U optimized for NR, when the UE establishes the PDN connection first through Gn-SGSN and the Gn-SGSN will pass a corresponding indication over Gn/Gp to the GGSN/P-GW.

- **Subscription Control:**

SGSN handles the reception of “NR as Secondary RAT Not Allowed” bit in Extended-Access Restriction Data IE in “Insert Subscriber Data” message from HLR.

- **Extended Bandwith:**

  SGSN handles the reception of "Extended Maximum Bit rate DL" and "Extended Maximum Bit rate UL" in AMBR IE received in the "Insert Subscriber Data" message from HLR.

- **Access Restriction Data:**

  SGSN supports Access Restriction data information in MM Context IE while receiving/sending from/to peer SGSN during ISRAU and SRNS Relocation procedures.

How It Works

Limitations

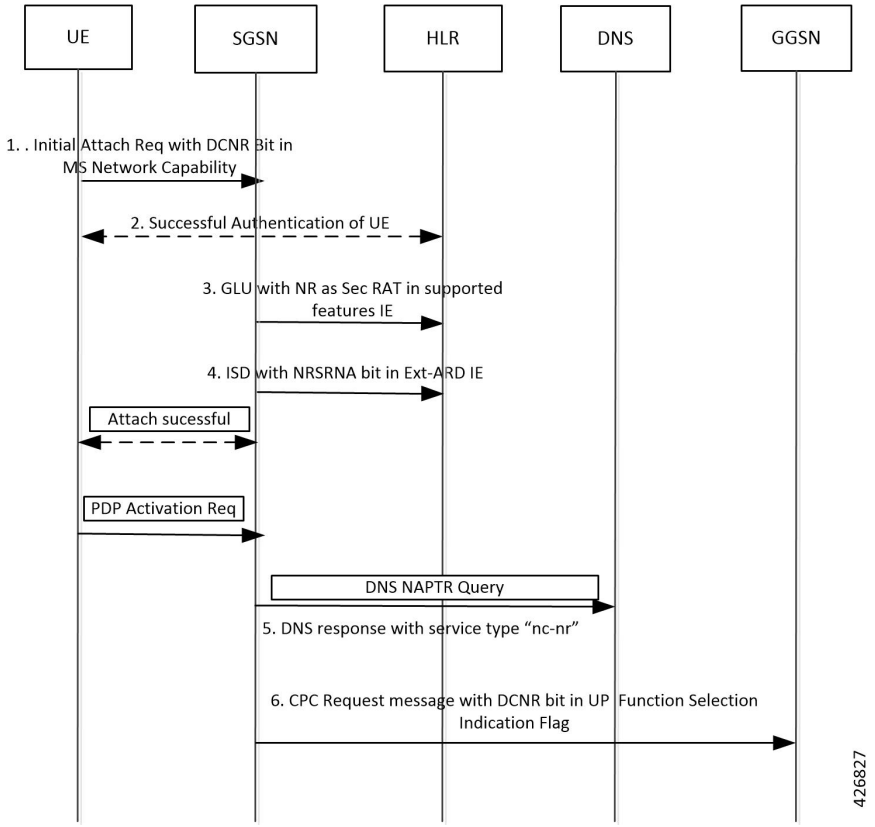
This section describes the known limitations for 5G NSA feature:

- To support EPC QOS parameters like "APN-AMBR", "E-ARP" and "UE-AMBR", “Support for EPC QoS Attributes on SGSN” feature must be enabled. Currently this feature is supported only on 3G not on 2G. So Extended Bandwidth support is only on 3G-SGSN.
- 5G-NSA enabled SGSN uses only MAP Protocol on the Gr Interface, Diameter Protocol on the s6d Interface is not supported.
- If HLR does not send "Extended-Access Restriction" data IE in Insert Subscribe Data message, SGSN assumes that NR as secondary RAT is allowed and it processes the UE request as DCNR enabled.
- When SGSN cannot find a collocated PGW/GGSN which “+nc-nr” in DNS response, SGSN falls back and triggers "A" query to get the normal GGSN information.
- SGSN with 5G-NSA feature enabled selects only the collocated PGW/GGSN in DNS response, for example “*x-3gpp-pgw x-gn+nc-nr/ x-3gpp-pgw x-gp+nc-nr*.”

Flows

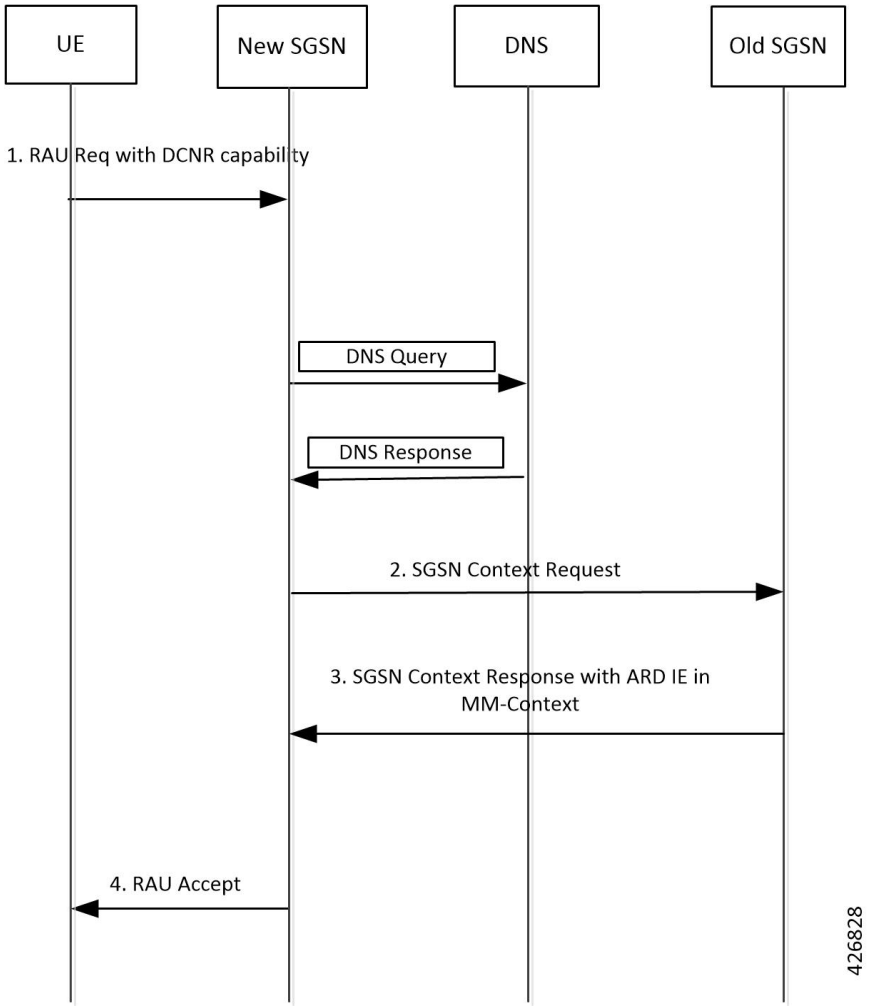
This section describes the call flow procedures related to SGSN for 5G NSA.

Figure 20: Initial Attach Request with DCNR



1. DCNR capable UE sends “DCNR bit” in NAS message “Attach Request” in “MS Network Capability” IE.
2. SGSN successfully authenticates the UE.
3. SGSN advertises the DCNR feature support by sending “NR as Secondary RAT” feature bit in “Supported Features”.
4. If HLR determines that the UE is not authorized for DCNR services, HLR sends Subscription-Data with “Extended Access-Restriction” carrying “NR as Secondary RAT Not Allowed”.
5. SGSN determines the Gateway which is NR capable from the DNS response.
6. SGSN sends Create PDP Context Request with the UP Function Selection Indication Flags coded with DCNR bit to the selected gateway.

Figure 21: Inter SGSN RAU



1. DCNR capable UE sets “DCNR bit” in NAS message “RAU Request” in “MS Network Capability” IE.
2. New-SGSN triggers SGSN Context Request message to OLD-SGSN where the UE is previously attached to get UE context.
3. OLD-SGSN fills the MM-Context with Access-Restriction Data IE with NRSRNA in SGSN Context Response message.
4. After Authentication and verifying subscription information, NEW SGSN sends RAU Accept message to UE.

Standards Compliance

Cisco's implementation of the 5G NSA feature complies with the following standards:

- 3GPP 23.003 Release 15.2.0 - 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Numbering, addressing and identification.

- 3GPP 23.401 Release 15.2.0 - General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.
- 3GPP 29.002 Release 15.2.0 - 3rd Generation Partnership Project; Technical Specification Group Core Networkand Terminals; Mobile Application Part (MAP) specification.
- 3GPP 24.008 Release 15.1.0 - 3rd Generation Partnership Project; Technical Specification Group Core Networkand Terminals; Mobile radio interfaceLayer3 specification; Core network protocols; Stage3.
- 3GPP 29.060 Release 15.1.0 - 3rd GenerationPartnershipProject Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP)acrossthe Gn and Gp interface.
- 3GPP 29.303 Release 15.1.0 - 3rd Generation Partnership Project; Technical Specification Group Core Networkand Terminals; Domain Name System Procedures; Stage3.
- 3GPP 29.303 Release 15.2.0 - 3rd Generation Partnership Project; Technical Specification Group Core Networkand Terminals; Domain Name System Procedures; Stage3.

Configuring 5G NSA for SGSN

This section describes how to configure 5G NSA to support SGSN.

Configuring 5G NSA involves:

Enabling DCNR in Call Control Profile

Use the following configuration to enable Dual Connectivity with New Radio (DCNR) to support 5G Non Standalone (NSA).

```
configure
  call-control-profile profile_name
    [ no | remove ] dcnr
    end
```

NOTES:

- **call-control-profile** *profile_name*: Creates an instance of a call control profile. *profile_name* specifies the name of the call control profile as an alphanumeric string of 1 to 64 characters.
- **no**: Disables the DCNR configuration in the call control profile.
- **remove**: Removes the DCNR configuration from the call control profile.

  Removes existing configuration related to DCNR at Call-Control-Profile level (either ‘dcnr’ or ’ no dcnr’), and behaviour depends on the configuration at sgsn-global level.

Configuring DCNR in SGSN Global Configuration

Use the following configuration to enable Dual Connectivity with New Radio (DCNR) for 5G NSA support in the SGSN Global Configuration mode.

With this configuration, SGSN processes the UEs with 5G capability and selects the gateways that are NR capable to inform the peer MME/SGSN nodes.

```
config
  sgsn-global
    [ no ] dcnr
    end
```

NOTES:

- **dcnr**: Configures DCNR to support 5G NSA.
- **no**: Disables the DCNR support.
- This feature is applicable only to Gn-SGSN.

Monitoring and Troubleshooting

This section provides information regarding show commands and bulk statistics available to monitor and troubleshoot the 5G NSA feature.

Show Commands and Outputs

show sgsn-mode

The output of this command includes the following fields:

SGSN Global Configuration:

- Dual Connectivity Support with NR capability

show subscribers sgsn-only/gprs-only full

The output of this command includes the following fields:

MS Network Capability:

- DCNR capability: Indicates MS is capable of DCNR or not.

Subscription Data:

Extended ARD:

- NR-As-Secondary-RAT-Not-Allowed - Advertises the DCNR feature support by sending “NR as Secondary RAT” feature bit towards HLR provided DCNR feature is configured at SGSN and UE advertises DCNR capability in NAS.

show gmm-sm statistics

The output of this command includes the following fields:

Session Statistics:

Attached Subscribers:

- 3G-with-DCNR-Attached - The total number of subscribers with DCNR allowed for 3G service.
- 2G-with-DCNR-Attached - The total number of subscribers with DCNR allowed for 2G service.

Activated Subscribers:

- 3G Activated with DCNR - Total number of activated subscribers with DCNR capable allowed for 2g service.
- 2G Activated with DCNR - Total number of activated subscribers with DCNR capable allowed for 2g service.

Activate PDP Contexts:

Total Actv PDP Ctx:

- 3G-Actv Pdp CTx with DCNR - The total number of active PDP contexts established with NR capable P-GW/GGSN.
- 2G-Actv Pdp Ctx with DCNR - The total number of active PDP contexts established with NR capable P-GW/GGSN.

Message Statistics:

Specific Procedures:

Attach Request:

- 3G-with-DCNR-Cap-Attached - Total number of 3G Attach Requests received from DCNR capable UEs.
- 2G-with-DCNR-Cap-Attached - Total number of 2G Attach Requests received from DCNR capable UEs.

Attach Accept:

Total-Attach-Accept:

- 3G-Attach-Accept-with-DCNR - Total number of 3G Attach Requests accepted with DCNR allowed for DCNR capable UEs.
- 2G-Attach-Accept-with-DCNR - Total number of 2G Attach Requests accepted with DCNR allowed for DCNR capable UEs.

Attach Complete:

- 3G-Att-Comp-with-DCNR-Cap - Total number of attach complete received for DCNR allowed UEs for 3G service.
- 2G-Att-Comp-with-DCNR-Cap - Total number of attach complete received for DCNR allowed UEs for 2G service.

Attach Reject:

- 3G-Attach-Reject-with-DCNR - Total number of 3G Attach Requests Rejected for DCNR capable UEs.
- 2G-Attach-Reject-with-DCNR - Total number of 2G Attach Requests Rejected for DCNR capable UEs.

Routing Area Update Request:

- 3G-RAU-Req-with-DCNR-Cap - Total number of 3G RAU Requests received from DCNR capable UEs.
- 2G-RAU-Req-with-DCNR-Cap - Total number of 2G RAU Requests received from DCNR capable UEs.

Routing Area Update Accept:

- 3G-RAU-Acc-with-DCNR-Cap - Total number of 3G RAU Requests accepted with DCNR allowed for DCNR capable UEs.
- 2G-RAU-Acc-with-DCNR-Cap - Total number of 2G RAU Requests accepted with DCNR allowed for DCNR capable UEs.

Routing Area Update Complete:

- 3G-RAU-Comp-with-DCNR-Cap - Total number of 3G RAU complete received for DCNR allowed UEs.
- 2G-RAU-Comp-with-DCNR-Cap - Total number of 2G RAU complete received for DCNR allowed UEs.

Routing Area Update Reject:

- 3G-RAU-Rej-with-DCNR-Cap - Total number of 3G RAU Requests Rejected for DCNR capable UEs.
- 2G-RAU-Rej-with-DCNR-Cap - Total number of 2G RAU Requests Rejected for DCNR capable UEs.

Session Management Messages Statistics:

- 3G-Actv-Request-with-DCNR-Capability - Total number of 3G Activation Requests received for DCNR allowed UEs.
- 2G-Actv-Request-with-DCNR-Capability - Total number of 2G Activation Requests received for DCNR allowed UEs.

Primary-Actv-Request:

- 3G-Primary-Actv-Request-with-DCNR-Capability - Total number of 3G primary Activation Requests received for DCNR allowed UEs.
- 2G-Primary-Actv-Request-with-DCNR-Capability - Total number of 2G primary Activation Requests received for DCNR allowed UEs

Activate Context Accept:

- 3G-Acvt-Accept-with-DCNR - Total number of 3G Primary Activation Accepted with PDP context established with NR capable P-GW/GGSN.
- 2G-Acvt-Accept-with-DCNR - Total number of 2G Primary Activation Accepted with PDP context established with NR capable P-GW/GGSN.

Activate Context Reject:

- 3G-Acvt-Reject-with-DCNR - Total number of 3G Primary Activation Rejected for DCNR allowed UEs
- 2G-Acvt-Reject-with-DCNR - Total number of 2G Primary Activation Rejected for DCNR. allowed UEs.

SRNS statistics:

Attempted

Inter-SRNS UE involved Inter-SRNS UE not involved (new SGSN with MME) -

- Inter-SRNS NRSRNA UE involved Inter-SRNS NRSRNA UE not involved (old SGSN) - Inter-SGSN SRNS from the local SGSN to the peer SGSN is attempted with relocation type 'UE not involved' and DCNR allowed.
- Inter-SRNS NRSRNA UE involved Inter-SRNS NRSRNA UE not involved (new SGSN) - Inter-SGSN SRNS to the local SGSN from the peer SGSN is attempted with relocation type 'UE not involved and DCNR allowed

Inter-SRNS UE not involved (new SGSN with MME):

- Inter-SRNS NRSRNA UE not involved (old SGSN) - Inter-SGSN SRNS from the local SGSN to the peer SGSN is attempted with relocation type 'UE not involved' and DCNR allowed
- Inter-SRNS NRSRNA UE not involved (new SGSN) – Inter-SGSN SRNS from the local SGSN to the peer SGSN is attempted with relocation type 'UE not involved' and DCNR allowed.

Sucessful:

Total SRNS:

- Intra-SGSN SRNS (new SGSN with MME) - Intra SGSN from local SGSN to peer MME is attempted with relocation type UE not Involved /Involved and DCNR allowed.
- Inter-SRNS NRSRNA UE involved (old SGSN) - Inter-SGSN SRNS to the peer SGSN from the local SGSN with dcnr is attempted with relocation type 'UE involved' and DCNR allowed.
- Inter-SRNS NRSRNA UE involved (new SGSN) - Inter-SGSN SRNS to the peer SGSN from the local SGSN with DCNR is attempted with relocation type 'UE involved’ and DCNR allowed.

Bulk Statistics

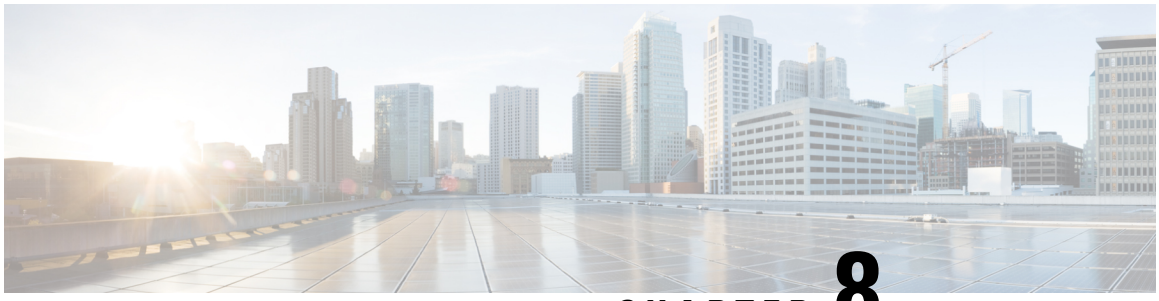
The following 5G NSA feature related bulk statistics are available in the SGSN schema.

Bulk Statistics	Description
2G-attached-with-dcnr	The total number of subscribers with DCNR allowed for 2G service.
2G-attached-pdp-with-dcnr	the total number of subscribers attached having PDF established with NR capable P-GW/GGSN.
2G-activated-pdp-with-dcnr	The total number of active PDP contexts established with NR capable P-GW/GGSN.
2G-attach-req-with-dcnr	The total number of 2G Attach Requests received from DCNR capable UEs.
2G-attach-accept-with-dcnr	The total number of 2G Attach Requests accepted with DCNR allowed for DCNR capable UEs.
2G-attach-reject-with-dcnr	The total number of 2G Attach Requests Rejected for DCNR capable UEs.

Bulk Statistics	Description
2G-rau-with-dcnr	The total number of 2G RAU Requests received from DCNR capable UEs.
2G-rau-accept-with-dcnr	The total number of 2G RAU Requests accepted with DCNR allowed for DCNR capable UEs.
2G-rau-complete-with-dcnr	The total number of 2G RAU complete received for DCNR allowed UEs.
2G-rau-reject-with-dcnr	The total number of 2G RAU Requests Rejected for DCNR capable UEs.
2G-total-active-with-dcnr	The total number of 2G Activation Requests received for DCNR allowed UEs.
2G-total-primary-active-with-dcnr	The total number of 2G primary Activation Requests received for DCNR allowed UEs.
2G-total-primary-active-accept-with-dcnr	The total number of 2G Primary Activation Accepted with PDP context established with NR capable P-GW/GGSN.
2G-total-primary-active-reject-with-dcnr	The total number of 2G Primary Activation Rejected for DCNR.allowed UEs.
3G-attach-complete-with-dcnr	The total number of attach complete received for DCNR allowed UEs.
2G-attach-complete-with-dcnr	The total number of attach complete received for DCNR allowed UEs.
3G-attached-with-dcnr	The total number of subscribers with DCNR allowed for 3G service.
3G-attached-pdp-with-dcnr	The total number of subscribers attached having pdp established with NR capable P-GW/GGSN.
3G-activated-pdp-with-dcnr	The total number of active PDP contexts established with NR capable P-GW/GGSN.
3G-attach-req-with-dcnr	The total number of 3G Attach Requests received from DCNR capable UEs.
3G-attach-accept-with-dcnr	The total number of 3G Attach Requests accepted with DCNR allowed for DCNR capable UEs.
3G-attach-reject-with-dcnr	The total number of 3G Attach Requests Rejected for DCNR capable UEs.
3G-rau-with-dcnr	The total number of 3G RAU Requests received from DCNR capable UEs.

Bulk Statistics	Description
3G-rau-accept-with-dcnr	The total number of 3G RAU Requests accepted with DCNR allowed for DCNR capable UEs.
3G-rau-complete-with-dcnr	The total number of 3G RAU complete received for DCNR allowed UEs.
3G-rau-reject-with-dcnr	The total number of 3G RAU Requests Rejected for DCNR capable UEs.
3G-total-active-with-dcnr	The total number of 3G Activation Requests received for DCNR allowed UEs.
3G-total-primary-active-with-dcnr	The total number of 3G primary Activation Requests received for DCNR allowed UEs.
3G-total-primary-active-accept-with-dcnr	The total number of 3G Primary Activation Accepted with PDP context established with NR capable P-GW/GGSN.
3G-total-primary-active-reject-with-dcnr	The total number of 3G Primary Activation Rejected for DCNR.allowed UEs.
Important It is an assumed that all the UEs are DCNR capable for the below mentioned counters.	
att_old_sgsn_inter_srns_dcnr_ue_involved	Inter-SGSN is attempted with relocation type 'UE involved' and DCNR allowed.
att_old_sgsn_inter_srns_dcnr_ue_not_involved	Inter-SGSN SRNS from the local SGSN to the peer SGSN is attempted with relocation type 'UE not involved' and DCNR allowed.
att_new_sgsn_inter_srns_dcnr_ue_involved	Inter-SGSN SRNS to the local SGSN from the peer SGSN is attempted with relocation type 'UE involved' and DCNR allowed.
att_new_sgsn_inter_srns_dcnr_ue_not_involved	Inter-SGSN SRNS to the local SGSN from the peer SGSN is attempted with relocation type 'UE not involved and DCNR allowed.
suc_old_sgsn_inter_srns_dcnr_ue_involved	Inter-SGSN SRNS to the peer SGSN from the local SGSN with DCNR is attempted with relocation type 'UE involved' and DCNR allowed.
suc_old_sgsn_inter_srns_dcnr_ue_not_involved	Inter-SGSN SRNS from the local SGSN to the peer SGSN is attempted with relocation type 'UE not involved' and DCNR allowed.
suc_new_sgsn_inter_srns_dcnr_ue_involved	Inter-SGSN SRNS to the peer SGSN from the local SGSN with DCNR is attempted with relocation type 'UE involved’ and DCNR allowed.

Bulk Statistics	Description
suc_new_sgsn_inter_srns_dcnr_ue_not_involved	Inter-SGSN SRNS from the local SGSN to the peer SGSN is attempted with relocation type 'UE not involved' and DCNR allowed.



CHAPTER 8

APN-OI-Replacement for Gn-SGSN

- Feature Description, on page 177
- How It Works, on page 178
- Monitoring and Troubleshooting, on page 180

Feature Description

Overview

Beginning with release 19.4, in compliance with 3GPP TS 29-003, decoding of the APN-OI-Replacement IE is supported by Cisco Gn-SGSNs using either a Gr MAP or an S6d Diameter interface.

The Gn-SGSN accepts the APN-OI-Replacement field included as part of the GPRS subscription. Typically, the field value, stored at the HLR/HSS as part of the subscription data, is a domain name for a specific GGSN. The value in the APN-OI-Replacement field is intended to replace the APN-OI (derived from the IMSI) during the GGSN selection process. The replacement results in the construction of a fully qualified domain name (FQDN) APN, for a preferred GGSN, to be used for DNS resolution.

Supported Functions

UE-Level

- The Gn-SGSN supports decoding of a UE-level APN-OI-Replacement IE from the HLR/HSS via either MAP or Diameter interface.
- The Gn-SGSN stores the UE-level APN-OI-Replacement value as a subscription database record.
- The Gn-SGSN uses the APN-OI-Replacement only for DNS translation in selection of a Home GGSN.
- The APN sent to other entities (GGSN/SGSN, CGF) is not affected by APN-OI replacement.

APN-Level

- The Gn-SGSN supports decoding of a APN-level APN-OI-Replacement IE from the HLR/HSS via either MAP or Diameter interface.
- The Gn-SGSN stores the APN-level APN-OI-Replacement value *per APN* as a subscription database record.

- The Gn-SGSN uses the APN-level APN-OI-Replacement, even when a UE-level APN-OI-Replacement is present, because the APN-level APN-OI-Replacement has higher priority.
- The Gn-SGSN uses the APN-OI-Replacement only for DNS translation while accessing Home GGSN.
- The APN sent to other entities (GGSN/SGSN, CGF) is not affected by APN-OI replacement.

Gn-SGSN

- The Gn-SGSN indicates APN-level and UE-level APN-OI replacements received in subscriptions as part of the output generated by the **show subscriber gprs-only | sgsn-only full all** command.
- The Gn-SGSN applies APN-level APN-OI-Replacement when both APN-level and UE-level APN-OI replacement are available for a PDP context.

Benefits

This feature makes it possible for the operator to use UE-level and/or APN-level APN-OI replacement to substitute an APN-OI per UE or per APN and then redirects the PDP session to a different GGSN.

This fully-compliant 3GPP functionality enables operators to differentiate service or customer UE and/or APN levels based on the HLR/HSS subscription.

Limitations

The Gn-SGSN does not handle EPS subscription. This means that even though the Gn-SGSN supports S6d, the APN-OI-Replacement in an EPS subscription is not applicable.

Related Product Support

Decoding of this AVP is supported by both the Cisco S4-SGSN and MME for EPS subscriptions.

License Information

This feature is enabled by default and does not require a feature license.

Configuration

Because this feature is 3GPP compliant and does not require enabling or configuration, there are no CLI commands or keywords specific to this feature.

How It Works

The Gn-SGSN supports decoding of the UE and/or APN level APN-OI-Replacement IE received in GPRS subscriptions on either the Gr interface or the S6d interface.

In accord with 3GPP TS 23.060:

- UE-level APN-OI-Replacement field values are conditionally stored as permanent data in the HSS/HLR and the SGSN.
- APN-level APN-OI-Replacement field values are conditionally stored as permanent data in the HSS and the SGSN.

- APN-level APN-OI-Replacement has the same role as UE-level APN-OI-Replacement. If both the APN-level APN-OI-Replacement and the UE-level APN-OI-Replacement are present, the APN-level APN-OI-Replacement has a higher priority than UE-level APN-OI-Replacement.

The format of the domain name used in the APN-OI-Replacement field (as defined in 3GPP TS 23.060 and 3GPP TS 23.401) is the same as the default APN-OI except that it may be preceded by one or more labels, each separated by a dot.

- Example 1: province1.mnc012.mcc345.gprs
- Example 2: ggsn-cluster-A.provinceB.mnc012.mcc345.gprs

The APN-OI-Replacement handling is case insensitive.

The APN constructed using the APN-OI-Replacement field is only used for DNS translation to locate the Home GGSN. DNS translation for other entities is unaffected.

Flow

1. During a 2G/3G Attach procedure, the Gn-SGSN receives an Insert Subscriber Data (ISD) during UGL/ULR from the HLR/HSS.
2. APN-OI-Replacement IE is present in the Subscription-Data AVP sent in an Insert-Subscriber-Data-Request (IDR) if the UE-level APN-OI-Replacement has been added or modified in the HSS.

   APN-OI-Replacement IE is present in the GPRS-Subscription-Data sent in an Insert-Subscriber-Data (ISD) if the UE-level APN-OI-Replacement has been added or modified in the HLR.
3. APN-OI-Replacement IE is present in the PDP-Context AVP sent within an Insert-Subscriber-Data-Request (IDR) if the APN-level APN-OI-Replacement has been added or modified in the HSS.

   APN-OI-Replacement IE is present in the PDP-Context IE in the GPRS-Data-List sent within an Insert-Subscriber-Data (ISD) if the APN-level APN-OI-Replacement has been added or modified in the HLR.
4. After receiving an APN-OI-Replacement from an HLR/HSS,
   - the Gn-SGSN decodes the IE,
   - the Gn-SGSN replaces the stored information (if any) with the received APN-OI-Replacement under the subscription dB record for the subscriber on the SGSN,
   - during activation of the PDP context, the Gn-SGSN presents this replacement APN-OI to be used for the DNS resolution to determine the GGSN.
5. The HLR (MAP) removes the UE-level APN-OI-Replacement by setting the "APN-OI-Replacement withdraw" bit of the Delete-Subscriber-Data (DSD), sent over Gr.

   The HSS removes the UE-level APN-OI-Replacement by setting the "APN-OI-Replacement" bit of the Delete-Subscriber-Data-Request (DSR) flag field of S6d.

Monitoring and Troubleshooting

Monitor Protocol

Monitor Protocol functionality is supported for this feature and can be used by enabling MAP (55), Diameter (36), and DNS Client (70).

⚠

Caution Protocol monitoring can be intrusive to subscriber sessions and could impact system performance. We recommend that you contact your Cisco Support Representative prior to using it for troubleshooting.

Output of "show" Commands

The Gn-SGSN displays received UE-level APN-OI-Replacements under GPRS subscriptions and APN-level APN-OI-Replacements under PDP subscription data of the output generated by the **show subscriber [gprs-only | sgsn-only] full imsi** *imsi* commands.

Quick Check

To quickly check for APN-OI-Replacement use the following **grep** command with either the **gprs-only** or the **sgsn-only** keyword:

show subscribers gprs-only full imsi *imsi* **| grep Repl**

The following illustrates the type of output generated by the above command. The first line is for UE-level replacement information and the second line illustrates APN-level replacement information:

```
 APN OI Replacement : abc.ggg.mnc009.mcc262.gprs
 APN OI Replacement: : ggg.mnc009.mcc262.gprs
```

Full Display

To generate the full output, use the same command without the **grep** option:

show subscribers gprs-only full imsi *imsi*

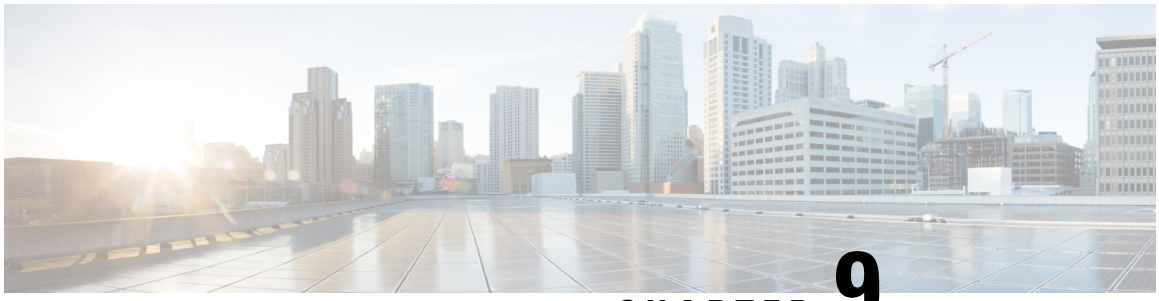
The following is a limited sample of the display that is generated. The entries for APN-OI-Replacement are in bold:

```
show subscribers sgsn-only full all

Username: 491740460103
  Access Type: sgsn                      Network Type: IP
  Access Tech: WCDMA UTRAN
  callid: 01317b21                       msid: 262090426000193
  state: Connected
  connect time: Sun Apr 24 12:20:44 2016 call duration: 00h00m11s
  idle time: 00h00m00s
  Imsimgr Instance: 1                    Temporary Imsimgr instance: 0
  Operator Policy Name: policy1
…
EPS Subscription:
  None:

GPRS Subscription:
  APN OI Replacement                 : abc.mnc009.mcc262.gprs
  PDP Subscription Data:
```

```
    PDP Context Id: 1
    APN: WAP98.TESTNETZ-VD2.DE
    APN OI Replacement:                : op1.mnc009.mcc262.gprs
PDP Type: IPv4
    PDP Address Type: Dynamic
    Charging Characteristics:  Normal Billing
    VPLMN Address Allowed : Not Allowed
…
…
```

The "APN OI Replacement" field under the GPRS Subscription section lists the information for a UE-level APN-OI-Replacement.

The "APN OI Replacement" field under the PDP Subscription Data section lists the information for an APN-level APN-OI-Replacement.



CHAPTER 9

APN Restriction

This chapter describes the APN Restriction feature and provides detailed information on the following:

- Feature Description, on page 183
- How it Works, on page 184
- Configuring APN Restriction, on page 186
- Monitoring and Troubleshooting the APN Restriction, on page 186

Feature Description

The reception, storage, and transfer of APN Restriction values is used to determine whether a UE is allowed to establish PDP Context or EPS bearers with other APNs. This feature is supported by both the Gn/Gp-SGSN and the S4-SGSN.

During default bearer activation, the SGSN sends the current maximum APN restriction value for the UE to the GGSN/P-GW in a Create PDP Context Request/ Create Session Request (CSR). The GGSN/P-GW will have an APN restriction value for each APN. The UE's APN Restriction value determines the type of application data the subscriber is allowed to send. If the maximum APN restriction of the UE (received in the CSR) and the APN Restriction value of the APN (for which activation is being requested) do not concur, then the GGSN/P-GW rejects activation. The maximum APN restriction for a UE is the most restrictive based on all already active default EPS bearers. The purpose of enabling APN Restriction in S4-SGSN is to determine whether the UE is allowed to establish EPS Bearers with other APNs based on the Maximum APN Restriction value associated with that UE.

This feature provides the operator with increased control to restrict certain APNs to UEs based on the type of APN. This feature requires no special license.

APN Restriction for SGSN is enabled/ disabled in the Call-control-profile configuration mode using the **apn-restriction** command.

Relationships to Other Features

APN Restriction value corresponding to each APN is known by the GGSN/P-GW. The Gn/S4-SGSN sends the Maximum APN Restriction of the UE to the GGSN/P-GW in a Create PDP Context Request/ Create Session Request. The GGSN/P-GW accepts or rejects the activation based on the Maximum APN Restriction of UE and APN Restriction value of that APN which is sent the Create PDP Context Request/ Create Session Request

How it Works

During default bearer activation the Gn/S4-SGSN sends the current Maximum APN Restriction value for the UE to the GGSN/ P-GW in the Create PDP Context Request/ Create Session Request (if it is the first activation for that UE or if the APN Restriction is disabled, Maximum APN restriction will be "0" in the Create PDP Context Request/ Create Session Request). The GGSN/P-GW has an APN restriction value for each APN. If the Maximum APN Restriction for the subscriber is received in the Create PDP Context Request/ Create Session Request and APN Restriction value of the APN to which activation is being requested do not concur then the GGSN/P-GW rejects the activation by sending a Create PDP Context / Create Session Response failure message to the G/S4-SGSN with EGTP cause "EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68)".

If the Maximum APN Restriction of the subscriber and APN Restriction of the APN to which activation is ongoing agree as per APN Restriction rules, the GGSN/P-GW sends the APN Restriction value of the APN in the Create PDP Context / Create Session Response as success during activation. The Gn/S4-SGSN updates the APN restriction value of that PDN connection with the value received from GGSN/P-GW in the Create PDP Context/ Create Session Response. The APN restriction value can be received by a new SGSN through context response and forward re-location request messages.

The combination of APN Restriction values of all the PDN connections of a particular UE should be valid and the maximum APN restriction value of the UE should be updated whenever the APN restriction value of a PDN connection is updated.

Table below displays the valid combinations of APN restriction values:

Table 13: APN restriction values

Maximum APN Restriction Value	Type of APN	Application Example	APN Restriction Value allowed to be established
0	No Existing Contexts or Restriction		All
1	Public-1	WAP or MMS	1, 2, 3
2	Public-2	Internet or PSPDN	1, 2
3	Private-1	Corporate (for example MMS subscribers)	1
4	Private-2	Corporate (for example non-MMS subscribers)	None

The valid combination of APN restriction values is achieved in the Gn/ S4-SGSN based on the APN restriction value of the most restrictive PDN connection. If the bearer with the most restrictive APN restriction value gets de-activated, the maximum APN restriction value is re-calculated from among the remaining active default bearers.

In the Create PDP Context /Create Session Request during default bearer activation, the Gn/S4-SGSN sends the Maximum APN Restriction Value for the UE. If no value is available (if this default bearer is the first activation) then, the Maximum APN restriction value will be "0" in Create Session Request. A value of "0" in the Create PDP Context / Create Session Request for Maximum APN restriction indicates there are no other existing PDN connections for the UE or APN restriction is disabled.

If the APN restriction value received in the Create PDP Context / Create Session Response during activation violates the current Maximum APN restriction, then the SGSN rejects the activation and also de-activates any other PDN connection to the same APN. The SGSN considers the APN restriction received in latest Create PDP Context / Create Session Response as the latest value of the APN restriction associated with that APN. If there are any other PDN connections to this APN, the SGSN updates the APN restriction associated with those PDN connections. If the APN restriction value is not violated then the SGSN updates the APN restriction value for that PDN connection and any other PDN connection to the same APN with the value received in the Create PDP Context / Create Session Response and re-calculates the Maximum APN restriction value for MS.

If APN restriction is enabled, but the SGSN does not receive any APN restriction value in the Create PDP Context / Create Session Response and if another PDN connection exists to the same APN, the value of APN restriction is copied from that APN. If no value is available, the APN restriction value is assumed to be "0".

If the current Maximum APN restriction value for the UE is present and the SGSN receives a new default bearer activation request to another APN, while the APN restriction feature is enabled, the activation is rejected with the appropriate sm cause.

If the Gn/ S4-SGSN receives a Create PDP Context/Create Session Response as failure from the P-GW with EGTP cause "EGTP_CAUSE_INCOMPATIBLE_APN_REST_TYPE (0x68)", then the Gn/ S4-SGSN sends an activate reject to the MS with SM cause "(112) APN restriction value incompatible with active PDP context". Any de-activate request sent to the MS due to APN Restriction violation also has the same SM cause.

For every new activation request, the SGSN re-calculates the Maximum APN Restriction from among other currently active PDN connections (excluding those PDNs for which any de-activation is ongoing.)

The APN restriction values are recovered during session recovery. In old SGSN ISRAU, the APN restriction associated with each PDN is sent to the peer in Context Response. In old SGSN SRNS re-location, the APN restriction associated with each PDN connection is sent to the peer in Forward Re-location Request.

In IRAT procedures, the APN restriction for each PDN connection is transferred internally during IRAT and these values are used for subsequent activations after IRAT.

In new SGSN ISRAU, the APN restriction values received in context response are used in the subsequent activations after ISRAU.

In new SGSN SRNS, the APN restriction values received in the forward re-location are used in subsequent activations after SRNS re-location.

Limitations

Consider the scenario where APN restriction is enabled, but no value for APN restriction is received in the Create PDP Context / Create Session Response and no other PDN connections exists to the same APN. An APN restriction value of "0" is assigned to that PDN connection to denote that APN restriction value is invalid for that PDN. During subsequent activations for the subscriber, if the SGSN receives a valid APN Restriction corresponding to the same APN, then the APN Restriction value will be updated for the existing PDNs as well. If not, when a subsequent activation happens with an APN for which SGSN receives valid APN Restriction value, the existing PDNs with invalid (that is "0") APN Restriction values will be de-activated. This behaviour is also observed when the subscriber changes from one PLMN to another PLMN, where the APN Restriction is enabled in the new PLMN but disabled in the old PLMN.

The SGSN does not support APN Restriction if it is enabled during an ongoing call. For APN Restriction to be applied correctly for a subscriber, all the PDP contexts of the subscriber should be created after the APN Restriction is enabled.

Standards Compliance

The APN Restriction feature complies with the following standards:

- 3GPP TS 23.060 (version 10)
- 3GPP TS 29.274 (version 10)

Configuring APN Restriction

This section describes how to configure the APN Restriction feature. The following command is used to configure the APN restriction feature:

```
config
 call-control-profile  profile_name
  apn-restriction update-policy deactivate { least-restrictive |
most-restrictive }
  exit
```

Notes:

- The least or most restrictive values of the APN restriction are applicable only for the Gn SGSN, as the APN restriction can be present in UPCQ/UPCR for Gn SGSN and this configuration is required to determine the PDN to be de-activated when an APN restriction violation occurs during modification procedures in the Gn SGSN. In the case of S4-SGSN, the APN restriction value is received by the S4-SGSN only in Create Session Response during activation. During activation in S4-SGSN, a PDN connection that violates the current Maximum APN restriction is always de-activated. Therefore in the case of S4-SGSN, this CLI is used only for enabling or disabling APN restriction.

For more information on this CLI refer to the *Command Line Interface Reference manual*.

Verifying the APN Restriction Configuration

The **show configuration** command is used to verify the configuration of the APN Restriction feature. Listed below is an example of the show configuration command where APN restriction is configured:

```
show configuration
 config
  call-control-profile test
   apn-restriction update-policy deactivate least-restrictive
   exit
   end
```

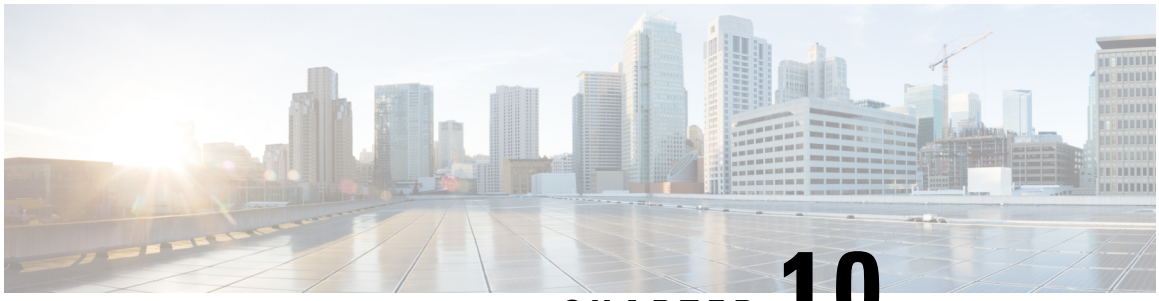
Monitoring and Troubleshooting the APN Restriction

This section provides information on how to monitor APN restriction and to determine that it is working correctly. The following show commands support the monitoring and trouble shooting of the APN restriction feature:

- The **show subscribers SGSN-only full** and **show subscribers gprs-only full** commands display the APN Restriction value of each PDP Context.
- The session-disconnect reason for APN Restriction is **sgsn-apn-restrict-vio.**

- The **show gmm-sm statistics verbose** command displays following counters related to the cause "APN restriction value incompatible with active PDP context":
  - Deactivation Causes Tx
  - 3G-APN Restr val Incomp With Ctx
  - 2G-APN Restr val Incomp With Ctx
  - Activate Primary PDP Context Denied
  - 3G-APN-Restriction Incompatible
  - 2G-APN-Restriction Incompatible

For detailed parameter descriptions see the *Statistics and Counters Reference*.



CHAPTER 10

Attach Rate Throttling

This chapter describes the Attach rate throttling feature and includes the following topics:

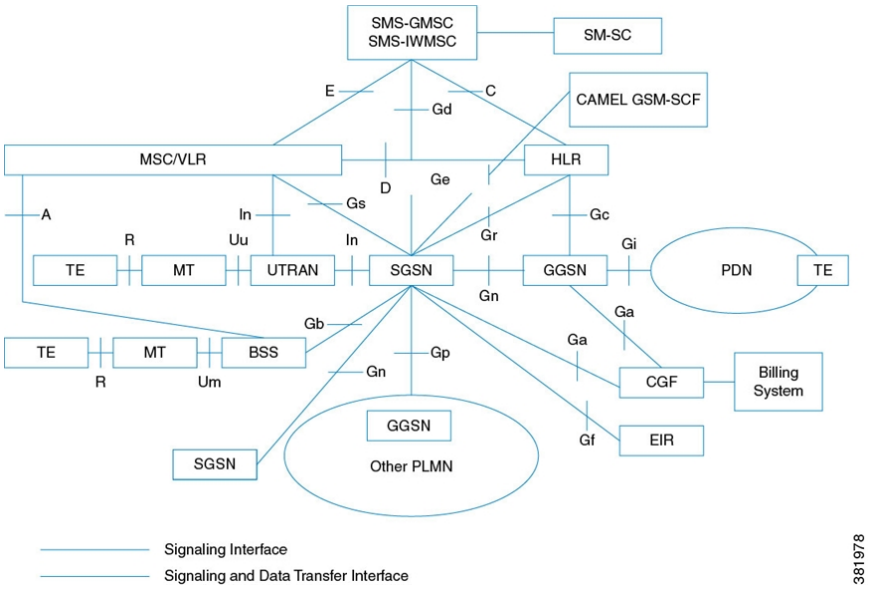
- Feature Description, on page 189
- How it Works, on page 190
- Configuring the Attach Rate Throttling Feature, on page 191
- Monitoring and Troubleshooting the Attach Rate Throttling Feature, on page 192

Feature Description

The SGSN is located at the core of the GPRS Network. It is connected to several nodes in the network like the HLR, GGSN, MSC/VLR, and RNC/BSC so on.

The diagram below depicts the SGSN and its network connections in a GPRS Network.

Figure 22: SGSN in a GPRS Network.



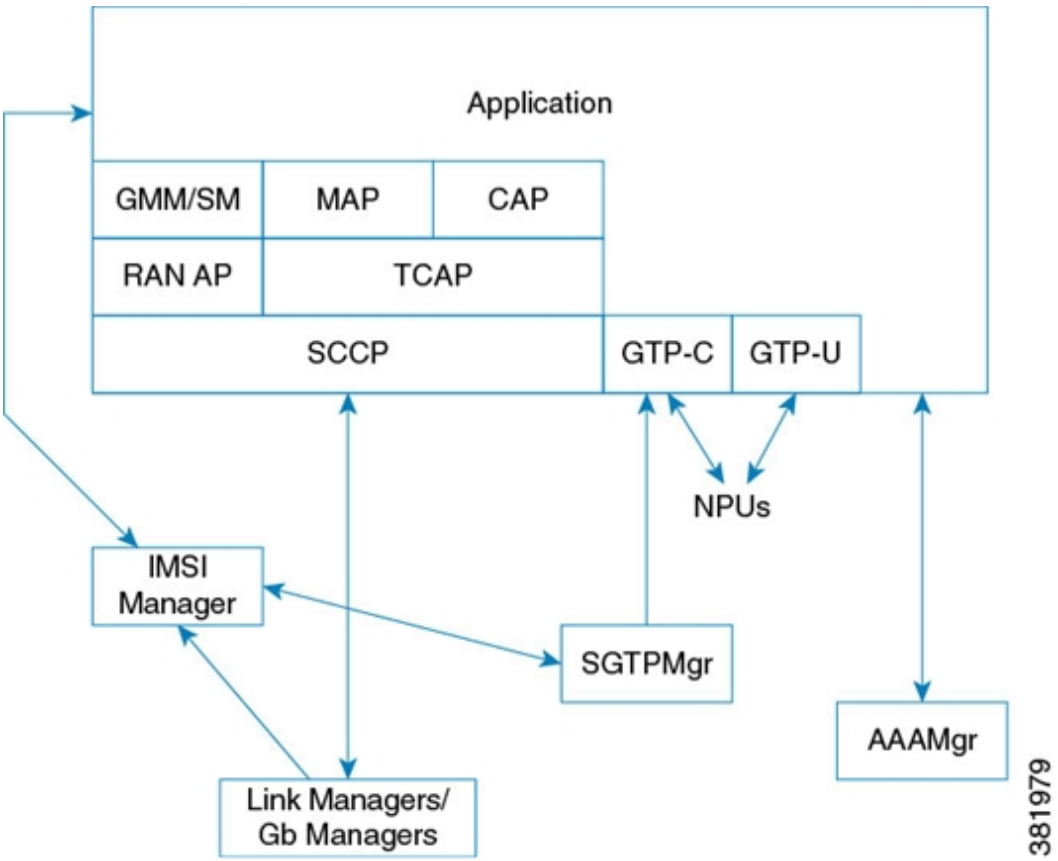
How it Works

Attach Rate Throttling Feature

The Mobile Stations access the services of a GPRS Network by attaching themselves to the network through SGSN nodes. The SGSN can process more than "5000" such attach requests per second. In a typical network the SGSN can be connected to other network elements over a narrow band link and these network elements may not able to process requests at high rates such as the SGSN. This may lead to an overload condition in other network elements. To prevent such scenarios, the Attach Rate throttling feature is designed, this feature limits the rate at which the SGSN processes requests.

The diagram below depicts the high level software architecture in a SGSN node:

Figure 23: Software architecture in a SGSN node.



In a SGSN node the Link Manager/Gb Managers and the IMSI Manager perform the following tasks:

1. **Link Manager/GbManager:**Manages the links towards different network elements such as RNC, HLR so on. The Attach requests and ISRAU requests received on the Link Manager/Gb Manager are sent to the IMSI Manager.
2. **IMSI Manager:** The IMSI Manager assigns the new connection requests to the various Session Managers. The assignment is done after verifying the load on the Session Managers. The Attach Rate Throttling feature is implemented at the IMSI Manager.

The IMSI manager is responsible for identifying the Session Manager to handle the incoming requests. The requests are then queued for the identified Session Manager. These queues are processed at the maximum possible rate. With the introduction of Attach Rate Throttling feature, an intermediary queue is introduced which buffers the incoming requests and processes these requests at the rate configured by the operator. The requests from the intermediary queue are processed at the configured attach rate and then forwarded to the identified Session Manager queue for normal processing. This allows the operator to cap the rate at which new requests are accepted by the SGSN. An overload scenario can be prevented with the introduction of the Attach Rate Throttling feature. The intermediary queues are operational only when the Attach Rate Throttling feature is enabled. If the feature is disabled, attach requests are directly queued for processing at the identified Session Manager.

Limitations

The operator must ensure that an optimal attach rate must be configured based on the network conditions:

1. If the incoming requests arrive at a very high rate and the attach rate configured to a very low rate, the requests will be dropped from the intermediary queue once the queue is full. The IMSI Manager can send a reject response with the appropriate reject cause codes for such all dropped requests or silently drop the requests.
2. If the configured attach rate is very low, the requests waiting time in the queue increases. The "t3310" timer at the MS expires and the MS will have to re-transmit the request. The IMSI Manager drops all requests which have waited in the queue for more than the configured wait time.

The configured Attach rate must have an optimal processing rate and waiting time.

Configuring the Attach Rate Throttling Feature

The following command is used to configure the Attach Rate Throttling feature, this command configures an attach rate throttle mechanism to control the number of new connections (attaches or inter-SGSN RAUs), through the SGSN, on a per second basis:

```
config
   network-overload-protection sgsn-new-connections-per-second
_new_connections action { drop | reject with cause { congestion | network
failure } } [ queue-size  queue_size  ] [ wait-time  wait_time ]
   default network-overload-protection sgsn-new-connections-per-second
   exit
```

Notes:

- The default mode of the command disables the Attach Rate Throttling feature.

  For detailed information on the command, see the *Command Line Interface Reference*.

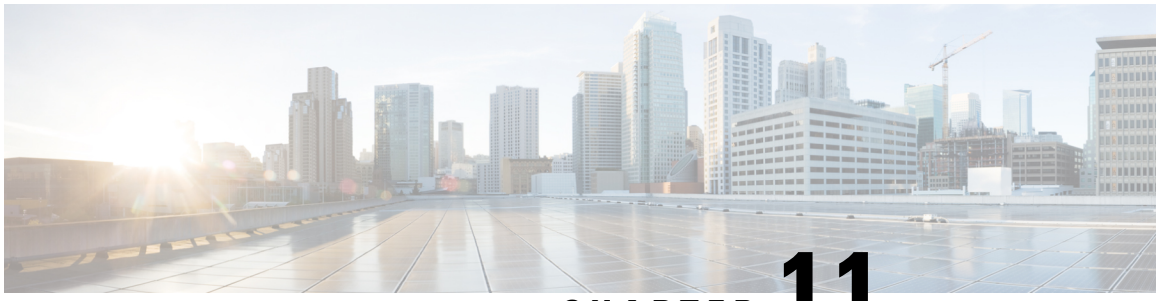
Monitoring and Troubleshooting the Attach Rate Throttling Feature

Attach Rate Throttling Show Commands and Outputs

This section provides information regarding show commands and/or their outputs in support of the Attach Rate Throttling feature.

The counters for this feature are available under the show command **show gmm-sm statistics**, as a part of the Network Overload Protection counters.

- Network Overload Protection
-
  - Number of valid packets processed in the last sec.
  - Number of packets in Q in the last tick
  - Packets to be dequeued in the last tick
  - Number of new requests processed from the pacing queue in the last tick
  - Number of requests dropped from the pacing queue in the last tick
  - Average Number of requests processed per min (1 min)
  - Average Number of requests processed per min (5 min)
  - Average Number of requests processed per min (10 min)



CHAPTER 11

Backup and Recovery of Key KPI Statistics

This feature allows the backup of a small set of GGSN, P-GW, SAEGW, and/or S-GW key KPI counters for recovery of the counter values after a session manager (SessMgr) crash.

This section includes the following information:

- Feature Description, on page 193
- How It Works, on page 193
- Configuring Backup Statistics Feature, on page 196
- Managing Backed-up Statistics, on page 197

Feature Description

Before the Backup and Recovery of Key KPI Statistics feature was implemented, statistics were not backed up and could not be recovered after a SessMgr task restart. Due to this limitation, monitoring the KPI was a problem as the SGSN would loose statistical information whenever task restarts occurred.

KPI calculation involves taking a delta between counter values from two time intervals and then determines the percentage of successful processing of a particular procedure in that time interval. When a SessMgr crashes and then recovers, the SGSN loses the counter values - they are reset to zero. So, the KPI calculation in the next interval will result in negative values for that interval. This results in a dip in the graphs plotted using the KPI values, making it difficult for operations team to get a consistent view of the network performance to determine if there is a genuine issue or not.

This feature makes it possible to perform reliable KPI calculations even if a SessMgr crash occurs.

How It Works

A key set of counters, used in KPI computation will be backed up for recovery if a SessMgr task restarts. The counters that will be backed up are determined by the KPIs typically used in several operator networks.

The backup of counters is enabled or disabled via configuration. The configuration specifies the product (currently only supported by the SGSN) for which counters will be backed up and also a time interval for the back up of the counters.

The backed up counters can be identified via CLI generated displays or via display of the four SGSN-specific backup statistics schemas: iups-bk, gprs-bk, map-bk, and sgtp-bk. The operator can use these schemas to

compute the KPI as statistics will have the recovered counters. During the display and the backup processes, both the normal counters and backed-up counters are cumulatively displayed or backed up.

- **iups-bk schema** - This schema is used for 3G GMM-SM counters which are backed up. The counters in this schema are pegged per IuPS service. Each line of output is per IuPS service. Additionally, there will be one set of consolidated counters for all IuPS services which is displayed with the SGSN service name.
- **gprs-bk schema** - This schema is used for 2G GMM-SM counters which are backed up. The counters in this schema are pegged per GPRS service. Each line of output is per GPRS service. Additionally, there will be one set of consolidated counters for all GPRS services which is displayed with the SGSN service name.
- **map-bk schema** - This schema is used for MAP and SMS counters which are backed up. The counters in this schema are pegged per MAP service. Each line of output is per MAP service.
- **sgtp-bk schema** - This schema is used for GTPU counters which are backed up. The counters in this schema are pegged per IuPS and SGTP service, one per line. Additionally, there will be one line of output which represents the counters consolidated for all IuPS and SGTP services.

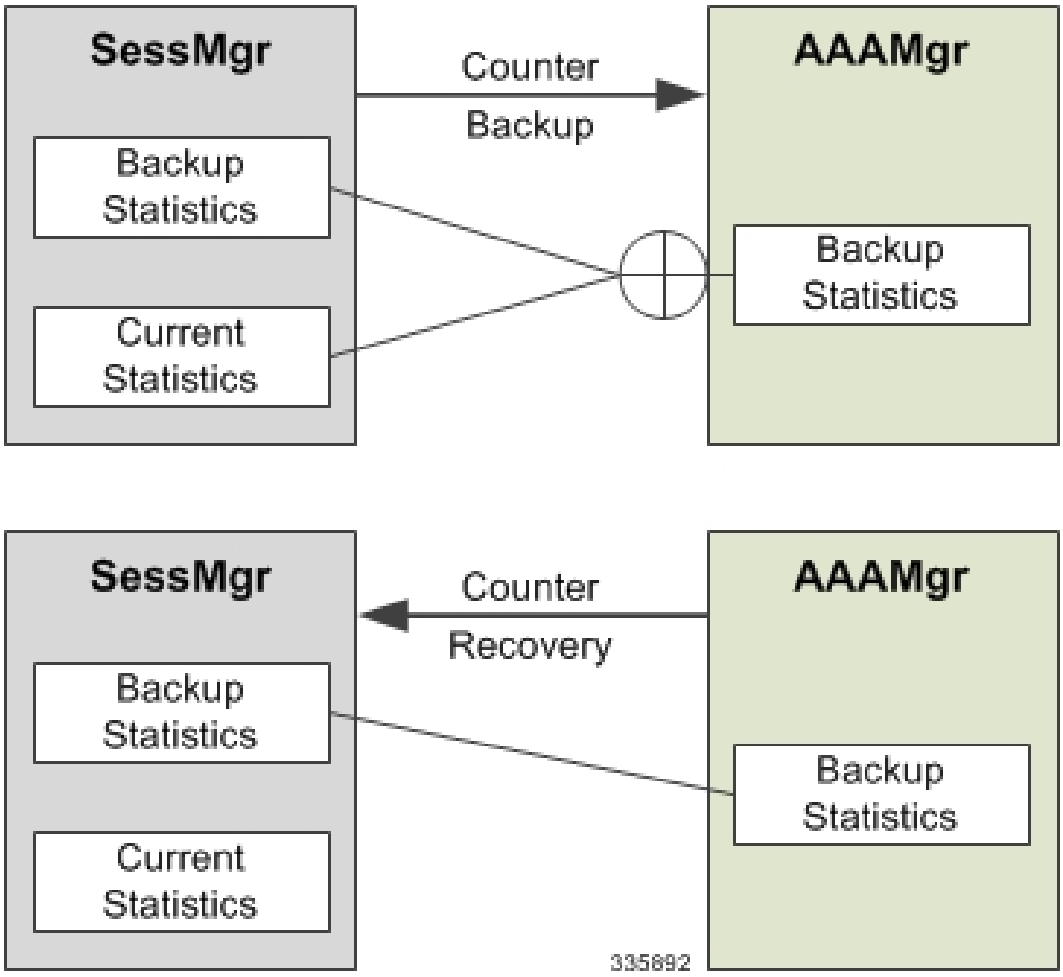
Architecture

When this feature is enabled (see *Configuring Backup Statistics Feature* below), the SGSN only backs up the counters maintained at the SessMgr. Counters maintained by other managers, such as the LinkMgr or SGTPMgr, are not backed up. The recovery function does not need to be configured or 'started' as it occurs automatically as needed when the feature is enabled.

The counters are backed up to the AAAMgr that is paired with the SessMgr. They are recovered from the AAAMgr after a SessMgr task is killed. This feature makes use of the session recovery framework to backup and retrieve the counters.

The following diagram depicts how backed-up statistics are maintained separately at the SessMgr and how the cumulative values are backed up and recovered from the AAAMgr after SessMgr task recovery completes.

Figure 24: Back Up and Recovery of Statistics for SGSN



Limitations

- A backup interval must be specified and counters are backed up only at the specified interval. For example, if the backup interval is specified as 5 minutes, then counters are backed up every 5 minutes. Suppose backup happened at Nth minute and the configured backup interval is for every 5 minutes, then if a task crash happens at N+4 minutes, the SGSN recovers only the values backed up at Nth minute and the data for the past 4 minutes is lost.
- Only service level statistics are backed up and recovered. Any KPI that is monitored per other granularity, such as per RA or per RNC, is not supported.
- Only statistics maintained at the SessMgr are backed up. Statistics at other managers, such as LinkMgr and GbMgr are not backed up.

Configuring Backup Statistics Feature

For the Backup and Recovery of Key KPI Statistics feature to work, it must be enabled by configuring the backup of statistics for the SGSN.

Configuration

The following CLI commands are used to manage the functionality for the backing up of the key KPI statistics feature

Enabling

The following configures the backup of statistics for the SGSN and enables the Backup and Recovery of Key KPI Statistics feature.

```
configure
     statistics-backup sgsn
     exit
```

Setting the Backup Interval

The following command configures the number of minutes (0 to 60) between each backup of the statistics. When the backup interval is not specified a default value of 5 minutes is used as the backup interval

```
configure
     statistics-backup-interval minutes
     exit
```

Disabling

The following configures the SGSN to disable the backing up of statistics for the SGSN.

```
configure
     no statistics-backup sgsn
     exit
```

Notes:

- When the new keyword is used, only the **recovered** values will be displayed.
- If no session manager crash has occurred, the above commands output displays with the normal counter values.
- If a session manager crash has happened, the above commands display the cumulative value so far (*including* the backed up value).
- The display of the counters will be similar to the **show sgsn-service statistics** command output with respect to naming and indentation. Only the subset of counters which are backed up will be displayed with the **recovered-values** option.

Verifying the Backup Statistics Feature Configuration

Use either the **show configuration** command or the **show configuration verbose** command to display the feature configuration.

If the feature was enabled in the configuration, two lines similar to the following will appear in the output of a **show configuration [verbose]** command:

```
statistics-backup  mme
statistics-backup-interval 5
```

Notes:

- The interval displayed is 5 minutes. 5 is the default. If the **statistics-backup-interval** command is included in the configuration, then the 5 would be replaced by the configured interval number of minutes.
- If the command to disable the feature is entered, then no statistics-backup line is displayed in the output generated by a **show configuration [verbose]** command.

Managing Backed-up Statistics

A new keyword, **recovered-values**, is used with existing show and clear commands to either generate a display of the backed-up statistics or to clear the backed-up statistics.

Displaying Backed-up Statistics

Use one of the following commands to generate a display of the backed up statistics:

- show gmm-sm statistics [recovered-values] [verbose]
- show gmm-sm statistics sgsn-service *sgsn_service_name* [recovered-values] [verbose]
- show gmm-sm statistics gprs-service *gprs_service_name* [recovered-values] [verbose]
- show gmm-sm statistics iups-service *iups_service_name* [recovered-values] [verbose]
- show map-statistics [recovered-values]
- show map statistics map-service *map_service_name* [recovered-values]
- show sms statistics [recovered-values]
- show sms statistics name *map_service_name* [recovered-values]
- show sms statistics [gprs-only | sgsn-only] [recovered-values]
- show sgtpu statistics [recovered-values]
- show sgtpu statistics iups-service *iups_service_name* [recovered-values]
- show sgtpu statistics sgtp-service *sgtp_service_name* [recovered-values]

Notes:

- When the **recovered-values** keyword is used, output includes both current + recovered backed-up statistical values.
- If no SessMmgr crash has occurred, then the recovered values in the output of the above commands will be 0 (zero).

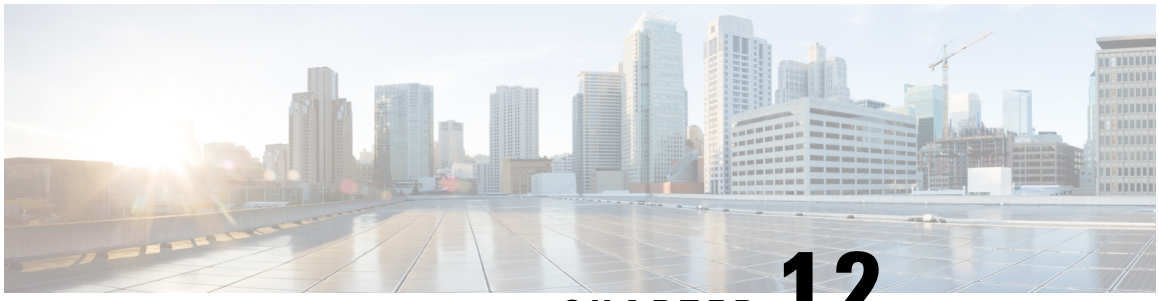
Clearing Backed-up Statistics

Use one of the following commands to clear (delete) the backed-up statistics. Note that the order entry for the service name identification varies in some of the commands. As well, the verbose keyword is not used with the **clear** commands.

- clear gmm-sm statistics [recovered-values]
- clear gmm-sm statistics [recovered-values] sgsn-service *sgsn_service_name*
- clear gmm-sm statistics [recovered-values] gprs-service *gprs_service_name*
- clear gmm-sm statistics [recovered-values] iups-service *iups_service_name*
- clear map-statistics [recovered-values]
- clear map statistics name *map_service_name* [recovered-values]
- clear sms statistics [recovered-values]
- clear sms statistics name *map_service_name* [recovered-values]
- clear sms statistics [gprs-only | sgsn-only] [recovered-values]
- clear sgtpu statistics [recovered-values]
- clear sgtpu statistics iups-service *iups_service_name* [recovered-values]
- clear sgtpu statistics sgtp-service *sgtp_service_name* [recovered-values]

Notes:

- When the **recovered-values** keyword is used, only the **recovered** values will be cleared.



CHAPTER 12

Cause Code #66

- Feature Description, on page 199
- How It Works, on page 200
- Configuring PDP Activation Restriction and Cause Code Values, on page 200
- Monitoring and Troubleshooting the Cause Code Configuration, on page 204

Feature Description

This feature is developed to achieve compliance with Release 11 3GPP Technical Specifications. The Release 11 3GPP Technical Specification introduced a new ESM/SM cause code "Requested APN not supported in current RAT and PLMN combination (cause code 66). This ESM/SM cause is used by the network to indicate that the procedure requested by the UE is rejected as the requested APN is not supported in the current RAT and PLMN. A UE which receives this cause will stop accessing the APN in the current RAT, but as soon as it enters another RAT type it will retry the APN.

In earlier releases only cause code 27 and cause code 33 were supported, these codes were not very effective in restricting APN in a particular RAT. For example, UE which has received cause 27 (with timer = 24hrs) will stop retrying a PDN connection in every RAT for 24 hrs. This is not the desired behavior in some cases APN cannot be restricted in a particular RAT. If the SGSN sends cause code 33 to the UE for an IMS APN, the UE/MS stops retrying the PDN connection for some time, but UE/MS will not automatically retry this APN in 4G, even though the APN is available there. The introduction of cause code 66 resolves this issue as the operator can block access to IMS APN in 2G/3G and can allow access in 4G.

Important This feature is applicable for both SGSN and MME.

Important This is a 3GPP Release 11 compliance feature, and will be applicable only to UEs capable of decoding ESM/SM cause code 66.

How It Works

This feature is developed for both SGSN and MME. In the SGSN, activation restriction of PDP context on the basis of access type can be configured using the restrict access-type command under the APN profile configuration mode. This command is now extended to MME; a new keyword "eps" is introduced to configure the APN profile to restrict the PDP context activation from EPS network access. If this CLI is enabled access to APN's associated with this APN profile are not allowed on MME/SGSN. By default, any activation on SGSN for this APN is rejected with cause code 'Requested APN not supported in current RAT and PLMN combination66'. During mobility scenarios the PDPs related to this APN are deactivated on the SGSN and the PDPs are also deactivated up to the GGSN/PGW.

On the MME attach is rejected if the default bearer related APN is not supported under the APN profile. By default the EMM cause and the ESM cause in attach reject are 'ESM failure19' and 66 respectively.

If the first default bearer APN is allowed, after a successful attach if the subsequent second default bearer APN is not supported, activation is rejected with cause 'Requested APN not supported in current RAT and PLMN combination66'. This is default MME behavior.

During mobility procedures on MME, if APN is not supported for bundle, bearers will deactivated all the way up to PGW and as well on MME for that particular bundle.

If the APN is not supported for all the bundles received from a peer node for a Tracking Area Update procedure at a new MME, Tracking Area Update is rejected with EMM cause 'No Suitable Cells In tracking area 15'.

If the APN is not supported for all the bundles received from a peer node for SRNS relocation procedure at the new MME, SRNS is rejected with GTPV2 cause 'Denied in RAT82' in Forward relocation response (if the peer node is MME/S4 SGSN). SRNS is rejected with GTPV1 cause 'Relocation failure213' in Forward relocation response if the peer node is a Gn Gp SGSN.

The operator can configure different cause values other than the default cause values mentioned in the scenarios described above. For SGSN/MME cause code remapping is done by configuring various options of the local-cause-code-mapping command under the Call Control Profile configuration mode (for both SGSN and MME) and MME Service Configuration mode (for MME only).

Standards Compliance

This feature is developed to comply with the following standards:

- 3GPP TS 24.301, Release 11 (version 11.14.0)
- 3GPP TS 23.401,Release 11 (version 11.11.0)
- 3GPP TS 24.008,Release 11 (version 11.15.0)
- 3GPP TS 23.060,Release 11 (version 11.12.0)

Configuring PDP Activation Restriction and Cause Code Values

The following configuration procedures are used to configure this feature. The access type restriction, cause code mapping for SGSN and MME can be configured using following procedures.

Configuring PDP Activation Restriction

The restrict access-type command under the APN profile configuration mode is used to configure PDP activation restriction on the basis of access type, a new command option for EPS networks is introduced for this feature. In earlier releases this command was supported only for GPRS and UMTS networks to perform QoS related restrictions. Now this command is also used to configure the APN not supported in particular RAT and PLMN combination. If this command is enabled, new PDP activations to an APN with which this APN profile is associated are rejected. During handovers PDPs/PDNs are deactivated if the APN name matches with this APN profile.

```
configure
   apn-profile profile_name
      [ no ] restrict access-type { eps |  { { gprs | umts } [ qos-class
{ background | conversational | interactive | streaming } ] } }
      default restrict access-type {  eps | gprs | umts }
      end
```

Notes:

- This command is disabled by default.
- In earlier releases this command was applicable only for SGSN. It is now supported by MME also.
- If the operator does not include the optional **qos-class** keyword option, then complete APN restriction is enabled and QoS related restrictions have no impact as QoS restriction is a subset of a complete APN restriction.

Configuring SM Cause Code Mapping for SGSN

The following command is used remap the cause code 66 to an operator desired cause code. This cause code is sent in activate rejection.

```
config
   call-control-profile profile_name
      [remove] local-cause-code-mapping apn-not-supported-in-plmn-rat
sm-cause-code cause_number
      exit
```

Notes:

- This mapping is not done by default.
- The keyword **apn-not-supported-in-plmn-rat** specifies the cause code for Requested APN not supported in current RAT and PLMN combination.
- The keyword **sm-cause-code** specifies the SM cause code to be used towards the UE. The value can be integer with range 1 up to 255.

Configuring ESM Cause Code Mapping for ESM Procedures (for MME)

The following command is used remap the ESM cause code sent in activate rejections (due to APN not supported) to an operator desired ESM cause code.

```
config
   call-control-profile profile_name
      [remove] local-cause-code-mapping apn-not-supported-in-plmn-rat
```

```
esm-cause-code cause_number esm-proc
     exit
```

Notes:

- This mapping is not done by default.
- The keyword **apn-not-supported-in-plmn-rat** specifies the cause code for Requested APN not supported in current RAT and PLMN combination.
- The keyword **esm-cause-code** specifies the ESM cause code to be used if a bearer management request is rejected due to this configuration. The value can be integer with range 1 up to 255.
- The specified esm-cause-code is used if an ESM procedure is rejected under the error condition **esm-proc**. This is specified as a keyword in the command.

Configuring EMM and ESM Cause Code Mapping for EMM Procedures (for MME)

The following command under the Call Control Profile configuration mode is used remap the EMM and ESM cause codes sent in activate rejections (due to APN not supported) to an operator desired ESM and EMM cause codes.

```
config
  call-control-profile profile_name
     [remove] local-cause-code-mapping apn-not-supported-in-plmn-rat
emm-cause-code cause_number esm-cause-code cause_number [ attach [ tau ] | tau
 [attach ] ]
     exit
```

Notes:

- This mapping is not done by default.
- The keyword **apn-not-supported-in-plmn-rat** specifies the cause code for Requested APN not supported in the current RAT and PLMN combination.
- The keyword **emm-cause-code** specifies the EMM cause code to be used if a NAS request is rejected due to this configuration. A valid EMM cause value is an integer from 2 through 111.
- The keyword **esm-cause-code** specifies the ESM cause code to be used if a NAS request is rejected due to this configuration. A valid ESM cause value is an integer from 8 through 112.
- The keyword **attach** specifies the cause code to be used if an attach procedure is rejected under the error conditions.
- The keyword **tau** specifies the cause code to be used if TAU procedure is rejected under the error conditions.

Configuring ESM Cause Code Mapping for ESM Procedures (MME Service Configuration Mode)

The following command under the MME Service Configuration mode is used remap the ESM cause code sent in activate rejections (due to APN not supported) to an operator desired ESM cause code.

```
config
  context <context_name>
   mme-service <service_name>
    local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code
```

```
  <cause_number> esm-proc
     default local-cause-code-mapping apn-not-supported-in-plmn-rat
esm-cause-code esm-proc
     exit
```

Notes:

- The default cause code for esm-proc is 66.
- The keyword **apn-not-supported-in-plmn-rat** is used to specify the cause code for Requested APN not supported in current RAT and PLMN combination.
- The keyword **esm-cause-code** is used to specify the ESM cause code to be used if a bearer management request is rejected due to this configuration. The ESM cause value is an integer with range 8 up to 112.
- The specified esm-cause-code is used if an ESM procedure is rejected under the error condition **esm-proc**. This is specified as a keyword in the command.

Configuring EMM and ESM Cause Code Mapping for EMM Procedures (MME Service Configuration Mode)

The following command under the MME Service configuration mode is used remap the EMM and ESM cause codes sent in activate rejections (due to APN not supported) to an operator desired ESM and EMM cause codes.

```
config
   context context_name
      mme-service service_name
         local-cause-code-mapping apn-not-supported-in-plmn-rat
emm-cause-code cause_number esm-cause-code cause_number  [ attach [ tau ] | tau
 [ attach ] ]
         default local-cause-code-mapping apn-not-supported-in-plmn-rat [
attach | tau ]
         exit
```

Notes:

- The default cause code values for Attach procedure are emm-cause-code 19 and esm-cause-code 66. The default cause code values for TAU procedure are emm-cause-code 15 and esm-cause-code 66.
- The keyword **apn-not-supported-in-plmn-rat** specifies the cause code for Requested APN not supported in current RAT and PLMN combination.
- The keyword **emm-cause-code** specifies the EMM cause code to be used if a NAS request is rejected due to this configuration. The EMM cause value is an integer with range 2 up to 111.
- The keyword **esm-cause-code** specifies the ESM cause code to be used if a NAS request is rejected due to this configuration. The ESM cause value is an integer with range 8 up to 112.
- The keyword **attach** specifies the cause code to be used if an attach procedure is rejected under the error conditions.
- The keyword **tau** specifies the cause code to be used if TAU procedure is rejected under the error conditions.

Verifying the Feature Configuration

The configuration of this feature can be verified using the following show commands.

Execute the **show configuration** command to verify the configuration, the output displays the following parameters based on the configuration:

- restrict access-type umts/gprs/eps
- local-cause-code-mapping apn-not-supported-in-plmn-rat sm-cause-code *cause_number*
- local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code *cause_number* esm-proc
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 19 esm-cause-code 66 attach
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 19 esm-cause-code 66 tau
- local-cause-code-mapping apn-not-supported-in-plmn-rat esm-cause-code 32 esm-proc
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 15 esm-cause-code 66 attach
- local-cause-code-mapping apn-not-supported-in-plmn-rat emm-cause-code 19 esm-cause-code 66 tau

Execute the **show apn-profile full** *profile_name* command to verify the configuration, the output displays the following parameters based on the configuration:

- Service Restriction for Access Type UMTS:
- Complete APN restricted : Enabled
- Service Restriction for Access Type GPRS:
- Complete APN restricted : Enabled
- Service Restriction for Access Type EPS:
- Complete APN restricted : Enabled

Execute the **show call-control-profile full** *profile_name* command to verify the configuration, the output displays the following parameters based on the configuration:

- Mapped SM Cause For Req APN not sup in current RAT and PLMN combination: Not Configured
- Mapped SM Cause For Req APN not sup in current RAT and PLMN combination: Requested service option not subscribed (33)
- Cause Code Mapping
- APN not supported PLMN-RAT esm-proc : Operator Determined Barring (esm-8)
- APN not supported PLMN-RAT Attach : ESM failure (emm-19), Requested APN not supported in current RAT and PLMN combination (esm-66)
- APN not supported PLMN-RAT TAU : ESM failure (emm-19), Requested APN not supported in current RAT and PLMN combination (esm-66)

Execute the **show mme-service name** *mme_service* command to verify the configuration, the output displays the following parameters based on the configuration:

- APN not supported PLMN-RAT esm-proc : Requested APN not supported in current RAT and PLMN combination (esm-66)
- APN not supported PLMN-RAT Attach : ESM failure (emm-19), Requested APN not supported in current RAT and PLMN combination (esm-66)
- APN not supported PLMN-RAT TAU : No Suitable Cells In tracking area (emm-15)

Monitoring and Troubleshooting the Cause Code Configuration

This section provides information on the show commands and bulk statistics available to support this feature.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of this feature.

show gmm-sm statistics verbose

The following new parameters are added to this show command to display the statistics for this feature:

- 3G-Pri-Actv-APN-Not-Sup-Rej
- 2G-Pri-Actv-APN-Not-Sup-Rej
- 3G-APN-Not-Supported-in-PLMN-RAT
- 2G-APN-Not-Supported-in-PLMN-RAT
- APN Not Supported in PLMN RAT combination Statistics
- 3G-Pdp-Dropped-During-New-SGSN-RAU
- 2G-Pdp-Dropped-During-New-SGSN-RAU
- 3G-Pdp-Dropped-During-New-SGSN-SRNS
- Pdp-Dropped-During-3G-To-2G-IRAT
- 3G-Actv-NRPCA-Reject
- Pdp-Dropped-During-2G-To-3G-IRAT

The following statistics are MME specific:

- APN not sup PLMN-RAT
- Inbound Inter node SRNS failure
- APN not sup in PLMN/RAT

Bulk Statistics

The following statistics are included in the MME and SGSN Schemas in support of the feature.

MME Schema

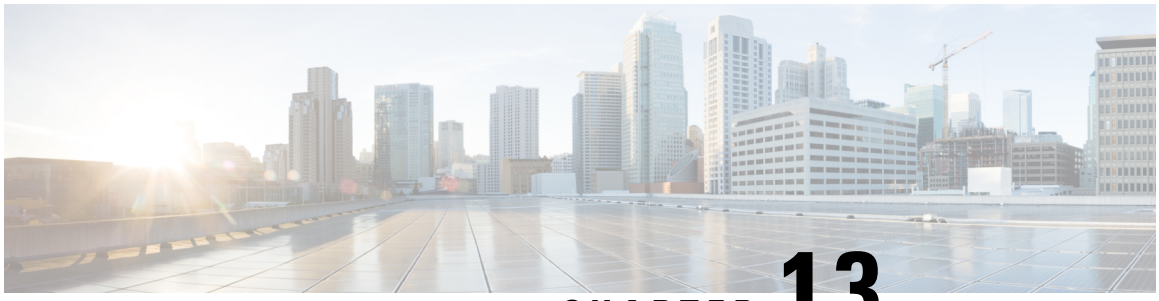
- inter-node-srns-proc-fail-apn-not-supported
- inter-node-tau-proc-fail-apn-not-supported
- tai-esm-msgtx-pdncon-rej-apn-not-sup-in-plmn-rat
- tai-emm-msgtx-attach-rej-apn-not-sup-in-plmn-rat
- attach-proc-fail-apn-not-sup-in-plmn-rat
- esm-msgtx-pdncon-rej-apn-not-sup-in-plmn-rat
- emm-msgtx-attach-rej-apn-not-sup-in-plmn-rat
- emmdisc-apnnotsupinplmnrat

SGSN Schema

- 3G-actv-rej-apn-not-supported-in-plmn-rat
- 2G-actv-rej-apn-not-supported-in-plmn-rat
- 3G-actv-rej-apn-not-supported-in-plmn-rat-cum
- 2G-actv-rej-apn-not-supported-in-plmn-rat-cum
- 2G-3G-irat-pdp-drop-apn-not-supported-in-plmn-rat
- 2G-israu-pdp-drop-apn-not-supported-in-plmn-rat
- 3G-israu-pdp-drop-apn-not-supported-in-plmn-rat

- 3G-srns-pdp-drop-apn-not-supported-in-plmn-rat
- 3G-nrpca-pdp-drop-apn-not-supported-in-plmn-rat
- 3G-2G-irat-pdp-drop-apn-not-supported-in-plmn-rat
- 2G-inter-svc-rau-pdp-drop-apn-not-supported-in-plmn-rat

For descriptions of these variables, see the information for the SGSN and MME schema in the *Statistics and Counters Reference*.



CHAPTER 13

Cause Code Mapping

Local Cause Code Mapping provides the operator with the flexibility to configure a preferred GMM cause code to be sent to the UE in response to various failures, such a MAP failures. This section identifies the various cause code mapping optionsand how they are configured.

- Cause Code Mapping, on page 207
- Feature Description, on page 207
- Configuring Cause Code Mapping, on page 208

Cause Code Mapping

Local Cause Code Mapping provides the operator with the flexibility to configure a preferred GMM cause code to be sent to the UE in response to various failures, such a MAP failures. This section identifies the various cause code mapping optionsand how they are configured.

Feature Description

This feature enables the operator to configure (map) preferred failure code information to send to the UE in reject messages.

Prior to release 16, the operator could map a preferred GMM reject cause code for the SGSN to send to a UE in place of MAP cause 'roaming not allowed' for MAP failures and to map a preferred GMM reject cause code to be sent in a RAU Reject for inbound peer SGSN address resolution failures.

Beginning with release 16, additional local cause code mapping is possible:

- Mapping GSM-MAP cause code "unknown-subscriber" to GMM cause code "gprs-service-not-allowed" if a response message comes without diagnostic information.
- Mapping GSM-MAP cause code unknown-subscriber with diagnostic information indicating gprs-subscription-unknown to a preferred GMM cause code.
- Mapping GSM-MAP cause code unknown-subscriber with diagnostic information indicating imsi-unknown to a preferred GMM cause code.
- Override the GMM cause sent to the MS in a RAU Reject during context transfer failure.
- Override the cause sent in a Deactivate Request, to an MS, due to the GGSN becoming unreachable.
- Mapping an SM cause code for Deactivate PDP Requests during a path failure towards the GGSN.

Configuring Cause Code Mapping

Each mapping of a cause code is configured slightly differently. Each is illustrated below.

Configuring GMM Cause Codes to Replace MAP Cause Codes

The following configures the SGSN to include a preferred GMM cause code, in Reject messages to the UE, in place of MAP failure cause 'unknown-subscriber' for MAP failures and inbound RAU context transfer failures. Optionally, the Operator can map a specific GMM cause code if the SGSN receives additional MAP failure diagnostic information.

```
configure
    call-control-profile profile_name
         local-cause-code-mapping map-cause-code { roaming-not-allowed
gmm-cause-code gmm-cause | unknown-subscriber { gmm-cause-code gmm-cause |
map-diag-info { gprs-subscription-unknown gmm-cause-code gmm_cause |
imsi-unknown gmm-cause-code gmm_cause } } }
         end
```

Notes:

- **unknown-subscriber** Instructs the SGSN to send a different GPRS mobility management (GMM) cause code to a UE when the UE's access request is rejected due to map cause 'unknown-subscriber'.
- **gmm-cause-code** *gmm_cause* identifies the replacement GMM cause code options include:
  - **gprs-serv-and-non-gprs-serv-not-allowed**
  - **gprs-serv-not-allowed**
  - **gprs-serv-not-in-this-plmn**
  - **location-area-not-allowed**
  - **network-failure**
  - **no-suitable-cell-in-this-la**
  - **plmn-not-allowed**
  - **roaming-not-allowed-in-this-la**
- **map-diag-info gprs-subscription-unknown gmm-cause-code** *gmm_cause* identifies a replacement GMM cause code if additional 'gprs-subscription-unknown' diagnostic MAP failure information is received when the UE's access request is rejected due to map cause 'unknown-subscriber'.
- **map-diag-infoimsi-unknown gmm-cause-code** *gmm_cause* identifies a replacement GMM cause code if additional 'imsi-unknown' diagnostic MAP failure information is received when the UE's access request is rejected due to map cause 'unknown-subscriber'.

Verifying Configuration to Replace MAP Cause Codes

Mapping is performed in the call control profile.

Run the **show call-control-profile full name** *profile_name* command and review the output. Look for the following lines to confirm the mapping configuration

```
Mapped Gmm Cause code for MAP cause Unknown Subscriber          : <gmm-cause-if-configured>
MAP cause Unknown Subscriber with Diag Info Gprs Subscription Unknown    :
<gmm-cause-if-configured>
```

```
MAP cause Unknown Subscriber with Diag Info Imsi Unknown                :
<gmm-cause-if-configured>
```

Configuring GMM Cause Code for RAU Reject due to Context Transfer Failure

This configuration uses the existing **rau-inter** command in the call control profile configuration mode. There is a new keyword configures a GMM failure cause code to be sent in a RAU Reject to the UE due to context transfer failures.

```
configure
    call-control-profile profile_name
         rau-inter ctxt-xfer-failure failure-code  fail_code
         end
```

Notes:

- *fail_code* enter value from 2 to 111 to identify the TS 124.008 GMM failure cause code for the **ctxt-xfer-failure** keyword.

For more information about these commands, refer to the *Command Line Interface Reference*.

Verifying Configuration for Context Transfer Failures

Mapping is performed in the call control profile.

Run the **show call-control-profile full name** *profile_name* command and review the output. Look for the following lines to confirm the mapping configuration

```
RAU Inter- Failure Code For Peer Sgsn Address Resolution        : <gmm-cause>
RAU Inter- Failure Code For Context Transfer                            : <gmm-cause>
```

Configuring SM Cause Codes

The following procedures illustrates the commands used to configure SM cause codes to override the default cause codes sent in Deactivate PDP Request due to GTPC path failure. It is up to the person entering the configuration to determine which of the 4 cause codes should be the new cause code.

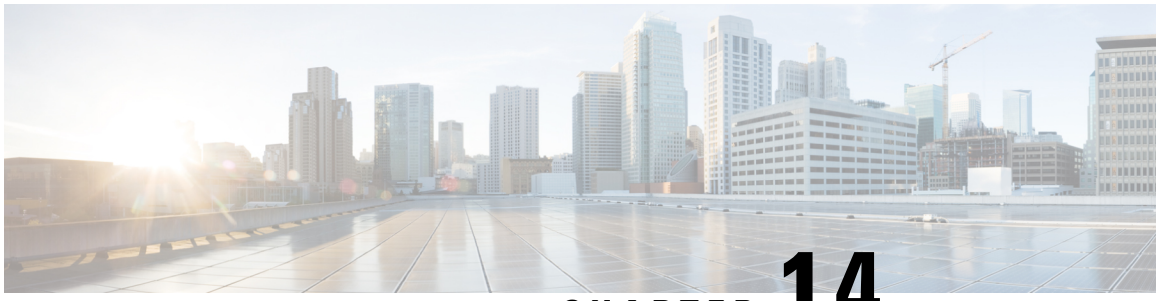
```
configure
     call-control-profile profile_name
         local-cause-code-mapping path-failure sm-cause-code {
insufficient-resources | network-failure | reactivation-requested  |
regular-deactivation }
         end
```

Verifying Configuration for SM Cause Codes

Mapping is performed in the call control profile.

Run the **show call-control-profile full name** *profile_name* command and review the output. Look for the following lines to confirm the mapping configuration

```
Mapped SM Cause Code For Path Failure      : <sm-cause>
```



CHAPTER 14

SGSN Controlling Peer Status Based on Heartbeat Message

This chapter describes the following topics:

- Feature Summary and Revision History, on page 211
- Feature Description, on page 211
- Configuring SGSN Controlling Peer Status Based on Heartbeat Message, on page 212

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	ASR 5000
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *SGSN Administration Guide*

Revision History

First Introduced.	21.17

Feature Description

SGSN considers the peer active only after receiving "ACK" for its heartbeat message. This feature is CLI Controlled for SGSN not to make the SCTP peer active after receiving heartbeat from the peer.

Configuring SGSN Controlling Peer Status Based on Heartbeat Message

This section provides information on the CLI commands to configure SGSN Controlling Peer Status Based on Heartbeat Message feature.

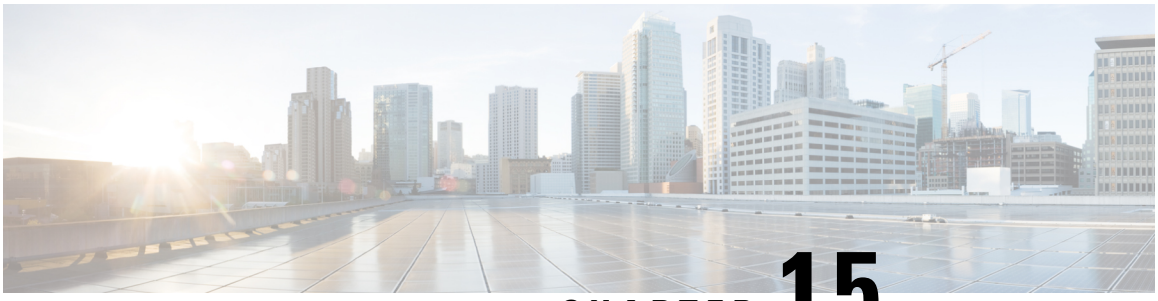
Configuring SCTP Peer Active Heartbeat Acknowledgment

Use the following configuration to configure SCTP peer active heartbeat acknowledgment.

```
configure
  ss7-routing-domain  SS7_routing_domain_index variant itu
    peer-server id server_id
       psp instance psp_instance
          no associate asp
             [ no ]sctp-peer active hbeat-ack
             end
```

NOTES:

- **no** : Removes peer active heart beat acknowledgment.
- **sctp-peer active hbeat-ack**: Configures SCTP peer active heartbeat acknowledgment.



CHAPTER 15

Default APN Selection Based on Context ID

This chapter describes the following topics:

- Feature Summary and Revision History, on page 213
- Feature Description, on page 213
- Configuring Default APN Selection Based on Context ID, on page 214

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	ASR 5000
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *SGSN Administration Guide*

Revision History

First Introduced.	21.16

Feature Description

Default APN Selection Based on Context ID feature adds the flexibility to select the subscription APN with given context ID when requested APN is not found in subscription. The default APN feature is invoked and is used to determine if the activation can be allowed by substituting the requested APN for one in subscription. The SGSN uses the subscribed APN which matches the configured context id.

Multiple Trigger Feature supports multiple instances of same of cli “apn-selection-default” where we can configure multiple default APNs based on different configuration. SGSN selects the first matched instance

and CLI instance's will be Stored in the same order in which it is defined during the configuration. The "apn-selection-default" and the order of cli "apn-selection-default" decides the priority. The context ID feature should be configured first to take the highest priority. This feature can be used with other features like first-subscription and lowest-context-id. This feature is CLI controlled.

Configuring Default APN Selection Based on Context ID

This section provides information on the CLI commands to configure Default APN Selection Based on Context ID.

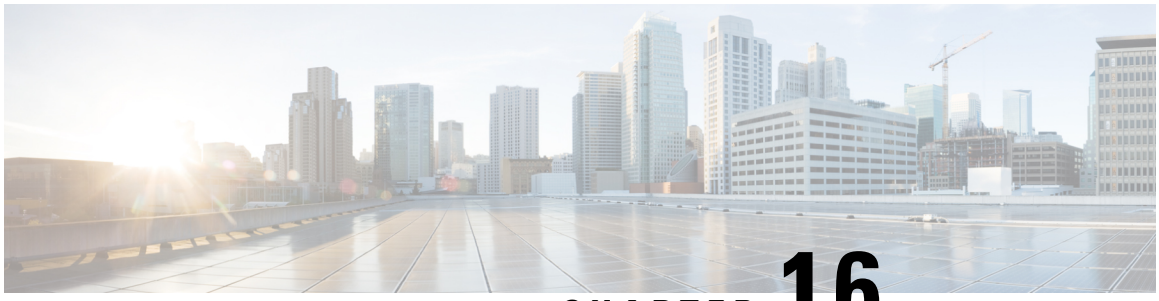
Configuring APN Selection Default

Use the following configuration to enable APN Selection Default.

```
configure
  apn-remap-table remap_table_name
    apn-selection-default context-id context_id_value [ orig-apn ]
    no apn-selection-default context-id context_id_value
    end
```

NOTES:

- **no** : Removes the subscription of APN based on context id.
- **apn-selection-default context-id** : Specifies that the APN will be used as the Default APN.
- **context-id** *context_id_value*: Specifies the usage of APN in subscription record with context ID matching the PDN type if normal APN selection fails. *context_id_value* must be an integer between 1 and 15.
- **orig-apn**: Sends the original APN in the ACTIVATE_DEFAULT_BEARER_REQUEST message to the UE.



CHAPTER 16

Direct Tunnel for 3G Networks

This chapter briefly describes the 3G UMTS direct tunnel (DT) feature, indicates how it is implemented on various systems on a per call basis, and provides feature configuration procedures.

Products supporting direct tunnel include:

- 3G devices (per 3GPP TS 23.919 v8.0.0):
  - the Serving GPRS Support Node (SGSN)
  - the Gateway GPRS Support Node (GGSN)

Important Direct tunnel is a licensed Cisco feature. A separate feature license is required for configuration. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

The SGSN determines if setup of a direct tunnel is allowed or disallowed. Currently, the SGSN is the only product that provide configuration commands for this feature. All other products that support direct tunnel do so by default.

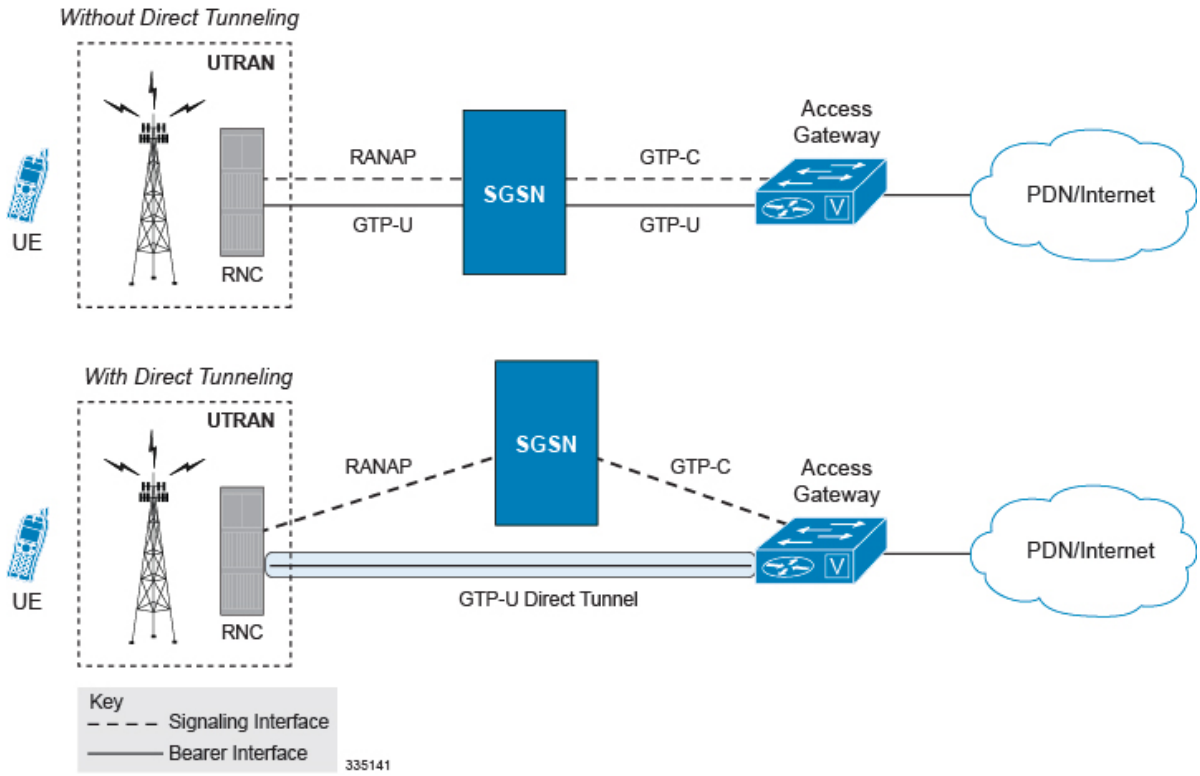
- Direct Tunnel Feature Overview, on page 215
- Direct Tunnel Configuration, on page 219

Direct Tunnel Feature Overview

The direct tunnel architecture allows the establishment of a direct *user plane* (GTP-U) tunnel between the radio access network equipment (RNC) and a GGSN.

Once a direct tunnel is established, the SGSN continues to handle the *control plane* (RANAP/GTP-C) signaling and retains the responsibility of making the decision to establish direct tunnel at PDP context activation.

Figure 25: GTP-U Direct Tunneling

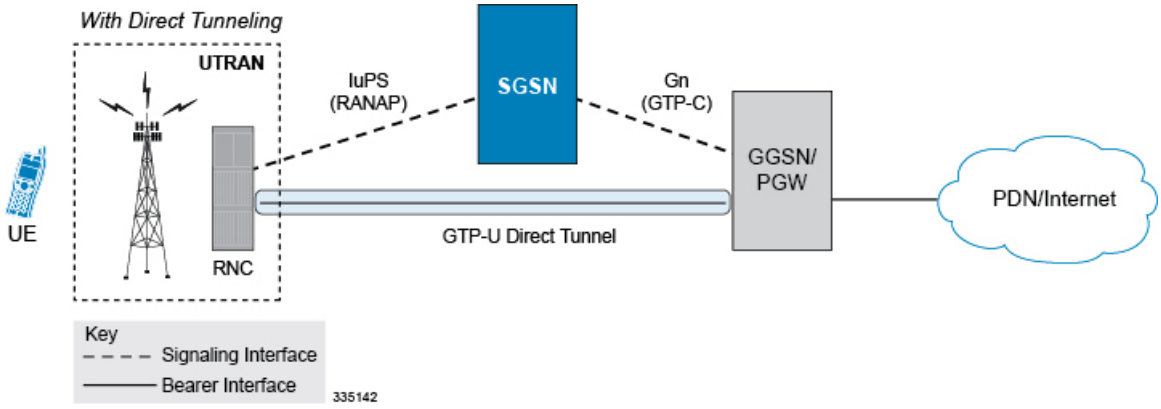


A direct tunnel improves the user experience (for example, expedites web page delivery, reduces round trip delay for conversational services) by eliminating switching latency from the user plane. An additional advantage, direct tunnel functionality implements optimization to improve the usage of user plane resources (and hardware) by removing the requirement from the SGSN to handle the user plane processing.

A direct tunnel is achieved upon PDP context activation in the following ways:

- **Gn/Gp Interface towards GGSN:** The SGSN establishes a user plane (GTP-U) tunnel directly between the RNC and the GGSN, using an Updated PDP Context Request toward the GGSN or the GGSN service of a collocated GGSN/P-GW.

Figure 26: Direct Tunneling - 3G Network

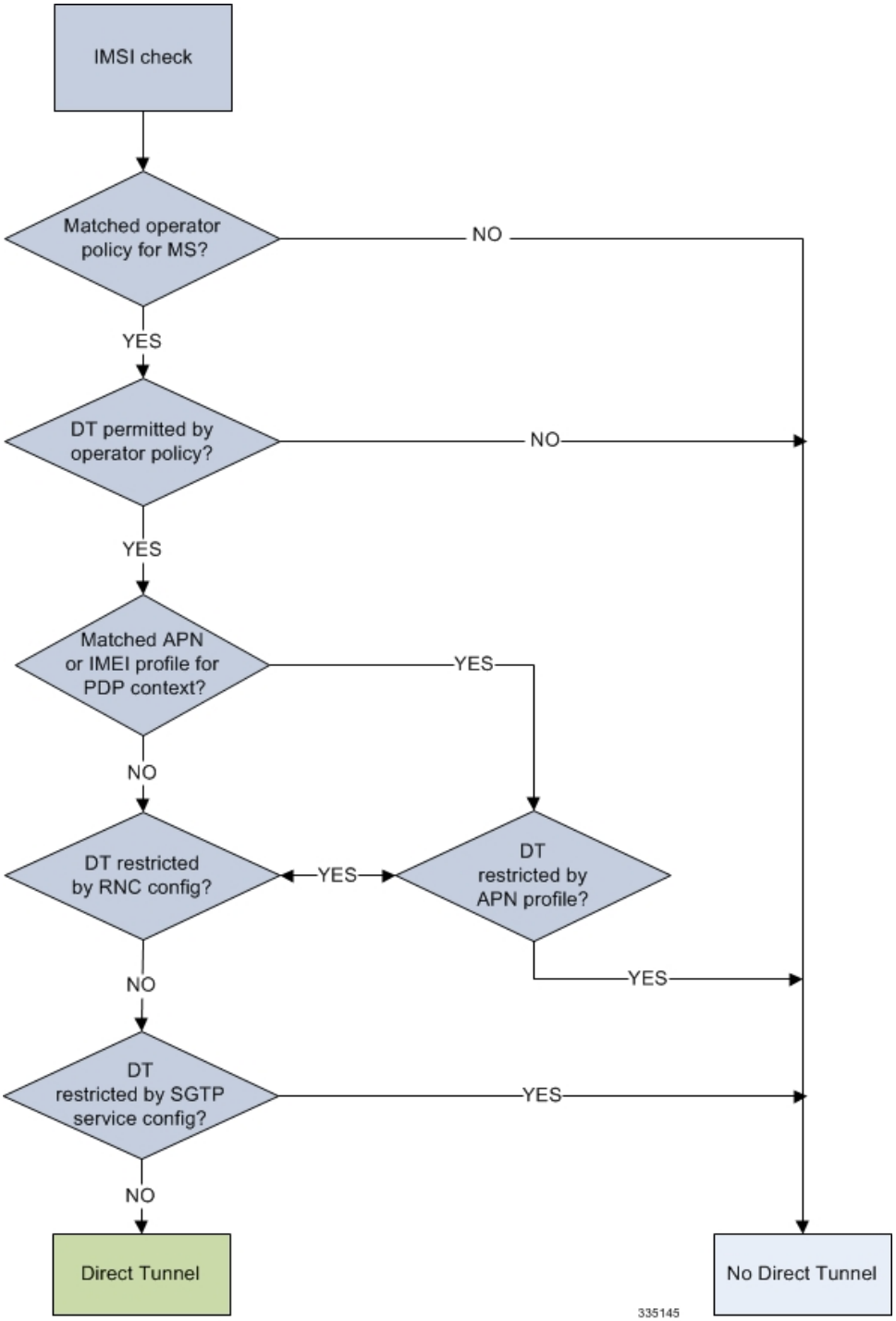


- **Gn/Gp Interface towards P-GW** When Gn/Gp interworking with pre-release 8 (3GPP) SGSNs is enabled, the GGSN service on the P-GW supports direct tunnel functionality. The SGSN establishes a user plane (GTP-U) tunnel directly between the RNC and the collocated PGW, using an Update PDP Context Message toward the GGSN/P-GW.

A major consequence of deploying a direct tunnel is that it produces a significant increase in control plane load on both the SGSN and GGSN components of the packet core. Hence, deployment requires highly scalable GGSNs since the volume and frequency of Update PDP Context messages to the GGSN will increase substantially. The SGSN platform capabilities ensure control plane capacity will not be a limiting factor with direct tunnel deployment.

The following figure illustrates the logic used within the SGSN to determine if a direct tunnel will be setup.

Figure 27: Direct Tunneling - Establishment Logic



Direct Tunnel Configuration

The following configurations are provided in this section:

- Configuring Direct Tunnel Support on the SGSN, on page 219

The SGSN direct tunnel functionality is enabled within an operator policy configuration. One aspect of an operator policy is to allow or disallow the setup of direct GTP-U tunnels. If no operator policies are configured, the system looks at the settings in the system operator policy named *default*.

By default, direct tunnel support is

- *disallowed* on the SGSN
- *allowed* on the GGSN/P-GW

Important If direct tunnel is allowed in the *default* operator policy, then any incoming call that does not have an applicable operator policy configured will have direct tunnel *allowed*.

For more information about operator policies and configuration details, refer to *Operator Policy*.

Configuring Direct Tunnel Support on the SGSN

The following is a high-level view of the steps, and the associated configuration examples, to configure the SGSN to setup a direct tunnel.

Before beginning any of the following procedures, you must have completed (1) the basic service configuration for the SGSN, as described in the *Cisco ASR Serving GPRS Support Node Administration Guide*, and (2) the creation and configuration of a valid operator policy, as described in the *Operator Policy* chapter in this guide.

Step 1 Configure the SGSN to setup GTP-U direct tunnel between an RNC and an access gateway by applying the example configuration presented in the Enabling Setup of GTP-U Direct Tunnels, on page 220.

Step 2 Configure the SGSN to allow GTP-U direct tunnels to an access gateway, for a call filtered on the basis of the APN, by applying the example configuration presented in the Enabling Direct Tunnel per APN , on page 220.

Important It is only necessary to complete either step 2 or step 3 as a direct tunnel can not be setup on the basis of call filtering matched with both an APN profile and an IMEI profile.

Step 3 Configure the SGSN to allow GTP-U direct tunnels to a GGSN, for a call filtered on the basis of the IMEI, by applying the example configuration presented in the Enabling Direct Tunnel per IMEI , on page 221.

Step 4 Configure the SGSN to allow GTP-U direct tunnel setup from a specific RNC by applying the example configuration presented in the Enabling Direct Tunnel to Specific RNCs, on page 221.

Step 5 *(Optional)* Configure the SGSN to disallow direct tunnel setup to a single GGSN that has been configured to allow it in the APN profile. This command allows the operator to restrict use of a GGSN for any reason, such as load balancing. Refer to the **direct-tunnel-disabled-ggsn** command in the *SGTP Service Configuration Mode* chapter of the *Command Line Interface Reference*.

Step 6 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Step 7 Check that your configuration changes have been saved by using the sample configuration found in the Verifying the SGSN Direct Tunnel Configuration, on page 223.

Enabling Setup of GTP-U Direct Tunnels

The SGSN determines whether a direct tunnel can be setup and by default the SGSN doesn't support direct tunnel.

Example Configuration

Enabling direct tunnel setup on an SGSN is done by configuring direct tunnel support in a call-control profile.

```
config
  call-control-profile policy_name
    direct-tunnel attempt-when-permitted [ to-ggsn | to-sgw ]
    end
```

Notes:

- A call-control profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.
- Beginning with Release 19.3.5, **to-ggsn** and **to-sgw** options have been added to the **direct-tunnel** command to enable the operator to select the interface the SGSN will use for its direct tunnel. For a collocated Gn/GP-SGSN and an S4-SGSN,
  - Use the keyword **attempt-when-permitted** without a filter to enable both interface types: GTP-U towards the GGSN and S12 towards the SGW.
  - Use the keyword **attempt-when-permitted** with the **to-ggsn** keyword filter to enable only the GTP-U interface between the RNC and the GGSN.
  - Use the keyword **attempt-when-permitted** with the **to-sgw** keyword filter to enable only the S4's S12 interface between the RNC and the SGW.
- To remove the direct tunnel settings from the configuration, use the following command: **direct-tunnel attempt-when-permitted [to-ggsn | to-sgw]**
- Direct tunnel is allowed on the SGSN but will only setup if allowed on both the destination node and the RNC.

Enabling Direct Tunnel per APN

In each operator policy, APN profiles are configured to connect to one or more GGSNs and to control the direct tunnel access to that GGSN based on call filtering by APN. Multiple APN profiles can be configured per operator policy.

By default, APN-based direct tunnel functionality is *allowed* so any existing direct tunnel configuration must be removed to return to default and to ensure that the setup has not been restricted.

Example Configuration

The following is an example of the commands used to ensure that direct tunneling, to a GGSN(s) identified in the APN profile, is enabled:

```
config
  apn-profile profile_name
    remove direct tunnel
    end
```

Notes:

- An APN profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.
- Direct tunnel is now allowed for the APN but will only setup if also allowed on the RNC.

Enabling Direct Tunnel per IMEI

Some operator policy filtering of calls is done on the basis of international mobile equipment identity (IMEI) so the direct tunnel setup may rely upon the feature configuration in the IMEI profile.

The IMEI profile basis its permissions for direct tunnel on the RNC configuration associated with the IuPS service.

By default, direct tunnel functionality is *enabled* for all RNCs.

Example Configuration

The following is an example of the commands used to enable direct tunneling in the IMEI profile:

```
config
  imei-profile profile_name
    direct-tunnel check-iups-service
    end
```

Notes:

- An IMEI profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.
- Direct tunnel is now allowed for calls within the IMEI range associated with the IMEI profile but a direct tunnel will only setup if also allowed on the RNC.

Enabling Direct Tunnel to Specific RNCs

SGSN access to radio access controllers (RNCs) is configured in the IuPS service.

Each IuPS service can include multiple RNC configurations that determine communications and features depending on the RNC.

By default, direct tunnel functionality is *enabled* for all RNCs.

Example Configuration

The following is an example of the commands used to ensure that restrictive configuration is removed and direct tunnel for the RNC is enabled:

```
config
   context ctx_name
      iups-service service_name
         rnc id rnc_id
            default direct-tunnel
            end
```

Notes:

- An IuPS service must have been previously created, and configured.
- An RNC configuration must have been previously created within an IuPS service configuration.
- Command details for configuration can be found in the *Command Line Interface Reference*.

Restricting Direct Tunnels

By default, GGSNs and RNCs are assumed to be capable of direct tunneling. The SGSN's direct tunnel functionality can be fine tuned to:

Disable direct tunneling for a specified GGSN(s). GGSNs are identified by their IP address, either IPv4 or IPv6. The command listed below can be repeated to disable direct tunneling for multiple GGSNs, thereby creating a 'disabled GGSN' list. Checking for a GGSN that is direct-tunnel-disabled is actually the last step in the PDP Activation procedure.

```
config
   context context_name
      sgtp-service service_name
         direct-tunnel-disabled-ggsn ip_address
         end
```

Restrict direct tunneling for an entire APN. The following configuration scenario prohibits direct tunneling setup to a GGSN for an entire APN - the APN associated with the profile.

```
config
   apn-profile profile_name
      direct-tunnel not-permitted-by-ggsn
      end
```

Restrict direct tunneling by a specific RNC. The following configuration scenario restricts the SGSN from attempting to setup a direct tunnel when a call originates from a specific RNC.

```
config
   context context_name
      iups-service service_name
         rnc id rnc_id
            direct-tunnel not-permitted-by-rnc
```

end

Verifying the SGSN Direct Tunnel Configuration

Enabling the setup of a GTP-U direct tunnel on the SGSN is not a straight forward task. It is controlled by an operator policy with related configuration in multiple components. Each of these component configurations must be checked to ensure that the direct tunnel configuration has been completed. You need to begin with the operator policy itself.

Verifying the Operator Policy Configuration

For the feature to be enabled, it must be allowed in the call-control profile, and the call-control profile must be associated with an operator policy. As well, either an APN profile or an IMEI profile must have been created/configured and associated with the same operator policy. Use the following command to display and verify the operator policy and the association of the required profiles:

show operator-policy full name *policy_name*

The output of this command displays profiles associated with the operator policy. The output also includes some values just as illustrative examples:

```
show operator-policy full name oppolicy1
Operator Policy Name = oppolicy1
Call Control Profile Name               : ccprofile1
  Validity                              : Valid
IMEI Range 99999999999990  to 99999999999995
  IMEI Profile Name                     : imeiprofile1
  Validity                              : Invalid
APN NI homers1
  APN Profile Name                      : apnprofile1
  Validity                              : Valid
APN NI visitors2
  APN Profile Name                      : apnprofile2
  Validity                              : Invalid
```

Notes:

- Validity refers to the status of the profile. Valid indicates that profile has been created and associated with the policy. Invalid means only the name of the profile has been associated with the policy.
- The operator policy itself will only be valid if one or more IMSI ranges have been associated with it - refer to the *Operator Policy* chapter, in this guide, for details.

Verifying the Call-Control Profile Configuration

Use the following command to display and verify the direct tunnel configuration for the call-control profiles:

show call-control-profile full name *profile_name*

The output of this command displays all of the configuration, including direct tunnel for the specified call-control profile.

```
Call Control Profile Name = ccprofile1
...
Re-Authentication                   : Disabled
Direct Tunnel                       : Not Restricted
GTPU Fast Path                      : Disabled
...
```

Verifying the APN Profile Configuration

Use the following command to display and verify the direct tunnel configuration in the APN profile:

show apn-profile full name *<profile_name>*

The output of this command displays all of the configuration, including direct tunnel for the specified APN profile.

```
Call Control Profile Name = apnprofile1
...
IP Source Validation                          : Disabled
Direct Tunnel                                 : Not Restricted
Service Restriction for Access Type > UMTS    : Disabled
...
```

Verifying the IMEI Profile Configuration

Use the following command to display and verify the direct tunnel configuration in the IMEI profile:

show imei-profile full name *<profile_name>*

The output of this command displays all of the configuration, including direct tunnel for the specified IMEI profile.

```
IMEI Profile Name = imeiprofile1
Black List                          : Disabled
GGSN Selection                      : Disabled
Direct Tunnel                       : Enabled
```

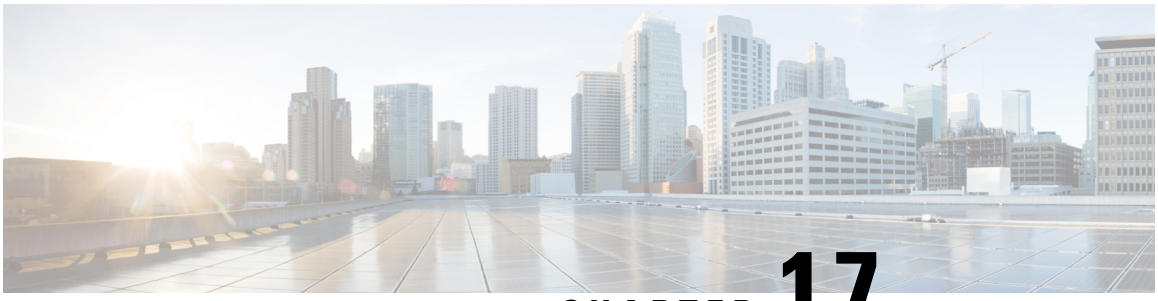
Verifying the RNC Configuration

Use the following command to display and verify the direct tunnel configuration in the RNC configuration:

show iups-service name *service_name*

The output of this command displays all of the configuration, including direct tunnel for the specified IuPS service.

```
IService name              : iups1
...
Available RNC:
   Rnc-Id                        : 1
   Direct Tunnel                 : Not Restricted
```



CHAPTER 17

Direct Tunnel for 4G (LTE) Networks

This chapter briefly describes support for direct tunnel (DT) functionality over an S12 interface for a 4G (LTE) network to optimize packet data traffic.

Cisco LTE devices (per 3GPP TS 23.401 v8.3.0) supporting direct tunnel include:

- Serving GPRS Support Node (S4-SGSN)
- Serving Gateway (S-GW)
- PDN Gateway (P-GW)

Important Direct Tunnel is a licensed Cisco feature. A separate feature license is required for configuration. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

The following sections are included in this chapter:

- Direct Tunnel for 4G Networks - Feature Description , on page 225
- How It Works, on page 228
- Configuring Support for Direct Tunnel, on page 257
- Monitoring and Troubleshooting Direct Tunnel, on page 260

Direct Tunnel for 4G Networks - Feature Description

The amount of user plane data will increase significantly during the next few years because of High Speed Packet Access (HSPA) and IP Multimedia Subsystem technologies. Direct tunneling of user plane data between the RNC and the S-GW can be employed to scale UMTS system architecture to support higher traffic rates.

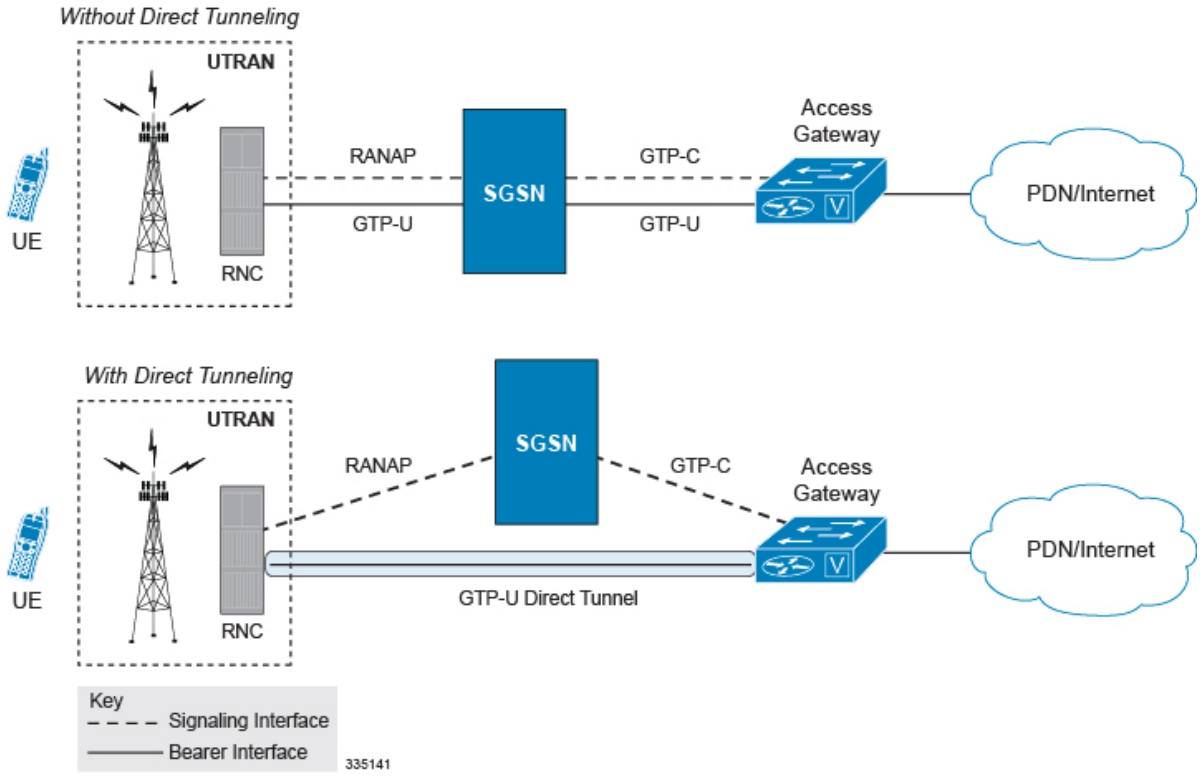
Direct Tunnel (DT) offers a solution that optimizes core architecture without impact to UEs and can be deployed independently of the LTE/SAE architecture.

Important Direct tunnel is a licensed Cisco feature. A separate feature license is required for configuration. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

Important Establishment of a direct tunnel is controlled by the SGSN; for 4G networks this requires an S4 license-enabled SGSN setup and configured as an S4-SGSN.

Once a direct tunnel is established, the S4-SGSN/S-GW continues to handle the *control plane* (RANAP/GTP-C) signaling and retains the responsibility of making the decision to establish direct tunnel at PDP context activation.

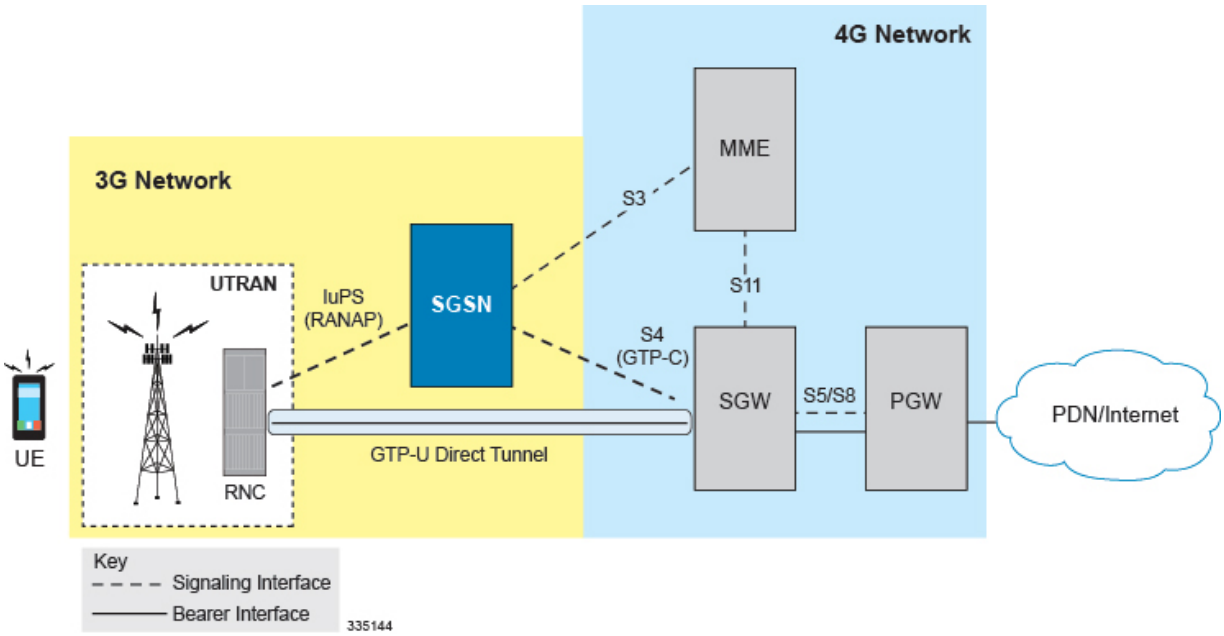
Figure 28: GTP-U Direct Tunneling



A direct tunnel improves the user experience (for example, expedites web page delivery, reduces round trip delay for conversational services) by eliminating switching latency from the user plane. An additional advantage, direct tunnel functionality implements optimization to improve the usage of user plane resources (and hardware) by removing the requirement from the S4-SGSN/S-GW to handle the user plane processing.

A direct tunnel is achieved upon PDP context activation when the S4-SGSN establishes a user plane tunnel (GTP-U tunnel) directly between the RNC and the S-GW over an S12 interface, using a Create Bearer Response or Modify Bearer Request towards the S-GW.

Figure 29: Direct Tunneling - LTE Network, S12 Interface



A major consequence of deploying a direct tunnel is that it produces a significant increase in control plane load on both the SGSN/S-GW and GGSN/P-GW components of the packet core. Hence, deployment requires highly scalable GGSNs/P-GWs since the volume and frequency of Update PDP Context messages to the GGSN/P-GW will increase substantially. The SGSN/S-GW platform capabilities ensure control plane capacity will not be a limiting factor with direct tunnel deployment.

S4-SGSN supports establishment of a GTP-U direct tunnel between an RNC and the S-GW under the scenarios listed below:

- Primary PDP activation
- Secondary PDP activation
- Service Request Procedure
- Intra SGSN Routing Area Update without S-GW change
- Intra SGSN Routing Area Update with S-GW change
- Intra SGSN SRNS relocation without S-GW change
- Intra SGSN SRNS relocation with S-GW change
- New SGSN SRNS relocation with S-GW change
- New SGSN SRNS relocation without S-GW relocation
- E-UTRAN-to-UTRAN Iu mode IRAT handover with application of S12U FTEID for Indirect Data Forwarding Tunnels as well
- UTRAN-to-E-UTRAN Iu mode IRAT handover with application of S12U FTEID for Indirect Data Forwarding Tunnels as well
- Network Initiated PDP Activation

Scenarios that vary at S4-SGSN when direct tunneling is enabled, as compared to DT on a 2G or 3G SGSN using the Gn interface, include:

- RAB Release
- Iu Release
- Error Indication from RNC

- Downlink Data Notification from S-GW
- Downlink Data Error Indication from S-GW
- MS Initiated PDP Modification
- P-GW Initiated PDP Modification while the UE is IDLE
- HLR/HSS Initiated PDP Modification
- Session Recovery with Direct Tunnel

The above scenarios exhibit procedural differences in S4-SGSN when a direct tunnel is established.

How It Works

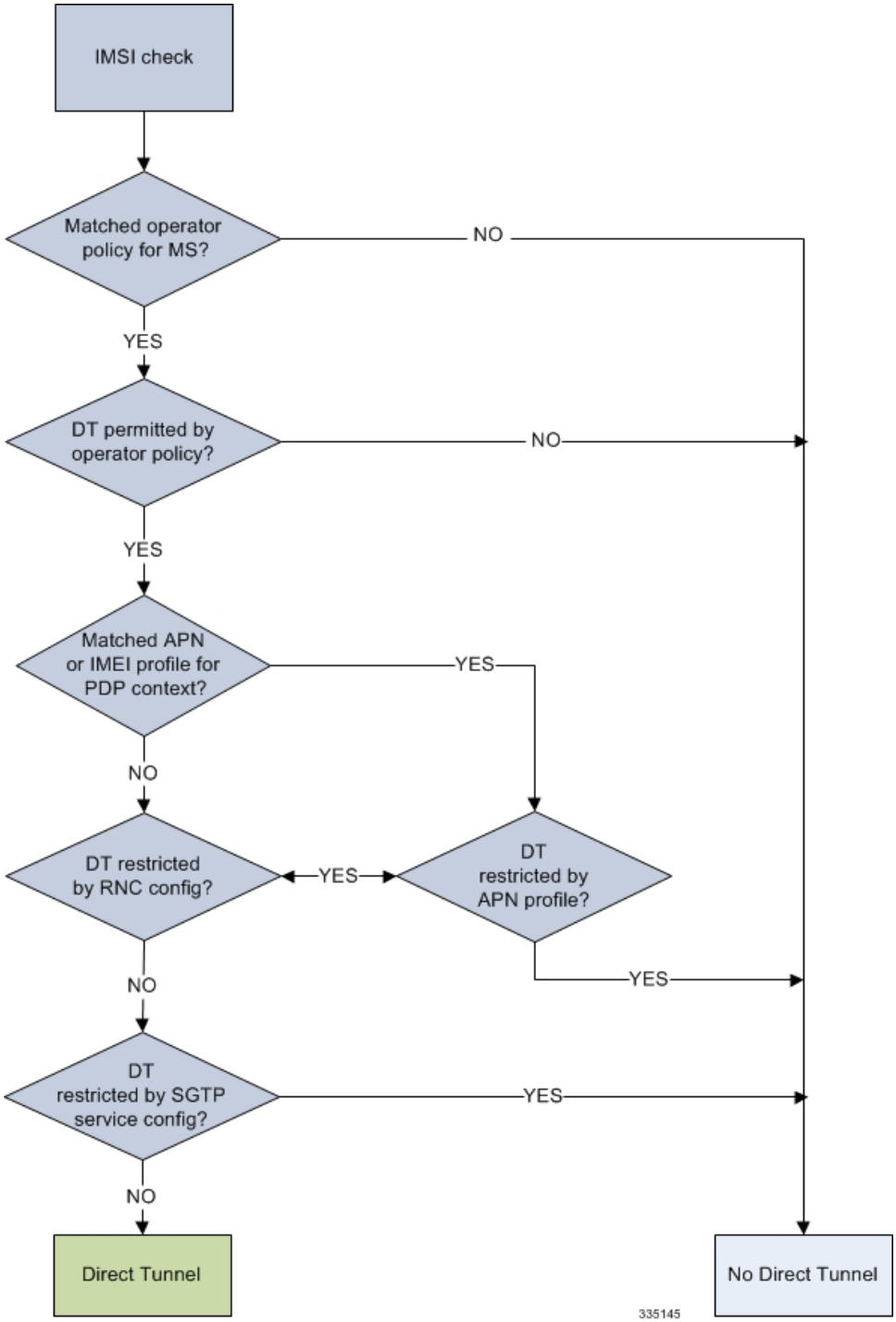
DT functionality enables direct user plane tunnel between RNC and SGW within the PS domain. With direct tunneling the S4-SGSN provides the RNC with the TEID and user plane address of the S-GW, and also provides the S-GW with the TEID and user plane address of the RNC.

The SGSN handles the control plane signaling and makes the decision when to establish the direct tunnel between RNC and S-GW, or use two tunnels for this purpose (based on configuration).

DT Establishment Logic

The following figure illustrates the logic used within the S4-SGSN/S-GW to determine if a direct tunnel will be setup.

Figure 30: Direct Tunneling - Establishment Logic



Establishment of Direct Tunnel

The S4-SGSN uses the S12 interface for DT.

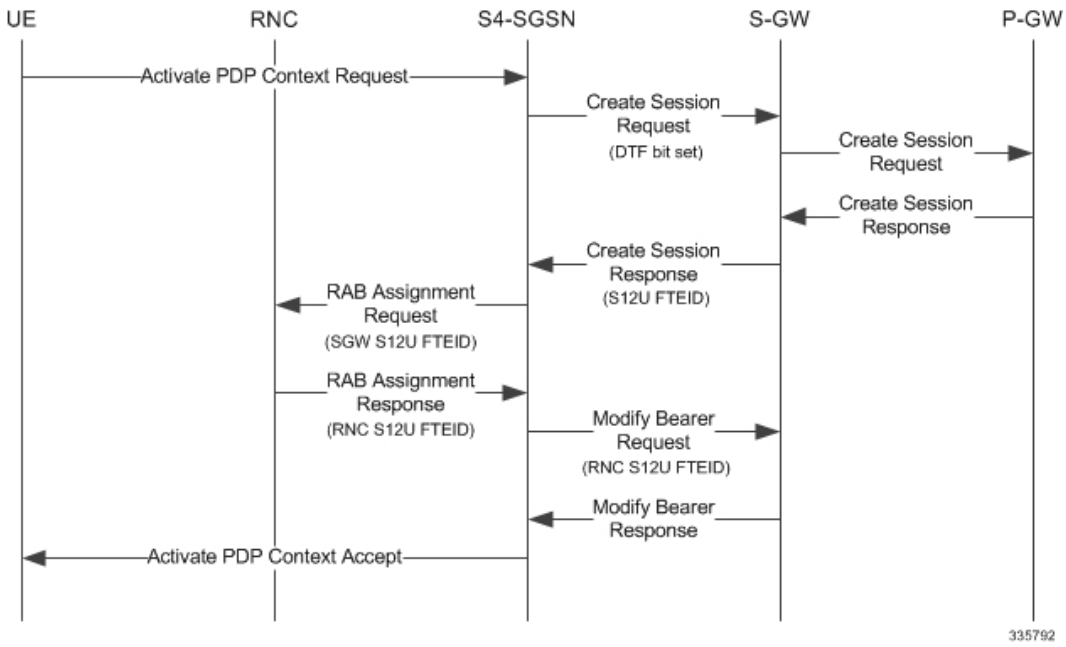
Direct Tunnel Activation for Primary PDP Context

For the PDP Context Activation procedure this solution uses new information elements (IEs) for the GPRS Tunnelling Protocol v2 (GTPv2) as defined in TS 29.274. SGSN provides the user plane addresses for RNC and S-GW as S12U FTEIDs as illustrated in the figure below.

The sequence for establishing a direct tunnel between the RNC and S-GW during PDP activation is as follows:

- SGSN sends a Create Session Request to the S-GW with the indication flag DTF (direct tunnel flag) bit set
- In its Create Session Response, the S-GW sends the SGSN an S12U FTEID (Fully Qualified Tunnel Endpoint Identifier).
- The SGSN forwards the S-GW S12U to the RNC during the RAB Assignment Request.
- In its RAB Assignment Response, the RNC sends the SGSN its transport address and Tunnel Endpoint ID (TEID).
- The SGSN forward the RNC S12 U FTEID o the S-GW via a Modify Bearer Request.

Figure 31: Primary PDP Activation with Direct Tunnel

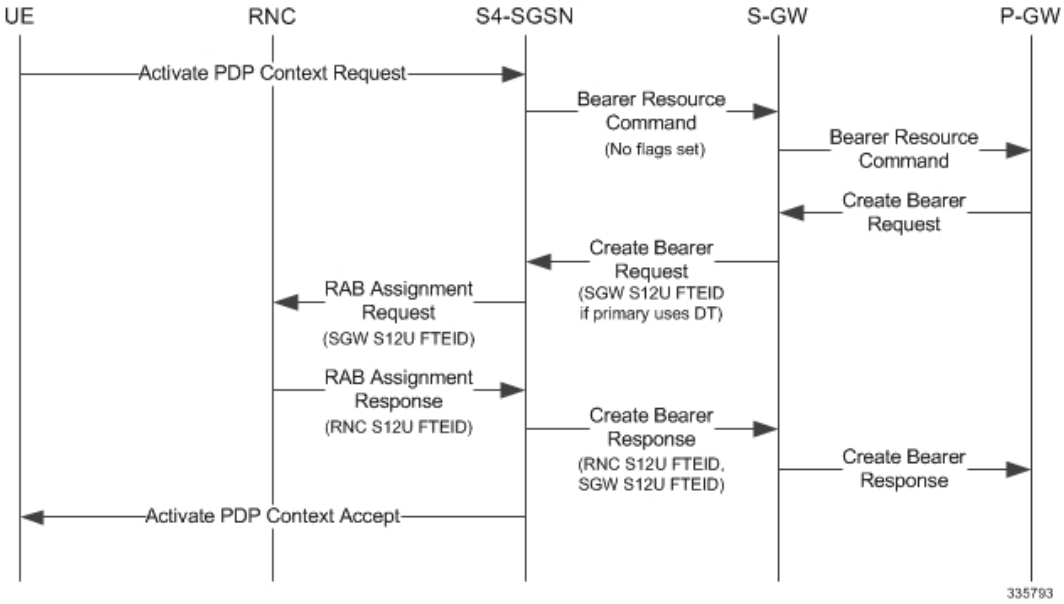


Direct Tunnel Activation for UE Initiated Secondary PDP Context

The following is the general sequence for establishing a direct tunnel for a Secondary PDP Context Activation:

- The SGSN sends a Bearer Resource Command to the S-GW with no flags set. (S-GW already knows Direct Tunnel is enabled for primary.)
- The S-GW sends a Create Bearer Response that includes the S12U FTEID to the SGSN.
- The SGSN forwards the S-GW S12U to RNC via a RAB Assignment Request.
- In its RAB Assignment Response, the RNC sends its transport address and TEID to the SGSN.
- The SGSN forwards the S12U TEID received from the RNC to the S-GW via a Create Bearer Response.

Figure 32: Secondary PDP Activation with Direct Tunnel



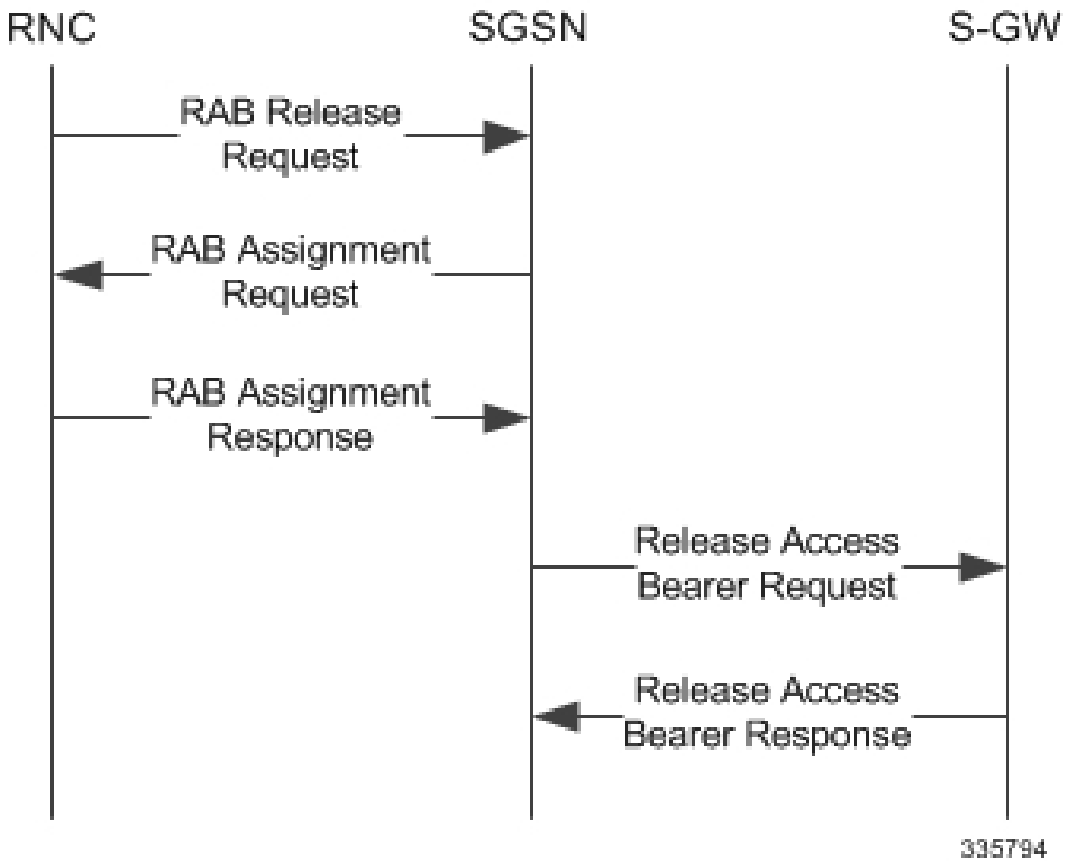
RAB Release with Direct Tunnel

If the SGSN receives a RAB Release Request from the RNC for bearer contexts activated with Direct Tunnel, it sends a Release Access Bearer Request to the S-GW.

Upon receiving the Release Access Bearer Request, the S-GW removes the S12 U RNC FTEID. If any downlink data appears, the S-GW sends a Downlink Data Notification because it does not have a user plane FTEID with which to forward data.

Bearers with a streaming or conversational class will not be included in the Release Access Bearer Request because these bearers should be deactivated. However, S4-SGSN currently does not support deactivation of streaming/conversational bearers upon RAB release.

Figure 33: RAB Release Procedure with Direct Tunnel



Important Operators should not use conversational or streaming class bearers in S4-SGSN.

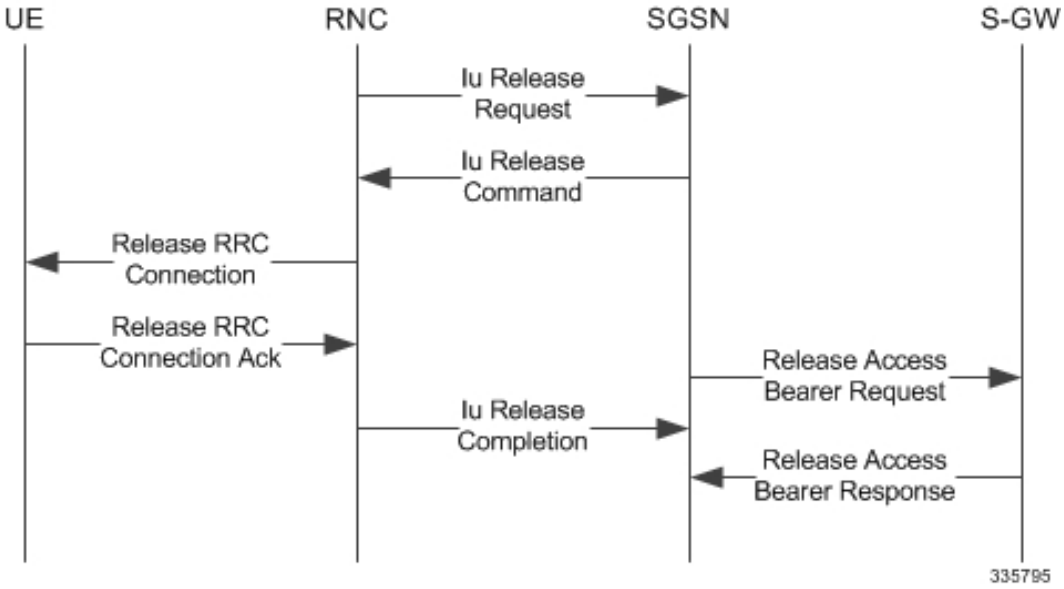
Iu Release with Direct Tunnel

If the SGSN receives an Iu Release and bearers are activated with direct tunneling, it sends a Release Access Bearer Request to the S-GW.

Bearers with a streaming or conversational class will not be included in the Release Access Bearer Request because these bearers should be deactivated. However, S4-SGSN currently does not support deactivation of streaming or conversational bearers upon Iu release.

Important Operators should not use conversational or streaming class bearers in S4-SGSN.

Figure 34: Iu Release Procedure with Direct Tunnel

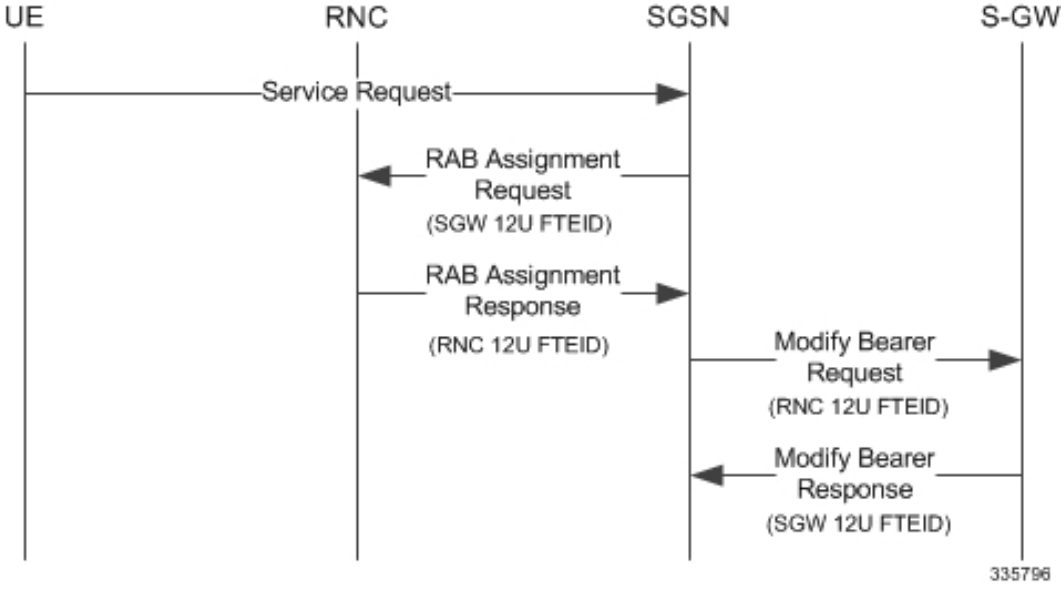


Service Request with Direct Tunnel

When a UE is Idle and wants to establish a data or signaling connection, it sends a Service Request for data. Alternatively a UE can also send a Service Request to the SGSN when it is paged by the SGSN.

Upon receiving a Service Request for data, the SGSN establishes RABs and sends a Modify Bearer Request to the S-GW with the 12U FTEID received from the RNC.

Figure 35: Service Request Procedure with Direct Tunnel



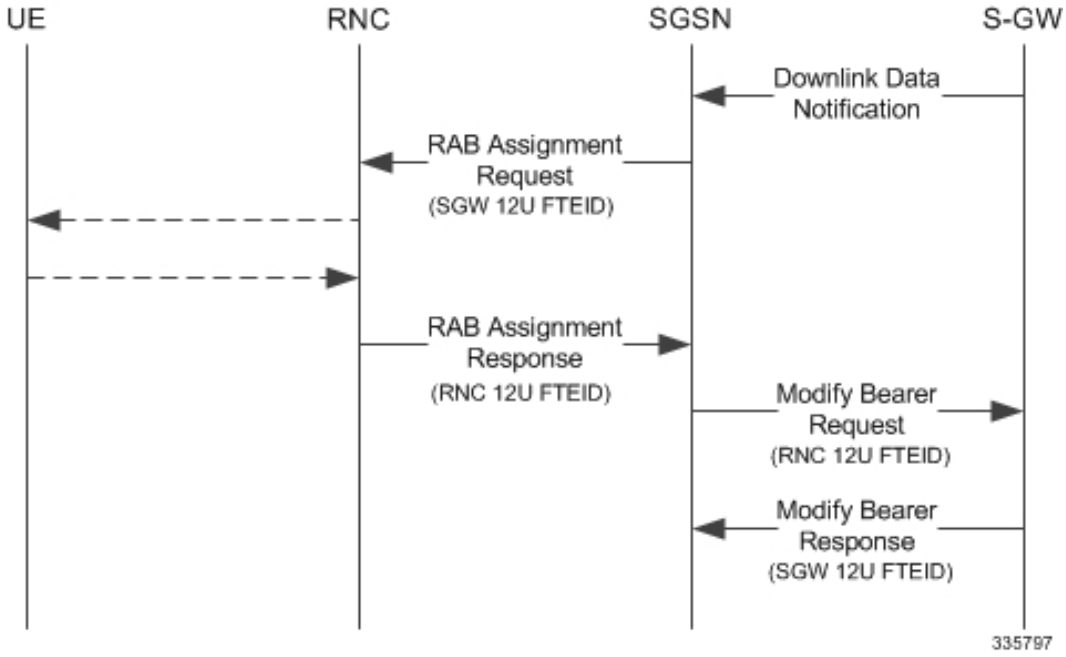
Downlink Data Notification with Direct Tunnel when UE in Connected State

When RABs are released (but UE retains an Iu connection with the SGSN), the SGSN notifies the S-GW to release the RNC side TEIDs via a Release Access Bearer Request.

If the S-GW receives any downlink GTPU data from the P-GW after receiving the Release Access Bearer Request, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data. So it signals the SGSN to establish the RABs. This signaling message is a Downlink Data Notification message from the S-GW.

If the Downlink Data Notification is received from the S-GW, all of the missing RABs are established and a Modify Bearer Request is sent to the S-GW with the RNC S12U FTEID

Figure 36: Downlink Data Notification with Direct Tunnel

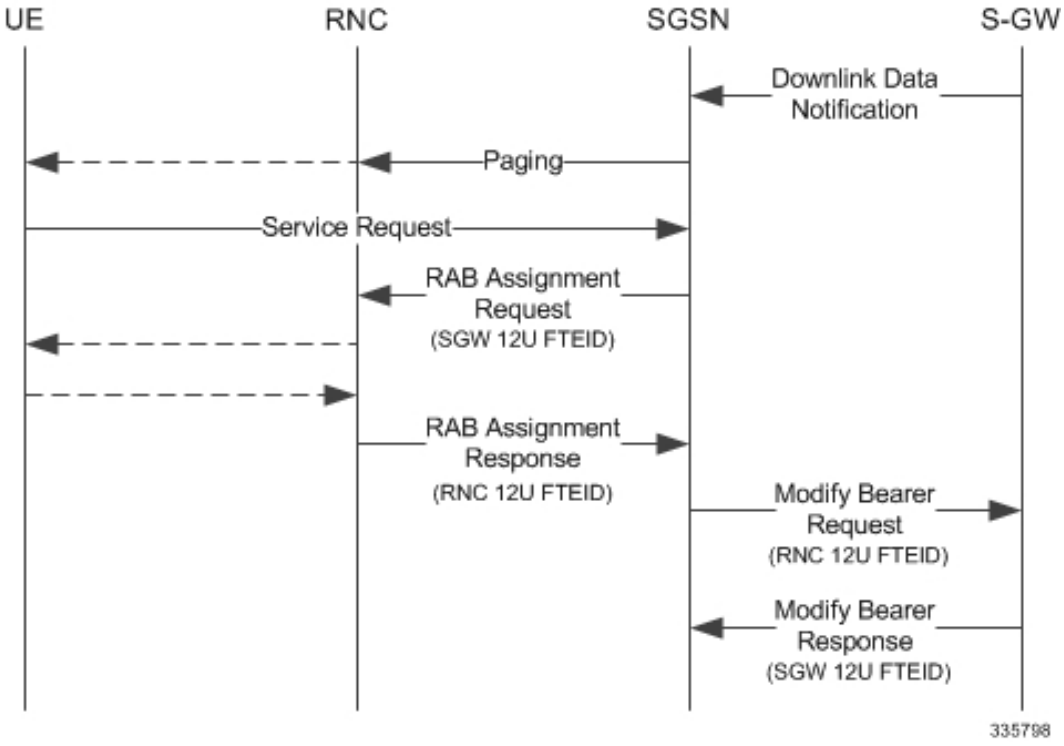


Downlink Data Notification with Direct Tunnel when UE in Idle State

When an Iu is released the UE goes IDLE. The SGSN informs the S-GW to release the RNC side TEIDs by sending a Release Access Bearer Request. After this point if the S-GW receives any downlink GTPU data from the P-GW, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data.

If the S-GW receives any downlink GTPU data after receiving the Release Access Bearer Request, it knows neither the RNC TEID nor SGSN user plane TEID to which to forward the data. So it signals the SGSN to establish the RABs. This signaling message is a Downlink Data Notification from the S-GW. If a Downlink Data Notification is received from S-GW when the UE is idle, the SGSN pages the UE before establishing the RABs. The SGSN sends a Modify Bearer Request to the S-GW with the RNC S12U FTEID.

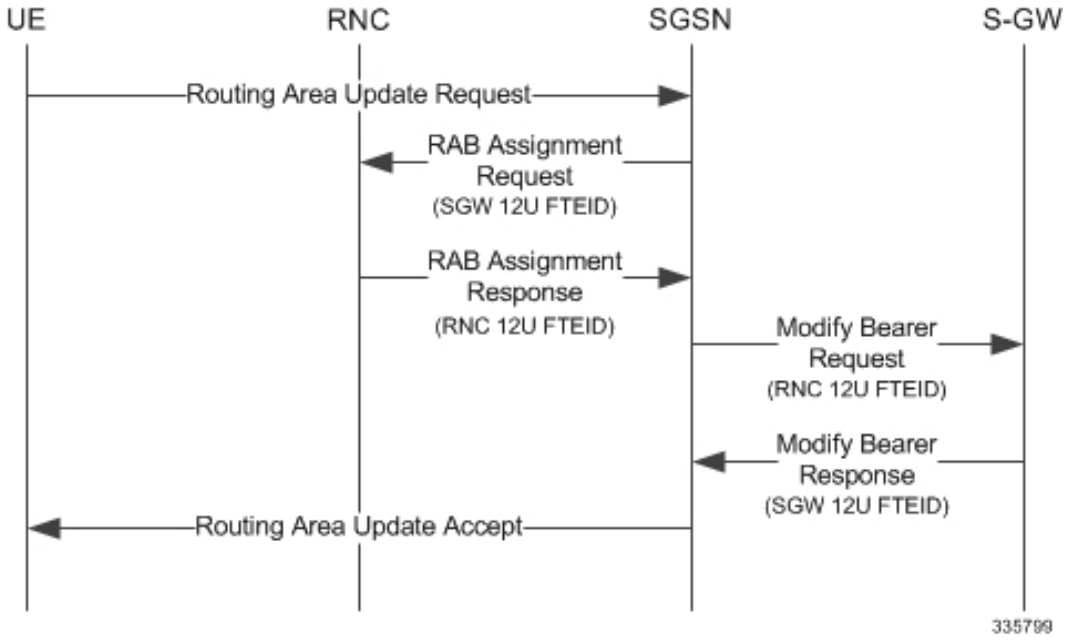
Figure 37: Downlink Data Notification when UE in Idle State



Intra SGSN Routing Area Update without SGW Change

For a Routing Area Update without an S-GW change with Direct Tunnel, the SGSN sends a Modify Bearer Request to the S-GW with the RNC FTEID. The SGSN will establish RABs with the target RNC only if the RABs were present with the source RNC.

Figure 38: Routing Area Update Procedure without SGW Change



The table below includes detailed behaviors for a Routing Area Update without S-GW change.

Table 14: Routing Area Update without S-GW Change Behavior Table

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Supported	No	Supported	No	No RAB establishment with new RNC. No Modify Bearer Request to S-GW
Intra RAU	Present	No RAB	Supported	No	Supported	No	No RAB establishment with new RNC. No Modify Bearer Request to S-GW

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Present	Some RABs	Supported	Do not care	Supported	No	Only the present RABs are established. MBR sent to S-GW with the bearers with RABs that are be modified and the rest released. The bearers without RABs will be deactivated post RAU. If PLMN changed then MBR will carry the new PLMN ID.
Intra RAU	Not Present	No RAB	Supported	Yes	Supported	No	No RAB establishment with new RNC. MBR is sent with only PLMN change. Bearer Context will not carry any TEID.
Intra RAU	Present	No RAB	Supported	Yes	Supported	No	Same as above.

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Not Supported	No	Supported	No	No RAB establishment with new RNC. Modify Bearer Request to S-GW with DTF set and no user FTEID.
Intra RAU	Present	No RAB	Not Supported	No	Supported	No	Same as above.
Intra RAU	Present	Some RABs	Not Supported	Do not care	Supported	No	Only the present RABs are established. MBR sent to S-GW with the bearers with RABs to be modified and the rest to be released. The bearers without RABs will be deactivated post RAU. If PLMN changed then MBR will carry the new PLMN ID.Modify Bearer.

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Not Supported	Yes	Supported	No	No RAB establishment with new RNC. MBR is sent with only PLMN change. SGSN will page / Service req / establish RABs when a downlink data notification is received.
Intra RAU	Present	No RAB	Not Supported	Yes	Supported	No	Same as above.
Intra RAU: New RNC does not support Direct Tunnel. No SGW relocation							
Intra RAU	Not Present	No RAB	Supported	Do not care	Not Supported	No	No RAB establishment with new RNC. SGSN sends Modify Bearer Request to S-GW with S4U TEID. If there is change in PLMN ID, then new PLMN ID will be carried.
Intra RAU	Present	No RAB	Supported	Do not care	No Supported	No	Same as above.

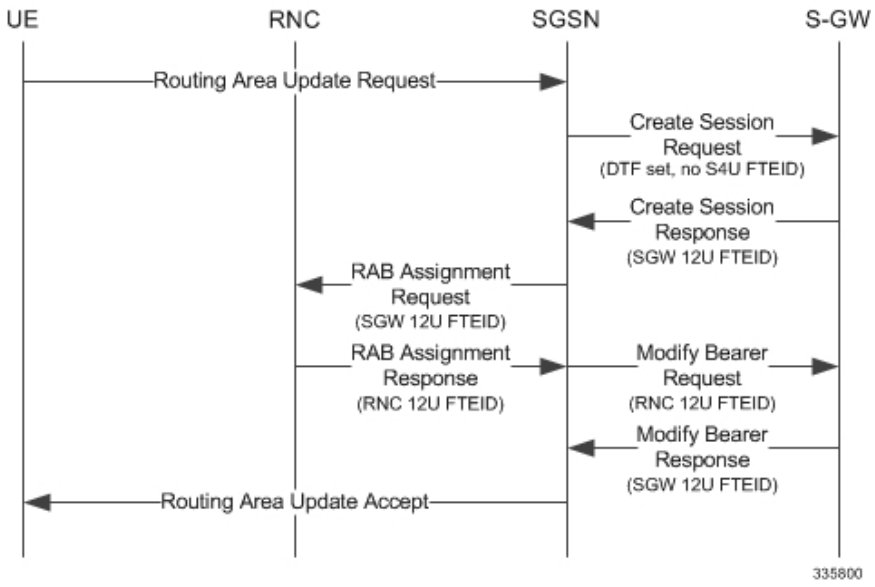
Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Present	Some RABs	Supported	Do not care	Not supported	No	Only the present RABs are established. MBR sent to S-GW with all bearers having S4U TEID. If there is change in PLMN ID, the new PLMN ID will be carried.

Routing Area Update with S-GW Change

In a Routing Area Update with an S-GW change, the SGSN sends a Create Session Request with DTF flag set and no user plane FTEID. In its Create Session Response,. the S-GW sends an S12U FTEID which is forwarded to the RNC via a RAB Assignment Request.

The SGSN sends the RNC FTEID received in the RAB Assignment Response to the S-GW in a Modify Bearer Request. There are many scenarios to consider during Intra SGSN RAU.

Figure 39: Routing Area Update Procedure with SGW Change



The table below includes detailed behaviors for a Routing Area Update with S-GW change.

Table 15: Routing Area Update with S-GW Change Behavior Table

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU: Both RNCs support Direct Tunnel. SGW relocation							
Intra RAU	Not Present	No RAB	Supported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U / S12U FTEID. S-GW will send its S12U TEID that SGSN stores as part of DP's remote TEID. SGSN will not initiate any MBR request to S-GW since no RABs are established with new RNC. If S-GW subsequently gets downlink data, SGSN will get DDN and establish RABs and send MBR.
Intra RAU	Present	No RAB	Supported	Do not care	Supported	Yes	Same as above.

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Present	Some RABs	Supported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U / S12U FTEID. S-GW sends its S12U TEID. RABs that are present will be established with new RNC. MBR will be initiated only with those RABs that are present rest of bearers to be removed.
Intra RAU: Old RNC does not support Direct Tunnel. SGW relocation							

Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Not Present	No RAB	Not Supported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U / S12U FTEID. S-GW sends its S12U TEID that SGSN stores as part of our DP's remote TEID. SGSN will not initiate any MBR request to S-GW since no RABs are established with new RNC. If S-GW subsequently gets downlink data, SGSN gets DDN and establishes RABs and sends MBR.
Intra RAU	present	No RAB	Not Supported	Do not care	Supported	Yes	Same as above.

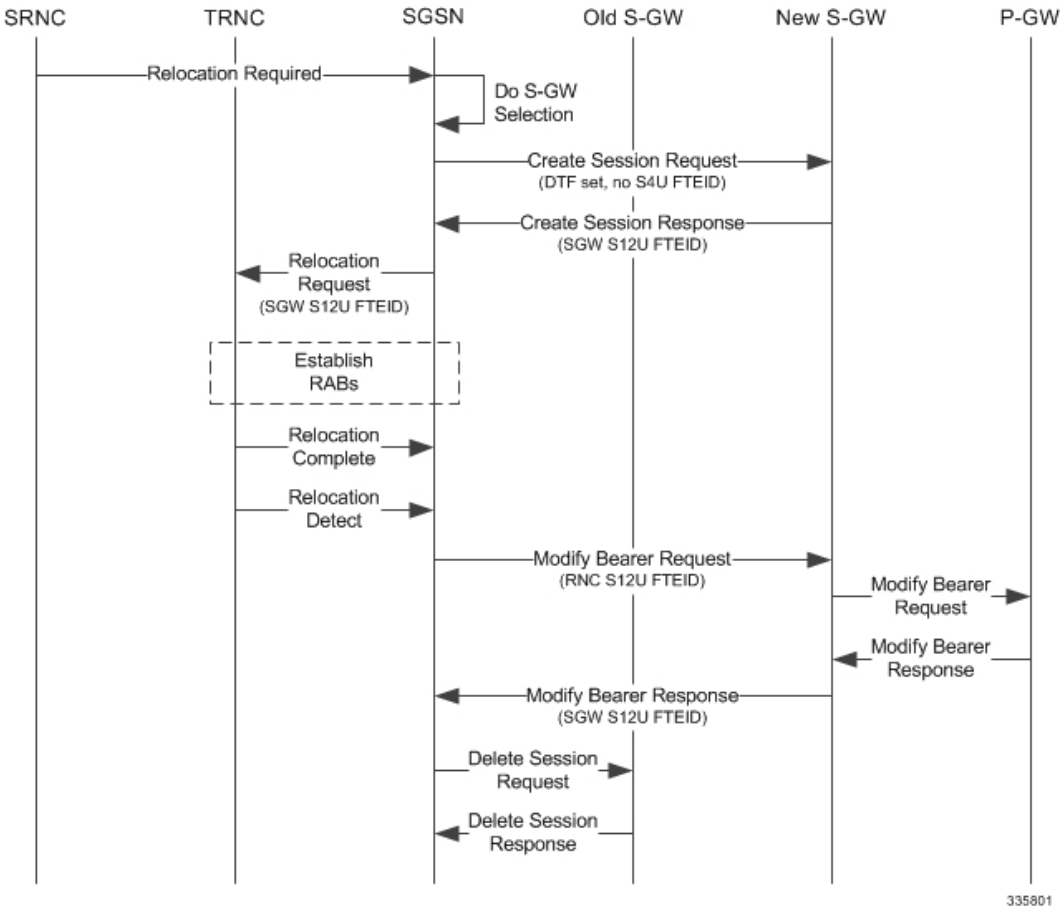
Scenario	Old RNC Status	Old RNC RAB	Old RNC DT Status	PLMN Change	NEW RNC DT Status	S-GW Change	SGSN Action
Intra RAU	Present	Some RABs	Not SUpported	Do not care	Supported	Yes	Send CSR request to new S-GW with DTF flag but no S4U / S12U FTEID. S-GW sends its S12U TEID. RABs that are present will be established with new RNC and MBR will be initiated only with those RABs that are present and the rest as bearers to be removed.
Intra RAU: New RNC does not support Direct Tunnel. SGW relocation							
Intra RAU	Not Present	No RAB	Supported	Do not care	Not Supported	Yes	CSR request without DTF flag and with S4U FTEID.
Intra RAU	Present	No RAB	Supported	Do not care	Not Supported	Yes	CSR request without DTF flag and with S4U FTEID.
Intra RAU	Present	Some rABs	Supported	Do not care	Not Supported	Yes	CSR request without DTF flag and with S4U FTEID. No deactivation of PDPs.

Intra SRNS with S-GW Change

In Intra SRNS (Serving Radio Network Subsystem) with S-GW change, the SGSN sends a Create Session Request with DTF flag set and no user plane FTEID. The Create Session Response from the new S-GW contains the SGW S12U FTEID which the SGSN forwards to the Target RNC in a Relocation Request.

The SGSN sends the RNC S12U FTEID to the new S-GW in a Modify Bearer Request.

Figure 40: Intra SRNS with S-GW Change

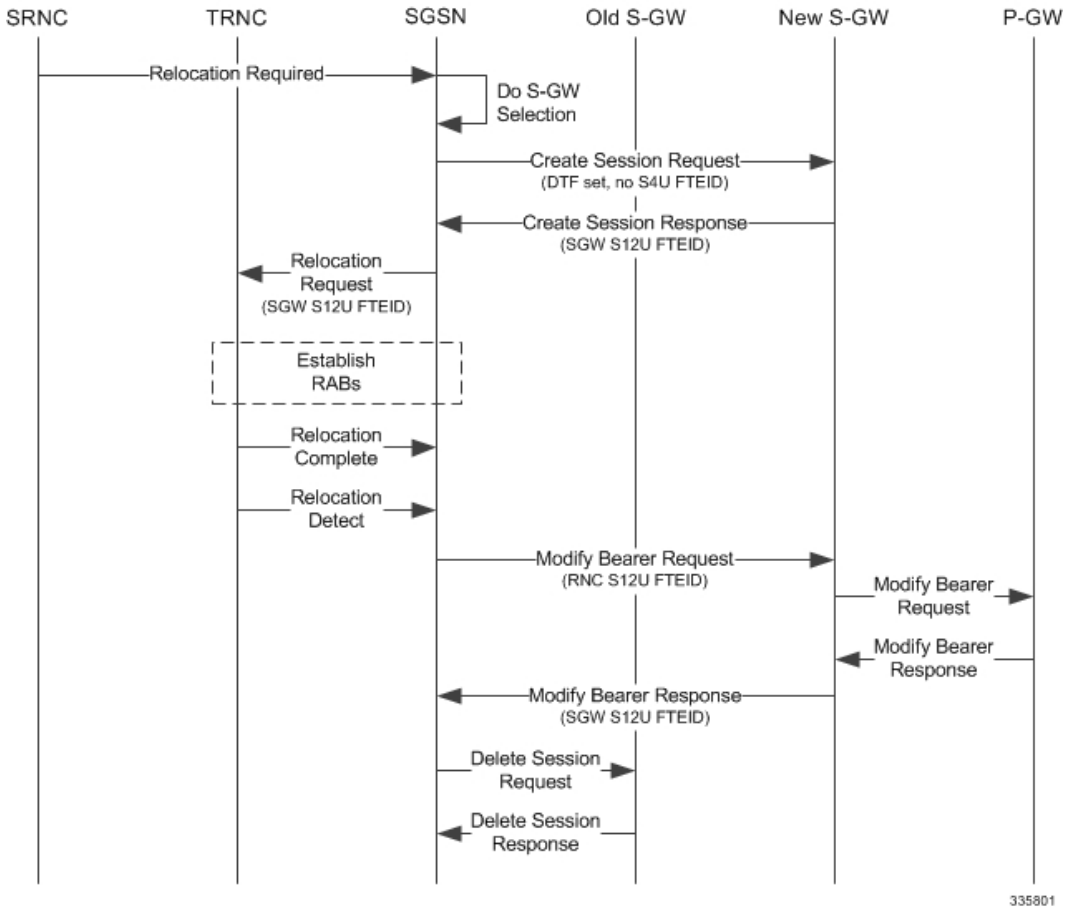


The table below includes detailed behaviors for intra SRNS scenarios.

Intra SRNS without S-GW Change

In Intra SRNS without S-GW change, a Relocation Request is sent with SGW S12U FTEID. The RNC S12U FTEID received is forwarded to the S-GW in a Modify Bearer Request.

Figure 41: Intra SRNS without S-GW Change



The table below includes detailed behaviors for intra SRNS scenarios.

Table 16: Intra SRNS Behaviors

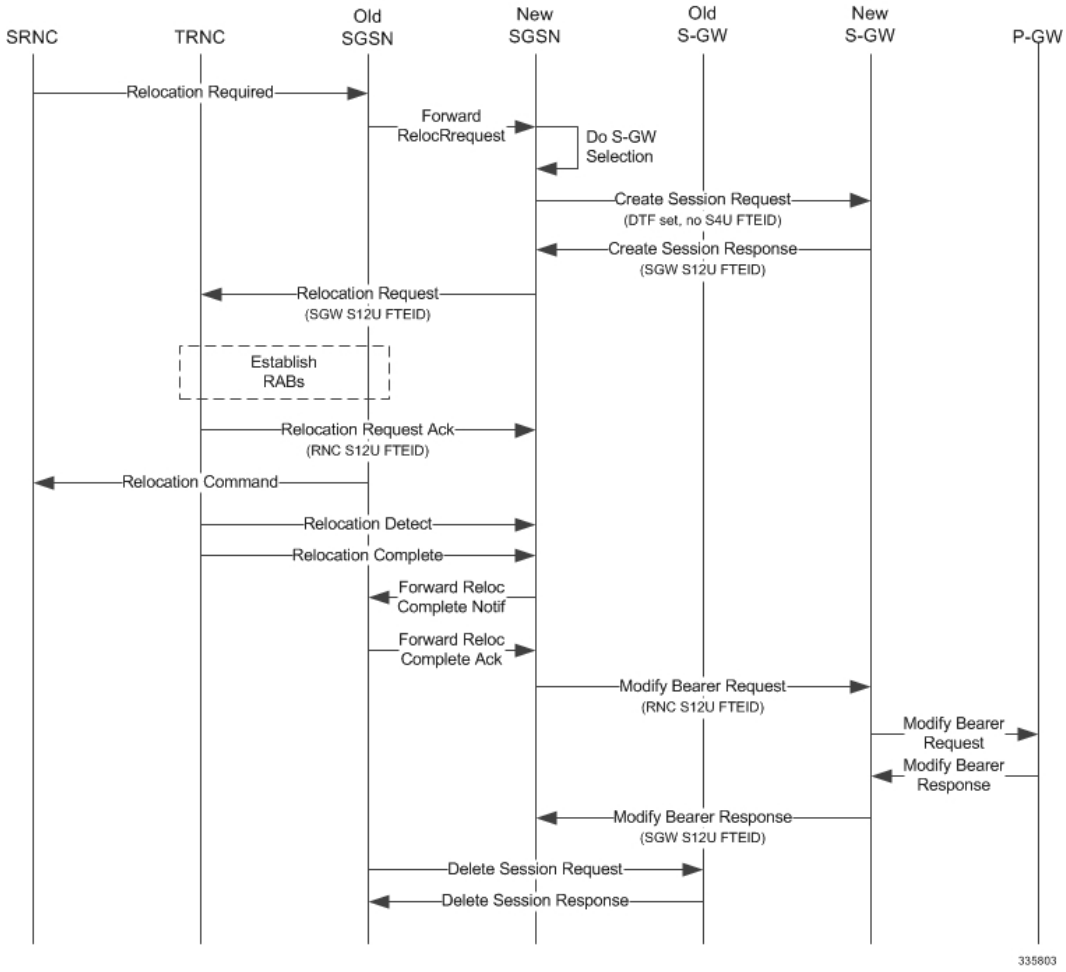
Old RNC DT Status	New RNC DT Status	S-GW Relocation	Behavior
Supported	Supported	No	Relocation Request to Target RNC is sent with S-GW S12 U FTEID. Modify Bearer Request to S-GW is sent with RNC S12 U FTEID.
Supported	Not Supported	No	Relocation Request to Target RNC is sent with SGSN S4 U FTEID. Modify Bearer Request to S-GW is sent with SGSN S4 U FTEID

Old RNC DT Status	New RNC DT Status	S-GW Relocation	Behavior
Not Supported	Supported	No	Relocation Request to Target RNC is sent with S-GW S12U FTEID. Modify Bearer Request to S-GW is sent with RNC S12 U FTEID.
Not Supported	Supported	Yes	Create Session Request to new S-GW is sent with DTF flag set and no user plane FTEID. Even if S-GW sent S4U FTEID in CSR Response SGSN internally treats that as an S12U FTEID and continues the relocation. Relocation Request to Target RNC is sent with S12 U FTEID received in Create Session Response. Modify Bearer Request to new S-GW is sent with RNC S12U FTEID
Supported	Not Supported	Yes	Create Session Request to new SGW is sent with S4 U FTEID. Relocation Request to Target RNC is sent with SGSN U FTEID.Modify Bearer Request is sent with SGSN S4U FTEID.
Supported	Supported	Yes	SGSN sends a Create Session Request to new SGW with DTF flag set and no user plane FTEID.Even if S-GW sent S4U FTEID in CSR Response, SGSN will internally treat that as S12U FTEID and continue the relocation. Relocation Request to the Target RNC is sent with the S12 U FTEID received in the Create Session Response. Modify Bearer Request to new S-GW is sent with RNC U FTEID.

New SRNS with S-GW Change and Direct Data Transfer

The new SGSN sends a Create Session Request with DTF flag set and no user plane FTEID to the new S-GW. The new SGSN sends the SGW S12U FTEID received in the Create Session Response in Relocation Request to the Target RNC. The new SGSN sends the RNC S12U FTEID received in a Relocation Request Ack to the new S-GW in a Modify Bearer Request.

Figure 42: New SRNS with S-GW Change with Data Transfer

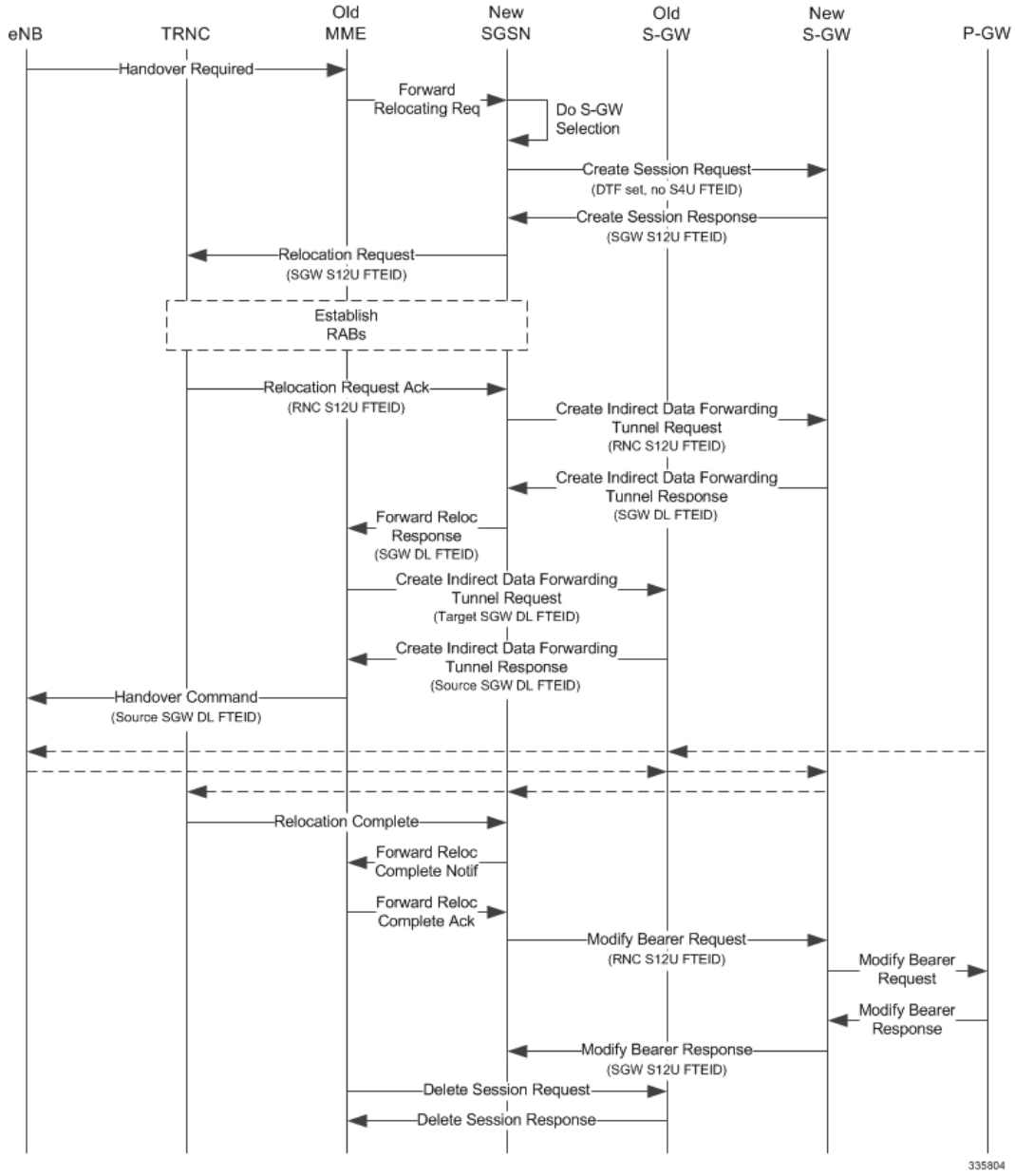


The table below includes detailed behaviors for New SRNS scenarios.

New SRNS with S-GW Change and Indirect Data Transfer

Indirect Data Transfer (IDFT) during a new SGSN SRNS happens during E-UTRAN-to-UTRAN connected mode IRAT handover. See the figure below for a detailed call flow.

Figure 43: New SRNS with S-GW Change and Indirect Data Transfer



The table below includes detailed behaviors for New SRNS scenarios.

Table 17: New SRNS Behaviors

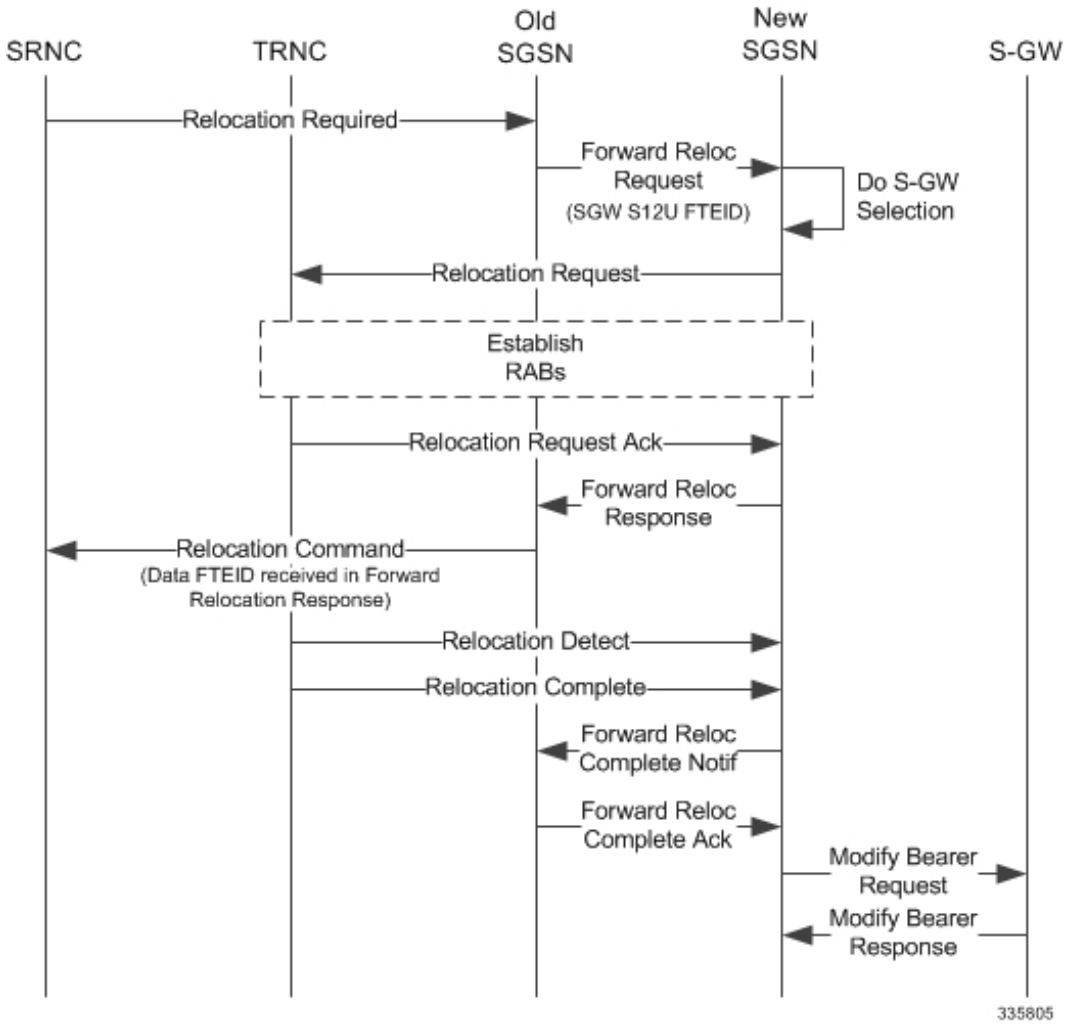
Target RNC DT Status	Direct Forwarding	S-GW Relocation	Behavior
Supported	No	No	Relocation Request with SGW S12U FTEID received in Forward Relocation Request. SGSN includes RNC U FTEID in Forward Relocation Response. RNC U FTEID is also sent in Modify Bearer Request with DTF flag set.
Supported	Yes	No	Relocation Request with SGW S12U FTEID received in Forward Relocation Request. In Forward Relocation Response RNC U FTEID is included. And in Modify Bearer Request RNC U FTEID is sent and DTF flag is set.
Supported	No	Yes	Create Session Request with DTF flag set and no user plane FTEID. Relocation Request is sent is SGW S12U FTEID received in Create Session Response. Even if SGW sent S4U FTEID in CSR Response we will internally treat that as S12U FTEID and continue the relocation. Create Indirect Data Forwarding Tunnel Request is sent with RNC FTEID received in Relocation Request Acknowledge.In Forward Relocation Response SGW DL U FTEID received in Create IDFT response is sent. Modify Bearer Request is send with DTF set and RNC U FTEID.

Target RNC DT Status	Direct Forwarding	S-GW Relocation	Behavior
Supported	Yes	Yes	Create Session Request with DTF flag set and no user plane FTEID. Relocation Request is sent with SGW S12U FTEID received in Create Session Response. Even if SGW sent S4U FTEID in CSR Response we will internally treat that as S12U FTEID and continue the relocation. In Forward Relocation Response RNC FTEID is sent and Modify Bearer Request is sent with DTF flag set and RNC U FTEID

Old SRNS with Direct Data Transfer

This scenario includes SRNS relocation between two SGSNs and hence IDFT is not applicable. Data will be forwarded between the source and target RNCs directly. Forward Relocation Request is sent with S12U FTEID.

Figure 44: Old SRNS with Direct Data Transfer



The table below includes detailed behaviors for Old SRNS.

Old SRNS with Indirect Data Transfer

Indirect Data Transfer (IDFT) during Old SGSN SRNS happens during UTRAN-to-E-UTRAN connected mode IRAT handover. A Forward Relocation Request is sent with SGW S12U FTEID.

Figure 45: Old SRNS with Indirect Data Transfer 4

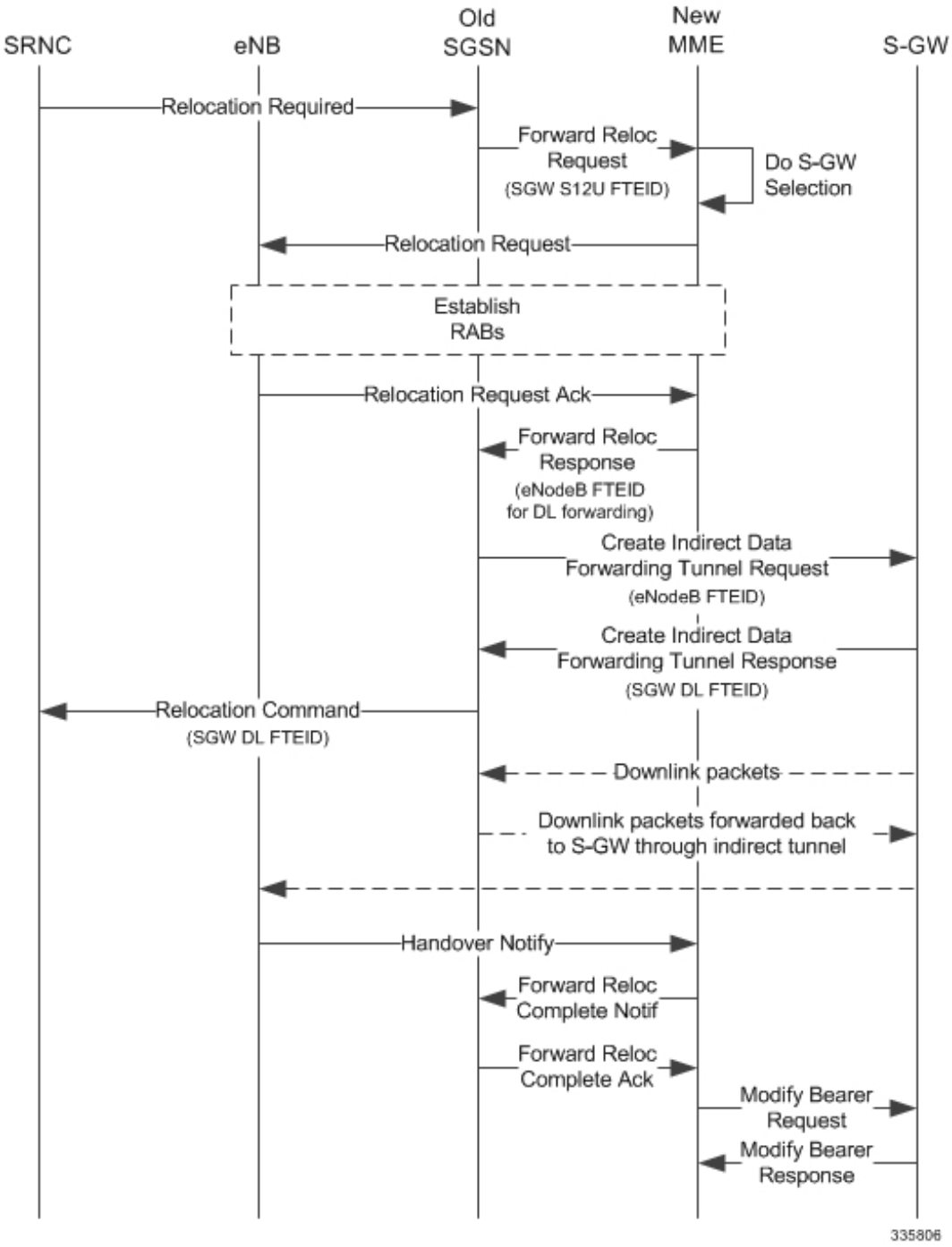


Table 18: Old SRNS Behaviors

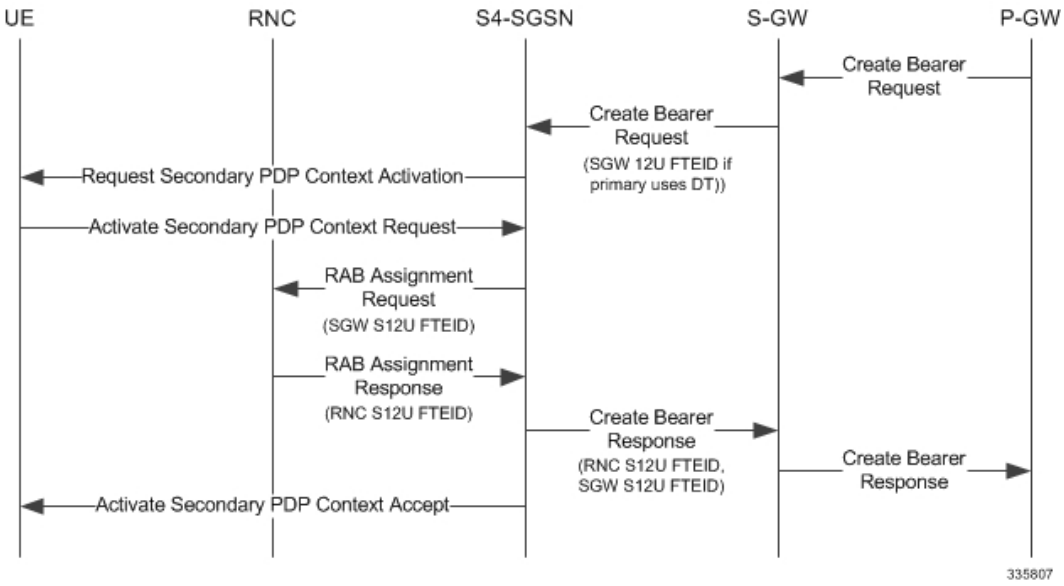
Source RNC DT Status	Direct Forwarding	S-GW Relocation	Behavior
Supported	No	No	Forward Relocation Request is send with SGW S12 U FTEID. If peer is MME, IDFT is applied. Then a Create Indirect Data Forwarding Tunnel Request is sent with User plane FTEID received in the Forward Relocation Response. This will be the eNB user plane FTEID. The SGW DL forwarding user plane FTEID received in the Create Indirect Data Forwarding Tunnel Response is sent in the Relocation Command.
Supported	Yes	No	Forward Relocation Request is sent with SGW S12 U FTEID. The eNB / RNC user plane FTEID received in the Forward Relocation Response is sent in the Relocation Command.
Supported	No	Yes	Forward Relocation Request is sent with SGW S12 U FTEID. If peer is MME, IDFT is applied. Then Create Indirect Data Forwarding Tunnel Request is sent with eNB User plane FTEID received in the Forward Relocation Response. The SGW DL forwarding user plane FTEID received in the Create Indirect Data Forwarding Tunnel Response is sent in the Relocation Command.

Source RNC DT Status	Direct Forwarding	S-GW Relocation	Behavior
Supported	Yes	Yes	Forward Relocation Request is sent with SGW S12 U FTEID. The eNB / RNC use plane FTEID received in the Forward Relocation Response is sent in the Relocation Command.

Network Initiated Secondary PDP Context Activation

The S-GW sends a Create Bearer Request for Network Initiated Secondary PDP Context Activation with the SGW S12U FTEID. This FTEID is sent in a RAB Assignment Request to the RNC. The RNC S12U FTEID received in the RAB Assignment Response is sent to the S-GW in a Create Bearer Response.

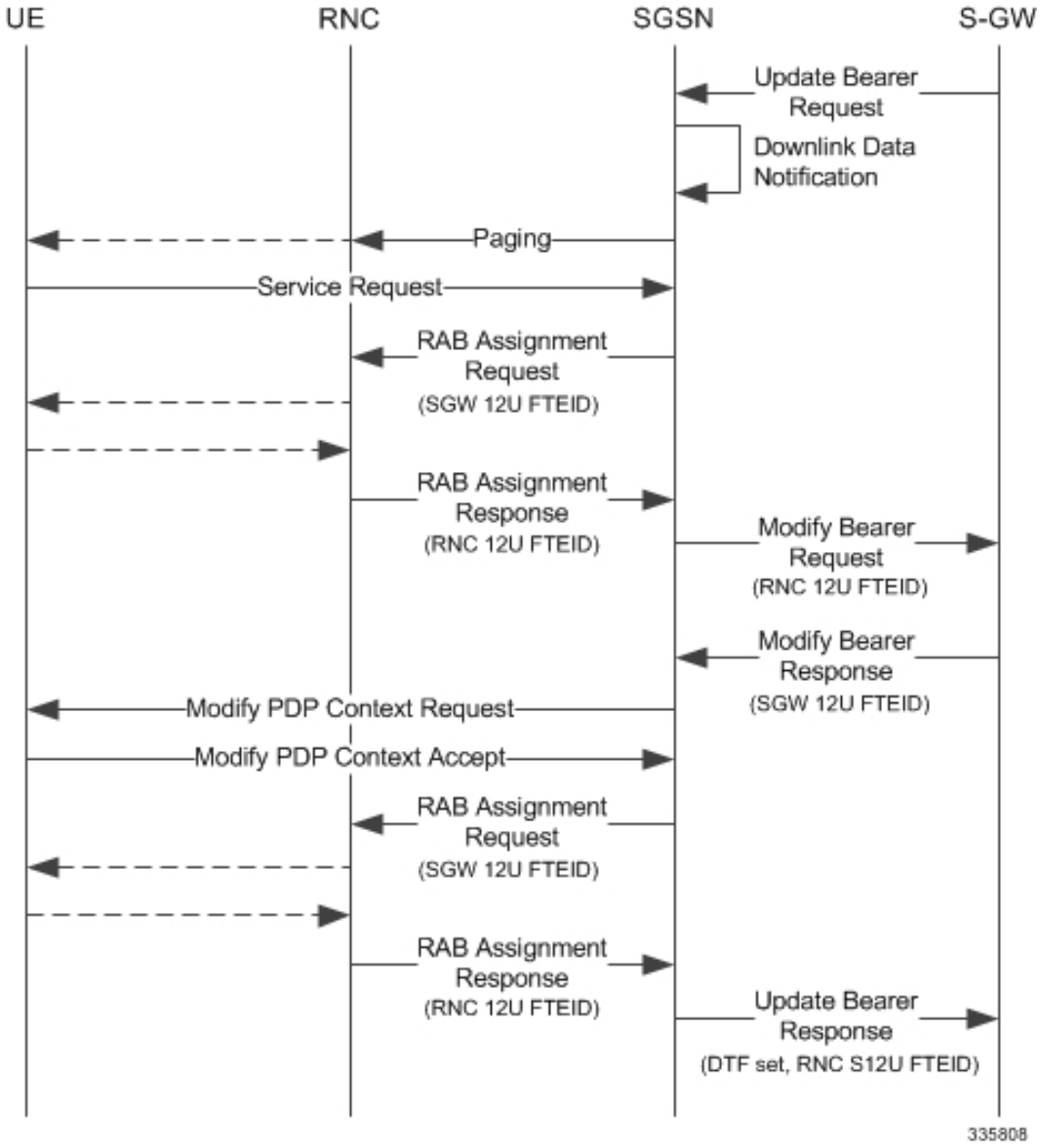
Figure 46: Network Initiated Secondary PDP Context Activation 5



PGW Init Modification when UE is Idle

If UE is in IDLE state and PGW Init Modification is received, the SGSN sends the first MBR. Upon getting PGW Init Modification in Idle State, the SGSN queues the PGW Init Modification and feeds a Downlink Data Notification internally. This sets up all RABs (using old QoS) and sends a Modify Bearer Request. When the Downlink Data Procedure is completed, the queued PGW Init Modification is processed.

Figure 47: PGW Init Modification when UE in Idle State



Limitations

During an intra RAU, intra SRNS or Service Request triggered by RAB establishment, if a few RABs fail the Modify Bearer Request the SGSN will mark those RABs as bearers to be removed. Under current specifications, it is not possible to send a Modify Bearer Request with a few bearers having S12U U-FTEIDs and a few bearers not having U-FTEIDs.

There is an ongoing CR at 3GPP to allow such Modify Bearer Requests and the S-GW should send DDN when it gets downlink data for the bearers that did not have U-FTEIDs. If this CR is approved, the SGSN will support (in a future release) sending a partial set of bearers with S12U FTEID and some bearers without any U-FTEID.

Standards Compliance

The Direct Tunnel complies with the following standards:

- 3GPP TS 23.060 version 10 sec 9.2.2 General Packet Radio Service (GPRS) Service description
- 3GPP TS 29.274 v10.5.0 3GPP Evolved Packet System (EPS) Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C)

Configuring Support for Direct Tunnel

The SGSN determines if setup of a direct tunnel is allowed or disallowed. Currently, the SGSN and S-GW are the only products that provide configuration commands for this feature. All other products that support direct tunnel do so by default.

By default, direct tunnel support is

- *disallowed* on the SGSN/S-GW
- *allowed* on the GGSN/P-GW

The SGSN/S-GW direct tunnel functionality is enabled within an operator policy configuration. One aspect of an operator policy is to allow or disallow the setup of direct GTP-U tunnels. If no operator policies are configured, the system looks at the settings in the operator policy named ***default***. If direct tunnel is allowed in the ***default*** operator policy, then any incoming call that does not have an applicable operator policy configured will have direct tunnel *allowed*. For more information about the purpose and uses of operator policies, refer to the section *Operator Policy*.

Configuring Direct Tunnel on an S4-SGSN

Configuration of a GTP-U direct tunnel (DT) requires enabling DT both in a call control profile and for the RNC.

Important Direct tunneling must be enabled at both end points to allow direct tunneling for the MS/UE.

Enabling Setup of GTP-U Direct Tunnel

The SGSN determines whether a direct tunnel can be setup and by default the SGSN does not support direct tunnel. The following configuration enables a GTP-U DT in a call control profile:

```
config
  call-control-profile policy_name
    direct-tunnel attempt-when-permitted [ to-ggsn | to-sgw ]
    end
```

Notes:

- A call-control profile must have been previously created, configured, and associated with a previously created, configured, and valid operator policy. For information about operator policy creation/configuration, refer to the *Operator Policy* chapter in this guide.

- Beginning with Release 19.3.5, **to-ggsn** and **to-sgw** options have been added to the **direct-tunnel** command to enable the operator to select the interface the SGSN will use for its direct tunnel. For a collocated Gn/GP-SGSN and an S4-SGSN,
  - Use the keyword **attempt-when-permitted** without a filter to enable both interface types: GTP-U towards the GGSN and S12 towards the SGW.
  - Use the keyword **attempt-when-permitted** with the **to-ggsn** keyword filter to enable only the GTP-U interface between the RNC and the GGSN.
  - Use the keyword **attempt-when-permitted** with the **to-sgw** keyword filter to enable only the S4's S12 interface between the RNC and the SGW.
- To remove the direct tunnel settings from the configuration, use the following command: **direct-tunnel attempt-when-permitted [to-ggsn | to-sgw]**
- Direct tunnel is allowed on the SGSN but will only setup if allowed on both the destination node and the RNC.

Enabling Direct Tunnel to RNCs

SGSN access to radio access controllers (RNCs) is configured in the IuPS service. Each IuPS service can include multiple RNC configurations that determine communications and features depending on the RNC. By default, DT functionality is enabled for all RNCs.

The following configuration sequence enables DT to a specific RNC that had been previously disabled for direct tunneling:

```
config
  context ctxt_name
    iups-service service_name
      rnc id rnc_id
        default direct-tunnel
        end
```

Notes:

- An IuPS service must have been previously created, and configured.
- An RNC configuration must have been previously created within an IuPS service configuration.
- Command details for configuration can be found in the *Command Line Interface Reference.*

Restricting Direct Tunnels

The following configuration scenario prohibits the S4-SGSN to setup direct tunneling over the S12 interface during Inter SGSN RAUs:

```
config
  call-control-profile profile_name
    rau-inter avoid-s12-direct-tunnel
    end
```

Restrict direct tunneling by a specific RNC. The following configuration scenario restricts the SGSN from attempting to setup a direct tunnel when a call originates from a specific RNC.

```
config
   context context_name
      iups-service service_name
         rnc id rnc_id
            direct-tunnel not-permitted-by-rnc
            end
```

Verifying the Call-Control Profile Configuration

Use the following command to display and verify the direct tunnel configuration for the call-control profiles:

show call-control-profile full name *<profile_name>*

The output of this command displays all of the configuration, including direct tunnel for the specified call-control profile.

```
Call Control Profile Name = ccprofile1
.
.
.
Re-Authentication
         : Disabled
Direct Tunnel
            : Not Restricted
GTPU Fast Path
            : Disabled
.
.
```

Verifying the RNC Configuration

Use the following command to display and verify the direct tunnel configuration in the RNC configuration:

show iups-service name *<service_name>*

The output of this command displays all of the configuration, including direct tunnel for the specified IuPS service.

```
IService name                                                  : iups1
.
.
.
Available RNC:
    Rnc-Id                                                        : 1
    Direct Tunnel                                              : Not Restricted
```

Configuring S12 Direct Tunnel Support on the S-GW

The example in this section configures an S12 interface supporting direct tunnel bypass of the S4 SGSN for inter-RAT handovers.

The direct tunnel capability on the S-GW is enabled by configuring an S12 interface. The S4 SGSN is then responsible for creating the direct tunnel by sending an FTEID in a control message to the S-GW over the S11 interfaces. The S-GW responds with it's own U-FTEID providing the SGSN with the identification information required to set up the direct tunnel over the S12 interface.

Important If you modify the **interface-type** command, the parent service (service within which the eGTP/GTP-U service is configured) will automatically restart. Service restart results in dropping of active calls associated with the parent service.

Use the following example to configure this feature.

```
configure
   context egress_context_name -noconfirm
      interface s12_interface_name
         ip address s12_ipv4_address_primary
         ip address s12_ipv4_address_secondary
         exit
      exit
   port ethernet slot_number/port_number
      no shutdown
      bind interface s12_interface_name egress_context_name
      exit
   context egress_context_name -noconfirm
      gtpu-service s12_gtpu_egress_service_name
         bind ipv4-address s12_interface_ip_address
         exit
      egtp-service s12_egtp_egress_service_name
         interface-type interface-sgw-egress
         validation-mode default
         associate gtpu-service s12_gtpu_egress_service_name
         gtpc bind address s12_interface_ip_address
         exit
      sgw-service sgw_service_name -noconfirm
         associate egress-proto gtp egress-context egress_context_name
egtp-service s12_egtp_egress_service_name
         end
```

Notes:

- The S12 interface IP address(es) can also be specified as IPv6 addresses using the **ipv6 address** command.

Monitoring and Troubleshooting Direct Tunnel

show subscribers sgsn-only

The output of this command indicates whether. Direct Tunnel has been established.

```
show subscribers sgsn-only full all
```

```
Username: 123456789012345
 Access Type: sgsn-pdp-type-ipv4        Network Type: IP
 Access Tech: WCDMA UTRAN
  |
  |
```

```
NSAPI: 05                                Context Type: Primary
Context initiated by: MS
Direct Tunnel : Established
```

show gmm-sm statistics sm-only

The output of this command indicates the number of total active PDP contexts with direct tunnels.

show gmm-sm statistics sm-only

```
Activate PDP Contexts:
 Total Actv PDP Ctx:
  3G-Actv Pdp Ctx:             1  2G-Avtv Pdp Ctx:       0
  Gn Interface:                1  Gn Interface:          0
  S4 Interface:                1  S4 Interface:          0
 Total Actv Pdp Ctx:
  with Direct Tunnel:          1
```

Direct Tunnel Bulk Statistics

Currently there are no bulk statistics available to monitor the number of PDP contexts with Direct Tunnel.

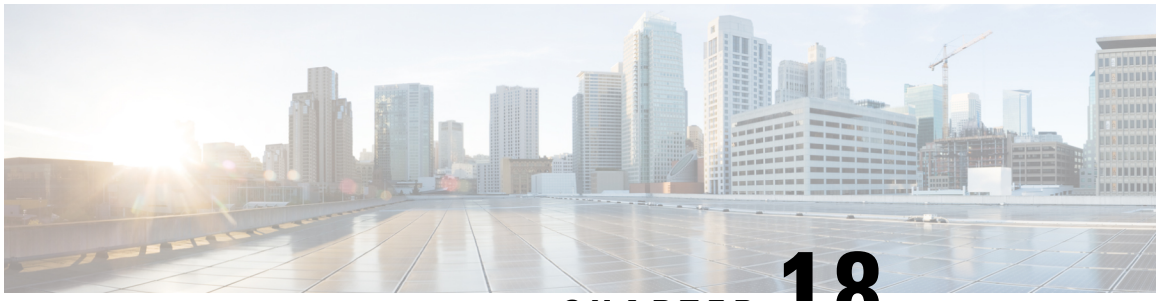
Bulk statistics under the EGTPC schema are applicable for both Direct Tunnel and Idle Mode Signalling Reduction (ISR) [3G and 2G]. The following statistics track the release access bearer request and response messages which are sent by the SGSN to the S-GW upon Iu or RAB release when either a direct tunnel or ISR is active:

- tun-sent-relaccbearreq
- tun-sent-retransrelaccbearreq
- tun-recv-relaccbearresp
- tun-recv-relaccbearrespDiscard
- tun-recv-relaccbearrespaccept
- tun-recv-relaccbearrespdenied

The following bulkstats under EGTPC schema track Downlink Data Notification (DDN) Ack and failure messages between the S-GW and the SGSN when either direct tunnel or ISR is active:

- tun-recv-dlinknotif
- tun-recv-dlinknotifDiscard
- tun-recv-dlinknotifNorsp
- tun-recv-retransdlinknotif
- tun-sent-dlinknotifackaccept
- tun-sent-dlinknotifackdenied
- tun-sent-dlinkdatafail

For complete descriptions of these variables, see the EGTPC Schema Statistics chapter in the *Statistics and Counters Reference*.



CHAPTER 18

EC-GSM Support on the SGSN

This feature describes the Extended Coverage class support on the SGSN in the following sections:

- Feature Description, on page 263
- How It Works, on page 264
- Standards Compliance, on page 264
- Limitations and Restrictions, on page 265
- Configuring EC-GSM on the SGSN, on page 265
- Monitoring and Troublshooting EC-GSM on the SGSN, on page 265

Feature Description

In the EC-GSM feature, the Base Service Station (BSS) allocates special physical resources needed for extended channels to reach a Mobile Station (MS) based on a given location. Coverage classes are defined for identifying the optimal level of repetitions to the reach the MS. This coverage class value is used by the BSS to reach the MS with optimal use of resources.

With this feature, the coverage extension frequency of 20 dB, which is beyond GSM coverage, can be achieved. This indicates a seven-fold improvement in the low-rate application range. The extended coverage frequency provides the ability to reach challenging locations – deep indoors, basements, remote areas where smart meters and sensors are deployed for monitoring purposes.

EC-GSM multiplexes with existing legacy GPRS and Extended GPRS (EGPRS) traffic channels that leads in easy deployment of EC-GSM in the existing EGPRS network with a minimal impact.

EC-EGPRS is an evolution of EGPRS providing a streamlined protocol implementation, reducing device complexity while supporting energy efficient operation with extended coverage compared to GPRS/EGPRS operation. EC-GPRS is also referred as EC-GSM. EC-GPRS aims to adapt and leverage existing 2G infrastructure to provide efficient and reliable IoT connectivity over an extended GSM Coverage to enable fast time to market.

A valid license key is required to enable the Extended Coverage Class feature. Contact your Cisco Account or Support Representative for information on how to obtain a license.

How It Works

An EC-GPRS abled MS supports extended coverage where one or more blind physical layer transmissions are used for both Uplink and Downlink. For more information, refer to the 3GPP TS 45.002 specifications information.

EC-GPRS MSs operate in four different coverage classes where each class is approximated with a level of extended coverage compared to GPRS/EGPRS operation denoted as CC1, CC2, CC3 and CC4 respectively.

In Idle-mode, the MS performs a coverage class selection and communicates the selected class to the network. In Packet transfer mode, the network performs the coverage selection and communicates the coverage class to the MS. For Paging, the MS communicates the coverage class to the network when required. For more details on selection procedures, refer to 3GPP TS 45.008 [15] and 3GPP TS 44.018 [6] specifications document.

The MS reports the extended coverage class during system access to the BSS, and the BSS relays the uplink and downlink coverage class of the MS in the UL-UNIDATA BSSGP message. The SGSN stores the coverage class information for the MS and relays it back in all the DL-UNITDATA BSSGP messages towards the MS.

Also, SGSN provides downlink coverage class of the MS in Perform Location Requests, and the MS Radio Access capability with the LCS feature enabled.

Coverage Class

Coverage class IEI consist of two-bit field tokens namely Uplink coverage class and Downlink coverage class. BSS communicates the class in the UL-UNITDATA BSSGP message to the SGSN.

The SGSN stores this IEI and relays it back in the DL-UNITDATA BSSGP message. Also SGSN provides the downlink coverage class of the MS in the Paging-PS request and the Perform Location Request (LCS).

Paging-PS

When performing a Paging-PS procedure, the SGSN include the following IEIs in support of EC-EGPRS:

- Downlink Coverage class: of the MS that was received in UL-UNITDATA previously.
- Global Cell ID: The corresponding Cell ID from where the coverage class is reported.
- MS Radio Access Capabilities.
- Paging Attempt information, which has the following two-bit field tokens:
  - Paging Attempt count: to indicate the current paging-retry request number.
  - Intended number of Paging attempts: to indicate maximum retries for paging-algorithms like cell, BSS, RA and LA.

Standards Compliance

The Extended Coverage Class for SGSN feature complies with the following standard:

- 3GPP TS 48.018 version 13.1.0, General Packet Radio Service (GPRS); Base Station System (BSS) -Serving GPRS Support Node (SGSN); BSS GPRS Protocol (BSSGP) (Release 13)

Limitations and Restrictions

The EC-GSM feature is functional only when all three nodes: SGSN, MS and BSS, are compliant with the feature requirements.

Configuring EC-GSM on the SGSN

The following CLI configuration allows SGSN to enable extended coverage support. The configuration supports:

- Handling of coverage class parameters in the BSSGP for the UL-UNITDATA and DL-UNITDATA messages.
- Paging Requests towards the BSS.
- Perform Location (LCS) request towards the BSS.

The configuration is provided under the SGSN Global Configuration mode.

```
configure
   sgsn-global
      [ no ] ec-gsm
      end
```

Notes:

- By default, this command is disabled.
- **no** disables the extended converage support in the SGSN.
- **ec-gsm** enables the extended coverage support on all gprs services.

Verifying EC-GSM for SGSN

Use the following command to verify the extended coverage class support on the SGSN:

show sgsn-mode

On executing the above command, the following new field(s) are displayed:

```
Extended Coverage Enhanced GPRS (EC-EGPRS/EC-GSM): Enabled
```

Monitoring and Troublshooting EC-GSM on the SGSN

Extended Coverage Class Support on the SGSN Show Command(s) and /or Outputs

This section provides information regarding show commands and their outputs for the Extended Coverage Class support on the SGSN feature.

show network-service-entity ip-config

The above show command provides the Network Service Entity (NSE) details, the feature supported by NSEI and the negotiated features by SGSN

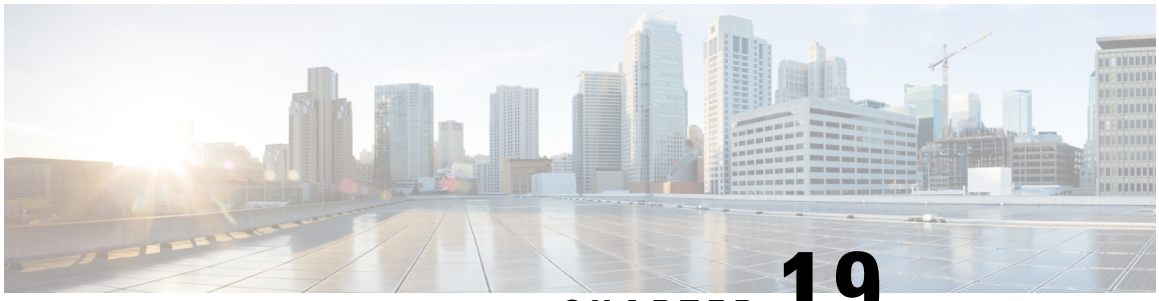
```
Peer Nse Name: - Peer Nse Id: 1
Config Type: Auto Config
Status: Unlocked
peer-nsvl: 0
port: 31000
ip-address: 192.168.71.2
data-weight: 1
sig-weight: 1
Features supported by NSEI: RIM EC-GSM
Features Negotiated by SGSN: EC-GSM
```

show-subscribers gprs-only full

The above command provides the Uplink and Downlink coverage class values for the subscriber.

On executing the above show command, the following new fields are displayed:

```
Username: 491740460103
Access Type: sgsn Network Type: IP
Access Tech: GPRS GERAN
Callid: 00004e21   Msid: 262090426000193
-----------
-----------
DRX parameter:
     Split PG Cycle Code: 7
     SPLIT on CCCH: Not supported by MS
     Non-DRX timer: max8 sec non-DRX mode after Transfer rate
     CN Specific DRX cycle length coefficient: Not Specified by MS
Uplink Coverage Class: 0
Downlink Coverage Class: 0
Negotiated Ciphering Algorithm: GEA0 (No Ciphering)
```



CHAPTER 19

Enhanced Whitelisting in SGSN

- Feature Summary and Revision History, on page 267
- Feature Description, on page 268
- How it Works, on page 268
- Configuring Enhanced Whitelisting in SGSN, on page 269

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *SGSN Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release
First introduced.	21.16

Feature Description

SGSN is enhanced to support whitelisting based on IMSI and MSISDN in LAC/RAC in addition to the HSS-based Regional Zone Code Restriction. This SGSN feature allows specific subscribers to connect to the network.

Operator policy based support is extended to support up to 10000 subscribers identies (IMSI/MSISDN) configuration. Subscribers are configured based on Routing Areas to enable subscriber whitelisting depending on its current Routing Area Identifier (RAI). A maximum of 10000 IMSI/MSISDN are allowed by LAC/RAC.

The following table lists the whitelist enhancement for SGSN.

Table 19: Whitelist Enhancement

	LAC	**RAC**
Specific IMSI	Supported	Supported from Release 21.16
Range of IMSI	Supported	Supported from Release 21.16
Group of IMSI (discrete + range)	Supported from Release 21.16	Supported from Release 21.16
Specific MSISDN	Supported from Release 21.16	Supported from Release 21.16
Range MSISDN	Supported from Release 21.16	Supported from Release 21.16
Group of MSISDN (discrete + range)	Supported from Release 21.16	Supported from Release 21.16

How it Works

Architecture

IMSI Group

The SGSN retrieves IMSI for the relevant operator policy, both by IMSI range and IMSI group. After retrieving the operator policy, the active Routing Area Identifier (RAI) with LAC/RAC information in the UE is verified against the operator policy routing-area-list by LAC/RAC combinations. If the RAI isn't available in the operator policy Routing Area List, the UE is rejected using the specific configured cause value.

The IMSI configuration supports up to 50 IMSI groups per SGSN. After creating IMSI groups, combination of IMSI and IMSI range together provide up to 500 unique IMSI values. Combination of discrete IMSI and IMSI range line are 20 per group. The IMSI group allows to configure multiple IMSIs and IMSI ranges per group to associates it to operator policy.

MSISDN Group

MSISDN group allows to configure multiple MSISDN and MSISDN ranges per group and associate the MSISDN group to an operator policy. The SGSN retrieves MSISDN for the relevant operator policy, both by MSISDN range and MSISDN group.

SGSN retrieving the operator policy, the active RAI with LAC/RAC information in the UE is verified against the operator policy routing-area-list by LAC/RAC combinations. If the RAI isn't available in the operator policy routing-area-list, the UE is rejected using the specific configured cause value.

The MSISDN configuration supports up to 50 MSISDN groups per SGSN. After creating MSISDN groups, combination of MSISDN and range together can be 500 unique MSISDN values. Combination of discrete MSISDN and range line are 20 per group.

MSIDSN Range

An MSISDN range allows associating a range of MSISDNs to an operator policy. The SGSN searches for operator policy based on the areas in which the MSISDN is retrieved (either through MAP/Diameter/GTP-C message or stored in existing UE context), both by MSISDN range and MSISDN group.

After retrieving a relevant operator policy, the SGSN verifies the active RAI which contains LAC/RAC in which the UE is in against the operator policy routing area list LAC/RAC combinations. If the active RAI is not confirmed, the UE is rejected using the specific configured cause value.

SRNS

The Gn/Gp SGSN and S4-SGSN support inter-SGSN and intra-SGSN Serving Radio Network Subsystem (SRNS) relocation. On the Gn/Gp SGSN, the SRNS relocation is triggered by subscribers (MS/UE) moving from one RNS to another. If the originating RNS and destination RNS are connected to the same SGSN but are in different routing areas, the behavior triggers an intra-SGSN Routing Area Update (RAU). If the RNSs are connected to different SGSNs, the relocation is by an inter-SGSN RAU.

Configuring Enhanced Whitelisting in SGSN

This section describes how to configure Enhanced Whitelisting in SGSN.

Configuring Discrete IMSI Numbers

Use the following configuration to configure discrete IMSI numbers.

```
configure
  imsi-group group_name
    [ no ] imsi mcc mcc mnc mnc msin msin
    end
```

NOTES:

- **mcc** *mcc*: Mobile Country Code of IMSI. *mcc* must be a three digit integer in the range of 000-999.
- **mnc** *mnc*: Mobile Network Code of IMSI. *mnc* must be a two or three digit integer in the range of 00-999.
- **msin** *msin*: 9/10 digit MSIN numbers, maximum of 500 per group.
- **no**: Disables the configured options.

Configuring IMSI Range

Use the following configuration to configure IMSI range.

```
configure
  imsi-group group_name
    [ no ] range mcc mcc mnc mnc msin first msin_first last msin_last
    end
```

NOTES:

- **range**: Range of MSIN numbers (Maximum 20 per group).
- **mcc** *mcc*: Mobile Country Code of IMSI. *mcc* must be a three digit integer in the range of 000-999.
- **mnc** *mnc*: Mobile Network Code of IMSI. *mnc* must be a two or three digit integer in the range of 00-999.
- **msin**: Mobile Subscriber International Number. Must be a maximun of 9 or 10 digit MSIN numbers. Maximum 500 per group.
- **first** *msin_first* : Start of Mobile Subscriber International Number Range. Must be a maximun of 9 or 10 digit MSIN numbers.
- **last** *msin_last*: End of Mobile Subscriber International Number Range. Must be a maximun of 9 or 10 digit MSIN numbers.
- **no**: Disables the configured options.

Configuring Discrete MSISDN Numbers

Use the following configuration to configure discrete list of MSISDN numbers.

```
configure
  msisdn-group group_name
    [ no ] msisdn cc cc number number
    end
```

NOTES:

- **msisdn** *cc*: Discrete list of MSISDN numbers (Combination of discrete and range lines is 20 per group).
- **cc** *cc*: Country Code of subscriber. Maximum 500 per group.

  cc must be three digit number between 1 to 999.
- **number** *number*: MSISDN number. Maximum 500 per group.

  number must be 1 to 14 digit number.

Associating MSISDN Range with Operator Policy

Use the following configuration to associate MSISDN range with Operator Policy.

```
configure
  sgsn-global
    msisdn-range cc cc number first start_range last last_range operator-policy
 policy_name
    no msisdn-range cc cc number first start_range last last_range
    end
```

NOTES:

- **msisdn-range** : MSISDN Range to which Operator Policy should be associated.
- **cc** *cc*: Country Code of MSISDN.

  cc must be three digit number between 1 to 999.
- **number** : Subscriber Number (and optional NDC/NPA) of MSISDN.
- **first** *start_range* : Starting range of MSISDN NDC/NPA/Subscriber Number Prefix. *start_range* must be a number up to 15 digits length.
- **last***last_range*: End range of MSISDN NDC/NPA/Subscriber Number Prefix. *last_range* must be a number up to 15 digits length.
- **operator-policy***policy_name*: MSISDN Operator Policy name.
- **no**: Disables the configured options.

Configuring MSISDN Range

Use the following configuration to configure MSISDN range of numbers .

```
configure
  msisdn-group group_name
    [ no ] range cc cc number first number_first last number_last
    end
```

NOTES:

- **range** : Range of MSISDN numbers (Combination of discrete and range lines is 20 per group).
- **cc** *cc*: Country Code of subscriber. *cc* must be a three digit number between 1 to 999.
- **number** : Specifies 1 to 14 digit. (Maximum 500 per group).
- **first** *number_first*: Starting value of MSISDN number. *number_first* must be a number from 1 to 14 digits.
- **last** *number_last*: Last value of MSISDN number. *number_last* must be a number from 1 to 14 digits.
- **no**: Disables the configured options.

Configuring Routing Area List

Use the following configuration to configure Routing Area List.

```
configure
  call-control-profile profile_name
    routing-area-list instance instance lac lac rac rac
    no routing-area-list instance instance
    end
```

NOTES:

- **routing-area-list instance** *instance*: Configure one particular instance. Instance number will be valid only if area code is configured for this instance. *instance* must be an integer in the range of 1-5.

- **lac** *lac*: Specifies the LAC value. *lac* must be an integer from 1 to 65535.
- **rac** *rac*: Specifies the RAC value. *rac* must be an integer from 0 to 255.
- **no**: Disables the configured options.

Configuring RAU-inter Restrict for SGSN

Use the following configuration to configure RAU inter-restrict for 2G and 3G.

```
configure
   call-control-profile profile_name
      [ no ] rau-inter restrict access-type { gprs routing-area-list
instance instance | umts routing-area-list instance instance  }
     end
```

NOTES:

- **rau-inter**: (SGSN) Inter SGSN Routing Area Update.
- **restrict**: Specifies restrict.
- **access-type**: Specifies the inclusion of Access Type Extension.
- **gprs**: Specifies the General Packet Radio Service
- **rau-inter**: (SGSN) Inter SGSN Routing Area Update.
- **routing-area-list** : (SGSN) RAC List to set allow/restrict of services in this routing area. Configure the area codes to define the service.
- **instance** *instance*: Configures one particular instance. *instance* must be an integer in the range of 1-5.
- **no**: Disables the configured options.

Configuring RAU-intra Allow for SGSN

Use the following configuration to configure RAU inter-allow for 2G and 3G.

```
configure
   call-control-profile profile_name
      [ no ] rau-intra allow access-type { gprs routing-area-list instance
 instance | umts routing-area-list instance instance }
     end
```

NOTES:

- **rau-intra**: (SGSN) Intra SGSN Routing Area Update.
- **allow**: Specifies allow.
- **access-type**: Specifies the inclusion of Access Type Extension.
- **gprs**: Specifies the General Packet Radio Service
- **rau-inter**: (SGSN) Inter SGSN Routing Area Update.

- **routing-area-list** : (SGSN) RAC List to set allow/restrict of services in this routing area. Configure the area codes to define the service.
- **instance** *instance*: Configures one particular instance. *instance* must be an integer in the range of 1-5.
- **no**: Disables the configured options.

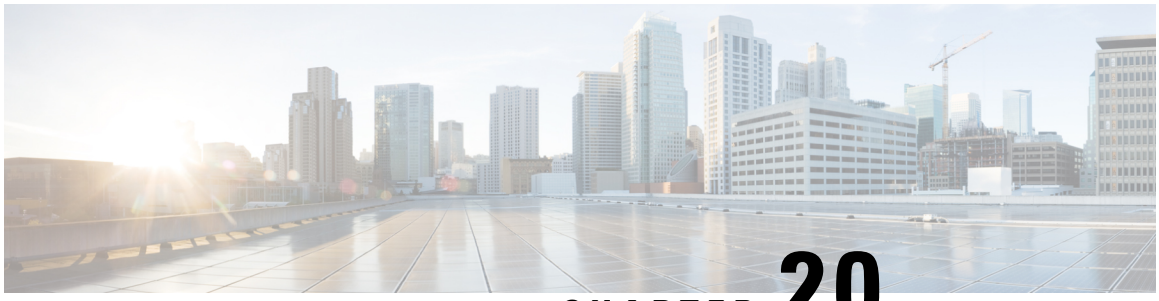
Configuring SRNS Intra

Use the following configuration to configure SRNS.

```
configure
   call-control-profile profile_name
      [ no ] srns-intra { allow location-area-list instance instance  |
restrict { all | location-area-list instance  instance}
     end
```

NOTES:

- **srns-intra**: (SGSN) SRNS Intra SGSN.
- **allow**: Specifies allow.
- **restrict**: Specifies restrict.
- **location-area-list** : (SGSN) LAC List to set allow/restrict of services in this location area. Configures the area codes to define the service.
- **instance** *instance*: Configures one particular instance. *instance* must be an integer in the range of 1-5.
- **no**: Disables the configured options.



CHAPTER 20

Exclude OPC in SCCP Calling-Party-Address on Gs Interface for Route-On-GT

- Feature Description, on page 275
- Configuring the Feature, on page 275
- Verifying the Configuration, on page 276

Feature Description

The SGSN sends Location Update Request (BSSAP+LOCATION-UPDATE-REQUEST) over the Gs interface but does not receive a Location Update Accept (BSSAP+LOCATION_AREA_UPDATE_ACCEPT) from some MSC/VLRs as the SGSN includes the Originating Point Code (OPC) in the SCCP calling-party-address IE when the routing-indicator is set to 'ROUTE on GT'. The MSC/VLRs are unable to perform GT-based routing due to the presence of OPC in the calling-party-address generated by SGSN. The OPC has to be excluded from the SGSN generated SCCP Calling Party Address towards MSC/VLR on Gs interface. The OPC is not relevant in the SCCP Calling Party Address when routing indicator is set to "Route on GT". A new CLI-based control is introduced for the operators on Gs-service to include or exclude the OPC in the SCCP calling-party-address if the routing indicator is 'Route on gt'. By default the SGSN includes the OPC in SCCP calling party address when the routing-indicator is set to 'ROUTE on GT'. The operational benefit of this feature is that the MSCs/VLRs can perform GT-based routing easily. This feature is compliant with ITU Q.714 standard.

Configuring the Feature

This section describes how the operator can choose to include or exclude OPC in the SGSN-generated SCCP calling-party-address if the routing indicator is 'Route on GT'.

```
config
   context context_name
      gs-service gs_srvc_name
          vlr vlr_name isdn-number E164_num [exclude-opc-in-sccp] {point-code
 pt_code
           | bssap+ ssn ssn [exclude-opc-in-sccp] [point-code pt_code]}
          exit
```

Notes:

- The **vlr** command is used to define the configuration of the VLR used in the GS Service. A new keyword **exclude-opc-in-sccp** is introduced in the **vlr** command under the GS Service Configuration Mode. The operator can configure this command to exclude or include OPC in the SGSN-generated SCCP calling-party-address for "route-on-gt".
- By default this keyword is not enabled and the OPC is included in the SCCP calling party address for “route-on-gt”.

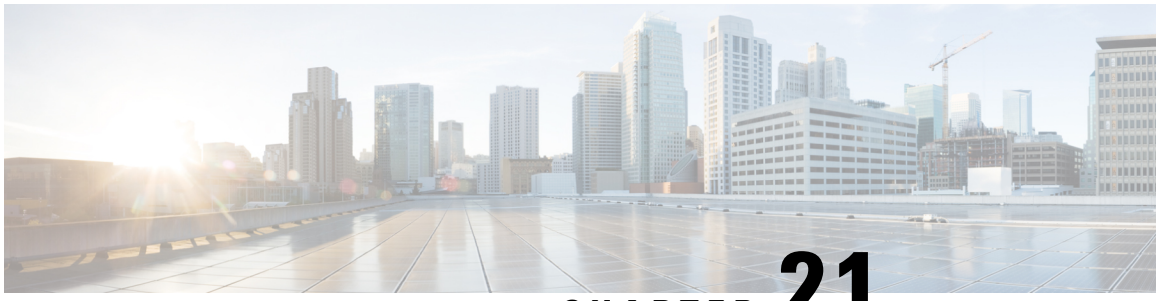
Verifying the Configuration

Execute the following command to verify the configuration of this feature.

show gs-service *service-name*

The new counter **OPC** in **SCCPCallingParty** Address is introduced which indicates if the **vlr** command is configured to either include or exclude OPC in the SCCP Calling Party Address if the routing indicator is 'Route on GT'.

- OPC in SCCPCallingParty Address: Included/Excluded



CHAPTER 21

GMM-SM Event Logging

With the introduction of this feature, the SGSN now supports limited use of event data records (EDRs). This chapters details the SGSN's event logging feature, with the use of EDRs, which is intended to facilitate subscriber-level troubleshooting. This feature is relevant for StarOS Release 12.0 (and higher) software supporting SGSN services within GPRS and UMTS networks.

This chapter provides the following information:

- Feature Description, on page 277
- Configuration, on page 283

Feature Description

Feature Overview

At any one time, the SGSN handles a large number of mobile stations (MS). In order to efficiently troubleshoot any issue for a single subscriber, it is necessary to know the events that have happened for that subscriber. Prior to this event logging feature, the SGSN did not support a debugging method that was event-based per subscriber.

The debugging framework will allow operators to troubleshoot problems related to a particular IMSI. The event logging feature will capture procedure-level information per subscriber. Upon completing a procedure, either successfully or unsuccessfully, the SGSN generates a procedure-summary or event report logging the event.

The SGSN uses the event reports to generate event data record (EDR) files comprised of logged information in comma-separated ASCII values - CSV format. The SGSN sends one ASCII formatted CSV record per line. The CSV records are stored in a file and are optionally compressed before sending to an external server. The storage space is limited, and therefore the CSV records need to be SFTed to an external server periodically. The transfer of the CSV record file from the SGSN and to the external server can be based on configurable PULL or PUSH models. In case of PUSH, the time-interval can be configured at the SGSN.

Events to be Logged

The following subscriber events will be logged:

- Attaches
- Activation of PDP Context

- Routing Area Update (RAU)
- Inter-SGSN RAU (ISRAU)
- Deactivation of PDP Context
- Detaches
- Authentications
- PDP Modifications

Event Record Fields

The EDRs include the following information in CSV format.

Important If particular information is not relevant or is unavailable for the procedure being logged, then the field is left blank.

Table 20: Event Record Fields for GMM/SM Event Logging

Field	Field Content	Field Information
1	header-field-1	Number from 1 to 512.
2	header-field-2	Number from 0 to 4294967295.
3	time	Format: YYYY-MMM-DD+HH:MM:SS
4	event-identity	Enumeration: Attach(0); Activate(1); LOCAL-RAU (2); NEW-ISRAU (3); OLD-ISRAU (4); Deactivation (5); Detach (6); Authentication (7); Modification (8).
5	result	Enumeration: Success (0); Reject (1); Aborted (2).
6	radio type	Enumeration: UTRAN (0); GERAN (1).
7	ATT type	Enumeration: GPRS-only; Comb.
8	RAU type	Enumeration: GPRS-only (0); Comb (1); Comb-IMSI-Attach(2); Periodic (3).
9	intra-RAU type	Enumeration: 2G -> 3G (-); 3G -> 2G (1); 2G -> 2G [Diff Serv] (2); 3G -> 3G [Diff Serv] (3); Local 2G (4); Local 3G (5).
10	origin-of-deactivation	Enumeration: HLR (0); GGSN (1); LOCAL (2); MS (3) .
11	cause-prot-indicator	Enumeration: GMM(0); GSM(1).

Field	Field Content	Field Information
12	gmm-cause/gsm-cause	Number between 0 and 255 to identify failure cause code. Refer to the 3GPP TS 24.008 specification, sections 10.5.5.14 (GMM cause codes) and 10.5.6.6 (SM cause codes) for an up-to-date listing.
13	disc-reason	Number 0 to 500 identifies Cisco proprietary detailed reason for session failure. To see the explanation for the SGSN-only disconnect reasons, see the *Statistics and Counters Reference*.
14	RAI	Routing area identifier in the format: ddd-ddd-xxxx-xx (d = decimal; x = hex).
15	Cell ID or SAI	One or the other, depends whether the event is generated in 3G or 2G. An integer between 0 and 65535.
16	SAC	Service area code, an integer between 0 and 65535.
17	MSISDN	Mobile subscriber's ISDN number consisting of 7 to 16 digits.
18	IMSI	Unique international mobile subscriber identity comprised of 1 to 15 digits.
19	P-TMSI	The packet-temporary mobile subscriber identity, an integer between 1 and 4294967295.
20	IMEISV	Unique 16 digit integer that indicates the IMEI with the software version to identify the equipment identity retrieval type.
21	HLR-number	16 digit integer that identifies a specific HLR.
22	APN-size	Number 1 to 128.
23	APN	Dotted alphanumeric string, typically includes the network identifier or the operator identifier to identify the access point node (APN).
24	GGSN IP/P-GW IP	Dotted string
25	Old SGSN IP	Dotted string
26	Old RAI	Routing area identifier in the format: ddd-ddd-xxxx-xx (d = decimal; x = hex)

Field	Field Content	Field Information
27	Number of PDP contexts transferred	Number from 1 to 11.
28	Number of PDP contexts dropped	Number from 1 to 11.
29	Requested QoS	Hex-digits. Refer to TS 24.008 for encoding.
30	Negotiated QoS	Hex-digits. Refer to TS 24.008 for encoding.
31	SGSN-IP-address	Dotted string
32	NSAPI	Added as part of the Activation EDR.
33	PDN-Info	Consists of nsapi, ggsn-address, ipv4-pdp-address, ipv6-pdp-address and are added as a part of the ISRAU EDR.
34	Service-Request-Trigger	Indicates the origin of the service request.
35	Service-Type	Indicates the type of service requested. The service type is classified as follows: • 0: Signalling. This Service type is triggered only from the Mobile Station. • 1: Data. This Service type is triggered only from the Mobile Station • 2: Page Response. This Service Type is triggered from either HLR, GGSN or SGSN.
36	Paging Attempts	Indicates the number of paging requests

The following table contains the availability of each field in each of the different event types:

- Type 1 - Attach
- Type 2 - Activate
- Type 3 - Local RAU
- Type 4 - New-ISRAU
- Type 5 - Old-ISRAU
- Type 6 - Deactivation
- Type 7 - Detach
- Type 8 - Authentication
- Type 9 - Modification

Table 21: Occurrence of Fields in Various Event Types

Field	Type1	Type2	Type3	Type4	Type5	Type6	Type7	Type8	Type9	Type10
SGSN-NUMBER	X	X	X	X	X	X	X	X	X	X
SEQUENCE-NO	X	X	X	X	X	X	X	X	X	X
TIME	X	X	X	X	X	X	X	X	X	X
EVENT-IDENTITY	X	X	X	X	X	X	X	X	X	X
RESULT	X	X	X	X	X	X	X	X	X	X
RAU-TYPE	X	X	X	X	X	X	X	X	X	X
ATT-TYPE	X									
RAU-TYPE			X	X						
INTRA-RAU-TYPE			X							
CHARGING-CHARACTERISTICS						X			X	
CAUSE-FOR-RECORD-CLOSING INDICATOR	C4	C5	C4	C4	C4	C5	C4	C4	C5	C4
GMM-CAUSE / GSM-CAUSE	C4	C5	C4	C4	C4	C5	C4	C4	C5	C4
DIAG-REASON	C1	C1	C1	C1	C1	C1	C1	C1	C1	C1
RAI	X	X	X	X	X	X	X	X	X	X
CELL-ID	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2
SAC	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2
MSISDN	C3	X	X	C3	X	X	C3	X	X	X
IMSI	X	X	X	X	X	X	X	X	X	X
PTMSI	C3	X	X	C3	X	X	C3	C3	X	X
IMEISV	C3	C3	C3	C3	C3	C3	C3	C3	C3	C3
HLR-NUMBER	C3	X	X	X	X	X	C3	C3	X	X
APN-SIZE		X				X			X	
APN		X				X			X	
GGSN-IP		C3		X					X	
OLD-SGSN-IP				X						

Field	Type1	Type2	Type3	Type4	Type5	Type6	Type7	Type8	Type9	Type10
OLD-RAI	X		X	X						
[illegible]				X						
[illegible]				X						
RequestedQoS		X							X	
NegotiatedQoS		X							X	
Self SGSN IP	X	X	X	X	X	X	X	X	X	
NSAPI		X								
PDN-Info			X	X	X					
[illegible]										X
Service-Type										X
Paging Attempts										X

Notes:

- C1:
  - event disc-reason will be empty for successful attach/new-rau/local-rau/activation/modification procedures.
  - disc-reason will be included for all old-rau/detach/deactivation.
  - disc-reason will be available for rejected/aborted attach/new-rau/local-rau/activation/modification procedures.
- C2: cell ID for 2G, SAC for 3G
- C3: information provided if available
- C4:
  - attach/new-rau/local/rau/detach will have reject case if an attach-reject or accept was sent with the cause value.
  - for authentication, only sync and mac failures will be logged if they are present - otherwise, the value will be left blank.
- C5:
  - cause is present only for activate-reject or modify-reject
  - deactivation will always have a cause
  - activate-accept might have a cause sent (e.g., single address bearers only allowed)

EDR Storage

The EDRs are stored in CSV format on an external server. The external server relieves the SGSN of the storage overhead and the post-processing overhead while the SGSN continues to perform call processing.

Architecture

The primary components of the feature architecture include:

- Session Manager (SessMgr) - reports events to the CDRMOD
- CDRMOD - stores EDR file in RAMDisk
- HardDisk Controller - transfers EDR files from RAMDisk to hard disk

Limitations

The reliability of event generation is limited by the CDRMOD framework, specifically:

- Any SessMgr death will result in the loss of event records that are not yet released to the CDRMOD.
- Any death of the CDRMOD proclet will result in the loss of records that are not yet written to the RAMDisk.
- Any reboot of the chassis will result in the loss of records that are not yet flushed to the hard disk or to an external server.
- In the case of overload of the CDRMOD, the SessMgr will ignore event records when its queue is full.
- The IMSI of the subscriber should be available while generating the EDR. Procedures which couldn't be associated with any particular IMSI will not generate EDRs, for example, the inter-SGSN-RAU being rejected because of its inability to contact the old-SGSN.
- GMM-SM Event Logging is not supported for 2G S4-SGSN.

Configuration

The following commands enable the SGSN to log GMM/SM events in EDR files for 3G services:

```
configure
     context ctx_name
          sgsn-service srvc_name
               [ default | no ] reporting-action event-record
```

Where:

- [default | no] - disables the logging function.

The following commands enable the SGSN to log GMM/SM events in EDR files for 2G services:

```
config
     context ctx_name
          gprs-service srvc_name
               [ default | no ] reporting-action event-record
```

Where:

- [default | no] - disables the logging function.

The following commands access the EDR module configuration mode commands to enable the operator to configure logging and file parameters and to configure file-transfer parameters.

```
config
     context ctx_name
          [ no ] edr-module active-charging-service
```

Where:

- no - disables the configured EDR logging and file parameters for the services in the context.

```
          [ default | no ] cdr [ push-interval | push-trigger |
remove-file-after-transfer | transfer-mode | use-harddisk ]
```

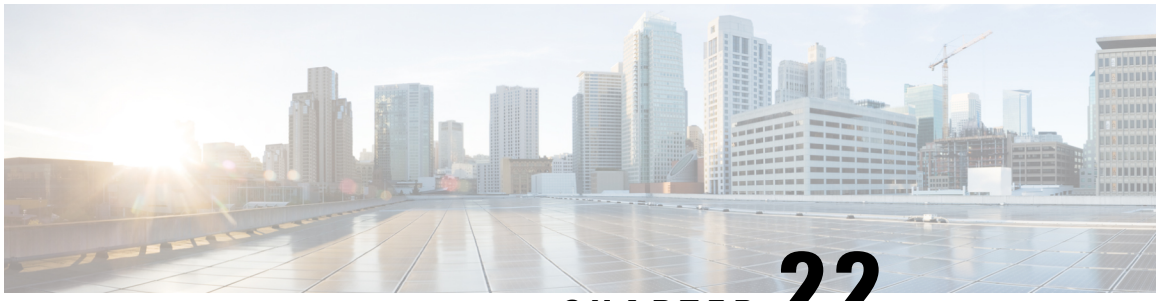
Where:

- cdr - configures the EDR transfer parameters
- default - restores default parameter values
- no - disables the configuration

```
          [ default | no ] file [ charging-service-name | compression |
current-prefix |  delete-timeout | directory | edr-format-name |
exclude-checksum-record | field-separator | file-sequence-number | headers
 | name | reset-indicator | rotation | sequence-number | storage-limit |
 time-stamp | trailing-text | trap-on-file-delete | xor-final-record
```

Where:

- file - configures file creation properties for the records
- default - restores the default file creation properties
- no - disables the configuration



CHAPTER 22

Graceful Assert Handling

This chapter describes the following topics:

- Feature Summary and Revision History, on page 285
- Feature Description, on page 285
- Configuring Graceful Assert Handling, on page 286
- Monitoring and Troubleshooting, on page 287

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	ASR 5500
Feature Default	Enabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	SGSN Administration Guide

Revision History

Revision Details	Release
First introduced.	21.5

Feature Description

The Graceful Assert Handling framework enables graceful handling of subscriber sessions for which ASSERT condition is hit during call execution. This is achieved without affecting other subscriber sessions on the same proclet.

Normally, when the ASSERT condition is hit, the Session Manager (SessMgr) proclet restarts and recovers all the subscriber sessions from the AAA Manager (AAAMgr). The recovered subscriber sessions are moved to IDLE state.

When Graceful Assert Handling is enabled, the SessMgr proclet will not be restarted. Instead, the SessMgr proclet recovers only the affected subscriber's session from the AAAMgr, and clears the existing subscriber's session on the SessMgr. The recovered subscriber sessions are moved to IDLE state. During the recovery procedure, all messages directed towards the subscriber are dropped. After recovery, the subscriber will continue to handle messages directed towards it. With this procedure, the remaining subscriber sessions on the SessMgr remain unaffected.

Configuring Graceful Assert Handling

Use the following configuration to enable or disable the Graceful Assert Handling framework. By default, this command is enabled.

```
configure
   debug controlled-assert s4sgsn
      [ disable | enable ] core-generation
      limit-per-asset asset_value
      [ no ] test file-name file_name line-number line_num [ sequence-number
seq_num ]
      end
```

Notes:

- **controlled-assert**: Configures the controlled assert framework.
- **s4sgsn**: Configures the S4-SGSN controlled assert.
- **core-generation**: Configures core generation for controlled assert. Default: Enabled.
- **limit-per-asset**: Configures the limit per assert for controlled assert. Default: 5.
- **test file-name** *file_name* **line-number** *line_num* **[sequence-number** *seq_num* **]**: Configures controlled assert test handling.
  - **file-name** *file_name*: Configures the file name where assert control is required. *file_name* must be an alphanumeric string of 1 through 254 characters.
  - **line-number** *line_num*: Configures the line number where assert control is required. *line_num* must be an integer from 1 to 4294967295.
  - **sequence-number** *seq_num*: Configures the sequence number where assert control is required. *seq_num* must be an integer from 1 to 100. Default: 1.
- **disable**: Disables the specified action for controlled assert framework.
- **enable**: Enables the specified action for controlled assert framework.
- **no**: Removes the specified test configuration related to controlled assert framework.

Monitoring and Troubleshooting

This section provides information on the show commands available to support Graceful Assert Handling.

Show Commands and/or Outputs

This section provides information regarding show commands and/or their outputs in support of the Graceful Assert Handling feature.

show session subsystem facility sessmgr instance <instance_num> debug-info verbose

This command displays statistics related to the Graceful Assert Handling framework. The following statistics in the sample output displays the number of times a particular ASSERT condition is hit along with file name, line number, and the last observed time.

Controlled Assert Stats:

Module Name: S4_SGSN

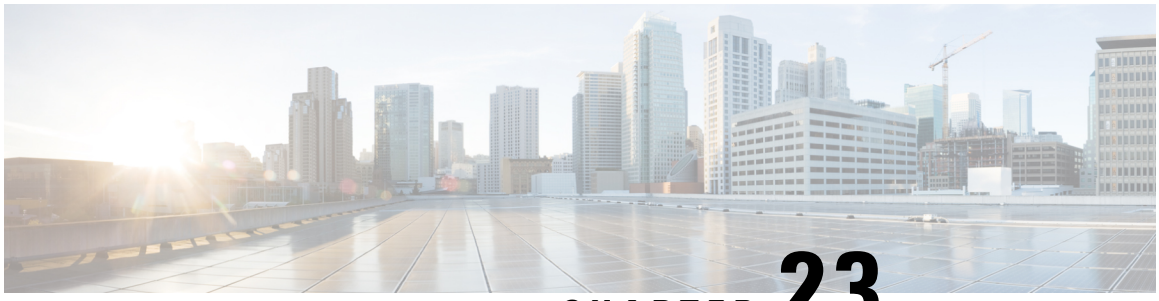
Asset Count: 3

Count File: Line Last Assert hit time (in sec)

1 sess/sgsn/sgsn-app/sm/sma_activate_fsm.c:1357 2017/09/26 07:20:53 EDT

2 sess/sgsn/sgsn-app/sm/smg_fsm_table.c:7859 2017/09/26 07:20:53 EDT

show session subsystem facility sessmgr instance <instance_num> debug-info verbose



CHAPTER 23

GTPU Error Indication Enhancement

- Feature Description, on page 289

Feature Description

This enhancement provides a solution to avoid GTPU Path Failure when a burst of GTPU Error Indication occurs. This enhancement is applicable only for SGSN.

Consider the following scenario:

1. Following a kernel crash and Hardware Failure (Fabric corruption) in a Demux Card, the SGSN is unable to respond Echo Requests from the GGSN. This results in Path Failure detection by the GGSN and a large number of sessions are cleaned up.
2. But the sessions are still active at the SGSN in PSC3 Cards where Session Manager is running. The SGSN sends uplink data for these sessions and this triggers a flood of GTPU Error Indications (~6 to ~9 million) from the GGSN to SGSN.
3. Simultaneously a Demux card migration is triggered in the SGSN to recover from the kernel crash and Hardware Failure. After the migration is completed, the SGSN restarts the Path Management Echo Requests. But the GGSN had already started sending Echo requests as soon as the new sessions were set up at the GGSN. This difference in the restarting of the Echo requests from both ends on the path leads to delay in detecting path failure between the SGSN and GGSN if echo responses are not received for any reason.
4. Once the Demux card has recovered at SGSN, the following are observed:
   - A flood of GTPU Error Indication messages further result in packet drops at the SGSN
   - The Echo Request causing another path failure at the GGSN
   - Echo Response cause a path failure on the SGSN with delay as well as loss of GTPU Error Indications at SGSN
5. This delay in Path Failure results in another flood of GTPU Error Indications in response to SGSN uplink data for the active sessions, which were already cleaned up at the GGSN (those created after first path failure). This flood of GTPU Error Indications results in additional packet drops at the SGSN. The cycle of cleaning up sessions and setting up new sessions continues until the SGSN is restarted.

The issue is resolved by creating an additional midplane socket for GTPU Error Indications so that flood of GTPU Error Indication will not create any impact on Path Management. New midplane socket and flows have been introduced to avoid path management failure due to flood of GTPU Error Indication packets. GTPU Echo Request/Response will continue to be received at existing midplane sockets. A new path for GTPU

Error Indication will prevent issues in Path Management towards GGSN or towards RNC and avoids un-wanted detection of path failures. This enhancement requires new flows to be installed at the NPU.

The following existing statistics are helpful in observing loss of packets and drop of GTPU Error Indication Packets:

show sgtpu statistics

Total Error Ind Rcvd: 0

Rcvd from GGSN: 0

Rcvd from RNC: 0

Rcvd from GGSN through RNC: 0

Rcvd from RNC through GGSN: 0

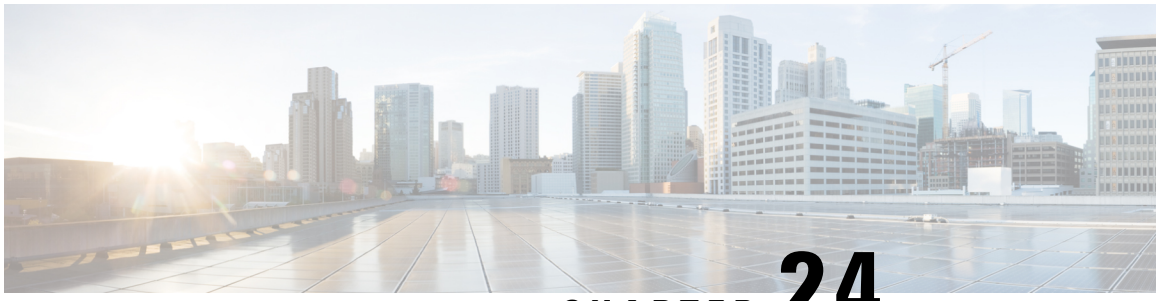
The following show commands are useful to verify the NPU related statistics:

- To check the flow id range associated with sgtpcmgr, use the following command:

  For ASR 5500: **show npumgr flow range summary**

- To check whether flow corresponding to GTPU Error Indication is installed or not, use the following command:

  For ASR 5500: **show npumgr flow statistics**



CHAPTER 24

Identity Procedure on Authentication Failure

- Feature Description, on page 291
- How It Works, on page 292
- Configuring Performance of Identity Procedure, on page 293
- Monitoring and Troubleshooting the Performance of Identity Procedure for Authentication Failure, on page 294

Feature Description

Performing Identity Procedure in response to authentication failures results in fewer subscribers losing network connectivity due to Authentication Rejects. In the network, authentication rejects due to authentication failures such as Sync failure, GSM authentication unacceptable, and MAC failure, cause loss of network connectivity to subscribers. Often uthentication failure is due to incorrectly sent authentication vectors, which could be due to a P-TMSI (Packet Temporary Mobile Subscriber Identity) collision in the network.

Authentication Failures

GSM Authentication Unacceptable

When a 3G MS/UE attaches and sends a RAU Request with P-TMSI identity, this means that this subscriber:

- was registered in the SGSN,
- received this P-TMSI identity from the SGSN,
- left the SGSN, and
- has returned to this SGSN.
- And in the time between leaving and returning, another subscriber, a 2G subscriber, has registered with this SGSN and has the same P-TMSI.

The SGSN tries to authenticate the returning 3G subscriber with the authentication vectors of the 2G subscriber. This causes the MS/UE to send authentication failure with cause "GSM authentication unacceptable" because the SGSN has sent RAND from the 2G subscriber when the 3G subscriber's MS/UE was expecting quintets.

MAC Failure

When a 2G MS sends a RAU Request (new SGSN RAU) with a P-TMSI identity, the SGSN tries to authenticate the new 2G subscriber with the authentication vectors of a different 2G subscriber. In this scenario, it appears as if IMSI-PTMSI collision occurs within the SGSN or it is due to the peer-SGSN sending vectors of another

subscriber or an incorrect IMSI in the Context Response. This results in authentication failure with cause "MAC failure".

Identity Procedure

In most cases, these forms of authentication failure can be resolved by the subscriber restarting their device - if the subscriber knows to try this.

MAC Failure

The SGSN supports performing an Identity Procedure on receiving MAC Failure in 3G and on MAC Failure during 2G Attach.

Beginning with release 19.2, the SGSN also supports performing Identity Procedure on MAC Failure in 2G New-ISRAU.

If the SGSN gets MAC failure for the first time from an MS/UE, the SGSN sends an SGSN-Context-ACK Failure message to the peer-SGSN and starts an Identity Procedure.

1. Once the SGSN receives the IMSI from the MS/UE in an Identity Response, if the IMSI is different from the IMSI received from the peer-SGSN then the SGSN will authenticate by fetching vectors from the HLR.
2. Next the SGSN tries to get the context from the peer-SGSN by initiating a new Context Request, including the IMSI obtained from the MS/UE, and the MS/UE validated flag is set.
3. The SGSN proceeds with the call.

If the IMSI is not found in the peer-SGSN, the SGSN sends RAU Reject with cause "MS Identity Cannot Be Derived by the Network". In accordance with the 3GPP specification, the MS/UE tries to register again using its IMSI.

GSM Authentication Unacceptable

Beginning with Release 19.2, the SGSN performs Identity Procedure on receiving GSM Authentication Unacceptable failure for 3G Attach, for 3G New-ISRAU, for 3G Intra-RAU, and for Inter-RAT.

If the SGSN gets the correct IMSI in the Identity Response, then the SGSN will try to authenticate the MS/UE again using the vectors from the HLR. If the authentication fails again, the SGSN send Authentication Reject to the MS/UE.

How It Works

3GPP specification TS 24.008, section 4.3.2.6 (c) suggest that "Upon the first receipt of an AUTHENTICATION FAILURE message from the MS with reject cause "MAC failure" or "GSM authentication unacceptable", the network may initiate the identification procedure. This is to allow the network to obtain the IMSI from the MS. When the SGSN receives authentication failure message with cause as GSM authentication unacceptable or MAC failure from a 3G/2G subscriber respectively, it will start identity procedure and authenticate the subscriber with vectors fetched using IMSI. This will avoid network loss to subscribers due to such PTMSI collision cases.

With Release 19.2, the SGSN performs Identity Procedure in accordance with 3GPP recommendations, as detailed below.

GSM Authentication Unacceptable

Scenarios:

- 3G Attach Request from a UE with P-TMSI (with the same P-TMSI the SGSN gave to a 2G subscriber now registered in the SGSN)
- 3G New-ISRAU with a P-TMSI

In the above scenarios, if authentication fails due to cause "GSM authentication unacceptable", then the SGSN performs the identity procedure and authenticates using vectors from the HLR.

In the case of a 3G Intra-RAU or Inter-RAT, if the arriving MS/UE is a different subscriber than the already registered one, then the SGSN rejects the RAU with cause "MS Identity Cannot be Derived by the Network", so the UE will use the IMSI at the next Attach.

MAC Failure in 2G

The SGSN will perform identity procedure if MAC failure is received for any of the following scenario:

- 2G Atach Request from a UE with P-TMSI (with a P-TMSI given to a different 2G subscriber now registered in the SGSN).
- 2G New-ISRAU with a P-TMSI

Configuring Performance of Identity Procedure

The default behavior of the SGSN is to perform identity procedure when authentication failures occur. The configuration noted below, allows the operator to disable or to re-enable the SGSN's default behavior.

With Release 19.2, the default behavior has been extended to enable the SGSN to initiate the identity procedure on receiving authentication failures with either cause "MAC Failure" or cause "GSM Authentication Failure".

The following command sequence configures the SGSN so that performance of the identity procedure upon receipt of an authentication failure is disabled:

```
config
  context context_name
    sgsn-service sgsn_srvc_name
      no gmm perform-identity-on-auth-failure
      end
```

Notes:

- If the default behavior has been disabled with the command sequence noted above, then to re-enable performance of the identity procedure upon receipt of an authentication failure, re-enter the sequence but do not include the **no** prefix with the **gmm perform-identity-on-auth-failure**command.

Verifying the Configuration

To determine the current configuration for this feature, issue the following command sequence in the Exec mode.

```
show sgsn-service name sgsn_srvc_name
```

The output generated by this command will include the following information field with either a 'Disabled' or 'Enabled' value :

```
GMM-Perform-Identity-After-Auth  :  Disabled
```

Monitoring and Troubleshooting the Performance of Identity Procedure for Authentication Failure

show gmm-sm statistics verbose

Statistics are available which track of the number of IMSI Identity Requests triggered in response to authentication failures noted in this chapter.

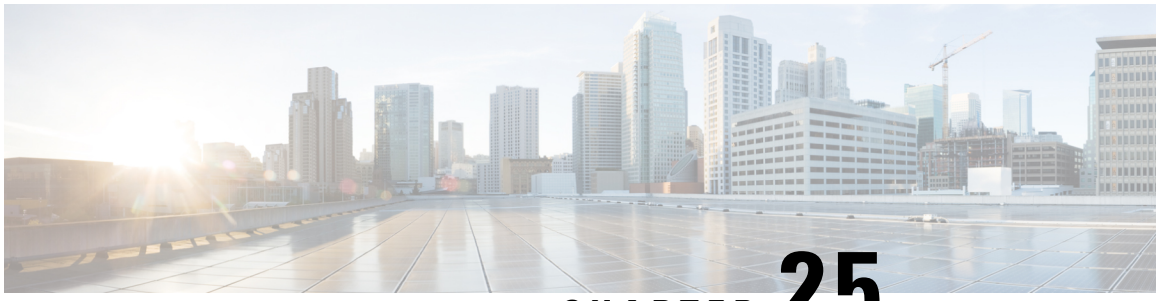
The **show gmm-sm statistics verbose** command from the Exec mode will generate an output that includes the following:

```
IMSI-Identity-Req triggered due to auth failures:
  3G-GSM Auth Unacc:       0           2G-MAC failure:      0
  3G-MAC failure:          0
```

show gmm-sm statistics

The number of IMSI identity requests initiated by the SGSN are captured in the following counter:

```
Total-IMSI-Identity-Req
```



CHAPTER 25

Idle Mode Signaling Reduction on the S4-SGSN

This chapter describes the Idle Mode Signaling Reduction (ISR) feature and its implementation and use on the S4-SGSN.

Important A separate feature license is required to enable the ISR feature. Contact your Cisco representative for licensing information.

- Feature Description, on page 295
- How ISR Works, on page 296
- Configuring Idle-Mode-Signaling Reduction, on page 301
- Monitoring and Troubleshooting the ISR Feature, on page 303

Feature Description

The Idle mode signaling reduction (ISR) feature on the S4-SGSN provides a mechanism to optimize and/or reduce signaling load during inter-RAT cell-reselection in idle mode (that is, in the ECM-IDLE, PMM-IDLE, and GPRS-STANDBY states). It is a mechanism that allows the UE to remain simultaneously registered in a UTRAN/GERAN Routing Area (RA) and an E-UTRAN Tracking Area (TA) list. This allows the UE to make cell reselections between E-UTRAN and UTRAN/GERAN without having to send any TAU or RAU requests, as long as the UE remains within the registered RA and TA list.

ISR is a feature that reduces the mobility signalling and improves the battery life of UEs. ISR also reduces the unnecessary signalling with the core network nodes and air interface. This is important especially in initial deployments when E-UTRAN coverage will be limited and inter-RAT changes will be frequent.

The benefit of the ISR functionality comes at the cost of more complex paging procedures for UEs, which must be paged on both the registered RA and all registered TAs. The HSS also must maintain two PS registrations (one from the MME and another from the SGSN).

Important The Gn/Gp SGSN does not support ISR functionality.

Relationships

The ISR feature on the S4-SGSN is related to:

- ISR must be enabled on the peer MME and SGW nodes.
- The SGSN must be configured with the following:
  - 2G Service + S4 Support
  - 3G Service + S4 Support
  - 2G + 3G Services + S4 Support

Important If the S4-SGSN is configured to support both 3G and 2G services, it is recommended to enable both 2G and 3G ISR functionality. This ensures that for the ISR activated subscribers, inter-RAT routing area updates between 2G and 3G preserve the ISR status if there is no SGW relocation.

How ISR Works

ISR requires special functionality in both the UE and the network (i.e. in the SGSN, MME, SGW and HSS) to activate ISR for a UE. The network can decide for ISR activation individually for each UE. ISR support is mandatory for E-UTRAN UEs that support GERAN and/or UTRAN and optional for the network. Note that the Gn/Gp SGSN does not support ISR functionality.

ISR is not activated on Attach. ISR can only be activated when a UE first registers in a RA on an SGSN and then registers in a TA on an MME or vice-versa. It is an inherent functionality of the mobility management (MM) procedures to enable ISR activation only when the UE is able to register via E-UTRAN and via GERAN/UTRAN. For example, when there is no E-UTRAN coverage there will be also no ISR activation. Once ISR is activated it remains active until one of the criteria for deactivation in the UE occurs, or until the SGSN or the MME indicate ISR is no longer activated during an update procedure, i.e. the ISR status of the UE has to be refreshed with every update.

When ISR is activated this means the UE is registered with both the MME and the SGSN. Both the SGSN and the MME have a control connection with the SGW. The MME and the SGSN are both registered at the HSS. The UE stores mobility management parameters from the SGSN (for example, P-TMSI and RA) and from the MME (for example, GUTI and TAs). The UE stores session management (bearer) contexts that are common for E-UTRAN and GERAN/UTRAN accesses. In an idle state the UE can reselect between E-UTRAN and GERAN/UTRAN (within the registered RA and TAs) without any need to perform TAU or RAU procedures with the network. the SGSN and MME store each other's address when ISR is activated.

The S4 SGSN supports the following scenarios for 2G ISR:

- ISR activation by SGSN on new SGSN RAU from MME
- ISR activation on SGSN in old SGSN RAU to MME
- Ready to standby state transition triggered Release Access Bearer Request to SGW
- Downlink data notification from SGW:
  - Downlink data notification UE responds to SGSN
  - Downlink data notification no response from UE
- Stop paging indication
- UE initiated detach for ISR activated subscriber under GERAN

- UE initiated detach under EUTRAN/MME initiated detach or Detach notification from MME
- SGSN initiated detach for ISR activated subscriber
- HSS/HLR initiated detach for ISR activated subscriber
- ISR deactivation due to delete bearer request with ISR deactivation cause
- ISR deactivation due to last PDN connection deletion (SGSN/UE/PGW/HSS/HLR-initiated)
- ISR deactivation due to SGW change
- ISR-deactivation due to context transfer between same Node types(S4 SGSN to and from S4 SGSN)
- Intra-RAU without SGW change for ISR-activated subscriber
- Inter-GPRS service RAU without SGW change for ISR-activated subscriber
- Intra-SGSN inter-system handover from 2G to 3G without SGW change for ISR activated subscriber
- Intra-SGSN inter-system handover from 3G to 2G without SGW change for ISR activated subscriber

The following scenarios are supported for 3G ISR:

- ISR activation by 3G SGSN on new 3G SGSN RAU from MME
- ISR activation by 3G SGSN on old 3G SGSN RAU to MME
- ISR activation by 3G SGSN on new 3G SGSN SRNS relocation from MME (Connected mode IRAT handover from MME to SGSN)
- ISR activation by 3G SGSN on old 3G SGSN SRNS relocation to MME (Connected mode IRAT handover from SGSN to MME)
- Iu release triggered Release Access Bearer Request to SGW
- Downlink data notification from SGW:
  - Downlink data notification UE responds to SGSN
  - Downlink data notification no response from UE
- Stop paging indication
- UE initiated detach for ISR activated subscriber under UTRAN
- UE initiated detach under EUTRAN/MME initiated detach or Detach notification from MME
- SGSN initiated detach for ISR activated subscriber
- HSS/HLR initiated detach for ISR activated subscriber
- ISR deactivation due to delete bearer request with ISR deactivation cause
- ISR deactivation due to last PDN connection deletion (SGSN/UE/PGW/HSS/HLR-initiated)
- ISR deactivation due to SGW change
- ISR-deactivation due to context transfer between same Node types (S4 SGSN to and from S4 SGSN)
- Intra-RAU without SGW change for ISR-activated subscriber
- Intra-SRNS without SGW change for ISR activated subscriber

Limitations

There are no known limitations to the 2G ISR feature.

For the 3G SGSN, if an ISR is already active between the SGSN and an MME and the system receives a relocation required towards an eNodeB served by the same ISR associated with the MME, the S4-SGSN first tears down the existing S3 tunnel and will initiate a forward relocation request on a new tunnel. If the procedure completes successfully, ISR association would be continued on the new tunnel. However, if the relocation is cancelled then the tunnel is lost and the ISR is deactivated.

Call Flows

This section provides various call flows that illustrate the primary procedures used for the ISR feature:

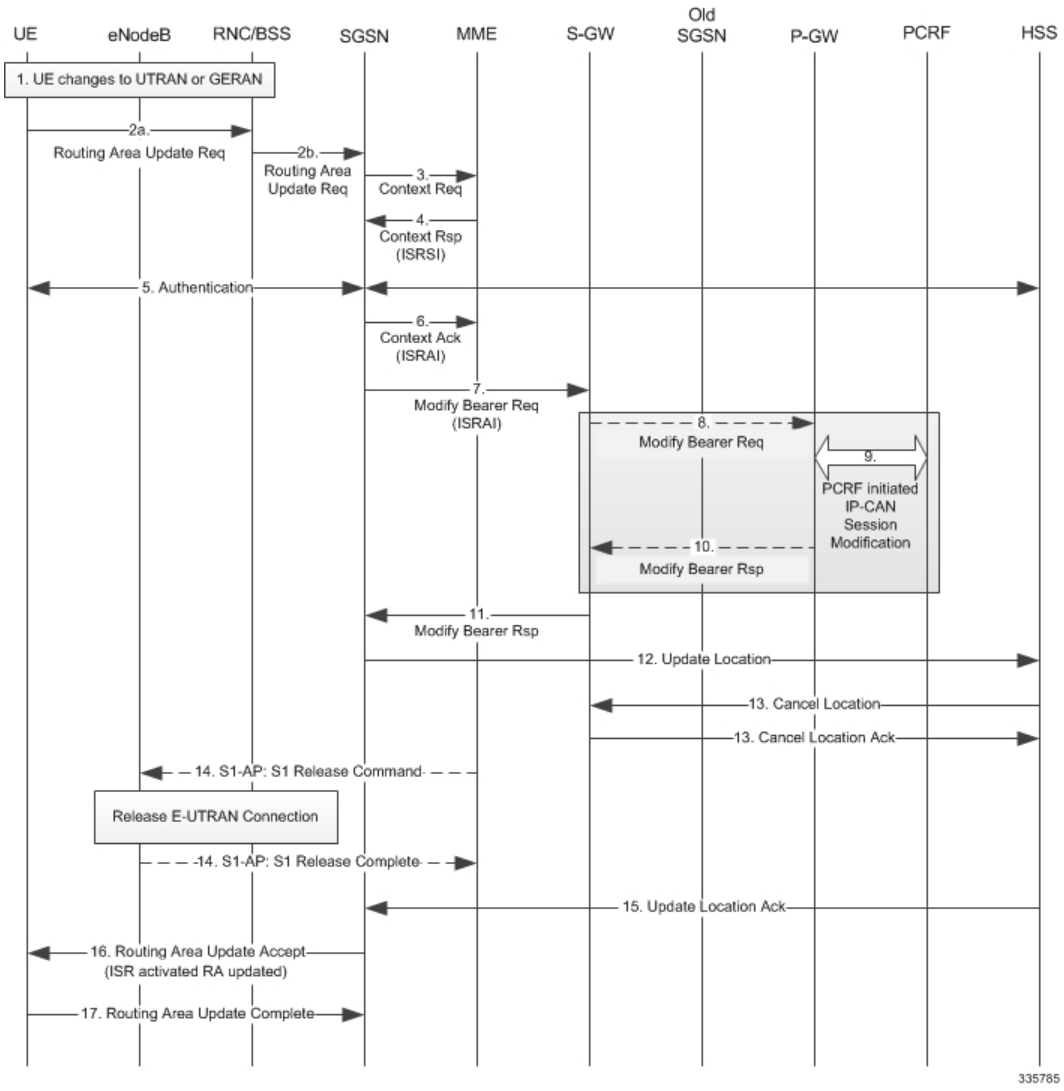
2G ISR Activation by the S4-SGSN

The following illustration shows the ISR activation procedure when initiated by the S4-SGSN for a 2G subscriber.

Note the following major procedural functions:

- E-URTRAN attach at the MME.
- A Routing Area Update is sent to the SGSN.
- The SGSN sends a Context Request to the MME upon receiving the RAU Request. If the MME supports ISR, it will set the ISRSI bit in the Context Response message.
- Upon receiving the Context Response from the MME, the GMM sets the ISRAI flag if ISR is already activated for the subscriber or if all of following conditions are satisfied:
  - The UE is EPC-capable.
  - ISR is enabled in the configuration.
  - The peer node is the MME.
  - The peer node has indicated that ISR is supported in the Context Response message.
- The SGSN will not activate ISR if there is change in SGW. So, the SGSN will be setting the 'ISRAI' bit in the Modify Bearer Request/Context Ack message provided there is no change in SGW and all of above conditions in the previous bullet point are satisfied.
- If the SGSN also monitors the *SGSN-MME-Separated* flag in the Update location Response or the *Separation Indicator* in Update Location Ack - ULA Flags IE to activate ISR for subscriber and ISR status is marked deactivated if not indicated by HLR/HSS.
- The SGSN sends a RAU accept with update type *RA updated and ISR activated* or *combined RA/LA updated and ISR activated* depending on the update request.
- The SGSN sends a Periodic RAU timer to the UE in a RAU accept message and also a GERAN/UTRAN Deactivate ISR timer (T3323) timer value to the UE. Parallel to the periodic RAU timer, the SGSN starts its mobile reachability timer (MNR timer) which is configurable. The default is 4 minutes greater than the periodic RAU timer. The UE is expected to contact the SGSN again within the mobile reachability timer duration either by sending a periodic RAU or some other signalling. If the UE fails to contact the SGSN during this timer, SGSN will start the implicit detach timer which by default is 4 minutes greater than T3323 timer. The implicit detach timer value is also configurable at the SGSN. If the UE fails to contact even within this implicit detach timer, then the SGSN will locally detach the UE and will send a Detach Notification with cause *Local detach* to the MME so that ISR gets deactivated at the MME.

Figure 48: ISR Activation on the S4-SGSN



2G ISR Activation by the MME

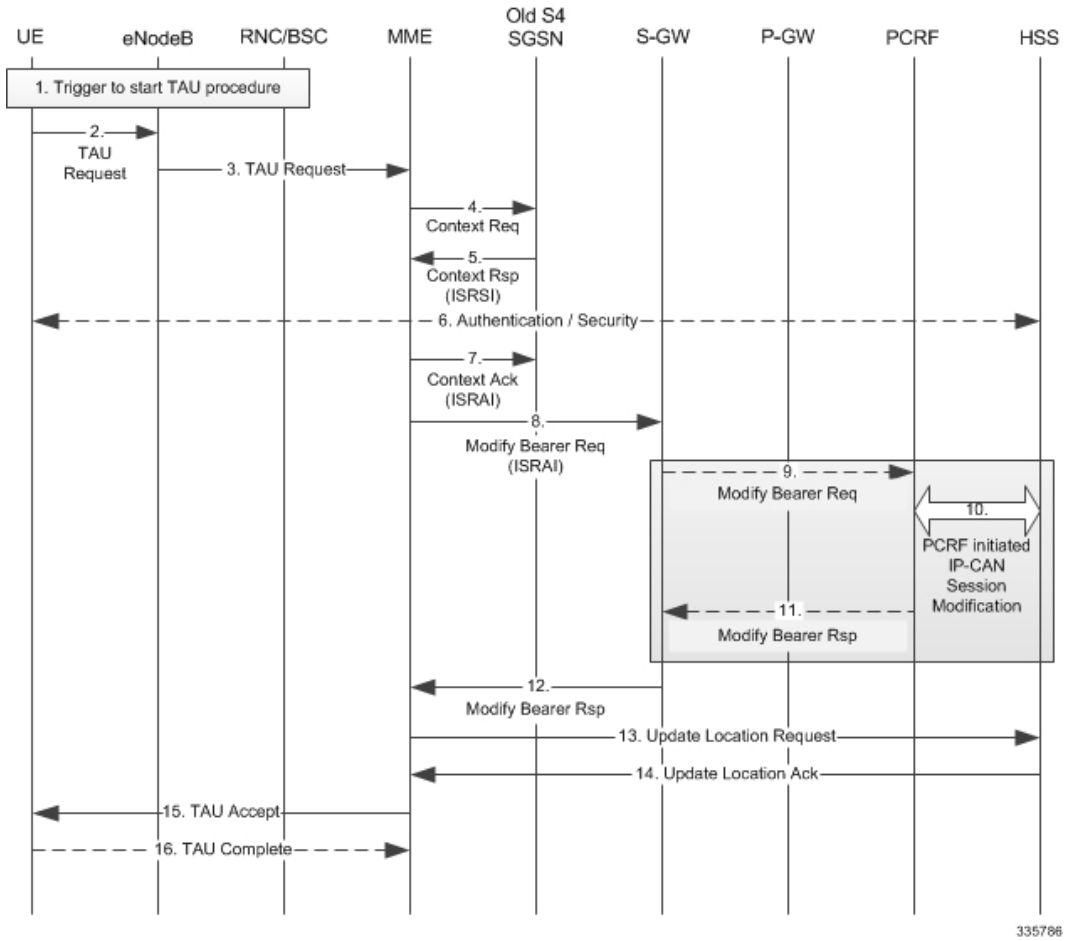
The following illustration shows the ISR activation procedure when initiated by the MME for a 2G subscriber.

Note the following major procedural functions:

- Context request from MME.
- The SGSN sends a Context Response to the MME with the 'ISRSI' bit set provided all of following conditions are satisfied:
  - The UE is EPC-capable.
  - The UE is ISR-capable.
  - The ISR is enabled by configuration.
  - The peer node is an MME.

- If the old node is an old S4-SGSN, the MME sends a Context Acknowledge (ISR Activated) message to the old SGSN.
- Unless ISR Activated is indicated by the MME, the old S4-SGSN marks in its context that the information in the Gateways is invalid. This ensures that the old S4-SGSN updates the Gateways if the UE initiates a RAU procedure back to the old S4-SGSN before completing the ongoing TAU procedure. If ISR Activated is indicated to the old S4-SGSN, this indicates that the old S4-SGSN shall maintain its UE context including authentication quintets and stop the inter-SGSN handover procedure guard timer (2G).When the UE is initially attached, the SGSN started the Mobile Reachability Timer (MNR timer). This timer value is slightly larger than the Periodic RAU Timer value given to the UE by SGSN. The default is 4 minutes longer. The UE is expected to contact SGSN through a periodic RAU or some other signalling message within this timer. If the UE did not contact SGSN within this timer, the S4-SGSN shall start the implicit detach timer with a slightly larger value than the UE's GERAN/UTRAN Deactivate ISR timer (T3323). The implicit detach timer value is also configurable at the SGSN. If the UE fails to contact even within this implicit detach timer, then the SGSN will locally detach the UE and will send a Detach Notification with cause *Local detach* to the MME so that ISR is deactivated at the MME.
- When ISR Activated is not indicated and an inter-SGSN handover procedure guard timer expires, the old SGSN deletes all bearer resources of that UE. As the Context Acknowledge from the MME does not include any S-GW change, the S4 SGSN does not send any Delete Session Request message to the S-GW.

Figure 49: 2G ISR Activation by the MME



Standards Compliance

The 2G ISR feature complies with the following standards:

- **TS 23.060 version 10**: *3rd Generation Partnership Project Technical Specification Group Services and System Aspects General Packet Radio Service (GPRS) Service description Stage 2*.
- **TS 23.401 version 10**: *3rd Generation Partnership Project Technical Specification Group Services and System Aspects General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access.*
- **TS 23.272 version 10**: *Universal Mobile Telecommunications System (UMTS) LTE 3GPP Evolved Packet System (EPS) Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C) Stage 3*.
- **TS 29.274 version 10**: *Universal Mobile Telecommunications System (UMTS) LTE 3GPP Evolved Packet System (EPS) Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C) Stage 3*.

Configuring Idle-Mode-Signaling Reduction

This section describes how to configure ISR on the S4-SGSN.

Configuring 2G ISR

Configuring 2G ISR includes creating a call-control-profile with ISR enabled for GPRS, and configuring an implicit-detach-timeout in the configured GPRS service on the S4-SGSN.

```
config
 call-control-profile name
 idle-mode-signaling-reduction access-type gprs
 end
config
      context plmn_name
 gprs-service gprs_service_name
                  gmm implicit-detach-timeout value
                  end
```

Notes:

- Where **call-control-profile** *name* specifies the name of the call-control-profile tin which 2G ISR functionality is to be configured.
- **gprs** enables 2G ISR functionality.
- Alternatively, **remove idle-mode-signaling-reduction access-type gprs** can be used to disable 2G ISR functionality.
- **context** *plmn_name* is the name of the public land mobile network context in which the GPRS (2G) service is configured.
- **gprs-service** *gprs_service_name* specifies the name of the configured GPRS (2G) service for which you want to configure the implicit-detach-timeout value.
- **gmm implicit-detach-timeout** *value* specifies the implicit detach timeout value to use for 2G ISR. Valid entries are from 240 to 86400 seconds. The default value is 3600 seconds.

Verifying the 2G ISR Configuration

This section describes how to verify the 2G ISR configuration.

To verify that 2G ISR and the gmm implicit-detach-timeout is configured:

```
show configuration
...
      call-control-profile name
 idle-mode-signaling-reduction access-type gprs
....
      context context_name
            gmm T3323-timeout value
 gmm implicit-detach-timeout value
```

To verify that 2G ISR is enabled in the call-control-profile:

```
show call-control-profile full name cc-profile-name
...
Treat as PLMN
 :Disabled
Idle-Mode-Signaling-Reduction (ISR) for UMTS               :Disabled
Idle-Mode-Signaling-Reduction (ISR) for GPRS                    :Enabled
Location Reporting for UMTS                                      :Disabled
...
```

Configuring 3G ISR

Configuring 3G ISR includes creating a call-control-profile with ISR enabled for UMTS, and configuring an implicit-detach-timeout in the configured SGSN service on the S4-SGSN.

```
config
 call-control-profile cc-profile-name
 idle-mode-signaling-reduction access-type umts
 end
config
 context context_name
 sgsn-service sgsn_service_name
 gmm T3323-timeout mins
 end
```

Notes:

- **idle-mode-signaling-reduction access-type umts** enables 3G ISR in the call-control-profile.
- **gmm t3323-timeout** *mins* specifies the amount of time, in minutes, the UE should wait after the Periodic RAU timer (t3312 timer) expiry before deactivating ISR. Valid entries are from 1 to 186. The default is 54.

Verifying the 3G ISR Configuration

This section describes how to verify the 3G ISR configuration.

To verify that 3G ISR is enabled and the gmm T3323 timeout is configured:

```
show configuration
...
      call-control-profile name
 idle-mode-signaling-reduction access-type umts
....
```

```
      context context_name
 gmm T3323-timeout value
...
```

To verify that 3G ISR is enabled in the call-control-profile:

```
show call-control-profile full name cc-profile-name
...
Treat as PLMN
 :Disabled
Idle-Mode_Signaling-Reduction (ISR) for UMTS                    :Enabled
...
```

Monitoring and Troubleshooting the ISR Feature

This section provides information on how to monitor the ISR feature and to determine that it is working correctly.

ISR Show Command(s) and Outputs

This section provides information regarding show commands and/or their outputs in support of the ISR feature.

show subscribers gprs-only full

This command provides information that indicates whether ISR is activated for 2G subscribers, provides the MME tunnel endpoint ID being used for the ISR-activated 2G subscriber, and the IP address of the MME associated with the ISR-activated 2G subscriber.

- ISR-Activated: (True or False)
- MME Ctrl Teid: (MME Control Tunnel Endpoint Identifier)
- MME IP Address: (IP address of MME)

show subscribers sgsn-only full

This command provides information that indicates whether ISR is activated for 3G subscribers, provides the specific S3 tunnel on the MME being used for this ISR-activated subscriber, and the IP address of the MME associated with the ISR-activated 3G subscriber.

- ISR-Activated: (True or False)
- MME Ctrl Teid: (MME Control Tunnel Endpoint Identifier)
- MME IP Address: (IP address of MME)

show s4-sgsn statistics (2G ISR)

The output of this command provides information on the various reasons for deactivations of ISR-activated 2G subscribers:

- 2G Intra RAU with SGW Relocation
- Detach Notification from MME to 2G
- 2G MS Initiated Detach
- 2G Cancel Location from HSS/HLR
- 2G Local Admin Detach

- 2G Implicit Detach Timer Expiry

show s4-sgsn statistics (3G ISR)

The output of this command tracks the number of ISR deactivations due to various reasons for a 3G ISR-activated subscriber:

- 3G Intra RAU with SGW Relocation
- 3G NW Initiated Detach
  - 3G MR IDT Expiry
- 3G MS Initiated Detach
- 3G Cancel Location from HSS/HLR
- 3G SRNS Abort
- 3G Local Admin Detach
- 3G SGW Change During SRNS

show gmm statistics (2G ISR)

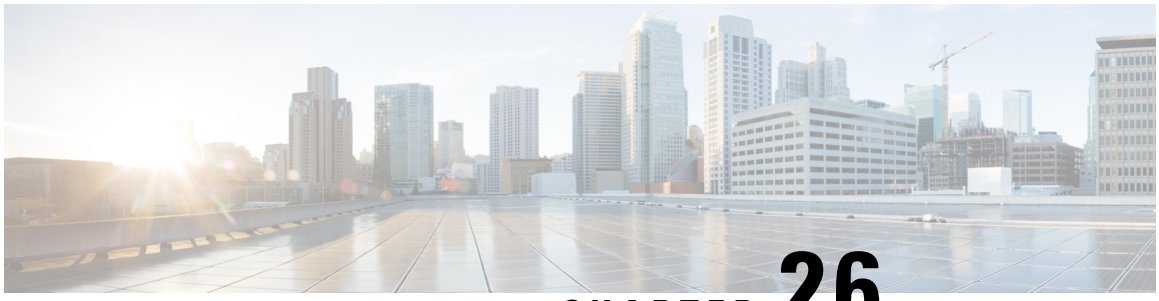
The output of this command indicates the total of currently activated 2G ISR subscribers:

- ISR Activated Subscribers:
  - 2G Intra RAU with SGW Relocation

show gmm statistics (3G ISR)

The output of this command tracks the number of currently ISR-activated 3G subscribers:

- ISR Activated Subscribers:
  - 3G-ISR-Activated



CHAPTER 26

IMSI Manager Broadcast Control

- Feature Description, on page 305
- How It Works, on page 306
- Configuring IMSI Manager Broadcast Control, on page 307
- Monitoring and Troubleshooting IMSI Manager Broadcast Control, on page 307

Feature Description

The IMSI Manager is the Demux process that selects the Session Manager instance based on the Demux algorithm logic to host a new session for 2G/3G/4G subscribers for SGSN/MME. The IMSI Manager maintains the IMSI-SMGR mapping for SGSN (2G/3G) and MME (4G) subscribers. The mapping maintained at IMSIMGR task is usually in sync with the mapping maintained at all session managers. But in some rare cases, there is a mismatch due to problems during the synchronization process. In such scenarios, the IMSIMGR task sends out a broadcast message to all session managers hoping that at least one of them will be hosting that session and could respond positively to this broadcast.

If none of the Session Managers respond with the mapping, the IMSI Manager considers it as request for an UNKNOWN (unregistered) subscriber and forwards it to a random Session Manager, which in turn sends an error response for the HLR request. The broadcasts from the IMSI Manager happen through a non-blocking vector call to all active Session Managers which can lead the IMSI Manager into a CPU overload condition considering the high number of session managers.

IMSI Manager broadcast control is implemented by the following:

- In IMSI Manager, broadcast disabling CPU threshold value defined; once the CPU utilization crosses this threshold, the IMSI Manager will not broadcast any unknown subscriber requests from HLR. Default value of this threshold is set as 50%. A CLI command is provided to optionally define the CPU threshold.
- In IMSI Manager, congestion threshold value of 70% is defined; once the CPU utilization crosses this threshold, the IMSI Manager will trigger congestion control action and will drop all unknown subscriber requests from HLR.

Important This feature is enabled by default.

How It Works

IMSI Manager Broadcast Control

IMSI Manager broadcast control is applicable only to SGSN. The MAP requests from the HLR arrives at the IMSI Manager as the Link Manager cannot find the Session manager instance from IMSI in the request. The following MAP requests arrive at the IMSI Manager:

1. CANCEL LOCATION REQUEST
2. Standalone INSERT SUBSCRIPTION DATA (ISD)
3. Delete Subscriber Data (DSD)
4. Provide Subscriber Location (PSL)

The IMSI Manager looks for the Session manager id which hosts the IMSI in its mapping table. If the mapping does not exist, the requests are broadcasted to all active Session Managers for finding the session or mapping. If all the Session managers respond with negative response, the IMSI Manager sends the MAP request to a random Session manager which in turn responds with a Map User Error response with cause as "Unidentified Subscriber". Broadcasting of request consumes a huge amount of IMSI Manager CPU capacity, it is also observed that the most of the unknown requests received genuine unknown subscriber requests sent by HLR and the HLR is incorrectly sending these requests to the SGSN. To conserve the IMSI Manager CPU, broadcasting of these requests are avoided.

IMSI Manager Broadcast Disabled During System Reboot

After a system reboot, the subscribers are not yet registered in the system. During this period, if HLR sends ISD or Cancel Location Requests to the system in huge numbers, these requests are broadcasted thus leading to an IMSI Manager CPU overload condition. To conserve IMSI manager CPU, the IMSI Manager will not perform any broadcasting for the UNKNOWN MAP requests from HLR for first 60 minutes after reboot of the system. This SGSN feature is enabled by default and is not configurable. After 60 mins, the behavior as per the CLI configuration for IMSI manager broadcasting will be applied.

Disabling Broadcast

Broadcasting is stopped when the IMSI Manager is busy handling heavy traffic (that is, when IMSI Manager reaches a specific CPU threshold). All the IMSI Manager instances monitor their CPU usage and when the CPU threshold is reached, broadcasting is stopped until the CPU comes down below the threshold value. Instead of broadcasting to all Session Managers, the request is sent to any random Session Manager which in turn sends the response back to the originating node. This feature is enabled by default and the default CPU threshold for disabling broadcasting is 50%. The configured CPU threshold overrides this default value.

Congestion Control

In IMSI Manager, congestion is triggered when CPU crosses 70%; once the CPU utilization crosses this threshold, the IMSI Manager will trigger congestion control action and will silently drop all unknown subscriber requests from HLR. No responses will be sent to peer originating the requests.

Note The thresholding application is a best effort at that instance and if the incoming rate of unknown messages is unusually high, a brief spike in the CPU usage of IMSIMGR task might occur.

Configuring IMSI Manager Broadcast Control

This section describes the configuration procedure for this feature.

A new keyword is added to the **task facility imsimgr** command under the Global Configuration mode to configure an IMSI Manager CPU threshold, once this threshold is reached the IMSI Manager stops broadcasting to conserve CPU.

```
configure
   task facility imsimgr { avoid-sessmgr-broadcast { cpu_threshold
percentage_value } | max integer_value | required-sessmgr  no_sess_mgrs |
sessmgr-sessions-threshold high-watermark high_value low-watermark low_value
 }
   end
```

Notes:

- The **cpu_threshold** keyword specifies the CPU value of the IMSI Manager in percentage.
- The *percentage_value* keyword is a percentage integer from 50% up to 70%. The default value is 50%.

Important After you configure the **task facility imsimgr max** command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Example:

The following command is used to disable all IMSI Manager Broadcasts:

```
task facility imsimgr avoid-sessmgr-broadcast
```

The following command is used to disable broadcast after the IMSI Manager CPU reaches 60%:

```
task facility imsimgr avoid-sessmgr-broadcast cpu_threshold 60
```

Monitoring and Troubleshooting IMSI Manager Broadcast Control

New statistics are introduced as a part feature which can be viewed in the Debug mode. The operator can use these statistics to get the current status of broadcasting, which is either broadcasting is enabled or disabled.

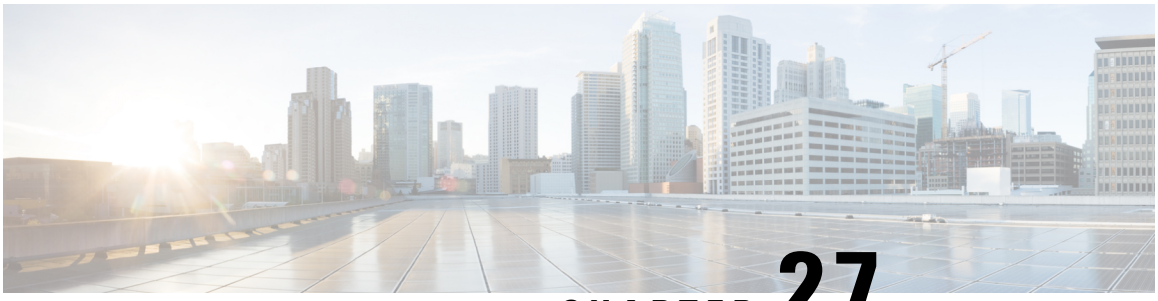
Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs:

show demuxmgr statistics imsimgr all

- Total Unknown Subscriber Request Rx counters
- Insert Subscriber Data req
- Delete Subscriber Data req
- Cancel location req
- Other unknown req
- Imsimgr-Sessmgr Broadcast statistics for unknown Subscriber requests
- Broadcast Current status (enabled/disabled and reason for disabling)
- Number of requests sent to Random smgr (after bcast failure rsp)
- Number of requests sent to Random smgr (broadcast disabled)
- Number of request dropped due to High CPU

Apart from the statistics listed above, SGSN Network Overload protection statistics which were only available in the show gmm-sm statistics are now available as a part of show demuxmgr statistics imsimgr all. The show output is realigned for better readability. Unusual logs are added in IMSIMGR to print the IMSI of subscriber and the unknown request type received from the peer node. Debug logs are also provided to display the current CPU usage and the request types that are dropped.



CHAPTER 27

IMSI Manager Overload Control

- Feature Description, on page 309
- Monitoring and Troubleshooting IMSI Manager Overload Control, on page 310

Feature Description

The IMSI Manager is the Demux process that selects the Session Manager instance based on the Demux algorithm logic to host a new session for 2G/3G/4G subscribers for SGSN/MME. The IMSI Manager maintains the IMSI-SMGR mapping for SGSN (2G/3G) and MME (4G) subscribers. The mappings maintained for all registered subscribers are synchronous with the Session Managers.

When the incoming attach rate is high at the IMSIMGR in a short span of time, the CPU consumption is very high and affects the normal processing activities of the IMSI Manager. At times this can lead to an IMSI Manager crash. Overload control methods are devised through this feature enhancement to keep the IMSI Manager CPU under control.

Important This feature is enabled by default.

IMSI Manager Overload Control

IMSI Manager Overload control is implemented on both SGSN and MME call flows. Attach rate throttling(network overload protection) is implemented in IMSI Manager to cap the rate at which new requests are accepted by SGSN and MME. This feature helps us process the incoming new subscriber requests (for example ATTACH/ISRAU) at a configured rate, therefore the HLR and other nodes are not overloaded. The SGSN and MME have separate pacing queues in the IMSI Manager to monitor the incoming rate of requests and have a separate network overload configuration as well.

For the SGSN, the following requests are paced using the pacing queues:

- Initial ATTACH (with IMSI , L-PTMSI ,F-PTMSI)
- Inter-SGSN RAU
- Empty-CR requests

In the MME, new connections are setup for the following events:

- UE initiated initial Attach

- All types of attach – IMSI, local GUTI, foreign GUTI, mapped GUTI, emergency and so on.
- UE initiated Inter-CN node TAU request requiring context transfer from old MME/SGSN
- TAU request with foreign GUTI or mapped GUTI
- Peer SGSN/MME initiated forward relocation request via Gn/S10/S3

With this feature enhancement when the incoming attach rate is high, the pacing queue becomes full and the further requests are either dropped or forwarded to Session Manager. The Session Manager in turn sends the reject response based on the configuration. When network overload protection action is set as "reject", the IMSI Manager has to forward overflowing requests from the pacing queue to Session Manager through a messenger call to send back error response. The IMSI Manager spends more time on messenger read and write. The IMSI Manager CPU reaches high values when the incoming call rate is very high (both SGSN/MME) though the network overload protection is configured. To ensure that the IMSI Manager CPU is under control, the IMSI Manager reduces certain messenger activities on reaching the default CPU threshold of 70%. This threshold value is fixed and this feature is enabled by default. This value is currently non-configurable. The IMSI Manager drops the overflowing requests from the pacing queue when the CPU crosses 70% mark instead of rejecting the request. Every IMSI Manager instance monitors its CPU usage independently and actions are taken according to the CPU usage.

Relationships to Other Features

Attach throttling feature will have an impact due to this feature enhancement. Once the CPU reaches the threshold of 70%, the messages will be dropped (irrespective of configured action).

Monitoring and Troubleshooting IMSI Manager Overload Control

New statistics are introduced as a part of feature which can be viewed in the Debug mode. The operator can use these statistics to find the number of requests dropped due to overload.

Show Command(s) and/or Outputs

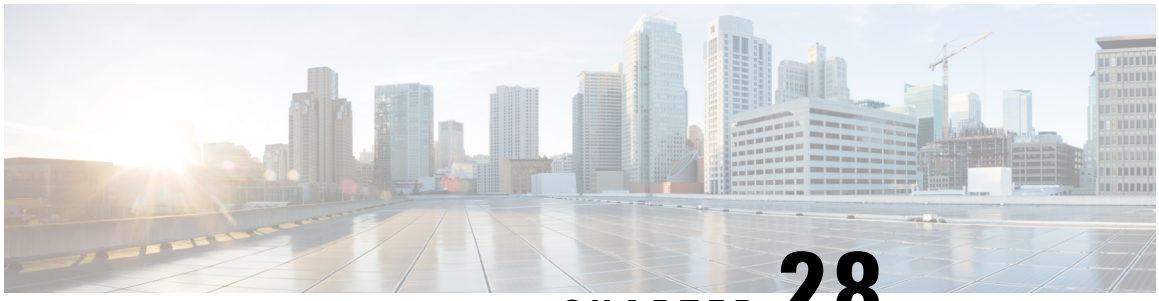
This section provides information regarding show commands and/or their outputs:

show demuxmgr statistics imsimgr all

These counters are available for both MME and SGSN separately.

- Requests dropped due to pacing queue with High Imsimgr CPU

Apart from the statistics listed above, SGSN Network Overload protection statistics which were only available in the show gmm-sm statistics are now available as a part of show demuxmgr statistics imsimgr all. The show output is realigned for better readability. Debug logs are also provided to display the current CPU usage.



CHAPTER 28

ISR with Circuit Switched Fallback

- ISR with CSFB - Feature Description, on page 311
- Call Flows, on page 312
- Relationships to Other Features, on page 315
- Relationships to Other Products, on page 315
- How it Works, on page 315
- ISR CSFB Procedures, on page 316
- Standards Compliance , on page 319
- Configuring ISR with Circuit Switched Fallback, on page 320
- Monitoring and trouble-shooting the CSFB feature, on page 320

ISR with CSFB - Feature Description

Idle-mode Signaling Reduction (ISR) feature allows the UE to move between LTE and 2G/3G without performing Tracking Area (TA) or Routing Area (RA) updates once it has been activated. A pre-requisite for ISR activation is that the UE, SGSN, MME, Serving GW and HSS all support ISR. At the first attach to the network, ISR is not activated. ISR can only be activated when the UE has first been registered in an RA on 2G/3G and then registers in a TA or vice versa.

If the UE first registers on GERAN/UTRAN and then moves into an LTE cell, the UE initiates a TA update procedure. In the TA update procedure, the SGSN, MME and Serving GW communicate their capabilities to support ISR, and if all the nodes support ISR, the MME indicates to the UE that ISR is activated in the TAU accept message.

Circuit-Switched Fallback (CSFB) is an alternative solution to using IMS and SRVCC to provide voice services to users of LTE. The IMS is not part of the solution, and voice calls are never served over LTE. Instead, the CSFB relies on a temporary inter-system that switches between LTE and a system where circuit-switched voice calls can be served.

The ISR feature must be enabled for the CSFB feature to work, the ISR feature is a license controlled feature.

The LTE terminals 'register' in the circuit switched domain when powered and attaching to LTE. This is handled through an interaction between the MME and the MSC-Server in the circuit-switched network domain over the SGs interface.

Consider the following scenarios:

- Voice calls initiated by the mobile user: If the user makes a voice call, the terminal switches from a LTE system to a system with circuit-switched voice support. Depending on where the UE latches on after completion of the voice call:
  - The packet-based services that are active on the end-user device at this time are handed over and continue to run in a system with circuit-switched voice support but with lower data speeds.

  OR

  - The packet-based services that are active on the end-user device at this time are suspended until the voice call is terminated and the terminal switches back to LTE again and the packet services are resumed.
- Voice calls received by the mobile user: If there is an incoming voice call to an end-user that is currently attached to the LTE system, the MSC-Server requests a paging in the LTE system for the specific user. This is done through the SGs interface between the MSC Server and the MME. The terminal receives the page, and temporarily switches from the LTE system to the system with circuit-switched voice support, where the voice call is received. Once the voice call is terminated, the terminal switches back to the LTE system.

Call Flows

To support CS fallback, existing procedures are modified and some additional CS fallback specific procedures added to the EPS. Additions are done to the "Attach" and "TA update" procedures which activate an interface called the SGs. This interface is between the MME and MSC. It is used by the MSC to send paging messages for CS calls to the UE on the LTE system.

Example of a CS fallback call

Figure 50: CS Fallback Call

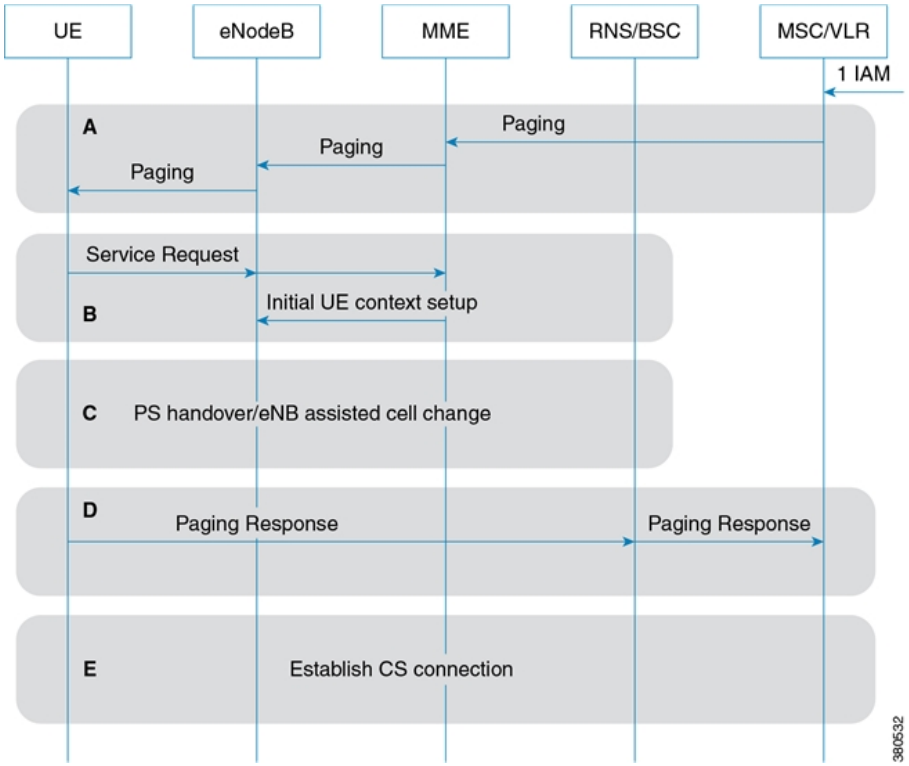


Table 22: Steps in a CS fallback call

Step	Description
1.	The MSC receives an incoming voice call and sends a CS page to the MME over a SGs interface.
2.	The MME uses the TMSI (or IMSI) received from the MSC to find the S-TMSI (which is used as the paging address on the LTE radio interface).
3.	The MME forwards the paging request to the eNodeB in the TAs where the UE is registered. The eNodeBs perform the paging procedures in all the cells in the indicated TAs.
4.	The paging message includes a special CS indicator that informs the UE that the incoming paging is for a terminating CS call.
5.	On receiving the paging message, the UE performs a service request procedure which establishes the RRC connection and sends a Service Request to the MME. The Service Request message includes a special CS Fall-back indicator that informs the MME that the CS fallback is required.

Step	Description
6.	This triggers the MME to activate the bearer context in the eNodeB with an indication to perform fallback to GERAN or UTRAN.
7.	The eNodeB selects a suitable target cell, by triggering the UE to send measurements on the neighbour cells, and initiates a handover or cell change procedure. The selection between handover or cell change procedure is based on the target cell capabilities and is configured in the eNodeB. **Note** If the target cell is a UTRAN cell, then MME can do subscriber context transfer using Forward Relocation Req / Rsp / Complete / Complete Ack messages and set up the radio contexts in UTRAN a-priori. However if the target cell is GERAN, then the SGSN currently does not support PS handover procedure and hence transfer of radio context from MME to 2G SGSN through Fwd reloc req / rsp /complete/complete ack procedure is not possible in the current release. In this scenario, CSFB is performed through a RRC release at the eNodeB and then a Suspend Request is sent to the SGSN.
8.	After a handover or cell change procedure, the UE detects the new cell and establishes a radio connection and sends a page response to the MSC, through the target RAN.
9.	When the page response arrives at the MSC, a normal mobile terminated call setup continues and CS call is activated towards the UE.

The CS fallback is primarily supports voice calls but it also supports other CS services. In the case of SMS services the UE need not switch to other radio interfaces. The UE can remain on LTE and still send and receive SMSes. The SMS messages are tunnelled between the UE and the MSC through the MME NAS signalling and the SGs interface.

When ISR is activated the UE is simultaneously registered at both SGSN and MME. So any paging for CS services occurs at both the SGSN and the MME. In a network if ISR is activated for an UE and CSFB is used in the network, the SGSN has to support additional call flows.

Relationships to Other Features

The CS Fallback feature is inter-works with the Idle Mode Signaling Reduction (ISR) feature. The CS Fallback feature is primarily for the EPS, but at the SGSN, it plays a role in deciding when the ISR feature should be activated or de-activated at the SGSN.

Relationships to Other Products

To enable ISR for subscriber peer nodes, the MME and SGW must support ISR functionality.

How it Works

Listed below are the scenarios where ISR with CSFB is impacted by the SGSN, these scenarios are applicable to both 2G and 3G when ISR is enabled:

1. The ISR is de-activated (by not sending ISR active status indication in RAU Accept message sent to UE) in the following cases:
   - The SGSN will not sent the ISR activated indication at combined RAU/LAU procedure (As per 3GPP TS23.272, section 4.3.5 ,release 11.2)
   - When the UE sends a combined RAU and LAU to a S4-SGSN, the SGSN checks the "Combined EPS/IMSI Attach Capability" bit in the "MS Network Capability" IE received. If that bit indicates CSFB and/or SMS over SGs is enabled for this UE, then the SGSN de-activates the ISR by not indicating the "ISR Activated" status in RAU Accept message sent to the UE. The SGSN in a CSFB/SMS over SGs configuration never indicates "ISR Activated" in combined RAU procedures for CSFB/SMS over SGs enabled UEs.
2. If CS Paging Indication is received from MME for an ISR activated subscriber, the SGSN pages to the subscriber indicating that the paging is for a CS call. When a Mobile Terminating call arrives at the MSC/VLR (via the G-MSC) for a UE that is camped on an E-UTRAN (ISR is active and the SGs interface is active between MSC and MME), the MSC/VLR sends a Page Request (SGsAP-PAGING-REQUEST) to the MME.

   As ISR is active and the UE is in ECM_IDLE state, the MME forwards the CS paging message received from the MSC/VLR to the associated SGSN. The MME gets the SGSN information in the regular ISR activation process. The MME builds a "CS Paging Indication" message, which is a GTPv2 message, from the SGsAP-PAGING_REQUEST to the correct SGSN. The SGSN receives the CS Paging Indication message from the MME, and sends paging messages to RNS/BSSs. This information is described in detail in 3GPP TS 23.060.
3. In Receive and handle "Alert MME Notification" and send "Alert MME "Acknowledge" scenarios.
4. When the SGSN sends an UE Activity Notification message over the S3 interface, if the MME sends an Alert MME Notification earlier for the same subscriber and the SGSN detects any UE activity (like Iu connection established and so on).
5. Handling the problem of Mobile Terminated voice calls getting dropped due to NULL SGs or SGs association at MSC/VLR, when the implicit detach timer expires at MME. In this case, the flag "EMM Combined UE Waiting" is set at the SGSN, this ensures waiting for a combined procedure (Combined RAU). A Combined RAU is forced if we receive a normal periodic RAU (non-combined) by sending an IMSI Detach request to UE. When a MME detaches the UE locally from E-UTRAN (due to PTAU timer

expiry and no contact with UE at E-UTRAN till the implicit detach timer expiry at MME) it sends a Detach Notification with cause "local detach" to the SGSN. The SGSN sets the "EMM Combined UE Waiting" flag if UE is CSFB capable and this flag will be reset only after combined RAU is received.

ISR CSFB Procedures

CS Paging Procedure

The call flow below depicts a CS Paging example:

Figure 51: CS Paging

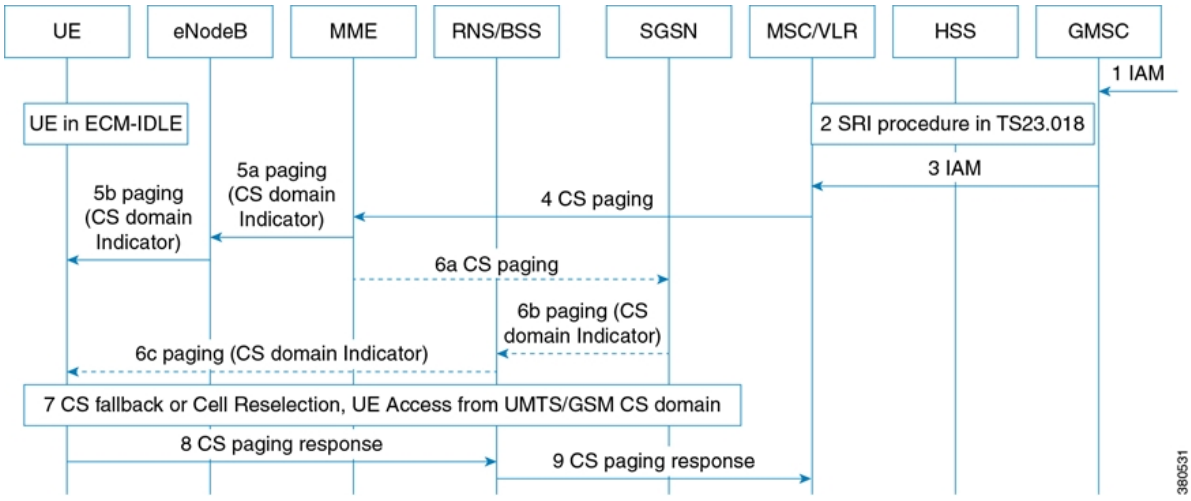


Table 23: Steps in a CS Paging Procedure

Step	Description
1.	A Mobile Terminating call arrives at MSC/VLR (via the G-MSC) for a UE which is camped on E-UTRAN.
2.	If the ISR is active and the SGs interface is active between MSC and MME, then the MSC/VLR sends a Page Request (SGsAP-PAGING-REQUEST) to the MME.
3.	As ISR is active and the UE is in ECM_IDLE state, the MME forwards the CS paging message received from the MSC/VLR to the associated SGSN. The MME receives the SGSN information in the regular ISR activation process. The MME builds a "CS Paging Indication" message, which is a GTPv2 message, from the SGsAP-PAGING_REQUEST to the correct SGSN.

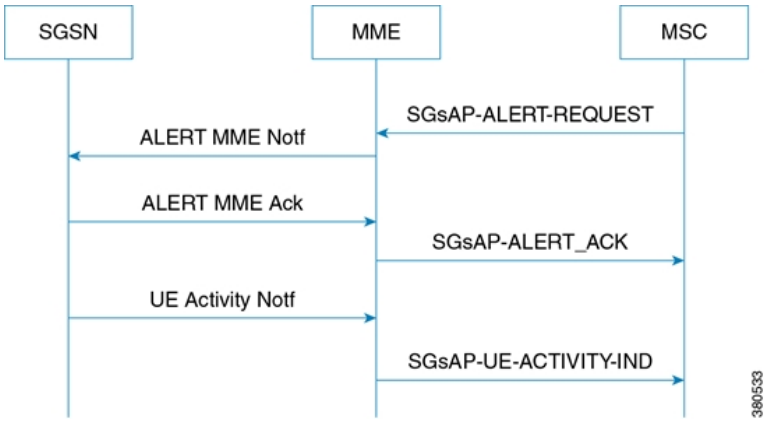
Step	Description
4.	The SGSN receives the CS Paging Indication message from the MME, and sends paging messages to RNS/BSSs.
5.	The RNS/BSS forwards the CS Paging Indication message to the UE.
6.	The CS fallback or Cell re-selection process progresses.
7.	Once the process is complete, the UE sends a CS Paging response to the RNS/BSS.
8.	The RNS/BSS forwards the CS Paging Response to the MSC/VLR.

For detailed information on CS paging procedure refer to 3GPP TS 23.060.

Alert and UE Notification Procedure

The call flow below depicts an Alert and UE Notification scenario:

Figure 52: Alert and UE Notification Procedure 0



1. The MSC/VLR requests the MME to report activity from a specific UE. The MSC/VLR sends a SGsAP Alert Request (IMSI) message to the MME where the UE is currently attached to an EPS network. On receiving the SGsAP Alert Request (IMSI) message, the MME sets a Non-EPS Alert Flag (NEAF). If NEAF is set for an UE, the MME informs the MSC/VLR of the next activity from that UE (and the UE is both IMSI and EPS attached) and clears the NEAF.
2. If ISR is activated for this UE, an "Alert MME Notification" message (GTPv2) is created based on above SGs message and sent on the S3 interface by the MME to the associated SGSN, in order to receive a notification when any activity from the UE is detected.
3. The SGSN sends an "Alert MME Acknowledge" and sets the SSAF flag, the "Alert MME Acknowledge" is a GTPv2 message to the MME in response to the Alert MME Notification message.
4. If any UE Activity is detected (UE is active, after an Iu connection is established), the SGSN sends a "UE Activity Notification message" to the MME over the S3 interface.

ISR De-activation Procedure

When the UE wants to perform a combined RAU/LAU, the SGSN verifies the "combined EPS/IMSI attach capability" bit in MS Network Capability and if it indicates that CSFB and/or SMS over SGs is enabled, then the SGSN de-activates ISR. The SGSN does not indicate that ISR is activated in the RAU Accept message.

Detach Procedures for CSFB Capable UEs

If the MME clears a subscriber then SGs association with the MSC is closed and leads to a drop of voice calls from the MSC. To avoid this issue a few changes are done in SGSN to establish the Gs association between the MSC and the SGSN on ISR de-activation.

If "Detach Notification" is received from the MME with Detach Type set as "Local Detach" and if the UE supports EMM Combined procedures then, the SGSN sends an IMSI Detach request to the UE and sets the "EMM Combined UE Waiting" flag.

If the SGSN then receives a Periodic RAU Request and the flag "EMM Combined UE Waiting" is set, an IMSI Detach is sent to the UE in order to ensure that next time the UE performs a Combined RAU. This enables Gs association between the SGSN and the MSC/VLR and the MT voice calls are not lost.

If the SGSN receives a Combined RAU Request when the flag "EMM Combined UE Waiting" is set, then this flag is cleared and Gs association is activated.

MS Initiated Last PDN De-activation Procedure

The MS initiated last PDN de-activation procedure is listed below:

1. The SGSN sends a DSR with OI=1, the cause not set to ISR deactivated.
2. PDP is deleted from the SGW and the PGW.
3. In SGSN all PDPs are de-activated. The S4 association is cleared.
4. In SGW all PDPs are de-activated. Both the S4 and S11 associations at the SGW are cleared.
5. The MME continues to retain the S11 tunnel.
6. Both the SGSN and MME retain the ISR and S3 tunnel active. The active S3 tunnel serves incoming voice calls if SGs association is retained at the MME.
7. If MME has a SGs association and if periodic TAU timer from UE expires, the MME performs the following actions:
   - The MME starts an implicit detach timer. If voice call is received at MSC/VLR when this timer is running then:
     a. The MSC/VLR sends a SGs page to the MME.
     b. The MME sends an S3 page to the SGSN.
     c. The SGSN pages the UE with the "CN Domain Indicator = CS domain", and if the UE responds to the page by doing a cell re-selection to CS domain, the MSC/VLR stops paging.
     d. The voice call is completed.
   - If the implicit detach timer expires:
     - The MME sends an EPS Detach Notification (IMSI detach) to the MSC/VLR.
     - The MME sends a Detach Notification with cause "Local detach" to the SGSN (Refer to 3GPP TS 23.272v10.08, section 5.3.2 point no. 3).
     - If the UE is "combined EPS/IMSI attach capable" (as derived from MS Network capability) and if ISR is active, the SGSN sends an IMSI detach request to the UE on receiving Detach Notification with cause "local detach".

- The SGSN sets a flag called "EMM Combined UE waiting" (Refer to 3GPP TS 23.272v10.08, section 5.5)
- If the IMSI detach request reaches the UE, the UE performs a Combined RAU, the "EMM Combined UE waiting" flag is cleared at the SGSN and Gs association is established between SGSN and MSC/VLR. ISR is deactivated at the UE.
- If the IMSI detach request does not reach the UE, then on next signaling from the UE based on the "EMM Combined UE waiting" flag being set, following action is taken:

  If an UE performs a periodic RAU or NAS Service Request, then the UE is forced to do an IMSI detach so that the UE does a Combined RAU again to establish Gs association.

PGW Initiated Last PDN De-activation Procedure

Listed below are the sequence of events which occur, if an UE is "combined EPS/IMSI attach capable" and the last PDN is de-activated due to PGW initiated de-activation or HSS initiated de-activation:

1. The SGW forwards the DBR to both the SGSN and the MME.
2. Both MME and SGSN de-activate the PDN, and locally de-activate ISR (Refer to 3GPP TS 23.401 v10.08, section 5.4.4.1 (Note 2 and 3) and 3GPP TS 23.060 v10.801, section 9.2.4.3B).
3. The MME need not send a Detach Notification to the SGSN.
4. Consider the scenario, where the SGSN is aware that it is a PGW initiated last PDN de-activation, the UE is "combined EPS/IMSI attach capable" (as derived from MS Network capability) and ISR was active earlier, the SGSN performs the following actions:
   - If the UE is in a PMM-CONNECTED state at the SGSN, then SGSN sends an IMSI detach request. The SGSN sets a flag called "EMM Combined UE waiting". If the UE receives this IMSI detach request, it performs a combined RAU into SGSN and at that point the Gs association is established and the "EMM Combined UE Waiting" flag is cleared by the SGSN.
   - If the UE is in an IDLE state at the SGSN, then the SGSN pages the UE to deliver the PDP de-activation request. If paging fails, the SGSN sets the "EMM Combined UE Waiting" flag. When this UE performs a combined RAU to SGSN at a later time or attaches to the SGSN, this flag is cleared.
5. If the UE is in an E-UTRAN coverage area then, the MME detaches the UE and the UE is re-attached to the network. If the UE is not in an UTRAN/GERAN coverage area, then the SGSN pages the UE prior to sending IMSI detach. This paging request fails.
6. If the UE does not receive an E-UTRAN detach request or a paging request from the SGSN, and at a later point if the UE returns to the SGSN with a periodic RAU / NAS Service Request, then the SGSN performs the following:
   - The "EMM Combined UE waiting" flag is set, this forces the UE to perform a IMSI detach so that the UE does a Combined RAU again to establish a Gs association.
7. If the UE receives the IMSI detach request sent in step (4), the UE performs a Combined RAU to establish Gs association. On receiving a Combined RAU, the SGSN clears the "EMM Combined UE waiting" flag.

Standards Compliance

The Idle mode signaling reduction complies with the following standards:

- 3GPP TS 23.060, version 10

- 3GPP TS 23.401, version 10
- 3GPP TS 23.272, version 10
- 3GPP TS 29.274, version 10

Configuring ISR with Circuit Switched Fallback

The following commands are used to configure 3G paging cause for CSFB:

```
config
    context context_name
      iups-service iups_service_name
         rnc id rnc_id
            [default | no ] ranap paging-cause-ie mme-signalling
paging_cause_value
          end
```

Where:

- The command **ranap paging-cause-ie mme-signalling** *paging_cause_value* is used to set the Paging Cause IE value for paging from MME due to Circuit Switch Fallback (CSFB). Listed below are the paging cause values which can be set:
  - 0 - Terminating conversational call
  - 1 - Terminating streaming call
  - 2 - Terminating interactive call
  - 3 - Terminating background call
  - 4 - Terminating low priority signaling
  - 5 - Terminating high priority signaling
- The default command resets the specific parameters value to default. In this case it is set to "5 - Terminating high priority signaling".
- The no form of the command suppresses the Paging Cause IE so that it is not included in responses to Paging Requests.

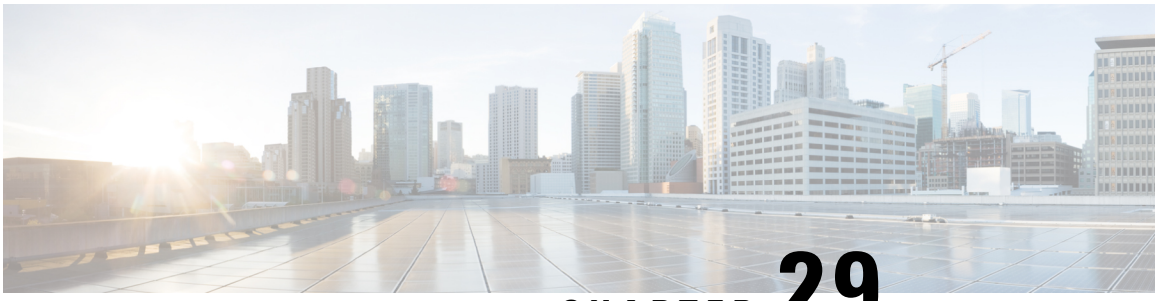
Monitoring and trouble-shooting the CSFB feature

The configuration can be verified by executing the show command **show iups-service**, the following parameter is displayed on executing the command:

- **MME-Signalling : Terminating Low Priority Signalling (4)**

The show command **show subscriber sgsn-only full all** has been updated to include a display for "SSAF" and "Emm_combined_ue_waiting" flags. The new parameters are displayed as below:

- **SSAF : False**
- **EMM Combined UE Waiting Flag : False**



CHAPTER 29

Location Services

- Location Services - Feature Description, on page 321
- How Location Services Works, on page 321
- Configuring Location Services (LCS) on the SGSN, on page 326
- Monitoring and Troubleshooting the LCS on the SGSN, on page 330

Location Services - Feature Description

The Location Services (LCS) feature enables the EPC MME and the GPRS/UMTS SGSN to use the SLg (MME) or Lg (SGSN) interface which provides the mechanisms to support specialized mobile location services for operators, subscribers, and third party service providers. Use of this feature and the SLg/Lg interface is license controlled.

The location information is reported in standard geographical co-ordinates (longitude and latitude) together with the time-of-day and the estimated errors (uncertainty) of the location of the UE. For external use, the location information may be requested by and reported to a client application associated with the UE, or a client within or attached to the core network. For internal use, the location information can be utilized by the SGSN for functions such as location assisted handover or to support other features.

Location information is intended to be used for

- location-based charging (e.g., home-location billing, roaming-location billing),
- location-based services (e.g., lawful interception, emergency calls),
- positioning services offered to the subscribers (e.g., mobile yellow pages, navigation applications on mobiles), and
- by the operator for service provider services such as network planning and enhanced call routing.

How Location Services Works

The SGSN LCS responsibilities center around UE subscription authorization and managing LCS positioning requests. The LCS functions of the SGSN are related to charging and billing, LCS co-ordination, location request, authorization and operation of the LCS services.

When using the Iu interface, before the SGSN can request location information of a target UE from the radio access network (RAN), an Iu signaling connection must have been established between the SGSN and the RAN. The SGSN sends a Location Request message to the RAN. The RAN determines the location of the target UE related to this Iu signaling connection and sends a Location Report to the SGSN over the same Iu

signaling connection. On the Iu interface, only one location request for a geographic location estimate can be ongoing at any time.

Only one location request can be ongoing at any time.

The operation begins with a LCS Client requesting location information for a UE from the LCS server. The LCS server will pass the request to the LCS functional entity (SGSN) in the core network. The LCS functional entitiy (SGSN) in the core network then:

1. verifies that the LCS Client is authorized to request the location of the UE or subscriber
2. verifies that location services are supported by the UE
3. establishes whether it (the MME/SGSN) is allowed to locate the UE or subscriber, for privacy or other reasons
4. establishes which network element in the radio access network (GERAN or UTRAN or E-UTRAN) should receive the Location Request
5. requests the access network (via the A, Gb, Iu or S1 interface) to provide location information for an identified UE, with indicated QoS
6. receives information about the location of the UE from the Access Network and forward it to the Client
7. sends appropriate accounting information to an accounting function.

Relationship to Other SGSN Functions

The Location Services feature utilizes several of the existing SGSN functionalities:

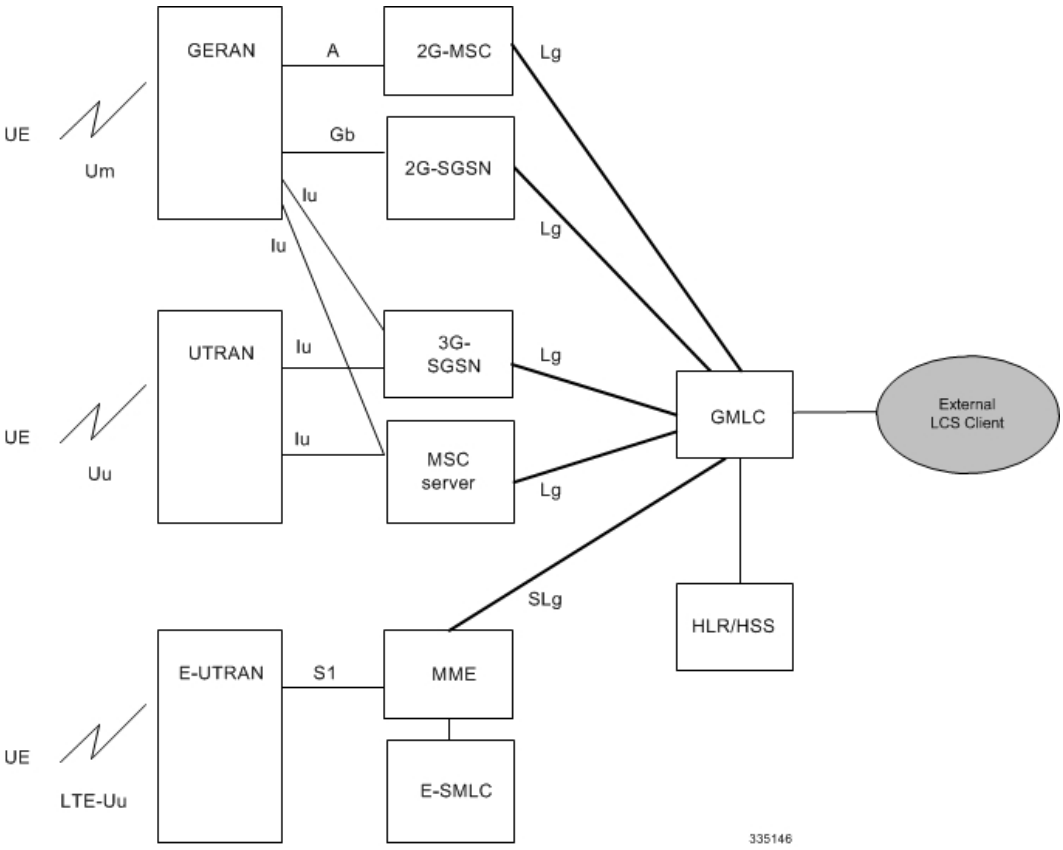
- Mobility Management module
- MAP Service module

Architecture

The MME is accessible to the Gateway Mobile Location Center (GMLC) via the SLg interface.

The SGSN is accessible to the GMLC via the Lg interface.

Figure 53: LCS Architecture



The SGSN informs the HLR/HSS regarding the LCS capabilities of UE in GPRS (2G) or UMTS (3G) networks. The SGSN may include the IP address of the V-GMLC associated with the SGSN in the MAP_UPDATE_GPRS_LOCATION message during Attach and ISRAU procedures.

Limitations

Currently, SGSN support is limited to:

1. A single location request at a time for the target UE. Concurrent location requests are not supported.
2. Only Provide Subscriber Location messages with the id as IMSI are supported.

Flows

Flows

Location Services call flows are standards compliant for the SGSN.

SGSN

Figure 54: 2G Mobile Terminating Location Request

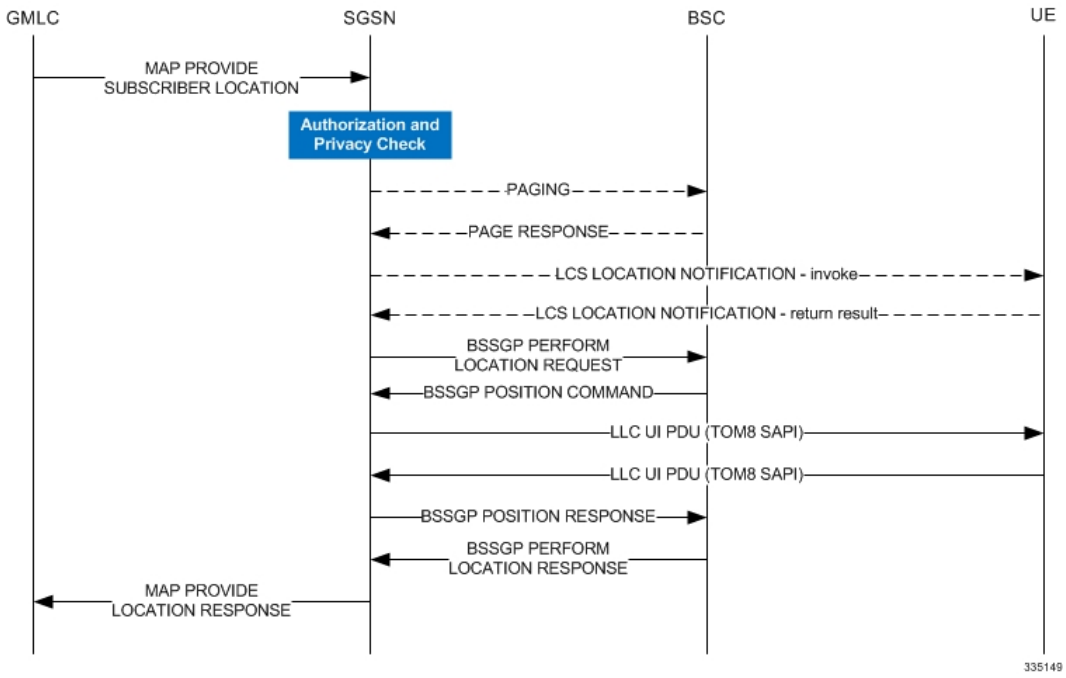
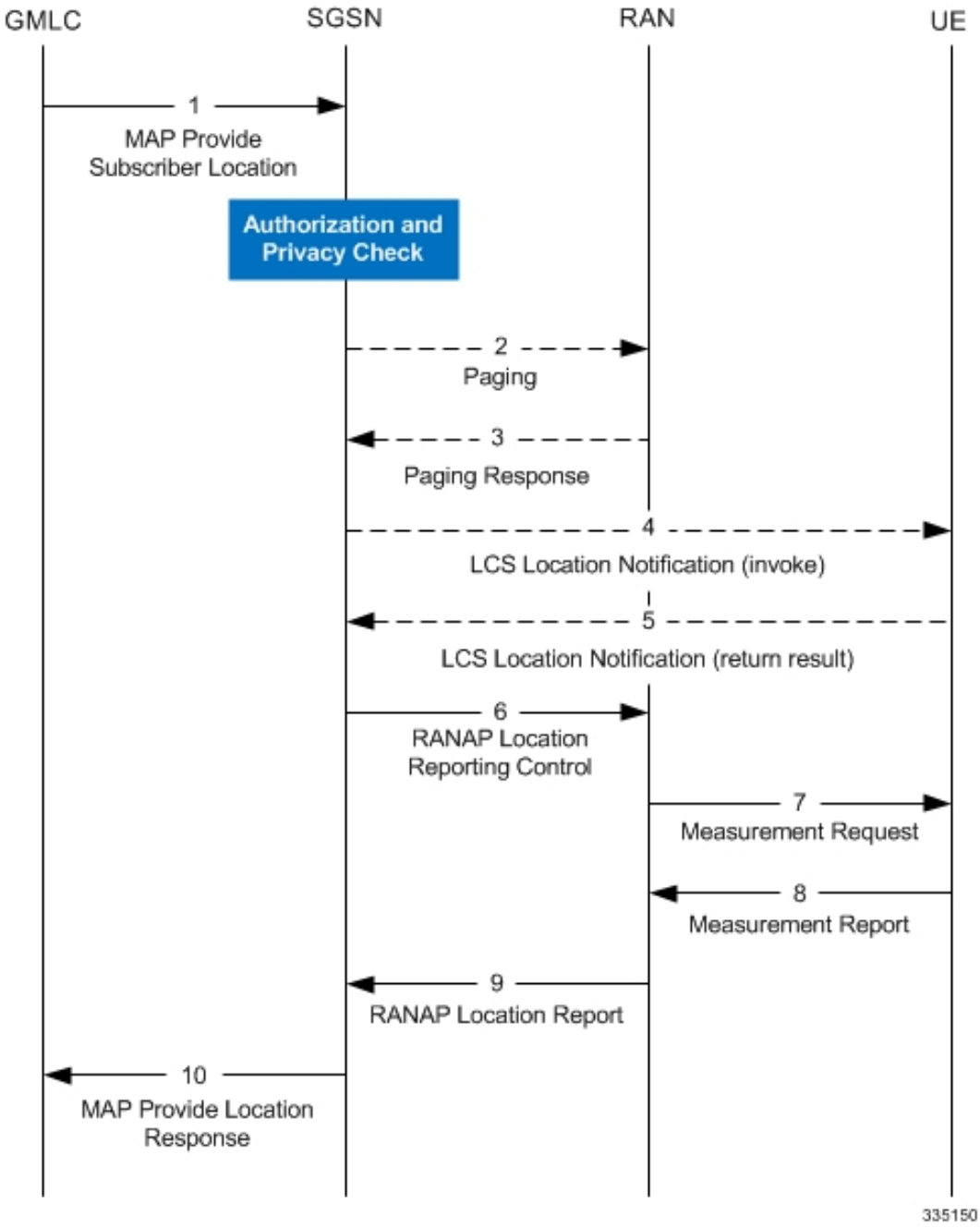


Figure 55: 3G Mobile Terminating Location Request



Standards Compliance

The SGSN's Location Services feature complies with the following standards:

- TS 3GPP 23.271, v9.6.0
- TS 3GPP 24.030, v9.0.0

- TS 3GPP 24.080, v9.2.0
- TS 3GPP 25.413, v9.8.0 (sections 8.19.2 and 8.20.2)
- TS 3GPP 29.002, v9.7.0

Configuring Location Services (LCS) on the SGSN

This section provides a high-level series of steps and the associated configuration examples to configure Location Services on the 2G or 3G SGSN -- or for both.

The commands could be issued in a different order, but we recommend that you follow the outlined order for an initial LCS configuration. All listed configuration steps are mandatory unless otherwise indicated.

Important For all the required configuration commands to be available and to implement the configuration, the SGSN must have loaded the license for the Lg interface.

Step 1 Enable Location Services on the SGSN.

Step 2 Identify the GMLC (in the MAP service) to which the SGSN connects for LCS access to the external LCS client.

Step 3 Configure the MAP service's M1 timer.

Important Step 3 is not mandatory but it is recommended.

Step 4 Create a location services configuration and associate the MAP service.

Step 5 Fine-tune LCS configuration per UE by defining LCS-related restrictions.

Step 6 Associate the location services configuration with the appropriate SGSN - GPRS (2G) service and/or UMTS (3G) service.

Step 7 Associate the location services configuration with an operator policy.

Step 8 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide*.

Step 9 Verify the configuration for each component by following the instructions provided in the *Verifying the Feature Configuration* section.

Enabling LCS

Location Services functionality is enabled globally for the SGSN.

```
config
     sgsn-global
          location-services
          end
```

Notes:

- This command enables and 'starts' LCS on the SGSN.
- This command also enables support for the Lg interface on the SGSN.

- Using the 'no' keyword stops LCS.

Identifying the GMLC

Use the MAP service configuration to identify the GMLC to which the SGSN connects for LCS access to the external LCS client. We recommend that you also configure the MAP service's M1 timer, however, this is option.

```
config
     context context_name
          map-service map_service_name
               gmlc { isdn E.164 | point-code point_code } gsn-address
ipv4_address [ source-ssn ssn ]
               timeout m1 seconds
               end
```

Notes:

- Only one GMLC can be configured per MAP service.
- SGSN includes the configured GMLC address as the value for the v-GMLC (an optional IE) in Update-GPRS-Location messages to the HLR. It is possible to configure the SGSN to exclude the GMLC address in Update-GPRS-Location messages, see *Configuring Exclusion of GMLC Address from Update-GPRS-Location Messages* below.
- **isdn** is the 1-15 digit E.164 number that identifies the GMLC.
- **point-code** is the address for the GMLC in dotted-decimal or decimal SS7 point-code format
- **gsn-address** is the IPv4 address for the GMLC
- **source-ssn** optionally identifies the source SSN value to be used.

Configuring Exclusion of GMLC Address from Update-GPRS-Location Messages

By default, the SGSN includes the GMLC address, configured in the MAP service, in all Update-GPRS-Location (UGL) messages going to the HLR. Some HLRs do not recognize the v_GMLC field or value when it arrives in the UGL. As a result, the HLRs reject the calls. This prevents roaming-in subscribers from using some networks where LCS is enabled.

Beginning with Release 19.4, it is possible to configure the SGSN to exclude the GMLC from the UGL message. This is done with a new keyword, **exclude-gmlc** , added to the **map** command in the Call-Contol Profile configuration mode. Use the following configuration, illustrated below, to exclude the GMLC from the UGL message:

```
config
   call-control-profile  profile_name
      map message update-gprs-location exclude-gmlc
      end
```

Notes:

- **exclude-gmlc** - This keyword configures the SGSN to exclude the GMLC address in the Update-GPRS-Location (UGL) messages sent to the HLR.
- To re-enable the default behavior to include the GMLC address in the map message, enter the following configuration command:

  ```
  remove map message update-gprs-location exclude-gmlc
  ```

- For information about the other keywords available for the **map** command, refer to the *Command Line Interface Reference*.

Creating the Location Service Configuration

This set of configuration commands creates a location service configuration and associates the MAP service with the location service. Up to 16 separate location services can be created.

```
config
     context context_name
          location-service loc_serv_name
               associate map-service map_serv_name
               end
```

Notes:

- The SGSN supports a maximum of 16 location service configuration. It should be noted that this number, 16, is not part of the SGSN's service configuration limit of 256.
- Associate the MAP Service configuration in which the GMLC is defined.

Fine-tuning the Location Service Configuration

Fine-tune the location service configuration per UE by defining LCS-related restrictions. The following commands will be used to configure the LCSN timer (location notification invoke procedures timer). Configuring the timer value is optional.

```
config
     context context_name
          location-service loc_serv_name
               timeout lcsn seconds
```

Notes:

LCSN timer range is 10 - 20 with a default of 15. seconds.

The following command is used to configure the UE available guard timer. Configuring this timer is optional.

```
config
     context context_name
          location-service loc_serv_name
               timeout ue-available-guard-timer ueagtimer_seconds
```

Notes:

This timer, set in seconds, is used to guard the packet-switched deferred location request (UE available event) procedures. It is an integer from 10 to 600. Default is 600.

The following command is used to configure area event invoke procedure timer. Configuring this timer is optional.

```
config
     context context_name
          location-service loc_serv_name
               timeout area-event-invoke-timer aietimer_seconds
```

Notes:

This timer, set in seconds, is used to guard the area event invoke procedure. It is an integer from 10 through 20. Default is 15.

The following command is used to configure periodic event invoke procedure timer. Configuring this timer is optional.

```
config
     context context_name
          location-service loc_serv_name
               timeout periodic-event-invoke-timer peitimer_seconds
```

Notes:

This timer, set in seconds, is used to guard the period location invoke procedure.. It is an integer from 10 through 20. Default is 15.

Associating the Location Service Config with the SGSN

Location service functionality can be associated with either the 3G SGSN via commands in the SGSN Service configuration mode or with the 2G SGSN via commands in the GPRS Service configuration mode.

The following associates the location service configuration with a 3G SGSN:

```
config
     context context_name
          sgsn-service service-name
               associate location-service loc_serv_name
```

Notes:

- To associate with a 2G SGSN, enter the GPRS service configuration mode in place of the SGSN service configuration mode.

Associating the Location Service Config with an Operator Policy

Location service functionality can be associated with an operator policy to provide granular control.

The following associates the location service configuration with a call-control profile by IMSI and these CLIs will disable/enable Mobile Terminating, Mobile Originating and/or Network Induced location requests by access-type.

```
config
     call-control-profile  ccprofile_name
               lcs-mt { allow | restrict } access-type { gprs | umts }
```

Notes:

- **lcs-mt** enables mobile-terminating location requests.

- replace **lcs-mt** with **lcs-mo** to enable the mobile-originating location requests, **lcs-ni** is not supported by SGSN.
- Default for the 3 **lcs** commands is **allow**

Verifying the LCS Configuration for the SGSN

View the location service configuration to verify the configurations created for the Location Service functionality, by using the following commands:

show location-service service { all | name *loc_serv_name*

View the MAP configuration to verify the MAP configurations created for the Location Service functionality, by using the following commands:

show map-service { all | name *map_serv_name* **}**

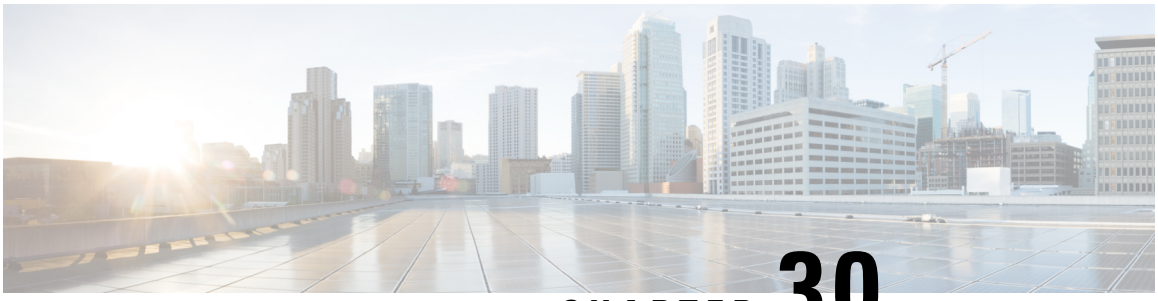
View the call-control profile configuration to verify the configurations created for the Location Service functionality, by using the following commands:

show call-control-profile full name *ccprof_name*

Monitoring and Troubleshooting the LCS on the SGSN

Use the commands listed below to monitor and/or troubleshoot the operation of the Location Services on the SGSN.

- **show map statistics name** *map-service-name*
- **clear map statistics name** *map-service-name*
- **show gmm-sm statistics**
- **show subscribers sgsn-only summary**
- **show subscribers gprs-only summary**
- **show location-service service {all | name** *location-service-name* **}**



CHAPTER 30

LORC Subscriber Overcharging Protection for S4-SGSN

The SGSN's Subscriber Overcharging Protection feature has been enhanced and now extends to the S4-SGSN to prevent both 2G and 3G subscribers from being overcharged when a loss of radio coverage (LORC) occurs over the S4 interface.

As part of this functionality, the operator configures all cause codes on the SGSN. If the SGSN receives a cause code, via Iu/Gb interfaces, that matches one of the cause codes configured on the SGSN, then the SGSN includes the ARRL (Abnormal Release of Radio Link) bit in the Release Access Bearer Request.

- Feature Description, on page 331
- How It Works, on page 332
- Configuring Subscriber Overcharging Protection, on page 335

Feature Description

Subscriber Overcharging Protection prevents subscribers from being overcharged when a loss of radio coverage (LORC) occurs.

Important In order for the Subscriber Overcharge Protection feature to be most effective, the SGSN supports initiation of Release Access Bearer Request on Iu-Release for all subscribers (even for non-ISR and non-DT cases). Refer to the section on *Release Access Bearer Requests* below for details.

LORC Subscriber Overcharge Protection on the S4-SGSN

LORC is standardized in 3GPP release 12.0 specifications. According to 3GPP TS 23.401, the SGSN includes the ARRL (Abnormal Release of Radio Link) Indication in Release Access Bearer Request messages if the Iu-Release procedure is due to an abnormal release of the radio link.

It should be noted that 3GPP has not defined LORC for UMTS / GPRS access in an EPS network. Currently, it is defined only for E-UTRAN access. However, the SGSN can use the defined 3GPP mechanism to achieve PDN pause of charging in UMTS / GPRS access as well.

With this feature the S4-SGSN should include the ARRL (Abnormal Release of Radio Link) bit in indication flags IE of Release Access Bearer Request when Iu-Release occurs due to the cause 'Radio Connection With UE Lost (46)' in 3G.

Also the S4-SGSN should include the ARRL (Abnormal Release of Radio Link) bit in indication flags IE of Release Access Bearer Request when Radio Status Bad ia received in 2G.

The operator configures all cause codes on the SGSN so if the SGSN receives a cause code via Iu/Gb interfaces that matches one of the cause codes configured on the SGSN, then the SGSN includes the ARRL bit in the Release Access Bearer Request.

Release Access Bearer Requests

3G (UMTS):

Upon RNC failure or Iu-Release, the SGSN preserves non-GBR (i.e., non-guaranteed bit rate) PDPs (interactive / background) by default. From release 15.0 onwards, for DT and ISR cases the SGSN supports sending Release Access Bearer Request on Iu-Release. In accordance with TS 23.060 v11.7.0, the SGSN can optionally send a Release Access Bearers Request to the S-GW to remove the downlink user plane on S4 for non-DT and non-ISR subscribers.

As part of this feature, the operator can configure the S4-SGSN to send Release Access Bearer Request on Iu-Release for non-DT and non-ISR subscribers. For DT and ISR subscribers, Release Access Bearer Initiation functions as it has done prior to this feature's implementation.

2G (GPRS):

Upon Ready-to-Standby, the SGSN preserves non-GBR (that is, non-guaranteed bit rate) PDPs (interactive / background) by default. From release 15.0 onwards, for ISR cases the S4-SGSN supports sending Release Access Bearer Request on Ready-to-Standby state transition. In accordance with 3GPP TS 23.060 v11.7.0, the SGSN optionally sends a Release Access Bearers Request to the S-GW to remove the downlink user plane on S4 for non-ISR subscriberes.

As part of this feature, the operator can configure the S4-SGSN to send Release Access Bearer Request on Ready-to-Standby or Radio Status Bad for non-ISR subscribers. For ISR subscribers, Release Access Bearer Initiation is independent and functions as it has done prior to this feature's implementation.

Relationships

- The S-GW should support receiving ARRL bit on S4 interface.
- For this feature to function effectively, the S-GW and P-GW also be configured to support the "PGW Pause of Charging" procedure.

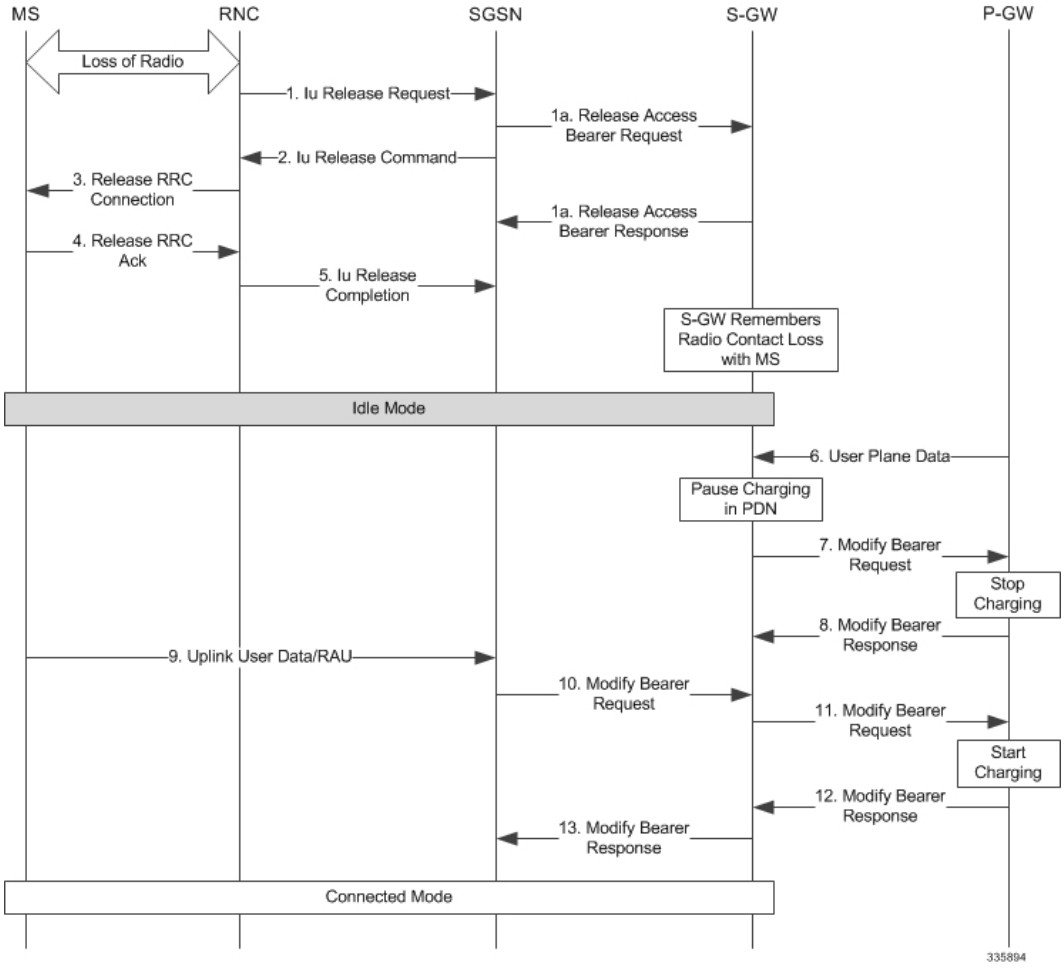
How It Works

The S4-SGSN handles LORC-based subscriber overcharging protection functionality in accordance with 3GPP specifications as described below.

3G Iu-Release Procedure and Overcharge Protection over S4

The following call flow is derived from section 12.7.3.2 of TS 23.060 v11.7.0 and it illustrates how the S4-SGSN handles the Iu-Release procedure due to LORC with the overcharging protection functionality enabled.

Figure 56: Iu-Release and Overcharging Protection on the S4



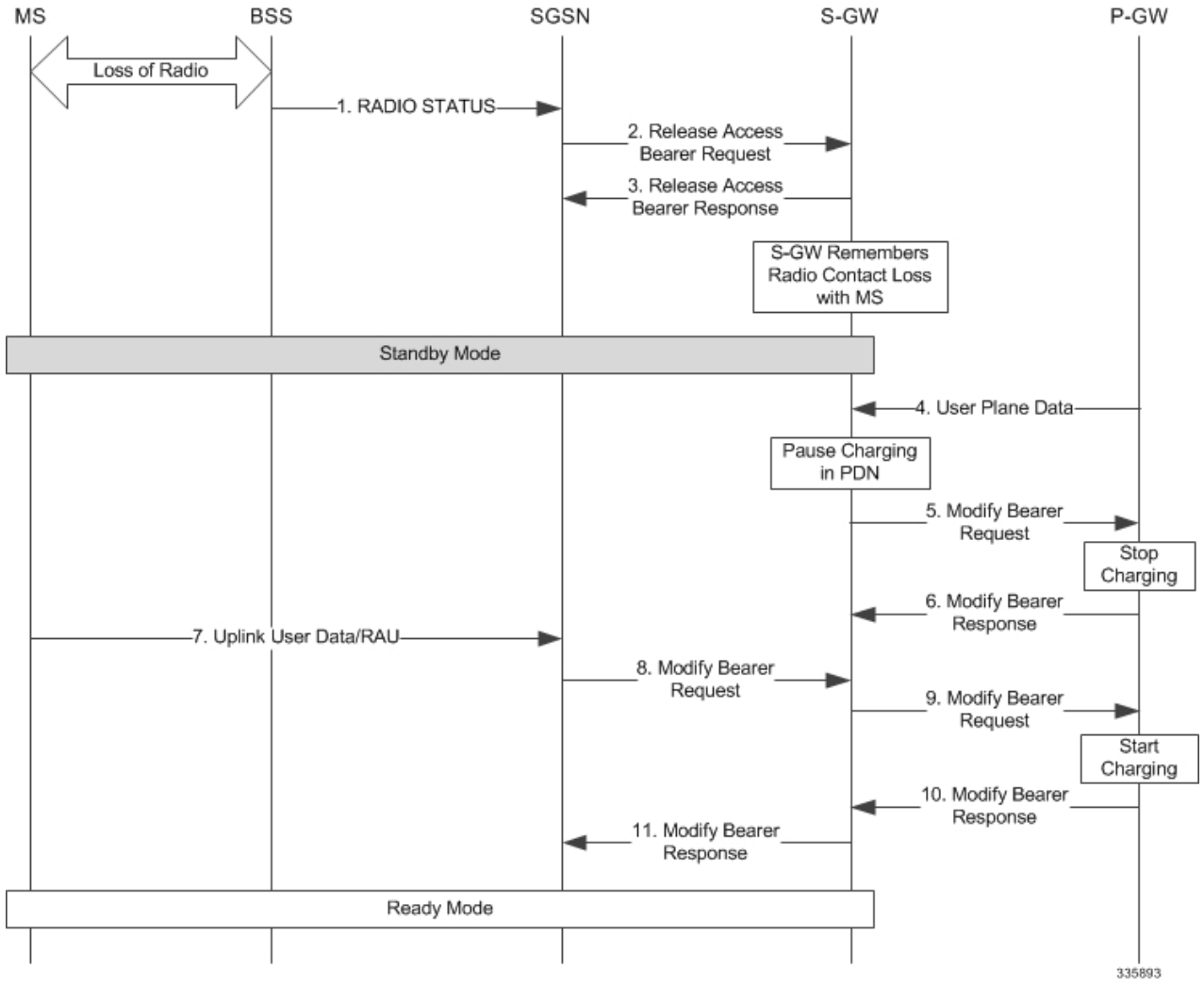
If the cause in the Iu-Release Request matches with the cause code configured under the LTE Policy and if overcharge protection is enabled under the SGSN-service, then the S4-SGSN includes ARRL (i.e., Abnormal Release of Radio Link) bit in the Release Access Bearer Request. For configuration details, refer to the section on *Configuring Subscriber Overcharging Protection*

2G Ready-to-Standby State Transition and Overcharge Protection over S4

The following flow is derived from section 8.1.3a of TS 23.060 v11.7.0 and it illustrates how the S4-SGSN handles the state transiton with regard to the overcharging protection functionality.

When idle mode packet buffering is performed on the S-GW, the SGSN needs to inform the S-GW each time that the MS changes from Ready state to Standby state. The following figure illustrates the procedure between the SGSN and the S-GW.

Figure 57: 2G Ready-to-Standby State Transition Using S4



If the BSSGP radio-cause code that is configured by the operator matches with the radio cause code received in the RADIO STATUS message and if the overcharge protection functionality is enabled under GPRS-service, then the SGSN includes the ARRL bit in Release Access Bearer Request. For configuration details, refer to the section on *Configuring Subscriber Overcharging Protection*.

Standards Compliance

Overcharging protection complies with the following standards:

- TS 23.060 version 11
- TS 23.401 version 11
- TS 29.274 version 11
- TS 25.413 version 11
- TS 48.018 version 11

Configuring Subscriber Overcharging Protection

Important In order for the Subscriber Overcharging Protection feature to be most effective, the operator should first enable sending the Release Access Bearer Request and next configure the cause codes for the SGSN for matching with received codes which enables the SGSN to include the Abnormal Release of Radio Link (ARRL) bit in the Release Access Bearer Request.

Important For details about all the commands listed in the Configuration sections below, refer to the *Command Line Interface Reference, StarOS Release 17*.

Enabling Release Access Bearer Request

The operator can control the sending of Release Access Bearer Request on Iu-Release for non-DT and non-ISR subscribers in 3G and on Ready-to-Standby or Radio-Status-Bad for non-ISR subscribers in 2G.

Use commands similar to those illustrated below to enable sending of the Release Access Bearer Request:

```
configure
    call-control-profile  profile_name
         release-access-bearer [ on-iu-release | on-ready-to-standby ]
        remove release-access-bearer [ on-iu-release | on-ready-to-standby
 ]
         end
```

Notes:

- **on-iu-release**: This optional keyword instructs the SGSN to send Release Access Bearer upon Iu-Release in a 3G network so that Release Access Bearer will be initiated for non-ISR and non-DT subscribers upon Iu-Release. For ISR and DT subscribers, Release Access Bearer will be initiated unconditionally.
- **on-ready-to-standby**: This optional keyword instructs the SGSN to send Release Access Bearer on Ready-to-Standby transition in a 2G network so that Release Access Bearer will be initiated for non-ISR subscribers on Ready-to-Standby transition. For ISR subscribers, Release Access Bearer will be initiated unconditionally.
- If no optional keywords are included with the **release-access-bearer** command, then the S4-SGSN applies Release Access Bearer for both 2G and 3G networks.

Configuring the Causes to Include ARRL in Release Access Bearer Request

In support of the subscriber overcharging protection functionality, the operator must configure all cause codes on the SGSN. If the SGSN receives a cause code via Iu/Gb interfaces that matches one of the cause codes configured on the SGSN, then the SGSN includes the ARRL (Abnormal Release of Radio Link) bit in the Release Access Bearer Request.

Configuring the Causes for 2G

Use the following configuration commands to define the cause codes received over the Gb interface for GPRS 2G service (BSSGP) when the SGSN initiates Release Access Bearer Request with ARRL bit set.

```
configure
  lte-policy
        cause-code-group group_name protocol bssgp
             radio-cause cause_code
             end
```

Notes:

- Under LTE Policy, the maximum number of cause code groups supported is 4. **Note** that this means that the total number of cause code groups available across all the services (SGSN+GPRS+MME) is 4.
- *group_name*: Enter an alphanumeric string up to 16 characters long.
- **bssgp**:
  - Accesses BSSGP Cause Code Group configuration mode for the commands to define the cause codes for the 2G service
  - Presents a prompt similar to the following: [local]sgsn-test(bssgp-cause-code)
  - **radio-cause**: A maximum of 16 BSSGP protocol radio cause codes can be defined per group. This command, in the new BSSGP Cause Code Group configuration mode, enables the operator to define multiple cause codes for the 2G service so that
    - if the BSSGP radio cause code configured by the operator matches with the radio cause received in the Radio Status message, and
    - if the Subscriber Overcharging Protection feature is enabled for 2G service in the GPRS-Service configuration (see command information above),
    - then the S4-SGSN includes ARRL (Abnormal Release of Radio Link) bit in Release Access Bearer Request message Initiated on Ready-to-Standby state transition.
  - Under each cause code group the maximum number of cause codes (ranap+bssgp+s1ap) that can be supported is 16.
  - *cause_code* : Enter an integer from 0 to 255 to identify a BSSGP protocol radio cause code, as defined in the *Radio Cause* section of the 3GPP TS 48.028 specification.

Note The SGSN does not support Enhanced Radio Status functionality therefore, the SGSN treats cause code values 0x03 and 0x04 as "Radio contact lost with MS". Therefore, the valid configurable cause codes values are 0, 1, and 2.

Configuring the Causes for 3G

Use the following configuration commands to define the cause codes received over the the Iu interface for UMTS 3G service (RANAP) when the SGSN initiates Release Access Bearer Request with ARRL bit set.

```
configure
  lte-policy
        cause-code-group group_name protocol ranap
             cause cause_code
             end
```

Notes:

- Under LTE Policy, the maximum number of cause code groups supported is 4. **Note** that this means that the total number of cause code groups available across all the services (SGSN+GPRS+MME) is 4.
- *group_name*: Enter an alphanumeric string up to 16 characters long.
- **ranap**:
  - Accesses the RANAP Cause Code Group configuration mode for the commands to define the cause codes for the 3G service
  - Presents a prompt similar to the following: [local]sgsn-test(ranap-cause-code)
  - **cause**: A maximum of 16 RANAP protocol cause codes can be defined per group. This command, in the new RANAP Cause Code Group configuration mode, enables the operator to define multiple cause codes for the 3G service so that
    - if the RANAP cause code configured by the operator matches with the radio cause received in the Iu-Release Request message, and
    - if the Subscriber Overcharging Protection feature is enabled for 3G service in the SGSN-Service configuration,
    - then the S4-SGSN includes ARRL (Abnormal Release of Radio Link) bit in Release Access Bearer Request message Initiated on Ready-to-Standby state transition.
  - Under each cause code group the maximum number of cause codes (ranap+bssgp+s1ap) that can be supported is 16.
  - *cause_code* : Enter an integer from 1 to 512 to identify a cause code. Valid options are listed in 3GPP TS 25.413 v11.5.0 (or later version), subsection on *Cause* in subsection for *Radio Network Layer Related IEs*.

Enabling Subscriber Overcharging Protection on S4

Configuring for 3G

Use commands similar to those illustrated below to

- enable or disable Subscriber Overcharging Protection feature for the S4-SGSN in the 3G network.
- associate a cause code group with the SGSN Service configuration.

```
configure
    context  context_name
         sgsn-service service_name
              s4-overcharge-protection ranap-cause-code-group group_name
              no s4-overcharge-protection
              end
```

Notes:

- *group_name*: Enter an alphanumeric string up to 16 characters long to identify the cause code group.

Important This CLI does not have any control over Release Access Bearer Initiation. If Release Access Bearer is going out of the S4-SGSN, the ARRL bit will be included if this CLI is enabled and if LORC (loss of radio coverage) is detected.

Configuring for 2G

Use commands similar to those illustrated below to

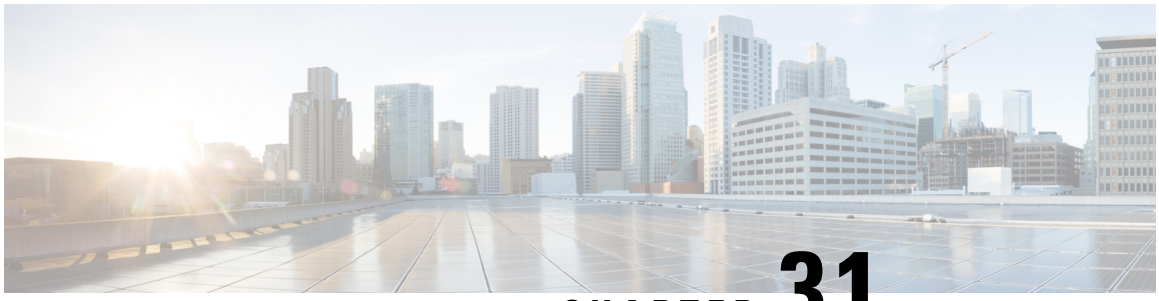
- enable Subscriber Overcharging Protection feature for the S4-SGSN in the 2G network.
- associate a cause code group with the GPRS Service configuration.

```
configure
    context  context_name
        gprs-service service_name
            s4-overcharge-protection bssgp-cause-code-group group_name
            end
```

Notes:

- *group_name*: Enter an alphanumeric string up to 16 characters long to identify the cause code group.

Important This CLI does not have any control over release access bearer initiation. If Release Access Bearer is going out of the S4-SGSN, the ARRL bit will be included if this CLI is enabled and if LORC (loss of radio coverage) is detected.



CHAPTER 31

MOCN for 2G SGSN

The SGSN has long supported Multi-Operator Core Network (MOCN) network sharing operations for the 3G SGSN. With Release 15.0, the SGSN now supports MOCN operations for 2G scenarios.

Important The MOCN network sharing functionality now requires a feature license for both 2G and 3G network sharing scenarios. Contact your Cisco representative for licensing information.

- Feature Description, on page 339
- How It Works, on page 341
- Configuring 2G MOCN, on page 345
- Monitoring and Troubleshooting 2G SGSN MOCN Support, on page 347

Feature Description

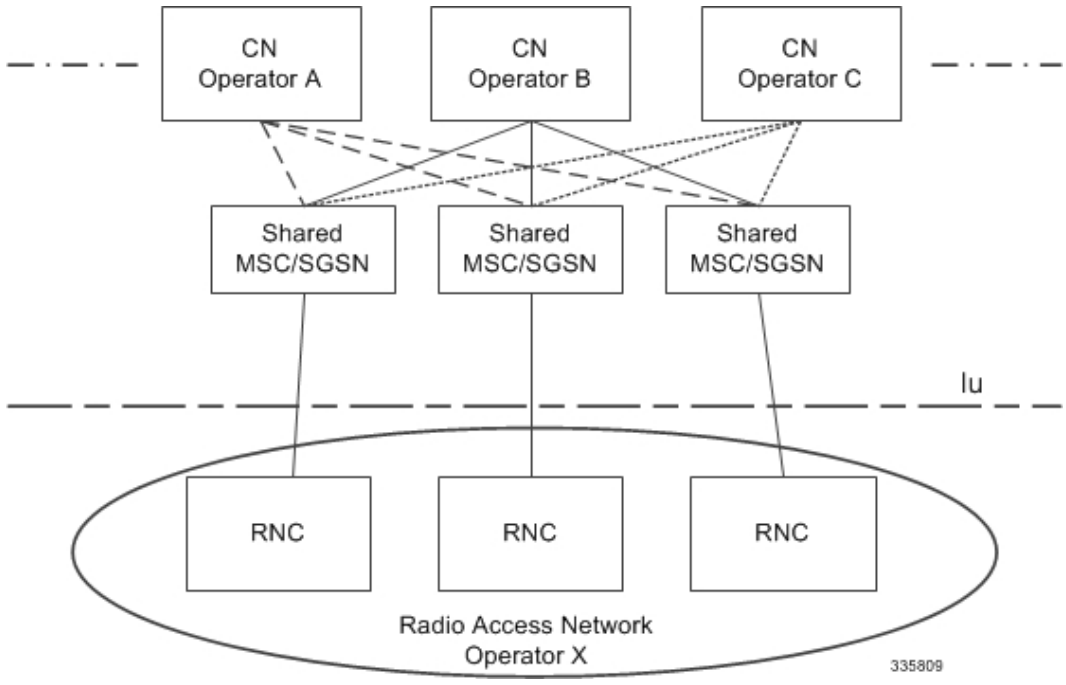
A Public Land Mobile Network (PLMN) is uniquely identified by the combination of a mobile country code and a mobile network code (the PLMN-Id). Sharing of radio resource and network nodes requires a PLMN network to support more than one than one PLMN-Id.

GPP defines two different configurations for supporting network sharing based on the resources being shared.

Gate Core Network (GWCN) Configuration

In this configuration, the radio access network and some core network services are shared among different operators. Each operator has its own network node for GGSN, HLR etc, while sharing SGSN and MSC with the rest of the radio network. The figure below depicts a GWCN configuration.

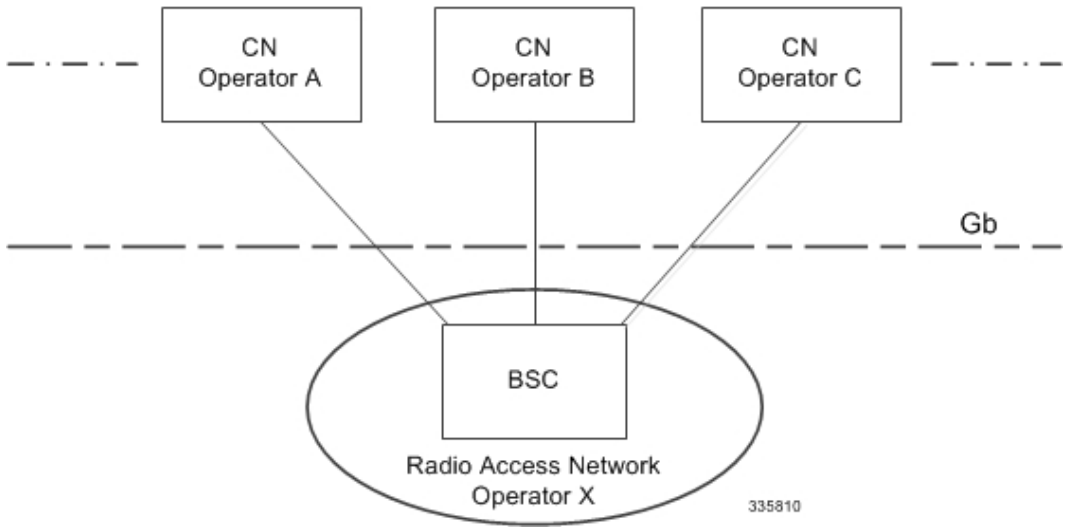
Figure 58: GWCN Configuration for Network Sharing



Multi Operator Core Network (MOCN) Configuration

In this configuration, the radio network is shared among different operators, while each operator maintains its separate core network. The figure below depicts a MOCN configuration.

Figure 59: MOCN Configuration



Relationships to Other Features

SGSN supports both MOCN and GWCN in 3G. GPRS. The MOCN feature can work with 3G network sharing. Inter-RAT from 3G to 2G in shared to non-shared area, and non-shared area to shared are supported.

To enable GPRS MOCN, the BSC also needs to support the GPRS MOCN. For "Supporting-MS", the MS shall have the capability to select the network from the PLMN details shared by the BSC. Currently, the SGSN supports only "non-supporting MS", thus the MS always selects the common PLMN.

How It Works

Automatic PLMN Selection in Idle Mode

This section briefly describes the normal PLMN selection procedure performed by MS along with modifications for network sharing.

Whenever MS is switched on or has just returned to network coverage after being out of coverage, it tries to select a network to register itself and receive network services. Traditionally, each network broadcasts its own PLMN-Id on common broadcast channels that are visible to all MSs in that area.

The MS starts by scanning for all the available radio networks in that area and creating an Available PLMN list. It then refers to the Equivalent PLMN list and Forbidden PLMN list (stored on its SIM) to prioritize the Available PLMN list. Once this prioritized PLMN list is available, the MS attempts registration with a PLMN based on priority.

With network sharing a single radio network is shared by more than one network operator. Information about the availability of multiple operators must be propagated to the MS so that it can correctly select a home or equivalent network from all available networks.

To advertise availability of multiple core network operators on a single radio network, broadcast information has been modified to contain a list of PLMN-Ids representing core network operators sharing the particular radio network. The traditional PLMN-Id broadcast by a radio network before network sharing support was available is known as a "common PLMN Id".

An MS that does not support network sharing (a non-supporting MS) sees only the "common PLMN Id", while an MS supporting network sharing (a supporting MS) is able to see the list of PLMN-Ids along with "common PLMN Id".

A supporting MS is responsible for selecting an appropriate core network, while the RNC and SGSN will help select an appropriate core network for a non-supporting MS.

MOCN Configuration with Non-supporting MS

In this scenario, only the radio network is shared by different network operators while each operator manages its own SGSN and the rest of the core network. The MS does not support network sharing it is unable to understand the modified broadcast information and would always choose the PLMN based on the advertised "common PLMN-Id".

The SGSN performs the following steps:

1. Extract the subscriber's IMSI.
    - If it is available, use IMSI in a BSSGP UL-UNITDATA message.

- For inter-SGSN RAU and a P-TMSI Attach Request, retrieve the IMSI from the old SGSN or the MS by doing an Identity Procedure.

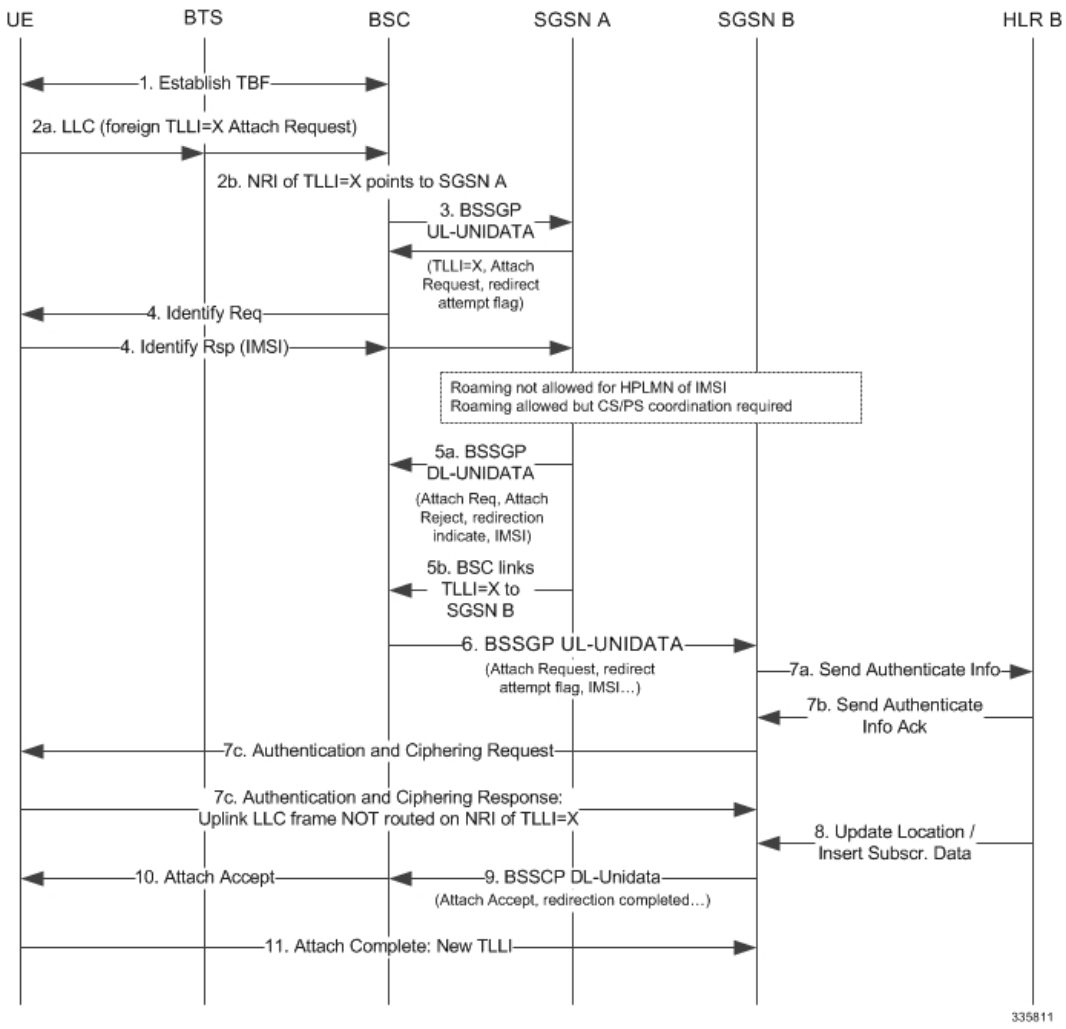
2. Based on the MCC-MNC from the IMSI, apply roaming control.
3. If the subscriber can be admitted in the SGSN, send a response message (Attach-Accept or RAU-Accept) with an Redirection-Completed IE via BSSGP UL-UNITDATA.
4. If the subscriber cannot be admitted in the SGSN, send a BSSGP DL-UNITDATA message to the BSC with a redirection indication flag set containing the reject cause, the attach reject message, and the original attach request message received from the UE. The IMSI is also included in the message.

Architecture

Redirection in GERAN with MOCN Configuration

The figure below illustrates the information flow for this configuration.

Figure 60: Information Flow for Redirection in GERAN (PS Domain)



1	Establish the TBF (Temporary Block Flow).
2	The BSC receives the LLC frame with foreign [or random] TLLI =X. The BSC works in a Shared RAN MOCN, and, therefore, forwards the message in a BSSGP ULUNITDATA message with an additional redirect attempt flag set. The flag indicates that the SGSN shall respond to the attach request with a BSSGP DL-UNITDATA message providing when relevant a redirection indication flag set to inform the BSC that a redirection to another CN must to be performed. The selection of a CN node is based on NRI (valid or invalid) or random selection. The mechanism defined for Gb-Flex in TS 23.236 [8] is used.
3	The SGSN receives the BSSGP UL-UNITDATA message with the redirect attempt flag set. It then knows it may have to provide the BSC with a redirection indication flag set or a redirection completed flag set.
4	The SGSN needs the IMSI of the UE retrieves it either from the old SGSN or from the UE as in this example. By comparing the IMSI with the roaming agreements of the CN operator, SGSN A discovers that roaming is not allowed or that roaming is allowed but CS/PS coordination is required. The Attach procedure is aborted.
5	5a) A BSSGP DL-UNITDATA message is sent back to the BSC with a redirection indication flag set containing the reject cause, the attach reject message, and the original attach request message received from the UE. The V(U) shall also be included in the message. The IMSI is also included in the message. The BSC selects a SGSN B in the next step. The already tried SGSN A is stored in the BSC during the redirect procedure so that the same node is not selected twice. 5b) The BSC makes a short-lived binding between the TLLI =X and SGSN ID so that it points to SGSN B.

6	The BSC sends a new BSSGP UL-UNITDATA to the next selected SGSN B with the original attach request message (for CS/PS coordination the BSSGP UL-UNITDATA may also be sent back to the first SGSN depending on the outcome of the coordination). Redirect attempt flag is set and IMSI is included to avoid a second IMSI retrieval from the UE or old SGSN and to indicate that PS/CS domain coordination has been done in BSC (if enabled in BSC). The V(U) shall also be included in the message. The SGSN B receiving the message starts its attach procedure.
7	SGSN B does support roaming for the HPLMN of the IMSI authentication is done and RAN ciphering is established. The value of V(U) in SGSN-B is set according to the received value from BSC. Uplink LLC frames are routed to SGSN B despite the NRI of the TLLI=X pointing to SGSN A.
8	SGSN B updates the HLR and receives subscriber data from HLR Subscriber data allows roaming, and the SGSN B completes the attach procedure.This includes the assignment of a new P-TMSI with an NRI that can be used by BSC to route subsequent signalling between UE and the correct SGSN (Gb-Flex functionality).
9	A BSSGP DL-UNITDATA Attach accept message is sent to BSC with the Redirection Completed flag set. The BSC knows that the redirect is finished and can forward the Attach Accept message to the UE and clean up any stored redirect data. SGSN B is allowed to reset the XID parameter only after the Attach Request is accepted.
10	The Attach Accept is forwarded to the UE. The UE stores the P-TMSI with the Gb-Flex NRI to be used for future signalling, even after power off.
11	UE responds with an Attach Complete message (P-TMSI [re-]allocation if not already made in Attach Accept). The Attach Complete uses the new TLLI. After this, the BSS releases the binding between TLLI=X and SGSN B.

If the BSC finds no SGSNs to redirect to after receiving a BSSGP DL-UNITDATA message with the Redirection Indication flag set, it compares the cause code with cause codes from other BSSGP DL-UNITDATA messages it has previously received for this UE. A cause code ranking is done and the "softest" cause code is chosen. The corresponding saved Attach Reject message is returned to the UE.

Each CN node that receives a BSSGP UL-UNITDATA, runs its own authentication procedure. This may in some rare situations cause the UE to be authenticated more than once. However, the trust-model used is that

one CN operator shall not trust an authentication done by another CN operator. This is not an optimal usage of radio resources, but given the rare occurrence of this scenario, the increased signalling is insignificant.

During the redirect procedure the BSC keeps a timer, which corresponds to the UE timer for releasing the RR connection (20 seconds). If the BSC when receiving a BSSGP DL-UNITDATA message with the Redirection Indication flag set finds that there is insufficient time for another redirect, further redirect attempts are stopped (for this Attach Request message). The UE will repeat its Attach Request four times (each time waiting 15 seconds before it re-establishes the RR connection for another try).

Standards Compliance

Support for 2G MOCN functionality on the SGSN complies with the following standards:

- 3GPP TS 23.251 Network Sharing: Architecture and functional description
- 3GPP TS 40.018 version 10.7.0 Release 10 BSSGP layer specification
- 3GPP TS 44.064 Mobile Station - Serving GPRS Support Node (MS-SGSN) Logical Link Control (LLC) Layer Specification
- 3GPP TS 24.008 Mobile radio interface Layer 3 specification Core network protocols

Configuring 2G MOCN

For details about the commands listed below, refer to the *Command Line Interface Reference* for the appropriate release.

GPRS MOCN Configuration

gprs-mocn

The SGSN mode **gprs-mocn** command enables or disables 2G MOCN support.

```
config
  sgsn-global
    gprs-mocn
    end
```

Verifying gprs-mocn Configuration

From the Exec mode, run the **show sgsn-mode** command and look for the line:

```
Multi Operator Core NW (MOCN)   : Enabled
```

Common PLMN-Id and List of PLMN Ids Configuration

plmn id

The following command sequence configures the common PLMN-Id and an optional list of dedicated PLMN-Ids in the GPRS service.

```
config
  context ctxt_name
```

```
    gprs-service  gprs_srvc_name
      plmn id mcc mcc_id mnc mnc_id  [ network-sharing common-plmn mcc
mcc_id mnc mnc_id [ plmn-list mcc mcc_id mnc mnc_id [ mcc mcc_id mnc mnc_id ] +
 ] ]
       end
```

Notes:

- + in the syntax above indicates that the mcc/mnc combination can be repeated as often as needed to define all PLMN-Ids needed in the list.

Verifying plmn id Configuration

From the Exec mode, run the **show gprs-service** command, including the **name** keyword to identify the specific GPRS service you configured above, and check the output for the following lines:

```
Network Sharing              : <Enabled/Disabled>
Common Plmn-id               : MCC: <mcc_id>, MNC:  <mnc_id>
Local PLMNS:
PLMN                         : MCC: <mcc_id>, MNC:  <mnc_id>
```

Network Sharing Configuration

network-sharing cs-ps-coordination

Next, the operator should configure cs-ps-coordination checking explicitly for homer or roamer subscribers and for the failure-code to be sent when the SGSN asks the BSC to perform CS-PS coordination.

The **network-sharing** command enables or disables the cs-ps coordination check for **homer** or **roamer**. It is also used to set the failure code that will be sent while the SGSN is requesting the BSC to provide CS-PS coordination.

```
config
  context <ctxt_name>
    gprs-service <gprs_srvc_name>
      network-sharing cs-ps-coordination [ roamer | homer | failure-code
 gmm-cause ]
       end
```

Notes: Variations of the network sharing command can be used to adjust the CS-PS configuration.

- **[no] network-sharing cs-ps-coordination roamer** enables/disables the cs-ps-coordination check for a roamer.
- **[no] network-sharing cs-ps-coordination homer** enables/disables the cs-ps-coordination check for a homer.
- **network-sharing cs-ps-coordination failure-code** *gmm-cause* sets the gmm cause value to be sent while cs-ps-coordination is required. This setting applies to both homer and roamer.
- **default network-sharing cs-ps-coordination** sets the cs-ps-coordination parameters to default. By default, checking for cs-ps-coordination is enabled for homer and roamer. The default failure code is 0xE.

Verifying network-sharing Configuration

From the Exec mode, run the **show gprs-service** command, including the **name** keyword, and check the output for the following lines:

```
CS/PS Co-ordination homer    : <Enabled/Disabled>
CS/PS Co-ordination roamer   : <Enabled/Disabled>
CS/PS Co-ordination failcode : <valid gmm cause>
```

network-sharing failure-code

The following command sequence sets the failure code that is used by GPRS MOCN if no failure cause is available when the SGSN sends an Attach/RAU Reject message

```
config
  context ctxt_name
    gprs-service gprs_srvc_name
      network-sharing failure-code gmm-cause
      end
```

Default network sharing failure-code is 7.

Verifying Failure Code Configuration

From the Exec mode, run the **show gprs-service name** command and look for the following line:

```
Network-sharing Failure-code : <gmm-cause>
```

Monitoring and Troubleshooting 2G SGSN MOCN Support

The output generated by the following show commands will assist you in monitoring and troubleshooting 2G SGSN MOCN support.

show sgsn-mode

From the Exec mode, run the **show sgsn-mode** command and look for the following line:

```
Multi Operator Core NW (MOCN)   : <Enabled/Disabled>
```

This line indicates whether or not MOCN has been enabled.

show gprs-service name

From the Exec mode, run **show gprs-service name** *gprs-service-name* and check the output for the following lines:

```
CS/PS Co-ordination homer    : <Enabled/Disabled>
CS/PS Co-ordination roamer   : <Enabled/Disabled>
CS/PS Co-ordination failcode : <valid gmm cause>
```

The above lines display details regarding cs/ps coordination for homer and roamer, as well as the GMM cause to be sent in the Reject message when cs/ps coordination is required.

```
Network-sharing Failure-code : <gmm-cause>
```

The above line displays the GMM cause to be sent as a Reject cause only when no valid cause code was derived while sending the Reject message. This gmm-cause is used for non-cs/ps coordination Rejects.

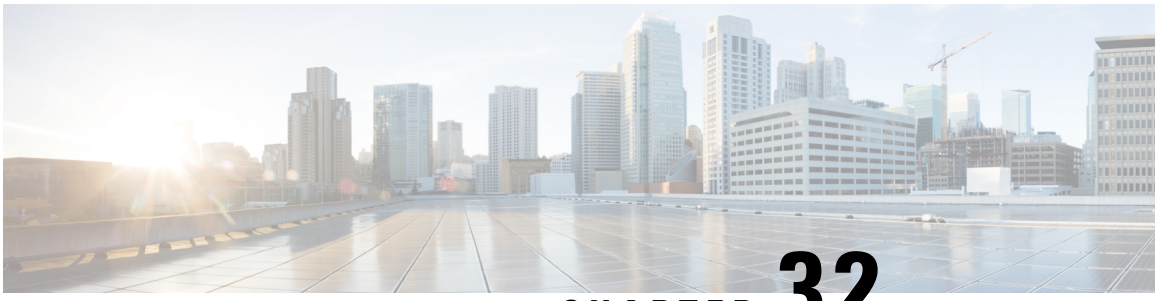
```
Network Sharing              : <Enabled/Disabled>
Common Plmn-id               : MCC: <mcc_id>, MNC:  <mnc_id>
Local PLMNS:
PLMN                         : MCC: <mcc_id>, MNC:  <mnc_id>
```

The above lines display details about the GPRS service with MOCN enabled, including the configured common PLMN-id and the list of local PLMN Ids.

show gmm-sm statistics verbose

From the Exec mode, run **show gmm-sm statistics verbose** and look for the following lines:

```
GPRS MOCN Attach Statistics
 Total Redirection Attempts Rcvd:
       Redirection attempts rcvd with bsgp imsi:         <value>
       Redirection attempts rcvd without bssgp imsi:     <value>
 Total Redirection Completes Sent:                       <value>
       Successful Redirection completes sent:            <value>
       Failure Redirection completes sent:               <value>
 Total Redirection Indications Sent:                     <value>
       Illegal PLMN:                                     <value>
       Illegal LA:                                       <value>
       No roaming:                                       <value>
       No gprs PLMN:                                     <value>
       No cell in LA:                                    <value>
       CS/PS Coord Rqrd:                                 <value>
       Others:                                           <value>

GPRS MOCN RAU Statistics
 Total Redirection Attempts Rcvd:                        <value>
       Redirection attempts rcvd with bssgp imsi:        <value>
       Redirection attempts rcvd without bssgp imsi:     <value>
 Total Redirection Completes Sent:                       <value>
       Successful Redirection completes sent:            <value>
       Failure Redirection completes sent:               <value>
 Total Redirection Indications Sent:                     <value>
       Illegal PLMN:                                     <value>
       Illegal LA:                                       <value>
       No roaming:                                       <value>
       No gprs PLMN:                                     <value>
       No cell in LA:                                    <value>
       CS/PS Coord Rqrd:                                 <value>
       Others:                                           <value>
```



CHAPTER 32

MTC Congestion Control

The SGSN's MTC (mobile type communications) Congestion Control feature implements General NAS-level congestion control and APN-based congestion control for both Session Management (SM) and Mobility Management (MM) in the SGSN. As well, the functionality associated with this feature also provides support for configuring and sending an Extended T3312 timer value to the MS.

This is an optional licensed feature. Speak with your Cisco Customer Representative for information about obtaining an MTC Feature license.

- Feature Description, on page 349
- How It Works, on page 350
- Configuring MTC Congestion Control, on page 356
- Monitoring MTC Congestion Control, on page 365

Feature Description

Congestion is detected based on various threshold-configurable parameters, such as (but not limited to) system CPU utilization, system memory utilization, service CPU utilization. This feature enables the operator to determine the SGSN's response to various congestion scenarios.

The MTC Congestion Control functionality gives the operator control over the congestion threshold settings and the actions taken in response to congestion. The operator defines a set of congestion actions in a congestion-action-profile. The selected actions are executed when congestion is detected.

Congestion control can be enabled as:

- General congestion control - applicable only for Mobility Management messages.
- APN-based congestion control for Mobility Management
- APN- based congestion control for Session Management

There are three levels of system-detected congestion: critical, major, and minor. The percentage at which these levels are hit is controlled via threshold configuration.

The operator defines the SGSN's congestion response actions for new calls, active calls, and SM-messages in congestion-action-profiles and association those congestion-action-profiles with the various congestion level.

In addition to system-detected congestion, the SGSN also provides a management option to trigger congestion. This option can be useful when testing system readiness and response.

Relationships

Other SGSN Features: Low Access Priority Indicator (LAPI) in S-CDRs. The SGSN allows for the use of the LAPI bit in S-CDRs of the custom24 dictionary. Use of this functionality is CLI controlled. For details about this functionality, refer to the *GTPP Interface Administration and Reference for StarOS Release 17*.

Other Products: While specific operations may vary, MTC Congestion Control functionality is also supported by the MME. For details, refer to the *MME Administration Guide for StarOS Release 17*

How It Works

SGSN Congestion Control

The deciding parameter for triggering congestion control in the SGSN will be the overall system CPU utilization, service CPU utilization, and system memory utilization. This information will be periodically monitored by the resource manager (ResMgr) which will informed the SGSN's IMSIMgr.

Mobility Management (MM) Congestion Control - For congestion control of MM messages, system-detected congestion is based on

- system CPU utilization,
- service CPU utilization
- system memory utilization

Session Management (SM) Congestion Control - For congestion control of session management messages, system-detected congestion is based only on system CPU utilization.

The MTC Congestion Control functionality enables the operator to configure different congestion-action-profiles, which applies at different threshold levels.

APN-level Congestion Control for MM

APN-level congestion control for mobility management (MM) is applied to those UEs that have subscribed for APNs configured for congestion control.

During system-level congestion, if the chosen congestion-action-profile has the "apn-based" parameter configured as enabled, then APN-based congestion control is applied.

Once the SGSN receives the subscription for a subscriber, if any of the subscribed APNs are configured for congestion control, then the call is rejected with a backoff timer value sent to the UE in the Reject message according to the following scenario:

- A random MM backoff timer (T3346) value, derived from the selected min-max range configured for that APN, is sent to the UE in Reject messages.
  1. The minimum and maximum range for the MM backoff timer value is selected from the APN Profile configuration.
  2. If the timer is not configured at the APN Profile level, then the SGSN takes the MM backoff timer as configured at either the GPRS or SGSN service level.
  3. If timer is not configured at the service level, then the default values (min-15 max-4320) are applied.

- If the subscriber retries Attach when the backoff timer is running, then the SGSN rejects the Attach, sending the remaining time for backoff in the Reject message.
- If the subscriber retries Attach with a change in signaling priority when the backoff timer is running, then the SGSN accepts the Attach, based on configuration for example,

  1. if Reject is associated with LAPI and APN-based parameters,
  2. then subscriber sends a message without LAPI
  3. then the Attach is accepted.

- If the subscriber retries Attach while backoff timer is running and the SGSN is not under congestion, then the backoff timer is cleared and the call Accepted.
- If the subscriber retries Attach after backoff timer expires, and if the SGSN continues under congestion, then a new backoff timer value is assigned and sent in the Attach Reject message.

APN-level Congestion Control for SM

APN-level congestion control for session management (SM) is applicable to both activation and modification types of SM messages. Detection of SM APN-based congestion is determined according to system utilization or O&M (triggered) congestion at any one of three levels: critical, major, minor with the following possible ropiness:

If congested:

- If the configured response action indicates the low access priority indicator (LAPI), then only SM messages with LAPI are rejected during congestion. If LAPI is not configured then all SM messages are rejected.
- A random SM backoff timer (T3396) value, derived from the selected min-max range configured for that APN, is sent to the UE in Reject messages.

  1. The minimum and maximum range for the SM backoff timer value is selected from the APN Profile configuration.
  2. If the timer is not configured at the APN Profile level, then the SGSN takes the SM backoff timer as configured at either the GPRS or SGSN service level.
  3. If timer is not configured at the service level, then the default values (min-15 max-4320) are applied.

- If the UE attempts to retry before expiry of the SM backoff timer and if the SGSN is still congested, then a new random value is included in the rejection message.
- A UE that is attached as a LAPI device may override its priority for PDN activation / secondary PDP activation (if the UE is a dual access priority device). SGSN will only consider the value of LAPI received in PDP Activation message for applying congestion control on activation procedure.
- If a LAPI UE has activated a PDN without LAPI (i.e., the UE is dual access priority capable) but is sending PDP Modification Request with LAPI bit, then the SGSN will apply congestion control for the modification procedure if LAPI-based APN congestion control for SM messages is configured.
- Dual access priority devices can send PDN Activation with LAPI but subsequent SM procedures without LAPI. In this scenario, SGSN does not apply congestion based on LAPI.
- For LAPI devices, the SGSN sends LAPI indication to the AAA module for inclusion in S-CDRs if the appropriate GTPP dictionary is configured.

Support for the Extended T3312 Timer

The SGSN supports sending the Extended T3312 timer value for Attach Accept and/or RAU Accept messages if the MS indicates support for extended periodic timer in the MS Network Feature Support.

Important The SGSN will not send an Extended T3312 value if offloading is enabled for that subscriber.

For both Gn-SGSN and S4-SGSN, a longer periodic RAU timer can be assigned to the M2M UEs based on subscription. The Subscribed-Period-RAU-TAU-Timer AVP is supported for the "Subscribed Period TAU/RAU Timer" via the SGSN's S6d interface. The Subscribed Period TAU/RAU Timer value can be included in the ISD (Insert Subscriber Data) from the HLR or in the ULA (Update Location Answer) from the HSS.

The maximum value for a standard T3312 timer value is 186 minutes and the new Extended T3312 timer maximum value is 18600 minutes. Using the longer value for routing area updates reduces network load from periodic RAU signaling.

Important Now, despite enabling the Extended T3312 timer in the SGSN's configuration, the SGSN may be prevented from sending the Extended T3312 timer value in messages as the SGSN also supports the "Subscribed Periodic TAU/RAU Timer Withdrawn" flag.

The SGSN also supports the Subscribed Periodic TAU-RAU Timer Withdrawn Flag in MAP DSD messages. When the flag is set in MAP DSD messages, it indicates to the SGSN that the subscriber no longer has a subscription for the "subscribed periodic RAU/TAU timer" (Extended T3312 timer) value, so

- the SGSN will delete any subscribed periodic RAU/TAU timer value information when it is received from the HLR, and
- the SGSN will no longer send Extended T3312 in Attach/RAU Accept messages for that subscriber even if the sending of the Extended T3312 is configured.

Limitations

The following resources for congestion detection are not yet supported:

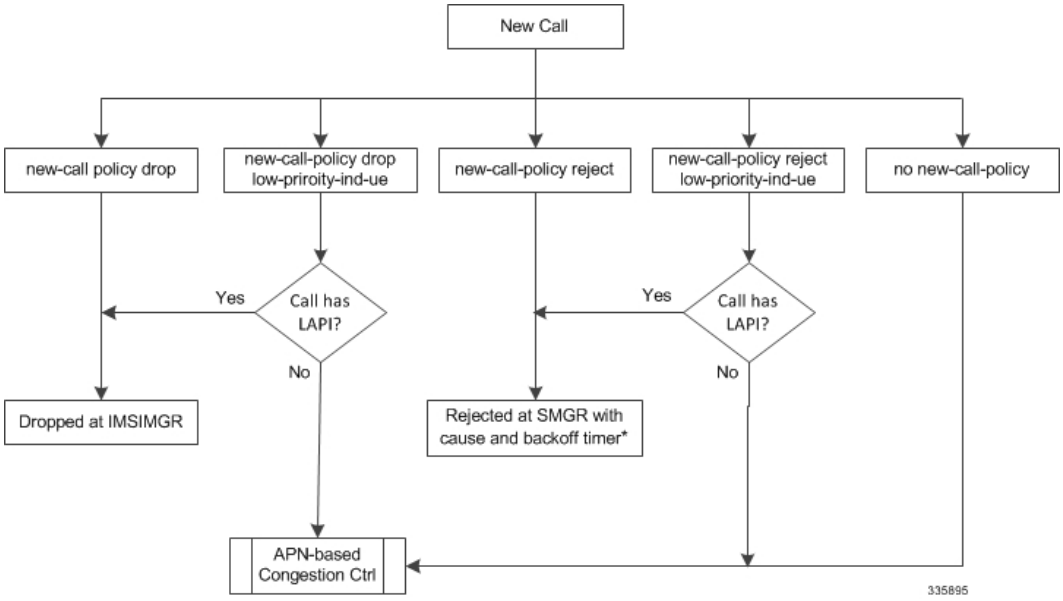
- License utilization
- Max session count

Flows for SGSN Congestion Control

New Call Policy for Congestion

The following flowchart explains how new calls are handled, during congestion, based on configuration.

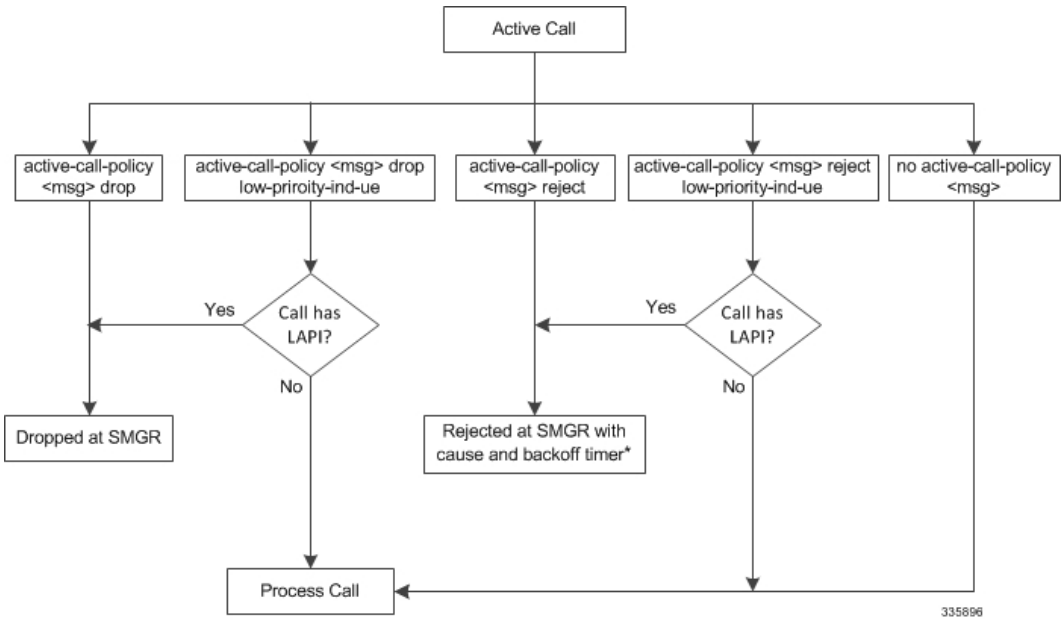
Figure 61: New Call Handling during Congestion



Active Call Policy for Congestion

The following flowchart explains how active calls are handled, during congestion, based on configuration.

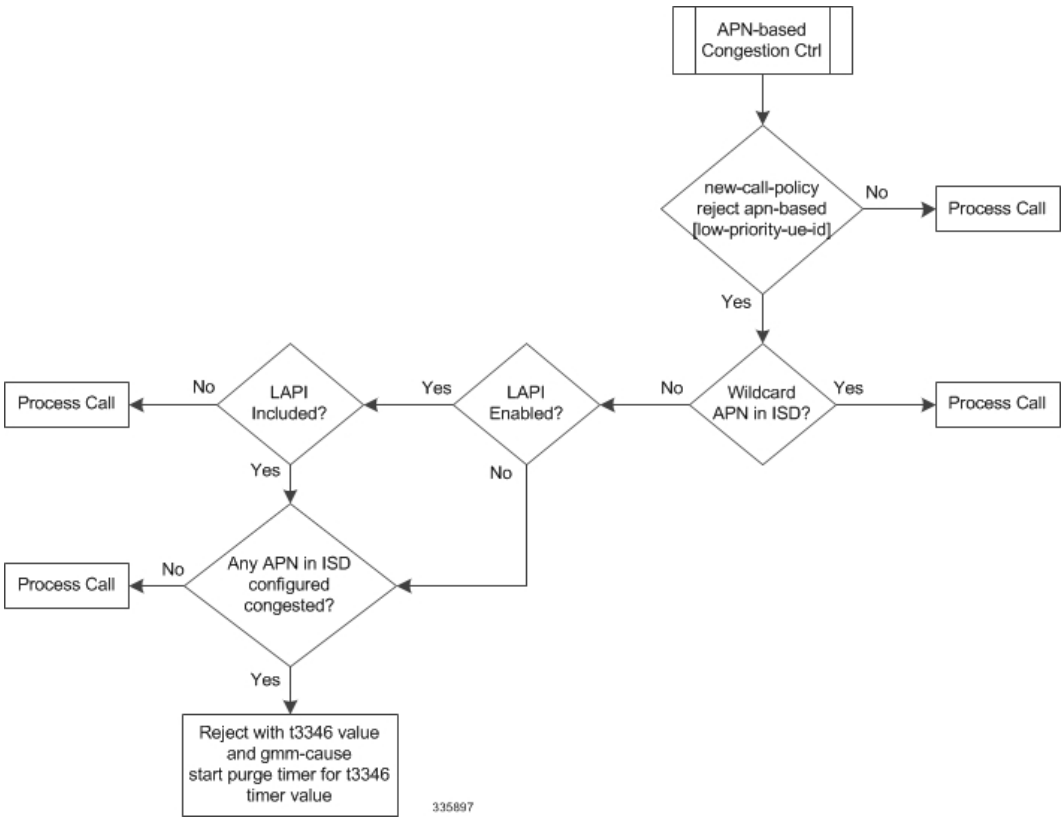
Figure 62: Active Call Handling during Congestion



Flows for APN-level Congestion Control for MM

The following flow chart illustrates the APN-level congestion control for mobility management.

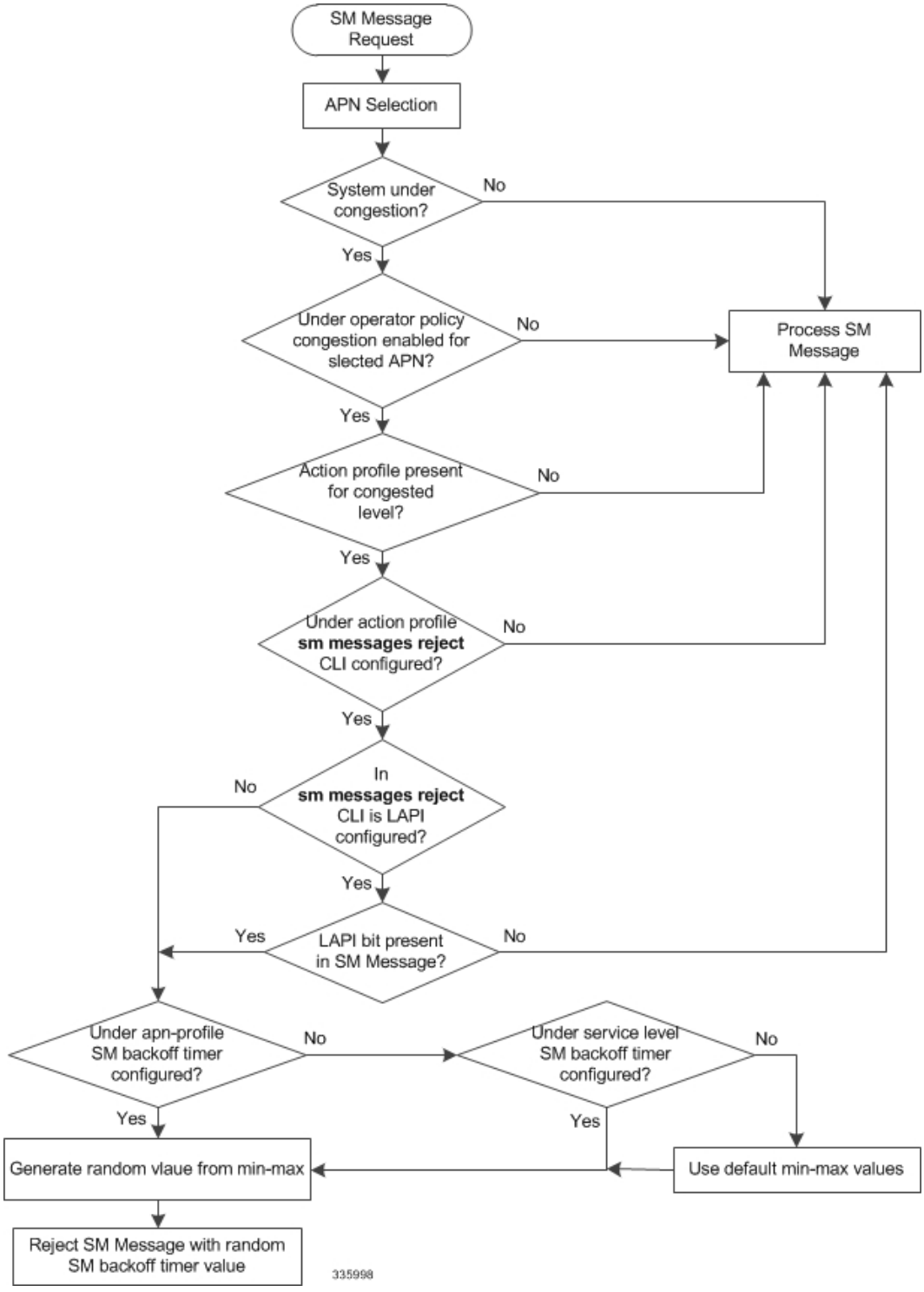
Figure 63: APN-level Congestion Control for MM



Flows for APN-level Congestion Control for SM

The following flow chart illustrates the APN-level congestion control for session management.

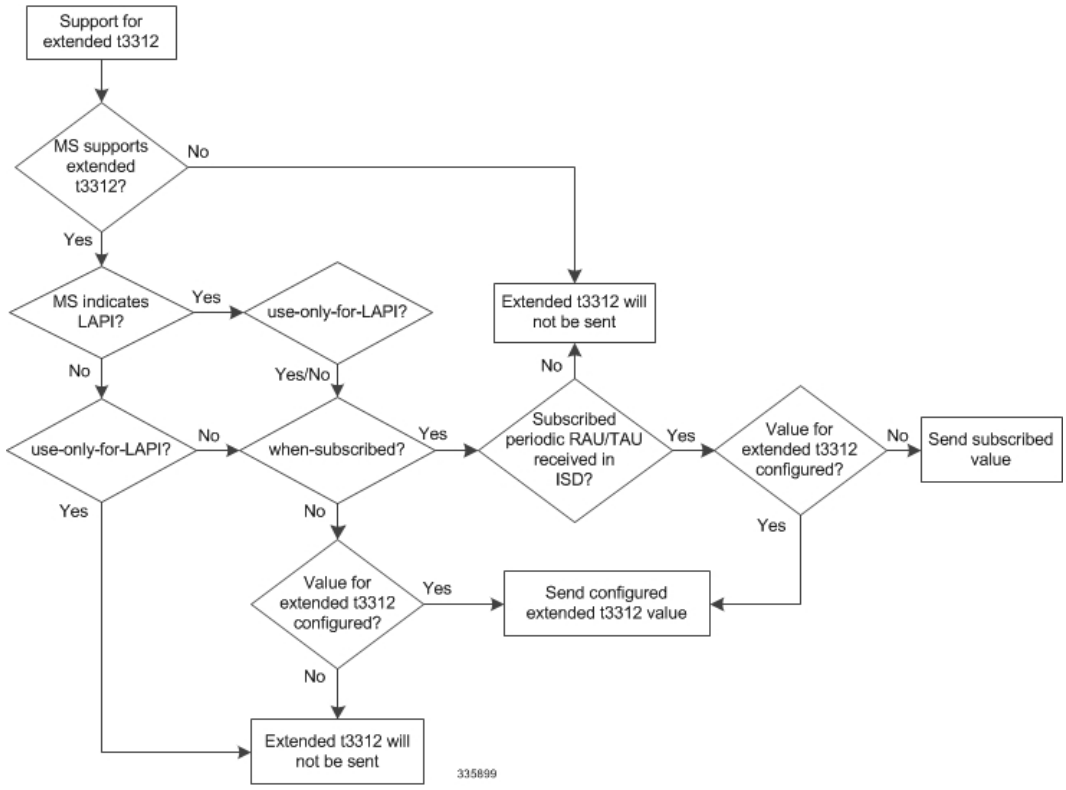
Figure 64: APN-level Congestion Control for SM



Handling Value for Extended T3312 Timer

The following flow chart explains how and when t3312 extended value is sent in Attach and RAU Accepts

Figure 65: Handling Value for Extended T3312 Timer



Standards Compliance

The MTC Congestion Control feature only implements some of the MTC overload control mechanisms defined by the 3GPP but for those it implements, they are in compliance with the 3GPP TS23.060 R10 specification.

Configuring MTC Congestion Control

This section illustrates the required and optional configuration steps for setting up MTC Congestion Control on the SGSN.

The following is broken into the following configuration components:

- Enabling Global-level Congestion Control
- Configuring System-detected Congestion Thresholds
- Configuring SGSN Congestion Control
- Configuring APN-based Congestion Control
- Configuring Extended T3312 Timer
- Configuring Backoff Timers

- Configuring O&M Triggered Congestion

Important Details for each of the commands listed in the following sections are available in the *Command Line Interface Reference*.

Enabling Global-level Congestion Control

The following configuration is ***mandatory*** to enable congestion control on the SGSN.

The following configuration accomplishes several tasks, all of which must be performed to enable congestion control on the SGSN.

1. Enables or disables global-level congestion control for the SGSN and the IMSIMgr.
2. Associates the SGSN's congestion-response action-profile with each of the three possible levels of congestion - critical, major, and minor.

```
configure
  congestion-control
  congestion-control policy { critical | major | minor } sgsn-service
action-profile action_profile_name
  end
```

Notes:

- **sgsn-service**: Identifies the StarOS service type in this case, the SGSN (Gn-SGSN and/or S4-SGSN).
- *action_profile_name*: Enter a string of 1 to 64 alphanumeric characters to identify the congestion-action-profile to associate with the congestion-control policy. *We recommend* that you remember the name(s) that you assign so that you will have them when you actually create and configure your congestion-action-profiles.
- Repeat the **congestion-control policy** command as needed to associate one or more congestion-action-profile(s) with each congestion level.

Verifying the Global-level Congestion Control Configuration

Use the command illustrated below to verify that congestion control has been enabled and to view the SGSN's congestion-control policy with the congestion-action-profile names association with the level of congestion severity.

The following command is entered from the Exec mode:

```
[local]SGSN1-NH show congestion-control configuration
```

The following provides a sample of the display generated by the command illustrated above:

```
[local]R16sgsn-Sim show congestion-control configuration
Congestion-control: enabled

Congestion-control Critical threshold parameters
  system cpu utilization:               80
...
...
Congestion-control Policy
...
   sgsn-service:
     Minor    Action-profile : ActProf6
```

Configuring System-detected Congestion Thresholds

The following configuration accomplishes several tasks, all of which are *optional*:

1. Associates utilization threshold(s) with a congestion severity level - critical, major, minor.
2. Enables detection based on System CPU Usage.
3. Enables detection based on System Memory Utilization.
4. Enables detection based on Service Control CPU Utilization

```
configure
  congestion-control threshold system-cpu-utilization { critical | major
 | minor } threshold_value
  congestion-control threshold system-memory-utilization { critical |
major | minor } threshold_value
  congestion-control threshold service-control-cpu-utilization { critical
 | major | minor } threshold_value
  end
```

Notes:

- *threshold_value*: Enter an integer from 1 to 100 to define a percentage threshold value.
- For congestion control of mobility management messages, any of the above parameters can be configured.
- For congestion control of session management messages, only "system-cpu-utilization" is supported.
- At present, only APN-based congestion control is applicable for session management messages.

Verifying System-detected Congestion Thresholds Configuration

Use the command illustrated below to verify thresholds you may have configured with the commands illustrated above. The display will include a section for Critical threshold parameters, Major threshold parameters, and Minor threshold parameters. The following display only illustrates samples for Critical threshold parameters.

The following command is entered from the Exec mode:

```
[local]SGSN1-NH show congestion-control configuration
```

The following provides a sample of the display generated by the command illustrated above:

```
[local]R16sgsn-Sim show congestion-control configuration
Congestion-control: enabled
Congestion-control Critical threshold parameters
  system cpu utilization:     80
  service control cpu utilization: 80
  system memory utilization: 80
  message queue utilization: 80
  message queue wait time: 5 seconds
  port rx utilization: 80
  port tx utilization: 80
  license utilization: 100
  max-session-per-service utilization: 80
  tolerance limit: 10
```

Notes:

- At this time, you are only setting the values for the first three displayed parameters.

Configuring SGSN Congestion Control

The following configuration is ***mandatory*** to enable congestion control on the SGSN.

Important Remember, congestion control must *also* be enabled with the **congestion-control** command in the Global Configuration mode. The following is not sufficient to enable congestion control on the SGSN.

The following configuration accomplishes several tasks, all of which must be performed to enable congestion control on the SGSN.

1. Enables or disables SGSN-level congestion control.
2. Creates and configures congestion-action-profiles.

```
configure
    sgsn-global
         congestion-control
              congestion-action-profile action_profile_name
                   active-call-policy { rau | service-req } { drop |
reject } [ low-priority-ind-ue ]
                  new-call-policy { drop | reject } [ low-priority-ind-ue
 ] [ apn-based ]
                   sm-messages reject [ low-priority-ind-ue ] [ apn-based
 ]
                 end
```

Notes:

- **congestion-control**: Opens the Congestion-Control configuration mode, in which the congestion control action-profile can be created.
- **congestion-action-profile** *action_profile_name*: Enter a string of 1 to 64 alphanumeric characters to create or identify a congestion-action-profile and/or to open the Congestion-Action-Profile configuration mode, which accesses the commands that define the congestion responses for:
  - active calls
  - new calls
  - SM messages
- A maximum of 16 action-profiles can be defined.
- **active-call-policy**: This command instructs the SGSN to drop or reject any active call messages when congestion occurs during an active call. The active call instructions in the congestion-action-profile can be refined to only drop or reject active call messages with LAPI.
- **new-call-policy**: This command instructs the SGSN to drop or reject any new calls (Attach Request messages or new Inter SGSN RAU messages) if new call messages are received during congestion. The new call instructions in the congestion-action-profile can be refined to only drop or reject new call messages with low access priority indicator (LAPI).
- **sm-messages**: This command instructs the SGSN to reject any SM signaling messages (activation or modification) during congestion. The congestion-action-profile parameter can be refined to only reject SM signaling messages with LAPI.

Important For SM congestion to work, the **apn-based** option must be configured with the **sm-messages reject** command .

- **rau | service-req** : Defines congestion response for Routing Area Update messages or Service Request messages.
- **drop | reject**: Defines the congestion response action, drop or reject, to be taken when RAU or Service Request messages are received during an active call.
- **low-priority-ind-ue**: Instructs the SGSN to only take defined action if messages include LAPI.
- **apn-based**: Instructs the SGSN to reject a new call based on the subscribed APN *if* congestion control is configured for that APN under an applicable Operator Policy.
- If both the LAPI and APN-based options are included in the action-profile, then the call event will only be rejected if both conditions are matched.

Verifying the SGSN Congestion Control Configuration

Use the command illustrated below to verify the configuration created with the commands in the *Configuring SGSN Congestion Control* section above.

The following command is entered from the Exec mode. NOTE that the entire command must be typed, tabbing does not function for this command.

```
[local]SGSN1-NH show sgsn-mode
```

The following provides a sample of the display generated by the command illustrated above:

```
[local]R16sgsn-Sim show sgsn-mode
Congestion Action Profile
-------------------------
Congestion Action Profile Name:profile1
New Call Policy               :Reject only LAPI devices
Active Call Policy            :
Routing Area Update           :Not configured
Service Request               :Reject
APN Based Congestion Control  :
MM messages                   :Not configured
SM messages                   :Reject
```

Configuring APN-based Congestion Control

The following configuration associates congestion control functionality with a specific APN so that congestion responses can be applied per APN.

```
configure
    operator-policy name  op_policy_name
         apn network-identifier apn_name congestion-control
         end
```

Notes:

- *op_policy_name*: Enter a string of 1 to 64 alphanumeric characters to create or identify an operator policy.
- *apn_name*: Enter a string of 1 to 63 characters, including dots (.) and dashes (-), to identify a specific APN network ID.

- **congestion-control**: Including this keyword associates congestion control functionality with the identified APN.
- During an Attach Request, new Inter SGSN RAU, or when receiving sm-messages, all subscribed APNs for mobility management (MM) or selected APNs for session management (SM) will be checked to determine if any of them is configured for congestion control, in which case the new call or sm-messages would be rejected.

Verifying the APN-based Congestion Control Configuration

Use the command illustrated below to verify the configuration created with the commands in the *Configuring APN-based Congestion Control* section above.

The following is entered from the Exec mode.

```
[local]SGSN1-NH show operator-policy full all
```

The following provides a sample of the display generated by the command illustrated above:

```
...
APN NI internet.com
APN Profile Name                :
Congestion-control              : Yes
...
```

Configuring Extended T3312 Timer

The Extended T3312 timer can be configured at two different levels: Call-Control Profile or Service-level (GPRS or SGSN).

Extended T3312 Timer Values for a 2G GPRS Network

Use the following configuration to enable Extended T3312 timer values in a 2G GPRS network environment.

```
configure
    context context_name
        gprs-service service_name
            gmm Extended-T3312-timeout { value exT3312_minutes |
when-subscribed } [ low-priority-ind-ue ]
            end
```

Notes:

- **value** : This keyword instructs the SGSN to send the defined Extended T3312 timer value in Attach or RAU Accept messages to the MS if the subscriber has a subscription for the Extended T3312 timer (Subscribed Periodic RAU/TAU Timer in ISD) and indicates support for the extended periodic timer via the MS Network Feature Support.
- *exT3312_minutes* : Enter an integer from 0 to 18600 to identify the number of minutes for the timeout default is 186 minutes.
- **when-subcribed**: This keyword instructs the SGSN to only send the Extended T3312 period RAU timer value in Attach or RAU Accept messages if the SGSN receives the timeout value in an ISD (Insert Subscriber Data) when the MS has indicated support in "MS Network Feature Support".
- **low-priority-ind-ue**: This keyword instructs the SGSN to include the Extended T3312 timer value only if the Attach/RAU Request messages include a LAPI (low access priority indicator) in the "MS Device Properties".

Extended T3312 Timer Values for a 3G GPRS Network

Use the following configuration to enable Extended T3312 timer values in a 3G UMTS network environment.

```
configure
    context  context_name
         sgsn-service  service_name
              gmm Extended-T3312-timeout  { value exT3312_minutes |
when-subscribed } [ low-priority-ind-ue ]
              end
```

Notes:

- **value** : This keyword instructs the SGSN to send the defined Extended T3312 timer value in Attach or RAU Accept messages to the MS if the subscriber has a subscription for the Extended T3312 timer (Subscribed Periodic RAU/TAU Timer in ISD) and indicates support for the extended periodic timer via the MS Network Feature Support.
- *exT3312_minutes* : Enter an integer from 0 to 18600 to identify the number of minutes for the timeout default is 186 minutes.
- **when-subcribed**: This keyword instructs the SGSN to only send the Extended T3312 period RAU timer value in Attach or RAU Accept messages if the SGSN receives the timeout value in an ISD (Insert Subscriber Data) when the MS has indicated support in "MS Network Feature Support".
- **low-priority-ind-ue**: This keyword instructs the SGSN to include the Extended T3312 timer value only if the Attach/RAU Request messages include a LAPI (low access priority indicator) in the "MS Device Properties".

Extended T3312 Timer Values in the Call-Control Profile

(Reminder: a configuration in the Call-Control Profile would override an **Extended-T3312-timeout** configuration done for either the GPRS or SGSN services. As well, a Call-Control Profile configuration enables the operator to fine-tune for Homers and Roamers.)

Use the following configuration to enable Extended T3312 timer values for all subscribers:

```
configure
    call-control-profile  profile_name
        gmm Extended-T3312-timeout  { value exT3312_minutes | when-subscribed
 } [ low-priority-ind-ue ]
         end
```

Notes:

- **value** : This keyword instructs the SGSN to send the defined Extended T3312 timer value in Attach or RAU Accept messages to the MS if the subscriber has a subscription for the Extended T3312 timer (Subscribed Periodic RAU/TAU Timer in ISD) and indicates support for the extended periodic timer via the MS Network Feature Support.
- *exT3312_minutes* : Enter an integer from 0 to 18600 to identify the number of minutes for the timeout default is 186 minutes.
- **when-subcribed**: This keyword instructs the SGSN to only send the Extended T3312 period RAU timer value in Attach or RAU Accept messages if the SGSN receives the timeout value in an ISD (Insert Subscriber Data) when the MS has indicated support in "MS Network Feature Support".
- **low-priority-ind-ue**: This keyword instructs the SGSN to include the Extended T3312 timer value only if the Attach/RAU Request messages include a LAPI (low access priority indicator) in the "MS Device Properties".

Verifying the Extended T3312 Configurations

To verify the configuration for the 2G network environment, use the following command:

```
[local]SGSN1-NH show gprs-service name  service_name
```

To verify the configuration for the 3G network environment, use the following command:

```
[local]SGSN1-NH show sgsn-service name  service_name
```

To verify the configuration for the Extended T3312 in the Call-Control Profile, use the following command:

```
[local]SGSN1-NH show call-control-profile full name profile_name
```

Configuring Backoff Timers

There are two backoff timers and they can each be configured at two different levels: Call-Control Profile or Service-level (GPRS or SGSN).

- T3346 MM Backoff Timer
- T3349 SM Backoff Time

T3346Timer Values at the Service Level

Use the following configuration to enable T3346 timer values for a 2G GPRS-service or for a 3G SGSN-service.

```
configure
    context  context_name
         ( gprs-service | sgsn-service } service_name
              gmm t3346 min  minimum_minutes max maximum_minutes
              end
```

Notes:

- *minimum_minutes*: Enter an integer from 1 to 15 to identify the minimum number of minutes default is 15 minutes.
- *maximum_minutes*: Enter an integer from 1 to 30 to identify the maximum number of minutes default is 30 minutes.
- If an Attach Request or RAU Request or Service Request is rejected due to congestion, then the T3346 value will be included in the reject message with GMM cause code 22 (congestion). The MM backoff timer value sent will be chosen randomly from within the configured T3346 timer value range.
- The timer will be ignored if an Attach Request or RAU Request is received after congestion has cleared.
- If T3346 timer value is configured in a Call-Control Profile then that value will override the backoff timer values defined for this GPRS Service configurations.

T3346Timer Values at the Call-Control Profile Level

Use the following configuration to enable T3346 timer values in a the Call-Control Profile.

```
configure
    call-control-profile ccpolicy_name
         gmm t3346 min  minimum_minutes max maximum_minutes
         end
```

Notes:

- *minimum_minutes*: Enter an integer from 1 to 15 to identify the minimum number of minutes default is 15 minutes.
- *maximum_minutes*: Enter an integer from 1 to 30 to identify the maximum number of minutes default is 30 minutes.
- If an Attach Request or RAU Request or Service Request is rejected due to congestion, then the T3346 value will be included in the reject message with GMM cause code 22 (congestion). The backoff timer value sent will be chosen randomly from within the configured T3346 timer value range.
- If T3346 timer value is configured in a Call-Control Profile then it will override the backoff timer values defined for either the SGSN Service or GPRS Service configurations.
- The timer will be ignored if an Attach Request or RAU Request is received after congestion has cleared.

Verifying the T3346 Configurations

To verify the configuration for the 2G service, use the following command:

```
[local]SGSN1-NH show gprs-service name service_name
```

To verify the configuration for the 3G service, use the following command:

```
[local]SGSN1-NH show sgsn-service name service_name
```

To verify the configuration for the in the Call-Control Profile, use the following command:

```
[local]SGSN1-NH show call-control-profile full name profile_name
```

Configuring O&M Triggered Congestion

Enabling Congestion

For operations and maintenance purposes (e.g., testing), this command triggers a congestion state at the global level.

```
sgsn trigger-congestion level { critical | major | minor }
```

Notes:

- **critical | major | minor**: Selecting one of the three congestion severity levels indicates the associated congestion-action-profile to be chosen and applied. Reminder: the profile is associated with the severity level with the **congestion-control policy** command.

Disabling Congestion

For operations and maintenance purposes (e.g., testing), this command clears congestion triggered using the **sgsn trigger congestion** command.

```
sgsn clear-congestion
```

Notes:

- If the command is applied then the SGSN resumes normal operations and does not apply any congestion control policy.

Monitoring MTC Congestion Control

The commands and displays illustrated below are additional commands that can be used to monitor the operations of the MTC Congestion Control functionality.

show session disconnect-reasons

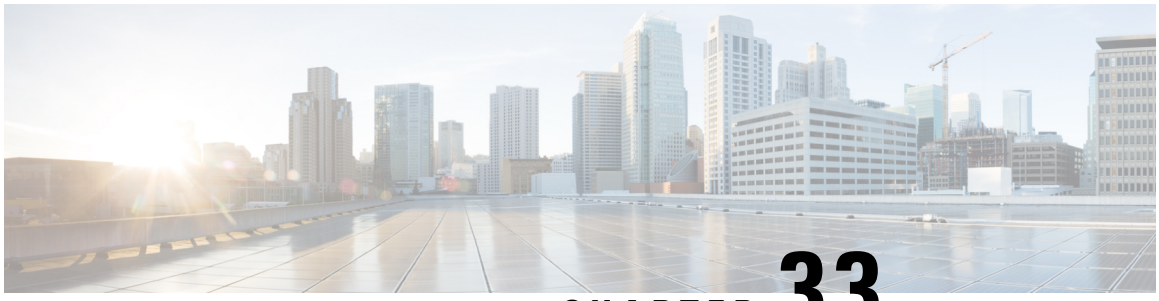
The following disconnect reason pegs calls (Attach and new Inter SGSN RAU) rejected due to APN-based congestion control. The following display is an example of what you might see when you issue the show command:

```
[local]bngnc3 show session disconnect-reasons
Session Disconnect Statistics
Total Disconnects: 1
Disconnect Reason                                Num Disc   Percentage
------------------------------------------------------------------------
mm-apn-congestion-control                               1   100.00000
```

show congestion-control statistics imsimgr all full

The following illustrates the fields for statistics generated if congestion control is engaged.

```
show congestion-control statistics imsimgr all full
 Current congestion status:                          Cleared
 Current congestion Type  :                          None
 Congestion applied:                                 0 times
 Critical Congestion Control Resource Limits
  system cpu use exceeded:
  service cpu use exceeded:
  system memory use exceeded:


SGSN Congestion Control:
   MM Congestion Level:                              None
   Congestion Resource:                              None
   SM Congestion Level:                              None
   O&M Congestion Level:                             None
```



CHAPTER 33

Network Requested Secondary PDP Context Activation

This chapter describes SGSN support for the Network Requested Secondary PDP Context Activation (NRSPCA) feature.

- Feature Description, on page 367
- How It Works, on page 368
- Configuring NRSPCA, on page 374
- Monitoring and Troubleshooting the NRSPCA Feature, on page 375

Feature Description

The SGSN supports Secondary PDP context activation by the network - NRSPCA.

3GPP TS 23.060 specifies two procedures for GGSN-initiated PDP Context Activation:

- **Network Requested PDP Context Activation** (NRPCA) is supported by SGSN but only for 3G access
- **Network Requested Secondary PDP Context Activation** (NRSPCA) is now supported by both Gn/Gp and S4 type SGSNs.

P-GW supports only the NRSPCA procedure. Network requested bearer control, uesed by P-GW and the SGSN, makes use of the NRSPCA procedure.

Benefits

NRSPCA allows the network to initiate secondary PDP context activation if the network determines that the service requested by the user requires activation of an additional secondary PDP context.

Network requested bearer control functionality is mandatory in EPC networks, requiring use of NRSPCA. With this feature S4-SGSN now supports network requested bearer control.

Relationships to Other Features

For NRSPCA on Gn/Gp SGSN, the sgtp-service configuration must include common IE flags in GTP messages.

Network requested activation must be enabled in the call-control profile.

NRSPCA must be supported on the GGSN used for the PDP session. SGSN indicates support of NRSPCA by setting the NRSN flag in the common flags IE of the Create PDP Context Request and the Update PDP Context Request/Response messages to GGSN.

For S4-SGSN, network requested activation must be enabled in the call-control profile.

How It Works

Gn/Gp SGSN

During PDP Context Activation Procedure the Bearer Control Mode (BSM) is negotiated. BCM is applicable to all PDP Contexts within the activated PDP Address/APN pair. It is either "MS_only" or "MS/NW".

For "MS/NW" both the MS and the GGSN may request the creation of additional PDP contexts for the PDP Address/APN pair. The MS uses the Secondary PDP Context Activation Procedure, whereas the GGSN uses NRSPCA. When BCM is "MS_only", the GGSN does not initiate NRSPCA.

The MS indicates support of Network Requested Bearer control through the Network Request Support UE (NRSU) parameter. Using the PCO IE during Primary PDP context Activation, NRSU is applicable to all PDP contexts within the same PDP address/APN pair. The SGSN indicates support of the Network Requested Bearer control to the GGSN through the Network Request Support Network (NRSN) parameter in common flags of the Created PDP Context Request during PDP activation.

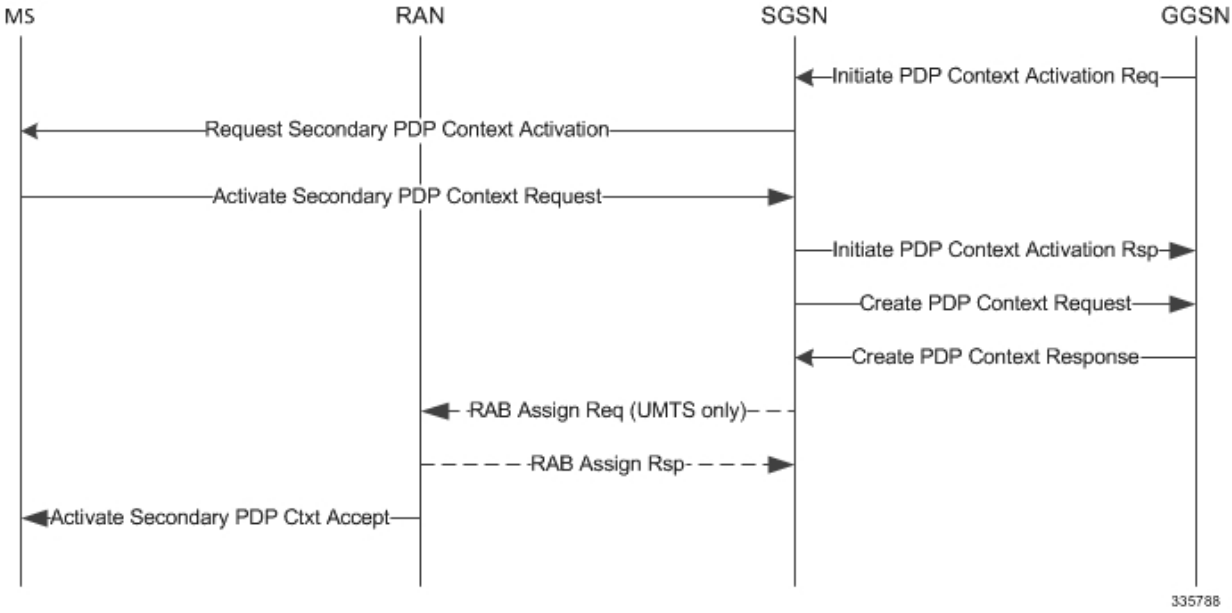
During a new SGSN RAU, the new SGSN indicates the support by means of the NRSN parameter in Update PDP Context Request. If common flags are not included in the Update PDP Context Request message, or the SGSN does not indicate support of the Network Requested Bearer control (NRSN flag is not set), the GGSN, following a SGSN-Initiated PDP Context Modification (triggered by SGSN change), performs a GGSN-Initiated PDP Context Modification to change the BCM to "MS-Only" for all PDP-Address/APN-pairs for which the current BCM is "MS/NW".

When BCM is "MS/NW", the GGSN may trigger activation of secondary PDP context based on local configuration or on PCRF/PCEF direction.

Successful Activation for Gn/Gp SGSN

The call flow below illustrates the NRSPCA procedure for a successful activation.

Figure 66: Call Flow: Successful Network Requested Secondary Activation (Gn/Gp)



GGSN initiates secondary PDP activation by sending an Initiate PDP Context Activation Request (linked NSAPI, requested Qos, TFT, PCO, correlation-Id) to SGSN. The SGSN sends a Requested Secondary PDP Context Activation (linked Ti, Ti, QoS Requested, TFT, PCO) message to MS. The QoS Requested, TFT and PCO are transparently passed through the SGSN.

The TFT sent by the GGSN contains the uplink packet filters to be applied at the MS. The GGSN uses the Correlation-Id is to correlate the subsequent Secondary PDP Context Activation procedure with the Initiate PDP Context Activation Request. The SGSN includes this correlation-Id in the subsequent Create PDP Context Request to GGSN.

The MS sends an Activate Secondary PDP Context Request (linked Ti, Ti, NSAPI, PCO, QoS Requested). Linked Ti, Ti, QoS Requested will be the same as received in a previous message from SGSN. The TFT sent by the MS will contain the downlink packet filters to be applied at GGSN.

On receiving a successful response (Activate Secondary PDP Context Request), the SGSN sends an Initiate PDP Context Activation Response with cause as Accepted to the GGSN. Additionally the SGSN sends a Create PDP Context Request (correlation-Id, linked NSAPI, NSAPI, TFT, PCO) to the GGSN. After the GGSN responds with a Create PDP Response with cause Accepted, the SGSN completes the procedure by sending an Activate Secondary PDP Context Accept to the MS.

Unsuccessful Activation for Gn/Gp SGSN

After sending a Requested Secondary PDP Context Activation to the MS, the SGSN starts the T3385 radio interface retransmission timer. Upon expiry the SGSN re-sends the message with a limit of maximum four retries. Upon the fifth expiry, the SGSN releases all allocated resources and sends an Initiate PDP Context Activation Response to the GGSN with cause as "MS is not GPRS responding".

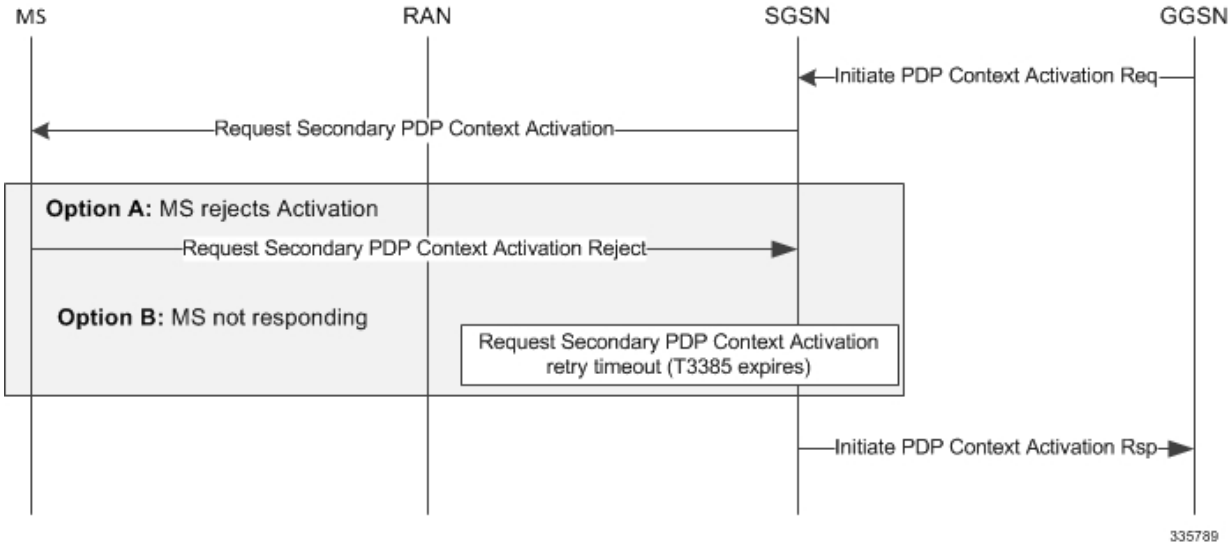
The MS may choose to reject the Secondary Activation by the network. In such cases, the MS sends a Requested Secondary PDP Context Activation Reject message with an appropriate cause. The SGSN informs the GGSN by sending an Initiate PDP Context Activation Response with an appropriate GTP cause mapped from Session Management (SM) cause. SM-to-GTP cause mapping is listed in the table below.

Table 24: SM-to-GTP Cause Mapping

SM Cause	GTP Cause
26, Insufficient resources	199, No resources available
31, activation rejected, unspecified	197, MS refuses
40, feature not supported	200, Service not supported
41, semantic error in TFT operation	215, semantic error in TFT operation
42, syntactical error in TFT operation	216, syntactical error in TFT operation
43, unknown PDP context	210, Context not found
44, semantic error in packet filter(s)	217, semantic error in packet filter(s)
45, syntactical error in packet filter(s)	218, syntactical error in packet filter(s)
46, PDP context without TFT already activated	221, PDP context without TFT already activated
48, activation rejected, BCM violation	227, BCM violation
95 - protocol error	197, MS refuses

Upon receipt of an Activate Secondary PDP Context Request or Requested Secondary PDP Context Activation Reject message, the SGSN stops the T3385 timer.

Figure 67: Call Flow: Unsuccessful Network Requested Secondary Activation (Gn/Gp)



The SGSN will reject the IPCA for the following conditions:

- Subscriber has switched to CS call with cause "GPRS connection suspended".
- Old SGSN RAU/SRNS is ongoing with cause "MS is not GPRS responding".
- IPCA Request is received when BCM is MS only with "BCM mode violation".
- The received Correlation Id is the same as that for another ongoing NRSPCA request for the same bundle with "Invalid Correlation Id".
- Linked context is in deactivating state (collision case), with "context not found".

- Failure conditions such as "memory allocation failure" are encountered with "No resources available".
- An operator policy restriction causes IPCA Req to be rejected with the configured cause under the call-control profile.

The following table lists the GTP causes in the Initiate PDP Context Activation Response that will initiate SGSN rejects.

Table 25: SGSN GTP Reject Causes

GTP Cause	Scenario
225, Invalid Correlation Id	SGSN stores the Correlation Id until completion of Activation. It rejects the newer NRSPCA activation if the GGSN uses the same value for two NRSPCA activations (uniquely identified by sequence number).
199, No resources available	Rejection is due to insufficient memory, the maximum number of temporary Ti allocations has been reached, or the NRSPCA procedure collides with a new SGSN RAU procedure.
210, Context not found	Rejection occurs because the PDP bundle identified by a linked NSAPI does not have any active PDP context.
197, GPRS connection Suspended	MS is in suspended state (CS call active).
196, MS is not GPRS responding	Rejection occurs if the Request Secondary PDP Context Activation message times out (T3385 timer), no response to Paging, PPF flag is set to 0, or the NRSPCA procedure collides with an old SGSN RAU/SRNS, intra-SGSN intersystem/RAT RAU.
Configured GTP cause, or 200, Service not supported (default)	Rejection is based on operator policy.
227, BCM violation	IPCA Request is received for a bundle with BCM set to MS only.

S4-SGSN

Successful Activation for S4-SGSN

A P-GW initiates a Secondary PDP activation by sending a Create Bearer Request (linked Bearer Identity, Bearer Ctx(s), PCO etc) to the S-GW. The S-GW then forwards the request to the S4-SGSN.

The Bearer Contexts contain Bearer level parameters such as TFT, Bearer level QoS, S5/8-U PGW FTeid, PCO, etc. The S-GW includes the S12-U SGW FTeid or S4-U SGW FTeid depending on whether an S12 or S4 interface is used. The S4-SGSN sends the Requested Secondary PDP Context Activation (linked Ti, Ti, Qos Requested, TFT, and PCO) message to MS.

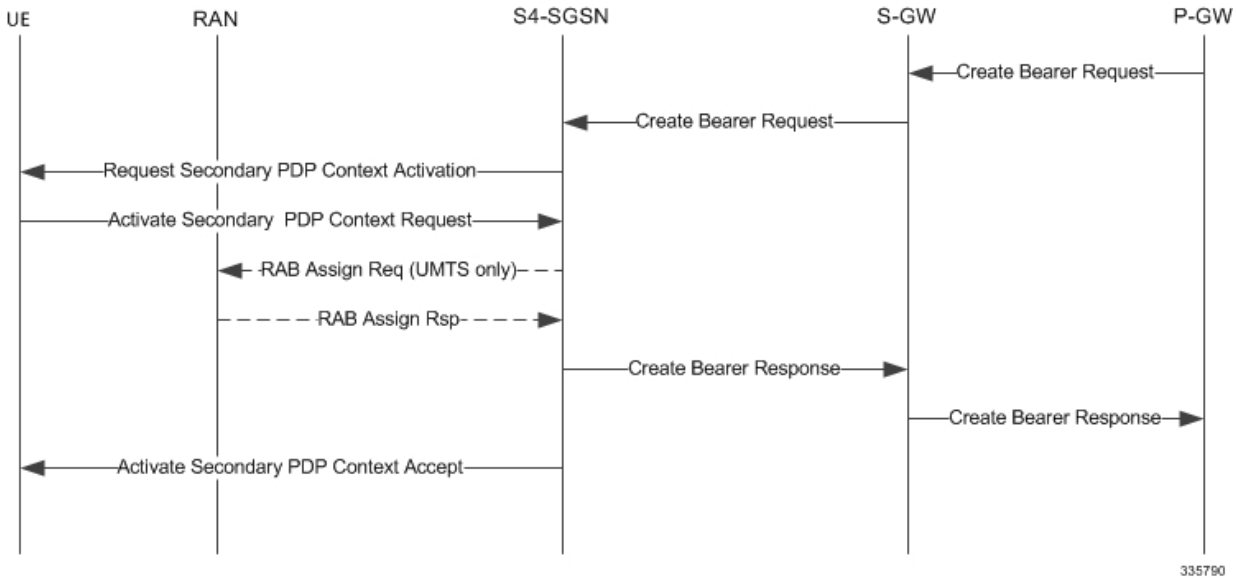
The QoS Requested, TFT and PCO are transparently passed through the S4-SGSN. The MS sends an Activate Secondary PDP Context Request (linked Ti, Ti, NSAPI, PCO, and QoS Requested). Linked Ti, Ti, Qos Requested will be as same as received in a previous message from the S4-SGSN. The TFT sent to MS may contain both the uplink and downlink packet filters.

On receiving a successful response (Activate Secondary PDP Context Request) in UMTS access, the S4-SGSN establishes RAB with the serving RNC and then sends a Create Bearer Response with Accepted cause to S-GW. For GPRS access, the RAB establishment is skipped.

The S4-SGSN includes the S4-U SGW FTeid (received in Create Bearer Request) in the Create Bearer Response to S-GW. S-GW uses this to correlate the Bearer Contexts in Response with that of Request. The S4-SGSN completes the procedure by sending an Activate Secondary PDP Context Accept to the MS.

A successful Network Requested Secondary PDP Context Activation Procedure is illustrated in the figure below.

Figure 68: Call Flow: Successful Network Requested Secondary Activation (S4-SGSN)



Unsuccessful Activation for S4-SGSN

After sending a Requested Secondary PDP Context Activation to the MS, the S4-SGSN starts the T3385 radio interface retransmission timer. Upon expiry the S4-SGSN resends the message, a maximum of four retries. Upon the fifth expiry, the S4-SGSN releases all allocated resources and sends a Create Bearer Response to the S-GW/P-GW with cause as "UE not responding".

The MS may choose to reject a Secondary Activation by network. In such cases, the MS sends a Requested Secondary PDP Context Activation Reject message with an appropriate cause. S4-SGSN informs the SGW/PGW by sending a Create Bearer Response with an appropriate GTPv2 cause mapped from an SM cause as shown in the table below.

Table 26: SM Cause to GTPv2 Cause Mapping

SM Cause	GTPv2 Cause
26, Insufficient resources	73, No resources available
31, activation rejected, unspecified	88, UE refuses
40, feature not supported	68, service not supported
41, semantic error in TFT operation	74, semantic error in TFT operation

SM Cause	GTPv2 Cause
42, syntactical error in TFT operation	75, syntactic error in TFT operation
43, unknown PDP context	64, context not found
44, semantic error in packet filter(s)	76, semantic error in packet filter(s)
45, syntactical error in packet filter(s)	77, syntactic error in packet filter(s)
46, PDP context without TFT already activated	85, UE context without TFT already activated
48, activation rejected, BCM violation	88, UE refuses
95 - protocol error	88, UE refuses

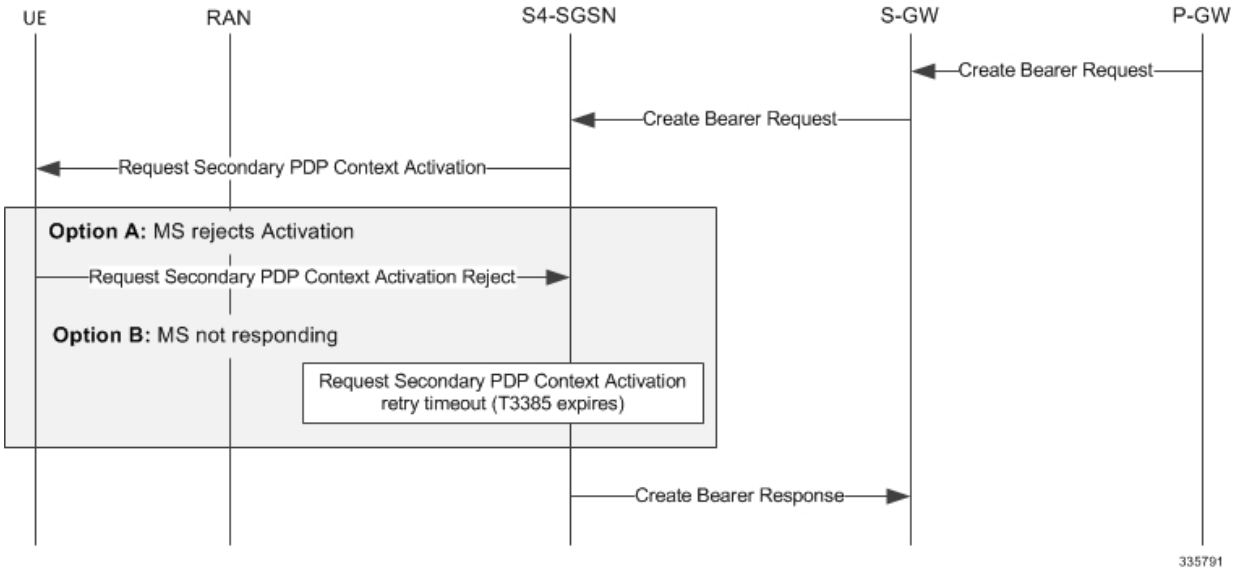
Upon receipt of an Activate Secondary PDP Context Request or Requested Secondary PDP Context Activation Reject message, the S4-SGSN stops the T3385 timer.

The S4-SGSN will reject a Create Bearer Request for the following conditions:

- Subscriber has switched to CS call with cause "Unable to page UE due to suspension".
- A collision occurs with an old SGSN RAU/SRNS with cause "Temporarily rejected due to handover procedure in progress".
- Linked context is in deactivating state (collision case) with "context not found".
- A failure conditions such as 'memory allocation failure" is encountered with "No resources available".
- Operator policy restriction rejects the CBR Req with the configured cause under the call-control profile.
- PPF flag is cleared with cause "Unable to Page UE".
- Paging failure or Request Secondary PDP activation request times out with cause "UE not responding".

An unsuccessful NRSPCA procedure is illustrated in the figure below.

Figure 69: Call Flow: Unsuccessful Network Requested Secondary Activation (S4-SGSN)



Limitations

Security function during NRSPCA procedure is not supported.

Standards Compliance

The NRSPCA feature complies with the following standards:

- 3GPP TS 23.060 version 10 General Packet Radio Service (GPRS)
- 3GPP TS 24.008 version 10 Mobile radio interface Layer 3 specification Core network protocols
- 3GPP TS 29.060 version 10 General Packet Radio Service (GPRS) GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface
- 3GPP TS 29.278 version 10 Customized Applications for Mobile network Enhanced Logic (CAMEL) CAMEL Application Part (CAP) specification for IP Multimedia Subsystems (IMS)

Configuring NRSPCA

Configuration of the NRSPCA feature requires:

- Enabling the common flags IE in SGTP service
- Including the NRSPCA feature in a specific call control profile

Sample NRSPCA Configuration

The first set of commands enables the common flags IE:

```
config
   context <context-name>
      sgtp-service <sgtp-service-name>
        gtpc send common-flags
        end
```

The second set of commands includes a new keyword (**secondary**) to configure NRSPCA in a call control profile.

```
config
   call-control-profile <profile_name>
     network-initiated-pdp-activation  secondary access-type  <gprs|umts>
{ all failure-code <failure_code> | location-area-list instance <instance>
failure-code <failure_code> }
       end
```

NOTES:

- **remove** added to the command disables NRSPCA by removing the network-initiated-pdp-activation definition from the configuration.
- There is no default form of the command.

Verifying the NRSPCA Configuration

show sgtp-service name <sgtp-service-name>

```
Service name                              : <sgtp-service-name>
Service-Id                                : 3
Context                                   : source
Status                                    : STARTED

Sending RAB Context IE                    : Enabled
Sending Common Flags IE                    : Enabled
Sending Target Identification Preamble    : Disabled
```

show call-control-profile full name <cc-profile-name>

```
Call Control Profile Name = <cc-profile-name>
Accounting Mode (SGW)                                 : None
Accounting stop-trigger (SGW)                         : Not configured

UMTS Secondary PDP Context Activation All              : Allow
UMTS PDP Context Activation All Failure Code           : 8
GPRS Nw Init Primary PDP Context Activation All        : Allow
GPRS Nw Init Primary PDP Ctxt Activation All Failure Code : 200
GPRS Nw Init Secondary PDP Context Activation All        : Allow
GPRS Nw Init Secondary PDP Ctxt Activation All Failure Code : 200
UMTS Nw Init Primary PDP Context Activation All        : Allow
UMTS Nw Init Primary PDP Ctxt Activation All Failure Code : 200
UMTS Nw Init Secondary PDP Context Activation All        : Allow
UMTS Nw Init Secondary PDP Ctxt Activation All Failure Code : 200
SRNS Intra All                                        : Allow
```

Monitoring and Troubleshooting the NRSPCA Feature

- The **show subscriber sgsn-only/gprs-only full** command indicates whether or not the Secondary PDP context was network initiated. The last received BCM from the GGSN (applicable for Gn/Gp only) is also be displayed.
- Two new disconnect reasons have been introduced:
  - sgsn-nrspca-actv-rej-by-ms MS sends a Request Secondary PDP Context Activation Reject message
  - sgsn-nrspca-actv-rej-by-sgsn For all other cases where NRSPCA context activation does not complete successfully
- Additional counters have been added to session management statistics in the output of the **show gmm-sm statistics** command to represent the session management messages used by NRSPCA. Similarly, counters have been added to the tunnel management statistics in the output of the **show sgtpc statistics** command. These counters are described in the next section.
- For NRSPCA activation failures, the Abort statistics in the verbose mode of the **show gmm-sm statistics** or **show gmm-sm statistics sm-only** command outputs provide reasons for the failure. The various counters are described in next section.
- Network initiated flag in SCDRs will be set for NRSPCA PDP contexts. Note that network initiated flag is present in only a few dictionaries, such custom24, custom13, and custom6.

NRSPCA show Commands

The following **show** commands are available in support of the NRSPCA feature:

- **show gmm-sm statistics sm-only** displays the Session Management messages exchanged for NRSPCA activation.
- **show sgtpc statistics** displays the GTPC messages exchanged for NRSPCA activation.
- **show subscribers sgsn-only/gprs-only full** indicates whether or not the Secondary PDP context was network initiated. Displays the last received BCM from the GGSN (applicable for Gn/Gp only).

show gmm-sm statistics sm-only

The following counters are included in the **show gmm-sm statistics sm-only** command output to support the NRSPCA feature. For detailed descriptions of these statistics, refer to the *Statistics and Counters Reference*.

Table 27: NRSPCA SM Statistics

NRSPCA SM Statistics	
Activate Context Request	
Actv-Request-Nrspca 3G-Actv-Request-Nrspca	2G-Actv-Request-Nrspca
Activate Context Request Retransmitted	
3G-Secondary-Actv-Drop-Nrspca	2G-Secondary-Actv-Drop-Nrspca
Activate Context Accept	
Actv-Accept-Nrspca 3G-Actv-Accept-Nrspca	2G-Actv-Accept-Nrspca
Activate Context Reject	
Actv-Reject-Nrspca 3G-Actv-Reject-Nrspca	2G-Actv-Reject-Nrspca
Network Initiated Secondary Activation Aborted (verbose only)	

NRSPCA SM Statistics	
3G-NRSPCA-Abort-GTP-Suspend 3G-NRSPCA-Abort-Handoff 3G-NRSPCA-Abort-Max-Retry-Attempts 3G-NRSPCA-Abort-Paging-Expiry 3G-NRSPCA-Abort-Linked-Ctx-Deactv 3G-NRSPCA-Abort-Linked-Ctx-Detach 3G-NRSPCA-Abort-Inter-RAT-Handoff 3G-NRSPCA-Abort-Iu-release 3G-NRSPCA-Abort-SRNS-Handoff 3G-NRSPCA-Abort-Intra-RAU 3G-NRSPCA-Abort-Intra-SRNS 3G-NRSPCA-Abort-RAB-Failure 3G-NRSPCA-Abort-Ctx-Deactv	2G-NRSPCA-Abort-GTP-Suspend 2G-NRSPCA-Abort-Handoff 2G-NRSPCA-Abort-T3385-Expiry 2G-NRSPCA-Abort-Paging-Expiry 2G-NRSPCA-Abort-Linked-Ctx-Deactv 2G-NRSPCA-Abort-Linked-Ctx-Detach 2G-NRSPCA-Abort-Inter-RAT-Handoff 2G-NRSPCA-Abort-Intra-RAU 2G-NRSPCA-Abort-Ready-Tmr-Expiry 2G-NRSPCA-Abort-Radio-Status 2G-NRSPCA-Abort-BVC-Block-Or-Reset
Request Secondary Pdp Context Activation	
Total-Request-Sec-Pdp-Ctxt-Req 3G-Request-Sec-Pdp-Ctxt-Req	2G-Request-Sec-Pdp-Ctxt-Req
Retransmission	
Total-Request-Sec-Pdp-Ctxt-Req 3G-Request-Sec-Pdp-Ctxt-Req	2G-Request-Sec-Pdp-Ctxt-Req
Request Secondary Pdp Context Activation Reject	
Total-Request-Sec-Pdp-Ctxt-Reject 3G-Request-Sec-Pdp-Ctxt-Reject	2G-Request-Sec-Pdp-Ctxt-Reject
Request Secondary Pdp Context Activation Denied (verbose only)	

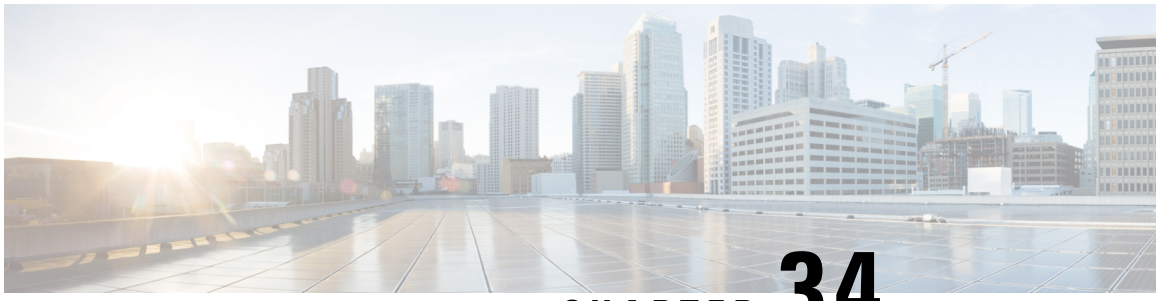
NRSPCA SM Statistics	
3G-Insufficient Resources	2G-Insufficient Resources
3G-Actv Rej Unspecified	2G-Actv Rej Unspecified
3G-Feature Not Supported	2G-Feature Not Supported
3G-Sem Err in TFT OP	2G-Sem Err in TFT OP
3G-Syntactic Err in TFT OP	2G-Syntactic Err in TFT OP
3G-Unknown Ctx	2G-Unknown Ctx
3G-Sem Err in Pkt Filter	2G-Sem Err in Pkt Filter
3G-Syntactic Err in Pkt Filter	2G-Syntactic Err in Pkt Filter
3G-Ctx No-Tft Already Activated	2G-Ctx No-Tft Already Activated
3G-Actv Rej BCM violation	2G-Actv Rej BCM violation
3G-Proto Err Unspecified	2G-Proto Err Unspecified
Request Secondary Pdp Context Activation Rejects Dropped	
3G-Request-Sec-Pdp-Ctxt-Rej-Dropped	2G-Request-Sec-Pdp-Ctxt-Rej-Dropped
Request Secondary Pdp Context Activation Aborted	
3G-NRSPCA-Abort-Subs-Detach	2G-NRSPCA-Abort-Subs-Detach
3G-NRSPCA-Abort-Linked-Ctx-Deactv	2G-NRSPCA-Abort-Linked-Ctx-Deactv
3G-NRSPCA-Abort-Max-Retry-Attempts	2G-NRSPCA-Abort-Max-Retry-Attempts
3G-NRSPCA-Abort-Paging-Expiry	2G-NRSPCA-Abort-Paging-Expiry
3G-NRSPCA-Abort-Subs-Suspend	2G-NRSPCA-Abort-Subs-Suspend
3G-NRSPCA-Abort-Handoff	2G-NRSPCA-Abort-Handoff
3G-NRSPCA-Abort-Inter-RAT-Handoff	2G-NRSPCA-Abort-Inter-RAT-Handoff
3G-NRSPCA-Abort-Intra-RAU	2G-NRSPCA-Abort-Intra-RAU
3G-NRSPCA-Abort-Iu-release	2G-NRSPCA-Abort-Ready-Tmr-Expiry
3G-NRSPCA-Abort-SRNS-Handoff	2G-NRSPCA-Abort-Radio-Status
3G-NRSPCA-Abort-Intra-SRNS	2G-NRSPCA-Abort-BVC-Block-Or-Reset
3G-NRSPCA-Abort-RAB-Failure	
3G-NRSPCA-Abort-Ctx-Deactv	
Secondary Pdp Context Activation Request Ignored (verbose only)	
Total-Actv-Request-Nrspca-Ignored	
3G-Actv-Request-Nrspca-Ignored	2G-Actv-Request-Nrspca-Ignored

show sgtpc statistics

The following counters are included in the **show sgtpc statistics** command output to support the NRSPCA feature. For detailed descriptions of these statistics, refer to the *Statistics and Counters Reference*.

Table 28: NRSPCA SGTPC Statistics

NRSPCA SGTC Statistics	
Initiate PDP Context Activation Request	
Total IPCA Req	
Initial IPCA Req	Retrans IPCA Req
Initiate PDP Context Activation Response:	
Total Accepted	
Initial IPCA Rsp	Retrans IPCA Rsp
Total Denied	
Initial IPCA Rsp	Retrans IPCA Rsp
Initiate PDP Context Activation Response Not Sent (verbose only)	
Linked PDP deact coll	Retrans IPCA Req bef MS rsp
Initiate PDP Context Activation Request Denied (verbose only)	
IPCA Req Denied	
No Resources Available	Service Not Supported
System Failure	Mandatory IE Incorrect
Mandatory IE Mis	Optional IE Incorrect
Invalid Message Format	Context not Found
Semantic Error in TFT	Syntactic Error in TFT
Semantic Error in Pkt Fltr	Syntactic Error in Pkt Fltr
MS Not GPRS Responding	MS Refuses
Invalid Correlation Id	PDP without TFT already Active
BCM Violation	MS GPRS Suspended
Unknown cause	



CHAPTER 34

Operator Policy

The proprietary concept of an operator policy, originally architected for the exclusive use of an SGSN, is non-standard and currently unique to the ASR 5500. This optional feature empowers the carrier with flexible control to manage functions that are not typically used in all applications and to determine the granularity of the implementation of any operator policy: to groups of incoming calls or to simply one single incoming call.

The following products support the use of the operator policy feature:

- MME (Mobility Management Entity - LTE)
- SGSN (Serving GPRS Support Node - 2G/3G/LTE)
- S-GW (Serving Gateway - LTE)

This document includes the following information:

- What Operator Policy Can Do, on page 381
- The Operator Policy Feature in Detail, on page 382
- How It Works, on page 386
- Operator Policy Configuration, on page 386
- Verifying the Feature Configuration, on page 392

What Operator Policy Can Do

Operator policy enables the operator to specify a policy with rules governing the services, facilities and privileges available to subscribers.

A Look at Operator Policy on an SGSN

The following is only a sampling of what working operator policies can control on an SGSN:

- APN information included in call activation messages are sometimes damaged, misspelled, missing. In such cases, the calls are rejected. The operator can ensure calls aren't rejected and configure a range of methods for handling APNs, including converting incoming APNs to preferred APNs and this control can be used in a focused fashion or defined to cover ranges of subscribers.
- In another example, it is not unusual for a blanket configuration to be implemented for all subscriber profiles stored in the HLR. This results in a waste of resources, such as the allocation of the default highest QoS setting for all subscribers. An operator policy provides the opportunity to address such issues by allowing fine-tuning of certain aspects of profiles fetched from HLRs and, if desired, overwrite QoS settings received from HLR.

A Look at Operator Policy on an S-GW

The S-GW operator policy provides mechanisms to fine tune the behavior for subsets of subscribers. It also can be used to control the behavior of visiting subscribers in roaming scenarios by enforcing roaming agreements and providing a measure of local protection against foreign subscribers.

The S-GW uses operator policy in the SGW service configuration to control the accounting mode. The default accounting mode is GTPP, but RADIUS/Diameter and none are options. The accounting mode value from the call control profile overrides the value configured in SGW service. If the accounting context is not configured in the call control profile, it is taken from SGW service. If the SGW service does not have the relevant configuration, the current context or default GTPP group is assumed.

The Operator Policy Feature in Detail

This flexible feature provides the operator with a range of control to manage the services, facilities and privileges available to subscribers.

Operator policy definitions can depend on factors such as (but not limited to):

- roaming agreements between operators,
- subscription restrictions for visiting or roaming subscribers,
- provisioning of defaults to override standard behavior.

These policies can override standard behaviors and provide mechanisms for an operator to circumvent the limitations of other infrastructure elements such as DNS servers and HLRs in 2G/3G networks.

By configuring the various components of an operator policy, the operator fine-tunes any desired restrictions or limitations needed to control call handling and this can be done for a group of callers within a defined IMSI range or per subscriber.

Re-Usable Components - Besides enhancing operator control via configuration, the operator policy feature minimizes configuration by drastically reducing the number of configuration lines needed. Operator policy maximizes configurations by breaking them into the following reusable components that can be shared across IMSI ranges or subscribers:

- call control profiles
- IMEI profiles (SGSN only)
- APN profiles
- APN remap tables
- operator policies
- IMSI ranges

Each of these components is configured via a separate configuration mode accessed through the Global Configuration mode.

Call Control Profile

A call control profile can be used by the operator to fine-tune desired functions, restrictions, requirements, and/or limitations needed for call management on a per-subscriber basis or for groups of callers across IMSI ranges. For example:

- setting access restriction cause codes for rejection messages
- enabling/disabling authentication for various functions such as attach and service requests

- enabling/disabling ciphering, encryption, and/or integrity algorithms
- enabling/disabling of packet temporary mobile subscriber identity (P-TMSI) signature allocation (SGSN only)
- enabling/disabling of zone code checking
- allocation/retention priority override behavior (SGSN only)
- enabling/disabling inter-RAT, 3G location area, and 4G tracking area handover restriction lists (MME and S-GW only)
- setting maximum bearers and PDNs per subscriber (MME and S-GW only)

Call control profiles are configured with commands in the Call Control Profile configuration mode. A single call control profile can be associated with multiple operator policies

For planning purposes, based on the system configuration, type of packet services cards, type of network (2G, 3G, 4G, LTE), and/or application configuration (single, combo, dual access), the following call control profile configuration rules should be considered:

- 1 (only one) - call control profile can be associated with an operator policy
- 1000 - maximum number of call control profiles per system (e.g., an SGSN).
- 15 - maximum number of equivalent PLMNs for 2G and 3G per call control profile
  - 15 - maximum number of equivalent PLMNs for 2G per ccprofile.
  - 15 - maximum number of supported equivalent PLMNs for 3G per ccprofile.
- 256 - maximum number of static SGSN addresses supported per PLMN
- 5 - maximum number of location area code lists supported per call control profile.
- 100 - maximum number of LACs per location area code list supported per call control profile.
- unlimited number of zone code lists can be configured per call control profile.
- 100 - maximum number of LACs allowed per zone code list per call control profile.
- 2 - maximum number of integrity algorithms for 3G per call control profile.
- 3 - maximum number of encryption algorithms for 3G per call control profile.

APN Profile

An APN profile groups a set of access point name (APN)-specific parameters that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN profile will be applied.

For example:

- enable/disable a direct tunnel (DT) per APN. (SGSN)
- define charging characters for calls associated with a specific APN.
- identify a specific GGSN to be used for calls associated with a specific APN (SGSN).
- define various quality of service (QoS) parameters to be applied to calls associated with a specific APN.
- restrict or allow PDP context activation on the basis of access type for calls associated with a specific APN.

APN profiles are configured with commands in the APN Profile configuration mode. A single APN profile can be associated with multiple operator policies.

For planning purposes, based on the system configuration, type of packet processing cards and 2G, 3G, 4G, and/or dual access, the following APN profile configuration rules should be considered:

- 50 - maximum number of APN profiles that can be associated with an operator policy.

- 1000 - maximum number of APN profiles per system (e.g., an SGSN).
- 116 - maximum gateway addresses (GGSN addresses) that can be defined in a single APN profile.

IMEI-Profile (SGSN only)

The IMEI is a unique international mobile equipment identity number assigned by the manufacturer that is used by the network to identify valid devices. The IMEI has no relationship to the subscriber.

An IMEI profile group is a set of device-specific parameters that control SGSN behavior when one of various types of Requests is received from a UE within a specified IMEI range. These parameters control:

- Blacklisting devices
- Identifying a particular GGSN to be used for connections for specified devices
- Enabling/disabling direct tunnels to be used by devices

IMEI profiles are configured with commands in the IMEI Profile configuration mode. A single IMEI profile can be associated with multiple operator policies.

For planning purposes, based on the system configuration, type of packet processing cards, type of network (2G, 3G, 4G, LTE), and/or application configuration (single, combo, dual access), the following IMEI profile configuration rules should be considered:

- 10 - maximum number of IMEI ranges that can be associated with an operator policy.
- 1000 - maximum number of IMEI profiles per system (such as an SGSN).

APN Remap Table

APN remap tables allow an operator to override an APN specified by a user, or the APN selected during the normal APN selection procedure, as specified by 3GPP TS 23.060. This atypical level of control enables operators to deal with situations such as:

- An APN is provided in the Activation Request that does not match with any of the subscribed APNs either a different APN was entered or the APN could have been misspelled. In such situations, the SGSN would reject the Activation Request. It is possible to correct the APN, creating a valid name so that the Activation Request is not rejected.
- In some cases, an operator might want to force certain devices/users to use a specific APN. For example, all iPhone4 users may need to be directed to a specific APN. In such situations, the operator needs to be able to override the selected APN.

An APN remap table group is a set of APN-handling configurations that may be applicable to one or more subscribers. When a subscriber requests an APN that has been identified in a selected operator policy, the parameter values configured in the associated APN remap table will be applied. For example, an APN remap table allows configuration of the following:

- APN aliasing - maps incoming APN to a different APN based on partial string match (MME and SGSN) or matching charging characteristic (MME and SGSN).
- Wildcard APN - allows APN to be provided by the SGSN when wildcard subscription is present and the user has not requested an APN.
- Default APN - allows a configured default APN to be used when the requested APN cannot be used for example, the APN is not part of the HLR subscription. In 21.4 and later releases, the configuration to enable default APN on failure of DNS query is enhanced to support S4-SGSN. When wildcard APN is

received in subscription, the DNS request is tried with the MS requested APN and on failure of DNS, it is retried with the APN value configured in the APN remap table.

APN remap tables are configured with commands in the APN Remap Table configuration mode. A single APN remap table can be associated with multiple operator policies, but an operator policy can only be associated with a single APN remap table.

For planning purposes, based on the system configuration, type of packet processing cards, type of network (2G, 3G, 4G, LTE), and/or application configuration (single, combo, dual access), the following APN remap table configuration rules should be considered:

- 1 - maximum number of APN remap tables that can be associated with an operator policy.
- 1000 - maximum number of APN remap tables per system (such as an SGSN).
- 100 - maximum remap entries per APN remap table.

Operator Policies

The profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. An operator policy binds the various configuration components together. It associates APNs, with APN profiles, with an APN remap table, with a call control profile, and/or an IMEI profile (SGSN only) and associates all the components with filtering ranges of IMSIs.

In this manner, an operator policy manages the application of rules governing the services, facilities, and privileges available to subscribers.

Operator policies are configured and the associations are defined via the commands in the Operator Policy configuration mode.

The IMSI ranges are configured with the command in the SGSN-Global configuration mode.

For planning purposes, based on the system configuration, type of packet processing cards, type of network (2G, 3G, 4G, LTE), and/or application configuration (single, combo, dual access), the following operator policy configuration rules should be considered:

- 1 maximum number of call control profiles associated with a single operator policy.
- 1 maximum number of APN remap tables associated with a single operator policy.
- 10 maximum number of IMEI profiles associated with a single operator policy (SGSN only)
- 50 maximum number of APN profiles associated with a single operator policy.
- 1000 maximum number of operator policies per system (e.g., an SGSN) this number includes the single default operator policy.
- 1000 maximum number of IMSI ranges defined per system (e.g., an SGSN).

Important SGSN operator policy configurations created with software releases prior to Release 11.0 are not forward compatible. Such configurations can be converted to enable them to work with an SGSN running Release 11.0 or higher. Your Cisco Account Representative can accomplish this conversion for you.

IMSI Ranges

Ranges of international mobile subscriber identity (IMSI) numbers, the unique number identifying a subscriber, are associated with the operator policies and used as the initial filter to determine whether or not any operator policy would be applied to a call. The range configurations are defined by the MNC, MCC, a range of MSINs, and optionally the PLMN ID. The IMSI ranges must be associated with a specific operator policy.

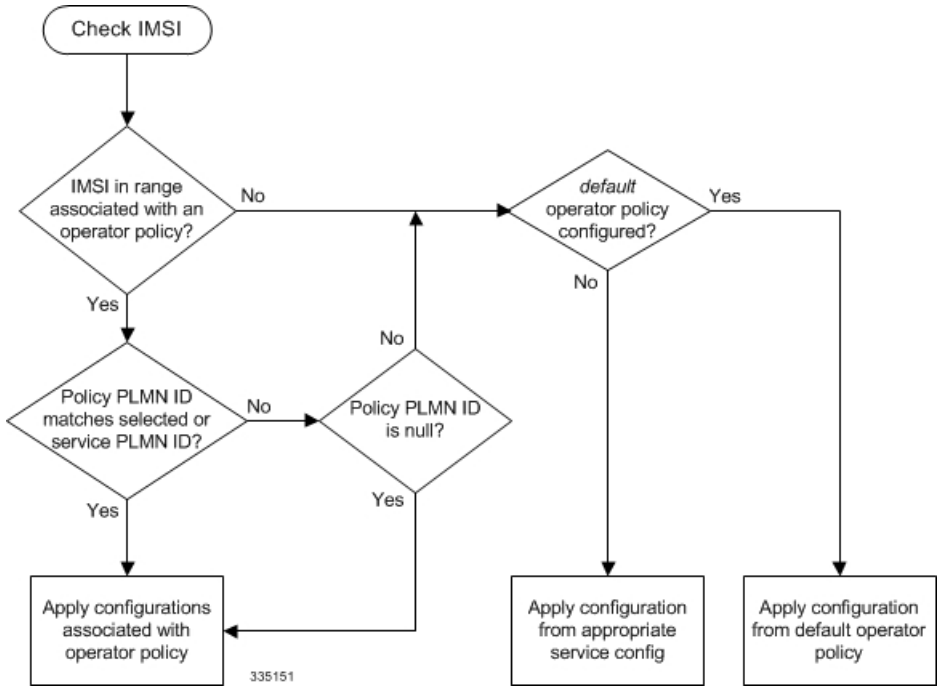
IMSI ranges are defined differently for each product supporting the operator policy feature.

How It Works

The specific operator policy is selected on the basis of the subscriber's IMSI at attach time, and optionally the PLMN ID selected by the subscriber or the RAN node's PLMN ID. Unique, non-overlapping, IMSI + PLMN-ID ranges create call filters that distinguish among the configured operator policies.

The following flowchart maps out the logic applied for the selection of an operator policy:

Figure 70: Operator Policy Selection Logic



Operator Policy Configuration

This section provides a high-level series of steps and the associated configuration examples to configure an operator policy. By configuring an operator policy, the operator fine-tunes any desired restrictions or limitations needed to control call handling per subscriber or for a group of callers within a defined IMSI range.

Most of the operator policy configuration components are common across the range of products supporting operator policy. Differences will be noted as they are encountered below.

Important This section provides a minimum instruction set to implement operator policy. For this feature to be operational, you must first have completed the system-level configuration as described in the *System Administration Guide* and the service configuration described in your product's administration guide.

The components can be configured in any order. This example begins with the call control profile:

Step 1 Create and configure a call control profile, by applying the example configuration presented in the Call Control Profile Configuration section.

Step 2 Create and configure an APN profile, by applying the example configuration presented in the APN Profile Configuration section.

Note It is not necessary to configure both an APN profile and an IMEI profile. You can associate either type of profile with a policy. It is also possible to associate one or more APN profiles with an IMEI profile for an operator policy (SGSN only).

Step 3 Create and configure an IMEI profile by applying the example configuration presented in the *IMEI Profile Configuration* section (SGSN only).

Step 4 Create and configure an APN remap table by applying the example configuration presented in the *APN Remap Table Configuration* section.

Step 5 Create and configure an operator policy by applying the example configuration presented in the *Operator Policy Configuration* section.

Step 6 Configure an IMSI range by selecting and applying the appropriate product-specific example configuration presented in the *IMSI Range Configuration* sections below.

Step 7 Associate the configured operator policy components with each other and a network service by applying the example configuration in the *Operator Policy Component Associations* section.

Step 8 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* .

Step 9 Verify the configuration for each component separately by following the instructions provided in the *Verifying the Feature Configuration* section of this chapter.

Call Control Profile Configuration

This section provides the configuration example to create a call control profile and enter the configuration mode.

Use the call control profile commands to define call handling rules that will be applied via an operator policy. Only one call control profile can be associated with an operator policy, so it is necessary to use (and repeat as necessary) the range of commands in this mode to ensure call-handling is sufficiently managed.

Configuring the Call Control Profile for an SGSN

The example below includes some of the more commonly configured call control profile parameters with sample variables that you will replace with your own values.

```
configure
  call-control-profile profile_name>
    attach allow access-type umts location-area-list instance list_id
    authenticate attach
    location-area-list instance instance area-code area_code
    sgsn-number E164_number
    end
```

Notes:

- Refer to the *Call Control Profile Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.
- This profile will only become valid when it is associated with an operator policy.

Configuring the Call Control Profile for an MME or S-GW

The example below includes some of the more commonly configured call control profile parameters with sample variables that you will replace with your own values.

```
configure
   call-control-profile profile_name
    associate hss-peer-service service_name  s6a-interface
    attach imei-query-type imei verify-equipment-identity
    authenticate attach
    dns-pgw context mme_context_name
    dns-sgw context mme_context_name
    end
```

Notes:

- Refer to the *Call Control Profile Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.
- This profile will only become valid when it is associated with an operator policy.

APN Profile Configuration

This section provides the configuration example to create an APN profile and enter the apn-profile configuration mode.

Use the **apn-profile** commands to define how calls are to be handled when the requests include an APN. More than one APN profile can be associated with an operator policy.

The example below includes some of the more commonly configured profile parameters with sample variables that you will replace with your own values.

```
configure
  apn-profile profile_name
    gateway-address 123.123.123.1 priority 1(SGSN only)
    direct-tunnel not-permitted-by-ggsn (SGSN only)
    idle-mode-acl ipv4 access-group station7 (S-GW only)
    end
```

Notes:

- All of the parameter defining commands in this mode are product-specific. Refer to the *APN Profile Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.
- This profile will only become valid when it is associated with an operator policy.

IMEI Profile Configuration - SGSN only

This section provides the configuration example to create an IMEI profile and enter the imei-profile configuration mode.

Use the **imei-profile** commands to define how calls are to be handled when the requests include an IMEI in the defined IMEI range. More than one IMEI profile can be associated with an operator policy.

The example below includes some of the more commonly configured profile parameters with sample variables that you will replace with your own values.

```
configure
  imei-profile profile_name
    ggsn-address 211.211.123.3
    direct-tunnel not-permitted-by-ggsn (SGSN only)
    associate apn-remap-table remap1
    end
```

Notes:

- It is optional to configure an IMEI profile. An operator policy can include IMEI profiles and/or APN profiles.
- This profile will only become valid when it is associated with an operator policy.

APN Remap Table Configuration

This section provides the configuration example to create an APN remap table and enter the apn-remap-table configuration mode.

Use the **apn-remap-table** commands to define how APNs are to be handled when the requests either do or do not include an APN.

The example below includes some of the more commonly configured profile parameters with sample variables that you will replace with your own values.

```
configure
  apn-remap-table table_name
    apn-selection-default first-in-subscription
    wildcard-apn pdp-type ipv4 network-identifier apn_net_id
    blank-apn network-identifier apn_net_id (SGSN only)
    end
```

Notes:

- The **apn-selection-default first-in-subscription** command is used for APN redirection to provide "guaranteed connection" in instances where the UE-requested APN does not match the default APN or is missing completely. In this example, the first APN matching the PDP type in the subscription is used. The first-in-selection keyword is an MME feature only.

- Some of the commands represented in the example above are common and some are product-specific. Refer to the *APN-Remap-Table Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.
- This profile will only become valid when it is associated with an operator policy.

Operator Policy Configuration

This section provides the configuration example to create an operator policy and enter the operator policy configuration mode.

Use the commands in this mode to associate profiles with the policy, to define and associate APNs with the policy, and to define and associate IMEI ranges. Note: IMEI ranges are supported for SGSN only.

The example below includes sample variable that you will replace with your own values.

```
configure
  operator-policy policy_name
    associate call-control-profile profile_name
    apn network-identifier apn-net-id_1 apn-profile apn_profile_name_1
    apn network-identifier apn-net-id_2 apn-profile apn_profile_name_1
    imei range <imei_number to imei_number imei-profile name profile_name
    associate apn-remap-table table_name
    end
```

Notes:

- Refer to the *Operator-Policy Configuration Mode* chapter in the *Command Line Interface Reference* for command details and variable options.
- This policy will only become valid when it is associated with one or more IMSI ranges (SGSN) or subscriber maps (MME and S-GW).

IMSI Range Configuration

This section provides IMSI range configuration examples for each of the products that support operator policy functionality.

Configuring IMSI Ranges on the MME or S-GW

IMSI ranges on an MME or S-GW are configured in the Subscriber Map Configuration Mode. Use the following example to configure IMSI ranges on an MME or S-GW:

```
configure
  subscriber-map name
    lte-policy
      precedence number match-criteria imsi mcc mcc_number mnc mnc_number msin
 first start_range last end_range operator-policy-name policy_name
      end
```

Notes:

- The precedence number specifies the order in which the subscriber map is used. 1 has the highest precedence.
- The operator policy name identifies the operator policy that will be used for subscribers that match the IMSI criteria and fall into the MSIN range.

Configuring IMSI Ranges on the SGSN

The example below is specific to the SGSN and includes sample variables that you will replace with your own values.

```
configure
  sgsn-global
    imsi-range mcc 311 mnc 411 operator-policy oppolicy1
    imsi-range mcc 312 mnc 412 operator-policy oppolicy2
    imsi-range mcc 313 mnc 413 operator-policy oppolicy3
    imsi-range mcc 314 mnc 414 operator-policy oppolicy4
    imsi-range mcc 315 mnc 415 operator-policy oppolicy5
    end
```

Notes:

- Operator policies are not valid until IMSI ranges are associated with them.

Associating Operator Policy Components on the MME

After configuring the various components of an operator policy, each component must be associated with the other components and, ultimately, with a network service.

The MME service associates itself with a subscriber map. From the subscriber map, which also contains the IMSI ranges, operator policies are accessed. From the operator policy, APN remap tables and call control profiles are accessed.

Use the following example to configure operator policy component associations:

```
configure
  operator-policy name
    associate apn-remap-table table_name
    associate call-control-profile profile_name
    exit
  lte-policy
    subscriber-map name
      precedence match-criteria all operator-policy-name policy_name
      exit
    exit
  context mme_context_name
    mme-service mme_svc_name
      associate subscriber-map name
      end
```

Notes:

- The **precedence** command in the subscriber map mode has other **match-criteria** types. The **all** type is used in this example.

Configuring Accounting Mode for S-GW

The **accounting mode** command configures the mode to be used for the S-GW service for accounting, either **GTPP** (default), **RADIUS/Diameter**, or **None**.

Use the following example to change the S-GW accounting mode from GTPP (the default) to RADIUS/Diameter:

```
configure
   context sgw_context_name
      sgw-service sgw_srv_name
         accounting mode radius-diameter
         end
```

Notes:

- An accounting mode configured for the call control profile will override this setting.

Verifying the Feature Configuration

This section explains how to display the configurations after saving them in a .cfg file as described in the *System Administration Guide*.

Important All commands listed here are under Exec mode. Not all commands are available on all platforms.

Verify that the operator policy has been created and that required profiles have been associated and configured properly by entering the following command in Exec Mode:

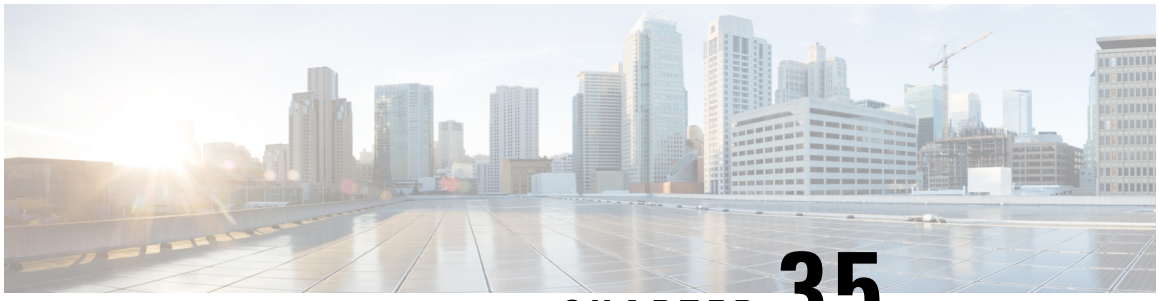
show operator-policy full name *oppolicy1*

The output of this command displays the entire configuration for the operator policy configuration.

```
show operator-policy full name oppolicy1
Operator Policy Name = oppolicy1
Call Control Profile Name                   : ccprofile1
   Validity                                 : Valid
APN Remap Table Name                        : remap1
   Validity                                 : Valid
IMEI Range 711919739      to       711919777
   IMEI Profile Name                        : imeiprof1
      Include/Exclude                       : Include
        Validity                            : Valid
APN NI homers1
   APN Profile Name                         : apn-profile1
      Validity                              : Valid
```

Notes:

- If the profile name is shown as "Valid", the profile has actually been created and associated with the policy. If the Profile name is shown as "Invalid", the profile has not been created/configured.
- If there is a valid call control profile, a valid APN profile and/or valid IMEI profile, and a valid APN remap table, the operator policy is valid and complete if the IMSI range has been defined and associated.



CHAPTER 35

Paging in Common Routing Area for 2G and 3G

- Feature Description, on page 393
- How it Works, on page 393
- Configuring Paging in Common Routing Area for 2G and 3G, on page 395
- Monitoring and Troubleshooting Paging in Common Routing Area for 2G and 3G feature, on page 395

Feature Description

If the RA is configured in both 2G and 3G, the SGSN now supports paging in both the RATs. In previous releases common Routing Area across 2G and 3G was not supported completely. Paging was done only in the last known RAT and power-off detach from other RAT was not supported.

With the introduction of this feature, the following enhancements have been made:

1. If paging has to be done in RA which is common across the RATs, the SGSN supports paging initiation in both the RATs.
2. The SGSN accepts power-off detach from the common RA.
3. If the MS is in STANDBY or PMM-IDLE state and a downlink packet arrives at the SGSN, paging is done. This is applicable for both A/Gb and Iu modes.

GPRS detach (power-off) may be initiated by the MS, but as the request is received in switched off mode the core network does not send a Detach Accept. When the Routing Area is shared across (Iu/Gb), the Detach Request is accepted at any of the modes and the subscriber details are cleared.

How it Works

This section describes the support for common Routing Area (RA) for 2G and 3G in detail. Consider the following 2G and 3G scenarios:

Paging in Common Routing Area for 2G subscriber

The Subscriber is attached in 2G and is in Standby state. Downlink data is received at the SGSN and it starts paging in both 3G and 2G as the RA is shared.

Scenario-1:

- A detach request (power off) is sent in 3G, stop paging in 2G
- Handle the detach request (power off).

Scenario-2:

- If detach request (power off) is sent in 3G, stop paging in 3G
- Indicate to the 2G network

Scenario-3:

- If page response arrives in 2G, stop paging in 3G
- Handle the page response in 2G.

Scenario-4:

- If service request arrives in 3G, drop the packet.

Any packet other than RAU, Attach and Detach (power off) as page response will be dropped in the other RAT.

In paging policy has to be RA based under GPRS service to initiate common RA paging.

To enable common Routing Area paging, the configured paging-policy under the GPRS service must be Routing Area based. If the paging-policy configuration is not Routing Area based BSSGP paging, this feature will not be supported though the Routing Area is shared.

Paging in Common Routing Area for 3G subscriber

The Subscriber is attached in 3G and is in an IDLE state. Downlink data is received at the SGSN and it starts paging in both 3G and 2G as the RA is shared.

Scenario-1:

- If a detach request (power off) is sent in 3G, stop paging in 2G.
- Handle detach request (power off).

Scenario-2:

- If a detach request (power off) is sent in 2G, stop paging in 2G.
- Indicate to 3G network.

Scenario-3:

- If service request is sent in 3G, stop paging in 2G.
- Handle the page response in 3G.

Scenario-4:

- If a page response (LLC PDU) arrives in 2G, drop the packet.

Any packet other than RAU, Attach and Detach (power off) as page response will be dropped in the other RAT.

The paging algorithm under GPRS service will be applicable if a BSSGP page is done for 3G subscriber. If the paging-policy configuration is not Routing Area based BSSGP paging, this feature will not be supported though the Routing Area is shared.

Once a valid response arrives, both the RANAP page and BSSGP page will be stopped. However, in case of expiry the other RAT will not be informed it will continue to page.

Standards Compliance

Support for Paging in Common Routing Area for 2G and 3G complies with the following standard:

- 3GPP TS 23.060 (version 10.0)

Configuring Paging in Common Routing Area for 2G and 3G

The following command is configured to enable support for this feature:

```
config
  sgsn-global
    no common-ra-paging
    exit
```

This command enables paging across common Routing Area (RA) for 2G and 3G. For more information on this command, see the *Command Line Interface Reference*.

Verifying the Paging in Common Routing Area for 2G and 3G Configuration

Execute the following command to verify the configuration of this feature:

show sgsn-mode

The following parameter indicates if common Routing Area paging is "Enabled" or "Disabled":

- Common RA Paging

Monitoring and Troubleshooting Paging in Common Routing Area for 2G and 3G feature

This section provides information on the show commands and bulk statistics available to support this feature.

Paging in Common Routing Area for 2G and 3G Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of the Paging in Common Routing Area for 2G and 3G feature:

show gmm-sm statistics

The following new parameters are added to this show command to display the statistics for this feature:

Paging Statistics

- Total-CRA-Page-Req-Same-RAT
- 3G-PS-CRA-Page-Req
- Total-CRA-Page-Ret-Same-RAT

- 3G-PS-CRA-Page-Ret-Req-in-2G
- Total-CRA-Page-Req-Other-RAT
- 3G-PS-CRA-Page-Req-in-2G
- Total-CRA-Page-Ret-Other-RAT
- 3G-PS-CRA-Page-Ret-Req
- Total-CRA-Page-Rsp-Same-RAT
- 3G-PS-CRA-Page-Rsp
- Total-CRA-Page-Rsp-Other-RAT
- 3G-PS-CRA-Attach-from-2G
- 3G-PS-CRA-RAU-from-2G
- 3G-PS-CRA-Power-Off-from-2G
- Total-CRA-Page-TO-Other-RAT
- 3G-PS-CRA-Timeout-in-2G
- Total-CRA-Page-Stop
- 3G-PS-CRA-Page-Stop
- 2G-PS-CRA-Page-in-3G
- 2G-PS-CRA-Page-Ret-Req-in-3G
- 2G-PS-CRA-Page-Req
- 2G-PS-CRA-Page-Ret-Req
- 2G-PS-CRA-Page-Rsp
- 2G-PS-CRA-Attach-from-3G
- 2G-PS-CRA-RAU-from-3G
- 2G-PS-CRA-Power-Off-from-3G
- 2G-PS-CRA-Timeout-in-3G
- 2G-PS-CRA-Page-Stop

Non-Paging Statistics

- 3G-CRA-Attach
- 3G-CRA-RAU
- 3G-CRA-Power-Off
- 2G-CRA-Attach
- 2G-CRA-RAU
- 2G-CRA-Power-Off

Paging in Common Routing Area for 2G and 3G Bulk Statistics

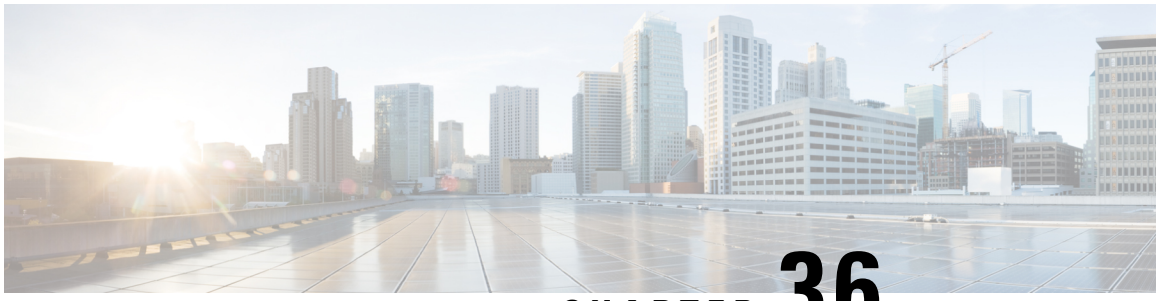
The following statistics are included in the SGSN Schema in support of this feature:

SGSN Schema

- common-ra-3g-page-req-same-rat
- common-ra-2g-page-req-same-rat
- common-ra-3g-page-req-ret-same-rat
- common-ra-2g-page-req-ret-same-rat
- common-ra-3g-page-req-other-rat
- common-ra-2g-page-req-other-rat
- common-ra-3g-page-req-ret-other-rat

- common-ra-2g-page-req-ret-other-rat
- common-ra-3g-page-rsp-same-rat
- common-ra-2g-page-rsp-same-rat
- common-ra-3g-page-rsp-attach-other-rat
- common-ra-2g-page-rsp-attach-other-rat
- common-ra-3g-page-rsp-rau-other-rat
- common-ra-2g-page-rsp-rau-other-rat
- common-ra-3g-page-rsp-power-off-other-rat
- common-ra-2g-page-rsp-power-off-other-rat
- common-ra-3g-page-timeout-other-rat
- common-ra-2g-page-timeout-other-rat
- common-ra-3g-page-stop
- common-ra-2g-page-stop
- common-ra-3g-attach-other-rat
- common-ra-2g-attach-other-rat
- common-ra-3g-rau-other-rat
- common-ra-2g- rau-other-rat
- common-ra-3g-power-off-other-rat
- common-ra-2g-power-off-other-rat

For descriptions of these variables, see "SGSN Schema Statistics" in the *Statistics and Counters Reference*.



CHAPTER 36

Page Throttling

This chapter describes the Page Throttling feature.

- Feature Description, on page 399
- How it Works, on page 400
- Configuring Page Throttling, on page 404
- Monitoring and Troubleshooting the Page Throttling feature, on page 406

Feature Description

The Page Throttling feature limits the number of paging messages going out of the SGSN. It provides flexibility and control to the operator who can now reduce the number of paging messages going out from the SGSN based on the network conditions. In some of the customer locations, the amount of paging messages initiated from the SGSN is very high due to the bad radio conditions. A higher number of paging messages results in the consumption of bandwidth in the network. This feature provides a configurable rate-limit, in which the paging message gets throttled at:

- Global level for both 2G and 3G accesses
- NSE level for 2G only
- RNC level for 3G only

This feature improves the bandwidth consumption on the radio interface.

Important A RLF license is required to configure a RLF Template.

Relationships to Other SGSN Features

The Page Throttling feature inter-works with common RA paging, in which paging messages are initiated from both 2G and 3G accesses or vice versa.

Introduction of the Page Throttling feature does not result in any changes to the existing paging procedures.

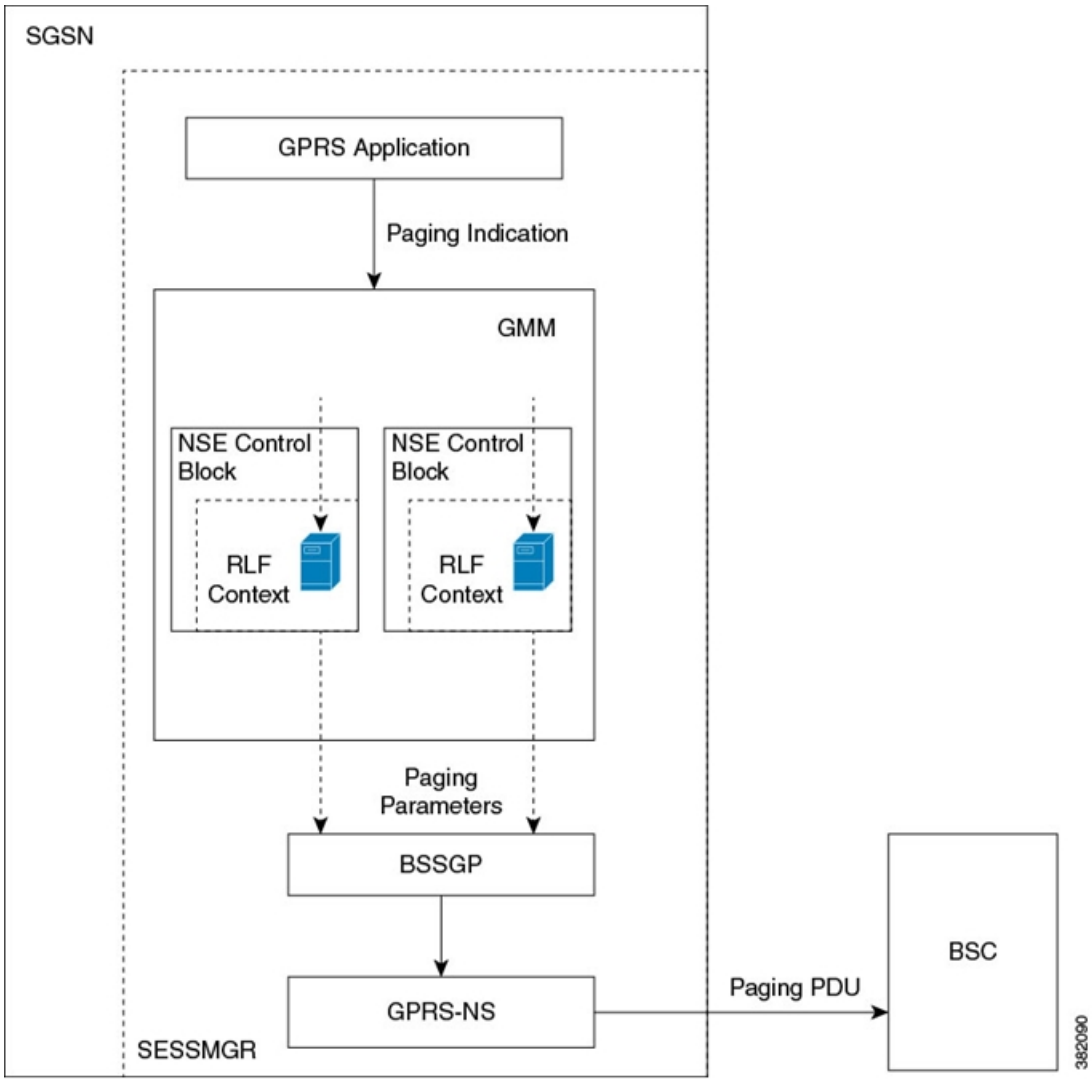
How it Works

The Rate Limiting Function (RLF) framework is used to limit the paging load sent from the SGSN. The Rate Limiting function is a generic framework which provides the rate-limiting functionality using the Token Bucket algorithm to achieve rate-limiting.

Page Throttling in a GPRS Scenario

The diagram below represents the design of the Page Throttling feature in a 2G scenario:

Figure 71: Paging Process in 2G with Rate Limiting



The following modules inter-work with each other to achieve page throttling in a GPRS scenario:

1. The Session Manager

2. The GPRS Application
3. The GMM Layer
4. The GPRS Stack
5. RLF Module

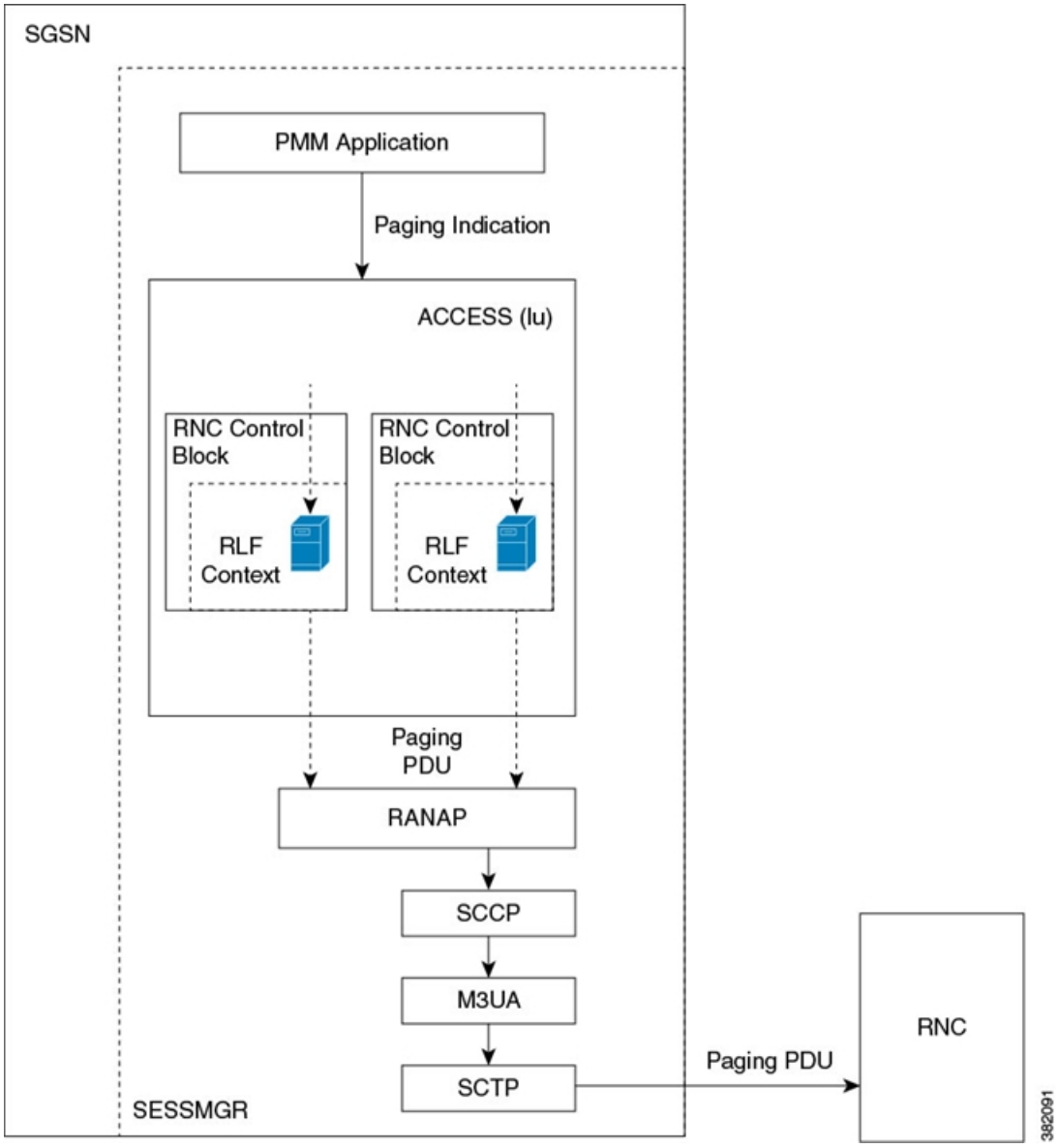
Consider the following GPRS scenario, where the SGSN wants to send downlink data or signaling messages to a subscriber and the subscriber is in a STAND-BY state:

1. The SGSN initiates a paging message to identify the subscriber's current location.
2. The GPRS application sends an indication to the GMM layer whenever it wants to page the MS either for signaling or data packets. Throttling of paging messages for GPRS is performed at the GMM layer in the Session Manager (SESSMGR). Throttling can be performed either at the Global or NSE level.
3. For throttling at the global level, the RLF context is created at the Session Manager level and is maintained in the GMM Control block in the GMM layer.
4. For throttling at the NSE level, the RLF context is created at the Session Manger level for each NSE and is maintained in the NSE control block in the GMM layer.
5. The GMM layer collects the information about the subscriber to be paged and sends it to the RLF module for throttling. The RLF template is configurable, and the RLF module performs the throttling function based on the thresholds configured in the template.
6. The RLF module applies the rate limiting algorithm based on the configured limits. It sends or queues paging message based on the configured limits, once the maximum rate or the configured threshold is reached the paging messages are dropped by the RLF module.
7. The GMM layer registers the call-back functions which are used by RLF module to send the paging messages out of SGSN.

Page Throttling in an UMTS Scenario

The diagram below represents the design of the Page Throttling feature in a 3G scenario:

Figure 72: Paging Process in 3G with Rate Limiting



The following modules inter-work with each other to achieve page throttling in a UMTS scenario:

1. The Session Manager
2. The PMM Application
3. The Access Layer
4. The RANAP Stack
5. RLF Module

Consider the following UMTS scenario, where the SGSN wants to send downlink data or signaling messages to a subscriber and the subscriber is in a STAND-BY state:

1. The SGSN initiates a paging message to identify the subscriber's current location.
2. The PMM application sends an indication to the Access layer whenever it wants to page the MS either for signaling or data packets. Throttling of paging messages for UMTS is performed at the Access layer in the Session Manager (SESSMGR). Throttling can be performed either at the Global or NSE level.
3. For throttling at the global level, the RLF context is created at the Session Manager level and is maintained in the Access layer.
4. Currently, the SGSN does not allow configuring the same RA in different RNCs across the IuPS services, instead it allows only within the same IuPS service. For throttling at the RNC level, the RLF context is created for each RNC and is maintained in the RNC control block of the Access layer in the Session Manager.
5. The Access layer collects the information about the subscriber to be paged and sends it to the RLF module for throttling. The RLF template is configurable, and the RLF module performs the throttling function based on the thresholds configured in the template.
6. The RLF module applies the rate limiting algorithm based on the configured limits. It sends or queues paging message based on the configured limits, once the maximum rate or the configured threshold is reached the paging messages are dropped by the RLF module.
7. The Access layer registers the call-back functions which are used by RLF module to send the paging messages out of SGSN.

Limitations

Listed below are the known limitations of the Page Throttling feature:

- In the SGSN Global configuration mode "interface" command, the NSE-NAME (already existing) and RNC-NAME (added as part of this feature) are not validated against the configuration under GPRS-SERVICE or IuPS-SERVICE. This configuration is used only for the purpose of associating the paging-rlf-template for the peer entity (either NSE/BSC or RNC). It is possible to change the ID to NAME mapping of both BSC and RNC. The BSC/RNC ID is used for associating the paging-rlf-template as well as throttling the paging messages internally even though the user can associate the paging-rlf-template using NAME explicitly.
- The rate limiting parameters for the rlf-template associated at global level should be configured in such a way that it applies to all configured NSE and RNC's. The SGSN does not guarantee a uniform distribution of message rate for each NSE/RNC while throttling at a global level.
- Page throttling is applicable to all RNC's whenever the operator configures the same RNC-ID with different PLMN-ID in different IuPS services. If the operator associates the Paging RLF template for that RNC-ID, the SGSN starts page throttling for both the RNC's irrespective of the PLMN.
- No mechanism is present to identify if the operator associates the paging-rlf-template by either configured RNC name or RNC identifier while generating the CLI for "show/save configuration". The paging-rlf-template CLI is always generated with the RNC name if the operator configured the name mapping even though the association is done using the RNC-ID otherwise the output is always generated with the RNC-ID.
- Currently, the show output "show sgsn mode interface-mgmt-status" displays a maximum of "32" characters (truncated value) of the name configured for both NSE/RNC and the RLF template name.
- The SGSN does not support paging load limitation to the common RA paging initiated in the other access.

- Whenever the operator removes the association of paging-rlf-template from a particular NSE/RNC and if the page-limiting is already enabled at global level, all the queued messages in RLF context maintained for that NSE/RNC will be flushed out by RLF and it does not accept any new paging messages for throttling. The RLF context for that NSE/RNC will be cleaned up after all the messages in the queue flushed out. All the new paging messages for that NSE/RNC will use the global RLF context for further rate-limiting.
- Currently, the paging message initiated for both signalling and data packets are treated with same priority as the generic RLF framework does not support priority for throttling.
- Run time association of Paging RLF template to global or per entity level (NSE/RNC) results in statistics discrepancy (when it gets associated during re-transmission of paging messages already in progress).
- This feature results in a performance impact whenever the GPRS service is configured with many NSE's and when the service is stopped or removed.

Configuring Page Throttling

The following commands are used to configure the Page Throttling feature. These CLI commands are used to associate/remove the RLF template for Page Throttling at the Global level, NSE level and RNC level at the SGSN.

To map RNC Name to RNC Identifier

The **interface** command is used to configure the mapping between the RNC Id and the RNC name. The operator can configure the paging-rlf-template either by RNC name or RNC identifier.

```
config
 sgsn-global
  interface-management
   [ no ] interface {gb peer-nsei | iu peer-rnc} {name value | id value }
   exit
```

Notes:

The **no** form of the command removes the mapping and other configuration associated for the RNC paging-rlf-template configuration from the SGSN and resets the behavior to default for that RNC.

Example configurations:

```
configure
   sgsn-global
      interface-management
         interface iu peer-rnc id 250 name bng_rnc1
         end
```

To associate a paging RLF template

This command allows the SGSN to associate a RLF template either at the global level which limits the paging messages initiated across both 2G (NSE level) and 3G (RNC level) access or at the per entity level either at RNC level for 3G access or at NSE level for 2G access.

```
config
 sgsn-global
  interface-management
   [ no ] paging-rlf-template { template-name template-name } { gb peer-nsei
 | iu peer-rnc } { name value | id value }
   exit
```

Notes:

If there no rlf-template is associated for a particular NSE/RNC then the paging load is limited based on the global rlf-template associated (if present). If no global rlf-template associated then, no rate-limiting is applied on the paging load.

```
sgsn-global
  interface-management
    paging-rlf-template template-name rlf1
    end
```

```
configure
  sgsn-global
    interface-management
      paging-rlf-template template-name rlf2 gb peer-nsei id 1
      end
```

```
configure
  sgsn-global
    interface-management
      paging-rlf-template template-name rlf2 iu peer-rnc name bng_rnc1
      end
```

For more information on the CLI commands, see the *Command Line Interface Reference*.

The RLF template can be configured under the global configuration mode which provides the option to configure the message-rate, burst-size, threshold and delay-tolerance for throttling or rate-limiting. To configure the RLF template, see the *Command Line Interface Reference*.

Verifying the Page Throttling Configuration

The Page Throttling feature configuration can be verified by executing the following show commands:

- **show configuration**

  Listed below are the parameters added for the Page Throttling feature:

  - **paging-rlf-template template-name**
  - **paging-rlf-template template-name gb peer-nsei id**
  - **paging-rlf-template template-name iu peer-rnc id**
  - **interface iu peer-rnc id rnc_id name name**

- **show sgsn-mode interface-mgmt-status**

  Listed below are the parameters added for the Page Throttling feature:

  - **Global Paging RLF template**

- **Paging RLF Template**

Monitoring and Troubleshooting the Page Throttling feature

This section provides information on the show outputs updated with new statistics to support the Page Throttling feature.

Page Throttling Show Command(s) and/or Outputs

Listed below are the show outputs and new statistics added for the Page Throttling feature:

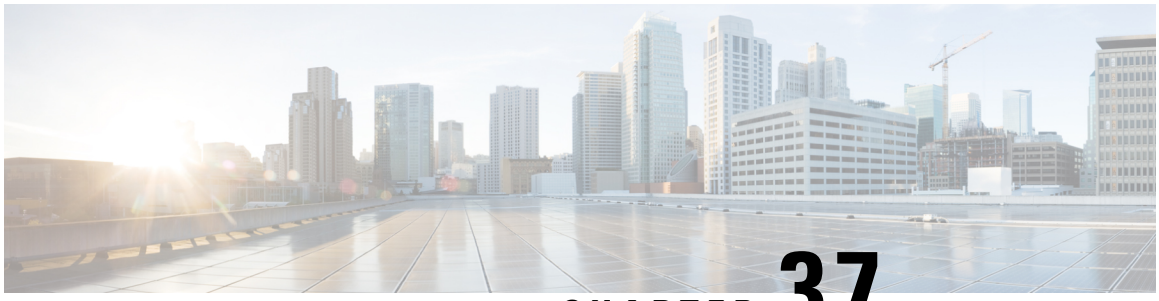
show gmm-sm statistics verbose

The following new statistics are added in the **show gmm-sm statistics verbose** status command to support the Page Throttling feature:

- 3G Page Throttling statistics
- PS-Page-Req sent by RLF
- Ret-PS-Page-Req sent by RLF
- PS-Page-Req dropped by RLF
- Ret-PS-Page-Req dropped by RLF
- PS-Page-Req dropped due to no memory
- 2G Page Throttling statistics
- Paging Request sent out by RLF
- Total-Page-Req sent
- Ret-Total-Page-Req sent
- Page-Requests-LA
- Ret-Page-Requests-LA
- Page-Requests-RA
- Ret-Page-Requests-RA
- Page-Requests-BSS
- Ret-Page-Requests-BSS
- Page-Requests-Cell
- Ret-Page-Requests-Cell
- Paging Request dropped by RLF
- Total-Page-Req dropped

- Ret-Total-Page-Req dropped
- Page-Requests-LA
- Ret-Page-Requests-LA
- Page-Requests-RA
- Ret-Page-Requests-RA
- Page-Requests-BSS
- Ret-Page-Requests-BSS
- Page-Requests-Cell
- Ret-Page-Requests-Cell
- PS-Page-Req dropped due to no memory

For detailed information and description of the parameters see, *Statistics and Counters Reference*.



CHAPTER 37

PGW Restart Notification in S4-SGSN

This chapter describes the PGW Restart Notification in S4-SGSN.

- Feature Description, on page 409
- Overview, on page 409
- How it Works, on page 410
- Configuring PGW Restart Notification in S4-SGSN, on page 411
- Monitoring and Troubleshooting PRN support in S4-SGSN, on page 412

Feature Description

The purpose of enabling PGW Restart Notification (PRN) in S4-SGSN is to provide a simple and optimized solution for handling the signaling overload on the SGSN when a PGW failure occurs. Until release 10, the SGW used to send Delete Bearer Request for every PDN connection activated through the failed PGW. This results in signaling overload on the SGSN. From 3GPP Release 10 specifications onwards it is possible for a SGW to indicate a PGW failure through a single PRN message to the SGSN.

When the SGW detects that a peer PGW has restarted or it is not reachable, it deletes all the PDN connections associated with that peer node and releases all the internal resources associated with those PDN connections.

The SGW sends a PGW Restart Notification only to the SGSNs that have configured advertisement of PGW restart notification in echo request/response messages. When the S4-SGSN receives this message, according to the control plane IP address of the restarted PGW and the control plane IP address of the SGW on the S4 interface included in the message, the S4-SGSN deletes all PDN connections associated with the SGW and the restarted PGW. The SGSN also releases any internal resources associated with those PDN connections.

The S4-SGSN sends a PGW Restart Notification Acknowledge message in response to the PGW Restart Notification message sent by the SGW.

Overview

Listed below is an overview of the PRN feature in the S4-SGSN:

- When the PGW Restart Notification is enabled at the S4-SGSN, the PRN bit in Node Features IE in Echo Request message is set. This indicates to the SGW that the S4-SGSN supports PGW Restart Notification message (PRN).

- The SGW sends the PRN message to the S4-SGSN in case of PGW node restart or if a path failure occurs. In case of PGW node restart the PRN arrives without any cause, but if a path failure has occurred the PRN is received with cause "PGW not responding".
- The S4-SGSN on receiving the PRN, deletes all PDN connections associated with the SGW and the restarted PGW. It also releases the internal resources associated with those PDN connections.
- The S4-SGSN prioritizes the PDN connections to be restored based on subscribed APN restoration priority (if received from the HSS). A locally configured value as default restoration priority shall be used for a user's PDN connection if it is not received from the HSS. Restoration priority value received in subscription record from HSS value has more priority over locally configured default value.
- If the S4-SGSN wants to restore the PDN connections, it does so by using the "reactivation requested" cause if restoration priority value is available irrespective of whether UE is in CONNECTED or IDLE state.
- Deactivation is performed with cause "regular deactivation" if the UE is in CONNECTED state and restoration priority is not available. If the UE is in IDLE state and restoration priority value is not available, then local deactivation is done.

How it Works

Listed below is a detailed description of how the PGW restart notification feature in S4-SGSN works:

1. The PRN support should be enabled through the **gtpc** command in egtp-service configuration mode.
2. If PRN is received and support for PRN is not configured then the S4-SGSN sends PRN Acknowledge message with EGTP_CAUSE_SERVICE_DENIED cause code.
3. If PRN is received and support for PRN is configured then S4-SGSN responds with PRN Acknowledge message with cause code EGTP_CAUSE_REQ_ACCEPTED.
4. When PRN is enabled at the S4-SGSN, the PRN bit in Node Features IE in Echo Request message is set. This indicates to the SGW that the S4-SGSN supports PGW Restart Notification message.
5. The SGW sends the PRN to the S4-SGSN in case of PGW node restart or path failure. In case of PGW node restart, PRN arrives without any cause. In case of path failure, PRN is received with cause specified as "PGW not responding". The behavior of S4-SGSN on receiving PRN is same in both scenarios.
6. When a PRN is received, the PDN connections are deleted based on SGW and PGW address received in PRN message.
7. The S4-SGSN restores the PDN connections by sending Deactivate Request to UE using sm cause "reactivation required".
8. Restoration will be done only when the restoration priority is received from the HSS subscription for that PDN or when the default apn-restoration priority is configured locally under the apn-profile.

Limitations

The PRN feature in S4-SGSN supports either IPv4 or IPv6 but not both at the same time.

Standards Compliance

The PRN feature in S4-SGSN complies with the following standards:

- 3GPP TS 23.007 version 11
- 3GPP TS 29.274 version 11

Configuring PGW Restart Notification in S4-SGSN

The following commands are used to configure the PGW restart notification support in the S4-SGSN:

Configure Node IE For PRN Advertisement

The following CLI command configures advertisement of PGW Restart Notification in echo request/response messages. This is an existing CLI command under the EGTP Service Configuration mode which has to be configured in order to inform SGW that S4-SGSN supports receiving PRN. The command option **node-feature pgw-restart-notification** has to be configured in order to inform SGW that S4-SGSN supports receiving PRN.

```
configure
    context context_name
        egtp_service service_name
           gtpc { bind { ipv4-address ipv4_address [ ipv6-address ipv6_address
 ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } | echo-interval
 seconds [ dynamic [ smooth-factor multiplier ] ] | echo-retransmission-timeout
 seconds | ip qos-dscp { forwarding_type } | max-retransmissions num  |
node-feature pgw-restart-notification | path-failure detection-policy
echo  | private-extension overcharge-protection | retransmission-timeout
 seconds  }
            exit
```

Configure Default APN Restoration Priority

The following CLI command configures APN restoration priority for an APN profile:

```
configure
    apn-profile profile_name
              apn-restoration priority priority_value
              exit
```

Notes:

- The PGW Restart Notification (PRN) message is sent by the S-GW when it detects a peer P-GW has re-started. The S4-SGSN on receiving the PRN message, uses the default apn-restoration priority value, if priority value is not available in HSS Subscription to prioritize the affected PDN connections for restoration. To restore PDN it is mandatory to get priority value from HSS in subscription record or default value must be configured under apn-profile.
- The priority value is an integer value from 1 through 16. Where "1" is the highest priority and "16" is the lowest priority.

Verifying the PRN Configuration in S4-SGSN

Execute the command **show egtp-service all** to verify the PRN support configuration in S4-SGSN:

```
show egtp-service all
```

The output of this command displays if the PRN support has been configured:

```
.
.
.
GTPC Node Feature

PGW Restart Notification
                                                    : Enabled
.
.
```

Monitoring and Troubleshooting PRN support in S4-SGSN

This section provides information on the show commands and disconnect reasons available to support this feature.

PGW Restart Notification Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of the PRN feature in S4-SGSN:

show s4-sgsn statistics

The following PDP Deletion Statistics have been added to the **show s4-sgsn statistics** command:

- PDP Deletion Statistics
- 3G S4 PDPs Deleted due to PGW Restart Notification
- 2G S4 PDPs Deleted due to PGW Restart Notification

show egtpc statistics

The following PGW Restart Notification statistics have been added to **show egtpc statistics** :

- PGW Restart Notification Request
- Total RX
- Initial RX
- Retrans RX
- PGW Restart Notification Ack
- Total TX
- Initial TX
- Accepted
- Denied
- Discarded

Notes:

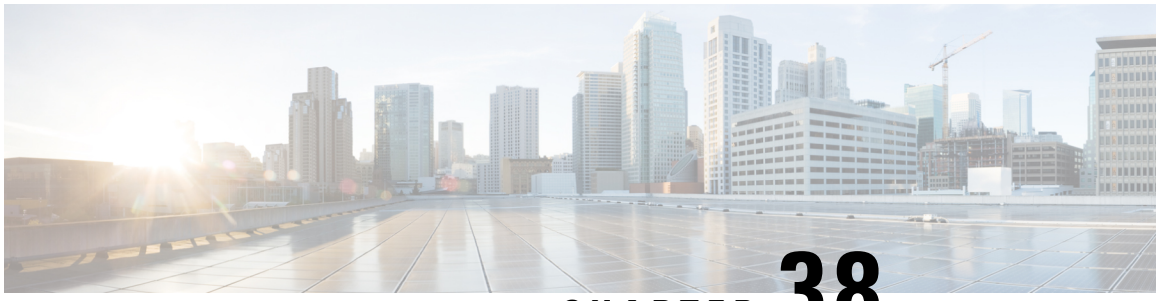
- When APN Restoration priority value is available, either through local configuration or through subscription received from HSS, then the SGSN sends Deactivation Request with SM Cause "Reactivation Required" towards MS after PGW Restart Notification Request from SGW.
- When APN Restoration priority value is not available and the subscriber is in Idle/Standby state, the SGSN deletes the affected bearers locally and does not trigger Paging Request towards the MS to send Deactivation Request.

- When APN Restoration priority value is not available and the subscriber is in Connected/Ready state, the SGSN will send Deactivation Request.

show session disconnect-reasons verbose

The following disconnect reason is used to track both PGW Restart or path failure and SGW path failure:

- sgsn-gtpc-path-failure(267)



CHAPTER 38

Quality of Service (QoS) Management for SGSN

This chapter describes the implementation of Quality of Service (QoS) related features and functionali ties in SGSN.

- Quality of Service Management, on page 415

Quality of Service Management

The network associates a certain Quality of Service (QoS) with each data transmission in the GPRS packet mode. The QoS attributes are collectively termed as a "QoS Profile". The PDP context stores the QoS Profile information. The QoS management is performed by using the PDP context management procedures, such as PDP context activation, modification and de-activation. QoS enables the differentiation between services provided.

SGSN Quality of Service Management

The SGSN applies an admission control function on each PDP context activation request. The function results in further processing of the request; that is, either negotiation of the QoS with the Mobile Subscriber (MS), or rejection of the PDP context activation request. The SGSN negotiates QoS with the MS when the level requested by the subscriber cannot be supported or when the QoS level negotiated from the previous SGSN cannot be supported at an inter-SGSN routing area update. The response to the mobile subscriber depends on the provisioned subscription data, the requested QoS, the QoS permitted by the Gateway node and the QoS permitted by the Radio Access Network.

Quality of Service Attributes

In an End-to- End Service the network user is provided with a certain Quality of Service, which is specified by a set of QoS attributes or QoS profile. The first list of attributes was defined in Release 97/98 of the 3GPP recommendations but these are now replaced by Release 99 3GPP recommendations. Many QoS profiles can be defined by the combination of these attributes. Each attribute is negotiated by the MS and the GPRS/UMTS/LTE network. If the negotiated QoS profiles are accepted by both parties then the network will have to provide adequate resources to support these QoS profiles.

In Release 97/98 recommendations, the PDP context is stored in the MS, SGSN and GGSN. It represents the relation between one PDP address, PDP type (static or dynamic address), the address of a GGSN that serves as an access point to an external PDN, and one Quality of Service (QoS) profile. PDP contexts with different

QoS parameters cannot share the same PDP address. In Release 99 recommendations a subscriber can use more than one PDP contexts with different QoS parameters and share the same PDP address.

Quality of Service Attributes in Release 97/98

In Release 97/98 of the 3GPP recommendations, QoS is defined according to the following attributes:

- **Precedence Class:** This attribute indicates the packet transfer priority under abnormal conditions, for example during a network congestion load.
- **Reliability Class:** This attribute indicates the transmission characteristics. It defines the probability of data loss, data delivered out of sequence, duplicate data delivery, and corrupted data. This parameter enables the configuration of layer "2" protocols in acknowledged or unacknowledged modes.
- **Peak Throughput Class:** This attribute indicates the expected maximum data transfer rate across the network for a specific access to an external packet switching network (from 8 Kbps up to 2,048 Kbps).
- **Mean Throughput Class:** This attribute indicates the average data transfer rate across the network during the remaining lifetime of a specific access to an external packet switching network (best effort, from 0.22 bps up to 111 Kbps).
- **Delay Class:** This attribute defines the end-to-end transfer delay for the transmission of Service Data Units (SDUs) through the GPRS network. The SDU represents the data unit accepted by the upper layer of GPRS and conveyed through the GPRS network.

Quality of Service Attributes in Release 99

The attributes of GPRS QoS were modified in Release 99 of the 3GPP recommendations in order to be identical to the ones defined for UMTS.

The quality of service is a type "4" information element with a minimum length of "14" octets and a maximum length of "18" octets.

The Release 99 of 3GPP recommendations defines QoS attributes such as Traffic class, Delivery order, SDU format information, SDU error ratio, Maximum SDU size, Maximum bit rate for uplink, Maximum bit rate for downlink, Residual bit error ratio, Transfer delay, Traffic-handling priority, Allocation/retention priority, and Guaranteed bit rate for uplink and Guaranteed bit rate for downlink. The attributes are listed below:

- **Traffic Class:** Indicates the application type (conversational, streaming, interactive, background). Four classes of traffic have been defined for QoS:
  - **Conversational Class:** These services are dedicated to bi-directional communication in real time (for example, voice over IP and video conferencing).
  - **Streaming Class:** These services are dedicated to uni-directional data transfer in real time (for example, audio streaming and one-way video).
  - **Interactive Class:** These services are dedicated to the transport of human or machine interaction with remote equipment (for example, Web browsing, access to a server and access to a database).
  - **Background Class:** These services are dedicated to machine-to-machine communication; this class of traffic is not delay sensitive (for example, e-mail and SMS).
- **Delivery Order:** Indicates the presence of an in-sequence SDU delivery (if any).
- **Delivery of Erroneous SDUs:** Indicates if erroneous SDUs are delivered or discarded.
- **SDU Format Information:** Indicates the possible exact sizes of SDUs.
- **SDU Error Ratio:** Indicates the maximum allowed fraction of SDUs lost or detected as erroneous.
- **Maximum SDU Size:** Indicates the maximum allowed SDU size (from "10" octets up to "1,520" octets).

- **Maximum Bit Rate for Uplink:** Indicates the maximum number of bits delivered to the network within a period of time (from "0" up to "8,640" Kbps).
- **Maximum Bit Rate for Downlink:** Indicates the maximum number of bits delivered by the network within a period of time (from "0" up to "8,640" Kbps).
- **Residual Bit Error Ratio:** Indicates the undetected bit error ratio for each sub-flow in the delivered SDUs.
- **Transfer Delay:** Indicates the maximum time of SDU transfer for 95th percentile of the distribution of delay for all delivered SDUs.
- **Traffic-Handling Priority:** Indicates the relative importance of all SDUs belonging to a specific GPRS bearer compared with all SDUs of other GPRS bearers.
- **Allocation/Retention Priority:** Indicates the relative importance of resource allocation and resource retention for the data flow related to a specific GPRS bearer compared with the data flows of other GPRS bearers (this attribute is useful when resources are scarce).
- **Guaranteed Bit Rate for Uplink:** Indicates the guaranteed number of bits delivered to the network within a period of time (from "0" up to "8,640" Kbps).
- **Guaranteed Bit Rate for Downlink:** Indicates the guaranteed number of bits delivered to the network within a period of time (from "0" up to "8,640" Kbps).
- **Maximum Bit Rate for Uplink (extended, octet 17):** This field is an extension of the Maximum bit rate for uplink in octet "8". The coding is identical to that of the Maximum bit rate for downlink (extended). It is used to signal extended Maximum bit rates in uplink (up to "256" Mbps)
- **Maximum Bit Rate for Downlink (extended, octet 15):** Used to signal extended bit rates for downlink delivered by the network (up to "256" Mbps). This attribute is supported in 3GPP Release 6 and beyond.
- **Guaranteed Bit Rate for Uplink (extended, octet 18):** This field is an extension of the Guaranteed bit rate for uplink in octet "12". The coding is identical to that of the guaranteed bit rate for downlink (extended). Used to signal extended Guaranteed bit rates in uplink (up to "256" Mbps)
- **Guaranteed Bit Rate for Downlink (extended, octet 16):** Used to signal extended Guaranteed bit rates in downlink (up to "256" MBps). This attribute is supported in 3GPP Release 6 and beyond.

Quality of Service Management in SGSN

QoS management comprises of approximately "23" individual parameters. As part of QoS Management, the SGSN negotiates the MS requested QoS with the following during PDP context Activation and Modification procedures:

- Subscribed QoS
- Local QoS capping limit (if configured)
- QoS sent by GGSN in tunnel management messages
- QoS sent by RNC in RAB assignment messages (UMTS only)

Each negotiation is between QoS parameters of the two sets, and the resulting negotiated QoS will be the lower of the two. QoS negotiation for Secondary PDP contexts is same as Primary PDP context.

For more information see, 3GPP TS 24.008 (section 10.5.6.5 "Quality of Service".

QoS Negotiation During an Activation Procedure

During an Activation procedure the MS requested QoS is negotiated with the subscribed QoS. Higher values are not valid in case of GPRS access, the SGSN restricts some of the QoS parameters during PDP activation in GPRS access. Listed below are the QoS parameters which are restricted in GPRS access:

- Maximum Bitrate (MBR) DL is capped to "472" kbps.

- Maximum Bitrate (MBR) UL is capped to "472" kbps.
- Peak Throughput (PR) is capped to "6" ("32000" octets/sec).
- Reliability class (RC) of "0x2", "Unacknowledged GTP; Acknowledged LLC and RLC, Protected data" is not supported. In such cases, RC is over-ridden as "0x3", "Unacknowledged GTP and LLC; Acknowledged RLC, Protected data"

The SDU Error ratio is capped in following cases:

- For Reliability Class "0x3", the SDU error ratio is capped to "4" ($1x10^{-4}$) if it exceeds a value of "4", a value greater than "4" represents stringent error ratios.
- For Reliability Class greater than "0x3", the SDU error ratio capped to "3" ($1x10^{-3}$) if the value provided exceeds "4".

For more information see, 3GPP TS 23.107 (Table 6 "Rules for determining R99 attributes from R97/98 attributes").

The QoS parameters are sent to GGSN in the Create PDP Context Request. On receiving a Create PDP Context Response, the QoS sent by GGSN is negotiated with the one sent by SGSN to GGSN. For GPRS access, this negotiated QoS is sent to the MS in Activate PDP Context Accept.

If the UE requests a subscribed traffic class, the SGSN defaults it to "Interactive" traffic class regardless of the configuration in the HLR subscription.

In a UMTS access scenario, the negotiated QoS is sent to RNC in RAB Assignment Request. By default, the SGSN includes Alternative Max Bit Rate with type set to "Unspecified". This indicates to the RNC that it can further negotiate the QoS downwards if either the RNC/UE cannot support the QoS value sent. The RNC may downgrade the QoS based on its current load/capability and include it in RAB Assignment Response. The SGSN does QoS negotiation once more with received QoS from the RNC. This is used as the negotiated QoS of PDP context and is sent to the MS in Activate PDP context Accept. If the RNC has downgraded the QoS, the same will be informed to GGSN by means of an Update PDP context procedure.

Important When the MS sends an Activate PDP Context Request, it may set all the QoS values to "0", this implies that the MS is requesting the SGSN to take QoS values from the subscription. In this case the SGSN negotiates the subscribed QoS with any locally configured QoS and sends the negotiated QoS value to GGSN.

QoS Negotiation During a Modification Procedure

The PDP Context Modification procedure can be MS initiated or Network initiated, it is used to change the current negotiated QoS. If it is a MS initiated PDP Context Modification procedure the QoS negotiation is similar to the QoS negotiation followed during an Activation procedure. The HLR or GGSN or SGSN (RNC in case of UMTS access) can perform a Network Initiated QoS modification.

For more information on "PDP Context Modification Procedure" see, 3GPP TS 24.008 section 6.1.3.3

HLR Initiated QoS Modification

The Subscription Information of a Subscriber may change due to the following:

- User action (The user may subscribe for a more premium service)
- Service provider action (The QoS is restricted on reaching download limits)

This change is relayed by the HLR to the SGSN through the Insert Subscription Data procedure. As per 3GPP TS 23.060 section 6.11.1.1 "Insert Subscriber Data procedure", the SGSN negotiates the current QoS with new subscribed QoS and initiates a Network Initiated PDP modification procedure only in case of QoS

downgrade. As part of this procedure, the GGSN (and RNC in case of UMTS access) is updated with the new negotiated QoS followed by the MS. If a failure occurs or no response is received from the MS for the Modify Request, the PDP context is deactivated.

The SGSN is compliant with 3GPP TS 23.060 Release 7 version. The specifications Release 8 and above specify a modified behavior when the UE is in a IDLE/STANDBY state. If the QoS is modified by the HLR when an UE is an IDLE/STANDBY state the PDP is de-activated. The SGSN is made compliant with this change to align its behavior with LTE elements like MME. Therefore the SGSN is compliant with both the Release 7 and Release 8 specifications.

GGSN Initiated QoS Modification

The GGSN may initiate a QoS Modification Request due to any of the following reasons:

- An External Trigger (PCRF)
- Current load or capability of the GGSN
- If the "No Qos negotiation" flag is set in the previous Tunnel Management Request from SGSN.

The SGSN negotiates this QoS with the subscription. The negotiated Qos is then sent to the UE in a Modify PDP Request. In an UMTS access scenario, the SGSN updates the new negotiated QoS to the RNC. The new negotiated Qos is then forwarded to the GGSN in response message.

SGSN Initiated QoS Modification

The SGSN initiated QoS Modification occurs during an Inter-RAT HO (2G to 3G / 3G or 2G), here the negotiated QoS in new access is different from the negotiated QoS in old access. The SGSN QoS initiated QoS Modification can also occur during a new SGSN ISRAU/SRNS procedure where the new negotiated QoS is different from the negotiated QoS received from the peer SGSN.

Whenever a UE performs an Intra or Inter SGSN HO, the SGSN receives the requested QoS, subscribed QoS and the negotiated QoS from the old access (during Intra SGSN HO) or from peer SGSN (during Inter SGSN HO). This requested QoS is then negotiated with the subscribed QoS. If the negotiated QoS is different from the received negotiated QoS, the SGSN initiates a network initiated QoS modification procedure to update the new negotiated QoS to the UE after completing the HO procedure.

RNC Initiated QoS Modification (UMTS access only)

In a RNC initiated QoS modification procedure the SGSN negotiates the QoS with the current negotiated QoS. In case of a downgrade, the SGSN updates the GGSN and MS with the new negotiated QoS.

For more information see, 3GPP TS 23.060 section 9.2.3.6 on "RAN-initiated RAB Modification Procedure"

No QoS Negotiation Flag

When the 'No QoS Negotiation' flag is set, the SGSN indicates to the GGSN not to negotiate the QoS. The "No QoS Negotiation" flag is set in the following scenarios:

- While sending Update PDP Context request during activation (Direct tunnel).
- During a service request for data with direct tunnel enabled for the subscriber, a UPCQ is initiated to inform the GGSN with the teid and the address of the RNC. This Update PDP context request has no negotiation bit set.
- Update PDP context request sent during preservation procedures.
- UPCQ sent to indicate establishment / removal of direct tunnel.
- Intra SGSN SRNS.
- Downlink data for the subscriber without active RABs and direct tunnel enabled for the subscriber, UPCQ is initiated to inform the GGSN of the teid and the address of the RNC. This Update PDP context request has "No QoS Negotiation" flag set.

- In all modification procedures (HLR, RNC, MS) if any other node other than the modifying entity has downgraded the QoS. For example, consider a HLR Initiated Modification procedure where the SGSN does the following signaling:
  - Initiates a UPCQ to inform the GGSN of the QOS change, GGSN sends a UPCR with same QOS as UPCQ.
  - Modify PDP context Request to MS, the MS sends a Modify PDP Accept.
  - RAB establishment request to the RNC, the RNC downgrades the QoS in the RAB assignment response.
  - The SGSN initiates a UPCQ to inform the GGSN of the new QoS sent in the previous step. This UPCQ will have no QoS negotiation bit set.
- If loss of Radio connectivity feature is enabled, then the Update PDP Context initiated to inform the GGSN that the MS is back in Radio Coverage will have the "No Qos Negotiation" bit set.

QoS Features

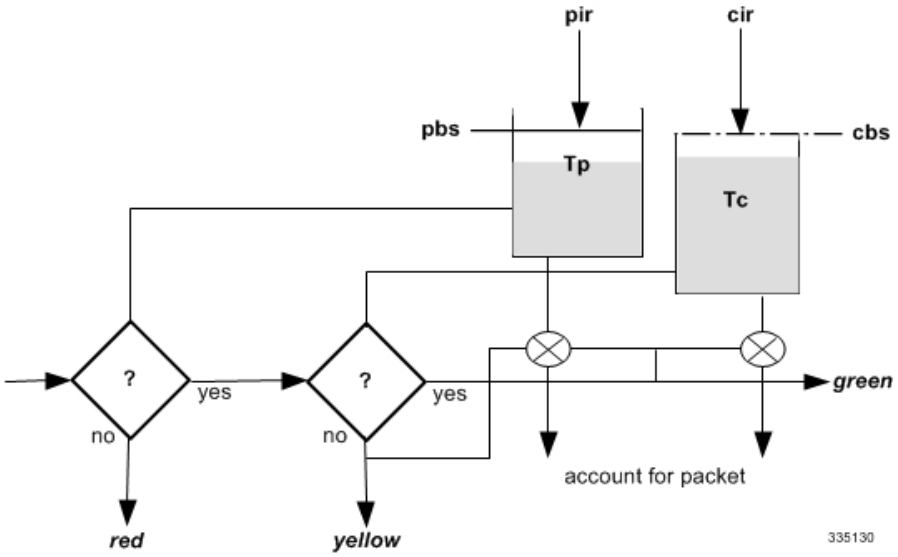
Traffic Policing

The SGSN can police uplink and downlink traffic according to predefined QoS negotiated limits fixed on the basis of individual contexts - either primary or secondary. The SGSN employs the Two Rate Three Color Marker (RFC2698) algorithm for traffic policing. The algorithm meters an IP packet stream and marks its packets either green, yellow, or red depending upon the following variables:

- **PIR:** Peak Information Rate (measured in bytes/second)
- **CIR:** Committed Information Rate (measured in bytes/second)
- **PBS:** Peak Burst Size (measured in bytes)
- **CBS:** Committed Burst Size (measured in bytes)

The following figure depicts the working of the TCM algorithm:

Figure 73: TCM Algorithm Logic for Traffic Policing



The policing function compares the data unit traffic with the related QoS attributes. Data units not matching the relevant attributes will be dropped or marked as not matching, for preferential dropping in case of congestion.

Procedure To Configure Traffic Policing:

This procedure is used to configure the actions governing the subscriber traffic flow. That is, if the flow violates or exceeds the configured, negotiated peak or committed data-rates. The SGSN performs traffic policing only if the command **qos rate-limit direction** is configured.

```
config
      apn-profile profile_name
 qos rate-limit direction { downlink | uplink } [ burst-size {
auto-readjust [ duration seconds ] | bytes } ] [ class { background |
conversational | interactive traffic_priority | streaming } ] [ exceed-action
 { drop | lower-ip-precedence | transmit } ] [ gbr-qci [
committed-auto-readjust durarion seconds ] ] [ non-gbr-qci [
committed-auto-readjust durarion  seconds ] ] [ violate-action { drop |
lower-ip-precedence | transmit } ] +
            exit
```

This command can be entered multiple times to specify different combinations of traffic direction and class.

The **remove** keyword can be used with the **qos rate-limit direction** command to remove the qos rate-limit direction entries from the configuration.

```
config
      apn-profile profile_name
 remove qos rate-limit direction { downlink | uplink } [ burst-size {
auto-readjust [ duration seconds ] | bytes } ] [ class { background |
conversational | interactive traffic_priority | streaming } ] [ exceed-action
 { drop | lower-ip-precedence | transmit } ] [ gbr-qci [
committed-auto-readjust durarion seconds ] ] [ non-gbr-qci [
committed-auto-readjust durarion  seconds ] ] [ violate-action { drop |
lower-ip-precedence | transmit } ] +
            exit
```

QoS Traffic Policing Per Subscriber

Traffic policing enables the operator to configure and enforce bandwidth limitations on individual PDP contexts for a particular traffic class. It deals with eliminating bursts of traffic and managing traffic flows in order to comply with a traffic contract.

The SGSN complies with the DiffServ model for QoS. The SGSN handles the 3GPP defined classes of traffic, QoS negotiation, DSCP marking, traffic policing, and support for HSDPA/HSUPA.

The per Subscriber traffic policing can be achieved by creating an operator policy for required subscribers (IMSI range) and associating the APN profile having the relevant qos-rate-limit configuration with the operator policy.

DSCP Marking and DSCP Templates

Differentiated Services Code Point specifies a mechanism for classifying and managing network traffic and providing Quality of Service (QoS) on IP networks. DSCP uses the 6-bit Differentiated Services Code Point (DSCP) field in the IP header for packet classification purposes. DSCP replaces the Type of Service (TOS) field.

The SGSN performs a DiffServ Code Point (DSCP) marking of the GTP-U packets according to the allowed-QoS to PHB mapping. The default mapping matches that of the UMTS to IP QoS mapping defined in 3GPP TS 29.208.

DSCP is standardized by the RFCs 2474 and 2475. DSCP templates contain DSCP code points for specific traffic types. DSCP is used to differentiate traffic types and the priority with which they should be allowed through the network. In MPC, DSCP templates are created and applied for signaling (2G/3G) and data traffic, where signaling takes precedence over the data plane. When signaling and data are sent through a single channel, critical signaling messages are adversely affected due to the queueing created by large chunks of data. With DSCP it is possible to have separate queues for signaling and data based on code point value and handle them based on relative precedence.

The SGSN supports DSCP marking of the GTP control plane messages on the Gn/Gp interface. This allows the QoS to be set on GTP-C messages, and is useful if Gn/Gp is on a less than ideal link. DSCP can also be configured at the NSEI level and this configuration has higher precedence over GPRS level configuration. DSCP marking is configurable through the CLI, with default being "Best Effort Forwarding".

The following configuration procedures are used to configure DSCP marking parameters:

1. **The IP command**

   The **ip** command is used to configure DSCP Marking which is used for sending packets of a particular 3GPP QoS class.

   ```
   config
         apn-profile profile_name
    ip { qos-dscp { { downlink | uplink } { background forwarding |
   conversational forwarding | interactive traffic-handling-priority priority
    forwarding | streaming forwarding } + } | source-violation { deactivate [
    all-pdp | exclude-from accounting | linked-pdp | tolerance-limit } |
    discard [ exclude-from-accounting ] | ignore }
               exit
   ```

   To reset the values to the default configuration, use the following procedure:

   ```
   config
         apn-profile profile_name
    default ip { qos-dscp [ downlink | uplink ] | source-violation }
               exit
   ```

   The following procedure is used to disable IP QoS-DSCP mapping:

   ```
   config
         apn-profile profile_name no ip qos-dscp { downlink | uplink } {
   background | conversational | interactive | streaming } +
             exit
   ```

2. **DSCP template configuration mode commands**

   DSCP template configuration mode commands are used to configure DSCP marking for control packets and data packets for Gb over IP. Any number of DSCP templates can be generated in the SGSN Global configuration mode and then a template can be associated with one or more GPRS Services via the commands in the GPRS Service configuration mode.

   The following configuration procedure is used to configure DSCP value for 3GPP QoS class downlink control packets:

```
config
      context context_name
          sgsn-global
              dscp-templatetemplate_name
 control-packet qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 |
af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4
| cs5 | cs6 | cs7 | ef }
               exit
```

The following command is used to configure the QoS DSCP value to "BE" (Best Effort):

```
config
      context context_name
          sgsn-global
              dscp-templatetemplate_name
  default control-packet
                  exit
```

The following configuration procedure is used to configure DSCP value for 3GPP QoS class downlink data packets:

```
config
      context context_name
          sgsn-global
              dscp-templatetemplate_name
 data-packet { background | conversationa | interactive { priority1 |
priority2 | priority3 } | streaming } qos-dscp { af11 | af12 | af13 |
 af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be |
cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
                  exit
```

The following command is used to configure the QoS DSCP value to "BE" (Best Effort):

```
config
      context context_name
          sgsn-global
              dscp-templatetemplate_name
 default data-packet { background | conversationa | interactive {
priority1 | priority2 | priority3 } | streaming }
                  exit
```

3. **The associate-dscp-template command**

   To associate a specific DSCP template with a specific service configuration (for example GPRS Service, IuPS Service, SGSN PSP Service) use the **associate-dscp-template** command.

   GPRS Service Configuration Mode:

```
config
      context context_name
          gprs-service service_name
 associate-dscp-template downlink template_name
              exit
```

   To disassociate a previously associated DSCP marking template:

```
config
      context context_name
          gprs-service service_name
 no associate-dscp-template downlink
              exit
```

IuPS Service Configuration Mode:

```
config
      context context_name
          iups-service service_name
 associate dscp-template downlink dscp_template_name
              exit
```

To disassociate a previously associated DSCP marking template:

```
config
      context context_name
          iups-service service_name
 no associate dscp-template downlink
              exit
```

SGSN PSP Configuration Mode:

```
config
      context context_name
          ss7-routing-domain  routing_domain_id variant variant_type
 associate { asp instance asp_num | dscp-template downlink template_name
}
              exit
```

To disassociate a previously associated DSCP marking template:

```
config
      context context_name
          ss7-routing-domain  routing_domain_id variant variant_type
 no associate [ asp | dscp-template downlink ]
              exit
```

4. **The peer-nse command, to associate DSCP template for NSEI**

   By using this command, a specific DSCP marking template can be identified to be associated with the peer-NSE. The DSCP template must first be created with SGSN Global configuration mode and then defined with the commands in the DSCP Template configuration mode. The template provides a mechanism for differentiated services code point (DSCP) marking of control packets and LLC signaling messages on Gb interfaces. The DSCP marking feature enables the SGSN to perform classifying and managing of network traffic and to determine quality of service (QoS) for the interfaces to an IP network.

   To associate a peer (remote) network service entity (NSEI) for a BSS with this GPRS service:

```
config
      context context_name
          gprs-service service_name
 peer-nsei nse_id { associate dscp-template downlink template_name | lac
lac_id rac rac_id | name peer_nsei_name | pooled }
              exit
```

   To remove the specified configuration from this peer-nsei configuration:

```
config
      context context_name
          gprs-service service_name
 no peer-nsei nse_id [ associate dscp-template downlink  | lac lac_id rac
 rac_id | name | pooled ]
                exit
```

5. **The gtpc command**

   To configure the DSCP marking to be used when sending GTP-C messages originating from the Session Manager and the SGTPC manager, use the following procedure:

```
config
      context context_name
          sgtp-service service_name
 gtpc { bind address ipv4_address | dns-sgsn context context_name |
echo-interval interval_seconds | echo-retransmission { exponential-backoff
 [ [ min-timeout timeout_seconds ] [ smooth-factor smooth_factor ] + ] |
timeout timeout_seconds }  | guard-interval interval_seconds | ignore
response-port-validation | ip qos-dscp dscp_marking | max-retransmissions
 max_retransmissions | retransmission-timeout timeout_seconds | send { common
 flags | rab-context | target-identification-preamble } }
                exit
```

   To reset the values to the default configuration, use the following procedure:

```
config
      context context_name
          sgtp-service service_name
 default gtpc { echo-interval  | echo-retransmission | guard-interval
| ignore response-port-validation | ip qos-dscp | max-retransmissions
 | retransmission-timeout | send { common-flags | rab-context |
target-identification-preamble } }
                exit
```

   The default value is "BE" (Best Effort).

Important To check values configured for DSCP templates, use the **show sgsn-mode** command.

Local QoS Capping

The QoS bit rate can be capped by the operator. The SGSN can be configured to limit the QoS bit rate parameter when the subscribed QoS provided by the HLR is lower than the locally configured value. Based on the configuration enabled, the SGSN can choose the QoS parameter configuration from the HLR configuration or from the local settings used in the APN profile. During session establishment the SGSN applies the lower of the two, that is either the HLR subscription or locally configured value.

The following procedure is used to configure the local Traffic Class (TC) parameters:

Important To enable any of the values/features configured with this command, the **qos prefer-as-cap** configuration (also in the APN profile configuration mode) must be set to either **local** or **both-hlr-and-local**.

```
config
      apn-profile profile_name qos class { background | conversational |
interactive | streaming } [ qualif_option ]
            exit
```

To remove the previously defined TC parameters, use the following procedure:

```
config
     apn-profile profile_name remove qos class { background | conversational
 | interactive | streaming } [ qualif_option ]
            exit
```

To specify the operational preferences of QoS Parameters (specifically the QoS bit rates), use the following procedure:

```
config
      apn-profile profile_name qos prefer-as-cap { both-hlr-and-local |
both-hss-and-local { local-when-subscription-not-available | minimum |
subscription-exceed-reject } | hlr-subscription | local }
            exit
```

To remove all the previous configurations and reset the values to default, use the following procedure:

```
config
      apn-profile profile_name remove qos prefer-as-cap
            exit
```

QoS Management When UE is Using S4-interface for PDP Contexts

The SGSN uses the S4 interface with EPC network elements S-GW or P-GW. The QoS parameters used in the EPC network are different from the ones used in GPRS/UMTS network. For more information refer to the 3GPP TS 23.203 section 6.1.7.

EPC QoS Parameters

- **QoS Class Identifier (QCI):** The QCI is scalar that is used as a reference to node specific parameters that control packet forwarding treatment (for example, scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration and so on.) and that have been pre-configured by the operator owning the node (for example, eNodeB). The standardized characters associated with a standard QCI are listed below:
  - Resource Type (GBR or Non-GBR)
  - Priority
  - Packet Delay Budget
  - Packet Error Loss Rate

Figure 74: QCI table

Packet Error Loss Rate. The one-to-one mapping of standardized QCI values to standardized characteristics is captured in table 6.1.7.QCI	Resource Type	Priority	Packet Delay Budget (NOTE 1)	Packet Error Loss Rate (NOTE 2)	Example Services
1 (NOTE 3)	GBR	2	100 ms	10^{-2}	Conversational Voice
2 (NOTE 3)		4	150 ms	10^{-3}	Conversational Video (Live Streaming)
3 (NOTE 3)		3	50 ms	10^{-3}	Real Time Gaming
4 (NOTE 3)		5	300 ms	10^{-6}	Non-Conversational Video (Buffered Streaming)
5 (NOTE 3)	Non-GBR	1	100 ms	10^{-6}	IMS Signalling
6 (NOTE 4)		6	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7 (NOTE 3)		7	100 ms	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8 (NOTE 5)		8	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9 (NOTE 6)		9			

NOTE 1: A delay of 20 ms for the delay between a PCEF and a radio base station should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface. This delay is the average between the case where the PCEF is located "close" to the radio base station (roughly 10 ms) and the case where the PCEF is located "far" from the radio base station, e.g. in case of roaming with home routed traffic (the one-way packet delay between Europe and the US west coast is roughly 50 ms). The average takes into account that roaming is a less typical scenario. It is expected that subtracting this average delay of 20 ms from a given PDB will lead to desired end-to-end performance in most typical cases. Also, note that the PDB defines an upper bound. Actual packet delays - in particular for GBR traffic - should typically be lower than the PDB specified for a QCI as long as the UE has sufficient radio channel quality.

NOTE 2: The rate of non congestion related packet losses that may occur between a radio base station and a PCEF should be regarded to be negligible. A PELR value specified for a standardized QCI therefore applies completely to the radio interface between a UE and radio base station.

NOTE 3: This QCI is typically associated with an operator controlled service, i.e., a service where the SDF aggregate's uplink / downlink packet filters are known at the point in time when the SDF aggregate is authorized. In case of E-UTRAN this is the point in time when a corresponding dedicated EPS bearer is established / modified.

NOTE 4: If the network supports Multimedia Priority Services (MPS) then this QCI could be used for the prioritization of non real-time data (i.e. most typically TCP-based services/applications) of MPS subscribers.

NOTE 5: This QCI could be used for a dedicated "premium bearer" (e.g. associated with premium content) for any subscriber / subscriber group. Also in this case, the SDF aggregate's uplink / downlink packet filters are known at the point in time when the SDF aggregate is authorized. Alternatively, this QCI could be used for the default bearer of a UE/PDN for "premium subscribers".

NOTE 6: This QCI is typically used for the default bearer of a UE/PDN for non privileged subscribers. Note that AMBR can be used as a "tool" to provide subscriber differentiation between subscriber groups connected to the same PDN with the same QCI on the default bearer.

380511

- **APN AMBR:** The APN-AMBR limits the aggregate bit rate that can be provided across all Non- GBR PDP contexts of the same APN (for example, excess traffic may get discarded by a rate shaping function). Each of those Non-GBR PDP contexts can potentially utilize the entire APN AMBR (for example, when the other Non-GBR PDP contexts do not carry any traffic). The GBR PDP contexts are outside the scope of APN AMBR. The PGW enforces the APN AMBR in downlink. Enforcement of APN AMBR in uplink may be done in the UE and additionally in the PGW.
- **UE AMBR:** The UE AMBR limits the aggregate bit rate that can be provided across all Non-GBR PDP contexts of a UE (for example, excess traffic may get discarded by a rate shaping function). Each of the Non-GBR PDP contexts can potentially use the entire UE AMBR (for example, when the other Non-GBR

PDP contexts do not carry any traffic). The GBR (real-time) PDP contexts are outside the scope of UE AMBR. The RAN enforces the UE AMBR in uplink and downlink.

- **E-ARP:** The EPC uses Evolved ARP, which has priority level ranging from "1" up to "15". Additionally, evolved ARP comprises of pre-emption capability and pre-emption vulnerability. The preemption capability information defines whether a bearer with a lower priority level should be dropped to free up the required resources. The pre-emption vulnerability information indicates whether a bearer is applicable for such dropping by a preemption capable bearer with a higher priority value.

  For handover between UTRAN/GERAN and E-UTRAN, refer to *3GPP TS 24.101 "Annexure-E"*. It defines the mapping rule between ARP and Evolved ARP during R99 QoS to EPS bearer QoS mapping and vice versa.

- **MBR:** Maximum Bit Rate indicates the maximum number of bits delivered to the network or by the network within a period of time. This parameter is as defined in GMM QoS Parameters. In EPC, these values are encoded as a "5" octet linear value but in GMM QoS it is a single octet or a two octet step wise value.

- **GBR:** Guaranteed Bit Rate indicates the guaranteed number of bits delivered to the network or by the network within a period of time. This parameter is as defined in GMM QoS Parameters. In EPC, these values are encoded as a "5" octet linear value but in GMM QoS it is a single octet or a two octet step wise value.

Subscription Types Supported by S4-SGSN

1. **EPC Subscription:** If a subscriber has an EPC subscription, the QoS in subscription data is sent in the EPC format.
2. **GPRS Subscription:** If the subscriber does not have an EPC subscription, the QoS in subscription data is sent in R99/R5/R7 format.

QoS Mapping

The S4-SGSN communicates the QoS parameters towards the S-GW and P-GW in EPC QoS.In UTRAN / GERAN access, the QoS carried over NAS messages to UE are in legacy GMM QoS R99/R5/R7 format (*Refer to, 3GPP TS 24.008 section 10.5.6.5*). However on the S4 / S5 / S16 / S3 interfaces the QoS is carried in EPC format (APN-AMBR, E-ARP and so on). A mapping is required between EPC QoS and GMM QoS, this mapping for EPS QoS to pre-release 8 QoS is defined in 3GPP TS 23.401, Annexure E.

Mapping Details

Information on the parameters mapped is listed below:

- APN-AMBR is mapped to MBR for non-GBR bearers.
- Per bearer MBR and GBR is mapped to MBR and GBR towards UE for GBR bearers.
- For information on other mapping values refer to, 3GPP TS 23.203, table 6.1.7.

Mapping is performed during the following scenarios:

- During Activate Accept (EPC QoS to GMM QoS)
- During Activation initiated Create Session Request (if GPRS subscription is used GMM QoS to EPC QoS mapping)
- During S4-SGSN to Gn SGSN handover (EPC QoS to GMM QoS)
- During HLR / HSS initiated QoS modification (if GPRS subscription is used GMM to EPC QoS towards SGW/PGW; towards UE EPC to GMM QoS for both types of subscription)

Calculation on UE-AMBR

The S4-SGSN sets the value of UE-AMBR as follows:

Value of used UE-AMBR = Sum of APN-AMBRs of all active PDN connections for the given UE, limited or capped by the subscribed UE-AMBR.

For more information refer to, 3GPP TS 23.401, section 4.7.3.

Important Local capping of UE-AMBR will be applicable in the upcoming software releases.

The calculated UE-AMBR is communicated to the RNC. The RNC enforces the UE level aggregate bit rate in both uplink and downlink directions. The RNC has to be R9 compliant. This functionality of sending IE to RNC will not be supported on release 15.0, it is planned for future releases.

To obtain E-ARP when GPRS subscription is used

To obtain E-ARP, configure ARP high and medium priority values at the Call Control Profile through the CLI command listed below:

qos gn-gp { arp high-priority *priority* **medium-priority** *priority* **| pre-emption { capability { may-trigger-pre-emption | shall-not-trigger-pre-emption } | vulnerability { not-pre-emptable | pre-emptable }**

For more information refer to, 3GPP TS 23.401, Annexure E

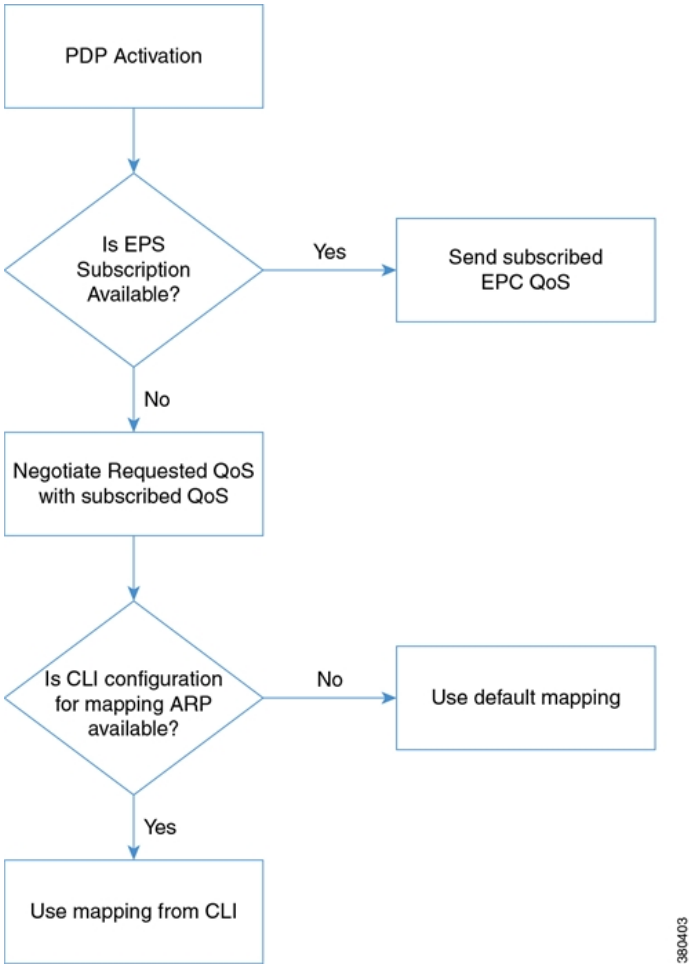
To obtain QCI when GPRS subscription is used

The mapping information on obtaining QCI when GPRS subscription is used is listed in 3GPP TS 23.401 (table E.3) and 3GPP TS 23.203 (table 6.1.7).

QoS Mapping from SGSN to SGW/PGW

The QoS Mapping from SGSN to SGW/PGW can be depicted as follows:

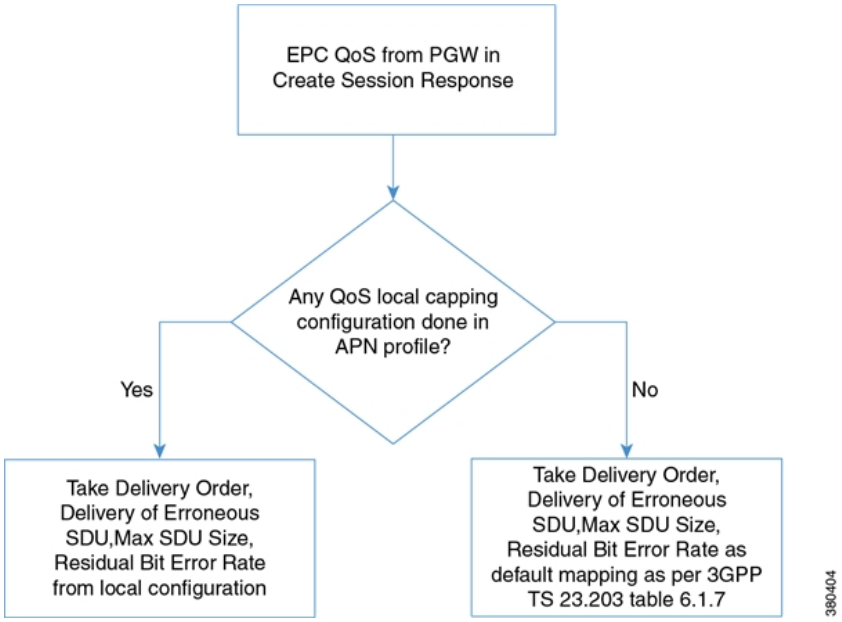
Figure 75: QoS Mapping from SGSN to SGW/PGW



QoS Mapping from SGSN to UE/RNC

The QoS Mapping from SGSN to UE/RNC can be depicted as follows:

Figure 76: QoS Mapping from SGSN to UE/RNC



Important QoS in GMM is an encoded octet. QoS in EPC is a linear "4" octet value in kbps. It is not possible to encode an odd value like "8991" kbps in GMM QoS.

QoS Handling Scenarios

Listed below are various QoS handling scenarios and QoS Mapping for each of the scenarios:

Scenario-1:

Description of the scenario:

1. Attach is received from an EPC capable UE.
2. The HLR subscription does not have EPS subscription data. Only GPRS subscription is present.
3. Activate a PDP context with all QoS parameters set to "subscribed".

Important For this scenario, PDP context activation through Gn/Gp interface by default is not done. Instead a S4 election is done as the UE is EPC capable. However, if the local operator policy overrides this to select Gn/Gp, then Gn/Gp is preferred.

QoS mapping for the scenario:

If S4 is the selected interface, then the subscribed MBR is mapped to APN AMBR. The EPS bearer QoS MBR is set to subscribed MBR (for conversational and streaming class bearers). For non-GBR bearers the EPS bearer QoS MBR is set to "0". If the traffic class is conversational or streaming, then the EPS bearer QoS GBR is set to subscribed GBR.

A detailed list of mapping:

1. APN AMBR = Subscribed MBR
2. Bearer QoS PVI = Taken from local policy [use call-control-profile qos gn-gp config]
3. Bearer QoS PCI = Taken from local policy [use call-control-profile qos gn-gp config]
4. Bearer QoS PL = Taken from local policy [use call-control-profile qos gn-gp config]
5. Bearer QoS QCI = Mapped from subscribed traffic class
6. Bearer QoS MBR UL and DL = Mapped from subscribed MBR + MBR-Extended for UL and DL
7. Bearer QoS GBR UL and DL = Zero for interactive or background traffic. For streaming or conversational it is mapped from subscribed GBR + Ext.GBR UL / DL

References:

3GPP TS 23.401 Annexure E and 3GPP TS 29.274 section 8.15.

Scenario-2:

Description of the scenario:

The scenario is same as Scenario-1 described above, the only change being inclusion of sending activate accept to UE.

1. Attach is received from an EPC capable UE.
2. The HLR subscription does not have EPS subscription data. Only GPRS subscription is present.
3. Activate a PDP context with all QoS parameters set to "subscribed".

Important For this scenario, PDP context activation through Gn/Gp interface by default is not done. Instead a S4 election is done as the UE is EPC capable. However, if the local operator policy overrides this to select Gn/Gp, then Gn/Gp is preferred.

QoS mapping for the scenario:

After the create session response is received from the S-GW, the following mapping shall be used to send the QoS towards UE:

1. Traffic Class = Mapped from QCI based on Table E.3 in 3GPP TS 23.401.
2. Delivery Order = Taken from local configuration [apn-profile --> qos --> class [traffic class] --> sdu --> delivery order]
3. Delivery of erroneous SDU = Taken from local configuration [apn-profile --> qos --> class [traffic class] --> sdu --> erroneous]
4. Maximum SDU Size = [apn-profile --> qos --> class [traffic class] --> sdu --> max size]
5. MBR Uplink = APN-AMBR-UL (if traffic class = interactive /background) or Bearer MBR-UL (if TC = streaming / conversational)
6. MBR DL = APN-AMBR-DL (if traffic class = interactive /background) or Bearer MBR-DL (if TC = streaming / conversational)
7. Residual BER = Taken from local config [apn-profile-->qos-->class [tc] --> residual-bit-error-rate
8. SDU error ratio = Mapped based on Table 6.1.7 in 3GPP TS 23.203
9. Transfer delay = Mapped based on Table 6.1.7 in 3GPP TS 23.203

10. THP = Mapped from QCI based on Table E.3 in 3GPP TS 23.401
11. GBR UL = "0" for interactive or background class traffic. Mapped from Bearer QoS GBR UL for conversational or streaming traffic.
12. GBR DL = "0" for interactive or background class traffic. Mapped from Bearer QoS GBR DL for conversational or streaming traffic.
13. Signaling Indication = Mapped from QCI as per Table E.3 3GPP TS 23.401
14. Extended bit rates will be present if the mapped MBR / GBR exceeds "8640" Kbps

Scenario-3:

Description of the scenario:

1. Attach is received from an EPC capable UE
2. The HLR subscription does not have EPS subscription data. Only GPRS subscription data is present.
3. A primary PDP context is activated with all QoS parameters set to some requested values.

QoS mapping for the scenario:

1. Negotiate the requested QoS with subscribed QoS. Map the negotiated QoS as described in Scenario-1.
2. After receiving a Create Session Response, map the accepted EPS QoS to R99+ QoS as described in Scenario-2 and send the Activate accept.

Scenario-4:

Description of the scenario:

1. Attach is received from an EPC capable UE
2. The HLR subscription has EPS subscription data.
3. A PDP context is activated with all QoS parameters set to "Subscribed" values or some requested values.

QoS mapping for the scenario:

1. For every primary PDP context to an APN, the EPS subscribed QoS is used as is.
2. Once the EPS bearer is activated, the Activate PDP Accept is sent by mapping the accepted QoS value as described in Scenario-2.

Scenario-5:

Description of the scenario:

1. Attach is received from an EPC capable UE
2. The HLR subscription has EPS subscription data.
3. A secondary PDP context is activated with all QoS parameters set to "Subscribed" values.

QoS mapping for the scenario:

The SGSN sends a Bearer Resource Command with the following parameters:

1. Linked EPS Bearer ID = EPS bearer ID of linked Primary PDP
2. PTI = Transaction ID received from the MS (In MME, the received PTI is used in the NAS message as the PTI towards S-GW. But for the SGSN PTI is not there in the NAS message. The 3GPP TS is not clear on what the SGSN should send as PTI, therefore TI is sent.

Flow QoS:

1. QCI = Mapped from requested Traffic Class, if TC= conversational / streaming

2. MBR UL = APN-AMBR last received from P-GW for primary PDP activation
3. MBR DL = APN-AMBR last received from P-GW for primary PDP activation
4. GBR UL = APN-AMBR last received from P-GW for primary PDP activation
5. GBR DL = APN-AMBR last received from P-GW for primary PDP activation
6. Else, the values will be MBR UL = "0", BR DL ="0", GBR UL = "0", GBR DL = "0"

Important The value sent in the Flow QoS does not have any impact as it is the P-GW which decides the correct QoS value to be provided. If the requested QoS is set to "subscribed" then as a placeholder value the APN-AMBR value is sent as the MBR and GBR values.

References:

3GPP TS 23.401 Annexure E and 3GPP TS 29.274 (sections 8.15 and 8.16).

Scenario-6:

Description of the scenario:

1. Attach is received from an EPC capable UE
2. The HLR subscription has EPS subscription data.
3. A secondary PDP context is activated with all QoS parameters set to specified values.

QoS mapping for the scenario:

The SGSN sends a Bearer Resource Command with the following parameters:

1. Linked EPS Bearer ID = EPS bearer ID of linked Primary PDP
2. PTI = Transaction ID received from the MS (In MME, the received PTI is used in the NAS message as the PTI towards S-GW. But for the SGSN PTI is not there in the NAS message. The 3GPP TS is not clear on what the SGSN should send as PTI, therefore TI is sent.

Flow QoS:

1. QCI = Mapped from requested Traffic Class, if TC= conversational or streaming.
2. MBR UL = Requested MBR UL, MBR DL = Requested MBR DL
3. GBR UL = Requested GBR UL, GBR DL = Requested GBR DL or GBR UL = "0", GBR DL = "0"

Important If the traffic class is conversational or streaming, the requested MBR or GBR values can be greater than the subscribed APN-AMBR.

References:

3GPP TS 23.401 Annexure E and 3GPP TS 29.274 (sections 8.15 and 8.16)

Scenario-7:

Description of the scenario:

1. Attach is received from an EPC capable UE
2. The HLR subscription does not have EPS subscription data.
3. A secondary PDP context is activated with all QoS parameters set to "Subscribed".

QoS mapping for the scenario:

The SGSN sends a Bearer Resource Command with the following parameters:

1. Linked EPS Bearer ID = EPS bearer ID of linked Primary PDP
2. PTI = Transaction ID received from the MS (In MME, the received PTI is used in the NAS message as the PTI towards S-GW. But for the SGSN PTI is not there in the NAS message. The 3GPP TS is not clear on what the SGSN should send as PTI, therefore TI is sent.

Flow QoS:

1. QCI = Mapped from requested Traffic Class, if TC= conversational or streaming
2. MBR UL = APN-AMBR-UL last obtained from P-GW for primary
3. MBR DL = APN-AMBR-DL last obtained from P-GW for primary
4. GBR UL = APN-AMBR-UL last obtained from P-GW for primary
5. GBR DL = APN-AMBR-UL last obtained from P-GW for primary
6. Else, MBR UL = "0", MBR DL = "0", GBR UL = "0", GBR DL = "0"

Scenario-8:

Description of the scenario:

1. Attach is received from an EPC capable UE
2. The HLR subscription does not have EPS subscription data.
3. A secondary PDP context is activated with all QoS parameters set to valid requested values.

QoS mapping for the scenario:

Cap the requested QoS with the subscribed QoS. Then use the negotiated QoS as described below, the SGSN sends a Bearer Resource Command with the following parameters:

1. Linked EPS Bearer ID = EPS bearer ID of linked Primary PDP
2. PTI = Transaction ID received from the MS (In MME, the received PTI is used in the NAS message as the PTI towards S-GW. But for the SGSN PTI is not there in the NAS message. The 3GPP TS is not clear on what the SGSN should send as PTI, therefore TI is sent.

Flow QoS:

1. QCI = Mapped from requested Traffic Class, if TC= conversational or streaming
2. MBR UL = MBR-UL negotiated
3. MBR DL = MBR-DL negotiated
4. GBR UL = GBR-UL negotiated
5. GBR DL = GBR-DL negotiated
6. Else, MBR UL = "0", MBR DL = "0", GBR UL = "0", GBR DL = "0"

Scenario-9:

Description of the scenario:

In-bound RAU or Forward Relocation Request for a subscriber, who was earlier attached on a Gn/Gp SGSN.

Important This scenario is currently not supported.

QoS mapping for the scenario:

1. APN-AMBR-UL = Subscribed MBR-UL
2. APN-AMBR-DL = Subscribed MBR-DL
3. Bearer QoS MBR = Negotiated MBR received from peer SGSN Bearer QoS GBR = "0", for Interactive or Background traffic classes and it is Negotiated GBR value for Conversational or Streaming traffic classes.
4. Bearer QoS - PVI = Use from Local Policy (use call-control-profile qos gn-gp configuration)
5. Bearer QoS - PCI = Use from Local Policy (use call-control-profile qos gn-gp configuration)
6. Bearer QoS - PL = Use from Local Policy (use call-control-profile qos gn-gp configuration), based on the negotiated ARP received.
7. Bearer QoS - QCI = Mapped from negotiated traffic class.

References:

3GPP TS 23.401 Annexure E and 3GPP TS 23.060 v8.9.0 (section 6.9.1.2.2.a)

Scenario-10:

Description of the scenario:

Outbound RAU or Forward Re-location Request is sent towards a Gn/Gp SGSN.

QoS mapping for the scenario:

1. Subscribed QoS = Mapped from subscribed EPS QoS
2. Requested QoS = Return the MS requested value
3. Negotiated QoS = Mapped from the current EPS QoS
4. The mapping of EPS QoS to pre- release "8" QoS is as described in scenario-2.
5. When mapping subscribed EPS QoS to pre-release "8" MBR and GBR the following rules are applied:
   - MBR-UL = APN-AMBR-UL
   - MBR-DL = APN-AMBR-DL
   - GBR-UL / DL = "0" (for TC = interactive / background)
   - GBR-UL / DL = APN-AMBR-UL / DL (for TC = interactive / background)

Scenario-11:

Description of the scenario:

Initiating modify a PDP towards UE from SGSN (for instances of P-GW initiated QoS modification, HSS initiated modification and so on.)

QoS mapping for the scenario:

The current EPS QoS at SGSN is mapped to pre-release "8" QoS as described in Scenario-2.

Important QoS in GMM is an encoded octet. QoS in EPC is a linear "4" octet value in kbps. It is not possible to encode an odd value like "8991" kbps in GMM QoS.

QoS Handling During Primary PDP Activation

QoS Handling When EPS Subscription is Available

1. The subscribed APN-AMBR and ARP values are sent in Create Session Request to SGW or PGW.
2. The PGW can change the APN-AMBR value in Create Session Response.
3. The SGSN accepts the APN-AMBR value sent by the PGW. No further negotiation happens as described in 3GPP TS 23.060 section 9.2.2.1A, list item "d".
4. In most cases the S4-SGSN does not perform any further QoS negotiation. (However, there is a special case of SGSN capping the bit rate sent to RAN at 16Mbps. This requirement will be supported in future releases).
5. The S4-SGSN maps the received APN-AMBR to MBR values as per the mapping table provided in 3GPP TS 23.203 Table 6.1.7 and 3GPP TS 23.401 Annex E.
6. The mapped MBR values are sent to the RNC in RAB assignment request and in Activate Accept to the UE.
7. In Release 14.0 local override of APN-AMBR / ARP based on CLI configuration is supported.

QoS Handling When Only GPRS Subscription is Available

1. The requested QoS from UE and the subscribed QoS are negotiated, the SGSN chooses the least of the two values as the negotiated output. If the requested QoS is the Subscribed QoS, the SGSN chooses the Subscribed QoS as is. If any local QoS capping is configured, the Negotiated QoS is the least of Requested QoS or Subscribed QoS capped by local values).
2. The Negotiated QoS is mapped to EPC QoS as per the mapping table in 3GPP TS 23.203 Table 6.1.7 and 3GPP TS 23.401 Annexure E.
3. The mapped values are sent in Create Session Request to the SGW or PGW.
4. The PGW is allowed to change the APN-AMBR value in Create Session Response.
5. The SGSN accepts the APN-AMBR value sent by the PGW. No further negotiation happens as described in 3GPP TS 23.060 section 9.2.2.1A, list item "d".
6. The S4-SGSN maps the received the APN-AMBR to MBR value as per the mapping table described in 3GPP TS 23.203 table 6.1.7 and 3GPP TS 23.401 Annexure "E".
7. The mapped MBR values are sent to the RNC in RAB assignment request and in Activate Accept to UE.

QoS Handling During Secondary PDP Activation

QoS Handling When EPS Subscription is Available

1. The Requested QoS is mapped to EPC QoS and sent in the Bearer Resource Command to the SGW or PGW.
2. If the traffic class requested is a non-GBR traffic class (interactive / background), the per bearer MBR / GBR values sent in Bearer Resource Command will all be zeroes.
3. The PGW sends a Create Bearer Request to the SGW or SGSN.
4. The SGSN sends a RAB assignment request to the RNC by mapping QoS as follows:
   a. If the bearer is a non-GBR: The APN-AMBR is mapped to MBR values and GBR is set to "0".
   b. If the bearer is GBR: The MBR / GBR values received in Create Bearer Request are sent to RNC / UE in the Secondary Activate Accept.

QoS Handling When Only GPRS Subscription is Available

1. The Requested QoS from the UE and the Subscribed QoS are negotiated. The SGSN chooses the least of the two values as the negotiated output. If the Requested QoS is mentioned as the Subscribed QoS, then the SGSN chooses the Subscribed QoS as is, if local QoS capping is not configured.
2. The Requested QoS is mapped to the EPC QoS and sent in the Bearer Resource Command to the SGW or PGW.
3. If the traffic class requested is a non-GBR traffic class (interactive / background), the per bearer MBR / GBR values sent in Bearer Resource Command will be all zeroes.
4. The PGW sends a Create Bearer Request to SGW or SGSN.
5. The SGSN sends a RAB assignment request to the RNC by mapping QoS as follows:
   a. If the bearer is non-GBR: The APN-AMBR is mapped to MBR values and the GBR value is set to "0".
   b. If the bearer is GBR: The MBR / GBR values received in the Create Bearer Request will be sent to RNC / UE in Secondary Activate Accept.

MS Initiated QoS Modification

- The MS sends a Modify PDP Context Request (TI, QoS Requested, TFT, and Protocol Configuration Options) message to the SGSN. Either QoS Requested or TFT or both may be included. The QoS Requested indicates the desired QoS profile, while the TFT indicates the TFT that is to be added or modified or deleted from the PDP context. Protocol Configuration Options may be used to transfer optional PDP parameters and/or requests to the PGW.
- The SGSN identifies the bearer modification scenario that applies and sends the Bearer Resource Command (TEID, LBI, PTI, EPS Bearer QoS (excluding ARP), TFT, EBI, RAT type, Protocol Configuration Options, serving network identity, CGI/SAI, User CSG Information, MS Info Change Reporting support indication, DL TEID and DL Address, DTI) message to the selected Serving GW.
  - An S4-based SGSN applies the BCM 'MS/NW' whenever the S4 is selected for a certain MS. The following table list the details of MS-initiated EPS bearer modification, MS/NW mode:

Table 29: MS-initiated EPS bearer modification, MS/NW mode

Sl No.	PDP context modification use case	Information provided by SGSN at S4 signaling
1.	Add TFT filters and increase QoS	QoS related to EPS Bearer, TFT filters added, TEID, EPS Bearer ID
2.	Increase of QoS related to one or more TFT filter(s)	QoS related to EPS Bearer filters, Impacted TFT filters, TEID, EPS Bearer ID
3.	Increase of QoS, TFT filters not specified	Not allowed in MS/NW mode
4.	Add/remove TFT filters, no QoS change	TFT filters added/removed, TEID, EPS Bearer ID

Sl No.	PDP context modification use case	Information provided by SGSN at S4 signaling
5.	Decrease QoS related to one or more TFT filter(s)	QoS related to EPS Bearer filters, Impacted TFT filters, TEID, EPS Bearer ID
6.	Remove TFT filters and decrease QoS	QoS related to EPS Bearer, TFT filters removed, TEID, EPS Bearer ID
7.	Decrease of QoS, TFT filters not specified	Not allowed in MS/NW mode
Note: Only the modified QCI and/or GBR parameters are forwarded by the SGSN.		

- The S4-SGSN may assume that the BCM mode of a bearer is MS/NW there are instances where the BCM mode negotiated between UE and PGW can be "UE only". In such cases, a UE sends a Modify PDP Request to the SGSN without a TFT. But SGSN cannot honor it in a R9 capable network since TAD is mandatory in BRC. In a R10 network, TAD is conditional optional on the S4 interface. Once the EGTP stack is upgraded to R10 compliance, the S4-SGSN honors PDP modification without TFT. For release 14.0, the SGSN rejects such PDP modifications.
- If the PDP modification is for non-GBR bearer, the SGSN sets the MBR and GBR values in Bearer Resource Command to "0". If the PDP modification is for GBR bearer, then SGSN sets the MBR and GBR values in Bearer Resource Command to the requested values.
- The Serving GW Forwards the message to the PGW.
- If the request is accepted, the PGW Initiated Bearer Modification Procedure is invoked by the PGW to modify the EPS Bearer indicated by the TEID.
    - The PDN GW sends an Update Bearer Request (TEID, EPS Bearer Identity, PTI, EPS Bearer QoS, APN-AMBR, TFT, Protocol Configuration Options, Prohibit Payload Compression, MS Info Change Reporting Action, and CSG Information Reporting Action) message to the Serving GW. The Procedure Transaction Id (PTI) parameter is used to link this message to the Request Bearer Resource Modification message received from the Serving GW.
- The Serving GW sends an Update Bearer Request (PTI, EPS Bearer Identity, EPS Bearer QoS, TFT, APN AMBR, Protocol Configuration Options, Prohibit Payload Compression, MS Info Change Reporting Action, CSG Information Reporting Action) message to the SGSN.
- In Iu mode, radio access bearer modification may be performed by the RAB Assignment procedure. If the radio access bearer does not exist, the RAB setup is done by the RAB Assignment procedure.
- The SGSN acknowledges the bearer modification by sending an Update Bearer Response (TEID, EPS Bearer Identity, DL TEID and DL Address, DTI) message to the Serving GW.
- The Serving GW acknowledges the bearer modification by sending an Update Bearer Response (TEID, EPS Bearer Identity) message to the PDN GW.
- The SGSN selects Radio Priority and Packet Flow Id based on QoS Negotiated, and returns a Modify PDP Context Accept (TI, QoS Negotiated, Radio Priority, Packet Flow Id, and Protocol Configuration Options) message to the MS.

HSS Initiated PDP Context Modification

- The Home Subscriber Server (HSS) initiated PDP context modification procedure is used when the HSS decides to modify the subscribed QoS, where typically QoS related parameters are changed. The parameters that may be modified are UE-AMBR, APN-AMBR QCI and Allocation/Retention Policy.
- The HSS initiates the modification by sending an Insert Subscriber Data (IMSI, Subscription Data) message to the SGSN. The Subscription Data includes EPS subscribed QoS (QCI, ARP) and the subscribed UE-AMBR and APN AMBR.
- The S4-SGSN then updates the stored Subscription Data and acknowledges the Insert Subscriber Data message by returning an Insert Subscriber Data Ack (IMSI) message to the HSS and sends the Modify Bearer Command (EPS Bearer Identity, EPS Bearer QoS, APN AMBR) message to the S-GW. The S-GW forwards the Modify Bearer Command (EPS Bearer Identity, EPS Bearer QoS, APN AMBR) message to the P-GW. Note that the EPS Bearer QoS sent in the Modify Bearer Command does not modify the per bearer bit-rate. It is sent to carry only a change in the ARP / QCI received from subscription. Also, the Modify Bearer Command can be sent only for the default bearer (primary PDP) in a PDN connection.
- The P-GW modifies the default bearer of each PDN connection corresponding to the APN for which subscribed QoS has been modified. If the subscribed ARP parameter has been changed, the P-GW shall also modify all dedicated EPS bearers having the previously subscribed ARP value unless superseded by PCRF decision. The P-GW then sends the Update Bearer Request (EPS Bearer Identity, EPS Bearer QoS [if QoS is changed], TFT, APN AMBR) message to the S-GW.
- The S-GW sends the Update Bearer Request (EPS Bearer Identity, EPS Bearer QoS (if QoS is changed) APN-AMBR, TFT) message to the SGSN. On completion of modification S4-SGSN acknowledges the bearer modification by sending the "Update Bearer Response (EPS Bearer Identity)" message to P-GW via S-GW. If the bearer modification fails, the P-GW deletes the concerned EPS Bearer.

PGW Initiated QoS Modification

- The P-GW sends the Update Bearer Request (TEID, EPS Bearer Identity, EPS Bearer QoS, APN-AMBR, Prohibit Payload Compression, MS Info Change Reporting Action, CSG Information Reporting Action, TFT, and Protocol Configuration Options) message to the S-GW.
  - The TFT is optional and included in order to add, modify or delete the TFT related to the PDP Context. Protocol Configuration Options is optional.
- The S- GW sends the Update Bearer Request (TEID, EPS Bearer Identity, EPS Bearer QoS, APN-AMBR, Prohibit Payload Compression, MS Info Change Reporting Action, CSG Information Reporting Action, TFT, and Protocol Configuration Options) message to the SGSN.
- In Iu mode, radio access bearer modification may be performed by the RAB Assignment procedure.
- The SGSN selects Radio Priority and Packet Flow Id based on the QoS Negotiated, and sends a Modify PDP Context Request (TI, PDP Address, QoS Negotiated, Radio Priority, Packet Flow Id, TFT, and PCO) message to the MS. The TFT is included only if it was received from the P-GW in the Update Bearer Request message. Protocol Configuration Options are sent transparently through the SGSN.
- The MS should accept the PDP context modification requested by the network if it is capable of supporting any modified QoS Negotiated as well as any modified TFT. For a successful modification the MS acknowledges by returning a Modify PDP Context Accept message. If the MS is incapable of accepting a new QoS Negotiated or TFT it shall instead de-activate the PDP context with the PDP Context Deactivation Initiated by MS procedure.

- On receiving the Modify PDP Context Accept message, or on completion of the RAB modification procedure, the SGSN returns an Update PDP Context Response (TEID, QoS Negotiated) message to the S-GW.
- The S-GW acknowledges the bearer modification to the P- GW by sending an Update Bearer Response (EPS Bearer Identity) message.

ARP Handling

Difference between Gn SGSN and S4 SGSN

In Create PDP Context response the GGSN sends {1, 2, and 3} as ARP value whereas the S-GW sends "15" value ARP in Create Session response. In Gn SGSN while sending the RAB assignment request, the Allocation retention priority values {1, 2, and 3} are mapped to "15" values so there is need of conversion from "3" values to "15" values.

In S4 SGSN, since the P-GW sends ARP in the "15" value range there is no need for conversion.

ARP values in Gn SGSN

According to GTPv1 3GPP TS 29.060 clause 7.7.34 Allocation/ Retention priority encodes each priority level defined in 3GPP TS 23.107 as the binary value of the priority level.

Quality of Service (QoS) Profile

The Quality of Service (QoS) Profile includes the values of the defined QoS parameters.

Octet "4" carries the Allocation/Retention priority octet that is defined in 3GPP TS 23.107. The Allocation/Retention priority octet encodes each priority level defined in 3GPP TS 23.107 as the binary value of the priority level.

The Allocation/Retention priority field is ignored by the receiver if:

- The QoS profile is pre-Release '99.
- The QoS profile IE is used to encode the Quality of Service Requested (QoS Req) field of the PDP context IE.

Octet "5" the QoS Profile Data Field is coded according to the 3GPP TS 24.008 [5] Quality of Service IE, octets 3-m. The minimum length of the field QoS Profile Data is "3" octets, the maximum length is "254" octets.

The clause 11.1.6 "Error handling" defines the handling of the case when the sent QoS Profile information element has a Length different from the Length expected by the receiving GTP entity.

Figure 77: Quality of Service (QoS) Profile Information Element

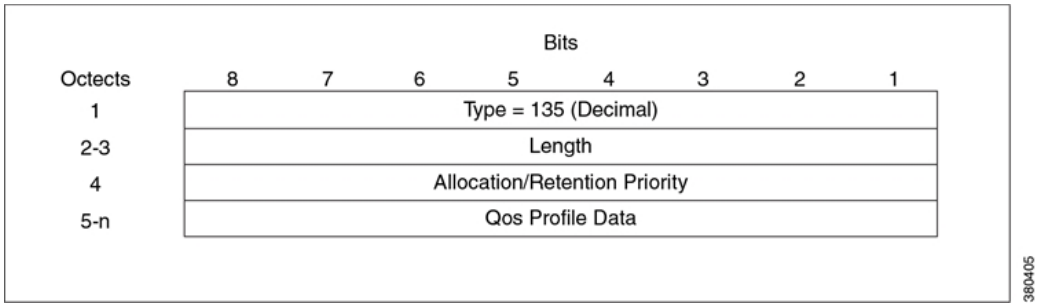


Figure 78: Value Ranges for UMTS Bearer Service Attributes

Traffic class	Conversational class	Streaming class	Interactive class	Background class
Maximum bitrate (kbps)	<= 256 000 (2)	<= 256 000 (2)	<= 256 000 (2)	<= 256 000 (2)
Delivery order	Yes/No	Yes/No	Yes/No	Yes/No
Maximum SDU size (octets)	Yes/No	Yes/No	Yes/No	Yes/No
SDU format information	(5)	(5)		
Maximum SDU size (octets)	Yes/No/- (6)	Yes/No/- (6)	Yes/No/- (6)	Yes/No/- (6)
Residual BER	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$ 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$5*10^{-2}$, 10^{-2}, $5*10^{-3}$ 10^{-3}, 10^{-4}, 10^{-5}, 10^{-6}	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$ (7)	$4*10^{-3}$, 10^{-5}, $6*10^{-8}$ (7)
SOU error ratio	10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-1}, 10^{-2}, $7*10^{-3}$, 10^{-3}, 10^{-4}, 10^{-5}	10^{-3}, 10^{-4}, 10^{-6}	10^{-3}, 10^{-4}, 10^{-6}
Transfer delay (ms)	100-maximum value	300 (8) - maximum value		
Guaranteed bit rate (kbps)	<= 256 000 (2)	<= 256 000 (2)		
Traffic handling priority			1 ,2,3 (9)	
Allocation/Retention priority	1,2,3	1,2,3	1,2,3	1,2,3
Source statistic descriptor	Speech/unknown	Speech/unknown		
Signalling Indication			Yes/No (9)	
Evolved Allocation/Retention priority - Priority Level - Pre-emption Capability - Pre-emption Vulnerability	1-15 Yes/No Yes/No	1-15 Yes/No Yes/No	1-15 Yes/No Yes/No	1-15 Yes/No Yes/No

380512

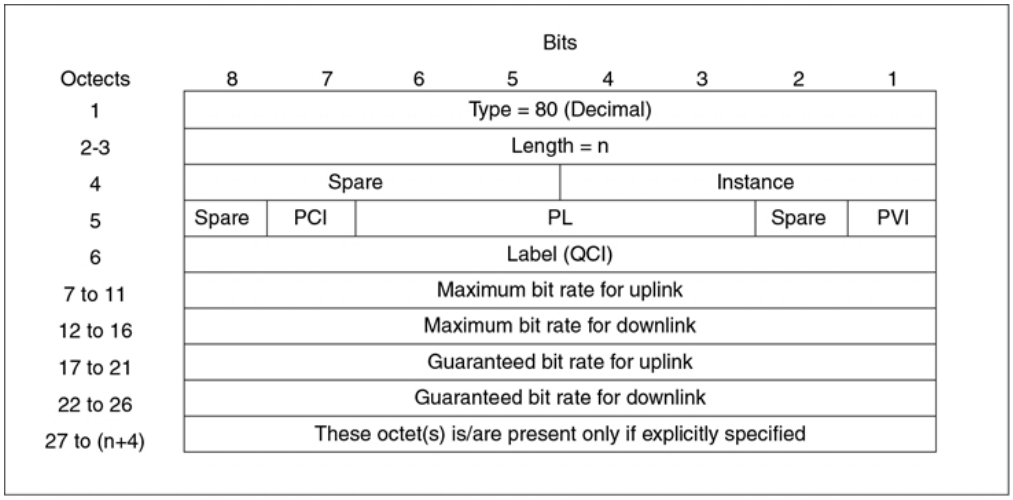
ARP values in S4 SGSN

The behavior of ARP values in S4 SGSN is according to GTPv2 3GPP TS 29.274 clause 8.15.

Bearer Quality of Service (Bearer QoS)

Bearer Quality of Service (Bearer QoS) is transferred through the GTP tunnels. The sending entity copies the value part of the Bearer l QoS into the Value field of the Bearer QoS IE.

Figure 79: Bearer Level Quality of Service (Bearer QoS)



Octet "5" represents the Allocation/Retention Priority (ARP) parameter. The meaning and value range of the parameters within the ARP are defined in 3GPP TS 29.212 [29]. The bits within the ARP octet are:

- Bit 1 - PVI (Pre-emption Vulnerability), see 3GPP TS 29.212[29], clause 5.3.47 Pre-emption-Vulnerability AVP.
- Bit 2 - Spare bit.
- Bits 3 up to 6 - PL (Priority Level), see 3GPP TS 29.212[29], clause 5.3.45 ARP-Value AVP. Priority Level encodes each priority level defined for the ARP-Value AVP as the binary value of the priority level.
- Bit 7 - PCI (Pre-emption Capability), see 3GPP TS 29.212[29], clause 5.3.46 Pre-emption-Capability AVP.
- Bit 8 - Spare bit.

Priority-Level AVP (All access types)

The values "1" up to "15" are defined, with value "1" as the highest level of priority.

Values "1" up to "8" should only be assigned for services that are authorized to receive prioritized treatment within an operator domain. Values "9" up to "15" can be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.

Pre-emption-Capability AVP

PRE-EMPTION_CAPABILITY_ENABLED (0)

This value indicates that the service data flow or bearer which is allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level.

PRE-EMPTION_CAPABILITY_DISABLED (1)

This value indicates that the service data flow or bearer is not allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. This is the default value applicable if this AVP is not supplied.

Pre-emption-Vulnerability AVP

PRE-EMPTION_VULNERABILITY_ENABLED (0)

This value indicates that the resources assigned to the service data flow or bearer which can be pre-empted and allocated to a service data flow or bearer with a higher priority level. This is the default value applicable if this AVP is not supplied.

PRE-EMPTION_VULNERABILITY_DISABLED (1)

This value indicates that the resources assigned to the service data flow or bearer which shall not be pre-empted and allocated to a service data flow or bearer with a higher priority.

Handling of ARP Values in Various Scenarios

Gn + GPRS Subscription

The following CLI command is used to send RAB parameters in RAB Assignment request:

```
config
      apn-profile profile_name
ranap allocation-retention-priority-ie subscription-priority priority class
 { { background | conversational | interactive | streaming } {
not-pre-emptable | priority | queuing-not-allowed |
shall-not-trigger-pre-emptable } + }
            exit
```

S4 + EPC subscription

For EPC subscription with S4 activation, ARP in RAB is filled from the Evolved ARP applied for the PDP context. The Evolved ARP applied is:

- Subscribed Evolved ARP if P-GW does not send any evolved ARP in Create Session Response.

Or

- Evolved ARP supplied by the P-GW.

S4+GPRS Subscription

For GPRS subscription with S4 activation, the ARP in RAB is filled from the Evolved ARP applied for the PDP context. The Evolved ARP applied is:

- Evolved ARP derived from the GPRS subscription using CLIs displayed below, when the P-GW does not send any Evolved ARP in Create Session Response:

```
config
      call-control-profile profile_name
qos { gn-gp | ue-ambr }
qos gn-gp { arp high-priority priority medium-priority priority | pre-emption
 { capability { may-trigger-pre-emption | shall-not-trigger-pre-emption
} | vulnerability { not-pre-emptable | pre-emptable }
            exit
```

Or

- Evolved ARP supplied by the P-GW.

The Evolved ARP applied is sent in RANAP towards the RNC.

Mapping EPC ARP to RANAP ARP

The ARP values are defined as per 3GPP TS 29.212 clause 5.3.46 and 5.3.47 for the Core Network Side.

The following values are defined:

- **PRE-EMPTION_CAPABILITY_ENABLED (0)**

  This value indicates that the service data flow or bearer which is allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level.

- **PRE-EMPTION_CAPABILITY_DISABLED (1)**

  This value indicates that the service data flow or bearer which is not allowed to get resources that were already assigned to another service data flow or bearer with a lower priority level. This is the default value applicable if this AVP is not supplied.

- **PRE-EMPTION_VULNERABILITY_ENABLED (0)**

  This value indicates that the resources assigned to the service data flow or bearer which can be pre-empted and allocated to a service data flow or bearer with a higher priority level. This is the default value applicable if this AVP is not supplied.

- **PRE-EMPTION_VULNERABILITY_DISABLED (1)**

  This value indicates that the resources assigned to the service data flow or bearer which shall not be pre-empted and allocated to a service data flow or bearer with a higher priority level.

For more information on ARP values and their definitions see, 3GPP TS 25.413 clause 9.2.1.3.

The ARP values defined are different on the RNC side and the Core Network side, the RAB assignment request is mapped according to the following table:

Table 30: RAB Assignment Request Mapping

RAB parameters (ARP)	ARP values received from SGW (According to 3GPP TS 29.212 clause5.3.46 and 5.3.47)	Mapping EPC ARP to RANAP ARP in RNC side (According to RANAP 3GPP TS 25.413 clause 9.2.1.3)
Pre-emption-Capability	PRE-EMPTION_CAPABILITY_ENABLED (0)	Pre-emption is triggered.
Pre-emption-Capability	PRE-EMPTION_CAPABILITY_DISABLED (1)	Pre-emption is not triggered.
Pre-emption-Vulnerability	PRE-EMPTION_VULNERABILITY_ENABLED (0)	Pre-emption is triggered.
Pre-emption-Vulnerability	PRE-EMPTION_VULNERABILITY_DISABLED (1)	Pre-emption is not triggered.

ARP configured in CC Profile

The QoS configured in the Call Control Profile is used if the S4 interface is chosen for PDP activation, but the subscription does not have an EPS subscription. Therefore, GPRS subscription data (which uses QoS in pre-release 8 format), will be mapped to EPS QoS. The Allocation and Retention policy will be mapped to EPS ARP using the configuration in the Call Control Profile.

If the QoS mapping configuration is not used, the following default mappings are used:

- Default ARP high-priority value = 5.
- Default ARP medium-priority value = 10.
- Default pre-emption capability = shall-not-trigger-pre-emption.
- .Default pre-emption vulnerability = not pre-emptable

The mapping is configured through the following CLI command:

```
config
      call-control-profile <profile_name>
qos { gn-gp | ue-ambr }
qos gn-gp { arp high-priority priority medium-priority priority | pre-emption
 { capability { may-trigger-pre-emption | shall-not-trigger-pre-emption
} | vulnerability { not-pre-emptable | pre-emptable }
            exit
```

The mapping of these configured values to EPC ARP is given in below, this table is present 3GPP TS 23.401:

Table 31: Mapping of Release 99 bearer parameter ARP to EPS bearer ARP

Release 99 bearer parameter ARP value	EPS bearer ARP priority value
1	1
2	H + 1
3	M + 1

In the above table H = High-priority value configured and M = Medium-priority value.

ARP-RP Mapping for Radio Priority in Messages

The SGSN can choose a preferred radio priority according to the ARP values sent by the GGSN and HLR using the ARP to RP mapping. These mappings will be used by the corresponding 2G and/or 3G services to choose the radio priority value while triggering messages (such as those listed below) towards the MS/UE:

- Activate PDP Accept.
- Modify PDP Request during network-initiated PDP modification procedure.
- Modify PDP Accept during MS-initiated PDP modification procedure provided the ARP has been changed by the network.

Important In releases prior to 15.0 MR4 ER5, the Radio priority was hardcoded to "4" irrespective of ARP values received by the SGSN from either a GGSN or an HLR.

The following commands are used to create profiles for mapping ARP to RP values and associate the mapping with SGSN (3G) and GPRS (2G) services.

Use the following command in the SGSN Global configuration mode to create an ARP-RP mapping profile:

```
configure
    sgsn-global
        qos-arp-rp-map-profile arp_profile_name
        no qos-arp-rp-map-profile arp_profile_name
        end
```

Notes:

- *arp_profile_name* - Enter a string of 1 to 64 alphanumeric characters to identify the mapping profile and moves into the ARP-RP mapping profile configuration mode.
- **no qos-arp-rp-map-profile** - Removes the profile definition from the configuration.

When the ARP-RP mapping profile is created, the default ARP-RP mapping is automatically included (see default values in the Notes section below). This **arp** command, in the ARP-RP mapping profile configuration mode, modifies the ARP-RP mapping for the profile.

```
configure
    sgsn-global
        qos-arp-rp-map-profile arp_profile_name
            arparp_value radio-priority rp_value
            end
```

Notes:

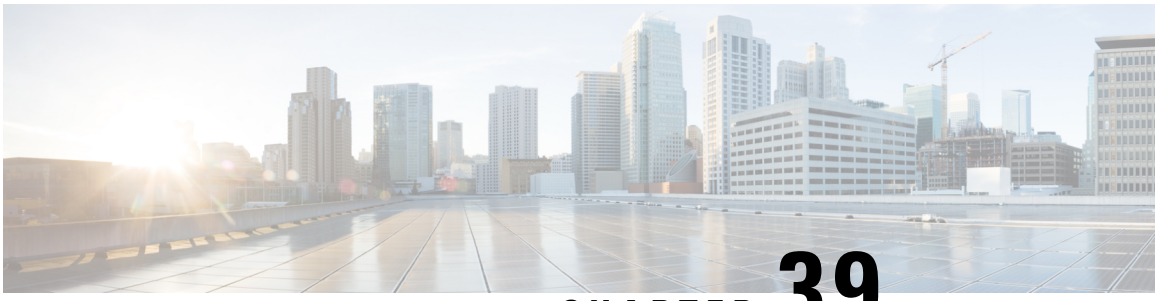
- *arp_value* - Defines the allocation retention priority. Enter an integer from 1 to 3.
- *rp_value* - Defines the radio priority. Enter an integer from 1 to 4.
- Default ARP-RP mapping would be
  - ARP1 RP4
  - ARP2 RP4
  - ARP3 RP4
- Use the **show sgsn-mode** command to display the ARP-RP profile and configuration.

The **radio-priority** keyword in the **sm** commands in both the GPRS-Service and SGSN-Service configuration modes. This keyword is used to associate an ARP-RP mapping profile with a 2G **and/or** a 3G service.

```
configure
    context context_name
        gprs-service service_name
            sm radio-priority from-arp arp_profile_name
            no sm radio-priority from-arp arp_profile_name
            end
```

Notes:

- This example illustrates the GPRS Service configuration mode, but either GPRS or SGSN Service configuration modes could be entered. The command sequent would have to be repeated, once for each type of service, to associate the ARP-RP profile with both types of services.
- **no sm radio-priority from-arp** - This command will remove the association from the configuration.
- Use the **show configuration** command to display the association.



CHAPTER 39

RAB Release for Attach on the Same IU Connection

- Feature Summary and Revision History, on page 449
- Feature Description, on page 450
- Configuring RAB Release for Attach on the Same IU Connection, on page 450
- Monitoring and Troubleshooting, on page 450

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *SGSN Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.12

Feature Description

With this release SGSN will send “RAB Assignment Request” with RABs to be released list to RNC and the session will be cleaned-up internally when “Attach Request” is received on Direct Transfer message on the existing IU connection.

Configuring RAB Release for Attach on the Same IU Connection

This section describes how to configure RAB Release for Attach on the Same IU connection.

Configuring RAB Assignment Request

Use the following configuration to send “RAB Assignment Request” with RABs to be released list to RNC by SGSN.

```
config
   context context_name
      iups-service  iups_service_name
            rnc id rnc_id
               [ no ]ranap rab-release-att-ext-iu
               end
```

Notes:

- **ranap rab-release-att-ext-iu** : When this CLI is configured, the SGSN will send “RAB Assignment Request” with RABs to be released list to RNC and the session will be cleaned-up internally when “Attach Request” is received on Direct Transfer message .
- **no**: Disables the configuration. By default this configuration is disabled.

Monitoring and Troubleshooting

This section provides information regarding show commands and bulk statistics available to monitor and troubleshoot the RAB Release for Attach on same IU connection.

Show Commands and Outputs

show iups-service name *service_name*

The output of this command includes the following fields:

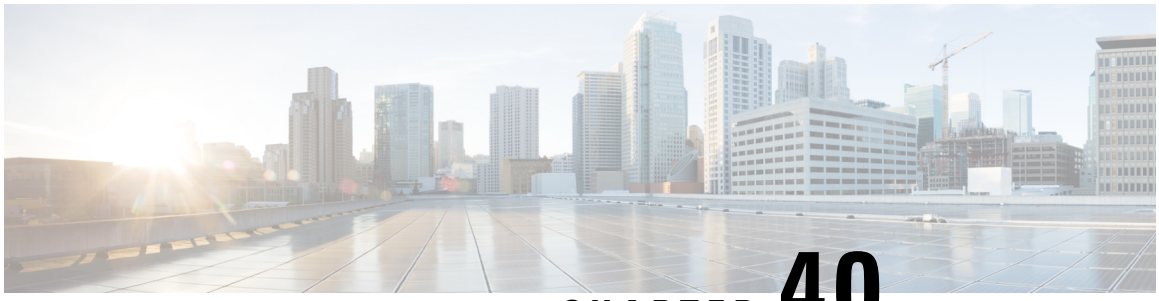
IUPS configuration Output

- Rab release for Attach Request on existing IU:

Verifying the RAB Release Extension configuration

The following command displays configuration information about Enable/Disable sending of RAB Release list to RNC when new Attach Request is received on same the IU connection.

show configuration



CHAPTER 40

RIM Message Transfer from BSC or RNC to eNodeB

This chapter describes how the SGSN transfers RIM messages to/from an MME (eNodeB) via GTPv1 protocol. It also provides details about RIM messages transferred to/from an MME (eNodeB).

- Feature Description, on page 453
- How It Works, on page 454
- Configuring RIM Msg Transfer to or from eNodeB, on page 456
- Monitoring and Troubleshooting RIM Msg Transfer, on page 457

Feature Description

RIM message transfer is one of the standards-based RAN Information Management procedures supported by the SGSN.

RAN Information Management (RIM)

RIM procedures provide a generic mechanism for the exchange of arbitrary information between RAN nodes. The RAN information is transferred via the SGSN core network node(s). In order to make the RAN information transparent for the core network, the RAN information is included in a RIM container that shall not be interpreted by the core network nodes.

The RAN information is transferred in RIM containers from the source RAN node to the destination RAN node by use of messages. The SGSN independently routes and relays each message carrying the RIM container.

In pre-15.0 releases, the SGSN supported RIM messages from BSS/RNC to another BSS/RNC belonging to a different or the same SGSNover GTPv1 protocol. Now, the SGSN also supports transfer of RIM messages to/from an MME (eNodeB) via GTPv1 protocol.

The SGSN uses existing CLI to enable the RIM transfer functionality. Whether or not the RIM message goes from/to BSC/RNC to/from BSC/RNC or to/from eNodeB is determined by the addressing. To transfer RIM messages to the MME (eNodeB),

- requires RIM functionality be enabled for the SGSN.
- requires the DNS server be configured to respond to a TAI-based DNS query

OR

- requires the MME (eNodeB) address be added to the SGSNs Call Control Profile

Relationships to Other Feature or Products

For this feature to work properly, the peer-MME for the eNodeB must also support RIM message handling.

How It Works

RIM Addressing

All the messages used for the exchange of RAN information contain the addresses of the source and destination RAN nodes. An eNodeB is addressed by tracking area identity (TAI) + eNodeB Identity (enbId).

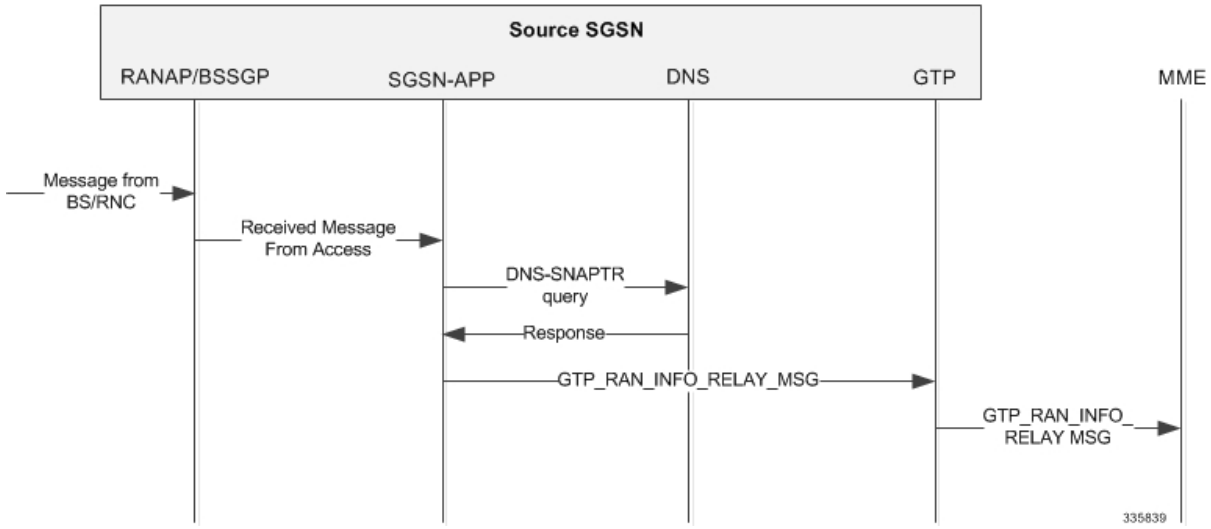
The source RAN node sends a message to its SGSN including the source and destination addresses. From the destination address, the SGSN shall decide whether or not it is connected to the destination RAN node. If the destination address is that of an eNodeB, then the SGSN uses the destination address to route the message, encapsulated in a GTPv1 message, to the correct MME via the Gn interface.

The MME connected to the destination RAN node decides which RAN node to send the message based on the destination address or the RIM routing address.

Call Flows - Transmitter of GTP RIM Msg

The following call flow illustrates how the SGSN behaves as the transmitter of GTP RIM messages.

Figure 80: Transmitting RIM Message



In the above illustration, the RIM message is transferred to the peer SGSN as follows:

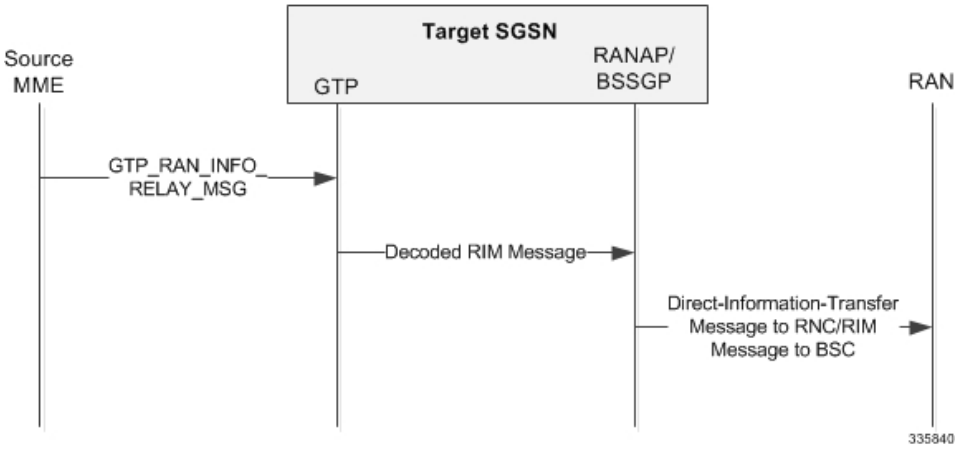
1. Upon receiving a RIM message from the network access BSS/RNC, the SGSN determines the RIM routing address type. If the message indicates that the target is an eNodeB, then SGSN searches for a locally configured MME address.

2. If a locally configured MME address is not available, then a DNS-SNAPTR query will be initiated to determine the MME address.
3. On receiving the DNS response and upon getting a valid MME address, an appropriate GTP API would be invoked.
4. On invocation of this API the GTP module will encode the RAN info relay message (as per TS 29.060) and dispatch the PDU to the peer MME.

Call Flows - Receiver of GTP RIM Msg

The following call flow illustrates how the SGSN behaves as the receiver of GTP RIM messages.

Figure 81: Receiving a GTP RIM Message



In this case, the SGSN has to decode the incoming GTP message correctly and forward the RIM message to the destination RNC/BSS.

1. SGSN would decode the received GTP RAN info relay message and construct a RANAP or BSSGP RIM message.
2. Appropriate actions would be taken to forward the RIM message to the destination RNC/BSS.

RIM Application

The RIM application processes the decoded RIM PDU from the access application. The routing area identifier (RAI) -- comprised of the mcc, mnc, rac -- is extracted from the destination address and is used to decide if the target routing area (RA) is local. If the RAI is locally available, the PDU is forwarded to either the RANAP or BSSGP stack based on the RIM routing address discriminator field.

The SGSN has a global list of local RAs. Each RA in turn has a list of RNCs and NSEIs that control it. If the destination RA is local, the list of NSEIs which serve the RAI is fetched. Each NSEI is searched for a matching cell id in the cellid-list. The PDU is then forwarded to the NSEI when signaling the BVCI.

If the RNC Id is in the destination cell identifier, then the IuPS service serving the local RAI is identified. The PDU is encoded in a RIM container and forwarded to the corresponding RANAP stack instance of that IuPS service.

If the eNodeB Id is in the destination cell identifier, then the PDU will be sent to the GTP app using the appropriate event.

The peer-MME address is resolved using the SGSN's local configuration or a DNS query for the TAI present in the destination address. For a successful DNS response, the PDU is encoded in a GTP RIM container and forwarded to the peer-MME. The SGTP service used will be the default SGTP service associated with the GPRS service or the SGSN service under which the source BSS/RNC was present. The RIM app drops a PDU if the DNS response fails. There will no retransmission or state-maintenance for the RIM PDU at the GTP-app.

Standards Compliance

The SGSN's RIM message transfer from/to eNodeB functionality complies with the following standards:

- 3GPP TS 29.060 version 11
- 3GPP TS 23.003 version 11
- 3GPP TS 25.413 version 11
- 3GPP TS 48.018 version 11
- 3GPP TS 24.008 version 11

Configuring RIM Msg Transfer to or from eNodeB

To enable successful RIM message transfer to/from an eNodeB, the following must be included in the SGSN's configuration:

- Configuring RIM functionality to work on SGSN
- Associating previously configured SGTP and IuPS services
- Configuring the peer-MME's address, in *one or both* of two ways
  - Configuring the peer-MME address locally
  - Configuring the DNS server

Configuring RIM Functionality

The following command sequences are used to enable RAN information management (RIM) functionality on the SGSN. The order in which these two configurations are performed is not significant.

The first command sequence enables RIM for the entire SGSN (global level).

```
configure
   sgsn-global
     ran-information-management
     end
```

The second command sequence associates the RNC configuration, the part of the IuPS service configuration governing the SGSN communication with any RNC, needs to have the RIM functionality enabled.

```
configure
   context context_name
     iups-service service_name
        rnc id rnc_id
           ran-information-management
           end
```

Associating Previously Configured SGTP and IuPS Services

The SGTP service configuration is a mandatory part of the SGSN's setup (refer to Configuring an SGTP Service in the SGSN Administration Guide), so an SGTP service configuration must already exist. The SGTP service is needed to send and/or receive GTPv1 protocol messages.

It is also a good idea to associate the IuPS service for the SGSN service to use for communication with the RAN.

The following illustrates the minimum configuration required to associate the SGTP and IuPS services for the RIM message transfers:

```
configure
  context context_name
     sgsn-service service_name
        associate sgtp-service service_name context context_name
        ran-protocol iups-service service_name
        end
```

Configuring the peer-MME's address - Locally

Use the Call Control Profile to define the peer-MME address.

Use the tac keyword to configure the tracking area code (TAC) of the target eNodeB that maps to the peer-MME address. For RIM message transfer, you also need to configure the Gn interface. The following is an example of the configuration to use:

```
configure
  call-control-profile profile_name
     peer-mme tac tac_value prefer local address ip_address interface gn
     end
```

Where:

- tac_value can be an entry from 1 to 65535.
- ip_address is the standard format address for either IPv4 or IPv6.
- gn is the interface selection used for RIM message transfer.

Configuring the peer-MME's address - for DNS Query

If using a DNS query to determine the peer-MME RIM address, then the DNS server must be pre-configured to respond to a TAI-based DNS query in the following format:
tac-lb<TAC-low-byte>.tac-hb<TAC-high-byte>.tac.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org

Monitoring and Troubleshooting RIM Msg Transfer

The show command statistics illustrated below, can be used to monitor or troubleshoot this functionality. Note that the selected output is only a portion of the information displayed by the command.

show gmm-sm statistics verbose

show gmm-sm statistics verbose

```
...
Ranap Procedures:
  Direct Transfer Sent:   0     Direct Transfer Rcvd:   0
```

show gmm-sm statistics verbose | grep RIM

show gmm-sm statistics verbose | grep RIM

```
...
RIM Message Statistics:
RIM Messages dropped:
  due to RIM disabled in SGSN:             0     due to RNC not Capable:     0
  due to RIM Routing Address not present:   0     due to RNC does not exist:   0
```

show sgtpc statistics verbose

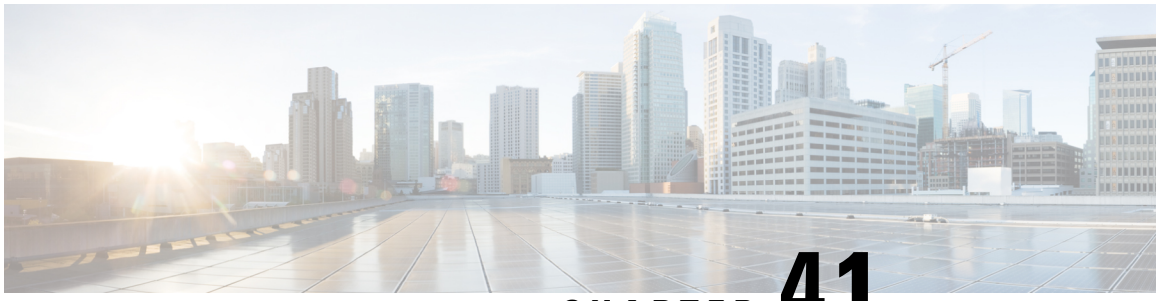
show sgtpc statistics verbose

```
...
RAN info Relay Msg:
Total messages received:         0  Total messages sent:  0
Total messages dropped:          0
  due to DNS failure:            0
  due to RIM disabled in SGSN:   0
  due to Invalid Routing Addr:   0
```

show bssgp statistics verbose

show bssgp statistics verbose

```
...
RIM Messages
  RAN Information messages received
  RAN Information messages transmitted
  RAN Information Request messages received
  RAN Information Request messages transmitted
  RAN Information ACK messages received
  RAN Information ACK messages transmitted
  RAN Information Error messages received
  RAN Information Error messages transmitted
  RAN Information Appln Error messages received
  RAN Information Appln Error messages transmitted
  RIM messages dropped
    due to RIM disabled in SGSN
    due to destination BSC not RIM capable
    due to destination cell does not exist
     due to invalid destination address
```



CHAPTER 41

RTLLI Management for 2G M2M Devices

- Feature Description, on page 459
- How It Works, on page 459
- Configuring RTLLI Management, on page 459
- Monitoring and Troubleshooting, on page 460

Feature Description

Fixed Random TLLI (RTLLI) Management for 2G M2M devices is intended to expand the operator's control of TLLI (temporary logical link identifier) in the following scenario:

When multiple M2M devices attempt PS Attaches, with the same fixed RTLLI coming from different NSEIs (network service entity identifier), the SGSN cannot distinguish between the devices. The SGSN functions ***as if*** the first device bearing an RTLLI is no longer attached and begins to communicate with the next device using that same RTLLI. With multiple M2M devices attempting attaches - all with the same RTLLI - the result is TLLI collision and dropped calls.

How It Works

This feature deals with Attach problems due to simultaneous IMSI attaches, all with the same fixed RTLLI.

Beginning with Release 16.3, it became possible to configure the SGSN to discard/drop Attach Request messages received from an MS with an RTLLI already in use on the SGSN by adding validation of the NSEI. Attach gets processed if the attach is coming from a different NSEI. This functionality is disabled by default.

Beginning with Release 19.3, to further reduce jumbling of authentication vectors across subscribers, the Fixed Random TLLI Handling mechanism extends the functionality noted above. A new verification table has been added to the GbMgr. The table maintains a list of TLLI + NSEI and if an incoming Attach Request includes a TLLI + NSEI already on the table then the call is dropped. This functionality is disabled by default.

Configuring RTLLI Management

No new commands or keywords have been added to the command line interface (CLI) in support of Fixed Random TLLI Management. Enabling / disabling this mechanism is integrated into existing CLI.

For information about the commands, parameters and parameter values, please check your *Command Line Interface Reference* manual for each of the commands listed below.

Important The following configurations should be performed during system boot up. It is not advisable to enable/disable this TLLI management functionality during runtime.

Verifying Both the RTLLI and the NSEI

To enable the SGSN to handle Attach Requests with the same fixed RTLLI by verifying both the RTLLI and the NSEI, use the following configuration:

```
config
  sgsn-global
    gmm-message attach-with-tlli-in-use discard-message only-on-same-nsei

     old-tlli invalidate tlli hex_value
     old-tlli hold-time time
     end
```

Notes:

- **only-on-same-nsei** - This keyword is required to enable this new verification mechanism.

Verifying Only the RTLLI

To enable the SGSN to handle Attach Requests with the same fixed RTLLI by verifying only the RTLLI, use the following configuration:

```
config
  sgsn-global
     gmm-message attach-with-tlli-in-use discard-message
     old-tlli invalidate tlli hex_value
     old-tlli hold-time time
     end
```

Notes:

- **only-on-same-nsei** - Do not include this keyword to disable this new verification mechanism. The system defaults to the verification mechanism provided with Release 16.3 (see *How It Works*).

Verifying Configuration

To verify if the functionality is enabled or disabled, use the following commands from the Exec mode:

```
show configuration | grep gmm-mess
show configuration | grep old-
show configuration verbose | grep old-
```

Monitoring and Troubleshooting

This section provides information for monitoring and/or troubleshooting the RTLLI Management functionality.

To see the statistics of attach drops that are due to same-RTLLI collisions, execute the show commands listed below. When you are looking at the generated statistics, consider the following:

- If the generated counter values are not increasing then collisions are not occurring.
- If the generated counter values are increasing then it means collisions are occurring and attaches were dropped.

Configured to Verify Both RTLLI and NSEI

If **gmm-message attach-with-tlli-in-use discard-message only-on-same-nsei** is configured then the following show command can give the drop count of attaches caused by same RTLLI and NSEI:

```
show gbmgr all parser statistics all | grep use

IMSI Key: 1487 P-TMSI Key: 0 attach with tlli in use : 592 <-- drops from existing table
with RTLLI+NSEI
Add P-TMSI Key: 0 attach drop tlli in use(pre tlli check): 297 <-- drops from new table
with RTLLI

IMSI Key : 1190 P-TMSI Key : 594 attach with tlli in use : 395
Add P-TMSI Key : 0 attach drop tlli in use(pre tlli check) : 198
```

Configured to Verify Only RTLLI

If "gmm-message attach-with-tlli-in-use discard-message" is configured then the following show command can give the drop count of attaches caused by same RTLLI:

```
show gbmgr all parser statistics all | grep use

 IMSI Key: 1487 P-TMSI Key: 0 attach with tlli in use : 592 <-- drops from existing table
with RTLLI
Add P-TMSI Key: 0 attach drop tlli in use(pre tlli check): 297 <-- drops from new table
with RTLLI

IMSI Key : 1190 P-TMSI Key : 594 attach with tlli in use : 395
Add P-TMSI Key : 0 attach drop tlli in use(pre tlli check) : 198
```

Verify Attach Rejects due to Same RTLLI

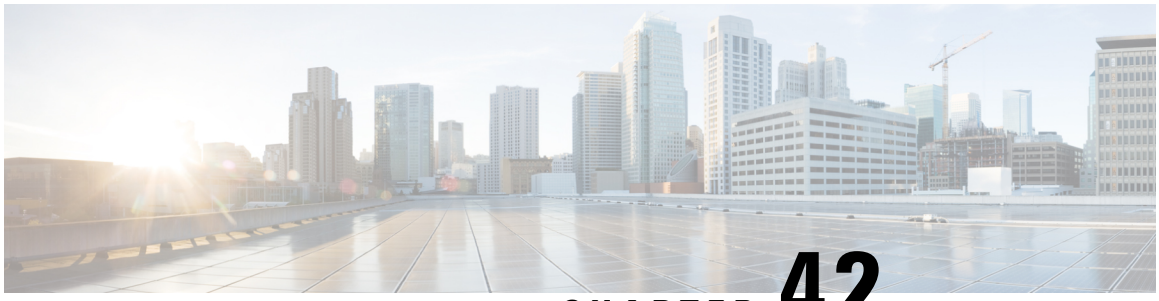
The following show command generates SessMgr counters that track the Attach Rejects due to same RTLLI collision:

```
show gmm sm stats | grep Same random tlli collision

Same random tlli collision: 10
```

Beginning with Release 19.3.5, the 'sgsn-implicit-detach(237)' session disconnect reason pegs when the 2G-SGSN rejects the Attach Request due to same RTLLI collision.

Beginning in Release 19.4, the following show command identifies the two bulk statistics the SGSN uses to track the number of times the SGSN rejects Attach Requests or Combined Attach Requests due to same RTLLI collision.

```
show bulkstats variables sgsn | grep colli
%2G-simple-attach-rej-randomtlli-collision%                  Int32     0   Counter
%2G-combined-attach-rej-randomtlli-collision%                Int32     0   Counter
```



CHAPTER 42

S4 interface Support For Non-EPC Devices

This chapter describes the S4 interface support for Non-EPC capable devices.

- Feature Description, on page 463
- How it Works, on page 464
- Configuring S4 Interface Support for Non-EPC Capable Devices, on page 465
- Monitoring and Troubleshooting S4 Interface Support for Non-EPC Capable devices, on page 466

Feature Description

The S4 interface support has been extended to Non-EPC capable devices. This support was only available for EPC service capable devices or subscribers with EPS subscription. S4 interface support to Non-EPC devices allows more control on interface selection and ability to handle QoS and legacy UE related behavior issues.

Overview

To enable S4 support for Non-EPC devices, interface selection options during first PDP activation have been added, these options allow the following:

1. S4 interface selection based on UEs EPC capability alone.
2. S4 interface selection only for UEs that are EPC capable and those that have EPS subscription.
3. S4 interface selection for all UEs having EPS subscription.
4. An option to always select S4 interface.

Important For all the options listed above (except option "2"), the HSS/HLR subscription could have both EPS and GPRS subscription. In such cases, the S4-SGSN prefers EPS subscription, but chooses the subscription that has the record for requested or default APN. The type of subscription chosen during the first PDP context activation is stored as UE level information and this is used to choose the same subscription for all subsequent primary PDP activations by the UE.

When the S4 interface is used and a Non-E-UTRAN capable device requests for PDP de-activation of only the primary PDP without de-activating the associated secondary PDP's (that is, without a teardown indicator), the SGSN deletes the associated secondary PDP contexts locally without informing UE.

When a Non-E-UTRAN capable UE activates a PDP context with Conversational or Streaming class (GBR bearers) and if Iu is released, the UE preserves the PDP with bit rate set to "0" kbps. However, when the S4-SGSN notices an Iu-Release, it has to de-activate the GBR bearers. Currently the S4-SGSN does not support the de-activation of GBR bearers. When S4-SGSN support for PDP context preservation procedures is added in a future release (for both EPC and Non-EPC devices), GBR bearers will be de-activated without informing the UE.

How it Works

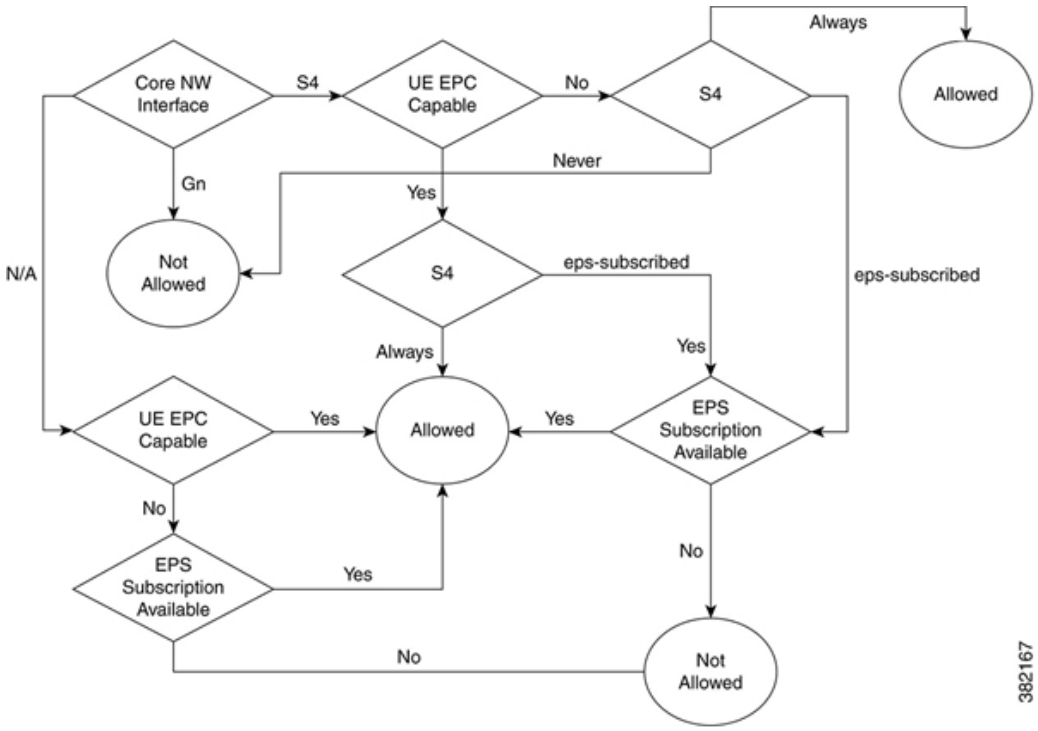
Architecture

To implement S4 interface support for Non-EPC capable devices the existing CLI command **sgsn-core-nw-interface** under the Call-Control-Profile configuration has been enhanced with options for interface selection during first PDP activation, the various options include:

1. Option to select the S4 interface based on UE's EPC capability alone.
2. Option to select the S4 interface only for UEs that are EPC capable and those that have EPS subscription.
3. Option to select the S4 interface for all UEs having EPS subscription
4. Option to select the S4 interface always.

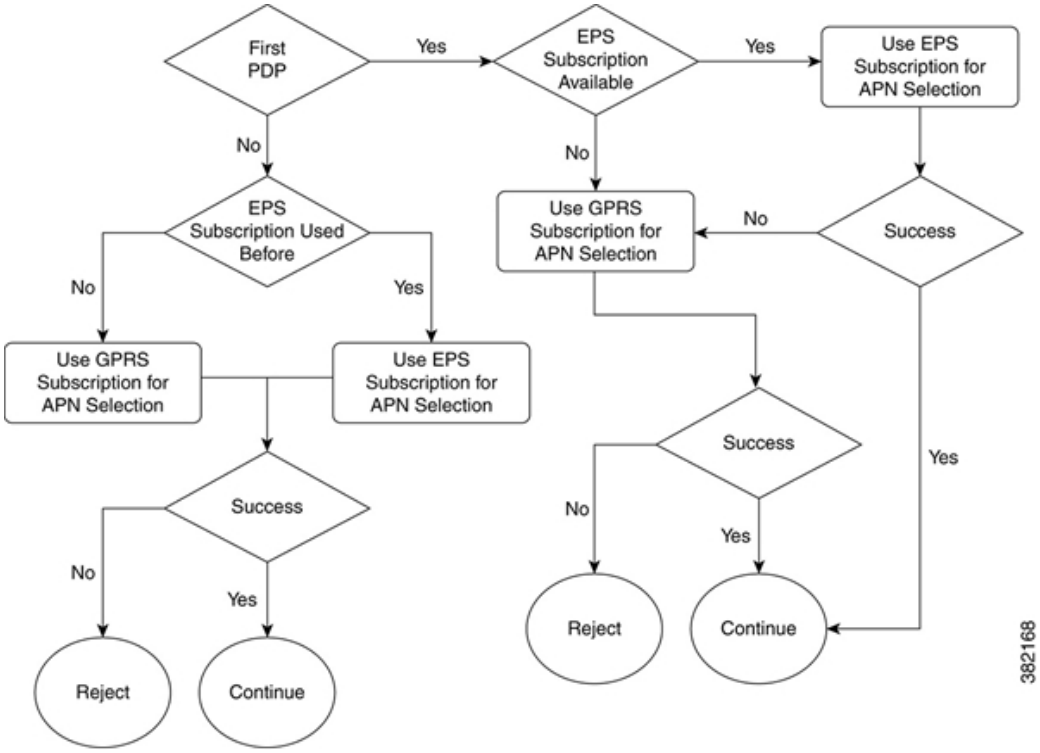
Various combinations of the options listed above can be configured and the logic UE can use the S4 interface based on the following logic:

Figure 82:



When the S4 interface is allowed, APN selection is performed based on the following logic:

Figure 83:



For more information on the CLI commands see, Command Line Interface Reference.

Limitations

1. QoS modification of non-GBR bearer - A Non-E-UTRAN capable UE can request QoS bit rate modification even for Non-GBR bearers. This functionality is currently not supported. The MS initiated QoS modification for primary PDP is rejected and QoS modification for non-GBR secondary PDP is handled by sending BRC with zero Flow QoS. The PGW can respond with UBR (with modified APN-AMBR) or DBR and both are handled appropriately.
2. Restricting APN-AMBR to "472" Kbps after 3G to 2G IRAT - Restricting APN-AMBR to "472" Kbps after 3G to 2G IRAT is based on the assumption that the PGW /PCRF decide on correct QoS based on RAT, hence additional signaling can be avoided. However, upgrading of APN-AMBR after 2G to 3G IRAT is supported, the SGSN can initiate bearer modification based on RNC / UE capabilities and same are honored by PGW/PCRF.

Configuring S4 Interface Support for Non-EPC Capable Devices

This section describes how to configure S4 interface support for Non-EPC capable devices.

Configuring selection of the S4 interface

The command **sgsn-core-nw-interface** in the Call-Control-Profile configuration is enhanced with keywords to support S4 interface selection:

```
config
 call-control-profile cc-profile name
  sgsn-core-nw-interface {gn | s4 [epc-ue {always | eps-subscribed} non-
 epc-ue {never | always | eps-subscribed}]}
  exit
```

Notes:

- When keywords or options are not selected with the selection of the S4 interface option, it implies that the SGSN will apply S4 interface always for both EPC and Non- EPC devices. This is also synonymous to the CLI command configured as **sgsn-core-nw-interface s4 epc-ue always non-epc-ue always**.
- To configure SGSN behavior supported in previous releases, the CLI is configured as **sgsn-core-nw-interface s4 epc-ue always non-epc-ue eps-subscribed**. This is also the default behavior when the CLI is not configured.

For more information on the CLI commands see, Command Line Interface Reference.

Monitoring and Troubleshooting S4 Interface Support for Non-EPC Capable devices

This section provides information on how to monitor S4 interface support for Non-EPC capable devices and to determine that it is working correctly.

S4 Interface Support for Non-EPC devices Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of the S4 interface support for Non-EPC devices.

show call-control-profile full name < >

This show command is updated with information about SGSN core network interface selection. The following new fields have been added:

- SGSN Core Network Interface Selection
- SGSN Core Network Interface Type
- S4 for EPC Capable Devices
- S4 for Non-EPC Capable Devices

The field **SGSN Core Network Interface Type** displays interface selected as either **Gn** or **S4**.

The field **S4 for EPC Capable Devices** displays the configuration as either **Always** or **When EPS Subscription Available**, based on the CLI configured in the command **sgsn-core-nw-interface** in the Call-Control Profile.

The field **S4 for Non-EPC Capable Devices** displays the configuration as **Never** or **Always** or **When EPS Subscription Available**, based on the CLI configured in the command **sgsn-core-nw-interface** in the Call-Control Profile.

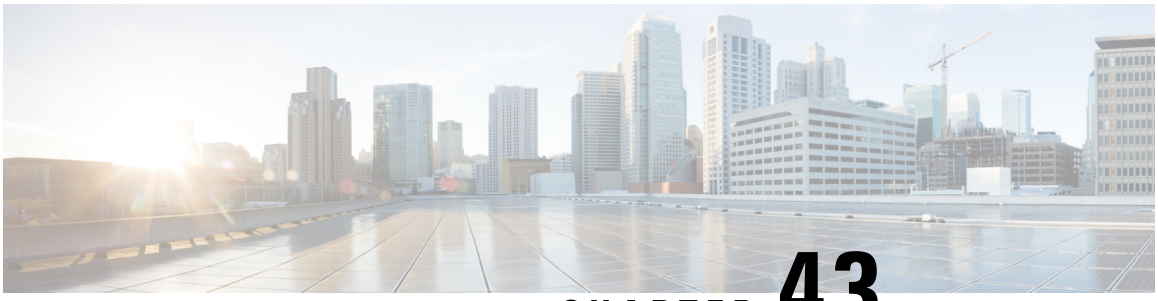
show subscribers sgsn-only full imsi < >

This show command is updated to display the subscription type being used for primary PDP activation. The field **Subscription Type** is added to the show output. The subscription type is displayed as either **EPS** or **GPRS**.

show subscribers gprs-only full imsi < >

This show command is updated to display the subscription type being used for primary PDP activation. The field **Subscription Type** is added to the show output. The subscription type is displayed as either **EPS** or **GPRS**.

show subscribers gprs-only full imsi < >



CHAPTER 43

S4-SGSN Suspend-Resume Feature

This chapter describes the S4-SGSN Suspend/Resume feature.

- Feature Description, on page 469
- How it Works, on page 470
- Configuring the S4-SGSN Suspend/Resume Feature, on page 480
- Monitoring and Troubleshooting the S4-SGSN Suspend/Resume Feature, on page 480

Feature Description

The S4-SGSN Suspend/Resume feature provides support for suspend/resume procedures from the BSS and a peer S4-SGSN.

When a UE is in a 2G coverage area wants to make a circuit switched voice call but the Class A mode of operation is not supported by the network, then the packet switched data session (PDP contexts) must be suspended before the voice call can be made. In this case, the BSS sends a Suspend Request to the SGSN. If the UE is already attached at that SGSN then the suspend request is handled via an intra-SGSN suspend/resume procedure. If the UE is not attached at the SGSN then the Suspend Request is forwarded to a peer SGSN/MME through GTPv2 and an inter-SGSN/SGSN-MME suspend procedure occurs. Once the UE completes the voice call, either the BSS sends a resume request to resume the suspended PDPs or the UE directly sends a Routing Area Update Request (RAU) in 2G which will be treated as an implicit resume.

The ability for a GPRS user to access circuit-switched services depends on the subscription held, the network capabilities, and the MS capabilities.

Suspension of GPRS Services

The MS sends a request to the network for the suspension of GPRS services when the MS or the network limitations make it unable to communicate on GPRS channels in one or more of the following scenarios:

1. A GPRS-attached MS enters dedicated mode and the support of the Class A mode of operation is not possible (for example, the MS only supports DTM and the network only supports independent CS and PS).
2. During CS connection, the MS performs a handover from Iu mode to A/Gb mode, and the MS or the network limitations make it unable to support CS/PS mode of operation, (for example, an MS in CS/PS mode of operation in Iu mode during a CS connection reverts to class-B mode of operation in A/Gb mode).
3. When an MS in class A mode of operation is handed over to a cell where the support of Class A mode of operation is not possible (for example, a DTM mobile station entering a cell that does not support DTM).

Relationships to Other Features

One of the following configurations must exist on the SGSN for the Suspend Resume feature to work properly on the S4-SGSN:

- 2G SGSN Service + S4-SGSN Support
- 3G SGSN Service + S4-SGSN Support
- 2G SGSN Service + 3G SGSN Service + S4-SGSN Support

Configuration procedures for the above deployments are available in this guide.

How it Works

S4-SGSN Suspend-Resume Feature

When a UE wants to make or receive a voice call via a GERAN circuit switched domain, and if the UE/BSS doesn't support DTM mode, then the BSS sends a Suspend Request to the SGSN to suspend any packet data transmission. This suspend request can be received on the same SGSN where a subscriber is already attached, or it can be received on an SGSN where the subscriber is not yet attached.

SGSN where subscriber is attached: The SGSN initiates an intra-SGSN suspend procedure and will have to suspend the data transmission all the way up to the PGW by sending a Suspend Request to the SGW/PGW. When the UE completes the CS call, it will resume the packet transmission. The BSS will send a Resume request in this case.

SGSN where subscriber is not yet attached: The SGSN initiates an inter-SGSN suspend procedure by sending a GTPv2 / GTPv1 Suspend Request to the peer SGSN/MME. The peer node will suspend the data transmission. When the UE completes the CS call, it may directly send a Routing Area Update request to the 2G SGSN to handover the packet switched contexts. The 2G SGSN will do a Context Request / Context Response / Context Ack procedure with the peer node and will send a Create Session Request (if SGW relocation occurs) or a Modify Bearer Request (if no SGW relocation occurs) to the SGW. The Modify Bearer Request at the PGW will be treated as an implicit Resume.

Limitations

The following are the known limitations for the S4-SGSN Suspend/Resume feature:

1. If a suspend request aborts an ongoing RAU triggered SGW relocation, the Create Session Request will be aborted and the PDN will be cleaned up. This is to avoid complexities in the state machine. If the system retained PDP, the system would have to recreate the tunnel towards the old SGW to PGW before sending the Suspend Notification. This would delay the Suspend procedure.
2. A Suspend Request from the default SGSN in a pool to the SGSN serving the NRI of the given PTMSI is not possible via the S16 interface due to a standards limitation. R10 specifications don't have a hop counter and UDP source port IEs in the Suspend Notification message and hence this limitation. This is corrected in R11 specifications. TheS4-SGSN will support this call flow only in later releases.
3. HSS initiated modification will be queued, if the Suspend preempts an HSS initiated modification while pending for an Update Bearer Request from the PGW. The queued procedure will be restarted in a subsequent procedure (RAU / Resume). Queued information will not be transferred to another RAT type, if a subsequent procedure changes the RAT type.

4. A Suspend Acknowledge with rejected cause will not be sent to the peer SGSN/MME when an inter-SGSN Suspend procedure is preempted by procedures such as RAU, Context Request, and Detach Request at the old SGSN. Suspend Acknowledge is not sent because it is very complex on the PMM-side to distinguish between two procedures as the PMM has the same state for both the inter-SGSN Suspend procedure and the inter-SGSN RAU procedure.

Call Flows

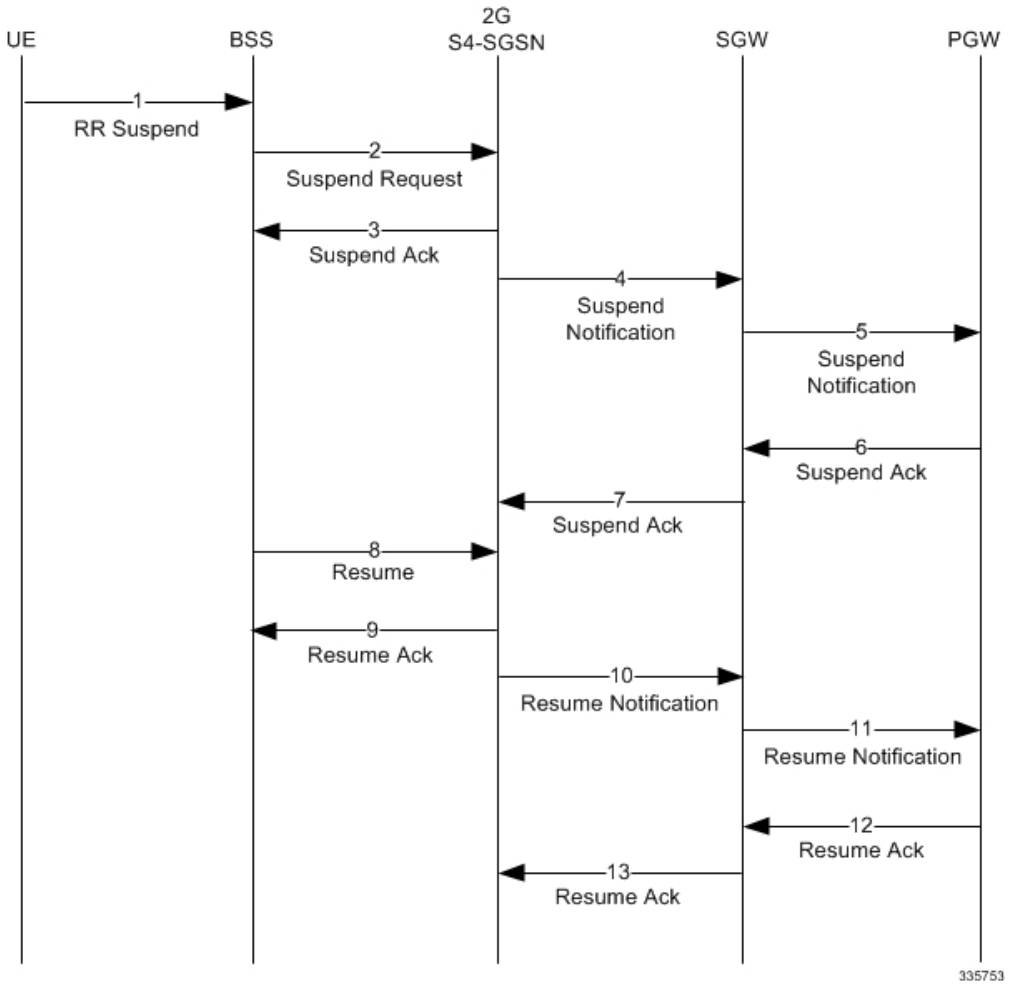
This section includes various diagrams that illustrate the Suspend/Resume call flow procedures, and the interface selection logic.

Intra-SGSN Suspend Procedure with Resume as the Subsequent Procedure

The intra-SGSN Suspend procedure with Resume as the subsequent procedure is illustrated in the following diagram.

- When a 2G SGSN receives a Suspend Request from the BSS and if the subscriber is already attached to the 2G SGSN, the PDPs shall be suspended. The SGSN then sends a Suspend Notification to the SGW, which subsequently is sent to the PGW to stop all data transmissions on non-GBR bearers.
- When a 2G SGSN receives a Resume Request from the BSS, and if the subscriber that is already suspended is attached to the 2G SGSN, the PDPs are resumed. The SGSN then sends a Resume Notification to the SGW, which subsequently is sent to the PGW to resume all data transmissions on non-GBR bearers.

Figure 84: Intra-SGSN Suspend Procedure with Resume as Subsequent Procedure

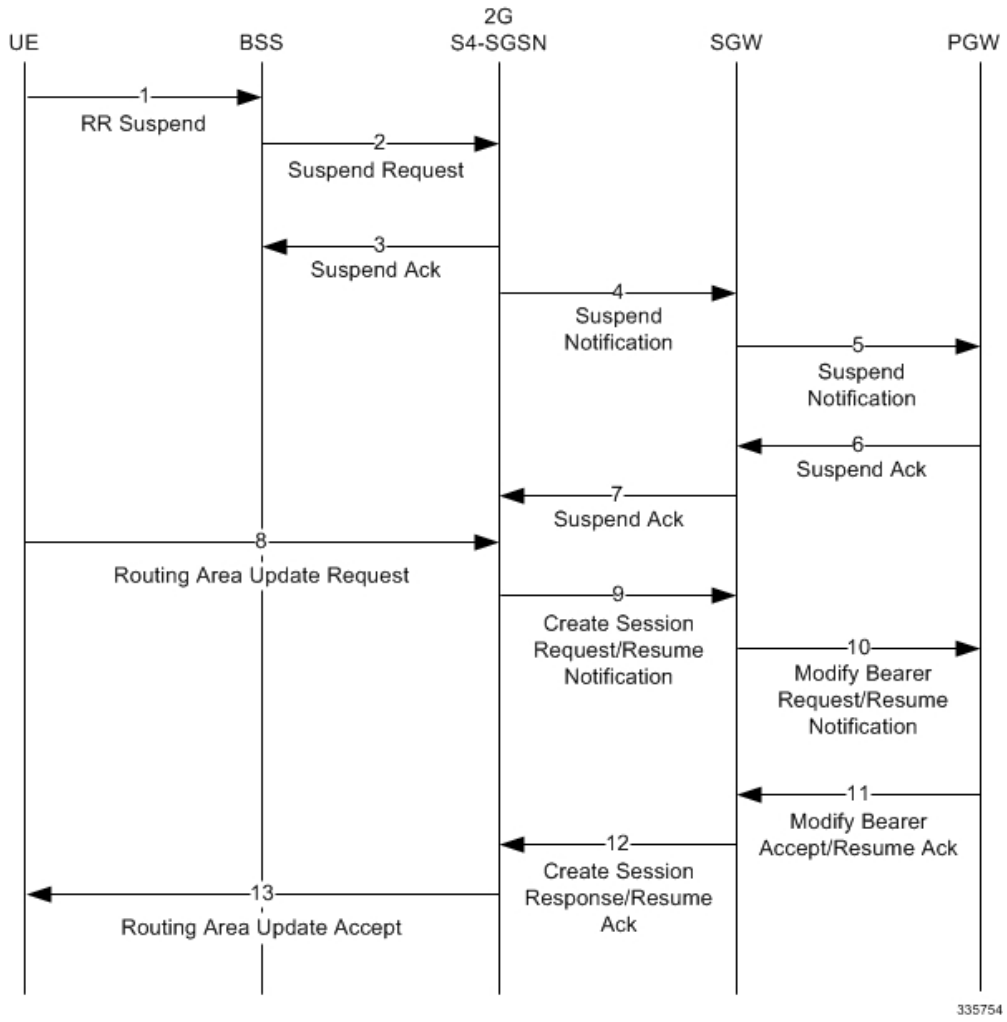


Intra-SGSN Suspend with Resume Procedure with Intra-RAU as Subsequent Procedure

An Intra-SGSN Suspend procedure call flow with an Intra-SGSN RAU procedure as the subsequent procedure is shown in the following illustration.

- If there is no SGW change for the RAU request, then the 2G-SGSN sends a Resume Notification to the SGW and the SGW then sends a Resume Notification to the PGW to resume all data transmissions.
- If there is a SGW change for the RAU request, then the 2G-SGSN sends a Create Session request to the SGW and the SGW sends a Modify Bearer Request to the PGW to resume all data transmissions.

Figure 85: Intra-SGSN Suspend Procedure with Intra-RAU as Subsequent Procedure

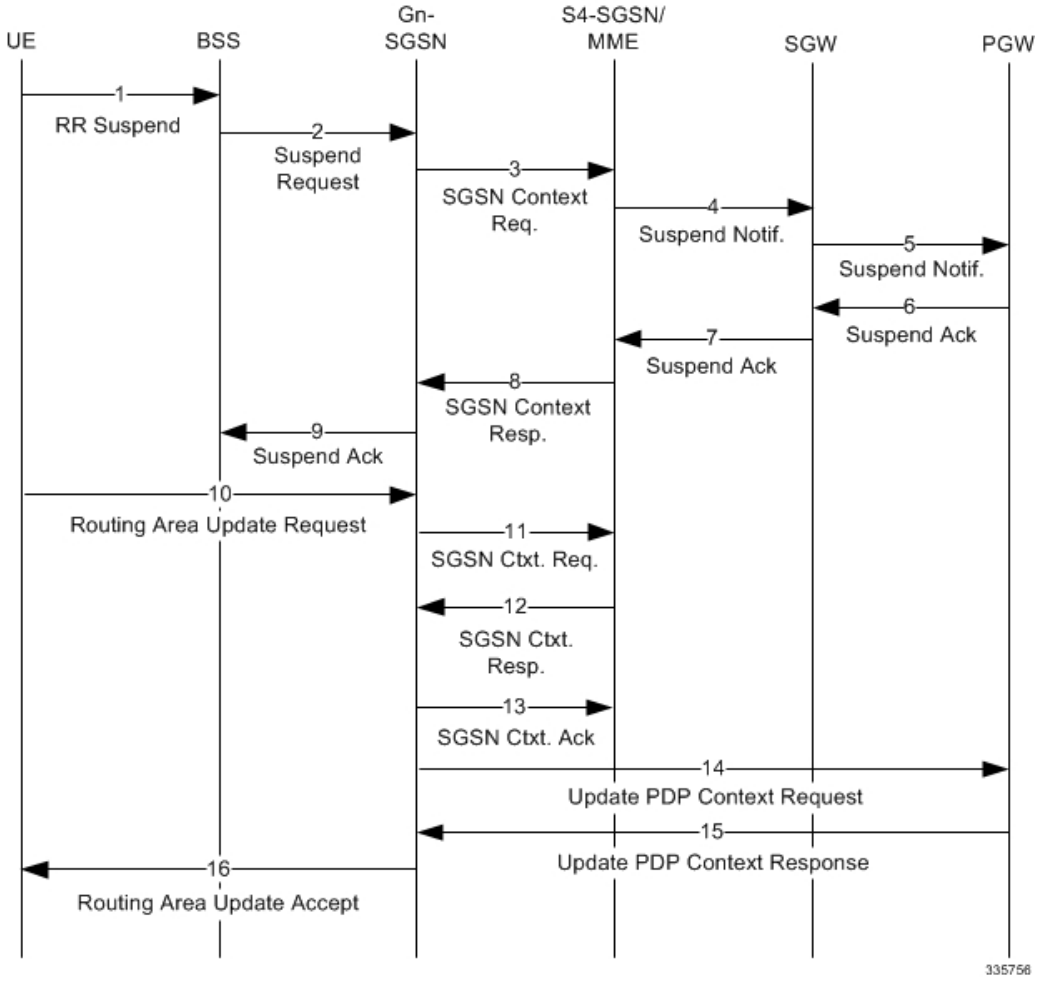


Inter-SGSN Suspend and Resume Procedure with Peer S4-SGSN/MME

The procedure for a new SGSN Suspend Request and Resume procedure with a peer S4-SGSN/MME is shown in the following diagram.

- When an S4-SGSN receives a Suspend Request from the BSS and if the subscriber is not attached to the 2G SGSN, the S4-SGSN will send a Suspend Notification to the peer S4-SGSN/MME.
- The new SGSN RAU is the Resume procedure after a new SGSN Suspend procedure has been completed. The SGSN sends a Create Session Request / Modify Bearer Request to the SGW which subsequently is sent to the PGW to resume all data transmissions on non-GBR bearers.
- When the Gn-SGSN receives a Suspend Request from the BSS and if the subscriber is not attached to the 2G SGSN, it sends a Suspend Notification to the peer Gn-SGSN / S4-SGSN/MME.

Figure 86: Inter-SGSN Suspend and Resume Procedure with Peer S4-SGSN/MME

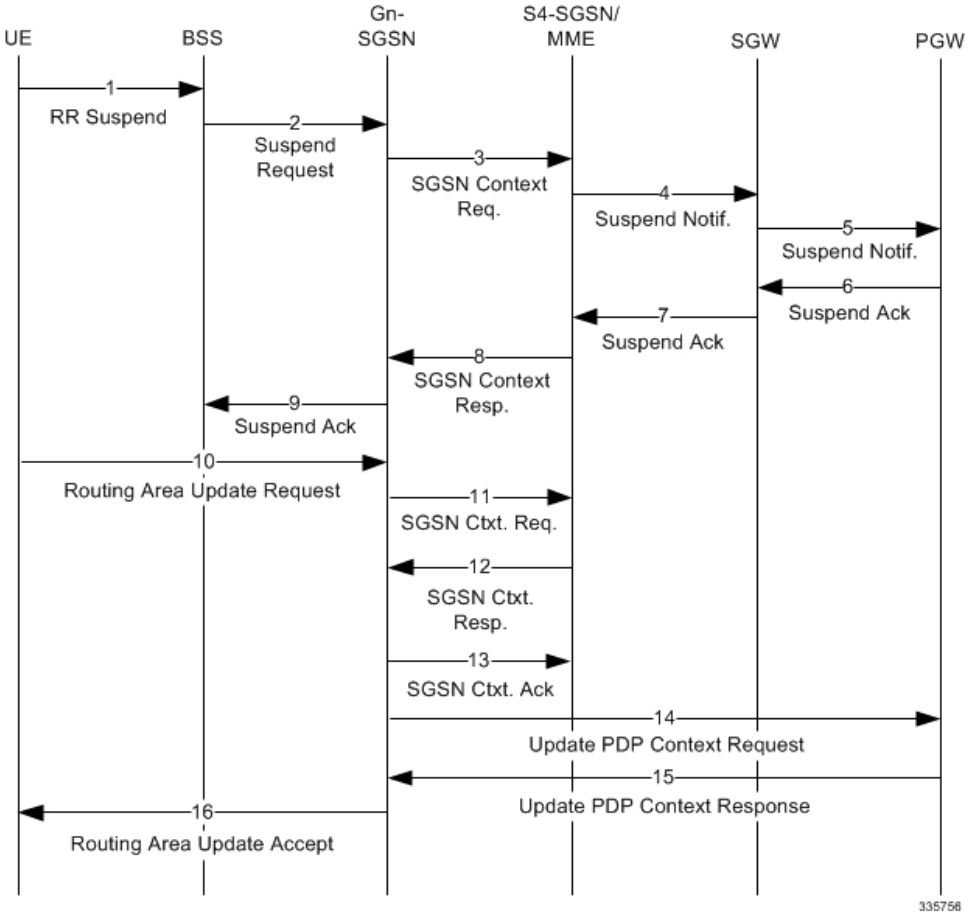


New Inter-SGSN Suspend and Resume Procedure from BSS to 2G Gn-SGSN

A new SGSN Suspend Request from the BSS to a 2G Gn-SGSN is shown in the following illustration.

- The new SGSN RAU is the Resume procedure after the new SGSN Suspend procedure has been completed. The Gn-SGSN sends an Update PDP Context Request to the GGSN which subsequently is sent to PGW to resume all data transmissions on non-GBR bearers.
- When the S4-SGSN receives a Suspend Request from the BSS and if the subscriber is not attached to the 2G SGSN and the peer is a Gn-SGSN, it sends a Context Request with Suspend header (GTPv1 Suspend Request) to the peer Gn-SGSN.

Figure 87: New Inter-SGSN Suspend and Resume Procedure from BSS to 2G Gn-SGSN

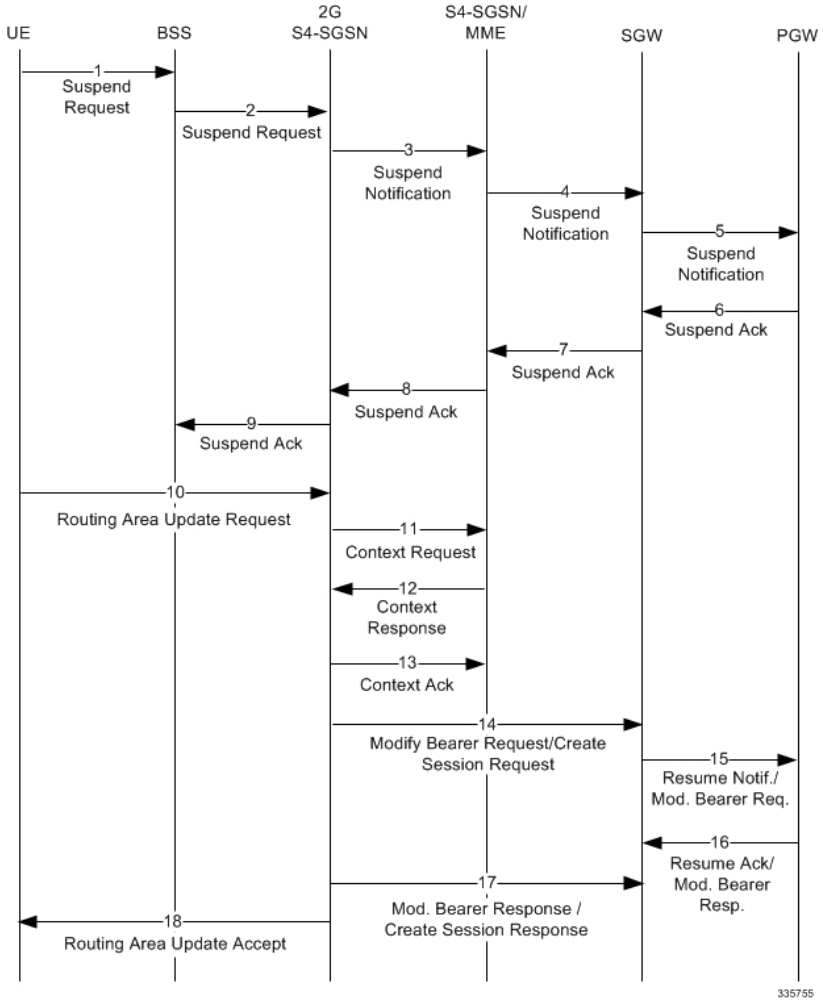


New SGSN Suspend and Resume Procedure with Peer Gn-SGSN as Old SGSN

The new SGSN Suspend procedure with a peer Gn-SGSN as the old SGSN is shown in the following illustration.

- The new SGSN RAU is the Resume procedure after the new SGSN Suspend procedure is completed. The SGSN sends a Create Session Request / Modify Bearer Request to the SGW which subsequently is sent to the PGW to resume all data transmissions on non-GBR bearers.

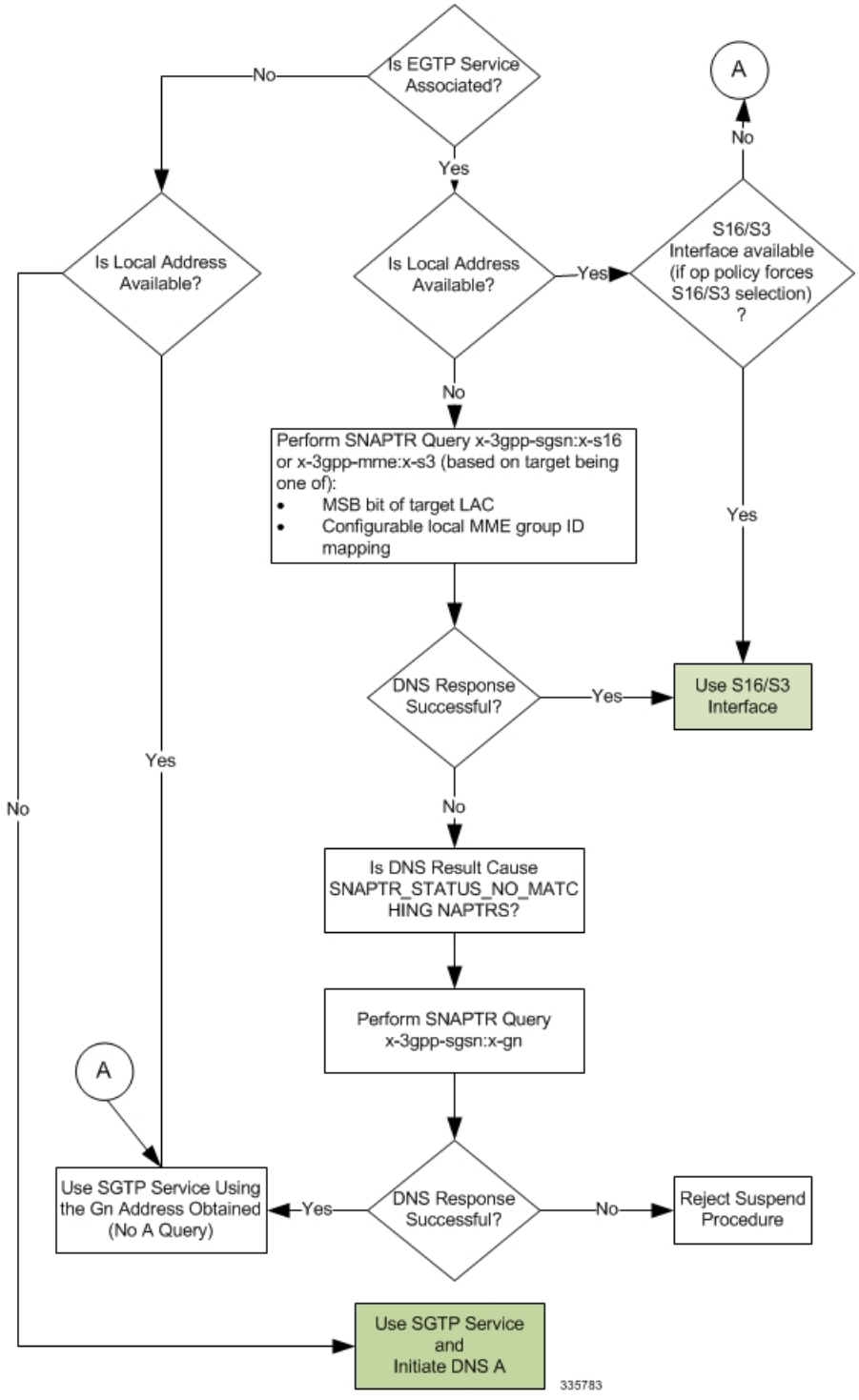
Figure 88: New SGSN Suspend and Resume Procedure with Peer Gn-SGSN as Old SGSN



Interface Selection Logic for Inter-SGSN Suspend (New SGSN) Procedure

Interface selection logic to find the peer address during the Inter SGSN Suspend (New SGSN Suspend) procedure is explained in the flowing flow chart.

Figure 89: Interface Selection Logic for Inter-SGSN Suspend (New Suspend) Procedure

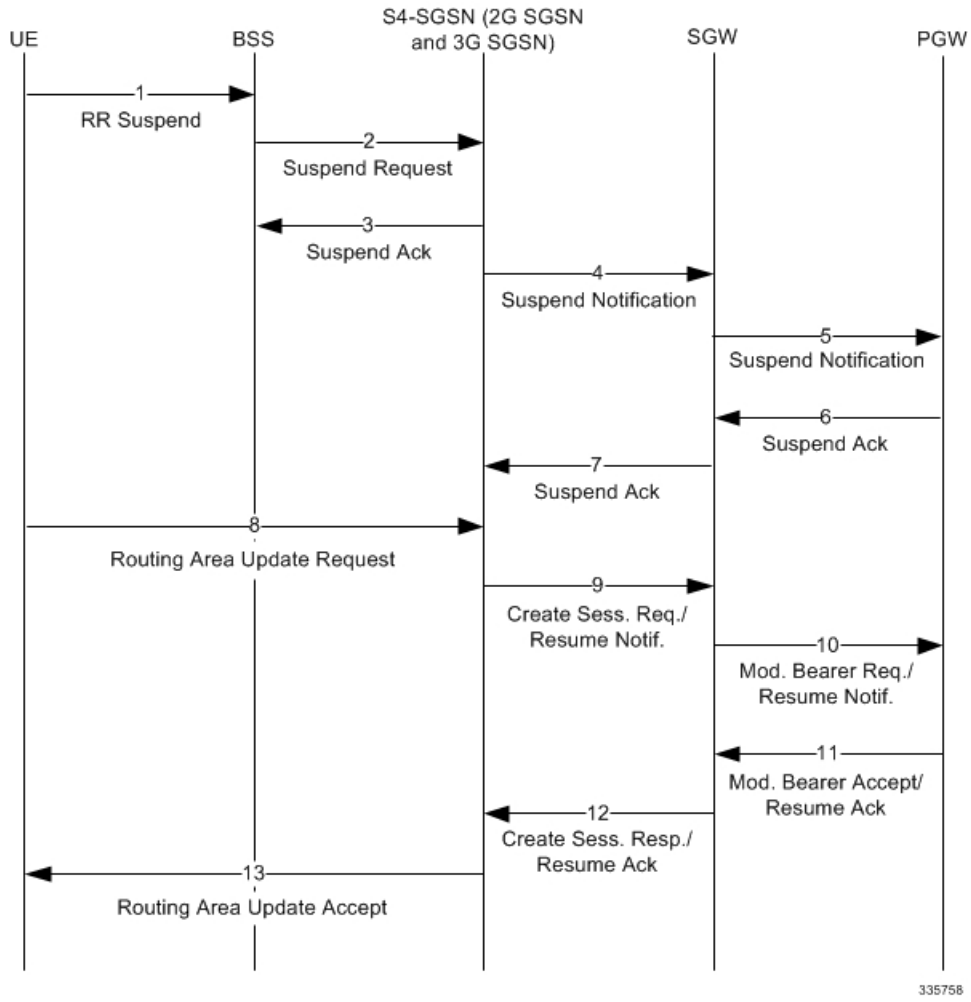


Intra-SGSN Inter-System Suspend and Resume Procedure

The intra-SGSN Inter-System Suspend and Resume procedure is shown in the following illustration. In this case, the BSS sends a Suspend Request to the 2G part of the SGSN. The 2G SGSN will internally send the request to the 3G S4-SGSN where the PDPs are anchored. The PDP contexts are then suspended by 3G S4-SGSN as shown in the diagram.

The RAU is the Resume procedure after the 2G-3G Inter-System Intra-SGSN Suspend procedure is completed. The SGSN sends a Create Session Request / Modify Bearer Request / Resume Notification to the SGW which subsequently is sent to PGW to resume all data transmissions on non-GBR bearers.

Figure 90: Intra-SGSN Inter-System Suspend and Resume Procedure



Inter-SGSN Inter-System Suspend and Resume Procedure

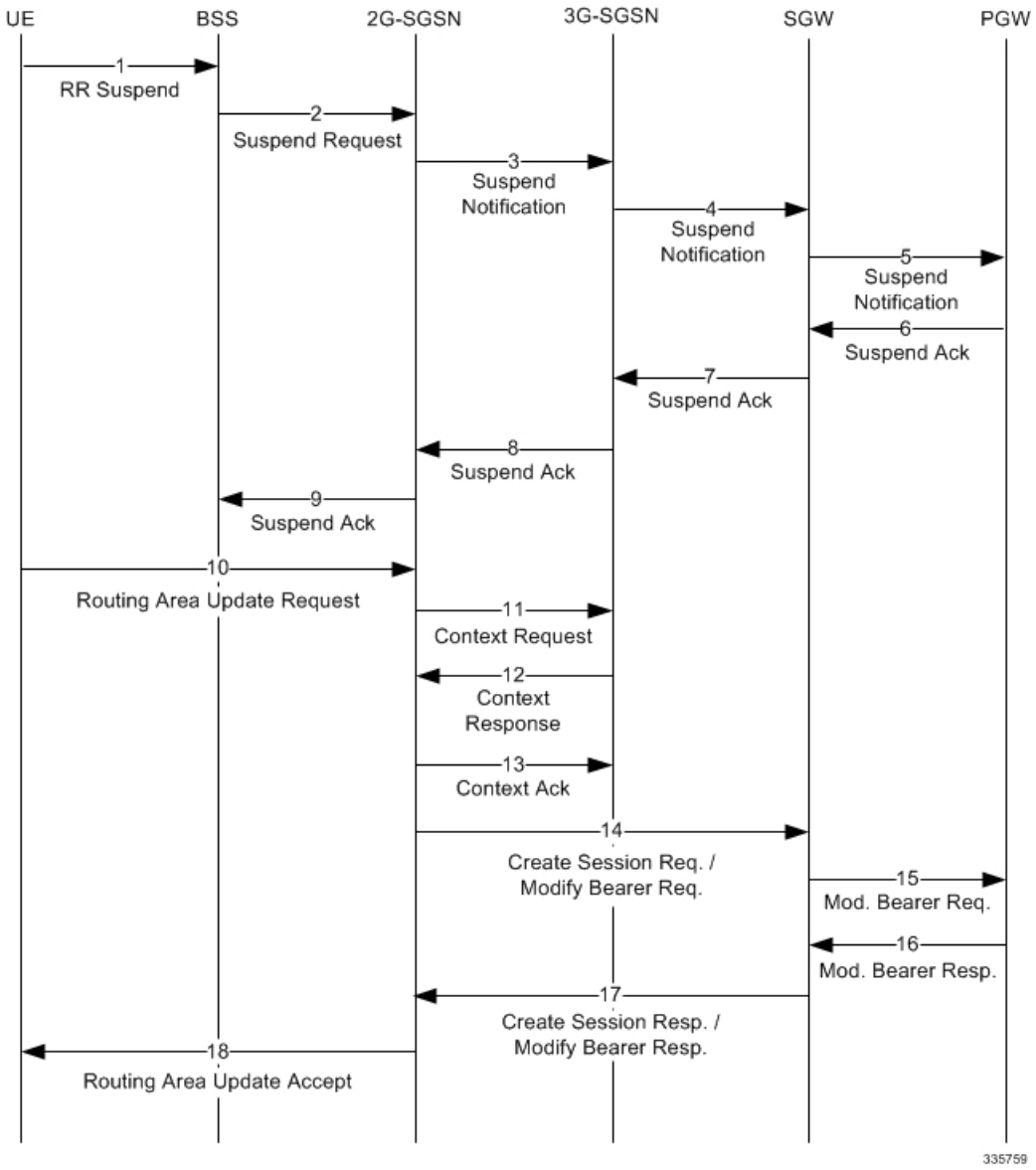
The inter-SGSN inter-system Suspend and Resume procedure is shown in the following illustration. This describes the scenario when the suspend message is received in an SGSN that is different from the SGSN currently handling the packet data transmission and would be valid for at least the following cases:

- MS performs inter-system handover from Iu mode to A/Gb mode during CS connection and the SGSN handling the A/Gb mode cell is different from the SGSN handling the Iu mode cell, (that is. the 2G and 3G SGSNs are separated).

The RAU is the Resume procedure after the 2G-3G Inter-System Inter-SGSN Suspend procedure has completed. The SGSN sends a Create Session Request / Modify Bearer Request to the SGW which subsequently is sent to PGW to resume all data transmissions on non-GBR bearers.

- If there is no SGW change for the RAU request, then the 2G-SGSN sends a Modify bearer request to the SGW. The SGW then sends a MBR all the way up to the PGW if the RAT type / Serving network changes. Otherwise it will send the Resume Request to the PGW to resume all data transmissions.
- If there is a SGW change for the RAU request, then the 2G-SGSN sends a Create Session Request to the SGW and the SGW sends a Modify Bearer Request to the PGW to resume all data transmissions.

Figure 91: Suspend and Resume Procedure for Inter-SGSN Inter-System Suspend and Resume



Standards Compliance

The Suspend/Resume feature on the S4-SGSN complies with the following standards:

- 3GPP TS 23.060 version 10.11.0 Release 10 - section 16.2.1 *3rd Generation Partnership Project Technical Specification Group Services and System Aspects General Packet Radio Service (GPRS) Service description Stage 2 (Release 10)*
- 3GPP TS 29.274 version 10.7.0 Release 10 - section 7.4 *3rd Generation Partnership Project Technical Specification Group Core Network and Terminals 3GPP Evolved Packet System (EPS) Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C) Stage 3 (Release 10)*
- 3GPP TS 23.272 version 10.11.0 Release 10 - section 6.7 (No PS HO Support) *3rd Generation Partnership Project Technical Specification Group Services and System Aspects Circuit Switched (CS) fallback in Evolved Packet System (EPS) Stage 2 (Release 10)*

Configuring the S4-SGSN Suspend/Resume Feature

No configuration is required to enable the S4-SGSN Suspend/Resume Feature.

Monitoring and Troubleshooting the S4-SGSN Suspend/Resume Feature

This section provides information on the show commands and bulk statistics available to support the Suspend/Resume feature.

S4-SGSN Suspend and Resume Feature Show Commands

This section provides information regarding show commands available in support of the S4-SGSN Suspend/Resume feature.

show subscriber gprs-only full all

If the state field in the output of this command reads Suspended, it indicates that a subscriber has been moved from the Ready state to the Suspended state in 2G. Once this state change occurs, operators can use the **show bssgp statistics** and s**how egtpc statistics** commands to view information on whether the Suspend procedure was successful or not.

```
Username: 123456789012345
Access Type: sgsn                                          Network Type: IP
Access Tech: GPRS GERAN
callid: 00004e25                                            msid: 262090426000193
state: Suspended
connect time: Mon Jun 17 02:27:40 2013    call duration: 00h00m14s
idle time: 00h00m14s
User Location (RAI): 26209-4369-19          Cell Global Identity: 3
IMEI(SV): n/a
```

If the state field in the output of this command reads Ready, it indicates that a subscriber has moved from the Suspended state to the Ready state in 2G. For example:

```
Username: 123456789012345
Access Type: sgsn                                          Network Type: IP
Access Tech: GPRS GERAN
callid: 00004e25                                            msid: 262090426000193
state: Ready
connect time: Mon Jun 17 02:27:40 2013    call duration: 00h00m14s
idle time: 00h00m14s
User Location (RAI): 26209-4369-19          Cell Global Identity: 3
IMEI(SV): n/a
```

show subscriber sgsn-only full all

If the state field in the output of this command reads Idle, it indicates that a subscriber has moved from the Connected state to the Idle state in 3G. For example:

```
Username: 123456789012345
Access Type: sgsn                                          Network Type: IP
Access Tech: GPRS GERAN
callid: 00004e25                                            msid: 262090426000193
state: Ready
connect time: Mon Jun 17 02:24:05 2013    call duration: 00h00m23s
idle time: 00h00m12s
User Location (RAI): 26209-4660-18          Service Area Code : 1202
Serving PLMN:          26209
IMEI(SV): n/a                                               Equipment Status
```

If the state field in the output of this command reads Idle, it indicates that a subscriber has moved from the Connected state to the Idle state in 3G. For example:

```
Username: 123456789012345
Access Type: sgsn                                          Network Type: IP
Access Tech: GPRS GERAN
callid: 00004e25                                            msid: 262090426000193
state: Connected
connect time: Mon Jun 17 02:24:05 2013    call duration: 00h00m23s
idle time: 00h00m12s
User Location (RAI): 26209-4660-18          Service Area Code : 1202
Serving PLMN:          26209
IMEI(SV): n/a                                               Equipment Status
```

show bssgp statistics verbose

The output of this command tracks the number of BSSGP messages (BSS Suspend procedure) transmitted and received at the SGSN. It does not track the number messages between the BSS and the peer S4-SGSN or peer MME. The **show egtpc statistics** command is used to track EGTPC messages transmitted and received between the SGSN and a peer S4-SGSN or peer MME. Operators can check number of suspend ack messages received to identify successful suspend procedures. The number of suspend nack messages indicate unsuccessful suspend procedures.

Table 32: show bssgp statistics verbose Command Output

suspend messages received:
Intra-Sgsn suspend message received:
Inter-Sgsn suspend message received:
Inter-System suspend message received:

suspend ack messages transmitted: Intra-Sgsn suspend ack message transmitted: Inter-Sgsn suspend ack message transmitted: Inter-System suspend ack message transmitted:
suspend nack messages transmitted: Intra-Sgsn suspend nack message transmitted: Inter-Sgsn suspend nack message transmitted: Inter-System suspend nack message transmitted:
resume messages received: resume ack messages transmitted: resume nack messages transmitted:

show egtpc statistics

The output of this command tracks the number of Suspend EGTPC messages transmitted and received from or to a peer SGSN/ MME or S-GW. The output also tracks the number of Resume EGTPC messages transmitted to S-GW.

Detailed descriptions of these counters are available in the *Statistics and Counters Reference*.

Table 33: show egtpc statistics Command Output for S4-SGSN Suspend/Resume Feature

CS Fallback Messages:
Suspend Notification:
Initial TX: Initial RX:
Retrans TX Discarded:
No Rsp RX:
Suspend Acknowledge:
Initial TX:
Initial RX:
Discarded:
Resume Notification
Initial TX:
Initial RX:
Retrans TX:
Discarded:
No Rsp RX
Resume Acknowledge:
Initial TX:
Initial RX:
Discarded:

show egtpc statistics verbose

The output of this command tracks the number of denied Suspend notification recived and transmitted procedures.

- Suspend Notification Denied TX means Suspend notification was denied due to any of errors listed in the table that follows.
- Suspend Notification Denied RX means a Suspend notification was received incorrectly from the peer S4-SGSN.

Detailed descriptions of these counters are available in the *Statistics and Counters Reference*.

Table 34: show egtpc statistics verbose Command Output for S4-SGSN Suspend/Resume Feature

Suspend Notification Denied		
Suspend Notification Denied TX		**Suspend Notification Denied RX**
Context not existent:		Context not existent:
Invalid message format:		Invalid message format:

Version not supported:		Version not supported:
Invalid length:		Invalid length:
Service not supported:		Service not supported:
Mandatory IE incorrect:		Mandatory IE incorrect:
Mandatory IE missing:		Mandatory IE missing:
System failure:		System failure:
No resources available:		No resources available:
Semantic error in TFT:		Semantic error in TFT:
Syntactic error in TFT:		Syntactic error in TFT:
Semantic error in Pkt Fltr:		Semantic error in Pkt Fltr:
Syntactic error in Pkt Fltr:		Syntactic error in Pkt Fltr:
Missing or unknown APN		Missing or unknown APN
GRE key not found:		GRE key not found:
Reallocation failure:		Reallocation failure:
Denied in RAT:		Denied in RAT:
Pref. PDN type unsupported:		Pref. PDN type unsupported:
All dynamic addr occupied:		All dynamic addr occupied:
UE ctx w/o TFT activated:		UE ctx w/o TFT activated:
Prot type not supported:		Prot type not supported:
UE not responding:		UE not responding:
UE refuses:		UE refuses:
Service denied:		Service denied:
Unable to page UE:		Unable to page UE:
No Memory:		No Memory:
User Auth Failed:		User Auth Failed:
Apn Access Denied:		Apn Access Denied:
Request Rejected:		Request Rejected:
Semantic error in TAD:		Semantic error in TAD:
Syntactic error in TAD:		Syntactic error in TAD:

Collision with Nw init Req:		Collision with Nw init Req:
UE page unable due to Susp:		UE page unable due to Susp:
Conditional IE missing:		Conditional IE missing:
Apn Restr Type Incompatible:		Apn Restr Type Incompatible:
Invalid len Piggybacked msg:		Invalid len Piggybacked msg:
Invalid remote Peer reply:		Invalid remote Peer reply:
PTMSI signature mismatch:		PTMSI signature mismatch:
IMSI not Known:		IMSI not Known:
Peer not responding:		Peer not responding:
Data Fwding not supported:		Data Fwding not supported:
Fallback to GTPV1:		Fallback to GTPV1:
Invalid Peer:		Invalid Peer:
Temp Rej due to HO in prog:		Temp Rej due to HO in prog:
Unknown:		Unknown:
Resume Notification Denied		
Resume Notification Denied TX		**Resume Notification Denied RX**
Context not existent:		Context not existent:
Invalid message format:		Invalid message format:
Version not supported:		Version not supported:
Invalid length:		Invalid length:
Service not supported:		Service not supported:
Mandatory IE incorrect:		Mandatory IE incorrect:
Mandatory IE missing:		Mandatory IE missing:
System failure:		System failure:
No resources available:		No resources available:
Semantic error in TFT:		Semantic error in TFT:
Syntactic error in TFT:		Syntactic error in TFT:
Semantic error in Pkt Fltr:		Semantic error in Pkt Fltr:
Syntactic error in Pkt Fltr:		Syntactic error in Pkt Fltr:

Missing or unknown APN		Missing or unknown APN
GRE key not found:		GRE key not found:
Reallocation failure:		Reallocation failure:
Denied in RAT:		Denied in RAT:
Pref. PDN type unsupported:		Pref. PDN type unsupported:
All dynamic addr occupied:		All dynamic addr occupied:
UE ctx w/o TFT activated:		UE ctx w/o TFT activated:
Prot type not supported:		Prot type not supported:
UE not responding:		UE not responding:
UE refuses:		UE refuses:
Service denied:		Service denied:
Unable to page UE:		Unable to page UE:
No Memory:		No Memory:
User Auth Failed:		User Auth Failed:
Apn Access Denied:		Apn Access Denied:
Request Rejected:		Request Rejected:
Semantic error in TAD:		Semantic error in TAD:
Syntactic error in TAD:		Syntactic error in TAD:
Collision with Nw init Req:		Collision with Nw init Req:
UE page unable due to Susp:		UE page unable due to Susp:
Conditional IE missing:		Conditional IE missing:
Apn Restr Type Incompatible:		Apn Restr Type Incompatible:
Invalid len Piggybacked msg:		Invalid len Piggybacked msg:
Invalid remote Peer reply:		Invalid remote Peer reply:
PTMSI signature mismatch:		PTMSI signature mismatch:
IMSI not Known:		IMSI not Known:
Peer not responding:		Peer not responding:
Data Fwding not supported:		Data Fwding not supported:
Fallback to GTPV1:		Fallback to GTPV1:

Invalid Peer:		Invalid Peer:
Temp Rej due to HO in prog:		Temp Rej due to HO in prog:
Unknown:		Unknown:

show sgtpc statistics verbose

The output of this comnand tracks the number of SGSN Context Request transmitted and received message transmitted from the peer Gn-SGSN. It also tracks the number of SGSN Context Response messages transmitted and received from a peer Gn-SGSN.

Table 35: show sgtpc statistics Command Output for S4-SGSN Suspend/Resume Feature

SGSN Context Request:	
Total SGSN-Ctx-Req TX:	Total SGSN-Ctx-Req RX:
Initial SGSN-Ctx-Req TX:	Initial SGSN-Ctx-Req RX:
SGSN-Ctx-Req-TX(V1):	SGSN-Ctx-Req-RX(V1):
Suspend-Req-Hdr-TX:	Suspend-Req-Hdr-RX:
SGSN-Ctx-Req-TX(V0):	SGSN-Ctx-Req-RX(V0):
Retrans SGSN-Ctx-Req TX:	Retrans SGSN-Ctx-Req RX:
Ret-SGSN-Ctx-Req-TX(V1):	Ret-SGSN-Ctx-Req-RX(V1):
Ret-Suspend-Req-Header-TX:	
Ret-SGSN-Ctx-Req-TX(V0):	Ret-SGSN-Ctx-Req-RX(V0):
SGSN Context Response:	
Total SGSN-Ctx-Rsp TX:	Total SGSN-Ctx-Rsp RX:
Denied TX:	Denied RX:
Suspend-Rsp-Hdr-TX:	Suspend-Rsp-Hdr-Rx:
Accepted TX:	Accepted RX:
Initial SGSN-Ctx-Rsp TX:	Initial SGSN-Ctx-Rsp RX:
SGSN-Ctx-Rsp-TX(V1):	SGSN-Ctx-Rsp-RX(V1):
Suspend-Rsp-Hdr-TX:	Suspend-Rsp-Hdr-RX:
SGSN-Ctx-Rsp-TX(V0):	SGSN-Ctx-Rsp-RX(V0):
Retrans SGSN-Ctx-Rsp TX:	Retrans SGSN-Ctx-Rsp RX:
Ret-SGSN-Ctx-Rsp-TX(V1):	Ret-SGSN-Ctx-Rsp-RX(V1):

Ret-SGSN-Ctx-Rsp-TX(V0):	Ret-SGSN-Ctx-Rsp-RX(V0):
	Decode Failure RX:

S4-SGSN Suspend and Resume Feature Bulk Statistics

The following statistics are included in various bulk statistics schema in support of the Suspend/Resume feature:

- **SGSN Schema**:
  - 2G-attach-fail-suspend-received
  - 2G-attach-fail-comb-suspend-received

For descriptions of these variables, see the *SGSN Schema Statistics* section in the *Statistics and Counters Reference*.

- **GPRS Schema**
  - bssgp-suspend-msg-rcvd
  - bssgp-suspend-ack-msg-sent
  - bssgp-suspend-nack-msg-sent
  - bssgp-resume-msg-rcvd
  - bssgp-resume-ack-msg-sent
  - bssgp-resume-nack-msg-sent

For descriptions of these variables, see *GPRS Schema Statistics* in the *Statistics and Counters Reference*.

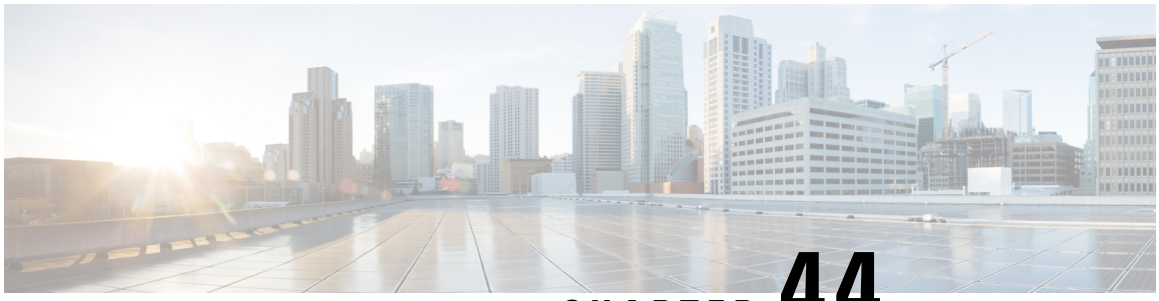
- **EGTPC Schema**:
  - csfb-sent-suspendnotf
  - csfb-sent-retranssuspendnotf
  - csfb-recv-suspendnotf
  - csfb-recv-suspendnotfDiscard
  - csfb-recv-suspendnotfNorsp
  - csfb-recv-retranssuspendnotf
  - csfb-sent-suspendack
  - csfb-sent-suspendackaccept
  - csfb-sent-suspendackdenied
  - csfb-recv-suspendack
  - csfb-recv-suspendackDiscard
  - csfb-recv-suspendackaccept
  - csfb-recv-suspenddenied
  - csfb-sent-resumenotf
  - csfb-sent-retransresumenotf
  - csfb-sent-resumeack
  - csfb-sent-resumeackaccept
  - csfb-sent-resumeackdenied
  - csfb-recv-resumeack
  - csfb-recv-resumeackDiscard

- csfb-recv-resumeackaccept
- csfb-recv-resumedenied

For descriptions of these variables, see *EGTPC Schema Statistics* in the *Statistics and Counters Reference*.

- **SGTP Schema**:
  - sgtpc-sgsn-ctxt-req-v1-tx
  - sgtpc-sgsn-ctxt-req-v1-rx
  - sgtpc-sgsn-ctxt-req-accept-tx
  - sgtpc-sgsn-ctxt-req-accept-rx
  - sgtpc-sgsn-ctxt-req-accept-v1-tx
  - sgtpc-sgsn-ctxt-req-accept-v1-rx
  - sgtpc-sgsn-ctxt-req-denied-tx
  - sgtpc-sgsn-ctxt-req-denied-rx
  - sgtpc-sgsn-ctxt-ack-accept-tx
  - sgtpc-sgsn-ctxt-ack-accept-rx
  - sgtpc-sgsn-ctxt-ack-accept-v1-tx
  - sgtpc-sgsn-ctxt-ack-accept-v1_rx
  - sgtpc-sgsn-ctxt-ack-denied-tx

For descriptions of these variables, see *SGTP Schema Statistics* in the *Statistics and Counters Reference*.



CHAPTER 44

SGSN Clear Subscriber Enhancement

- Feature Summary and Revision History, on page 491
- Feature Description, on page 492
- Configuring Clear Subscriber, on page 492

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Configuration Required
Related Changes in This Release	Not applicable
Related Documentation	• *Command Line Interface Reference* • *SGSN Administration Guide*

Revision History

Revision Details	Release
First introduced.	21.14

Feature Description

New keyword ‘sgsn-only’ and ‘gprs-only’ keywords introduced under-existing "clear subscribers" to clear 3g and 2g subscriber, ‘lai’ CLI added under sgsn-only/gprs-only reads the location area identity parameters which are “mcc, mnc and lac.” These parameters are passed on to the existing ‘clear subscribers’ framework. The existing framework handles the new location parameters and finds the matching subscribers and all the matching subscribers (both 2g and 3g subscribers) are cleared.

Configuring Clear Subscriber

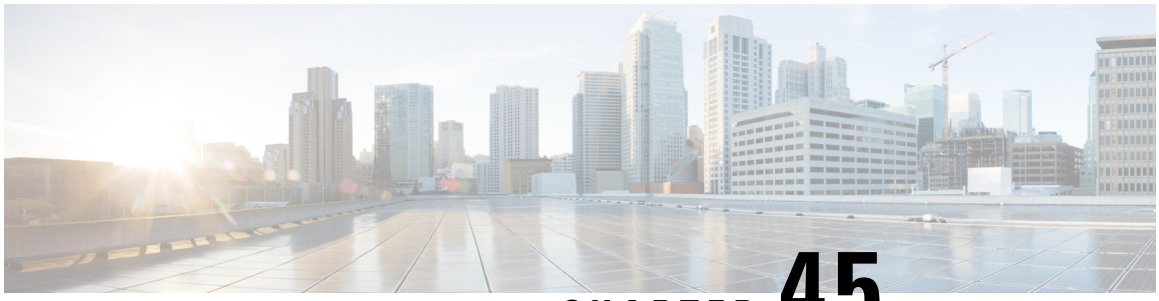
Clear Subscribers Enhancement

Below key words are introduced to clear subscriber.

clear subscribers { gprs-only | sgsn-only }lai mcc *mobile_country_code* **mnc** *mobile_network_code* **lac** *location_area_code*
end

Notes:

- **gprs-only**: Specifies the clearing of SGSN 2G subscribers only.
- **sgsn-only**: Specifies the clearing of SGSN 3G subscribers only.
- **lai**: Specifies location area identity.
- **mcc** *mobile_country_code*: Specifies mobile country code. *mobile_country_code* must be a string of size 3 to 3 ranging from 100 through 999.
- **mnc** *mobile_network_code*: Specifies mobile network code.*mobile_network_code* must be a string of size 2 to 3 ranging from 00 through 999.
- **lac** *location_area_code*: Specifies location area code. *location_area_code* must be an integer from 1 to 65535.



CHAPTER 45

SGSN-MME Combo Optimization

This section describes Combo Optimization available for a co-located SGSN-MME node. It also provides detailed information on the following:

- Feature Description, on page 493
- How It Works, on page 494
- Configuring the Combo Optimization, on page 497
- Monitoring and Troubleshooting Combo Optimization , on page 498

Feature Description

The SGSN and MME can be enabled simultaneously in the same chassis and, though co-located, they each behave as independent nodes. This Combo Optimization feature enables the co-located SGSN and MME to co-operate with each other in order to achieve lower memory and CPU utilizations and to reduce signaling towards other nodes in the network. When functioning as mutually-aware co-located nodes, the SGSN and the MME can share UE subscription data between them.

Important This feature is supported by both the S4-SGSN and the Gn-SGSN. For the feature to apply to a Gn-SGSN, the Gn-SGSN must be configured to connect to an HSS. Combo Optimization for an SGSN-MME node is a licensed Cisco feature. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys section of the Software Management Operations chapter in the System Administration Guide*.

Overview

The load on S6d/S6a interfaces towards an HSS is reduced effectively by utilizing the resources in a co-located SGSN-MME node scenario. Requests for subscription data in Update Location Request (ULR) are skipped by setting the 'skip-subscriber-data' bit in the ULR flags this, in turn, reduces the load on the HSS. The Skip Subscriber Data AVP is used and the subscriber data is shared across the SGSN and the MME services.

As per 3GPP TS 29.272, setting the 'skip-subscriber-data' bit in the ULR indicates that the HSS may skip sending subscription data in Update Location Answer (ULA) to reduce signaling. If the subscription data has changed in the HSS after the last successful update of the MME/SGSN, the HSS ignores this bit and sends the updated subscription data. If the HSS skips sending the subscription data, then the GPRS-Subscription-Data-Indicator flag can be ignored.

Important The SGSN supported the Skip-Subscription-Data bit prior to Release 18.0. Support for this functionality was added to the MME in Release 18.0.

Ensuring that packets are routed internally reduces network latency for S3/Gn interface messages. This is achieved by configuring the SGTP and EGTP services in the same context for the SGSN and the MME configurations.

For outbound Inter-RAT SRNS Relocations, the MME gives preference to the co-located SGSN, irrespective of the order/priority or preference/weight configured for the SGSN entry in DNS Server. When Inter-RAT handovers take place between the co-located MME and the SGSN, the new call arrives at the same Session Manager that hosted the call in the previous RAT. If the subscription data is available for a given UE at the co-located SGSN, then the MME does not need to request this data from the HSS and provides UE subscription data obtained from the SGSN. This optional function can be turned on or off through the MME Service configuration.

Combo Optimization is available for subscribers with an EPC-enabled UE and an EPC subscription configured at the HSS. During handoff from 4G to 3G or 4G to 2G, the EPC subscription will be copied from the MME. Combo Optimization is also applicable for Non-EPC subscribers if core-network-interface is selected as S4 for the EPS-subscription.

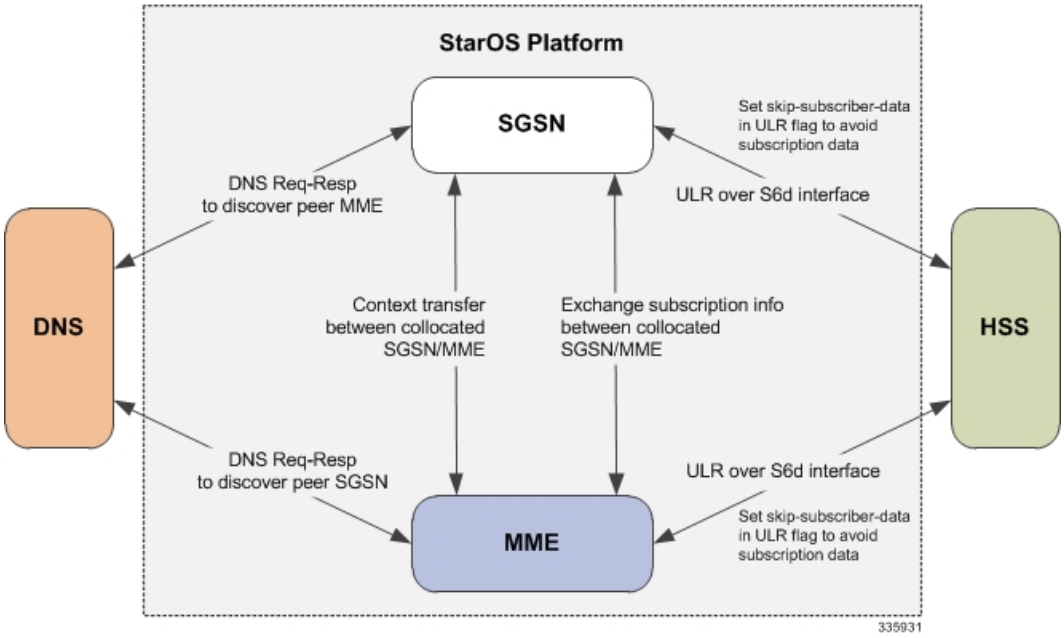
How It Works

Subscriber Movement from MME to SGSN: Subscription information is first fetched by the MME. On subscriber movement to a co-located SGSN, the SGSN sends a ULR with "skip-subscriber-data" flag set and the HSS sends a ULA (with or without subscription data depending on time of MME update).

Subscriber Movement from SGSN to MME: Subscription information is first fetched by the SGSN. On subscriber movement to a co-located MME, the MME sends a ULR with "skip-subscriber-data" flag set and the HSS sends a ULA (with or without subscription data depending on time of SGSN update).

Architecture

Figure 92: SGSN-MME Combo Node



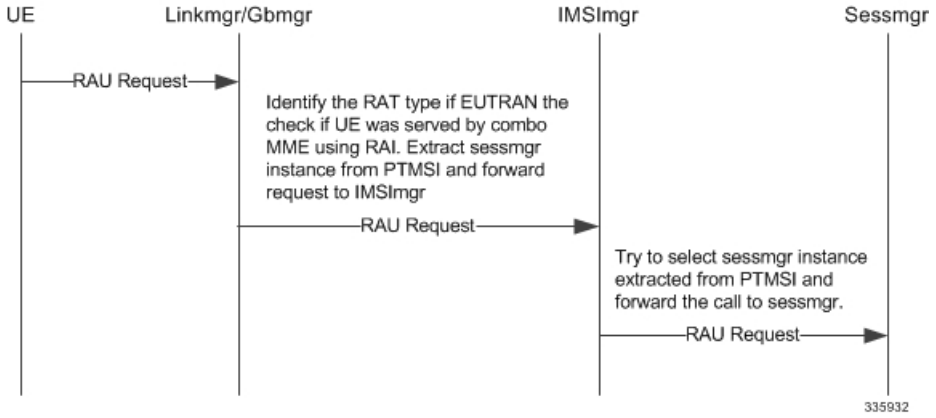
The above diagram displays the interworking of various modules when the Combo Optimization feature is enabled in a co-located SGSN-MME setup.

When the subscriber does RAU from MME to SGSN, or vice versa, a DNS query is initiated to fetch the address of the peer node. Based on the IP address obtained, the peer MME or SGSN is selected. When a DNS response is received with a list of peer SGSN addresses, the MME matches the configured EGTP/SGTP SGSN service address in the system and uses it for the S3/Gn UE Context Transfer procedures. If a DNS response is not received and a locally configured EGTP/SGTP SGSN service is present as a peer-SGSN, the peer-SGSN will be selected. Context transfer and copying of subscription information happens internally between the SGSN and the MME nodes. The SGSN maintains the s6d interface towards the HSS and the MME maintains the S6a interface towards the HSS. All network-initiated messages are sent separately towards the SGSN and the MME nodes respectively.

Flows

This section includes various diagrams that illustrate the session manager (SessMgr) selection logic during RAU, SRNS, and Attach procedures:

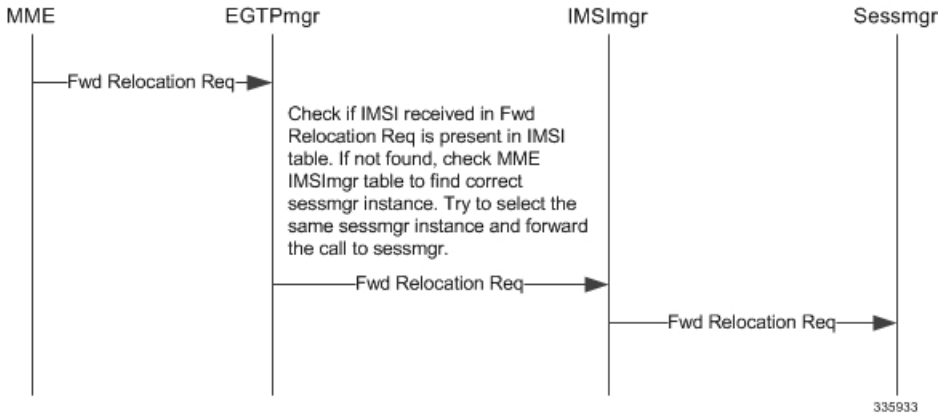
Figure 93: Selection of SessMgr Instance during RAU from MME to SGSN



Listed below is the SessMgr instance selection logic during a RAU procedure from the MME to SGSN:

1. A RAU request from UE is forwarded to the LinkMgr or GbMgr.
2. The LinkMgr identifies if the RAU is local and extracts the SessMgr instance from the PTMSI and forwards the request to IMSIMgr.
3. The IMSIMgr tries to select the SessMgr instance extracted from the PTMSI and forwards the request to the selected SessMgr.

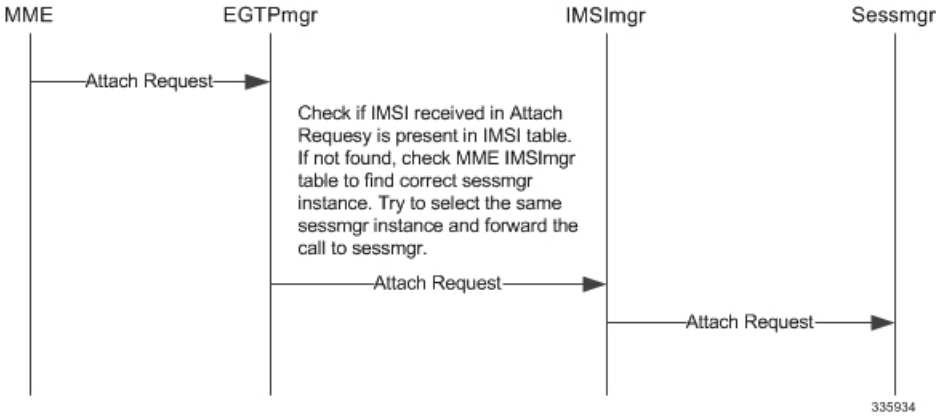
Figure 94: Selection of SessMgr Instance during SRNS



Listed below is the SessMgr instance selection logic during an SRNS procedure:

1. During an SRNS procedure, the MME service sends a Forward Relocation Request to the EGTPCMgr.
2. The EGTPCMgr forwards the request to the IMSIMgr.
3. The IMSIMgr uses the IMSI received in the request message to identify the SessMgr instance and forwards the request to the appropriate SessMgr instance.

Figure 95: Selection of SessMgr Instance during Attach



Listed below is the SessMgr instance selection logic during an Attach procedure:

1. During Attach procedure, the LinkMgr/GbMgr forwards the request to the IMSIMgr.
2. The IMSIMgr first verifies if the IMSI is present in the SGSN's IMSI table. If it is not present, the MME's IMSI table is verified. Once the entry is found the request is forwarded to the appropriate SessMgr.
3. If the entry is not found in either table, then an alternate SessMgr instance is used to process the call.

Limitations

Subscription information is shared between MME and SGSN only when both are connected to an HSS. Combo Optimization is not be applicable if either the MME or the SGSN is connected to an HLR. Though the subscription information is shared between the SGSN and MME services, a separate HSS service and diameter endpoint will be maintained for both the SGSN and the MME. All network-initiated messages are received separately for both the MME and the SGSN. Subscription data is copied based on time-stamp validation.

A small impact on the performance is observed during Inter-RAT handoffs as subscription data is exchanged between the SGSN and the MME. This impact is a limited increase in the number of instructions per handoff per UE depending on the number of APNs configured for the UE in the HSS.

It is necessary that the HSS honors the request from the MME/SGSN and not send subscription data when 'Skip-Subscriber-Data' flag is set in the ULR. However, there are some known and valid cases where the HSS ignores this flag for example, if the UE's subscription data changed since the last time the UE attached in 4G. (Typically, UE subscription data does not change frequently, therefore, HSS overrides are less frequent.)

Configuring the Combo Optimization

This section describes how to configure the Combo Optimization for an SGSN-MME combo node.

By default, Combo Optimization is not enabled. This command both enables or disables Combo Optimization on an SGSN-MME combo node.

```
config
      lte-policy
            [ no ] sgsn-mme subscriber-data-optimization
            end
```

Note:

- **no** as a command prefix disables Combo Optimization.

The following CLI (applicable only to the SGSN in the combo node), under the call-control profile configuration mode, controls requests for GPRS subscription information from the HSS:

```
config
   call-control-profile profile_name
      hss message update-location-request gprs-subscription-indicator [
never | non- epc-ue ]
      end
```

Verifying Combo Optimization Configuration

Execute the following command to verify the configuration of this feature.

show lte-policy sgsn-mme summary

The following field value indicates if data optimization on the SGSN-MME combo node is "Enabled" or "Disabled":

- subscriber-data-optimization

Monitoring and Troubleshooting Combo Optimization

This section provides information on the show commands and bulk statistics available to monitor and troubleshoot Combo Optimization for the SGSN-MME combo node, and for each element separately.

Monitoring Commands for the SGSN-MME Combo Node

This section provides information regarding show commands and/or their outputs in support of the Combo Optimization feature on the SGSN-MME Combo Node:

show hss-peer-service statistics all

The following new fields are added to the show output to display the subscription data statistics:

- Subscription-Data Stats
- Skip Subscription Data
- Subscription-Data Not Received

The Skip Subscription Data statistic is incremented when the ULR is sent with the skip-subscription-data flag set. The Subscription-Data Not Received statistic is incremented if the HSS does not send the subscription data in the ULA when skip-subscription-data flag is set in ULR. The difference between the Skip Subscription Data and Subscription-Data Not Received gives us the number of times HSS does not honor the skip-subscription-data flag.

Monitoring Commands for the SGSN

This section provides information regarding show commands and/or their outputs in support of the Combo Optimization feature on the **SGSN**:

show demux-mgr statistics imsimgr all sgsn

The following new fields are added in the show output to display the number of RAU, Attach, PTIMSI attach and Forward relocation requests arriving from a subscriber attached with co-located MME:

- IMSI attach with context in co-located MME
- P-TMSI attach with mapped P-TMSI of co-located MME
- RAU with mapped P-TMSI of co-located MME
- Fwd reloc request from co-located MME

show subscribers sgsn-only summary

The following new field is added in the show output to display the number of subscribers currently sharing subscription information with the MME:

- Total HSS subscribers sharing subscription-info

show subscribers gprs-only summary

The following new field is added in the show output to display the number of subscribers currently sharing subscription information with MME:

- Total HSS subscribers sharing subscription-info

show subscribers sgsn-only full all

The STN-SR , ICS-indicator , Trace-Data and CSG subscription information is now displayed under the **show subscribers sgsn-only full all** output. These AVPs are currently used by MME only .Values are displayed as received from HSS without any format changes.

- Trace Data
- Trace Reference
- Trace Depth
- Trace NE Type List
- Trace Interface List
- Trace Event List
- OMC Id
- Trace Collection Entity
- STN-SR
- ICS-Indicator
- CSG Subscription
- CSG ID
- Expiration Date

show subscribers gprs-only full all

The STN-SR, ICS-indicator, Trace-Data and CSG subscription information is now displayed under the **show subscribers gprs-only full all** output. These AVPs are currently used only by the MME. Values are displayed as received from HSS without any format changes.

- Trace Data
- Trace Reference
- Trace Depth
- Trace NE Type List
- Trace Interface List
- Trace Event List
- OMC Id
- Trace Collection Entity
- STN-SR
- ICS-Indicator
- CSG Subscription
- CSG ID
- Expiration Date

show session subsystem facility aaamgr instance

The following new fields are added in the show output to display the total number of CSG subscription records and Trace data records:

- SGSN: Total Trace data records
- SGSN: Total CSG data records

Monitoring Commands for the MME

This section provides information regarding show commands and/or their outputs in support of the Combo Optimization feature on the **MME**:

show mme-service statistics handover

The following new statistics are added to the show output to display the information about Inter-RAT Optimized Handoffs between the co-located SGSN and MME:

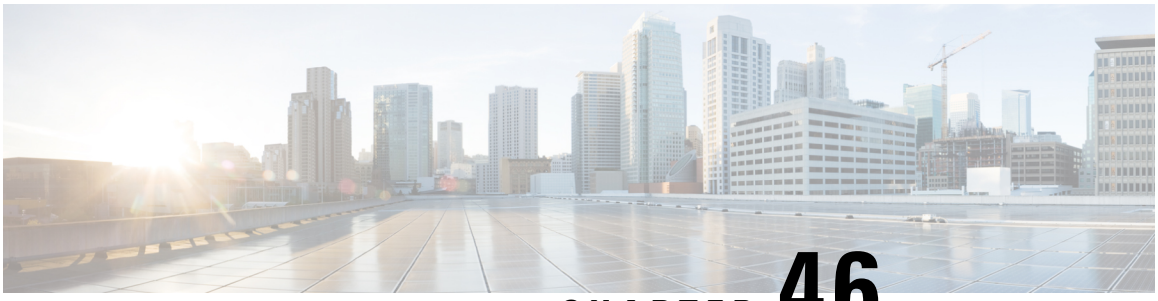
- Inter-RAT Optimized Handoffs Between Co-located MME and SGSN
- Outbound MME to SGSN RAU procedure
- Attempted
- Success
- Failures
- Inbound SGSN to MME TAU procedure
- Attempted
- Success
- Failures
- Outbound MME to SGSN Connected Mode Handover
- Attempted
- Success

- Failures
- Inbound SGSN to MME Connected Mode Handover
- Attempted
- Success
- Failures

Bulk Statistics for Monitoring the MME in an SGSN-MME Combo Node

The following bulk statistics in the MME schema facilitate tracking MME optimization functionality for the SGSN-MME nodes when co-located in the same chassis with the Combo Optimization functionality enabled:

- optimized-out-rau-ho-4gto2g3g-attempted
- optimized-out-rau-ho-4gto2g3g-success
- optimized-out-rau-ho-4gto2g3g-failures
- optimized-in-tau-ho-2g3gto4g-attempted
- optimized-in-tau-ho-2g3gto4g-success
- optimized-in-tau-ho-2g3gto4g-failures
- optimized-out-s1-ho-4gto2g3g-attempted
- optimized-out-s1-ho-4gto2g3g-success
- optimized-out-s1-ho-4gto2g3g-failures
- optimized-in-s1-ho-2g3gto4g-attempted
- optimized-in-s1-ho-2g3gto4g-success
- optimized-in-s1-ho-2g3gto4g-failures



CHAPTER 46

SGSN Pooling

This chapter describes the SGSN Pooling feature.

- Feature Description, on page 503
- How it Works, on page 505
- Configuring the SGSN Pooling feature, on page 512
- Monitoring and Troubleshooting the SGSN Pooling feature, on page 514

Feature Description

An SGSN pool is a collection of SGSNs configured to serve a common geographical area for a radio network. This common part is referred to as the SGSN pool service. SGSN Pooling is also referred to as Iu/Gb flex support based on if the access is 3G or GPRS respectively.

An SGSN pool provides a flexible and resource-efficient architecture with built-in network redundancy for the GPRS/UMTS packet core network. Each BSC/RNC has the ability to connect to all SGSNs in the pool. If any SGSN becomes unavailable, any terminal attached to that SGSN will be automatically re-routed to another SGSN in the pool by the BSC/RNC. This implies that the SGSN pool provides network level redundancy. SGSN failure is discovered by the BSCs/RNCs and the uplink traffic from the terminal is routed to another SGSN in the pool. The substituting SGSN orders the terminal to re-attach and re-activate any PDP contexts. Therefore service availability is maintained. Please note that all SGSNs in a pool are required to have the same capacity, feature sets and scalability and hence the same vendor, failing which might lead to varying subscriber experience across SGSNs.

In a pooled network, Inter-SGSN routing area updates (RAUs) are avoided and this provides a faster response time, compared to non-pooled networks. With SGSN pool for GPRS/UMTS, Inter-SGSN RAU is replaced by Intra-SGSN RAU, for terminals moving within the pool area. Intra-SGSN RAU provides reduced interruption time for data transfer, compared to Inter-SGSN RAU. Furthermore, due to the fewer Inter-SGSN RAUs, there is less signaling generated on the Gr interface.

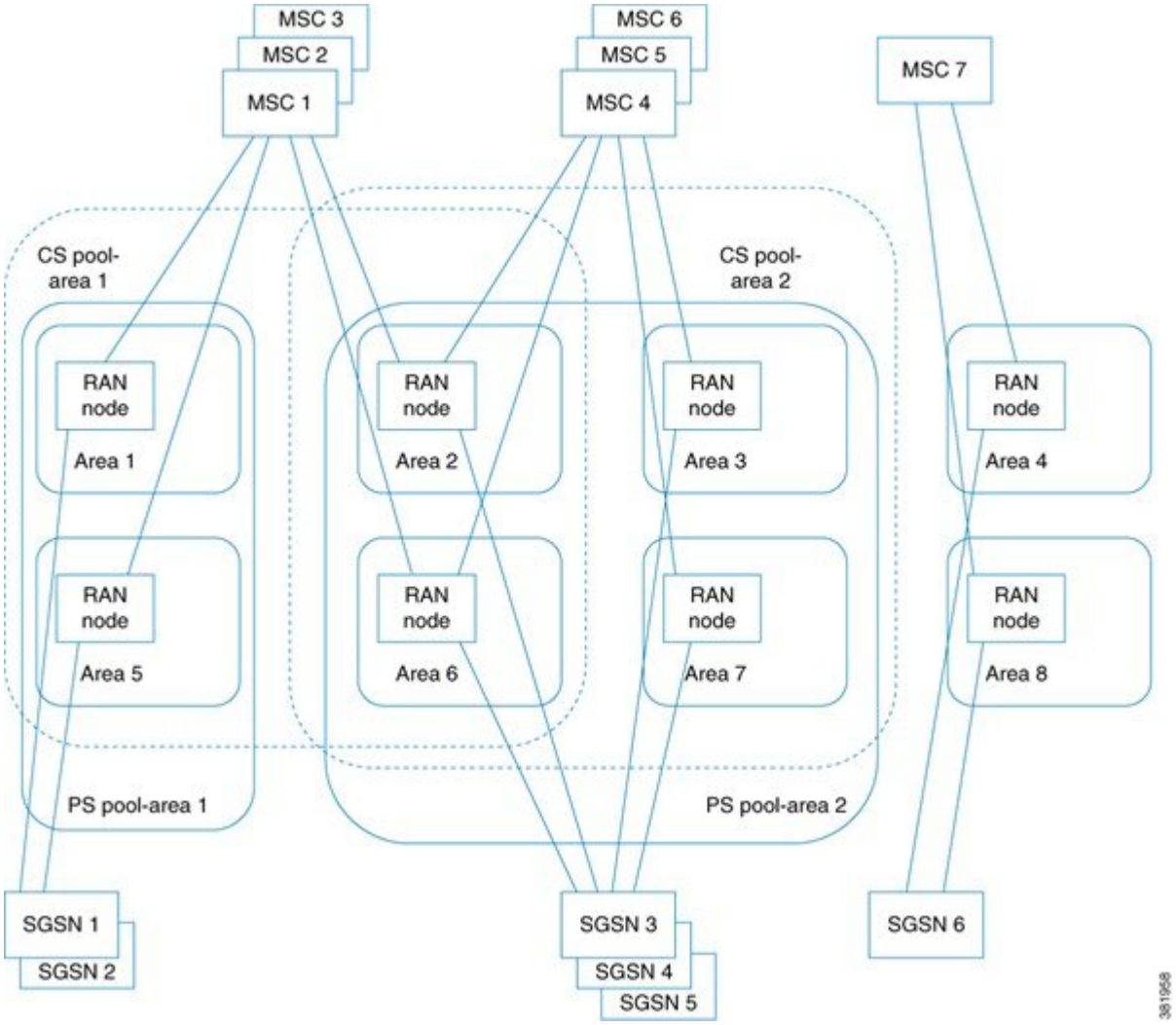
When an UE connects to an SGSN in the pool, by Attach or Inter-SGSN RAU (ISRAU) procedures, the UE is allocated a Packet Temporary Mobile Subscriber Identity (P-TMSI) containing a Network Resource Identifier (NRI) identifying the SGSN. The BSC/RNC then identifies the SGSN from the NRI, and routes the user data to the correct SGSN. Load-sharing between the SGSN pool members is thus based on the NRI routing algorithm in the BSC/RNC. UEs that have not yet been assigned a P-TMSI, and MSs without matching NRI, are distributed among the pool members by the BSC/RNC according to the traffic distribution procedure. Once a UE has been allocated a P-TMSI, it stays connected to the same SGSN as long as it remains in the pool area. This period can be quite long, since MSs normally keep the P-TMSI even after power off.

A valid license key is required to enable the SGSN Pooling feature. Contact your Cisco Account or Support representative for information on how to obtain a license.

A Basic Pool Structure

A basic SGSN pool structure is depicted in the diagram below:

Figure 96: A basic pool structure



- Multiple SGSNs form a single logical entity called SGSN pool.
- SGSN pools service areas larger than stand-alone SGSN service areas.
- This set up is compatible with non-pool aware nodes and is transparent to the end-user.

Benefits of SGSN Pooling

1. **Increased Availability:** If one SGSN fails, another SGSN from the pool can substitute it. Any node can be taken out of a pool during maintenance.

2. **Increased Scalability:** More number of SGSN nodes can be added to the pool.
3. **Reduced Signaling:** Number of inter-SGSN routing area updates is reduced.

Pooling Requirements

Listed below are the requirements to support pooling:

1. The SGSN should support configuration of NRI and use that NRI in all the PTMSI issued.
2. If the SGSN is configured as a default SGSN, it should relay SGSN Context Request / Identification request received from peer SGSN (outside of pool) to SGSN (in pool) anchoring that subscriber anchoring SGSN in pool.
3. Support of non-broadcast RAI, null-NRI configurations to allow off-loading of self-SGSN and handle the off-loading of a peer SGSN.

How it Works

P-TMSI - NRI and Coding

Every SGSN is configured with one or several NRIs (O&M). One of these NRIs is part of every Packet temporary Mobile Subscriber identity (P-TMSI) which the SGSN assigns to an UE for connecting via pooled BSC/RNC. For non-pooled BSC/RNC SGSN sets all NRI bits to "0". The P-TMSI allocation mechanism in the SGSN generates P-TMSIs which contain one of the configured NRIs in the relevant bit positions. A NRI has a flexible length up to "6" bits). The maximum number of SGSNs in a pool is limited to "63" (One NRI value reserved for NULL-NRI).

P TMSI is of length "32" bits, where the two top most bits are reserved and always set to "11". The NRI field is included at the beginning of P TMSI starting at bit "23" and down up to bit "18". The most significant bit of the NRI is located at bit "23" of the P TMSI regardless of the configured length of the NRI

Once a subscriber attaches to a new SGSN, a new P-TMSI is allocated by the P-TMSI re-allocation procedure. That P-TMSI contains the NRI of the SGSN. This is also the case when an Inter-SGSN RA update or an Inter-System Change (IRAT) occurs.

Non-Broadcast LAC and RAC

The LAC and RAC information is made available by off-loading the SGSN to the UE in the GMM_ATTCH_ACCEPT/GMM_RAU_ACCEPT message along with the NULL-NRI in the P-TMSI. This value is different from the LAC and RAC that an UE receives from BSS/UTRAN as broadcast information. These parameters are set unique per SGSN node.

SGSN Address Resolution

The following kinds of SGSN address resolution can be identified:

1. Address resolution with NRI.
2. Address resolution without NRI.

Address Resolution with NRI

A NRI based look-up occurs in the following scenarios:

1. An Inter-SGSN RAU occurs within a pooled area. This could be due to one of the SGSNs offloading the subscribers or due to a Gb/ Iu link failure on one of the SGSNs.
2. An Inter-SGSN RAU occurs from a pooled to a non-pooled SGSN. The GTP_SGSN_CONTEXT_REQUEST is routed to the default SGSN in the pool. The default SGSN looks up for the Gn address of the member in the pool based on the NRI retrieved from the P-TMSI in the GTP_SGSN_CONTEXT_REQUEST message received. A local configuration of these entries has to be present in the SGSN Operator Policy.
3. When offloading is enabled, the nb-rai and null-nri of the SGSN which is being offloaded should be configured in the cc-profiles of other SGSN's in the pool. Unless a entry is present, a periodic RAU will not be accepted in the other SGSN's carrying that nb-rai and null-nri.A local configuration of these entries has to be present in the SGSN Operator Policy.

Address resolution without NRI

Address resolution without NRI is used for Inter-SGSN RAU between non-pooled areas or between multiple pools. In this case the SGSN context request is routes towards the default SGSN, which in turn relays the GTP message to the right SGSN based on the NRI value in the P-TMSI.

Refer to the configuration section for the procedure to "Configure an Operator Policy".

Mobility Inside the Pool

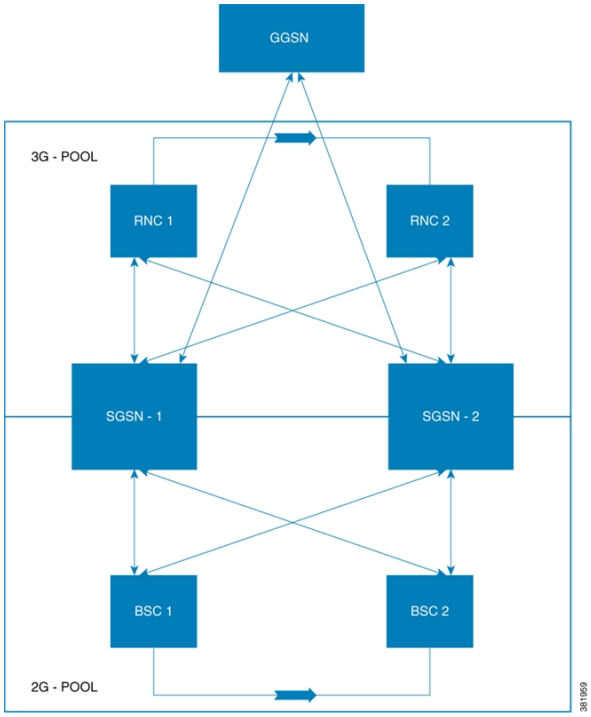
The distribution of UEs in a pool is handled by the BSCs/RNCs.

1. The UE sends an Attach Request or a RA Update Request to a SGSN.
2. This request passes through the BSC/RNC.
3. The BSC/RNC uses the NRI to locate the SGSN.
4. Once the SGSN is located Gb/Iu connection is set up.

If the NRI from the UE is invalid or does not match any of the NRIs of the pool members, the request is directed to one of the pool members by the BSC/RNC. International Mobile Subscriber Identity (IMSI) attaches are also distributed among the SGSN pool members by the BSCs.

Once a P-TMSI containing the NRI of a pool member has been assigned to an UE, the UE stays attached to that pool member as long as it remains in that pool service area. The frequency of inter-SGSN RA updates decreases, as the UE can move over a greater geographical area for one SGSN.

Figure 97: Mobility inside the pool



Consider the scenario depicted in the diagram above:

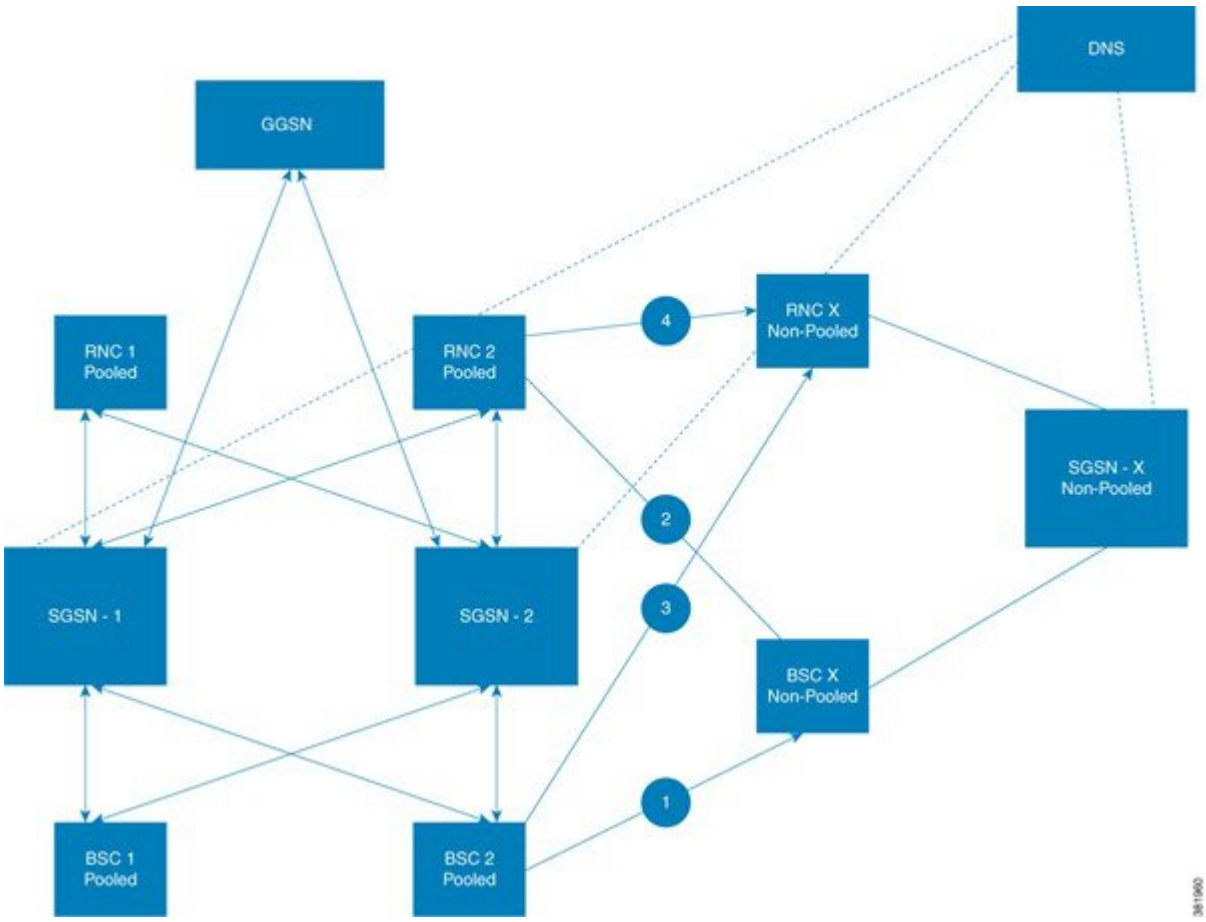
1. A subscriber attached to SGSN-1 through RNC-1 moves under the coverage area of RNC-2, while being attached to SGSN-1. This results only in an Intra-SGSN RAU.
2. A subscriber attached to SGSN-1 through BSC-1 moves under the coverage area of BSC-2, while being attached to SGSN-1. This results only in an Intra-SGSN RAU.

Important Inter-SGSN RAU within the pool is not very common unless one of the SGSNs within the pool is offloading the subscribers or the Gb/Iu link towards one of the SGSNs from a BSC/RNC is unavailable.

Mobility Outside the Pool

When an UE leaves a pool service area and performs an Attach or a RA update to an SGSN outside the pool service area, the new SGSN cannot identify the old SGSN based on the old Routing Area Identity (RAI). Finding the address of the old SGSN is facilitated by a DNS query with RAI specified. First the new SGSN uses the RAI to identify the default SGSN in the pool. The new SGSN then fetches the subscriber data from the old SGSN and continues with the routing area update procedure.

Figure 98: Mobility outside the Pool



Consider the scenario depicted in the diagram above:

The subscriber movement can be traced through the numbers 1, 2, 3 and 4 in the diagram.

1. The SGSN-X is not pooled. The SGSN-X queries the DNS to identify the source SGSN from where the UE arrived to initiate a GTP_SGSN_CONTEXT_REQUEST.
2. The DNS responds back with the IP address of the default SGSN in the pool, which could be either SGSN-1 or SGSN-2 or both.
3. The address resolution is performed based on the LAC and RAC similar to other Inter-SGSN RAU.
4. The designated default SGSN relays the GTP message to the source SGSN in the pool, which is located using the NRI in the P-TMSI and hence the DNS query with NRI, LAC and RAC.
5. In the implementation above both SGSN-1 and SGSN-2 are designated as default SGSNs to load share the GTP signaling traffic.
6. For every LAC/RAC in the pooled areas the DNS resolves the query into two IP addresses pertaining to the Gn loopback addresses of SGSN-1 and SGSN-2 respectively.

MS Offloading

MS offloading is a procedure of offloading the subscribers from one SGSN in the pool to another SGSN within the same pool. Offloading is performed during the following scenarios:

1. The operator wants to carry out a scheduled maintenance.
2. The operator wants to perform a load re-distribution.
3. To avoid an overload.

Offloading has to be performed with minimum impact on the end users.

Types of MS Offloading:

1. Null-NRI based.
2. Target-NRI based.
3. IMSI based offloading

Null-NRI based Offloading

Null-NRI based offloading is carried out in the following three phases:

Phase - 1

1. UEs performing a RAU or Attach are moved to other SGSN in the pool.
2. When the SGSN receives the Routing Area Update or Attach request, it returns a new P-TMSI with the null-NRI, and non-broadcast LAC and RAC in the accept message.
3. A new Routing Area Update is triggered by setting the periodic routing area update timer to a sufficiently low value in the accept message.
4. The UE sends a new Routing Area Update, the BSC then routes this RAU to a new SGSN due to the presence of a null-NRI. The BSC uses a round robin mechanism to allocate an SGSN for this UE.

Phase - 2

1. All PDP context activation requests are rejected and the UEs are requested to detach and re-attach (Detach request sent from the network with cause code "reattach required").
2. When the UEs re-attach, the SGSN moves them as described above in "Phase 1", that is, by sending the null-NRI and non-broadcast LAC and RAC and triggering a periodic RAU update.

Phase -3

This phase includes scanning through the remaining UEs and initiating a detach procedure for them. The UEs are requested to detach and re-attach, this results in the UEs moving as described in "Phase 1".

UEs being moved from one SGSN can be stopped from registering to the same SGSN again by issuing a CLI command in BSCs connected to the pool. UEs moving into a pool area may also be stopped from registering into a SGSN being off-loaded in the same manner. The move operation will not overload the network, as throttling is supported for both Attach and Inter SGSN RAU procedures.

Target-NRI based offloading

Target NRI based offloading was primarily introduced so that subscribers can be offloaded to a chosen SGSN. In the case of NULL-NRI based offloading there is no control on which SGSN the subscribers are offloaded to. SGSN offloads subscribers by assigning NB-RAI, stamping Target-NRI in PTMSI and reducing periodic routing area update timer during Attach/RAU accept messages.

IMSI-based offloading is carried in the following three phases:

IMSI based offloading

With Target-NRI based method of offloading though there is control on the SGSN to which the subscribers are offloaded, there is no control on the subscribers being offloaded to the SGSN. IMSI-based offloading enhancement allows the operator to choose the subscribers to be offloaded to a particular SGSN.

Phase -1

When a Attach accept or a RAU accept is issued, the offloading configuration is verified and if offloading is enabled, the corresponding NRI is issued (if it is not issued earlier). In case the specific IMSI based offloading configuration is configured, the configured target-nri is used. When offloading is enabled, if ptmsi allocation configuration is absent, a ptmsi is allocated to the subscriber in Attach/RAU accept.

Phase -2

On receiving an activation trigger from the MS, the subscriber is detached and the re-attach required is set to true. The MS will return an attach in due time, after which the MS is offloaded to another SGSN by setting the Target-NRI and NB-RAI appropriately.

Phase -3 0

The subscriber is cleared unconditionally and a detach is sent by setting the re-attach required to true. The subscriber is lost at this stage. In the next attach, the subscriber is offloaded to the configured SGSN.

For information on the procedure to configure MS-Offloading, refer to the section "Configuration of SGSN Pooling - Procedure to configure MS-Offloading".

Iu/Gb Flex support over S16/S3 interface

SGSN Pooling support has been extended to S16/S3 interface. The enhancement also includes support for default SGSN functionality for S16/S3 interface as in the case of Gn interface. The peer SGSN in this case is a S4-SGSN. The incoming message (EGTP_CONTEXT_REQ/IDENTIFICATION_REQ) is received from a non-pooled SGSN, it is forwarded to the old-SGSN if the SGSN is configured as default SGSN. The SGSN in a pool is identified on the basis on NRI value and OLD- RAI value. The NRI value is extracted from PTMSI.

Backward compatibility and default SGSN functionality

If a default SGSN that is serving a pool-area receives EGTP signaling it resolves the ambiguity of the multiple SGSNs per RAI by deriving the NRI from the P-TMSI. The SGSN relays the EGTP signaling to the old SGSN identified by the NRI in the old P-TMSI unless the default SGSN itself is the old SGSN. For default-SGSN functionality to work, static IP address entries are mandatory in the call-control profile.

Messages are relayed by the Default-SGSN (Default SGSN functionality and pooling are enabled) in following cases:

- Pooled local RAI and non-local NRI
- Non-local RAI and Null-NRI
- Non-local RAI and Target-NRI

For "Non-local RAI and Null-NRI" and "Non-local RAI and Target-NRI" options, the NB-RAI of other SGSN is considered. It is non-local to the SGSN. No other configuration entries are present at the SGSN other than cc-profile entries.

Mobility Management

The MS performs RA Updates and Attachments, which result in a change of the serving SGSN. In these procedures the new SGSN requests MS specific parameters from the old SGSN. The default SGSN node uses the old RA together with the NRI to derive the signaling address of the old SGSN from its configuration data.

Address and TEID for the Control Plane

- The relaying SGSN forwards the Context Request message to the interface of the old SGSN. The incoming request can arrive over a S3 interface in case of MME or S3 in case of S4-SGSN. However the old RAI interface will be always S16.
- When the default-sgsn relays the message, if the UDP port number is absent in the request received, the default-sgsn adds the "UDP source port number" IE while relaying. This is applicable for both Context Request and Identification Request relay functionality.
- If in an Identification request message, "Address for control plane" is an optional IE. A SGSN within the same SGSN pool with the old SGSN receives the Identification request message it includes the old IP address of the received message in this optional parameter if this IE is not present and relays the message to the old SGSN.
- In cases where default-sgsn has to send a negative response, it sends the message to the IP as indicated in the "S3/S16 Address and TEID for Control Plane" IE and destination port set as indicated by "UDP source port number" IE.
- If an SGSN within the same SGSN pool with the old SGSN receives this message, the SGSN decrements the Hop Counter if this IE is present in the received message. Otherwise, the SGSN includes a Hop Counter with a configured value and relays the message to the old SGSN. This is applicable for both Context Request and Identification Request relay functionality.

For more information refer to 3GPP TS 29.274 (Table 7.3.5-1: Information Elements in a Context Request, Table 7.3.8-1: Information Elements in an Identification Request).

For information on procedure to configure Iu/Gb flex on S16/S3 interface refer to the section "Configuration of SGSN Pooling - Procedure to configure default SGSN (S16/S3 interface)".

Standards Compliance

The SGSN Pooling feature complies with the following standards:

- 3GPP TS 23.236
- 3GPP TS 29.274

Configuring the SGSN Pooling feature

2G-SGSN pool configuration

Listed below are the pre-requisite CLI configurations that should be enabled to configure a 2G SGSN Pool:

1. 2G SGSN Pooling configuration is done under the GPRS service in the Gb context.
2. The NRI value, NRI length, Null-NRI value and non-broadcast LAC/RAC are configured for the GPRS service.
3. The GPRS service is capable of handling both pooled and non-pooled BSCs.

GPRS Service Configuration:

```
config
 context context_name
 gprs-service service_name
 peer-nsei nse_id pooled
 nri length nri_length { nri-value nri_value | null-nri-value null_nri_value non
 broadcast-lac lac_id  rac rac_id [ nri-value value ]}
             exit
```

Notes:

- The above configuration must be repeated each time a BSC is added.
- The command **peer-nsei** is used to render a BSC as pooled or non-pooled.

3G-SGSN pool configuration

Listed below are the pre-requisite CLI configurations that should be enabled to configure a 3G SGSN pool:

1. 3G SGSN pooling configuration is done under the IuPS service in the Iu context.
2. The NRI value, NRI length, Null-NRI value and non-broadcast LAC/RAC are configured for the SGSN service.
3. The IuPS service is capable of handling both pooled and non-pooled RNCs.

IuPS Service Configuration

```
config
 context <context_name>
  iups-service <service_name>
   rnc id <rnc_id>  pooled
   exit
```

SGSN Service Configuration

```
config
 context <context_name>
  sgsn-service <service_name>
```

```
  nri length  nri_length [ nri-value nri_value | null-nri-value null_nri_value
non-broadcast mcc mcc mnc mnc lac lac_id rac rac_id nri-value value ]
  default nri
  no nri
  exit
```

To Configure a Default SGSN

This procedure is common to both 2G and 3G SGSN pooling configurations. The SGSN can be configured as a "default SGSN" in the pool under the SGTP service in the Gn context. This configuration is to be performed only once to render a SGSN as a "default SGSN".

```
config
 context <context_name>
  sgtp-service <service_name>
   pool {default-sgsn | hop-counter count}
   exit
```

Procedure to Configure a Default SGSN (S16/S3 interface)

The following CLI command under the eGTP Service Configuration mode is used to configure the default SGSN:

```
config
 context <context_name>
  egtp-service <service_name>
   pool {default-sgsn | hop-counter count}
   exit
```

The default SGSN receives inbound SGSN context request messages and forwards it to the correct SGSN in the pool based on the NRI bits of the P-TMSI. If the incoming message EGTP_CONTEXT_REQ/ IDENTIFICATION_REQ has the hop count IE, the default SGSN decrements the count by one and forwards it to the Old-SGSN. The hop count is not over written even if it is configured. If the hop count IE is missing with incoming message then the then hop count configured gets populated. If no value is configured the default value is chosen. The hop Counter prevents endless relaying of context/identification request. Each relaying SGSN keeps decrementing the hop-counter value if received from the peer-sgsn, otherwise the SGSN includes hop-counter IE. If default-sgsn receives request having hop counter "0", it does not relay the request.

Procedure to Configure an Operator Policy

Step 1:

```
config
 operator-policy (default | name policy_name) [-noconfirm]
```

Step 2:

```
config
 call-control profile profile_name
 sgsn-address {  nri nri | rac rac-id lac lac_id | rnc_id rnc_id } [ nri nri
] prefer { fallback-for-dns | local } address { ipv4 ip_address | ipv6
ip_address } interface { gn | s16 }
```

Procedure to Configure MS Offloading

The SGSN **offload** command is used to configure the MS offloading procedure.

The following CLI command (for phase 1 and phase 2 of offloading) is issued for each GPRS/SGSN service:

sgsn offload { gprs-service *service_name* **| sgsn-service** *service_name* **} { activating [imsi** *imsi* **| nri-value** *nri_value* **| stop [imsi** *imsi* **| nri-value** *nri_value* **]] | connecting [nri-value** *nri_value* **| stop [imsi** *imsi* **| nri-value** *nri_value* **| target-nri** *target_nri* **] | t3312-timeout** *seconds* **[nri-value** *nri_value* **| target-nri** *target_nri* **] | target-nri** *target_nri* **[imsi** *imsi* **| target-count** *num_to_offload* **] }**

Important Various combinations of the same command is issued based on whether it is a 2G, 3G, Null-NRI based offloading, Target-NRI based offloading or IMSI based offloading and so on.

The following CLI has to be issued for the phase-3 of offloading:

clear subscribers sgsn-service*service_name* **{nri[<val> | any]}**

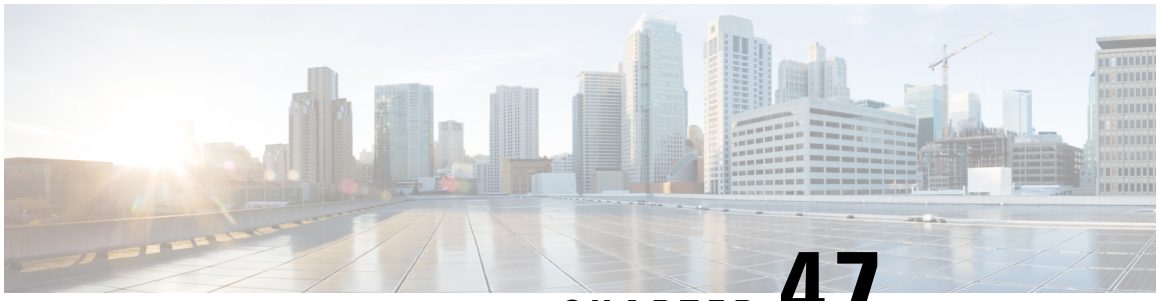
Consider and SGSN node which was offloaded due to a maintenance requirement, once this SGSN is again operational it will not recover the subscribers attached before the maintenance occurred. In due course this SGSN will be leveraged, with subscribers moved from (partial offload) two or three most loaded SGSNs.

Monitoring and Troubleshooting the SGSN Pooling feature

SGSN Pooling Show Command(s) and/or Outputs

This section provides information regarding show commands and their outputs in support of the SGSN Pooling:

- **show subscribers sgsn-only/gprs-only full all**
- **show sgsn-pool statistics sgsn-service**
- **show sgsn-pool statistics gprs-service**



CHAPTER 47

SGSN Processes Uplink Data Status IE in Service Request

This chapter describes the SGSN Processesing the Uplink Data Status IE in Service Request.

- Feature Description, on page 515
- Standards Compliance, on page 515
- Configuring Processing of Uplink Data Status IE in Service Request, on page 515
- Monitoring and Troubleshooting the Feature, on page 516

Feature Description

The Gn SGSN now supports processing of Uplink Data Status IE in Service Request; RABs are established for NSAPIs present in the Uplink Data Status IE. With this feature enhancement the RAB's are selectively established for NSAPIs which require uplink data transfer. In earlier releases RABs were established for all PDPs. Support has been added to decode Uplink Data Status IE in the Service Request. Performance improvement and reduced signaling are observed as RABs are established only for NSAPIs which require uplink data transfer.

A new CLI command has been provided under the Call Control Profile to enable or disable this feature. The user can configure the CLI to either ignore or process the Uplink Data Status IE in Service Request. This feature is enabled by default.

Standards Compliance

This feature complies with the 3GPP TS24.008.

Configuring Processing of Uplink Data Status IE in Service Request

This section describes the configuration procedure for this feature. The following new CLI command under the Call Control Profile is used enable or disable processing of Uplink Data Status IE in Service Request

```
config
 call-control-profile profile_name
 [remove] ignore-ul-data-status
 exit
```

Notes:

- This feature is enabled by default, to disable the feature use the command **ignore-ul-data-status**.
- To enable this feature use the command **remove ignore-ul-data-status**.
- When this feature is enabled, RAB is established for NSAPIs present in the Uplink data status IE. RABs are not established if the NSAPI PDPs are not present in the SGSN. If the Uplink data Status IE contains NSAPI not known to the SGSN, the SGSN establishes all the RAB's. RAB's are not established if corresponding NSAPI is absent in the PDP-Context Status IE.
- When this feature is disabled, if Uplink data status IE is received in service request the SGSN ignores it and establishes RABs for all the PDPs.

Verifying the Configuration

The **show call-control-profile full** command is used to verify the configuration of this feature. The following field displays whether the Uplink Data Status IE is **Processed** or **Ignored**:

- Uplink data status IE in service request

Monitoring and Troubleshooting the Feature

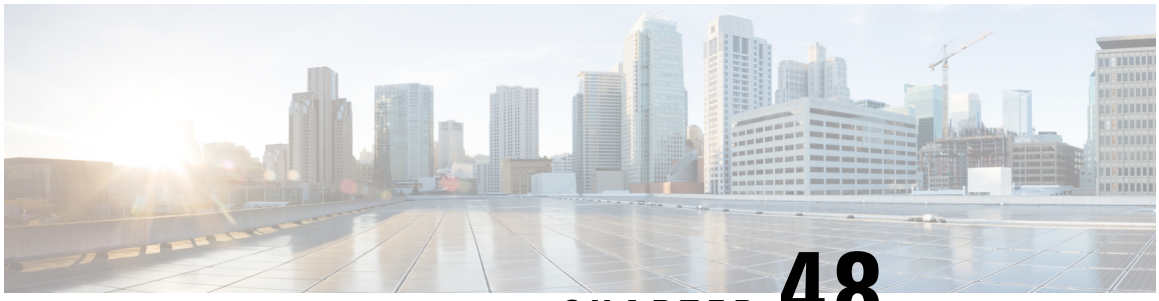
This section provides information on how to monitor the processing of Uplink Data Status IE in Service Request.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs when the Uplink Data Status IE is processed:

show gmm-sm statistics

This show command is updated to display the number of RABs not re-established due to absence of NSAPI bit set in the Uplink Data Status IE. This field is also used as a measure to verify the reduction in radio signaling. The new field **Rab-Not-Re-Estd-UL-Data-Stat** is added to the show output.



CHAPTER 48

SGSN Serving Radio Network Subsystem Relocation

This chapter describes the SGSN Serving Radio Network Subsystem Relocation (SRNS) feature.

- Feature Description, on page 517
- How it Works, on page 518
- Configuring SRNS Relocation on the SGSN, on page 553
- Monitoring and Troubleshooting SRNS Relocation, on page 555

Feature Description

The SRNS relocation feature facilitates connected mode inter-RAT handovers between UTRAN (3G) networks or between UTRAN and EUTRAN (LTE) networks. The advantage of this feature is that the radio bearer establishment occurs before the actual handover at the target.

The Gn/Gp SGSN and S4-SGSN support inter- and intra-SGSN SRNS relocation to enable:

- Handovers of an MS from one RNC to another RNC
- Handovers of an MS from one RNC to an eNodeb

The S4-SGSN supports the optional setup of indirect data forwarding tunnels (IDFT) between the eNodeB and the RNC via the SGW during connected mode handovers. This allows the S4-SGSN to support connected mode handovers between the UTRAN and E-UTRAN networks across the S3 interface. IDFT is not supported on the SGSN across the Gn interface.

The SRNS Relocation feature is included with the base SGSN license. It does not require an additional feature license.

Relationships to Other Features

This section describes how the SRNS Relocation feature relates to other SGSN features.

- For an SGSN operating via the Gn/Gp interfaces, a 3G service (sgsn-service) must be configured and enabled before SRNS Relocation can be configured.
- For an S4-SGSN, both a 3G service (sgsn-service) and S4-SGSN support (egtp-service) must be configured before SRNS Relocation can be configured.
- If operators are using non-standard LAC ranges, then a network-global-mme-id-mgmt-db must be configured and associated with the sgsn-service.

For detailed instructions on configuring the above, refer to the appropriate chapters in this guide.

How it Works

SRNS Relocation on the SGSN (Gn/Gp)

On the Gn/Gp SGSN, the SRNS relocation feature is triggered by subscribers (MS/UE) moving from one RNS to another. If the originating RNS and destination RNS are connected to the same SGSN but are in different routing areas, the behavior triggers an intra-SGSN Routing Area Update (RAU). If the RNSs are connected to different SGSNs, the relocation is followed by an inter-SGSN RAU.

The following table describes the interface selection logic for the various types of SRNS relocation that can occur when the interface used for a subscriber is Gn for PDP contexts. Note that the Gn/Gp SGSN SRNS relocation selection logic is applicable in the following instances:

- An S4-SGSN is configured (both the S4 license and EGTP service are available), but a given subscriber uses the Gn interface for PDP contexts.
- Only the Gn/Gp interfaces are utilized on the SGSN. S4 support is not configured.

Table 36: Interface Selection Logic for SRNS Relocation on the SGSN Gn/Gp

Sl.No	RNC Release Compliance	Target Type Sent in Rel. Req.	LAC Configured as MME Group ID	LAC MSB Set	Peer Type	DNS Query Type	Interface IP Provided by DNS	Interface Chosen
1	R8+	eNodeB	Not Applicable	Irrelevant	MME	When the Gn interface is used, the system maps the eNB ID to the RNC ID as follows: The MSB 12 bits of the 20 bit eNB ID is mapped to RNC ID. DSN A query with RNC ID FQDN is sent and Gn address is selected.	Gn	Gn

Sl.No	RNC Release Compliance	Target Type Sent in Rel. Req.	LAC Configured as MME Group ID	LAC MSB Set	Peer Type	DNS Query Type	Interface IP Provided by DNS	Interface Chosen
2	R8+	RNC	Not Applicable	Irrelevant	SGSN	DNS A Query with RNC ID FQDN	Gn	Gn
3	Pre R8	RNC	Irrelevant	Irrelevant	It is not important to a Gn SGSN if the peer is an MME or an SGSN. For a Gn SGSN, a peer MME is treated just like an SGSN	DNS A Query with RNC ID FQDN	Gn	Gn

SGSN (Gn/Gp) SRNS Relocation Call Flow Diagrams

This section provides call flow diagrams and process descriptions for the following SGSN Gn/Gp SRNS Relocation scenarios:

- Inter-SGSN (Gn/Gp) SRNS Relocation Call Flow
- Intra-SGSN (Gn/Gp) SRNS Relocation Call Flow

The Inter-SGSN (Gn/Gp) SRNS Relocation procedure is illustrated in the following diagram.

Figure 99: Inter-SGSN Gn/Gp SRNS Relocation Call Flow

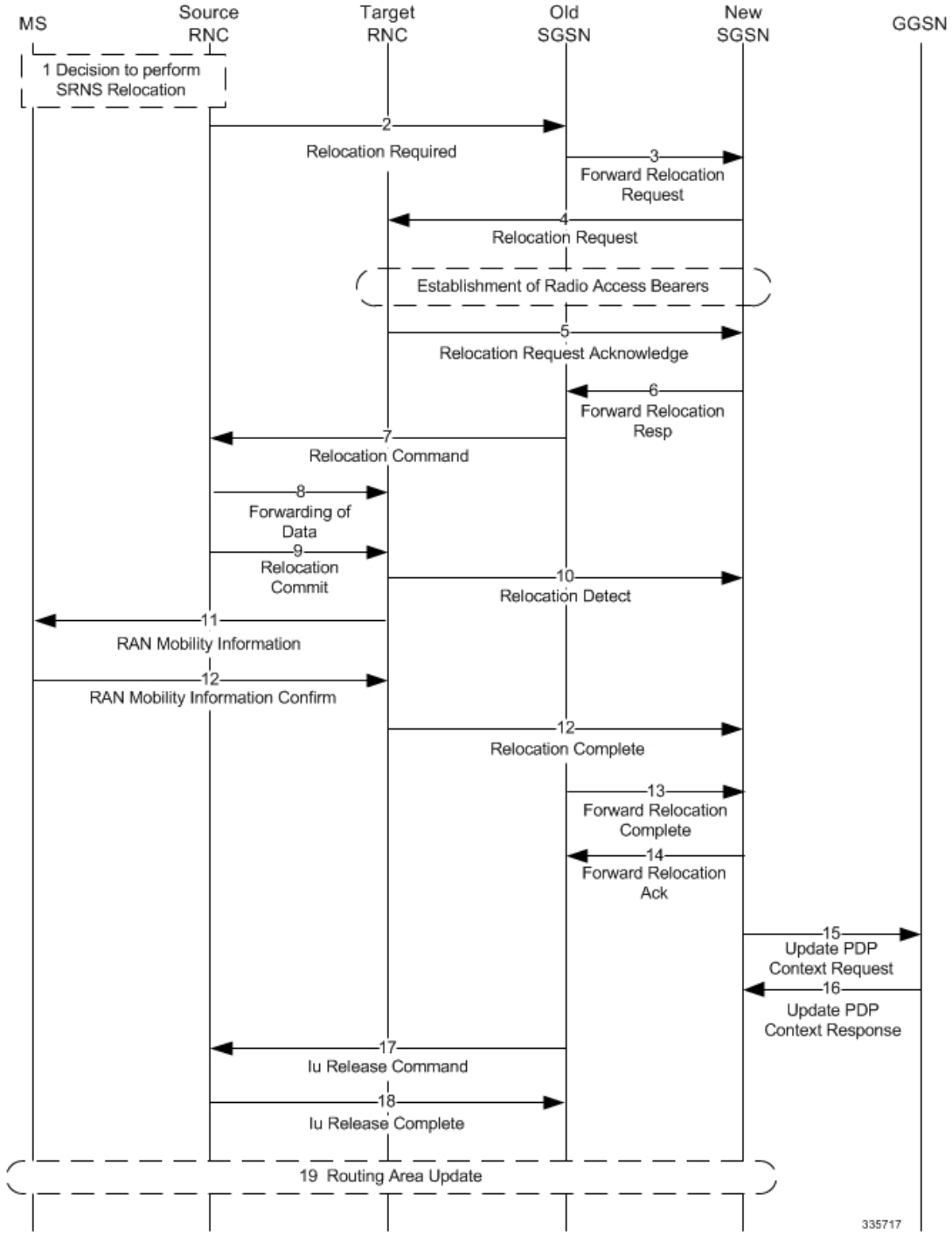


Table 37: Inter-SGSN (Gn/Gp) SRNS Relocation Process Description

Step	Description
1	The source SRNC decides to perform/initiate SRNS relocation.
2	The source SRNC sends a Relocation Required message (Relocation Type, Cause, Source ID, Target ID, Source RNC to target RNC transparent container) to the old SGSN.
3	The old SGSN determines from the Target ID that an inter-SGSN SRNS relocation is required. A DNS A query is performed for the target RNC ID FQDN to obtain the target SGSN IP address. The old SGSN then sends a Forward Relocation Request to the new SGSN.
4	The new SGSN sends a Relocation Request message to the new RNC. At this point, radio access bearers have been established.
5	The new RNC sends a Relocation Request Response message to the new SGSN.
6	When resources for the transmission of user data between the new RNC and the new SGSN have been allocated and the new SGSN is ready for relocation of SRNS, the Forward Relocation Response message (Cause, RANAP Cause, and RAB Setup Information) is sent from the new SGSN to the old SGSN.
7	The old SGSN continues the relocation of SRNS by sending a Relocation Command message to the old RNC. The old SGSN sends the RAB setup information received in the Forward Relocation Response in a Relocation Command to the old RNC. This enables the old RNC to establish a data path with new RNC so that it can forward the data packets.
8	The old SRNC may, according to the QoS profile, begin the forwarding of data for the RABs to be subject for data forwarding.
9	Before sending the Relocation Commit the uplink and downlink data transfer in the source, the SRNC shall be suspended for RABs, which require a delivery order. The source RNC starts the data-forwarding timer. When the old SRNC is ready, the old SRNC triggers the execution of relocation of SRNS by sending a Relocation Commit message (SRNS Contexts) to the new RNC over the Iur interface.

Step	Description
10	The target RNC sends a Relocation Detect message to the new SGSN when the relocation execution trigger is received.
11	The new RNC sends a RAN Mobility Information message. This message contains UE information elements and CN information elements.
12	When the new SRNC receives the RAN Mobility Information Confirm message, i.e. the new SRNCID + S-RNTI are successfully exchanged with the MS by the radio protocols, the target SRNC initiates the Relocation Complete procedure by sending the Relocation Complete message to the new SGSN.
13	The old SGSN sends a Forward Relocation Complete message.
14	The old SGSN sends a Forward Relocation Acknowledgement to the new SGSN. to signal to the new SGSN the completion of the SRNS relocation procedure.
15	Upon receipt of the Relocation Complete message, the CN switches the user plane from the old RNC to the new SRNC. The new SGSN sends Update PDP Context Request messages to the GGSN.
16	The GGSN sends Update PDP Context Response messages to the new SGSN.
17	The old SGSN sends an Iu Release Command message to the old RNC.
18	The old RNC sends an Iu Release Complete message to the old SGSN.
19	After the MS has finished the RNTI reallocation procedure, and if the new Routing Area Identification is different from the old one, the MS initiates the Routing Area Update procedure.

The intra-SGSN Gn/Gp SRNS Relocation procedure is illustrated in the following figure.

Figure 100: Intra-SGSN Gn/Gp SRNS Relocation Call Flow

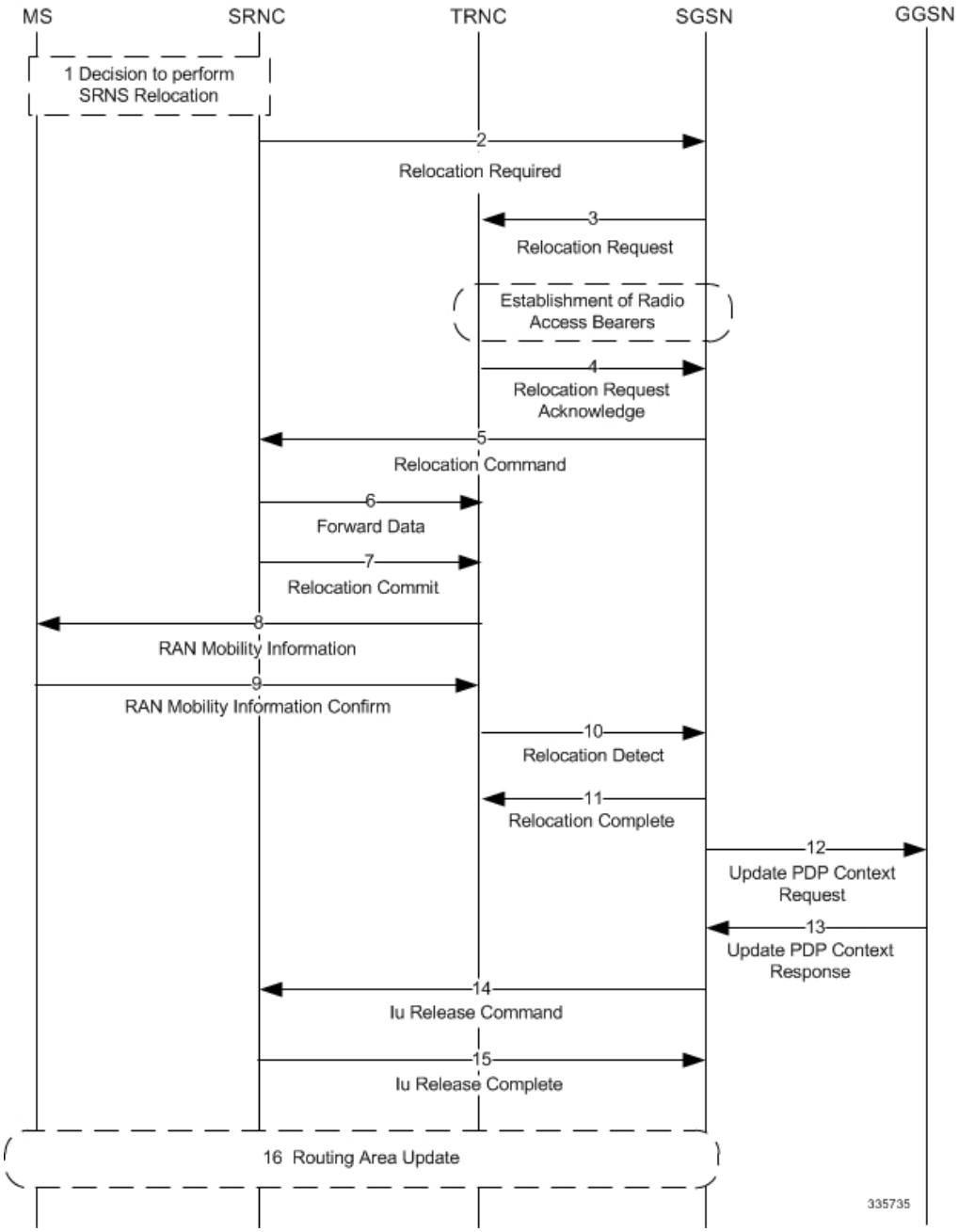


Table 38: Intra-SGSN (Gn/Gp) SRNS Relocation Process Description

Step	Description
1	The source SRNC decides to perform/initiate SRNS relocation.

Step	Description
2	The old RNC sends a Relocation Required message to the SGSN.
3	The SGSN sends a Relocation Request message to the new RNC. At this point, radio access bearers have been established.
4	The new RNC sends a Relocation Request Acknowledgement message to the SGSN.
5	The SGSN sends a Relocation Command to the old RNC and the UE is detached from the old RNC and attached to the new RNC.
6	The old SRNC may, according to the QoS profile, begin the forwarding of data for the RABs to be subject for data forwarding.
7	Before sending the Relocation Commit the uplink and downlink data transfer in the source, the SRNC shall be suspended for RABs, which require a delivery order. The source RNC starts the data-forwarding timer. When the old SRNC is ready, the old SRNC triggers the execution of relocation of SRNS by sending a Relocation Commit message (SRNS Contexts) to the new RNC over the Iur interface.
8	The new RNC sends a RAN Mobility Information message. This message contains UE information elements and CN information elements.
9	When the new SRNC receives the RAN Mobility Information Confirm message, i.e. the new SRNCID + S-RNTI are successfully exchanged with the MS by the radio protocols, the target SRNC initiates the Relocation Complete procedure by sending the Relocation Commit message to the new SGSN.
10	The new RNC sends a Relocation Detect message to the SGSN.
11	The SGSN sends a Relocation Complete message to the new RNC.
12	If Direct Tunnel was established during intra-SGSN SRNS relocation, the SGSN sends Update PDP Context Request messages to the GGSN.
13	If Direct Tunnel was established during intra-SGSN SRNS relocation, the SGSN sends Update PDP Context Response messages to the GGSN.

Step	Description
14	The SGSN sends an Iu Release Command to the old RNC.
15	The old RNC releases the Iu connection and sends a Release Complete message to the SGSN.
16	After the MS has finished the RNTI reallocation procedure, and if the new Routing Area Identification is different from the old one, the MS initiates the Routing Area Update procedure.

SRNS Relocation on the S4-SGSN

On the S4-SGSN, the SRNS relocation feature is triggered by subscribers (MS/UE) moving between an eNodeB and an RNC or between two RNCs.

If the originating and destination nodes are connected to the same S4-SGSN but are in different routing areas, the behavior triggers an intra-SGSN Routing Area Update (RAU).

If the nodes are connected to different S4-SGSNs, the relocation is followed by an inter-SGSN RAU. This RAU occurs over a RANAP direct transfer. As a result, it does not trigger Context Request/Context Response/Context Ack procedures with the old SGSN/MME. These procedures are otherwise performed during a normal SGSN RAU.

The GTPv2 protocol is used for SRNS relocation between two RNCs and between an eNodeB and an RNC.

In addition to supporting Inter-SGSN SRNS relocation across the Gn interface, the S4-SGSN supports SRNS relocation for the following scenarios across the S3 (S4-SGSN to MME) and S16 (S4-SGSN to S4-SGSN) interfaces:

- Inter-SGSN SRNS relocation over the S16 interface
- UTRAN-to-E-UTRAN connected mode Inter-RAT handover over the S3 interface
- E-UTRAN-to-UTRAN connected mode Inter-RAT handover over the S3 interface

As part of the SRNS relocation feature implementation on the S4-SGSN, the SGSN application also supports the gtpv2 (egtp) protocol for:

- Inter-SGSN SRNS relocations over the S16 interface
- MME - SGSN SRNS relocations over the S3 interface

S4-SGSN SRNS relocation interface selection logic is based on the following assumptions:

- If the egtp-service is configured, it is assumed the network is EPC capable and therefore must require a DNS SNAPTR.
- If the egtp-service is configured on the S4-SGSN, then for outbound SRNS relocation, the system always performs a DNS SNAPTR as follows:
- - x-S16 if the peer detected is another S4-GSN, or x-S3 if the peer detected is an MME (based on whether the target is an eNodeB/the MSB of the target LAC being 1, or, if a local MME group ID is configured).
  - x-gn if a local configuration for a peer SGSN or MME exists with a Gn address, or, if DNS SNAPTR returned a GN address.

If both DNS queries fail, the system rejects the SRNS relocation.

The following table describes the interface selection logic for the various types of SRNS relocation that can occur when the interface used for a subscriber is S4 for PDP contexts.

Table 39: Interface Selection Logic for S4-SGSN SRNS Relocation

Sl.No	RNC Release Compliance	Target Type Sent in Relocation Request	LAC Configured as MME Group ID	LAC MSB Set	Peer Type	Type of DNS Query	Interface IP Provided by DNS	Interface Chosen
1	R8+	eNodeB	n/a	n/a	MME	DNS SNAPTR w/ service type x-3gpp-mme:x-s3 and TAC FQDN	S3	S3
2	R8+	eNodeB	n/a	n/a	MME	DNS SNAPTR w/ service type x-3gpp-mme:x-s3 and TAC FQDN	Gn	When a TAC FQDN is used to query the MME address the system expects that the MME supports S3 interface. If this is the case, the S3 interface is chosen. If DNS returns a Gn address, then the system rejects the Relocation, and sends a Relocation Preparation Failure to the source RNC.
3	R8+	RNC	n/a	n/a	SGSN	DNS SNAPTR w/ service type x-3gpp-sgsn:x-s16 and RNC ID FQDN	S16	S16

Sl.No	RNC Release Compliance	Target Type Sent in Relocation Request	LAC Configured as MME Group ID	LAC MSB Set	Peer Type	Type of DNS Query	Interface IP Provided by DNS	Interface Chosen
4	R8+	RNC	n/a	n/a	SGSN	DNS SNAPTR w/ service type x-3gpp-sgsn:x-s16 and RNC ID FQDN	Gn	Gn
5	Pre R8	RNC (A pre R8 RNC cannot send eNB as the target type. Currently, operators configure eNB ID to RNC ID mapping in such these pre R8 RNCs so that the SGSN receives an RNC ID that is actually mapped from the eNB ID)	Yes	Irrelevant	MME	DNS SNAPTR w/ service type x-3gpp-mme:x-s3 and MME GI + MME Code FQDN	S3	S3
6	Pre R8	RNC	Yes	Irrelevant	MME	DNS SNAPTR w/ service type x-3gpp-mme:x-s3 and MME GI + MME Code FQDN	Gn	Gn
7	Pre R8	RNC	No	Yes	MME	DNS SNAPTR w/ service type x-3gpp-mme:x-s3 and MME GI + MME Code FQDN	S3	S3

Sl.No	RNC Release Compliance	Target Type Sent in Relocation Request	LAC Configured as MME Group ID	LAC MSB Set	Peer Type	Type of DNS Query	Interface IP Provided by DNS	Interface Chosen
8	Pre R8	RNC	No	Yes	MME	DNS SNAPTR w/ service type x-3gpp-mmex-s3 and MME GI + MME Code FQDN	Gn	Gn
9	Pre R8	RNC	No	No	SGSN	DNS SNAPTR w/ service type x-3gpp-sgsnx-sl6 and RNC ID FQDN	S16	S16
10	Pre R8	RNC	No	No	SGSN	DNS SNAPTR w/ service type x-3gpp-sgsnx-sl6 and RNC ID FQDN	Gn	Gn

IDFT Support During Connected Mode Handovers

The S4-SGSN supports the setup of indirect data forwarding tunnels (IDFT) between the eNodeB and the RNC via the SGW during connected mode handovers.

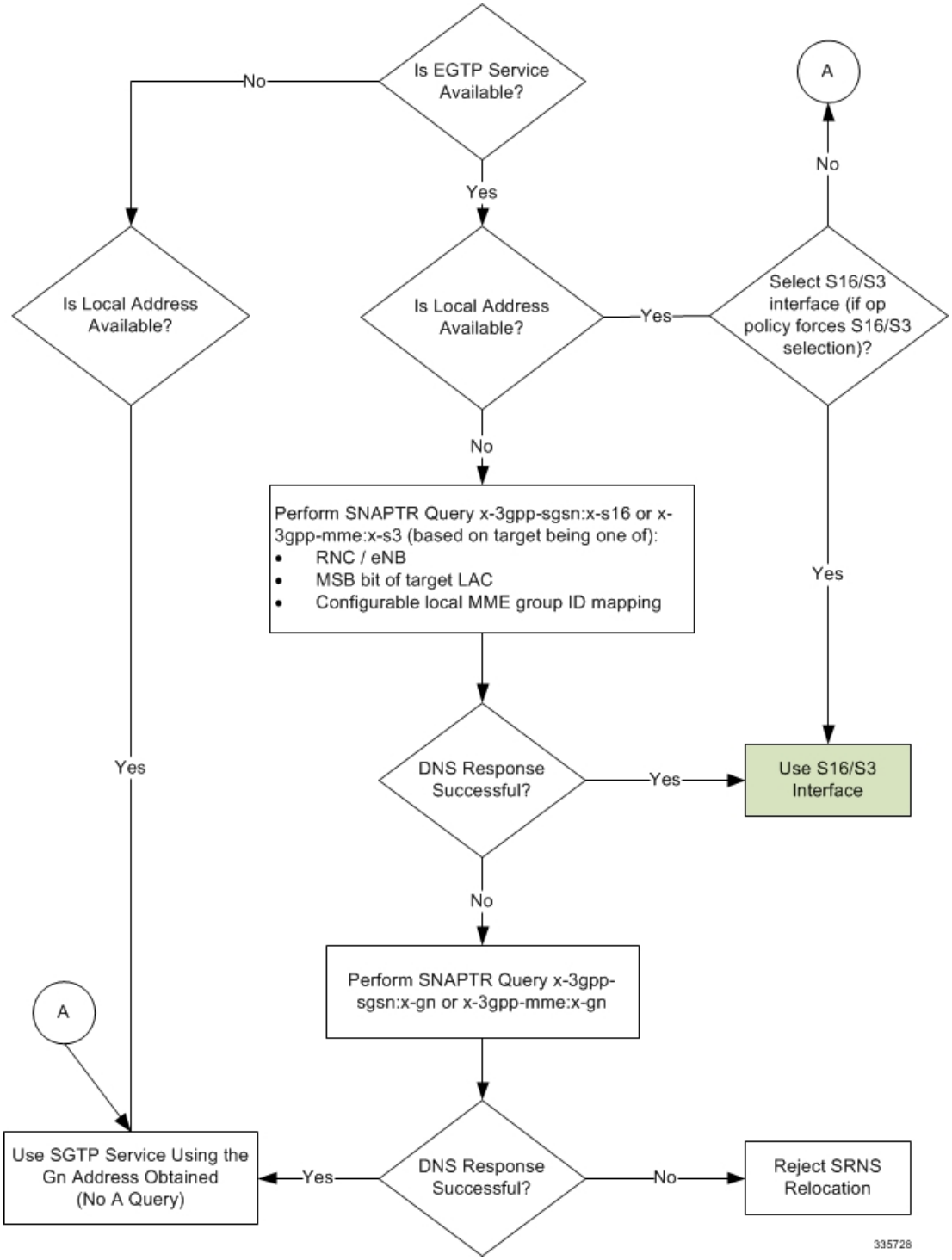
Once enabled, IDFT is employed under the following conditions:

- **If the SGSN is the old node**:
  - The target node to which the connected mode handover is initiated should be an eNodeB (i.e., the SGSN performs the handover to the MME).
  - The **enb-direct-data-forward** CLI setting is **not** configured as the source RNC configuration (in RNC Configuration Mode).
- **If the SGSN is the new node**:
  - The source node from which connected mode handover is initiated is an eNodeB (i.e., the MME is performing a handover to the SGSN).
  - The **enb-direct-data-forward** setting is **not** configured in the source RNC configuration (in RNC Configuration Mode).
  - The source MME indicated that it does not support direct forwarding via a Forward Relocation Request.

Important If the target SGSN did **not** relocate to a new SGW, IDFT setup does not apply at the SGSN. The target SGSN sets up an indirect data forwarding tunnel with the SGW only if the SGW is relocated. If the SGW is not relocated, then it is the source MME that sets up the indirect data forwarding tunnel between source the eNodeB and target RNC through the SGW.

The following diagram illustrates the interface selection logic for S4-SGSN connected mode handovers.

Figure 101: Interface Selection Logic for S4-SGSN SRNS Connected Mode Handovers



S4-SGSN SRNS Relocation Call Flow Diagrams

This section provides call flow diagrams for the following S4-SGSN SRNS relocation scenarios:

- Inter-S4-SGSN SRNS Relocation without SGW Relocation
- Inter-S4-SGSN Relocation with SGW Relocation
- Intra-S4-SGSN SRNS Relocation without SGW Relocation
- Inter-S4-SGSN Relocation with SGW Relocation
- S4-SGSN E-UTRAN to UTRAN Connected Mode Handover without SGW Relocation
- S4-SGSN UTRAN to E-UTRAN Connected Mode Handover with SGW Relocation Call Flow
- S4-SGSN Inter-SGSN SRNS Relocation with Hard Handover and SGW Relocation

Figure 102: S4 Inter-SGSN SRNS Relocation without SGW Relocation Call Flow

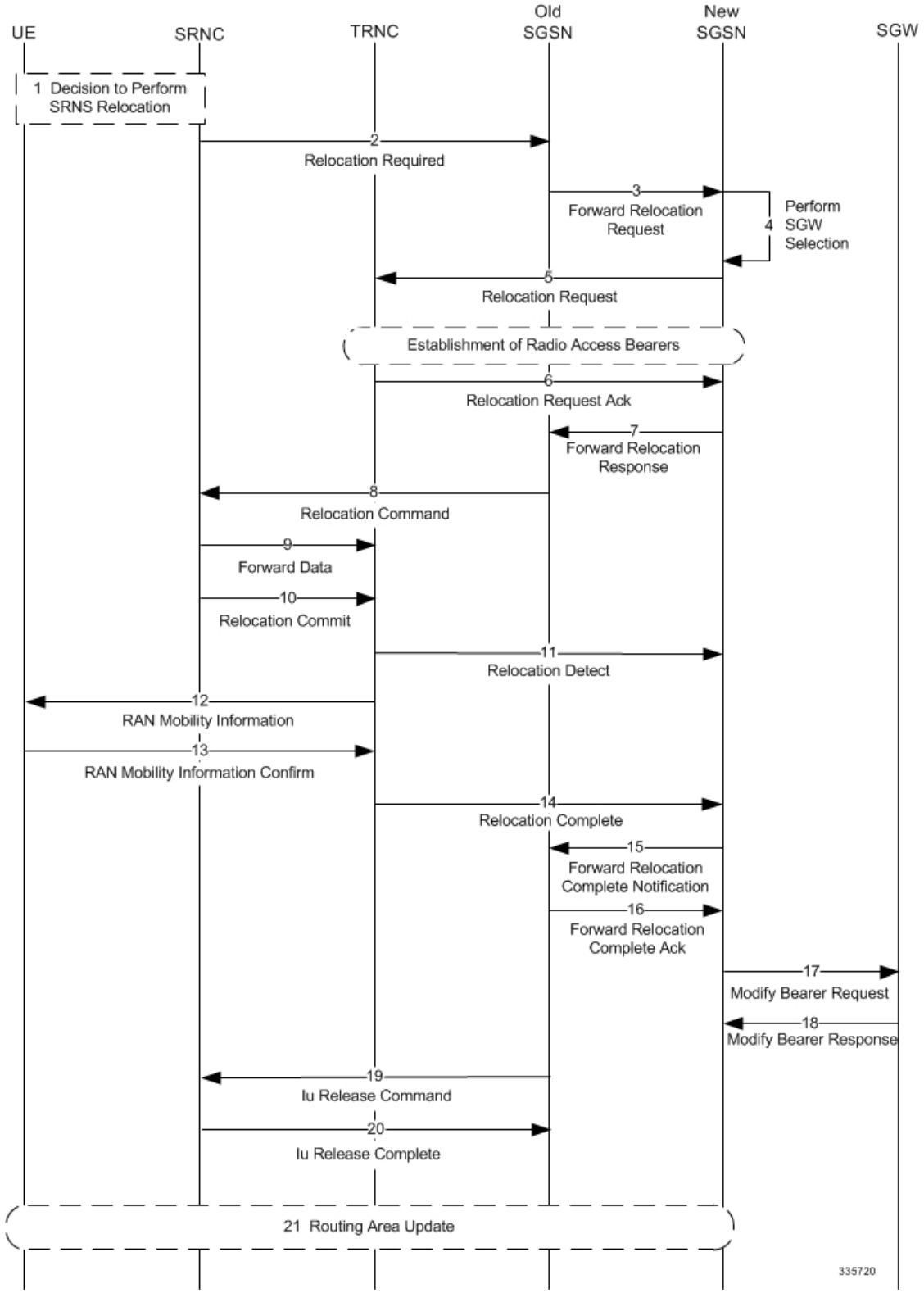


Table 40: Inter-S4-SGSN SRNS Relocation without SGW Relocation Process Description

Step	Description
1	The decision is made to perform SRNS relocation.
2	The old RNC sends a Relocation Required message to the old SGSN.
3	The old SGSN sends a Forward Relocation Request to the new SGSN.
4	The new SGSN performs SGW selection, but does not select a new SGW, as the subscriber is anchored at the same SGW as it was previously.
5	The new SGSN sends a Relocation Request message to the new RNC. At this point, Radio Access Bearers are established.
6	The new RNC sends a Relocation Request Acknowledgment to the new SGSN.
7	The new SGSN sends a Forward Relocation Response to the old SGSN. In this message, the old SGSN sends the RAB context information of the new RNC, which was obtained from the Relocation Request Ack message.
8	The old SGSN sends a Relocation Command to the old RNC. The old SGSN sends the new RNC RAB context information to the old RNC in the Relocation Command message so that old RNC can forward packets to the new RNC.
9	The old SRNC may, according to the QoS profile, begin the forwarding of data for the RABs to be subject for data forwarding.
10	Before sending the Relocation Commit the uplink and downlink data transfer in the source, the SRNC shall be suspended for RABs, which require a delivery order. The source RNC starts the data-forwarding timer. When the old SRNC is ready, the old SRNC triggers the execution of relocation of SRNS by sending a Relocation Commit message (SRNS Contexts) to the new RNC over the Iur interface.
11	The new RNC sends a Relocation Detect message to the new SGSN.
12	The new RNC sends a RAN Mobility Information message. This message contains UE information elements and CN information elements.

Step	Description
13	When the new SRNC receives the RAN Mobility Information Confirm message, i.e. the new SRNCID + S-RNTI are successfully exchanged with the MS by the radio protocols, the target SRNC initiates the Relocation Complete procedure by sending the Relocation Commit message to the new SGSN.
14	The new RNC sends a Relocation Complete message to the new SGSN.
15	The new SGSN sends a Forward Relocation Notification Complete message to the old SGSN.
16	The new SGSN sends a Forward Relocation Complete Ack message to the old SGSN.
17	The new SGSN sends a Modify Bearer Request to the SGW.
18	The SGW sends a Modify Bearer Response to the new SGSN.
19	The old SGSN sends an Iu Release Command message to the old RNC.
20	The old RNC sends an Iu Release Complete message to the old SGSN.
21	After the MS has finished the RNTI reallocation procedure, and if the new Routing Area Identification is different from the old one, the MS initiates the Routing Area Update procedure.

Figure 103: Inter-S4-SGSN Relocation with SGW Relocation

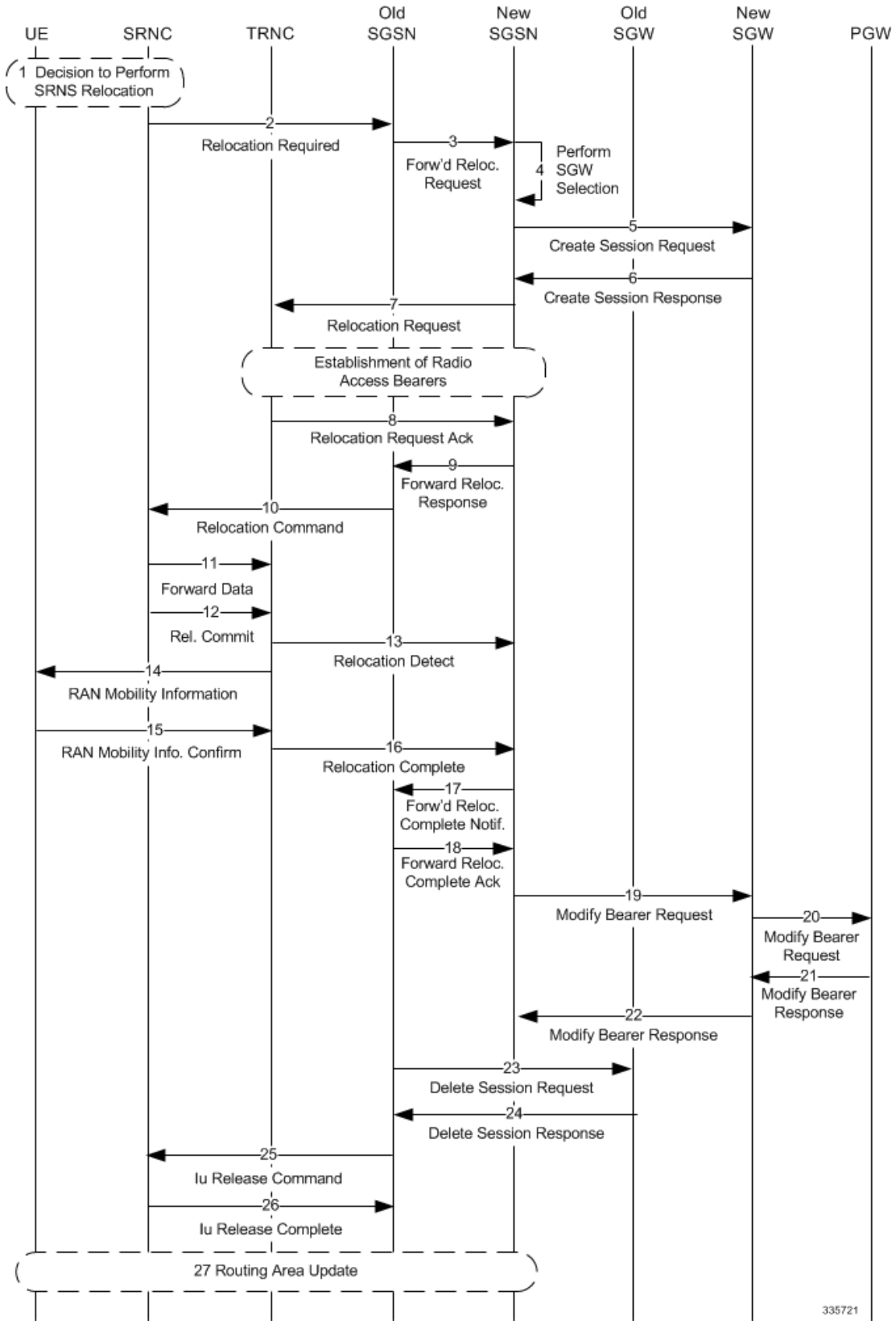

UE
SRNC
TRNC
Old SGSN
New SGSN
Old SGW
New SGW
PGW
1 Decision to Perform SRNS Relocation
2 Relocation Required
3 Forw'd Reloc. Request
4 Perform SGW Selection
5 Create Session Request
6 Create Session Response
7 Relocation Request
Establishment of Radio Access Bearers
8 Relocation Request Ack
9 Forward Reloc. Response
10 Relocation Command
11 Forward Data
12 Rel. Commit
13 Relocation Detect
14 RAN Mobility Information
15 RAN Mobility Info. Confirm
16 Relocation Complete
17 Forw'd Reloc. Complete Notif.
18 Forward Reloc. Complete Ack
19 Modify Bearer Request
20 Modify Bearer Request
21 Modify Bearer Response
22 Modify Bearer Response
23 Delete Session Request
24 Delete Session Response
25 Iu Release Command
26 Iu Release Complete
27 Routing Area Update
335721

Table 41: Inter-S4-SGSN Relocation with SGW Relocation Process Description

Step	Description
1	The decision is made to perform SRNS relocation.
2	The old RNC informs the old SGSN that relocation is required by sending a Relocation Required message.
3	The old SGSN initiates the relocation resource allocation procedure by sending a Forward Relocation Request message to the new SGSN.
4	The new SGSN performs SGW selection.
5	The new SGSN sends a Create Session Request to the new SGW with Indication Flags - Operations Indication bit = 0. The new SGW will not send a Modify Bearer Request to the PGW at this time.
6	The new SGW sends a Create Session Response to the new SGSN.
7	The new SGSN sends a Relocation Request to the new RNC. At this point radio access bearers are set up between the new RNC and the new SGSN.
8	The new RNC sends a Relocation Request Acknowledge message to the new SGSN.
9	The new SGSN sends a Forward Relocation Response message to the old SGSN. In this message, the old SGSN sends the RAB context information of the new RNC, which was obtained from Relocation Request Acknowledge message.
10	The old SGSN sends a Relocation Command to the old RNC. The old SGSN sends the new RNC RAB context information to the old RNC in the Relocation Command so that the old RNC can forward packets to the new RNC.
11	The old SRNC may, according to the QoS profile, begin the forwarding of data for the RABs to be subject for data forwarding.
12	Before sending the Relocation Commit the uplink and downlink data transfer in the source, the SRNC shall be suspended for RABs, which require a delivery order. The source RNC starts the data-forwarding timer. When the old SRNC is ready, the old SRNC triggers the execution of relocation of SRNS by sending a Relocation Commit message (SRNS Contexts) to the new RNC over the Iur interface.

Step	Description
13	The new RNC sends a Relocation Detect message to the new SGSN.
14	The new RNC sends a RAN Mobility Information message. This message contains UE information elements and CN information elements.
15	When the new SRNC receives the RAN Mobility Information Confirm message, i.e. the new SRNCID + S-RNTI are successfully exchanged with the MS by the radio protocols, the target SRNC initiates the Relocation Complete procedure by sending the Relocation Commit message to the new SGSN.
16	The new RNC sends a Relocation Complete message to the new SGSN.
17	The new SGSN sends a Forward Relocation Complete Notification message to the old SGSN.
18	The old SGSN sends a Forward Relocation Complete Ack message to the new SGSN.
19	The new SGSN sends a Modify Bearer Request message to the new SGW.
20	The SGW sends a Modify Bearer Request message to the PGW.
21	The PGW sends a Modify Bearer Response to the new SGW.
22	The SGW sends a Modify Bearer Response to the new SGSN.
23	The old SGSN sends a Delete Session Request to the old SGW.
24	The old SGW sends a Delete Session Response to the old SGSN.
25	The old SGSN sends an Iu Release Command message to the old RNC.
26	The old RNC sends an Iu Release Complete message to the old SGSN.
27	After the MS has finished the RNTI reallocation procedure, and if the new Routing Area Identification is different from the old one, the MS initiates the Routing Area Update procedure.

Figure 104: Intra-S4-SGSN SRNS Relocation without SGW Relocation

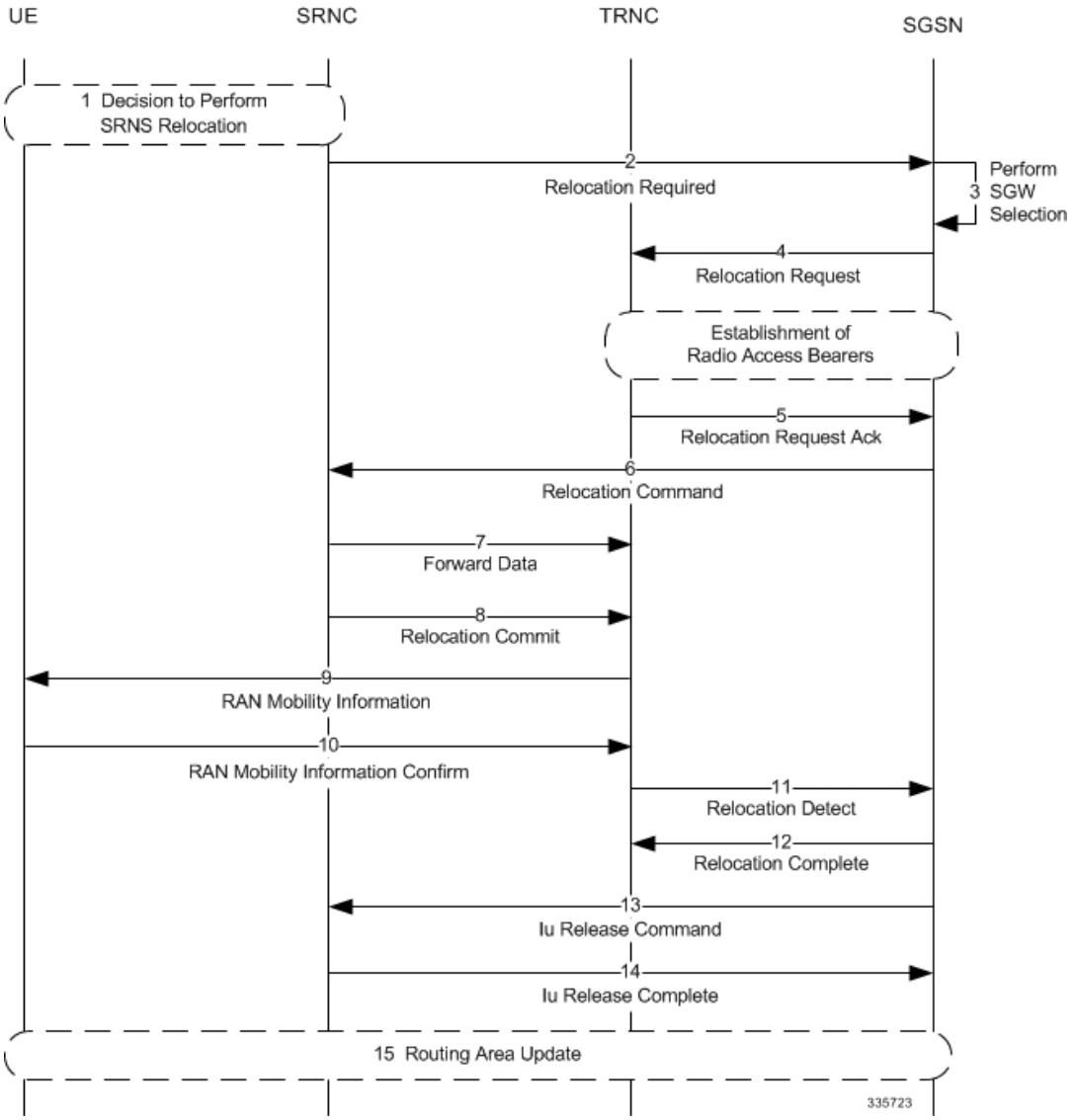


Table 42: Intra-S4-SGSN SRNS Relocation without SGW Relocation Process Description

Step	Description
1	The decision is made to perform SRNS relocation.
2	The old RNC sends a Relocation Required message to the SGSN.
3	The SGSN performs SGW selection, but does not select a new SGW, as the subscriber is anchored at the same SGW as it was previously.

Step	Description
4	The SGSN sends a Relocation Request message to the new RNC. At this point, radio access bearers have been established.
5	The new RNC sends a Relocation Request Acknowledgment message to the SGSN.
6	The SGSN sends a Relocation Command to the old RNC and the UE is detached from the old RNC and attached to the new RNC.
7	The old SRNC may, according to the QoS profile, begin the forwarding of data for the RABs to be subject for data forwarding.
8	Before sending the Relocation Commit the uplink and downlink data transfer in the source, the SRNC shall be suspended for RABs, which require a delivery order. The source RNC starts the data-forwarding timer. When the old SRNC is ready, the old SRNC triggers the execution of relocation of SRNS by sending a Relocation Commit message (SRNS Contexts) to the new RNC over the Iur interface.
9	The new RNC sends a RAN Mobility Information message. This message contains UE information elements and CN information elements.
10	When the new SRNC receives the RAN Mobility Information Confirm message, i.e. the new SRNCID + S-RNTI are successfully exchanged with the MS by the radio protocols, the target SRNC initiates the Relocation Complete procedure by sending the Relocation Commit message to the new SGSN.
11	The new RNC sends a Relocation Detect message to the SGSN.
12	The SGSN sends a Relocation Complete message to the new RNC.
13	The SGSN sends an Iu Release Command to the old RNC.
14	The old RNC releases the Iu connection and sends a Release Complete message to the SGSN.
15	After the MS has finished the RNTI reallocation procedure, and if the new Routing Area Identification is different from the old one, the MS initiates the Routing Area Update procedure.

Figure 105: Intra-S4-SGSN Relocation with SGW Relocation

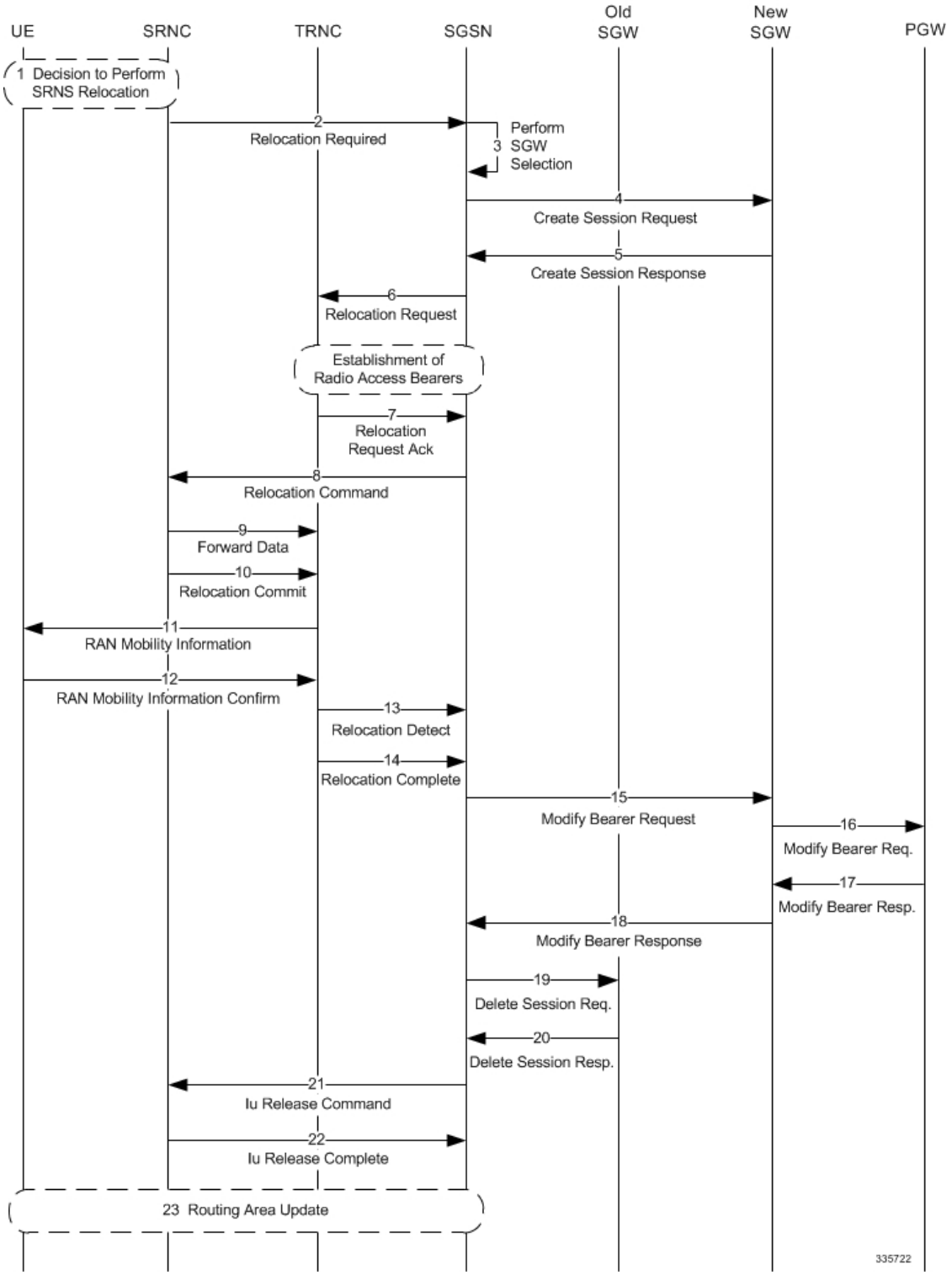


Table 43: Intra-S4-SGSN Relocation with SGW Relocation Process Description

Step	Description
1	The decision is made to perform SRNS relocation.
2	The old RNC sends a Relocation Required message to the SGSN.
3	The SGSN selects a new SGW for the UE.
4	The SGSN sends a Create Session Request to the new SGW with Indication Flags - Operations Indication bit=0. The new SGW does not send a Modify Beater Request to the PGW at this time.
5	The new SGW sends a Create Session Response to the SGSN.
6	The SGSN sends a Relocation Request to the new RNC. At this point, radio access bearers have been established.
7	The new RNC sends a Relocation Request Acknowledge message to the SGSN.
8	The SGSN sends a Relocation Command to the old RNC.
9	The new RNC sends a RAN Mobility Information message. This message contains UE information elements and CN information elements.
10	When the new SRNC receives the RAN Mobility Information Confirm message, i.e. the new SRNCID + S-RNTI are successfully exchanged with the MS by the radio protocols, the target SRNC initiates the Relocation Complete procedure by sending the Relocation Commit message to the new SGSN.
11	The new RNC sends a RAN Mobility Information message. This message contains UE information elements and CN information elements.
12	When the new SRNC receives the RAN Mobility Information Confirm message, i.e. the new SRNCID + S-RNTI are successfully exchanged with the MS by the radio protocols, the target SRNC initiates the Relocation Complete procedure by sending the Relocation Commit message to the new SGSN.
13	The new RNC sends a Relocation Detect message to the SGSN.

Step	Description
14	The new RNC sends a Relocation Complete message to the SGSN.
15	The SGSN sends a Modify Bearer Request message to the new SGW.
16	The new SGW sends a Modify Bearer Request to the PGW.
17	The PGW sends a Modify Bearer Response to the new SGW.
18	The new SGW sends a Modify Bearer Response to the SGSN.
19	The SGSN sends a Delete Session Request to the old SGW.
20	The old SGW sends a Delete Session Response to the SGSN.
21	The SGSN sends an Iu Release Command to the old RNC.
22	The old RNC sends an Iu Release Complete message to the SGSN.
23	After the MS has finished the RNTI reallocation procedure, and if the new Routing Area Identification is different from the old one, the MS initiates the Routing Area Update procedure.

Figure 106: S4-SGSN E-UTRAN to UTRAN Connected Mode Handover without SGW Relocation Call Flow

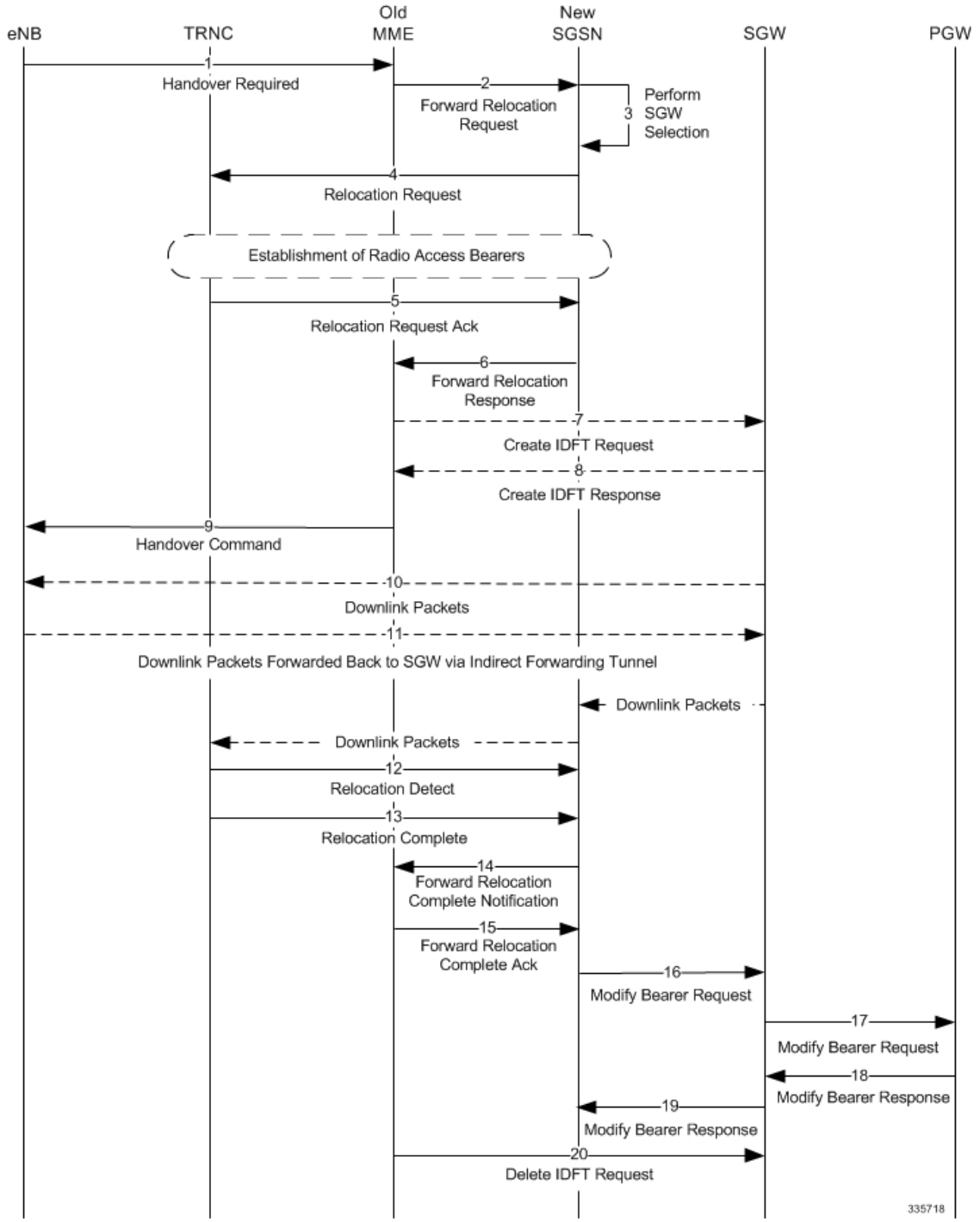


Table 44: S4-SGSN E-UTRAN to UTRAN Connected Mode Handover without SGW Relocation Process Description

Step	Description
1	The eNodeB determines that relocation is required and sends a Relocation Required message to the old MME.
2	The old MME sends a Forward Relocation Request message to the new SGSN.
3	The new SGSN performs SGW selection for the UE.
4	The new SGSN sends a Relocation Request message to the new RNC. At this time, radio access bearers are established.
5	The new RNC sends a Relocation Request Ack message to the new SGSN.
6	The new SGSN sends a Forward Relocation Response to the old MME.
7	The old MME sends a Create Indirect Data Forwarding Tunnel Request message to the SGW (if IDFT is configured on the SGSN and MME).
8	The SGW sends a Create Indirect Data Forwarding Tunnel Response message to the old MME (if IDFT is configured on the SGSN and MME).
9	The old MME sends a Handover Command message to the eNodeB.
10	Downlink packets are sent from the SGW to the eNodeB.
11	Downlink packets are sent from the eNodeB to the SGW via Indirect Data Forwarding Tunnel (if IDFT is configured on the new SGSN and the old MME). Downlink packets then are sent from the SGW to the new SGSN, and finally, from the new SGSN to the new RNC.
12	The new RNC sends a Relocation Detect message to the new SGSN.
13	The new RNC sends a Relocation Complete message to the new SGSN.
14	The new SGSN sends a Forward Relocation Complete Notification message to the old MME.
15	The old MME sends a Forward Relocation Complete Ack message to the new SGSN.

Step	Description
16	The new SGSN sends a Modify Bearer Request message to the SGW.
17	The new SGW sends a Modify Bearer Request message to the PGW.
18	The PGW sends a Modify Bearer Response message to the SGW.
19	The new SGW sends a Modify Bearer Response message to the new SGSN.
20	After timer expiry, the old MME sends a Delete IDFT Tunnel Request to the SGW and deletes the IDFT tunnel.

Figure 107: S4-SGSN UTRAN to E-UTRAN Connected Mode Handover with SGW Relocation Call Flow

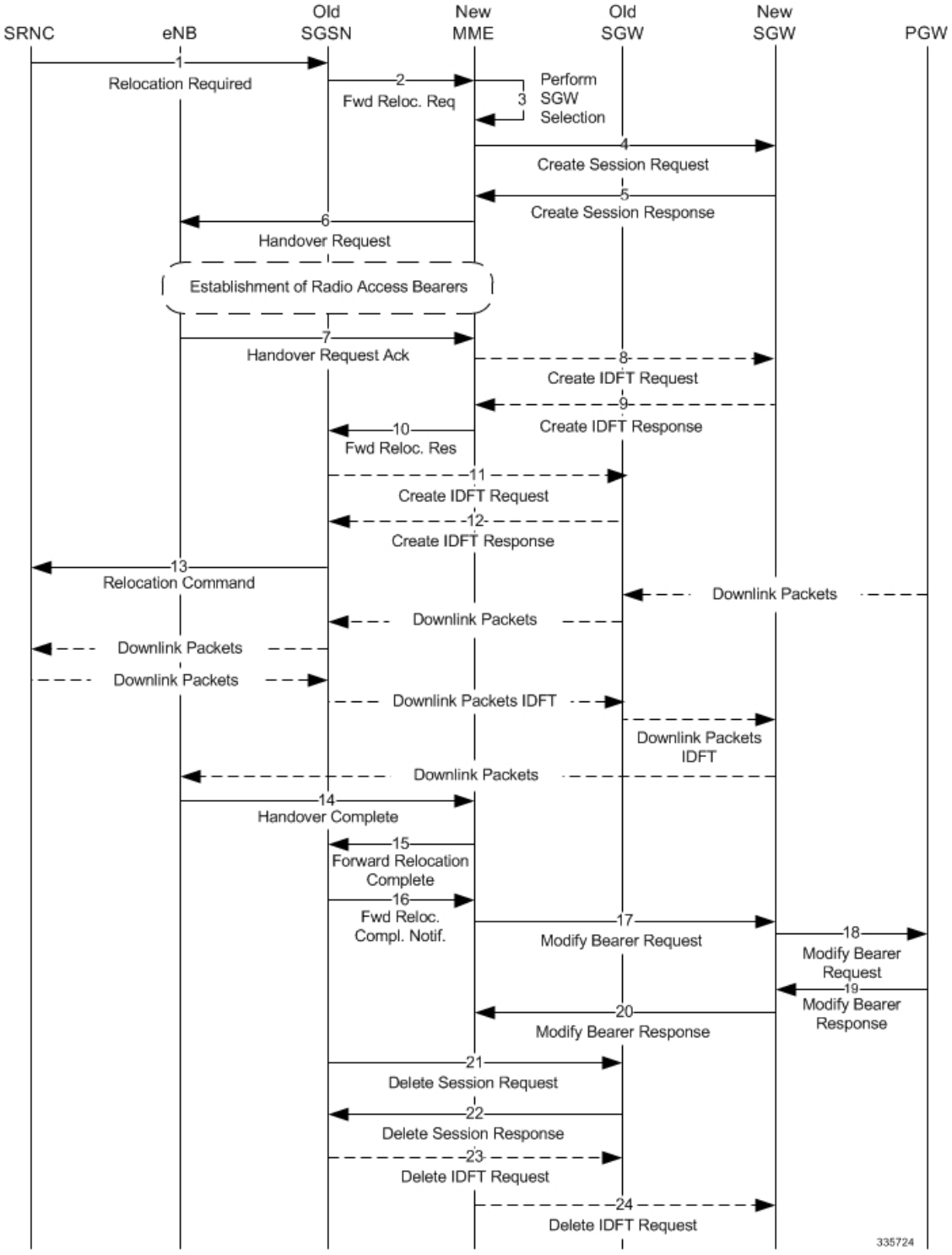


Table 45: S4-SGSN UTRAN to E-UTRAN Connected Mode Handover with SGW Relocation Process Description

Step	Description
1	The old RNC determines that relocation is required for a UE and sends a Relocation Required message to the old SGSN.
2	The old SGSN sends a Forward Relocation Request message to the new MME.
3	The new MME performs the selection of a new SGW.
4	The new MME sends a Create Session Request message to the new SGW.
5	The new SGW sends a Create Session Response to the new MME.
6	The new MME sends a Handover Request message to the eNobeB. At this point radio access bearers are established.
7	The eNodeB sends a Handover Request Ack message to the new MME.
8	The MME sends an Indirect Data Forwarding Tunnel Request to the new SGW.
9	The new SGW sends an Indirect Data Forwarding Tunnel Response to the new MME. The new SGW sends the SGW DL data forwarding TEID to the MME in this message.
10	The new MME sends a Forward Relocation Response message to the old SGSN. The new MME forwards the SGW DL data forwarding TEID received in step 9 to the old SGSN in this message.
11	The old SGSN sends a Create IDFT Request to the old SGW. The old SGSN sends the SGW DL data forwarding TEID received in step 10 to the old SGW in this request. This enables the old SGW to setup an indirect forwarding path towards the new SGW.
12	The old SGW sends a Create IDFT Response to the old SGSN. The old SGW sends the SGW DL data forwarding TEID to the SGSN in this message. The SGSN will forward the re-forwarded downlink packets back to the old SGW to this TEID.

Step	Description
13	The old SGSN sends a Relocation Command to the old RNC. Downlink packets are then routed through the architecture in the following manner: • PGW to old SGW • Old SGW to old SGSN • Old SGSN to old RNC • Old RNC to old SGSN • Old SGSN to old SGW • Old SGW to new SGW • New SGW to eNodeB
14	The eNodeB sends a Handover Complete message to the new MME.
15	The new MME sends a Forward Relocation Complete message to the old SGSN.
16	The old SGSN sends a Forward Relocation Complete Notification message to the new MME.
17	The new MME sends a Modify Bearer Request to the new SGW.
18	The new SGW sends a Modify Bearer Request to the PGW.
19	The PGW sends a Modify Bearer Response to the new SGW.
20	The new SGW sends a Modify Bearer Response to the new MME.
21	After timer expiry, the old SGSN sends a Delete Session Request to the old SGW.
22	The old SGW sends a Delete Session Response to the old SGSN.
23	The old SGSN also sends a Delete IDFT Request to the old SGW.
24	Similar to the timer started at the old SGSN, the new MME also would have started a timer to guard the holding of the IDFT tunnel created there. Upon expiry of this timer, the new MME sends a Delete IDFT Request to the new SGW.

Figure 108: S4-SGSN Inter-SGSN Hard Handover and SGW Relocation (Part 1)

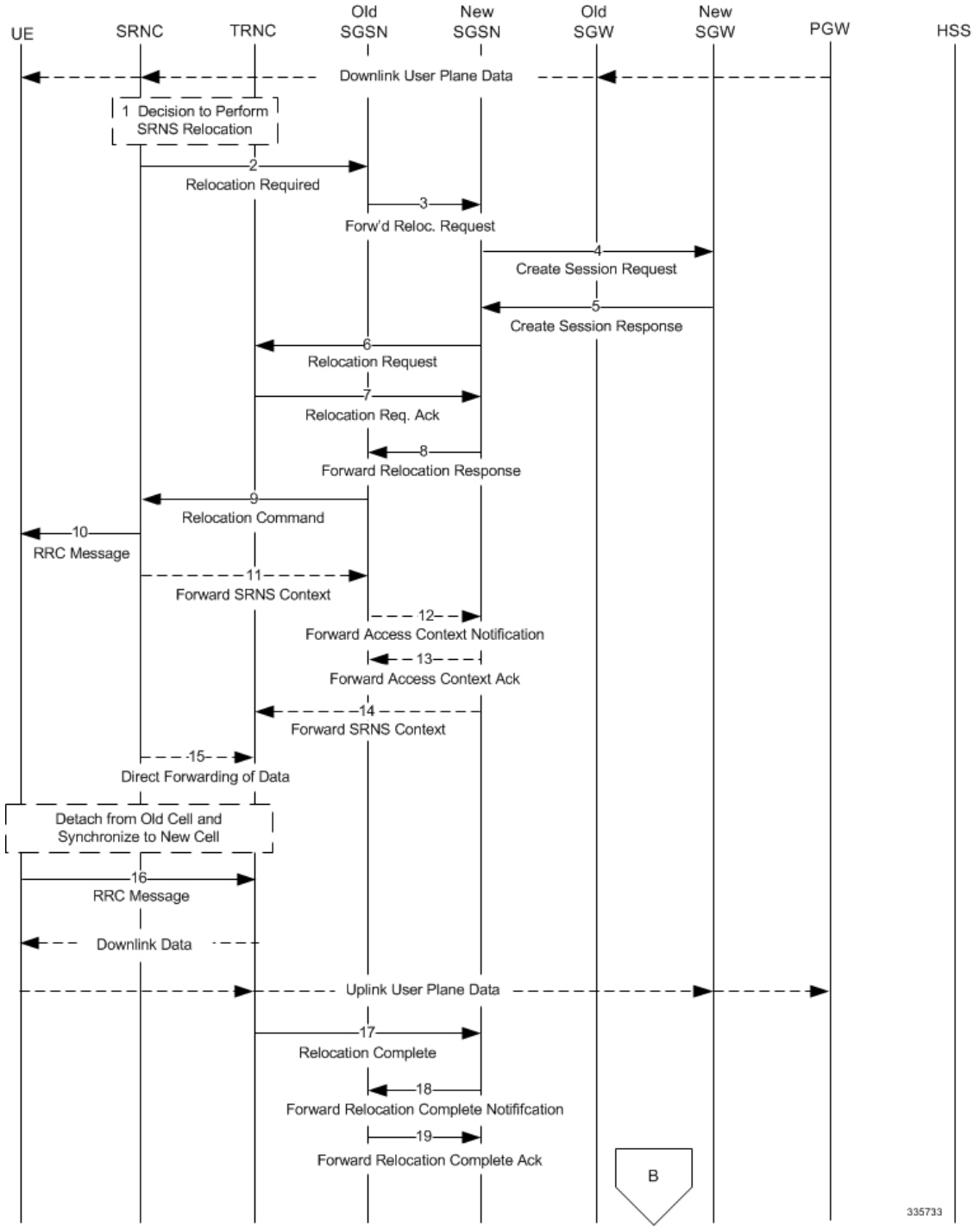


Figure 109: S4-SGSN Inter-SGSN Relocation with Hard Handover and SGW Relocation (Part 2)

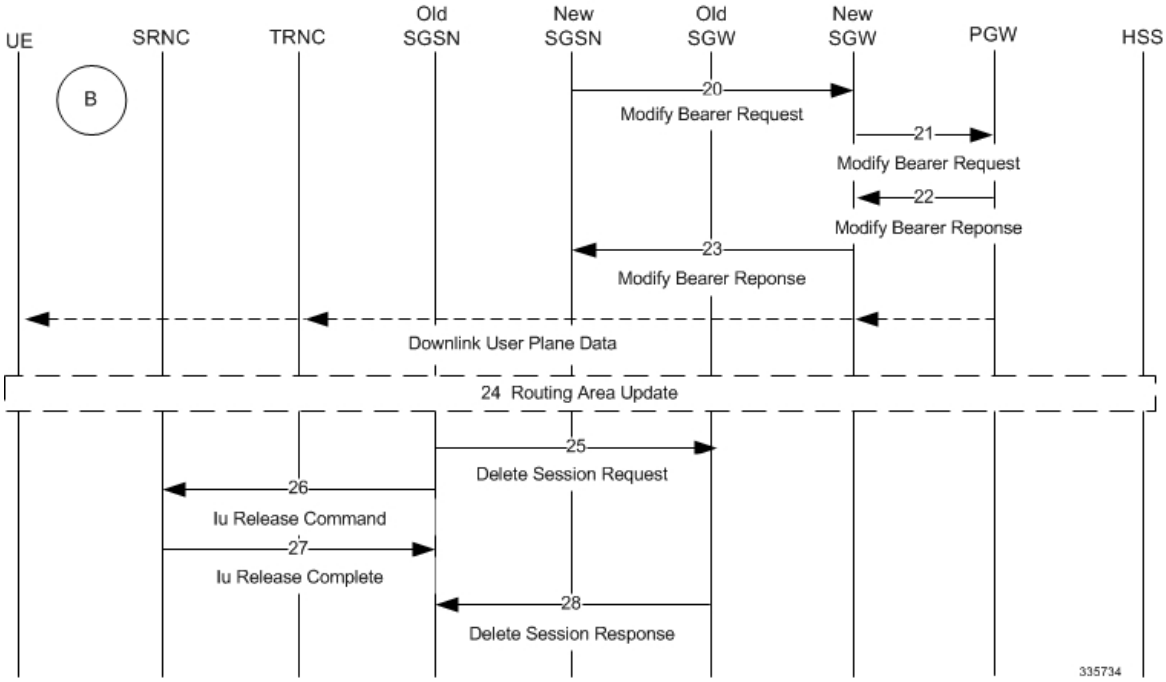


Table 46: S4-SGSN Inter-SGSN Hard Handover with SGW Relocation Process Description

Step	Description
1	The decision is made to initiate relocation.
2	The source RNC sends a Relocation Required message to the target RNC.
3	The old SGSN selects the new SGSN and sends a Forward Relocation Request message to the new SGSN.
4	The new SGSN sends a Create Session Request message to the new SGW.
5	The new SGW sends a Create Session Response back to the new SGSN.
6	The new SGSN sends a Relocation Request message to the new RNC.
7	The new RNC sends a Relocation Request Acknowledgment back to the new SGSN.
8	The new SGSN sends a Forward Relocation Response message to the old SGSN.

Step	Description
9	The old SGSN sends a Relocation Command to the old RNC.
10	The old RNC sends the RRC message to the UE. Upon reception of this message the UE will remove any EPS bearers for which it did not receive the corresponding EPS radio bearers in the target cell.
11	The old RNC sends a Forward SRNS Context message to the old SGSN.
12	The old SGSN sends a Forward Access Context Notification message to the new SGSN.
13	The new SGSN sends a Forward Access Context Acknowledge message to the old SGSN
14	The new SGSN sends a Forward SRNS Context message to the new RNC. At this point, the UE detaches from the old RNC and attaches to the new RNC.
15	The source RNC should start direct forwarding of downlink data from the source RNC towards the target RNC for bearers subject to data forwarding.
16	The UE sends an RRC message to the new RNC. Downlink packets forwarded from the old RNC can be sent to the UE. In addition, uplink packets can be sent from the UE, which are forwarded to the new SGW and then on to the PGW.
17	The new RNC sends a Relocation Complete message to the new SGSN.
18	The new SGSN then ends a Forward Relocation Complete Notification message to the old SGSN.
19	The old SGSN sends a Forward Relocation Complete Acknowledgement message to the new SGSN.
20	The new SGSN sends a Modify Bearer Request message to the new SGW for each PDN connection.
21	The new SGW sends a Modify Bearer Request message to the PGW.
22	The PGW sends a Modify Bearer Response message to the new SGW.

Step	Description
23	The new SGW sends a Modify Bearer Response message to the new SGSN. The PGW begins sending downlink packets to the new SGW, which in turn sends them to the new RNC, and then to the UE.
24	The UE initiates a Routing Area Update procedure. This RAU occurs on a RANAP Direct Transfer and therefore does not involve a Context transfer with the peer SGSN.
25	The old SGSN sends a Delete Session Request to the old SGW.
26	The old SGSN sends an Iu Release Command to the old RNC.
27	The old RNC then sends a Iu Release Complete message to the old SGSN.
28	The old SGW sends a Delete Session Response message to the old SGSN.

Standards Compliance

The SGSN SRNS Relocation feature complies with the following standards:

- **SGSN Gn/Gp SRNS Relocation**: 3GPP TS 23.060 V8.10.0 (2010-09): 3rd Generation Partnership Project Technical Specification Group Services and System Aspects General Packet Radio Service (GPRS) Service description Stage 2 (Release 8)
- **S4-SGSN (S3/S16) SRNS Relocation**: 3GPP TS 23.060 V9.8.0 (2011-03): 3rd Generation Partnership Project Technical Specification Group Services and System Aspects General Packet Radio Service (GPRS) Service description Stage 2 (Release 9)
- **MME to 3G SGSN Hard Handover and Relocation**: LTE General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (3GPP TS 23.401 version 9.8.0 Release 9)

Configuring SRNS Relocation on the SGSN

This section provides examples of how to configure the SRNS relocation feature on the SGSN. An optional configuration example is also provided for enabling IDFT.

Configuring the SRNS Relocation Feature

Configuring the SRNS Relocation feature includes creating a call-control-profile and then enabling intra- and/or inter-SGSN SRNS relocation via the Command Line Interface (CLI).

```
config
 call-control-profile cc-profile name
```

```
 srns-intra all failure-code integer
 srns-inter all failure-code integer
 end
config
      context context_name
            iups-service iups_service_name
                  inter-rnc-procedures source-rnc-as-target
```

Notes:

- *cc-profile-name* is the name assigned to this call-control-profile
- **srns-intra all** enables intra-SGSN SRNS relocations for all location areas.
- **srns-inter all** enables inter-SGSN SRNS relocations for all location areas.
- failure-code *integer* specifies the failure code that applies to SRNS relocations.
- Optionally, operators can use the **restrict** and **allow** keywords to identify specific location areas where SRNS relocation will, or will not, occur. For detailed information on these optional keywords, refer to the *Command Line Reference*.
- **inter-rnc-procedures source-rnc-as-target**: *Optional*. Configures the SGSN to support SRNS relocation for those scenarios where the source RNC is behaving as the target RNC. The default is not to allow SRNS relocation in those scenarios.

Enabling IDFT (Optional, S4-SGSN Only)

To enable support of IDFT between the eNodeB and a specified RNC via the SGW during connected mode handovers on the S4-SGSN:

```
config
 context context_name
 iups-service iups_service_name
 rnc id rnc_id
 no enb-direct-data-forward
 end
```

Where:

- **no enb-direct-data-forward** enables the setup of IDFT between the eNodeB and the RNC via the SGW for connected mode inter RAT handovers. If IDFT is enabled, the SGSN/MME will send the IDFT request towards the SGW.
- To disable IDFT, enter the **enb-direct-data-forward** command.

Verifying the SRNS Feature Configuration

This section describes how to verify that SRNS feature configuration.

The following commands provide information on how the SRNS relocation feature is configured:

```
show call-control-profile full all
show call-control-profile full name cc-profile-name
```

The output of these commands includes the complete SRNS configuration for the specified Call Control Profile. For example:

```
show call-control-profile name cc-profile-name
...      ...      ...
SRNS Intra All                                          :  Allow
```

```
SRNS Intra All Failure Code                    : 10
SRNS Inter All                                                 : Allow
SRNS Inter All Failure Code                    : 15
...      ...      ...
```

The following command provides information on how IDFT is configured:

show iups-service name *service_name*

The output of this command indicates whether IDFT is enabled or disabled for the RNC configuration. If the E-Node Direct Data Forwarding setting reads "Disabled," then IDFT is enabled. If it reads "Enabled," then IDFT is disabled.

show iups-service name *service-name*

```
..      ..      ..
Available RNC:
..      ..      ..
 E-NodeB Direct Data Forwarding        : Disabled
..      ..      ..
```

Monitoring and Troubleshooting SRNS Relocation

This section provides information that assists operators in monitoring and troubleshooting the SRSN Relocation feature.

SRNS Bulk Statistics

The following statistics are included in the SGSN Schema in support of the SRNS Relocation feature. For detailed descriptions of these bulk statistics, refer to the *Statistics and Counters Reference*.

Table 47: SRNS Relocation Feature Bulk Statistics

Bulk Statistics Supporting SRNS Relocation Feature	
SRNS-ctxt-req-sent	srns-ctx-deny-ip-up-failure
SRNS-ctxt-rsp-rcvd	srns-ctx-deny-reloc-alloc-expiry
SRNS-ctxt-req-tmr-expired	srns-ctx-deny-reloc-failure-target-system
SRNS-ctxt-total-pdp-acc	srns-ctx-deny-invalid-rdb-id
SRNS-ctxt-total-pdp-rej	srns-ctx-deny-no-remaining-rab
SRNS-data-fwd-cmd-sent	srns-ctx-deny-interaction-with-other-proc
srns-ctx-deny-rab-preempt	srns-ctx-deny-integrity-check-fail
srns-ctx-deny-reloc-overall-tmr-exp	srns-ctx-deny-req-type-not-supported
srns-ctx-deny-reloc-prep-tmr-exp	srns-ctx-deny-req-superseeded
srns-ctx-deny-reloc-complete-tmr-exp	srns-ctx-deny-rel-due-to-ue-sig-con-rel
srns-ctx-deny-queuing-tmr-exp	srns-ctx-deny-res-optimization-reloc

Bulk Statistics Supporting SRNS Relocation Feature	
srns-ctx-deny-reloc-triggered	srns-ctx-deny-req-info-unavail
srns-ctx-deny-unable-to-est-reloc	srns-ctx-deny-reloc-due-to-radio-reason
srns-ctx-deny-unknown-target-rnc	srns-ctx-deny-reloc-unsupport-target-sys
srns-ctx-deny-reloc-cancel	srns-ctx-deny-directed-retry
srns-ctx-deny-reloc-success	srns-ctx-deny-radio-con-with-ue-lost
srns-ctx-deny-cypher-algo-no-support	srns-ctx-deny-rnc-unable-to-estab-all-rfcs
srns-ctx-deny-conflict-cypher-info	srns-ctx-deny-deciphering-keys-unavail
srns-ctx-deny-failure-radio-if-proc	srns-ctx-deny-dedicated-assist-data-unavail
srns-ctx-deny-rel-utran-reason	srns-ctx-deny-reloc-target-not-allowed
srns-ctx-deny-utran-inactivity	srns-ctx-deny-location-reporting-congestion
srns-ctx-deny-time-crit-relocation	srns-ctx-deny-reduce-load-in-serving-cell
srns-ctx-deny-req-traffic-class-unavail	srns-ctx-deny-no-radio-res-avail-target-cell
srns-ctx-deny-invalid-rab-param-val	srns-ctx-deny-geran-iu-mode-failure
srns-ctx-deny-req-max-bit-rate-unavail	srns-ctx-deny-access-restrict-shared-nwtk
srns-ctx-deny-req-max-bit-rate-dl-unavail	srns-ctx-deny-in-reloc-nwt-support-puesbine
srns-ctx-deny-req-max-bit-rate-ul-unavail	srns-ctx-deny-traffic-target-more-src-cell
srns-ctx-deny-req-gbr-unavail	srns-ctx-deny-mbms-no-multicat-svc-for-ue
srns-ctx-deny-req-gbr-dl-unavail	srns-ctx-deny-mbms-unknown-ue-id
srns-ctx-deny-req-gbr-ul-unavail	srns-ctx-deny-mbms-sess-start-no-data-bearer
srns-ctx-deny-req-trans-delay-not-achieve	srns-ctx-deny-mbms-superseed-nnsf
srns-ctx-deny-inval-rab-param-combo	srns-ctx-deny-mbms-ue-linking-already-done
srns-ctx-deny-violation-for-sdu-param	srns-ctx-deny-mbms-ue-delinking-failure
srns-ctx-deny-violation-traffic-hanlde-prio	srns-ctx-deny-tmgi-unknown
srns-ctx-deny-violation-for-gbr	srns-ctx-deny-ms-unspecified-failure
srns-ctx-deny-usr-plane-ver-unsupported	srns-ctx-deny-no-response-from-rnc

Show Command Output Supporting the SRNS Relocation Feature

This section provides information regarding CLI show commands that provide output to support of the SRSN Relocation feature.

The following show commands are available in support of the SRNS Relocation feature on the SGSN and the S4-SGSN:

show s4-sgsn statistics all

show gmm-sm statistics

The following counters are included in the **show gmm-sm statistics** command output to support the SRNS Relocation feature. These statistics provide information on RAN application messages and the total number of attempted and successful SGSN Gn/Gp and S4-SGSN SRNS relocations. These totals are further subdivided by SRNS relocation type. Note that these statistics apply to the SGSN (Gn/Gp) and the S4-SGSN on the SGSN-RNC-UE interface side. For detailed descriptions of these statistics, refer to the *Statistics and Counters Reference*.

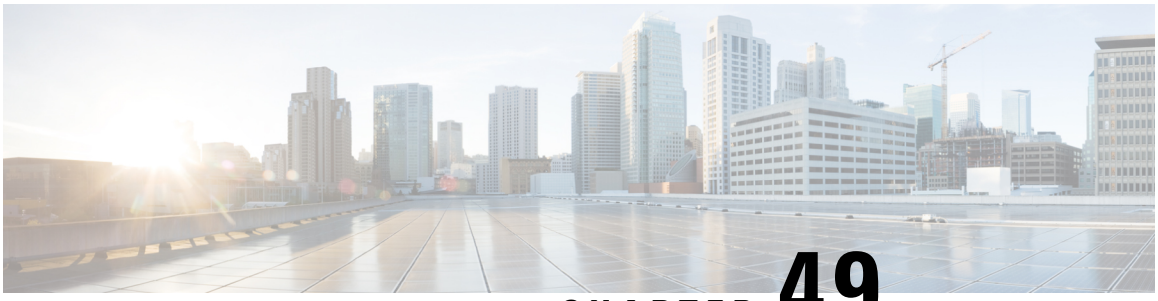
Table 48: GMM SM Statistics Supporting SRNS Relocation

GMM SM Statistics Supporting SRNS Relocation	
RANAP Procedures	
Relocation Required	Relocation Complete
Relocation Request	Relocation Command
Relocation Failure	Relocation Request Ack
Relocation Cancel	Relocation Prep Failure
Relocation Detect	Relocation Cancel Ack
3G-SRNS Stats	
Attempted	Successful
Total SRNS	Total SRNS
Intra-SGSN SRNS	Intra-SGSN SRNS
Intra-SRNS UE involved	Intra-SRNS UE involved
Intra-SRNS UE not involved	Intra-SRNS UE not involved
Inter-SGSN SRNS	Inter-SGSN SRNS
Inter-SRNS UE involved (old SGSN)	Inter-SRNS UE involved (old SGSN)
Inter-SRNS UE not involved (old SGSN)	Inter-SRNS UE not involved (old SGSN)
Inter-SGSN UE involved (new SGSN)	Inter-SGSN UE involved (new SGSN)
Inter-SGSN UE not involved (new SGSN)	Inter-SGSN UE not involved (new SGSN)
Inter-SGSN UE involved (old SGSN with MME)	Inter-SGSN UE involved (old SGSN with MME)
Inter-SGSN UE not involved (old SGSN with MME	Inter-SGSN UE not involved (old SGSN with MME
Inter-SGSN UE involved (new SGSN with MME)	Inter-SGSN UE involved (new SGSN with MME)
Inter-SGSN UE not involved (new SGSN with MME)	Inter-SGSN UE not involved (new SGSN with MME)

The following counters are included in the **show s4-sgsn statistics all** command output in support of the SRNS Relocation feature. These statistics apply to the S4 interface network level. They provide information on the number and type of SRNS SGW relocations, SRNS procedure aborts, and IDFT packets and bytes sent to and from the SGW (if IDFT is enabled). For detailed descriptions of these statistics, refer to the *Statistics and Counters Reference*.

Table 49: Statistics Supporting S4-SGSN SRNS Relocation

Statistics Supporting SRNS Relocation on the S4-SGSN
SGW Relocations
3G Intra SGSN SRNS Relocation
3G Inter SGSN SRNS Relocation (S16)
MME-SGSN SRNS Relocation (S3)
Procedure Abort Statistics
3G Intra SRNS Abort Due to Total CSR Failure
3G New SGSN SRNS Abort Due to Total CSR Failure
GTPU Statistics
IDFT packets to SGW
IDFT packets from SGW
IDFT bytes to SGW
IDFT bytes from SGW



CHAPTER 49

SGSN Support for IMSI Manager Scaling

- Feature Description, on page 559
- How it Works, on page 559
- Configuring Support for Multiple IMSI Managers, on page 560
- Monitoring and Troubleshooting the Multiple IMSI Manager Support, on page 561

Feature Description

The IMSI Manager is a de-multiplex process that selects the Session Manager instance based on the de-multiplex algorithm logic to host a new session. The IMSI Manager process also maintains the mapping of IMSI/F-PTMSI (UE identifier) to the Session Manager instance. Currently only a single instance of the IMSI Manager task is present on the SGSN or SGSN and MME combo nodes. This feature is developed to increase the number of IMSI Manager Instances. The maximum number of IMSI Managers supported on SSI remains at "1". This feature is only supported on Cisco ASR 5500 and VPC-DI platforms.

The IMSI Manager task is a bottleneck during single event performance testing, the Attach/RAU rates are restricted to a lower value than desired on the ASR 5500 platform. The IMSI Manager receives new session requests from the Link Manager (3G) and Gb Manager (2G) processes in the SGSN. It also receives messages from the MME Manager (12 instances) processes in the MME. On DPC2, one instance of IMSI Manager will not be sufficient to support the number of Session Manager Instances on ASR 5500 and VPC-DI platforms. Scaling up the number of IMSI Manager Instances improves the single event performance numbers of SGSN and MME. It also helps in utilizing the full capability of the ASR 5500 and VPC-DI platforms.

How it Works

Detailed Description

The LINKMGR, GBMGR and the MMEMGR select an IMSIMGR instance that needs to be contacted for session setup. Each subscriber session in the Session Manager maintains the IMSIMGR instance number that "hosts" the mapping for this IMSI. This information is required while communicating during audit and session recovery scenarios.

When a single IMSI manager instance is present, there is only one centralized entry point for new calls into the system. Network overload protection is configured using the command "network-overload-protection", new call acceptance rates are configured and controlled using this command. Once the configured rate is

reached the new calls are dropped. When there are multiple IMSI manager instances, the configured new call acceptance rate is distributed equally across all IMSI Manager instances to throttle new calls.

The IMSI manager manages target (NRI and count) based offloading. Though number of IMSI Manager instances is increased, only the first IMSI Manager instance is allowed to perform the target based offloading. It keeps track of the total offloaded subscribers for every Target-NRI from all Session Managers and notifies all the Session Managers on attaining Target-count for that Target-NRI.

Several race handling scenarios like ISRAU-Attach collision scenario, Inter-MME TAU attach (FGUTI) on attach (IMSI) collision scenario and so on can occur, specific measures have been taken to ensure these race handling scenarios are handled correctly in a multiple IMSI Manager instance scenario.

The control plane messaging throughput on the ASR 5500 platform is increased, therefore Performance degradation or congestion is not observed during multiple IMSI Manager instance recovery after a crash or an unplanned card migration. Also mechanisms are devised to ensure there is no impact on Session Manager recovery and Session Manager Thresholding.

The Monitor subscriber next-call option is used to trace the next incoming call into the system. With multiple IMSI Manager instances, the Session Controller now sends the next-call details to IMSI manager instance 1. So the next incoming call through IMSI manager instance "1" is monitored.

The IMSI managers are updated with information on critical parameters that lead to congestion control. The IMSI managers have to inform the congestion status to all Link Managers and Gb Managers. In order to avoid multiple IMSI managers sending information to all Link Managers and Gb Managers, only the first IMSI Manager instance informs the congestion status to all Link Managers and Gb Managers. Also only the first IMSI Manager instance sends the traps indicating congestion status this reduces the number of traps to be sent.

From this release onwards, the Diameter Proxy Server queries the IMSI Manager instances to obtain IMSI/IMEI/MSISDN to Session manager instance mapping information.

Relationships to Other Features

Many SGSN and MME features are based on the assumption that there is only one IMSI Manager and there is only one centralized entry point to the system, this assumption now no longer holds good with multiple IMSI manager instances. Workarounds have been arrived at to ensure there are no changes observed during such scenarios. Examples of such scenarios are listed below:

- **MME per service session limit:** The per MME service session limits are enforced by each IMSI manager instance. The per service session limit is configured by the command **bind s1-mme max-subscribers** *number*.
- **MME traps generated by IMSI Manager:** Each IMSI Manager instance generates traps for new call allowed/disallowed independently. The trap information includes the IMSI Manager instance information

Configuring Support for Multiple IMSI Managers

The following configuration command is used to configure the number of IMSIMGR tasks that are required in the system:

```
config
    task facility imsimgr { avoid-sessmgr-broadcast | max integer_value |
required-sessmgr  no_sess_mgrs | sessmgr-sessions-threshold high-watermark
```

high_value **low-watermark** *low_value* **}**
end

Notes:

- The keyword **max** denotes the number of IMSI managers spawned in the system. This keyword is supported only on ASR 5500 and VPC-DI platforms. A maximum of "4" IMSI Manager can be configured.

Important After you configure the **task facility imsimgr max** command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

- The default number of IMSI Managers supported is "4" on ASR 5500 and VPC-DI platforms.
- This is a boot-time configuration and should be added in the configuration file before any SGSN/MME related configuration is created or any IMSI Manager is started. Run-time configuration of this CLI is not valid. Any such attempt will result in the following error message being displayed:

```
New config requires system restart to be effective. Please save config and restart.
```

- This configuration should be added in the configuration file and the system should be re-loaded to apply this new configuration.

The **sgsn imsimgr** command in the Exec mode initiates audit for managing the SGSN's IMSI manager's (IMSIMgr) IMSI table. The command is updated with a new keyword **instance** to extend support for multiple IMSI Managers. The audit is initiated from only one specified instance of IMSI Manager at a time.

sgsn imsimgr { instance *instance_id* **} { add-record** *imsi* **sessmgr instance** *sessmgr* **| audit-with sessmgr { all | instance** *sessmgr* **} | remove-record** *imsi* **}**

Verifying the Configuration

Execute the **show configuration** command to verify the number of IMSI Managers configured:

```
task facility imsimgr max 4
```

Monitoring and Troubleshooting the Multiple IMSI Manager Support

This section provides information on the show commands available to support this feature.

Multiple IMSI Managers Show Command(s) and/or Outputs

show linkmgr all

The following new parameters are added to this show command to display the statistics for this feature:

- IMSIMGR Selection counters
- IMSIMGR 1
- IMSIMGR 2
- IMSIMGR 3
- IMSIMGR 4

show linkmgr instance parser statistics all

The following new parameters are added to this show command to display the statistics for this feature:

- Messenger Counters
- IMSIMGR Selection counters
- IMSIMGR 1
- IMSIMGR 2
- IMSIMGR 3
- IMSIMGR 4

show gbmgr instance parser statistics all

The following new parameters are added to this show command to display the statistics for this feature:

- Messenger Counters
- IMSIMGR Selection counters
- IMSIMGR 1
- IMSIMGR 2
- IMSIMGR 3
- IMSIMGR 4

show demuxmgr statistics imsimgr verbose

The following new parameter is added to this show command to display the statistics for this feature:

- IMSIMGR instance number

show demux-mgr statistics sgtpcmgr instance < id >

The following new parameters are added to this show command to display the statistics for this feature:

- Interactions with IMSI Manager
- Num requests sent to IMSIMgr
- Num requests not sent to IMSIMgr
- Num requests bounced from IMSIMgr
- Num responses received from IMSIMgr
- Num responses with unknown IMSI
- Num Forwarded Relocation Request forwarded
- Num Relocation Cancel Requests With IMSI forwarded
- Num Forward Relocation Requests rejected by IMSIMGR
- Num Relocation Cancel Requests rejected by IMSIMGR

show session subsystem facility mmemgr instance < id >

New counters are added in the MME manager to count the number of requests sent towards the IMSI managers:

- IMSIMGR Selection counters
- IMSIMGR 1
- IMSIMGR 2
- IMSIMGR 3
- IMSIMGR 4

show subscribers mme-only full all/ show mme-service session full all

The IMSI Manager instance holding the mapping entry for a subscriber session is displayed as part of the subscriber session information:

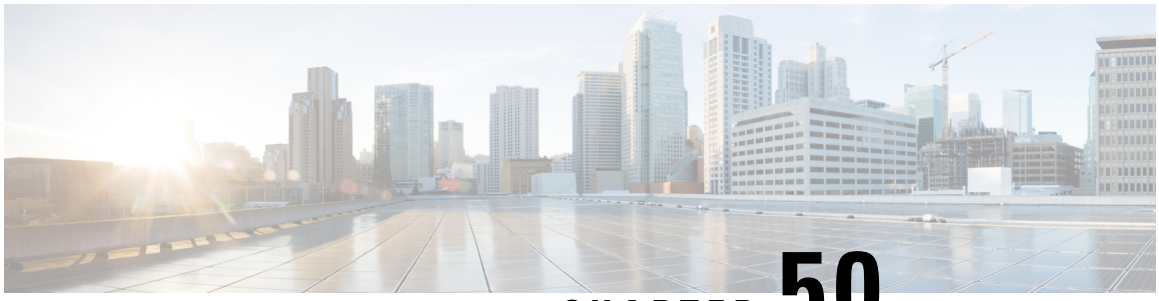
- Imsimgr Instance

show mme-service db record call-id <id>

The following new parameters are added to this show command to display the statistics for this feature:

- Sessmgr Instance
- Imsimgr Instance
- MME Service
- Lookup Keys
- IMSI
- Service-id

show mme-service db record call-id <id>



CHAPTER 50

SGSN Support for Peer-Server Blocking

This chapter describes SGSN support for Peer-Server Blocking.

- Feature Description, on page 565
- How it Works, on page 566
- Configuring Peer-Server Blocking , on page 568
- Monitoring and Troubleshooting the Peer-Server Blocking , on page 569

Feature Description

The validity of SCTP redundancy has to be tested by simulating fail overs when new RNCs/STPs have to be commissioned. Peer-Server Blocking support has been added to prevent any issues during commissioning of new RNCs/STPs.

The Peer Server Blocking feature provides the following functionalities:

1. The SCTP association can be either brought up or down in order to test the redundancy of the same.
2. The PSPs can be brought down without removing the configuration.
3. The SGSN supports a new configuration command under the psp-instance to block/unblock peer endpoint and this configuration is pushed to the Link Manager to achieve peer-server blocking.
4. The SGSN sends a SCTP Shutdown to the remote endpoint and marks the endpoint as LOCKED when the PSP is configured as blocked and if the PSP is in ESTABLISHED state.
5. The SGSN initiates a SCTP INIT when a blocked PSP is un-blocked and if the SGSN is a client and is asp-associated.
6. The SGSN replies with an ABORT when the peer sends INIT in LOCKED state.
7. The SGSN marks the remote endpoint as LOCKED when the PSP is configured as blocked and if the PSP is in a CLOSED state.
8. The PSP state is recovered if the Link Manager expires and no messages are initiated after recovery if the PSP is in locked state.

Supported Number of SCTP Links

The SCTP links are configured as PSP instances per peer server.

In releases prior to 21.5, SGSN supports 12 SCTP links per peer server and 12 Link Manager instances. For a fully loaded chassis with 12 Link Manager Instances, 12 Application Server Processes (ASPs) could be configured with each PSP instance mapped directly to one ASP such that loads get equally distributed and also supports redundancy.

In release 21.5, the number of SCTP links that SGSN supports has been increased from 12 links to 32 links. For configuring more than 12 PSPs, the PSP instances must be mapped in a round-robin technique to the ASPs in order to achieve load distribution.

How it Works

The SCTP associations are between PSPs and ASPs. The control to bring down a SCTP association is added at the PSP level. The option for **shutdown/no shutdown** is added under each PSP configuration. This information is stored in SCT and is forwarded to the Session Controller. The Session Controller sends this configuration request to the Master Link Manager via a messenger call. The Link Manager receives the configuration from the Master Manager. Based on the current association state and the CLI (**shutdown/no shutdown**) issued the following actions are taken:

1. If the CLI **shutdown** is issued, the shutdown flag is set. When the association is in an ESTABLISHED state, the Link Manager initiates a SCTP SHUTDOWN towards the peer and moves to the LOCKED state after shutdown procedure is completed.
2. If the CLI **no shutdown** is issued, the shutdown flag is not set and this serves as a trigger to INIT towards the peer, provided the PSP is already in LOCKED state and SGSN is configured as client. A SCTP INIT is triggered towards the peer. If the association is in any state other than LOCKED state, the configuration is ignored.

The following table provides information on various Peer Server blocking scenarios based on the CLI configuration:

CLI configuration	Current Association State	SGSN Action	Result Association State
shutdown	LOCKED	1. No action taken. 2. Association remains in LOCKED state.	
shutdown	CLOSED	1. Association is marked as LOCKED. 2. SCTP Abort is sent on receiving Init from peer, and the Init is dropped.	LOCKED
shutdown	COOKIE-WAIT	1. Association is marked as LOCKED. 2. SCTP Abort is sent for every subsequent Init from peer.	LOCKED

CLI configuration	Current Association State	SGSN Action	Result Association State
shutdown	COOKIE-ECHOED	1. Association is marked as LOCKED. 2. SCTP Abort is sent on receiving Init from peer and the Init is dropped.	LOCKED
shutdown	ESTABLISHED	1. SCTP SHUTDOWN is initiated 2. The association is moved to the LOCKED state after SCTP shutdown procedure is complete	LOCKED
shutdown	SHUTDOWN-PENDING SHUTDOWN-SENT SHUTDOWN-RECEIVED SHUTDOWN-ACK SENT	Once the SCTP shutdown procedure is completed the association is moved to the LOCKED state.	LOCKED
no shutdown	LOCKED	If SGSN is the client, an INIT is initiated and the association is moved to COOKIE-WAIT state. If SGSN is the server the association is moved to CLOSED state	COOKIE-WAIT (on triggering INIT)/CLOSED
no shutdown	CLOSED COOKIE-WAIT COOKIE-ECHOED ESTABLISHED	No action required.	No change in state
no shutdown	SHUTDOWN-PENDING SHUTDOWN-SENT SHUTDOWN-RECEIVED SHUTDOWN-ACK SENT	No action required, an Error is displayed until the shutdown procedure completed and PSP is moved to either LOCKED state (if the shutdown procedure is due to a previous "shutdown" on PSP) or CLOSED state (if the shutdown is due to some other reason).	No change in state

Configuring Peer-Server Blocking

The following command is used to configure the Peer-Server Blocking feature:

```
config
  ss7-routing-domain routing_domain_id variant variant_type
    peer-server id server_id
      psp instance id
        [ no ] shutdown
        end
```

Notes:

- In release 21.5, the number of SCTP links that SGSN supports has been increased from 12 links to 32 links.

  psp instance *id*: In release 21.5, *id* must be an integer from 1 to 32. In releases prior to 21.5, *id* is an integer from 1 to 12.

- On configuring **shutdown**, the PSP is brought down via a SCTP Shutdown procedure (if association is already ESTABLISHED) or Abort (any other association state) and it is marked LOCKED. The SGSN does not initiate any messages towards the peer and any message from the peer will be responded with a SCTP Abort, when the PSP is in a LOCKED state.
- On configuring **no shutdown**, the PSP is marked unlocked and the SGSN initiates an association establishment towards the peer. This is the default configuration for a PSP. The default is **no shutdown**.

Listed below are the error codes added to support the Peer-Server blocking feature:

- Once the CLI is configured if the operator tries to re-configure the same CLI again, a CLI failure is displayed. This suppresses the Link Manager error logs while trying to push same configuration twice.

  The error code displayed is:

  Failure: PSP: Re-configuring same value

- During an ongoing shutdown procedure if the command **no shutdown** is executed, the execution of the command will be unsuccessful and a CLI failure error message is displayed.

  The error code displayed is:

  Cannot unlock PSP during ongoing shutdown procedure

  This ensures that the shutdown procedure is graceful. The command **no shutdown** can be configured only when there is no ongoing shutdown procedure.

Verifying the Peer-Server Blocking Configuration

Use the following show command to verify the Peer-Server Blocking configuration:

```
show ss7-routing-domain num sctp asp instance num status peer-server id
num peer-server-process instance num
```

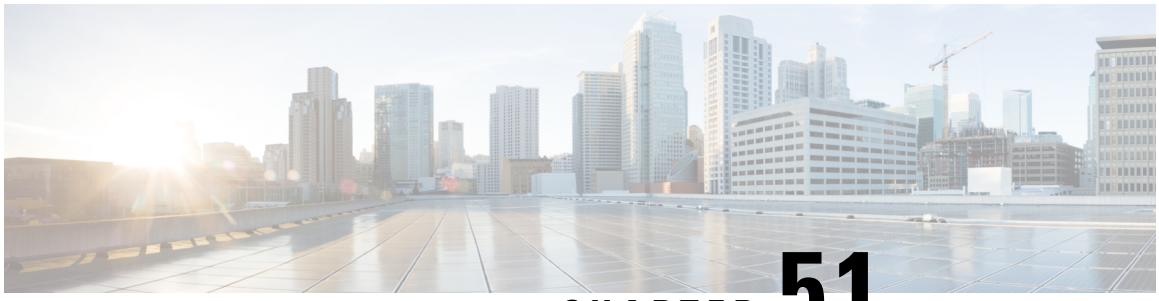
The field **Association State** is displayed as **LOCKED** when the PSP is locked via the **shutdown** CLI.

Monitoring and Troubleshooting the Peer-Server Blocking

The following traps are generated on locking a PSP via **shutdown** CLI:

- SCTPAssociationFail
- M3UAPSPDown
- SS7PCUnavailable
- M3UAPSDown

The trap M3UAPSPDown additionally indicates the cause, the cause value indicated is Administrative-Shutdown.



CHAPTER 51

Support for EPC QoS Attributes on SGSN

- Feature Description, on page 571
- How It Works, on page 572
- Configuring EPC QoS Support on SGSN, on page 573
- Monitoring and Troubleshooting EPC QoS Support on SGSN, on page 574
- Troubleshooting EPC QoS Support on SGSN, on page 575

Feature Description

The Gn-Gp SGSN now supports EPC QoS parameters during PDP Activation/Modification procedures. Support is added for Evolved-ARP, APN-AMBR and UE-AMBR QoS parameters. The purpose of adding this support is to achieve end to end synchronization of QoS parameters during IRAT (3G/4G) mobility procedures. In previous releases it was observed that there is no synchronization between QoS parameters during TAU/RAU mobility from a 4G scenario to a 3G scenario or vice versa.

Overview

The EPC QoS attributes now supported Gn SGSN can be briefly described as below:

Evolved-ARP (E-ARP): Evolved allocation or retention priority specifies the relative importance of a Radio Access Bearers as compared to other Radio Access Bearers for allocation or retention of the Radio access bearer. The EPC uses Evolved ARP, which has priority level ranging from "1" up to "15". Additionally, evolved ARP comprises of pre-emption capability and pre-emption vulnerability. The preemption capability information defines whether a bearer with a lower priority level should be dropped to free up the required resources. The pre-emption vulnerability information indicates whether a bearer is applicable for such dropping by a preemption capable bearer with a higher priority value.

APN-AMBR (per APN Aggregate Maximum Bit Rate): The APN-AMBR limits the aggregate bit rate that can be provided across all Non- GBR PDP contexts of the same APN (for example, excess traffic may get discarded by a rate shaping function). Each of those Non-GBR PDP contexts can potentially utilize the entire APN AMBR (for example, when the other Non- GBR PDP contexts do not carry any traffic). The PGW enforces the APN AMBR in downlink. Enforcement of APN AMBR in uplink may be done in the UE and additionally in the PGW.

UE-AMBR: The UE AMBR limits the aggregate bit rate that can be provided across all Non-GBR PDP contexts of a UE (for example, excess traffic may get discarded by a rate shaping function). Each of the Non-GBR PDP contexts can potentially use the entire UE AMBR (for example, when the other Non-GBR

PDP contexts do not carry any traffic). The GBR (real-time) PDP contexts are outside the scope of UE AMBR. The RAN enforces the UE AMBR in uplink and downlink.

With this feature enhancement the SGSN now supports the following functionalities:

1. EPC QoS parameters for Gn/Gp interface activated PDPs are supported.
2. The Gn-Gp SGSN reads the EPC QoS parameters from the HLR/HSS and the user.
3. The Gn-Gp SGSN now performs capping of the QoS parameters and sends the negotiated values towards the GGSN and RAN.

How It Works

During PDP context activation/modification, Inbound ISRAU/SRNS and Standalone ISDs the SGSN sends negotiated E-ARP and APN-AMBR values to the GGSN. The SGSN reads the Subscribed QoS values from the HSS/HLR and from the user (configured through the CLI commands), based on the QOS capping configured the SGSN caps the QoS values.

The QoS profile configuration mode is used to configure the APN-AMBR values; this mode is now enhanced to configure E-ARP values. The QoS-profile is associated to APN profile which is selected based on the APN name, the QoS profile now contains locally configured E-ARP and APN-AMBR values. The command **prefer-as-cap** is configured to instruct either to take values from HLR/HSS or local configuration or the minimum of these two.

If the APN profile is not configured, E-ARP and APN-AMBR values are same as the subscribed values provided by the HSS/HLR. If E-ARP and APN-AMBR values are locally configured in the QoS profile, subscribed E-ARP and APN-AMBR values are overridden with locally configured values. This enforcement is done for all contexts which are activated in the SGSN for the first time or during Inter SGSN RAU when the user shifts from other SGSNs to our SGSN or during context activation when a user switches from 2G to 3G or vice versa.

The SGSN calculates the authorized UE-AMBR equal to the sum of all the APN-AMBRs. If the calculated UE-AMBR is greater than subscribed value it is capped to subscribed value.

The SGSN sends the negotiated E-ARP and APN-AMBR values in the following GTPV1 messages to the GGSN during PDP activation/modification or when subscription is received with new values of E-ARP and APN-AMBR:

- Create PDP Context Request.
- Update PDP Context Request
- Update PDP Context Response

The SGSN receives the E-ARP and APN-AMBR in the following GTPV1 messages from the GGSN during PDP activation/modification:

- Create PDP Context Response.
- Update PDP Context Response
- Update PDP Context Request

If the GGSN replies with changed values of E-ARP and APN-AMBR then the downgraded values will be accepted immediately, but upgraded values are accepted only if the allow upgrade option is configured through the CLI.

The following CLI under the Call Control Profile is configured to allow upgrade of E-ARP:

override-arp-with-ggsn-arp

If the GGSN replies with changed values of APN-AMBR then the upgrade and downgrade values are accepted unconditionally.

The SGSN sends negotiated E-ARP, UE-AMBR , APN-AMBR in the following GTPV1 messages to the peer SGSN/MME during Inter- SGSN RAU and SRNS procedures:

- SGSN Context Response.
- Forward Relocation Request

The SGSN sends E-ARP and UE-AMBR in the following RANAP messages to RNC during RABs establishment and modification procedures:

- RAB assignment Request.
- RAB Modification Request

Standards Compliance

This feature complies with the following 3GPP standards:

- 3GPP TS 29.060 (version 12.0.0)
- 3GPP TS 25.413 (version 12.0.0)

Configuring EPC QoS Support on SGSN

The following commands are used to configure EPC QoS Support on Gn SGSN:

Configuring QoS Profile to Support EPS QoS Parameters in GTPv1 messages

The following new command has been introduced in the QoS Profile configuration mode to enable or disable the SGSN to send EPC QoS parameters to GGSN:

```
config
  quality-of-service-profile profile_name
    [remove] epc-qos-params-in-gtpv1 { eps-subscription | gprs-subscription
 }
    exit
```

Notes:

- This command is disabled by default.
- On enabling this command E-ARP and APN-AMBR parameters are included in the GTPV1 SM messages towards the GGSN
- If the keyword **eps-subscription** is configured, the EPC QoS parameters from EPS subscription are sent to the GGSN. (Note: This option is not supported in this release)
- If the keyword **gprs-subscription** is configured, E-ARP and APN-AMBR from the GPRS subscription are sent. The UE-AMBR value is read from the user (local capping).

Configure E-ARP values in the Quality of Service Profile

A new keyword is introduced in the **class** command under the QoS profile configuration mode to configure the E-ARP values.

```
config
  [remove] class { background | conversational | interactive | streaming
 } evolved-arp { preemption-capability capability_value |
preemption-vulnerability vulnerability_value | priority-level level_value  }
  exit
```

Notes:

- This command is disabled by default.
- Use the keyword **preemption-capability** to configure the preemption capability value. The value is configured as "0" or "1".
- Use the keyword **preemption-vulnerability** to configure the preemption capability value. The value is configured as "0" or "1".
- Use the keyword **priority-level** to configure the priority level of the E-ARP. The priority can be configured as any value in the range "1" up to "15".

Configure Local Capping in the Quality of Service Profile

The existing command **prefer-as-cap** is used to instruct the SGSN to use either the local or subscription or both-subscription-and-local (lower of either the locally configured QoS bit rate or the subscription received from HLR/HSS) QoS configuration value as the capping value for the QoS parameters.

```
config
 quality-of-service-profile profile_name
  prefer-as-cap [ both-subscription-and-local | subscription | local ]
  exit
```

Configure Override of E-ARP Values Provided by GGSN

The existing command **[remove] override-arp-with-ggsn-arp** under the Call Control Profile is used to enable or disable the ability of the SGSN to override an Allocation/Retention Priority (ARP) value with one received from a GGSN. If there is no authorized Evolved ARP received from the GGSN, by default the SGSN continues to use the legacy ARP included in the Quality of Service (QoS) Profile IE.

```
config
 call-control-profile profile_name
  [remove] override-arp-with-ggsn-arp
  exit
```

Verifying the Configuration

The configuration can be verified by executing the show command **show quality-of-service-profile full all**. The following parameter is displayed if **gprs-subscription** is selected in the **epc-qos-params-in-gtpv1** command:

Sending of epc-qos-params to GGSN : Enabled with GPRS Subs

Monitoring and Troubleshooting EPC QoS Support on SGSN

This section provides information on the show commands available to support this feature.

Show Command(s) and/or Outputs

Listed below are the show outputs and new statistics added for EPC QoS support on SGSN:

show subscriber sgsn-only full all

The following new statistics are added in the **show subscriber sgsn-only full all** command:

- Evolved Allocation/Retention Priority
- Priority level
- Pre-emption Vulnerability
- Pre-emption Capability
- AMBR
- Negotiated APN-AMBR UL
- Negotiated APN-AMBR DL
- Max-Requested-Bandwidth-UL
- Max-Requested-Bandwidth-DL
- Applied UE-AMBR DL

Troubleshooting EPC QoS Support on SGSN

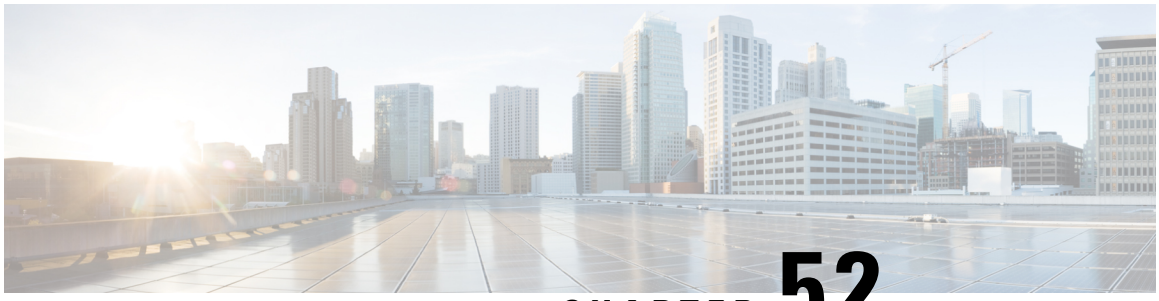
This section provides troubleshooting information for some common scenarios which might occur when EPC QoS parameter support is enabled on the SGSN.

If EPC QoS parameters are not being sent to the GGSN, execute the following troubleshooting procedure:

- Ensure that E-ARP and APN-AMBR values are received in subscription from HLR/HSS.
- Verify if **epc-qos-params-in-gtpv1** command is configured in the QoS profile. Execute the command **show quality-of-service-profile full all** to verify the configuration.The following statistic is displayed based on the configuration:
  - **Sending of epc-qos-params to GGSN : Enabled with GPRS Subs**

If UE-AMBR is not being sent to the RNC, execute the following troubleshooting procedure:

- Ensure that the UE-AMBR is received in subscription from HLR/HSS.
- Verify if sending of UE-AMBR is configured for the RNC. Execute the show command **show iups-service all** to verify the configuration. The following statistic is displayed based on the configuration:
  - **UE Aggregate Maximum Bit Rate : IE included in message**



CHAPTER 52

Support For QoS Upgrade From GGSN or PCRF

This chapter describes the Support for QoS Upgrade feature.

- Feature Description, on page 577
- How it Works, on page 577
- Configuring Support for QoS upgrade from GGSN/PCRF, on page 579

Feature Description

The SGSN negotiates the Requested QoS with Subscribed QoS from HLR (the HLR Subscribed QoS can be over-ridden by the local configuration). The SGSN includes this Negotiated QoS in Create PDP Context Request and Update PDP Context Request messages to the GGSN, the negotiate QoS is capped to the Subscribed QoS and cannot exceed it. The "Upgrade QoS Supported" flag is not set, and the GGSN cannot negotiate a QoS higher than that sent by the SGSN.

This feature enables the functionality, where the SGSN can set the "Upgrade QoS Supported" flag within the common flags IE in Tunnel management messages, Create PDP Context Request and Update PDP Context Request messages. The SGSN accepts the QoS from GGSN in Create PDP Context Response, Update PDP Context Request/Response messages as the Negotiated QoS for the PDP session.

In a 3G scenario, if QoS is downgraded by the RNC then SGSN sets the "No QoS negotiation" flag in the common Flags IE of the corresponding Update PDP Context Request. The "QoS upgrade supported" flag is not set.

How it Works

A new configuration CLI is provided under the APN Profile configuration mode to support the QoS upgrade feature. If this CLI is configured, the SGSN sets the "Upgrade QoS Supported" bit in the Common Flags IE in Create PDP Context Request and Update PDP Context Request. The SGSN accepts the QoS from the GGSN in Create PDP Context Response, Update PDP Context Request/Response as the Negotiated QoS for the PDP session.

A detail description of the implementation of the QoS upgrade feature in various 3G scenarios is provided below:

The "Upgrade QoS Supported" flag in Create PDP Context Request and Response messages

1. During the primary and secondary PDP context activation, if support to send "Upgrade QoS Supported" flag is configured under the APN-Profile, the SGSN sets the flag while sending the Create PDP Context Request.
2. The Create PDP Context Response arrives from the GGSN. If the configuration for "Upgrade QoS Supported" flag is enabled under the APN-Profile, the GGSN requested QoS is handled.

A CLI option is provided to enable or disable the keyword **prefer-as-cap subscription**. Based on the configuration of this keyword, the following QoS processing occurs:

- The keyword **prefer-as-cap subscription** is disabled: The SGSN accepts the QoS in the Create PDP Context Response as the negotiated QoS. This negotiated QoS can be downgraded by the RNC during RAB assignment. If the RNC downgrades the QoS then "Upgrade QoS Supported" flag is not set in the corresponding Update PDP Context Request message.
- The keyword **prefer-as-cap subscription** is enabled: The SGSN negotiates the QoS received in the Create PDP Context Response with the Subscribed QoS. After negotiation if the QoS is downgraded, the "Upgrade QoS Supported" flag not set in the Update PDP Context Request message.

The "Upgrade QoS Supported" flag in Update PDP Context Request and Response messages

If support to send "Upgrade QoS Supported" flag is configured under the APN-Profile and "No QoS negotiation' flag is not set, the SGSN sets the "Upgrade QoS Supported" flag while sending the Update PDP Context Request. The "Upgrade QoS Supported" flag is not set in every Update PDP Context Request, for example, in preservation and direct tunnel this flag is not set in Update PDP Context Request message. The relationship between the "No QoS negotiation" flag and the "Upgrade QoS Supported" flags in Update PDP Context Request messages is summarized as:

- If "No QoS negotiation" flag is set, the "Upgrade QoS Supported" flag is not set.
- If "No QoS negotiation" flag is not set, the "Upgrade QoS Supported" flag is set.

A CLI option is provided to enable or disable the keyword **prefer-as-cap subscription**. Based on the configuration of this keyword, the following QoS processing occurs:

- The keyword **prefer-as-cap subscription** is disabled: The SGSN accepts the QoS in the Create PDP Context Response as the Negotiated QoS. This Negotiated QoS can be downgraded by the RNC during RAB assignment. If the RNC downgrades the QoS then "Upgrade QoS Supported" flag is not set in the corresponding Update PDP Context Request message.
- The keyword **prefer-as-cap subscription** is enabled: The SGSN negotiates the QoS received in the Create PDP Context Response with the Subscribed QoS. After negotiation if the QoS is downgraded, the "Upgrade QoS Supported" flag not set in the Update PDP Context Request message.

A detail description of the implementation of the QoS upgrade feature in various 2G scenarios is provided below:

The "Upgrade QoS Supported" flag for Create PDP Context Request and Response

1. During the primary and secondary PDP context activation, if support to send "Upgrade QoS Supported" flag is configured under the APN-Profile, the SGSN sets the flag while sending the Create PDP Context Request.

2. The Create PDP Context Response arrives from the GGSN. If the configuration for "Upgrade QoS Supported" flag is enabled under the APN-Profile, the GGSN requested QoS is handled.

A CLI option is provided to enable or disable the keyword **prefer-as-cap subscription**. Based on the configuration of this keyword, the following QoS processing occurs:

- The keyword **prefer-as-cap subscription** is disabled: The SGSN accepts the QoS in the Create PDP Context Response as the Negotiated QoS. In an ideal 2G scenario where all the parameters are configured appropriately at the GGSN/PCRF, an upgrade beyond "472" kbps does not occur. If the GGSN sends QoS greater than "472" kbps, this requested bitrate is capped to "472" kbps.
- The keyword **prefer-as-cap subscription** is enabled: The SGSN negotiates the QoS received in the Create PDP Context Response with the Subscribed QoS. After negotiation if the QoS is downgraded, the "Upgrade QoS Supported" flag not set in the Update PDP Context Request message.

The "Upgrade QoS Supported" flag for Update PDP Context Request and Response

If support to send "Upgrade QoS Supported" flag is configured under the APN-Profile and "No QoS negotiation' flag is not set, the SGSN sets the "Upgrade QoS Supported" flag while sending the Update PDP Context Request. The "Upgrade QoS Supported" flag is not set in every Update PDP Context Request, for example, in preservation and direct tunnel this flag is not set in Update PDP Context Request message. The relationship between the "No QoS negotiation" flag and the "Upgrade QoS Supported" flags in Update PDP Context Request messages is summarized as:

- If "No QoS negotiation" flag is set, the "Upgrade QoS Supported" flag is not set.
- If "No QoS negotiation" flag is not set, the "Upgrade QoS Supported" flag is set.

A CLI option is provided to enable or disable the keyword **prefer-as-cap subscription**. Based on the configuration of this keyword, the following QoS processing occurs:

- The keyword **prefer-as-cap subscription** is disabled: The SGSN accepts the QoS in the Create PDP Context Response as the Negotiated QoS. This Negotiated QoS can be downgraded by the RNC during RAB assignment. If the RNC downgrades the QoS then "Upgrade QoS Supported" flag is not set in the corresponding Update PDP Context Request message.
- The keyword **prefer-as-cap subscription** is enabled: The SGSN negotiates the QoS received in the Create PDP Context Response with the Subscribed QoS. After negotiation if the QoS is downgraded, the "Upgrade QoS Supported" flag not set in the Update PDP Context Request message.

Configuring Support for QoS upgrade from GGSN/PCRF

The following command is used to configure the support for QoS upgrade from GGSN/PCRF:

```
config
 apn-profile profile_name
   qos allow-upgrade access-type { gprs | umts }[ prefer-as-cap
subscription ]
   remove qos allow-upgrade access-type { gprs | umts }
   end
```

Notes:

- The "Upgrade QoS Supported" flag is now set in "Create PDP Context" and "Update PDP Context" messages sent by SGSN. The SGSN signals the availability of this functionality by use of the "Upgrade QoS Supported" bit within the Common Flags IE. The SGSN sets the "Upgrade QoS Supported" bit within the Common Flags IE to "1" within the "Create PDP Context" and "Update PDP Context"
- If keyword **prefer-as-cap subscription** is enabled, SGSN accepts a higher QoS in the Create/Update PDP Context Response than sent in Create/Update PDP Context Request, but negotiates and restricts the value within HLR/local subscribed QoS. If this keyword is disabled, the SGSN accepts the QoS in Create PDP Context Response and Update PDP Context Response as the Negotiated QoS (this QoS may be downgraded by the RNC in case of UMTS access).

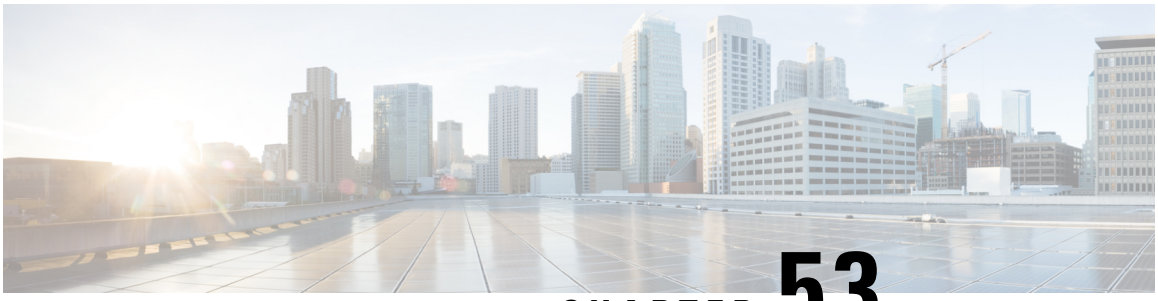
For more information on the command, see *Command Line Interface Reference*.

Verifying the QoS Upgrade Support Configuration

The configuration can be verified by executing the show command **show apn-profile full name <apn_profile_name>**. The following parameters are displayed on executing the command:

1. Allow QoS Upgrade from GGSN
2. QoS Upgrade From GGSN (UMTS)
3. Capped with Subscribed QoS
4. QoS Upgrade From GGSN (GPRS)
5. Capped with Subscribed QoS

For description of the fields listed above see, *Statistics and Counters Reference*.



CHAPTER 53

Support for SGSN QoS based on PLMN, RAT Type

This chapter describes the Support for SGSN QoS based on PLMN, RAT type.

- Feature Description, on page 581
- How it Works, on page 581
- Configuring SGSN Support for RAT Type based QoS Selection , on page 582
- Monitoring and Troubleshooting RAT Type Based QoS Selection, on page 583

Feature Description

SGSN support for QoS selection based on RAT type is introduced through this feature, this functionality improves the Operator Policy based QoS Control capabilities. Currently, the SGSN supports only PLMN based QoS selection. The Operator policy on SGSN allows the operators to control QoS for visiting subscribers (National or International roaming-in subscribers or MVNO subscribers) on an APN basis depending on the PLMN-ID or IMSI range. APN profiles are configured under the Operator Policy as either default for all APN or specific profiles for particular APN.

The following limitations are encountered when only PLMN based QoS selection is supported:

1. When co-locating MME and SGSN into the same node, separate Operator Policy can be configured for E-UTRAN on the MME and both GERAN/UTRAN on the SGSN but not for GERAN and UTRAN separately on the SGSN.
2. The Operator policy currently allows to 'allow' or 'restrict' access to the network based on zone-code (set of LA/SA for 2G/3G and TA for LTE) but does not allow restricting the QoS in specific area of the network based on zone-code.

To overcome the limitations listed above, Operator Policy based QoS Control capabilities are introduced based on RAT-Type or a combination of RAT-Type with PLMN-ID or IMSI range.

How it Works

With the introduction of QoS selection based on RAT type, several QoS profiles can now be configured and associated with the APN profile with the access type marked as either GPRS or UMTS.

Listed below are the SGSN functions now supported for QoS selection:

1. Configuration of QoS based on RAT type

2. Configuration of QoS based on PLMN, this configuration automatically happens as the Operator policy is PLMN based. The QoS Profile is configured on RAT basis.
3. SGSN provides support for configuring APN-AMBR and UE-AMBR per RAT Type.

The SGSN supports configuring all the R99 QoS parameter under the APN profile except for Traffic class. It also supports configuring the R97 QoS parameters namely Delay Class, Reliability class, Peak throughput, Precedence class and Mean Throughput. This configuration is used to over-ride the HLR provided Subscribed QoS value or the configured values are used in combination with subscribed values.

QoS capping has to be performed at various levels like the RAT-Type and PLMN. To achieve QoS capping at different levels, the QoS parameters under the APN profile are also made available under a new profile called the "QoS-profile". The QoS-profile also provides support for over-riding the R97 QoS parameters, Traffic class, UE-AMBR and the APN-AMBR (UE-AMBR and APN-AMBR applicable only for S4-SGSN). This feature enhancement supports backward compatibility.

The QoS Profile can be associated with the APN profile, for each access-type independently or as common to profile.

At the APN profile level, if QoS parameters (R99 parameters except traffic class) as well as a QoS profile are configured, then the QoS profile takes precedence over the QoS parameters.

QoS parameters in QoS profile and APN profile are identical. The new QoS profile provides the modular approach in configuring QoS parameters and associate it to APN Profile per RAT Type.

QoS profile also provides an additional configuration (when compared to apn-profile) named "prefer-tc". This configuration allows the operator to override the Traffic class received in Subscription. "prefer-tc" works closely with "prefer-as-cap" configuration; either:

1. If "prefer-as-cap" is set to both subscription and local then SGSN will negotiate the traffic class configured to traffic class subscribed. Further QoS parameters under this traffic class will be negotiated.
2. If "prefer-as-cap" is set to local then QoS parameters under local configuration will be negotiated with requested for QoS capping.

If operator configures "prefer-tc" then he is expected to configure all the QoS parameters of all traffic class under QoS profile.

Configuring SGSN Support for RAT Type based QoS Selection

This section provides information on configuring SGSN support for QoS selection based on PLMN, RAT Type. The following commands have to be configured to enable RAT type based QoS selection:

Configuring APN Profile and QoS Profile Association

Use the following command to associate an APN profile with a QoS profile:

```
config
 apn-profile profile_name
  associate quality-of-service-profile profile_name access-type [ gprs  |
umts ]
   remove associate quality-of-service-profile profile_name access-type [
```

```
gprs  | umts ]
  exit
```

Notes:

This command is used to associate the specified Quality of Service profile with the APN profile. The access-type must be configured as either **gprs** or **umts**.

Configuring the Quality of Service Profile

Use the following commands under the new CLI configuration mode "Quality of Service Profile" to configure the QoS parameters:

```
config
 quality-of-service-profile <qos_profile_name>
    apn-ambr max-ul mbr-up max-dl mbr-dwn
    remove apn-ambr
    class { background | conversational | interactive | streaming } [
qualif_option ]
    remove class { background | conversational | interactive | streaming
 } [ qualif_option ]
    description description
    remove description
    end
    exit
    prefer-as-cap [ both-subscription-and-local | subscription | local ]
    prefer-tc [ background | conversational | streaming | interactive ]
    remove prefer-tc
    exit
```

For details about the commands listed above, refer to the *Command Line Interface Reference*.

Monitoring and Troubleshooting RAT Type Based QoS Selection

This section provides information on how to monitor the QoS Selection feature and to determine that it is working correctly.

Show Command(s) and/or Outputs

The following show commands are used to monitor this feature:

show apn-profile full [all | name]

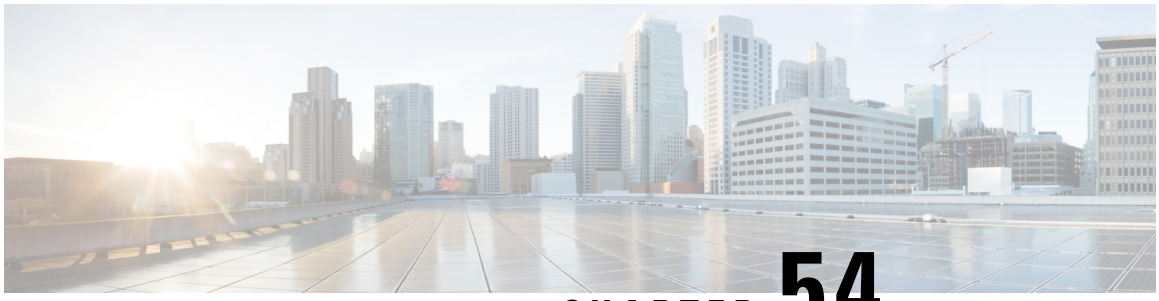
The following parameters are introduced in the **show apn-profile full [all | name]**:

- Associated Quality of Service Profile Name (UMTS)
- Validity
- Associated Quality of Service Profile Name (GPRS)

show quality-of-service-profile [all | full [all | name] | name]

This new show command is introduced to support this feature. The following parameters are displayed on execution of this command:

- QoS Profile Name
- Description
- Preferred Traffic Class
- Quality of Service Capping
- Prefer Type
- Traffic Class
- Sdu delivery order
- Delivery Of Erroneous Sdus
- Max Bit Rate Uplink
- Max Bit Rate Downlink
- Allocation/Retention Priority
- Guaranteed Bit Rate Uplink
- Guaranteed Bit Rate Downlink
- Sdu Max Size
- Minimum Transfer delay
- Sdu Error Ratio
- Residual BE R
- QoS APN-AMBR
- Max uplink
- Max downlink



CHAPTER 54

Support for RAT/Frequency Selection Priority ID (RFSP-ID)

This chapter describes the SGSN Support for RAT/Frequency Selection Priority ID.

- Feature Description, on page 585
- How it Works, on page 585
- Configuring Support for RAT/Frequency Selection Priority ID, on page 588
- Monitoring and Troubleshooting the the Support for RFSP-ID, on page 589

Feature Description

SGSN supports sending of the RAT/Frequency Selection Priority (RFSP ID) from subscription or a local overridden value towards RNC BSC. The RNC/BSC use the subscribed RFSP ID or locally overridden value at the SGSN to choose the Radio frequency. RANAP Direct transfer Extension, RANAP Common ID Extension and DL-Unitdata message will be encoded with RFSP ID. RFSP ID is sent in Common ID message to RNC. RFSP ID is sent in DL-Unitdata PDU and PS handover related messages to BSC. RFSP ID will also be send in BSSGP DL-UNITDATA msg

How it Works

Encoding and De-coding of RFSP Ids in different scenarios

Encoding of RFSP-Id in DL-unit data:RFSP Id is encoded as "Subscriber Profile ID for RAT/Frequency priority" IE in DL-UnitData message as per 3GPP TS 48.018 (version 10.8.0, Section 10.2.1).

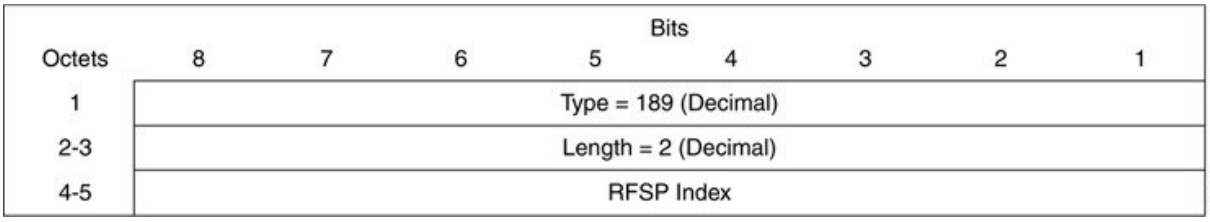
Figure 110: Subscriber Profile ID for RAT/Frequency priority coding

	8	7	6	5	4	3	2	1
Octet 1	IEI							
Octet 2	Length Indicator							
Octet 3	Octet 3 contains the value part of the Subscriber Profile ID for RAT/Frequency priority IE.							

382460

Encoding of Subscribed RFSP Index and RFSP Id in GTPC-V1 messages: RFSP ID will be encoded in GTPC-V1 message as per 3GPP TS 29.060 (version 11.8.0 Release 11, Section 7.7.88)

Figure 111: Encoding of Subscribed RFSP Id in GTPC-V1 messages



De-coding of RFSP-ID in a MAP message: The RFSP-Id in EPS-Subscription Data IE is received as part of Insert Subscriber Data request for Gn/Gp SGSN. The decoding of RFSP-Id is done as per 3GPP TS 29.272 (Version 11.9.0, Section 7.3.46).

De-coding of RFSP-Id AVP in Subscription data from the S6d interface: The RFSP ID is grouped in Subscription Data AVP on receiving ULA from HSS over the S6d interface. This is used in the S4-SGSN. This AVP is of type Unsigned 32 as per 3GPP TS 29.272 (Version 11.9.0, Section 7.3.46).

In the SGSN MAP module, the MAP module is enhanced to de-code the RFSP-Id in Insert Subscriber Data request as part of Update GPRS Location procedure. Since RFSP-Id and APN profile are optional parameters the DB record will be updated as follows:

1. If RFSP ID is present in EPS subscription and the override value is present in the Call Control Profile for that RFSP-Id then the RFSP-Id is modified with the overridden value and stored in the mm-ctxt DB parameter. If override value is not present in the Call Control Profile for RFSP-Id then RFSP Id received in ISD request is used.
2. If RFSP-Id is not present in the EPS Subscription, then default override RFSP-Id is used.

In the 3G Access module, the RFSP ID for the UE is sent to the RNC through the following RANAP IEs:

- **Common ID IE:**

  Before setting up the RRC connection RNC needs to be notified with RFSP ID, the RFSP ID is sent to the RNC using Common ID procedure. The Common ID is sent during Attach, RAU and Service request.

- **Direct Transfer IE:**

  If there is a change in the RFSP ID, the RNC is notified with the RFSP-ID in the Direct Transfer message. Along with the direct transfer IE, the latest value of the RFSP ID is notified to the RNC (for example, after GLU, ULR/ULA procedure).

- **Source RNC-To Target RNC-Transparent Container-Ext IE:**

  The Subscriber Profile ID for RFP IE is transferred from Source RNC to Target RNC as a part of Source RNC-To Target RNC-Transparent Container-Ext IE during SRNS re-location procedure.

In the 3G MM module, during Attach the default RFSP-ID is sent in the Common ID. message towards RNC before retrieving Subscription data from HLR. The RFSP-ID will be fetched from EPS Subscription Data. RFSP-ID will be overridden based on:

1. If RFSP-ID is present in EPS subscription and the override value is present in the Call Control Profile for that RFSP-ID then the RFSP-ID is modified with the overridden value and stored in the mm-ctxt DB parameter. If override value is not present in the Call Control Profile for RFSP-ID then RFSP-ID received in ISD request is used.

2. If RFSP-ID is not present in the EPS Subscription, then default override RFSP-ID is used.

The final RFSP ID is encoded as "Subscriber Profile ID for RAT/Frequency priority" as per 3GPP TS 48.018 (Section 10.2.1) in the next Direct transfer message containing Attach Accept.

In a 2G module, the DL-data unit messages are encoded with RFSP-ID as "Subscriber Profile ID for RAT/Frequency priority" IE in DL-UnitData message as per 3GPP TS 48.018 (Section 10.2.1).

Idle Mode Handover

Consider the following Idle Mode Handover scenarios:

- **Inter-SGSN RAU New SGSN**

  Subscriber moves to a Gn/Gp SGSN

  - Routing Area Update request is received at the Gn/Gp SGSN.
  - After DNS, the old node found to be a Gn/Gp SGSN.
  - The new SGSN sends a Context request in the SGSN Context Request (GTPv1) to the old SGSN.
  - New SGSN decodes the Context Response in GTPv1 format for the RFSP ID and overrides the same. The RFSP ID is then stored in the mm-context.

  Subscriber moves to S4-SGSN

  The Routing Area Update request is received at the S4-SGSN, SGSN sends the Context Request to Old SGSN:

  1. After DNS the old node found to be Gn/Gp SGSN. The S4-SGSN sends the Context request in SGSN Context Request (GTPv1) to the old SGSN. The new SGSN decodes the Context Response in GTPv1 format for the RFSP ID and overrides the same. The RFSP ID is then stored in the mm-context.
  2. After DNS the old node found to be S4 SGSN/MME, the new SGSN sends the Context request in SGSN Context Request (GTPv2) to the S4-SGSN/MME. The new SGSN decodes the Context Response in GTPv2 format for the RFSP ID and override the same. The RFSP ID is then stored in the mm-context.

- **Inter-SGSN RAU Old SGSN**

  When a SGSN receives the Context request in GTPv1 format, the SGSN Context response is sent back to the sender SGSN in GTPv1 format with RFSP ID encoded as per the 3GPP TS 29.060 (Release 8, Version 8.16.0, Section 7.7.88) in mm-context.

  When a SGSN receives the Context request in GTPv2 format, the SGSN Context response is sent back to the sender SGSN in GTPv2 format with RFSP ID encoded.

Connected Mode Handover

- **Inter-SRNS New SGSN**

  When a Gn/Gp-SGSN receives a Forwards Relocation Request from the Old SGSN as a result of the SRNS Re-location Procedure, it decodes the RFSP ID from the GTPv1 formatted message and applies overriding policy before saving it in the mm-context.

  When a S4-SGSN receives Forwards Re-location Request from an Old Gn/Gp SGSN as a result of SRNS Re-location Procedure, it decodes the RFSP ID from the GTPv1 formatted message and applies the overriding policy before saving it in the mm-context.

  When a S4-SGSN receives a Forwards Re-location Request from an Old S4-SGSN/MME as a result of SRNS Re-location Procedure, it decodes the RFSP ID from GTPv2 formatted message and applies the overriding policy before saving it in the mm-context.

- **Inter-SRNS old SGSN**

  When a Gn/Gp SGSN receives a re-location request from the RNC as a part of the SRNS Re-location Procedure, it encodes the Forward Relocation Request with RFSP ID in GTPv1 formatted message.

  When a S4-SGSN receives a re-location request from the RNC as a part of the SRNS Re-location Procedure, it encodes the Forward Re-location Request with RFSP ID in GTPv2 formatted message.

Standards Compliance

This feature complies with the following standards:

- 3GPP TS 48.018 (Release 8)
- 3GPP TS 23.060 (Release 8)
- 3GPP TS 25.413 (Release 8)
- 3GPP TS 29.002 (Release 8)
- 3GPP TS 29.272 (Release 8)
- 3GPP TS 25.413 (version 11.5.0)
- 3GPP TS 48.018 (version 10.8.0)
- 3GPP TS 29.060 (version 11.8.0)
- 3GPP TS 29.272 (version 11.9.0)
- 3GPP TS 29.002 (version 11.7.0)

Configuring Support for RAT/Frequency Selection Priority ID

Listed below are the commands to configure the support for RFSP ID:

1. This command configures the RAT frequency selection priority override parameters for this call control profile. A new keyword **eutran-ho-restricted** *value* has been introduced to configure the value for RAT frequency selection priority when Handover to EUTRAN is restricted.

   ```
   config
    call-control profile profile_name
               rfsp-override { default value | eutran-ho-restricted value
   | ue-val value new-val value + }
               remove rfsp-override { default  | eutran-ho-restricted |
   ue-val value }
             exit
   ```

2. This command is introduced to enable or disable the inclusion of the Subscriber Profile ID for RAT/Frequency priority IE in RANAP Direct transfer Extension and Common Id. Extension messages.

   ```
   config
    context <context_name>
    iups_service <service_name>
    rnc id rnc_id
   ```

```
ranap rfsp-id-ie
no ranap rfsp-id-ie
                exit
```

3. Configure this command to exclude or include RAT/Frequency Selection Priority (RFSP ID) in BSSGP DL-Unitdata messages to the BSC.

```
config
 sgsn-global
 bssgp-message dl-unitdata rfsp-id exclude
 default bssgp-message dl-unitdata rfsp-id exclude
         exit
```

For more information on the commands see, *Command Line Interface Reference*.

Monitoring and Troubleshooting the the Support for RFSP-ID

Use the commands listed below to monitor and/or troubleshoot the support for RFSP ID.

Show Command(s) and/or Outputs

This section provides information regarding show commands and/or their outputs in support of the RFSP ID:

show call-control profile

The following new field is added in the show output to display the configured value for RAT frequency selection priority when Handover to EUTRAN is restricted:

- Rfsp-override eutran-ho-restricted

show subscribers sgsn-only full all

The following new field is added in the show output to display the value of the RFSD Id. Used:

- RFSP Id in Use

show subscribers gprs-only full all

The following new field is added in the show output to display the value of the RFSD Id. Used:

- RFSP Id in Use

show iups-service name

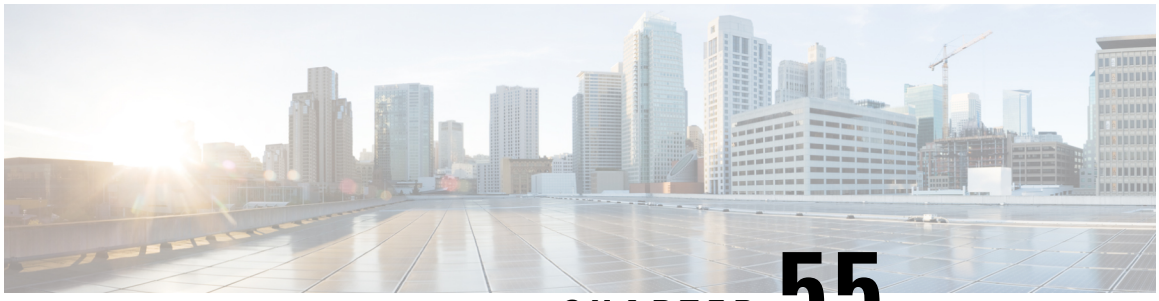
The following new field is added in the show output to display if the Subscriber Profile ID for RAT/Frequency priority IE is included or not in the outbound RANAP Direct transfer Extension and Common Id Extension message:

- RFSP ID

show sgsn-mode

The following new field is added in the show output to display if the RFSP ID is either included or excluded in BSSGP DL-Unitdata messages to the BSC:

- DL Unitdata Tx



CHAPTER 55

Subscriber Overcharging Protection

Subscriber Overcharging Protection is a proprietary, enhanced feature that prevents subscribers in UMTS networks from being overcharged when a loss of radio coverage (LORC) occurs. This chapter indicates how the feature is implemented on various systems and provides feature configuration procedures. Products supporting subscriber overcharging protection include Cisco's Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN).

The individual product administration guides provide examples and procedures for configuration of basic services. Before using the procedures in this chapter, we recommend that you select the configuration example that best meets your service model, and configure the required elements for that model, as described in the respective guide.

Important Subscriber Overcharging Protection is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

This chapter covers the following topics in support of the Subscriber Overcharging Protection feature:

- Feature Overview, on page 591
- Overcharging Protection - GGSN Configuration, on page 593
- Overcharging Protection - SGSN Configuration, on page 594

Feature Overview

Subscriber Overcharging Protection enables the SGSN to avoid overcharging the subscriber if/when a loss of radio coverage (LORC) occurs.

When a mobile is streaming or downloading files from external sources (for example, via a background or interactive traffic class) and the mobile goes out of radio coverage, the GGSN is unaware of such loss of connectivity and continues to forward the downlink packets to the SGSN.

Previously, upon loss of radio coverage (LORC), the SGSN did not perform the UPC procedure to set QoS to 0kbps, as it does when the traffic class is either streaming or conversational. Therefore, when the SGSN did a Paging Request, if the mobile did not respond the SGSN would simply drop the packets without notifying the GGSN; the G-CDR would have increased counts but the S-CDR would not, causing overcharges when operators charged the subscribers based on the G-CDR.

Now operators can accommodate this situation, they can configure the SGSN to set QoS to 0kbps, or to a negotiated value, upon detecting the loss of radio coverage. The overcharging protection feature relies upon the SGSN adding a proprietary private extension to GTP LORC Intimation IE to messages. This LORC Intimation IE is included in UPCQ, DPCQ, DPCR, and SGSN Context Response GTP messages. One of the functions of these messages is to notify the GGSN to prevent overcharging.

The GGSN becomes aware of the LORC status by recognizing the message from the SGSN and discards the downlink packets if LORC status indicates loss of radio coverage or stops discarding downlink packets if LORC status indicates gain of radio coverage for the UE.

The following table summarizes the SGSN's actions when radio coverage is lost or regained and LORC overcharging protection is enabled.

Table 50: LORC Conditions and Overcharging Protection

Condition	Triggered by	SGSN Action	LORC Intimation IE - private extension payload
Loss of radio coverage (LORC)	RNC sends Iu release request with cause code matching configured value	Send UPCQ to GGSN Start counting unsent packets/bytes Stop forwarding packets in downlink direction	No payload
Mobile regains coverage in same SGSN area	MS/SGSN	Send UPCQ to GGSN Stop counting unsent packets/bytes Stop discarding downlink packets	New loss-of-radio-coverage state and unsent packet/byte counts
Mobile regains coverage in different SGSN area	MS/SGSN	Send SGSN Context Response message to new SGSN Stop counting unsent packets/bytes	Unsent packet/byte counts
PDP deactivated during LORC	MS/SGSN	Send DPCQ to GGSN Stop counting unsent packets/bytes	Unsent packet/byte counts
PDP deactivated during LORC	GGSN	Send DPCR to GGSN Stop counting unsent packets/bytes	Unsent packet/byte counts

Triggering Iu Release Procedure

When SGSN receives the RAB Release Request with cause "Radio Connection with UE Lost" from RNC, it triggers the Iu Release Command. RNC then sends the Iu Release Complete message to SGSN.

SGSN proceeds with the following steps when it receives the RAB Release Request with cause "Radio Connection with UE Lost":

- SGSN verifies if the **ranap rabrel-with-radiolost** CLI command is enabled.
- If the **ranap rabrel-with-radiolost** CLI command is enabled, then SGSN triggers the Iu Release Command towards the RNC to release the Iu connection for that specific UE.

Overcharging Protection - GGSN Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the GGSN to support subscriber overcharging protection.

Important This section provides the minimum instruction set to configure the GGSN to avoid the overcharging due to loss of radio coverage in UMTS network. For this feature to be operational, you must also implement the configuration indicated in the section *Overcharging Protection - SGSN Configuration* also in this chapter. Commands that configure additional function for this feature are provided in the *Command Line Interface Reference*.

These instructions assume that you have already configured the system-level configuration as described in *System Administration Guide* and the *Gateway GPRS Support Node Administration Guide*.

To configure the system to support overcharging protection on LORC in the GGSN service:

Step 1 Configure the GTP-C private extension in a GGSN service by applying the example configurations presented in the *GTP-C Private Extension Configuration* section below.

Step 2 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Step 3 Verify configuration of overcharging protection on LORC related parameters by applying the commands provided in the *Verifying Your GGSN Configuration* section in this chapter.

GTP-C Private Extension Configuration

This section provides the configuration example to configure the GTP-C private extensions for GGSN service:

```
configure
  context vpn_context_name
    ggsn-service ggsn_svc_name
      gtpc private-extension loss-of-radio-coverage
      end
```

Notes:

- *vpn_context_name* is the name of the system context where specific GGSN service is configured. For more information, refer *Gateway GPRS Support Node Administration Guide*.
- *ggsn_svc_name* is the name of the GGSN service where you want to enable the overcharging protection for subscribers due to LORC.

Verifying Your GGSN Configuration

This section explains how to display and review the configurations after saving them in a *.cfg* file (as described in the *Verifying and Saving Your Configuration* chapter in this book) and how to retrieve errors and warnings within an active configuration for a service.

Important All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the overcharging protection support configuration.

Step 1 Verify that your overcharging support is configured properly by entering the following command in Exec Mode:

show ggsn-service name *ggsn_svc_name*

The output of this command displays the configuration for overcharging protection configured in the GGSN service *ggsn_svc_name*.

```
Service name:                          ggsn_svc1
    Context:                           service
    Accounting Context Name:           service
    Bind:                              Done
    Local IP Address:  192.169.1.1         Local IP Port:   2123
...
...
    GTP Private Extensions:
        Preservation Mode
        LORC State
```

Step 2 Verify that GTP-C private extension is configured properly for GGSN subscribers by entering the following command in Exec Mode:

show subscribers ggsn-only full

The output of this command displays the LORC state information and number of out packets dropped due to LORC.

Overcharging Protection - SGSN Configuration

This section provides a high-level series of steps and the associated configuration examples for configuring the SGSN to support subscriber overcharging protection.

Important This section provides a minimum instruction set to configure the SGSN to implement this feature. For this feature to be operational, you must also implement the configuration indicated in the section *Overcharging Protection - GGSN Configuration* also in this chapter.

Command details can be found in the *Command Line Interface Reference*.

These instructions assume that you have already completed:

- the system-level configuration as described in the *System Administration Guide*,

- the SGSN service configuration as described in the *Serving GPRS Support Node Administration Guide*, and
- the configuration of an APN profile as described in the *Operator Policy* chapter in this guide.

To configure the SGSN to support subscriber overcharging protection:

Step 1 Configure the private extension IE with LORC in an APN profile by applying the example configurations presented in the *Private Extension IE Configuration* section.

Note An APN profile is a component of the Operator Policy feature implementation. To implement this feature, an APN profile must be created and *associated* with an operator policy. For details, refer to the *Operator Policy* chapter in this book.

Step 2 Configure the RANAP cause that should trigger this UPCQ message by applying the example configurations presented in the *RANAP Cause Trigger Configuration* section.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Step 4 Verify the SGSN portion of the configuration for overcharging protection on LORC related parameters by applying the commands provided in the *Verifying the Feature Configuration* section.

Private Extension IE Configuration

This section provides the configuration example to enable adding the private extension IE that will be included in the messages sent by the SGSN when a loss of radio coverage occurs in the UMTS network:

```
configure
  apn-profile apn_profile_name
    gtp private-extension loss-of-radio-coverage send-to-ggsn
    end
```

Note:

- *apn_profile_name* is the name of a previously configured APN profile. For more information, refer to the *Operator Policy* chapter, also in this book.

RANAP Cause Trigger Configuration

This section provides the configuration example to enable the RANAP cause trigger and define the trigger message value:

```
configure
  context context_name
    iups-service iups_service_name
      loss-of-radio-coverage ranap-cause cause
      end
```

Notes:

- *context_name* is the name of the previously configured context in which the IuPS service has been configured.

- *cause* is an integer from 1 to 512 (the range of reasons is a part of the set defined by 3GPP TS 25.413) that allows configuration of the RANAP Iu release cause code to be included in messages. Default is 46 (MS/UE radio connection lost).

RANAP RAB Release Configuration

This section provides the configuration example to configure the Iu Release Command when SGSN receives the RAB Release Request with cause 46 (radio connection with UE lost) is received.

```
configure
  context context_name
    iups-service iups_service_name
      rnc id
        [ no ] ranap rab-release-with-radiolost
        end
```

Notes:

- When **no ranap rab-release-with-radiolost** is configured, SGSN will send the RAB Assignment Request with RAB Release to RNC.
- This command is disabled by default.
- This command applies to Gn-SGSN only.

Verifying the Configuration

Execute the following command to verify the configuration of this feature:

```
show iups-service all
```

The **Rab release with Radio lost** field in the output of this command indicates whether RAB Release Request with cause 46 is enabled or disabled.

Verifying the Feature Configuration

This section explains how to display the configurations after saving them in a *.cfg* file as described in the *Verifying and Saving Your Configuration* chapter elsewhere in this guide.

Important All commands listed here are under Exec mode. Not all commands are available on all platforms.

These instructions are used to verify the overcharging protection support configuration.

Step 1 Verify that your overcharging support is configured properly by entering the following command in Exec Mode:

```
show apn-profile full name apn_profile_name
```

The output of this command displays the entire configuration for the APN profile configuration. Only the portion related to overcharging protection configuration in the SGSN is displayed below. Note that the profile name is an example:

```
APN Profile name:               : apnprofile1
Resolution Priority:            : dns-fallback
```

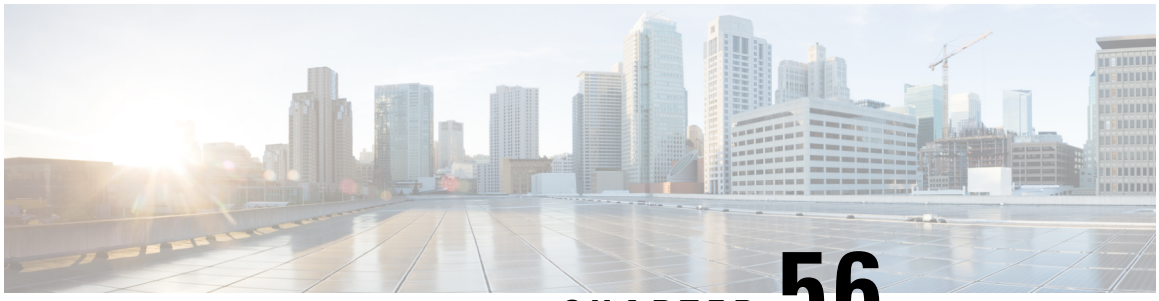
```
...
...
Sending Private Extension Loss of Radio Coverage IE
      To GGSN                   :  Enabled
      To SGSN                   :  Enabled
```

Step 2 Verify the RANAP Iu release cause configuration by entering the following command in the Exec Mode:

show iups-service name *iups_service_name*

The output of this command displays the entire configuration for the IuPS service configuration. Only the portion related to overcharging protection configuration (at the end of the display) is displayed below. Note that the IuPS service name is an example:

```
Service name                  : iups1
Service-ID                    : 1
...
...
Loss of Radio Coverage
Detection Cause in Iu Release : 46
```



CHAPTER 56

Topology-based Gateway Selection

This chapter provides information about the Topology-based Gateway (GW) Selection feature supported by both the Gn/Gp-SGSN and the S4-SGSN. The feature enables an SGSN to select a co-located GW node or topologically (geographically) closer GW nodes.

- Feature Description, on page 599
- How It Works, on page 600
- Configuring Topology-based GW Selection , on page 602
- Monitoring Topology-based GW Selection, on page 604

Feature Description

Topology-based GGSN or co-located P-GW selection is provided in the Gn/Gp-SGSN and topology-based P-GW and S-GW selection is provided in the S4-SGSN.

Selecting a co-located or topologically (geographically) close GW node results in lower latency and prevents unnecessary traversal of the packets in the network.

For the Gn/Gp-SGSN

For the Gn/Gp-SGSN, topology-based GW selection is supported for the following call flows:

- **1st Primary Activation** to select the GGSN or co-located P-GW that is topologically (geographically) closer to the SGSN.
- **Subsequent Primary Activation** to select the GGSN or co-located P-GW that is topologically closer to the SGSN.

Important If there are multiple PDN connections, topology-based selection begins on the first active GGSN or co-located P-GW.

For the S4-SGSN

For the S4-SGSN, topology-based GW selection is supported for the following call flows:

- **1st Primary Activation** to select the topologically closer or co-located S-GW / P-GW node pair.
- **Subsequent Primary Activation** to select the P-GW that is topologically closer or co-located to the already selected SGW.

- **Intra RAU** to select the S-GW that is topologically closer or co-located to the already selected P-GW.
- **Intra SRNS** to select the S-GW that is topologically closer or co-located to the already selected P-GW.
- **Inter New SGSN RAU** to select the S-GW that is topologically closer or co-located to the already selected P-GW.
- **Inter New SRNS** to select the S-GW that is topologically closer or co-located to the already selected P-GW.
- **IRAT** to select the S-GW that is topologically closer or co-located to the already selected P-GW.

Important If there are multiple PDN connections, topology-based GW selection begins on the first active P-GW.

How It Works

Selection of a co-located node or a topologically closer node is based on string comparison of canonical node names included in two or more sets of records received in a DNS S-NAPTR query result.

A canonical node name (a multi-labeled substring of the hostname) is a unique name representing a node. For comparison, the canonical node names are derived from the hostnames received in the DNS records. For co-located nodes, the canonical node names strings must be exactly same. Each node may have different hostnames assigned to each supported interface based on service and protocol.

According to 3GPP TS 29.303 [4.3], hostnames must adhere to the following format:

```
<topon|topoff>.<single-label-interface-name>.<canonical-node-name>
```

for example:

```
topon.s5-gtp.pgw.dc.central.bang.kar.3gppnetwork.org.
```

- "topon" indicates that the canonical node name can be used for topology match.
- "second-label-interface-name" of "s5-gtp" indicates that this hostname belongs to S5 interface supporting GTP protocol.
- "canonical-node-name" is the portion "pgw.dc.central.bang.kar.3gppnetwork.org"

The canonical node name is obtained by stripping off the first two labels.

First Primary Activation - Gn/Gp-SGSN

Topology matching is applicable only for primary activation for the Gn/Gp-SGSN and is based primarily on canonical node name comparison. Canonical node name for the SGSN must be defined as part of the SGSN Global configuration (see *Configuring Topology-based GW Selection for Gn/Gp-SGSN*). The canonical node names for the GGSN and/or the P-GW are the substring of hostnames received in the DNS results with query using APN-FQDN. Topology-based GW selection can only be achieved in the Gn/Gp SGSN through S-NAPTR query, which must be enabled as part of the feature configuration. If the SGSN's canonical node name is not configured, then GW selection will proceed as though topology is not enabled.

Primary Activation - S4-SGSN

First primary activation involves selection of both the P-GW and S-GW nodes.

If "topology" is configured (see *Configuring Topology-based GW Selection for S4-SGSN*), then the S4-SGSN shall apply topology-based selection for the P-GW and the S-GW node selection. If "weight" is configured, then the highest degree node pair is selected. If CSR fails, then the next highest degree node pair is selected, which maybe a different P-GW and S-GW node pair than the pair previously selected.

Primary Activation for Subsequent PDN

For a UE, all PDN connections must use the same S-GW. So, in subsequent PDN connections the S-GW is already selected. Therefore, topology will be applied to find the closest P-GW to the selected S-GW.

If the 'topology' option is configured (part of **gw-selection** configuration - see *Configuring Topology-based GW Selection for S4-SGSN*) and the hostname for the existing S-GW has the "topoff" prefix, then the co-located S-GW/P-GW node will be selected, if available.

Intra RAU, New SGSN RAU, Intra SRNS, New SRNS, IRAT

Assuming 'topology' option is configured (see *Configuring Topology-based GW Selection for S4-SGSN*) then for all of these procedures selection of the S-GW node will be based on the available P-GW. Therefore, the SGSN will do DNS with RAI-FQDN to get the list of S-GW hostnames and apply topology matching to determine the hostname of an available P-GW.

Before performing the topology matching, the SGSN checks to determine if the existing S-GW address is available in the DNS result. If the S-GW address is listed as available, then the SGSN continues with the S-GW. If the S-GW address is not listed as available in the query results, then the SGSN looks for an S-GW that is co-located or a topologically-closer to the available P-GW.

We must also consider how the P-GW hostname is selected when multiple PDN connections are available. Currently, the SGSN selects the first available valid P-GW hostname from the list of PDN connections. For in-bound roamers, the PDN connection belongs to the home network P-GW will not be used for topology matching.

Limitations

- Topology matching is not applicable for inbound roamers with home routed PDN connections, as the hostnames are under different operator's administrative control.
- Topology-based GW selection may not be applicable if the P-GW and/or the S-GW address is locally configured or if the static P-GW address is received from the HSS (because the hostname/canonical node name would not be available for topology matching).

Standards Compliance

This feature complies with the following standards:

- TS 23.060 version 10
- TS 29.303 version 10
- TS 29.274 version 10

Configuring Topology-based GW Selection

Topology-based GW selection is configured via the SGSN's CLI.

Configuration for this feature includes one or more of the following tasks, depending on the type of SGSN:

- enabling topology-based selection,
- enabling co-location-based selection,
- enabling weight (considering degree and order of GW listing in the DNS record) as a selection factor,
- configuring GW-type preference for selection,
- configuring canonical name (Gn/Gp-SGSN only),
- enabling S-NAPTR queries for GGSN selection (Gn/Gp-SGSN only).

For details on all of the command listed below, refer to the release-specific *Command Line Interface Reference*.

Configuring GW Selection

Configuring this feature is done at the call control profile level for both S4-SGSN and Gn/Gp-SGSN.

The **gw-selection** command in the call control profile configuration mode configures the parameters controlling the gateway selection process for both the Gn/Gp-SGSN and the S4-SGSN.

Important When configuring for a Gn/Gp-SGSN, use the P-GW options to identify either a GGSN or a co-located P-GW.

```
configure
    call-control-profile   profile_name
        gw-selection { { co-location | pgw weight | sgw weight | topology
 } [ weight [ prefer { pgw | sgw } ] ] }
         end
```

Notes:

- **co-location** enables the SGSN to select topologically closer P-GW and S-GW nodes, irrespective of the 'topon' or 'topoff' prefix being present in the hostname received in the results of the DNS query.
- **pgw weight** enables the SGSN to apply load balancing during selection of P-GW nodes.
- **sgw weight** enables the SGSN to apply load balancing during selection of S-GW nodes.
- **topology** enables the SGSN to select topologically closer P-GW and S-GW nodes, only when 'topon' prefix is present in the hostname received as part of the DNS query results.
- **weight** enables load balancing during selection of a node. When topology is applicable, **weight** instructs the SGSN to apply weight-based selection only on node pairs with the same degree and order.
- **prefer** instructs the SGSN to consider weight values for preferred GW type (P-GW or S-GW) during the first primary activation.

Verifying the GW Selection Configuration

Use the following command to display and verify the GW selection configuration in the call control profile configuration. The output of this command displays all of the profile configuration and the GW-selection portion is towards the bottom of the display.

```
show call-control-profile full name profile_name
```

Configuring DNS Queries for the Gn/Gp-SGSN

Configuring the required S-NAPTR query functionality for the Gn/GP-SGSN involves enabling the S-NAPTR query function and

Use the follow commands to enable the SGSN to use GGSN S-NAPTR queries. This capability is defined on a per APN basis.

```
configure
    apn-profile profile_name
         apn-resolve-dns-query snaptr [ epc-ue    non-epc-ue ]
         end
```

Notes:

- **epc-ue** - S-NAPTR queries applicable for EPC-capable UE.
- **non-epc-ue** - S-NAPTR queries applicable for non-EPC-capable UE.
- If neither of the keywords are included, then S-NAPTR query is applicable to all UE, both EPC-capable UE and non-EPC capable UE.

Use the following commands to identify the context where the DNS-client is configured. If this is not done then the S-NAPTR DNS query will look for the DNS-client configuration in the context where the SGTP service is configured.

```
configure
   call-control-profile profile_name
     dns-pgw context  context_name
     end
```

Important Issuing this series of commands assumes that you have already created a DNS-client instance with the **dns-client** command in the Context configuration mode and you have configured the DNS-client with the commands in the DNS-Client configuration mode.

Verifying the DNS Queries Configuration for the Gn/Gp-SGSN

Use the following commands to display and verify the S-NAPTR DNS Query configuration in the APN profile configuration and the call control profile configuration.

```
show apn-profile full name profile_name
show call-control-profile full name profile_name
```

Configuring DNS Queries for the S4-SGSN

Use the following commands to identify the context where the DNS-client is configured. If this is not done then the S-NAPTR DNS queries based on either APN-FQDN or RAI-FQDN will look for the DNS-client configuration in the context where the eGTP service is configured.

```
configure
   call-control-profile profile_name
     dns-pgw context  context_name
```

```
dns-sgw context  context_name
end
```

Important Issuing this series of commands assumes that you have already created a DNS-client instance with the **dns-client** command in the Context configuration mode and you have configured the DNS-client with the commands in the DNS-Client configuration mode.

Important It is recommended to execute the S4 SGSN configuration commands during the maintenance window. After configuring the node, re-start the node to activate the configuration commands. This will ensure that the node is in a consistent state and S4 SGSN service instability scenarios are avoided.

Verifying the DNS Queries Configuration for the S4-SGSN

Use the following commands to display and verify the S-NAPTR DNS Query configuration in the call control profile configuration.

```
show call-control-profile full name profile_name
```

Configuring the Canonical Node Name for the Gn/Gp-SGSN

In order for the Gn/Gp-SGSN to support Topological Gateway Selection, use the following commands to define the SGSN's canonical node name in the SGSN's configuration. (This is not needed for the S4-SGSN).

```
configure
     sgsn-global
          canonical-node-name canonical_node_name
          end
```

Notes:

- *canonical_node_name* is a fully or properly qualified domain name for example sgsn.div.bng.kar.3gppnetwork.org

Verifying the Canonical Node Name Configuration

Use the following commands to display and verify the canonical node name configuration. It is easy to find as it is the first item in the display.

```
show sgsn-mode
```

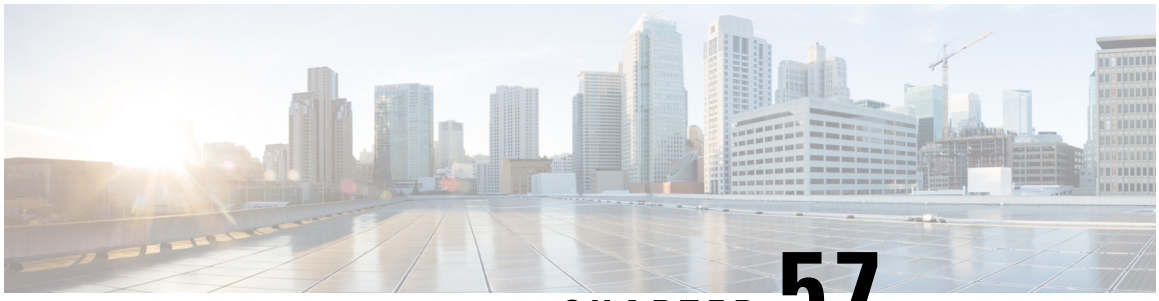
Monitoring Topology-based GW Selection

The following show command displays the hostname(s) for selected S-GW and P-GW. A small sampling of the output is displayed as an example.

show subscribers [gprs-only | sgsn-only] full

```
 SGW u-teid: [0x80000001] 2147483649
   SGSN u-teid: [0x80000001] 2147483649
SGW HostName: topon.s4.sgw.campus.bng.kar.3gppnetwork.org
PGW HostName: topon.s5.pgw.campus.bng.kar.3gppnetwork.org
Charging Characteristics:
Normal Billing
```

show subscribers [gprs-only | sgsn-only] full



CHAPTER 57

Triggering Iu Release Command Procedure

This chapter describes the following topics:

- Feature Summary and Revision History, on page 607
- Feature Description, on page 608
- Configuring RAB Messages with Cause 46, on page 609
- Monitoring and Troubleshooting, on page 610

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN
Applicable Platform(s)	• ASR 5500 • VPC-DI • VPC-SI
Feature Default	Disabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *SGSN Administration Guide* • *Statistics and Counters Reference*

Revision History

Important Revision history details are not provided for features introduced before releases 21.2 and N5.1.

Revision Details	Release
SGSN triggers the Iu Release procedure when it receives: • RAB Release Request with cause 46 "Radio Connection With UE Lost". • RAB Assignment Response with cause 46 "Radio Connection With UE Lost". This feature is available in 21.8.4 and 21.9 releases.	21.8
First introduced.	Pre 21.2

Feature Description

SGSN triggers the Iu Release Command procedure to RNC when it receives the RAB Release Request with cause 46 "Radio Connection With UE Lost" and the RAB Assignment Response with cause 46 "Radio Connection With UE Lost".

Support for RAB Release Request with cause 46

In releases prior to 21.8: When SGSN receives the RAB Release Request with cause "Radio Connection With UE Lost" from RNC, it responds with the same cause code in RAB Assignment Request (cause RAB Release). RNC then sends the RAB Assignment Response with cause RAB Release followed by Iu Release Command with cause "No Remaining RAB" to SGSN.

In 21.8 and later releases: When SGSN receives the RAB Release Request with cause "Radio Connection With UE Lost" from RNC, it triggers the Iu Release Command with cause "Normal Release". RNC then sends the Iu Release Complete message to SGSN.

The Iu release procedure is handled through the **ranap rabrel-with-radiolost** CLI command configured in the RNC Configuration mode.

SGSN proceeds with the following steps when it receives the RAB Release Request with cause "Radio Connection With UE Lost":

- SGSN verifies if the **ranap rabrel-with-radiolost** CLI command is enabled.
- If the **ranap rabrel-with-radiolost** CLI command is enabled, then SGSN triggers the Iu Release command towards the RNC to release the Iu connection for that specific UE.

Support for RAB Assignment Response with cause 46

In releases prior to 21.8: When RNC sends the RAB Assignment Response with cause "Radio Connection With UE Lost", SGSN sends the RAB Assignment Request with the cause "Radio Connection With UE Lost". Multiple retries are done before RNC sends the Iu Release Request message.

In 21.8 and later releases: When RNC sends the RAB Assignment Response with cause "Radio Connection With UE Lost", SGSN sends the Iu Release Command immediately and there are no RAB Assignment Request retries.

The Iu release procedure is handled through the **ranap rab-arsp-ue-radio-lost** CLI command configured in the RNC Configuration mode.

SGSN proceeds with the following steps when it receives the RAB Assignment Response with cause "Radio Connection With UE Lost":

- SGSN verifies if the **ranap rab-arsp-ue-radio-lost** CLI command is enabled.
- If the **ranap rab-arsp-ue-radio-lost** CLI command is enabled, then SGSN triggers the Iu Release Command towards the RNC to release the Iu connection for that specific UE.

Configuring RAB Messages with Cause 46

This section describes how to trigger the Iu Release Command procedure with cause 46 "Radio Connection With UE Lost".

Configuring RAB Assignment Response

Use the following configuration to enable or disable handling of the RAB Assignment Response with cause 46 (Radio Connection With UE Lost). SGSN sends the Iu Release Command with normal cause to RNC when it receives the RAB Assignment Response with cause 46.

```
configure
  context context_name
    iups-service service_name
      rnc id rnc_id
        [ no ] ranap rab-arsp-ue-radio-lost
        end
```

NOTES:

- **iups-service** *service_name*: Creates an IuPS service instance and enters the IuPS Service Configuration mode. This mode defines the configuration and usage of IuPS interfaces between the SGSN and the RNCs in the UMTS radio access network (UTRAN).

  service_name specifies the IuPS service name as a unique alphanumeric string of 1 through 63 characters.
- **rnc id** *rnc_id*: Sets the identification number of the RNC configuration instance. *rnc_id* must be an integer from 0 to 65535.
- When **no ranap rab-arsp-ue-radio-lost** is configured, SGSN will send the RAB Assignment Request with RAB Release to RNC.
- This command applies to Gn-SGSN only.
- This command is disabled by default.

Configuring RAB Release Request

Use the following configuration to enable or disable handling of the RAB Release Request with cause 46 (Radio Connection With UE Lost). SGSN sends the Iu Release Command to RNC when it receives the RAB Release Request with cause 46.

```
configure
  context context_name
```

```
iups-service service_name
  rnc id rnc_id
    [ no ] ranap rab-release-with-radiolost
    end
```

NOTES:

- **iups-service** *service_name*: Creates an IuPS service instance and enters the IuPS Service Configuration mode. This mode defines the configuration and usage of IuPS interfaces between the SGSN and the RNCs in the UMTS radio access network (UTRAN).

  service_name specifies the IuPS service name as a unique alphanumeric string of 1 through 63 characters.

- **rnc id** *rnc_id*: Sets the identification number of the RNC configuration instance. *rnc_id* must be an integer from 0 to 65535.
- When **no ranap rab-release-with-radiolost** is configured, SGSN will send the RAB Assignment Request with RAB Release to RNC.
- This command applies to Gn-SGSN only.
- This command is disabled by default.

Monitoring and Troubleshooting

This section provides information regarding show commands and bulk statistics available to monitor and troubleshoot this feature.

Show Commands and Outputs

show iups-service all

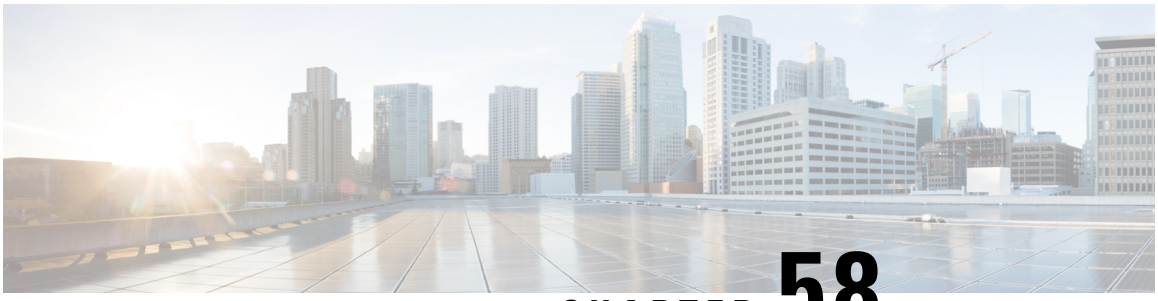
The output of this command includes the following fields:

- **Rab release with Radio lost** — Indicates whether RAB Release Request with cause 46 "Radio Connection With UE Lost" is enabled or disabled.
- **Rab assignment response with UE Radio lost** — Indicates whether RAB Assignment Response with cause 46 "Radio Connection With UE Lost" is enabled or disabled.

Bulk Statistics

The following bulk statistics are available in the SGSN schema.

- Iu-release-command-with-radio-lost-ue — Total number of Iu interface release commands due to RAB Release Request with radio lost received.
- Iu-release-command-rab-ass-rsp-with-radio-lost-ue — Total number of Iu interface release commands due to RAB Assignment Response with radio lost received.



CHAPTER 58

UDPC2 Support for MME/SGSN

This chapter includes the following topics:

- Feature Description, on page 611
- How It Works, on page 612
- Configuring MME/SGSN Support on UDPC2, on page 614

Feature Description

The MME and SGSN support the UDPC2 hardware. The maximum number of MME managers supported per chassis on Cisco ASR 5500 with DPC is 24, to support UDPC2 on ASR 5500 the maximum number of MME managers have been increased to 36.

The CLI command **task facility mmemgr per-sesscard-density { high | normal }** under the Global Configuration mode is used to configure the density (number of MME managers) of MME managers per session card. The disadvantage of this command is that it does not allow configuration of specific number of MME managers per card, but allows the operator to configure only high or normal density. This CLI is deprecated and new CLI commands are introduced to provide the operator with more flexibility to configure number of MME managers per active session cards (or per active session VM in case of VPC) and the total number of MME managers. The MME managers are now moved to Non-Demux card, therefore the number of managers depends on the number of session cards per chassis. The new CLI command enables the operator to spawn the maximum or desired number of MME managers even when the chassis is not fully loaded on the ASR 5500 platform. For VPC DI the operator can restrict max number of MME managers per chassis, if operator desires to scale with more session VMs without requiring additional MME managers.

In UDPC2, the number of Session Managers in ASR 5500 is increased from 336 to 1008.

Note The StarOS does not support ASR 5500 deployment with mixed usage of DPC and DPC2 cards. All session cards in one ASR 5500 have to be of the same type.

Note All product specific limits, capacity and performance, will remain same as compared to ASR 5500 with DPC.

MME Scaling on DPC2 to 2xDPC

This feature enhancement provides improved CEPS (Call Events Per Second) and session capacity utilization for MME/SGSN on the ASR 5500 DPC2 platform. It is observed that the current MME/SGSN deployments limit the maximum session/subscriber capacity utilization as the CPU reaches its maximum threshold for some proclets though sufficient memory is available in the system and in the proclet for additional sessions/subscribers. With this enhancement, the session utilization capacity is doubled (2X) on the ASR 5500 DPC2 platform for a specific call model.

This feature has increased the limits for the following MME/SGSN specific proclets on ASR 5500 DPC2 platform:

- The maximum number of MME managers per chassis has been increased to "48" on ASR 5500 DPC2 platform.
- The maximum number of MME managers per Non-Demux card has been increased to "8" on ASR 5500 DPC2 platform.
- The maximum number of IMSI managers per Demux card has been increased to "8" on ASR 5500 DPC2 platform.

MMEMGR Scaling on DPC

In this feature enhancement, the load on the MME managers are distributed widely with the increase in the number of MME managers. This enhancement is most likely seen in a standalone MME deployment, where the difference in the usage of MME manager CPU and Session Manager CPU is apparent.

This feature has increased the limits of the following MME/SGSN proclets on the ASR 5500 DPC Platform:

- The maximum number of MME managers per chassis has been increased to "36" on the ASR 5500 DPC platform.

How It Works

The number of MME managers for a platform is predefined and not configurable. The operator can now configure the desired number of MME managers defined for each platform. The **task facility mmemgr max** *value* CLI command is introduced to configure the number of MME managers. If the operator does not configure the desired number of MME managers, a default number of predefined MME managers will be configured on the chassis.

Note After you configure the **task facility mmemgr max** command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

The table below depicts the default and maximum number of MME managers per chassis for each platform:

Platform	Default number of MME Managers per chassis	Maximum number of MME Managers per chassis
ASR 5500 with DPC	24	36 For releases prior to 21.1: 24
ASR 5500 with DPC2	48 For releases prior to 21.0: 36	48 For releases prior to 21.0: 36
SSI MEDIUM/LARGE	2	2
SSI SMALL	1	1
SCALE MEDIUM/LARGE	24	48 For releases prior to 20.0: 24

The number of MME managers for a session card could be configured based only on the density per session card/VM. With the introduction of the **task facility mmemgr per-sesscard-count** *number* CLI command, the operator can now configure the number of MME managers per session card. If the operator does not configure the desired number of MME managers per session card, a default number of MME managers will be spawned on the session card.

Note After you configure the **task facility mmemgr per-sesscard-count** command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

The table below depicts the default and maximum number of MME managers configurable per session card for different platforms/cards:

Platform	Default number of MME Managers per session card	Maximum number of MME Managers per session card
ASR 5500 with DPC	4	6
ASR 5500 with DPC2	8 For releases prior to 21.0: 6	8 For releases prior to 21.0: 6
SSI MEDIUM/LARGE	2	2
SSI SMALL	1	1
SCALE MEDIUM/LARGE	1	2

Configuring the number of MME managers helps to scale the number of eNodeB connections.The maximum number of eNodeB connections supported by MME is 128K per ASR 5500 chassis. Having more number of MME managers ensures better CPU utilization, load balancing across MME managers and improved message communication between session managers and MME managers.

Configuring MME/SGSN Support on UDPC2

This section describes how to configure the required number of MME managers per session card and the desired number of MME managers per chassis.

Configuring MME Managers per Session Card

The following CLI command is deprecated from release 19.2 onwards. It was introduced in release 18.0 and is valid till release 19.0. When an operator using this configuration command upgrades to release 19.2, this CLI is mapped to a new CLI command **task facility mmemgr per-sesscard-count** *count*.

This CLI command is deprecated as it does not allow the operator to configure the required number of MME managers per session card. This command only allows two predefined modes of either "high" or "normal" density.

```
configure
   task facility mmemgr per-sesscard-density { high | normal }
   end
```

The following CLI command is introduced to configure the desired number of MME managers per session card:

```
configure
   task facility mmemgr per-sesscard-count count
   default task facility mmemgr per-sesscard-count
   end
```

Note After you configure the **task facility mmemgr per-sesscard-count** command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

NOTES:

- The maximum number of MME managers that can be configured per session card varies based on the platform/VM and card type. However, the upper limit of MME managers that can be configured per session card is set to "6" for releases up to 20.0 and to “8” from release 21.0 onwards.
- This command is not specific to any platform or card type. It is applicable and available to all platforms and card types.
- The **default** keyword resets the number MME managers per session card to the default number of MME managers per session card/VM. By default this CLI is not configured. When this CLI is not configured, the default number of MME managers per session card will be selected based on platform and card type. The default values are listed below:

Platform/VM and card type	Default number of MME managers per session card
ASR 5500 DPC	4

Platform/VM and card type	Default number of MME managers per session card
ASR 5500 DPC2	8 **Note** Releases prior to 21.0, the default number of MME managers per session card supported was only "6".
SSI MEDIUM/LARGE	2
SSI SMALL	1
SCALE LARGE/MEDIUM	1

- The **per-sesscard-count** *count* keyword is used to set the maximum number of MME managers per session card. *count* must be an integer ranging from 1 to 6 for releases up to 20.0 and 1 to 8 from release 21.0 onwards.

  The maximum number of MME managers allowed per session card based on the platform/VM and card type is listed below:

Platform/VM and card type	Maximum number of MME managers per session card
ASR 5500 DPC	6
ASR 5500 DPC2	8 For releases prior to 21.0: 6
SSI MEDIUM/LARGE	2
SSI SMALL	1
SCALE LARGE/MEDIUM	2

Usage Example

Listed below is an example where 3 MME managers are configured per session card on an ASR 5500 platform with DPC2 card:

task facility mmemgr per-sesscard-count 3

Listed below is an example where default number of MME managers configured per session card on an ASR 5500 platform with DPC card:

default task facility mmemgr per-sesscard-count

Configuring MME Managers per Chassis

The following CLI command is introduced to configure the desired number of MME managers per chassis:

```
configure
  task facility mmemgr max value
```

```
default task facility mmemgr max
end
```

Note After you configure the **task facility mmemgr max** command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

NOTES:

- The maximum number of MME managers that can be configured per chassis varies based on the platform. However, the upper limit of MME managers per chassis is set to 48.

  Note Note: For releases prior to 20.0 the upper limit of MME managers per chassis was set to "36".

- This CLI is not configured by default. The **default** keyword resets the number of MME managers per chassis to the default values. The default values are listed below:

Platform/VM and card type	Default number of MME managers per chassis
ASR 5500 DPC	24
ASR 5500 DPC2	48 **Note** For releases prior to 21.0 the default number of MME managers per chassis was “36”.
SSI MEDIUM/LARGE	1
SSI SMALL	1
VPC-DI or SCALE LARGE/MEDIUM	24

- The keyword **max** *value* keyword is used to set the maximum number of MME managers per chassis. *value* must be an integer ranging from 1 to 48.

  Note For releases prior to 20.0, the upper limit of MME managers per chassis was set to "36".

  The maximum number of MME managers allowed per chassis based on the platform/VM and card type is listed below:

Platform/VM and card type	Maximum number of MME managers per chassis
ASR 5500 DPC	36 For releases prior to 21.1: 24

Platform/VM and card type	Maximum number of MME managers per chassis
ASR 5500 DPC2	48 For releases prior to 21.0: 36
SSI MEDIUM/LARGE	2
SSI SMALL	1
VPC-DI or SCALE LARGE/MEDIUM	48 For releases prior to 20.0: 24

Usage Example

Listed below is an example where 5 MME managers are configured per chassis on an ASR 5500 platform with DPC2 card:

task facility mmemgr max 5

Listed below is an example where default number of MME managers configured per chassis on an ASR 5500 platform with DPC card:

default task facility mmemgr max

Verifying the Configuration

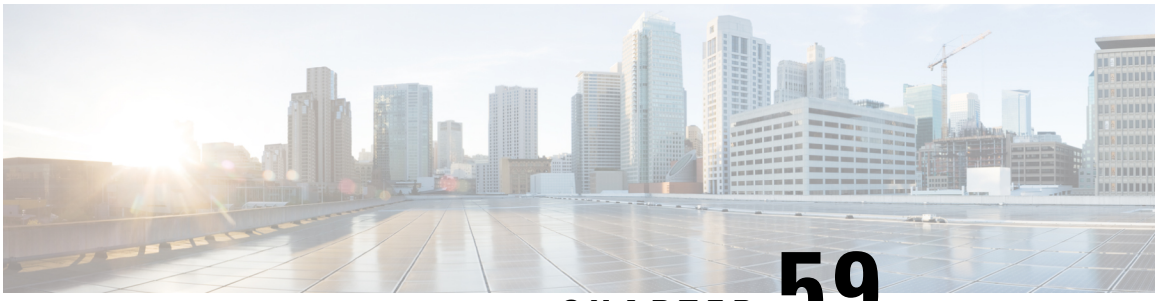
The **show configuration** command is used to verify the configuration of this feature. The output displays the configured values of number of MME managers per chassis or number of MME managers per session card.

If "5" MME managers are configured per chassis the following output is displayed on issuing the **show configuration** command:

task facility mmemgr max 5

If "2" MME managers are configured per session card the following output is displayed on issuing the show configuration command:

task facility mmemgr per-sesscard-count 2



CHAPTER 59

UTRAN to E-UTRAN Handover

This chapter describes the following topics:

- Feature Summary and Revision History, on page 619
- Feature Description, on page 620
- Configuring UTRAN to E-UTRAN Handover, on page 620
- Monitoring and Troubleshooting, on page 621

Feature Summary and Revision History

Summary Data

Applicable Product(s) or Functional Area	SGSN (S4-SGSN)
Applicable Platform(s)	• ASR 5000 • ASR 5500 • VPC-DI • VPC-SI
Feature Default	Enabled - Configuration Required
Related Changes in This Release	Not Applicable
Related Documentation	• *Command Line Interface Reference* • *SGSN Administration Guide* • *Statistics and Counters Reference*

Revision History

Revision Details	Release

First introduced. This feature is available in 21.5.10 and 21.9 releases.	21.5.10

Feature Description

The UTRAN to E-UTRAN Handover feature is used to check and avoid including the RAB IDs in the "Relocation Command" message. When this feature is enabled, the SGSN includes the RAB IDs in the "RABs To Be Released List" IE in the "Relocation Command" message if the MME does not include the F-TEID information in the "Forward Relocation Response" message (existing behavior).

When this feature is disabled, the SGSN will not include the following IEs in the "Relocation Command" message if the MME does not include the F-TEID information.

- RABs Subject To Data Forwarding List
- RABs To Be Released List

Configuring UTRAN to E-UTRAN Handover

This section describes how to configure UTRAN to E-UTRAN Handover feature.

Configuring eNodeB Data Forwarding

Use the following configuration to configure enable forwarding of data from the RNC to eNodeB.

```
configure
  context context_name
    iups-service service_name
      rnc id rnc_id
        [ no ] enb-data-forward
        end
```

NOTES:

- **iups-service** *service_name*: Creates an IuPS service instance and enters the IuPS Service Configuration mode. This mode defines the configuration and usage of IuPS interfaces between the SGSN and the RNCs in the UMTS radio access network (UTRAN).

  service_name specifies the IuPS service name as a unique alphanumeric string of 1 through 63 characters.

- **rnc id** *rnc_id*: Sets the identification number of the RNC configuration instance. *rnc_id* must be an integer from 0 to 65535.
- **enb-data-forward**: Enables the forwarding of data from this RNC to eNodeB.
- **no**: Disables the forwarding of data from this RNC to eNodeB.
- This command is enabled by default.

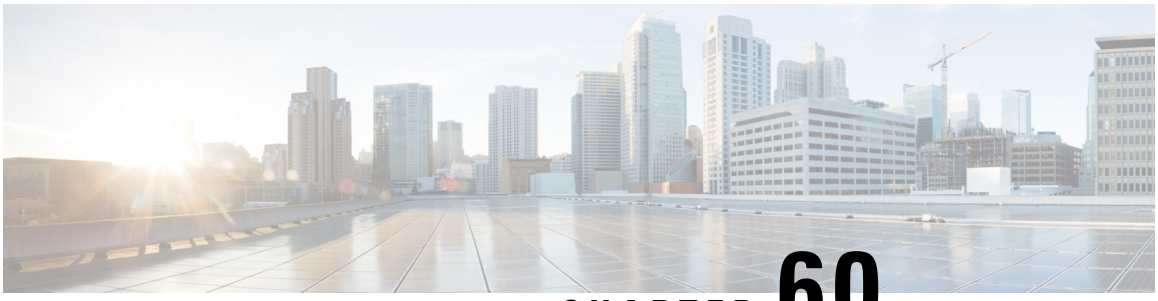
Monitoring and Troubleshooting

This section provides information on show commands and their corresponding outputs for the UTRAN to E-UTRAN Handover feature.

Show Commands and Outputs

show iups-service all

The output of this command includes the "E-NodeB Data Forwarding" field to indicate whether eNodeB Data Forwarding support is enabled or disabled.



CHAPTER 60

Monitoring, Troubleshooting and Recommendations

- Monitoring, Troubleshooting and Recommendations, on page 623
- Monitoring , on page 624
- Troubleshooting, on page 628
- Recommendations, on page 632

Monitoring, Troubleshooting and Recommendations

Monitoring and troubleshooting the SGSN are not unrelated tasks that use many of the same procedures. This chapter provides information and instructions for using the system command line interface (CLI), primarily the **show** command, to monitor service status and performance and to troubleshoot operations.

The **show** commands used for monitoring and troubleshooting include keywords (parameters) that can fine-tune the output to produce information on all aspects of the system, ranging from current software configuration through call activity and status. The keywords, used in the procedures documented in this chapter, are intended to provide the most useful and in-depth information for monitoring the system. To learn about all of the keywords possible, refer to the *Command Line Interface Reference*. To learn about the details for the information in the **show** command outputs, refer to the *Statistics and Counters Reference*.

In addition to the CLI documented in this chapter, the system supports other monitoring and troubleshooting tools:

- SNMP (Simple Network Management Protocol) traps that indicate status and alarm conditions. Refer to the *SNMP MIB Reference* for a detailed listing of these traps.
- bulk statistics (performance data) which can be accessed in various manners. For a complete list of SGSN supported statistics, refer to the *Statistics and Counters Reference*. For information about configuring the formats for static collection, refer to the *Command Line Interface Reference*.
- threshold crossing alerts for conditions that are typically temporary, such as high CPU or port utilization, but can indicate potentially severe conditions. For information on threshold crossing alert configuration, refer to the *Thresholding Configuration Guide*.

The monitoring and troubleshooting procedures are organized on a task-basis with details for:

- Monitoring (information required regularly)
  - Daily Standard Health Check
  - Monthly System Maintenance

    - Semi-Annual Check
- Troubleshooting (information required intermittently)
    - Overview of Possible Fault Types
    - Single and Mass Problem Scenarios
    - Reference Materials (information required infrequently)

Monitoring

This section contains commands used to monitor system performance and the status of tasks, managers, applications, and various other software components. Most of the procedure commands are useful for both maintenance and diagnostics.

There is no limit to the frequency that any of the individual commands or procedures can be implemented, however, the organization of tasks into three unique sets of procedures suggests a recommendation for minimal implementation:

- Daily Standard Health Check
- Monthly System Maintenance
- Semi-Annual Check

Daily - Standard Health Check

The standard health check is divided into three independent procedures:

- Health Check - Hardware & Physical Layer
- Health Check - System & Performance
- Health Check - SGSN-Specific Status & Performance

Health Check - Hardware & Physical Layer

The first set of commands are useful for monitoring the hardware status for the entire system. The second set of commands check the status of hardware elements within the chassis and provide some verification of the physical layer status. The operational parameters for the hardware are included in the *Hardware Installation and Administration Guide*. Note that all hardware elements generate alarms in the case of failure.

Table 51: Hardware Status Checks

To Do This:	Enter This Command:
All hardware problems generate alarms, the following checks can be replaced by reviewing the trap history.	**show snmp trap history**
Check the status of the PFUs. Output indicates the power level for the cards in the chassis. All active cards should be in an "ON" state.	**show power chassis**
Check the power status of an individual chassis.	**show power all**
View the status of the fan trays. In case of a fan problem, refer to your support contract to contact the appropriate service or sales representative.	**show fans**

To Do This:	Enter This Command:
View the LED status for all installed cards. All LEDs for active cards should be green.	**show leds all**
Checking the temperatures confirms that all cards and fan trays are operating within safe ranges to ensure hardware efficiency.	**show temperature**

Table 52: Physical Layer Status Check

To Do This:	Enter This Command:
View mapping of the line cards-to-controlling application cards.	**show card mappings**
View a listing of all installed application cards in a chassis. Determine if all required cards are in active or standby state and not offline. Displays include slot numbers, card type, operational state, and attach information.	**show card table** **show card table all**
Display a listing of installed line cards with card type, state, and attach information. Run this command to ensure that all required cards are in Active/Standby state. No card should be in OFFLINE state.	**show linecard table**
View the number and status of physical ports on each line card. Output indicates Link and Operation state for all interfaces -- UP or down.	**show port table all**
Verify CPU usage and memory.	**show cpu table** **show cpu information**

Health Check - System & Performance

Most of these commands are useful for both maintenance and diagnotics, and if the system supports a "combo" (a co-located SGSN and GGSN), then these commands can be used for either service.

Table 53: System & Performance Checks

To Do This:	Enter This Command:
Check a summary of CPU state and load, memory and CPU usage.	**show cpu table**
Check availability of resources for sessions.	**show resources session**
Review session statistics, such as connects, rejects, hand-offs, collected in 15-minute intervals.	**show session counters historical**
View duration, statistics, and state for active call sessions.	**show session duration** **show session progress**

To Do This:	Enter This Command:
Display statistics for the Session Manager.	**show session subsystem facility sessmgr all**
Check the amount of time that the system has been operational since the last downtime (maintenance or other). This confirms that the system has not rebooted recently.	**show system uptime**
Verify the status of the configured NTP servers. Node time should match the correct peer time with minimum jitter.	**show ntp status**
Check the current time of a chassis to compare network-wide times for synchronisation or logging purposes. Ensure network accounting and/or event records appear to have consistent timestamps.	**show clock universal**
View both active and inactive system event logs.	**show logs**
Check SNMP trap information. The trap history displays up to 400 time-stamped trap records that are stored in a buffer. Through the output, you can observe any outstanding alarms on the node and contact the relevant team for troubleshooting or proceed with SGSN troubleshooting guidelines.	**show snmp trap history**
Check the crash log. Use this command to determine if any software tasks have restarted on the system.	**show crash list**
Check current alarms to verify system status.	**show alarm outstanding all** **show alarm all**
View system alarm statistics to gain an overall picture of the system's alarm history.	**show alarm statistics**

Daily - Health Check- SGSN-Specific Status and Performance

These commands are useful for both maintenance and diagnotics.

Table 54: SGSN-Specific Status and Performance Checks

To Do This:	Enter This Command:
Check the status and configuration for the Iu-PS services. In the display, ensure the "state" is "STARTED" for the Iu interface.	**show iups-service all**
Check the configuration for theMAP services features and some of the HLR and EIR configuration. In the display, ensure the "state" is "STARTED" for the Gr interface.	**show map-service all**
Check the configuration for the SGSN services in the current context. In the display, ensure the "state" is "STARTED" for the SGSN.	**show sgsn-service all**

To Do This:	Enter This Command:
Check the SS7 Signalling Connection Control Part (SCCP) network configuration and status information, for example, check the state of the SIGTRAN. The display should show all links to all RNC/subsystem are available, as well as those toward the HLR.	**show sccp-network all status all**
Check the configuration and IDs for SS7 routing domains	**show ss7-routing-domain all**
Check the connection status on SS7 routes.	**show ss7-routing-domain <> routes**
Snapshot subscriber activity and summary of PDP context statistics.	**show subscribers sgsn-only**
Check the configured services and features for a specific subscriber.	**show subscribers sgsn-only full msid** *<msid_number>*

Monthly System Maintenance

Depending upon system usage and performance, you may want to perform these tasks more often than once-per-month.

Table 55: Irregular System Maintenance

To Do This:	Enter This Command:
Check for unused or unneeded file on the CompactFlash.	**dir /flash**
Delete unused or unneeded files to conserve space using the delete command. Recommend you perform next action in list	**delete /flash/***<filename>*
Synchronise the contents of the CompactFlash on both SMCs to ensure consistency between the two.	**card smc synchronize filesystem**
Generate crash list (and other "show" command information) and save the output as a tar file.	show support details <to location and filename> • [file:]{ /flash | /pcmcia1 | /hd }[/directory]/file_name • tftp://{ host[:port] }[/directory]/file_name • [ftp: | sftp:]//[username[:password]] { host }[:port][/directory]/file_name

If there is an issue with space, it is possible to remove alarm and crash information from the system - however, it is not recommended. Support and Engineering personnel use these records for troubleshooting if a problem should develop. We recommend that you request assigned Support personnel to remove these files so that they can store the information for possible future use.

Every 6 Months

We recommend that you replace the particulate air filter installed directly above the lower fan tray in the chassis. Refer to the *Replacing the Chassis' Air Filter* section of the *Hardware Installation and Administration Guide* for information and instruction to performing this task.

Table 56: Verify the Hardware Inventory

To Do This:	Enter This Command:
View a listing of all cards installed in the chassis with hardware revision, part, serial, assembly, and fabrication numbers.	**show hardware card** **show hardware inventory** **show hardware system**
View all cards installed in the chassis with hardware revision, and the firmware version of the on-board Field Programmable Gate Array (FPGAs).	**show hardware version board**

Troubleshooting

Troubleshooting is tricky unless you are very familiar with the system and the configuration of the system and the various network components. The issue is divided into three groups intended to assist you with diagnosing problems and determining courses of action.

Problems and Issues

Table 57: Possible Problems

Problem	Analysis
Users cannot Attach to the SGSN - Attach Failure	Typically, the root cause is either a fundamental configuration error or a connection problem either on the system (the SGSN) or the network. Configuration changes may have been made incorrectly on either the SGSN or on the signalling network or access network equipment.
Users can Attach to the SGSN but cannot Activate a PDP Context.	In most cases, this type of problem is related either to an issue with the LAN connectivity between the SGSN and the DNS server or a general connectivity problem between the SGSN and a GGSN.
Users can Attach to the SGSN, they can Activate a PDP Context but data transfer isn't happening.	The problem could be between the GGSN and an external server. The PDP Context indicates that the tunnel between the SGSN and the GGSN is intact, but the lack of data transfer suggests that external servers can not be reached.

Problem	Analysis
Users can Attach to the SGSN, they can Activate a PDP Context but they encounter other problems.	Problems, such as slow data transfer or a session disconnect for an already established session, can be caused by congestion during high traffic periods, external network problems, or handover problems.

Troubleshooting More Serious Problems

You will see that the commands from the Daily Health Check section are also used for troubleshooting to diagnose problems and possibly discover solutions. And of course, your Support Team is always available to help.

Causes for Attach Reject

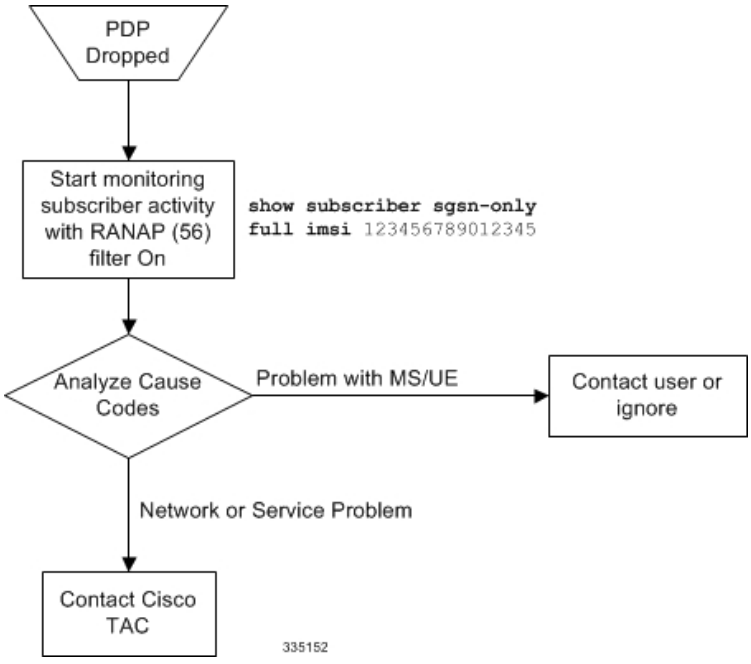
If an SGSN receives Attach Request messages but responds with Attach Rejects, then the reason might be found in one of the cause codes. These codes are included as attributes in the Reject messages and can be seen during monitoring with the following command:

```
monitor subscriber IMSI
```

Single Attach and Single Activate Failures

To troubleshoot an Attach or Activate problem for a single subscriber, you will need to begin with the subscriber's MS-ISDN number. The attached flow chart suggests commands that should assist with determining the root of the problem:

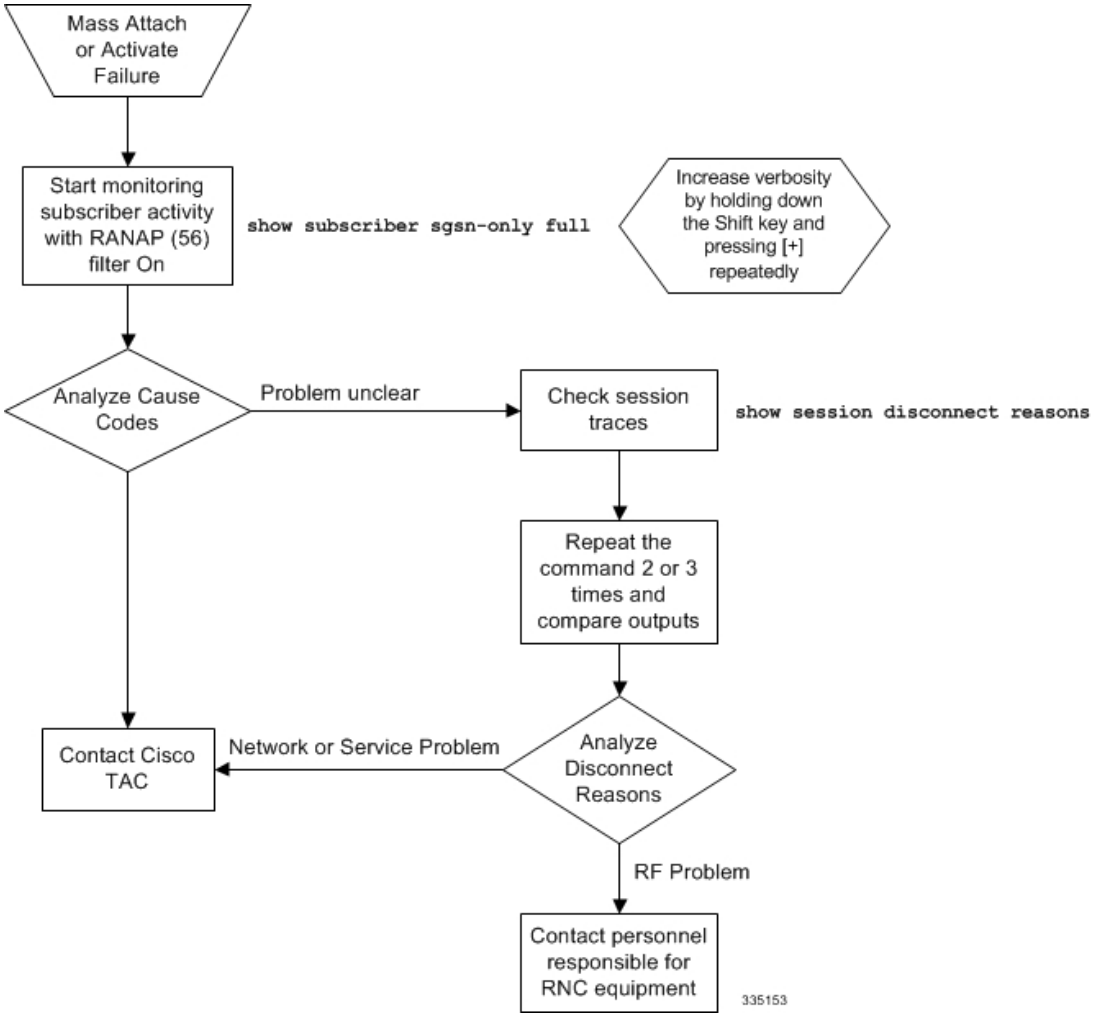
Figure 112: Troubleshooting Single Attach/Activate Failures



Mass Attach and Activate Problems

The following flow chart is intended to help you diagnose the problem and determine an appropriate response:

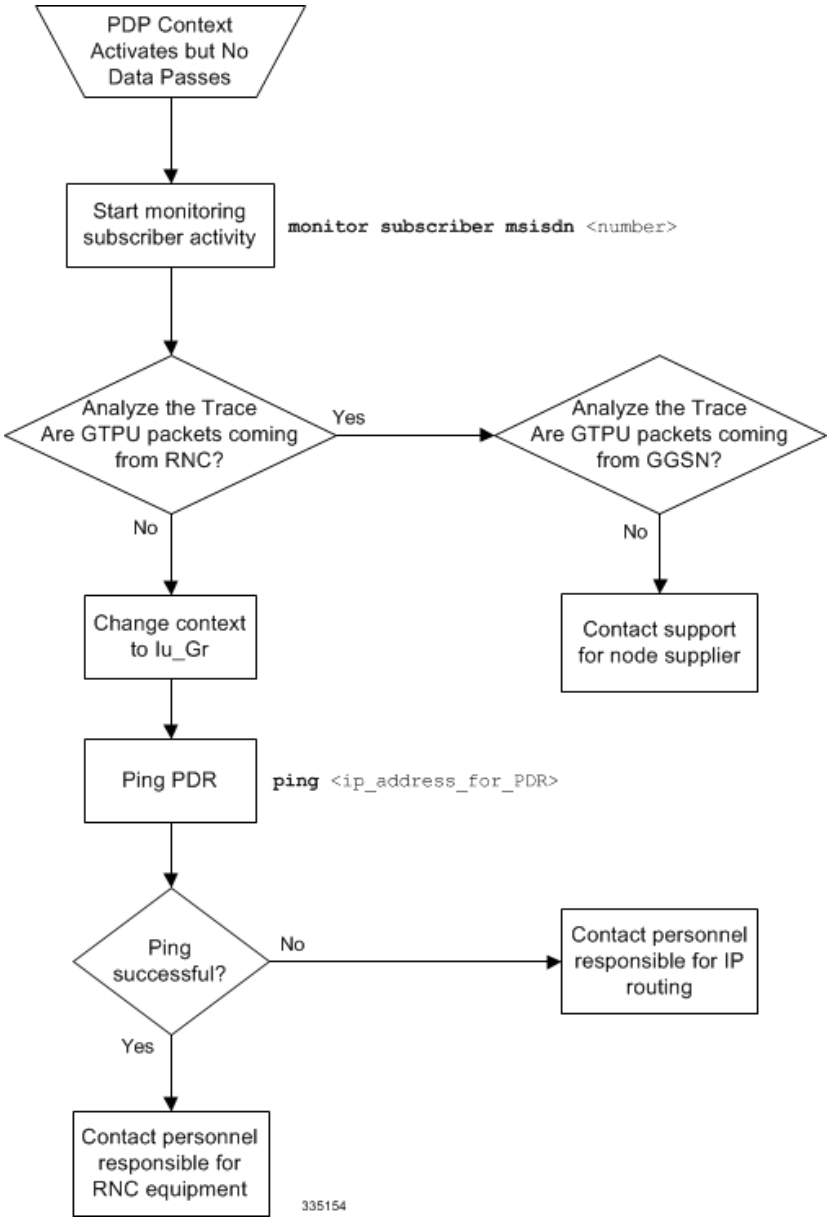
Figure 113: Troubleshooting Multiple Attach/Activate Failures



Single PDP Context Activation without Data

In a situation where the subscriber has PDP Context Activation but data is going through, the following procedure will facilitate problem analysis. To begin, you must first obtain the subscriber's MS-ISDN number.

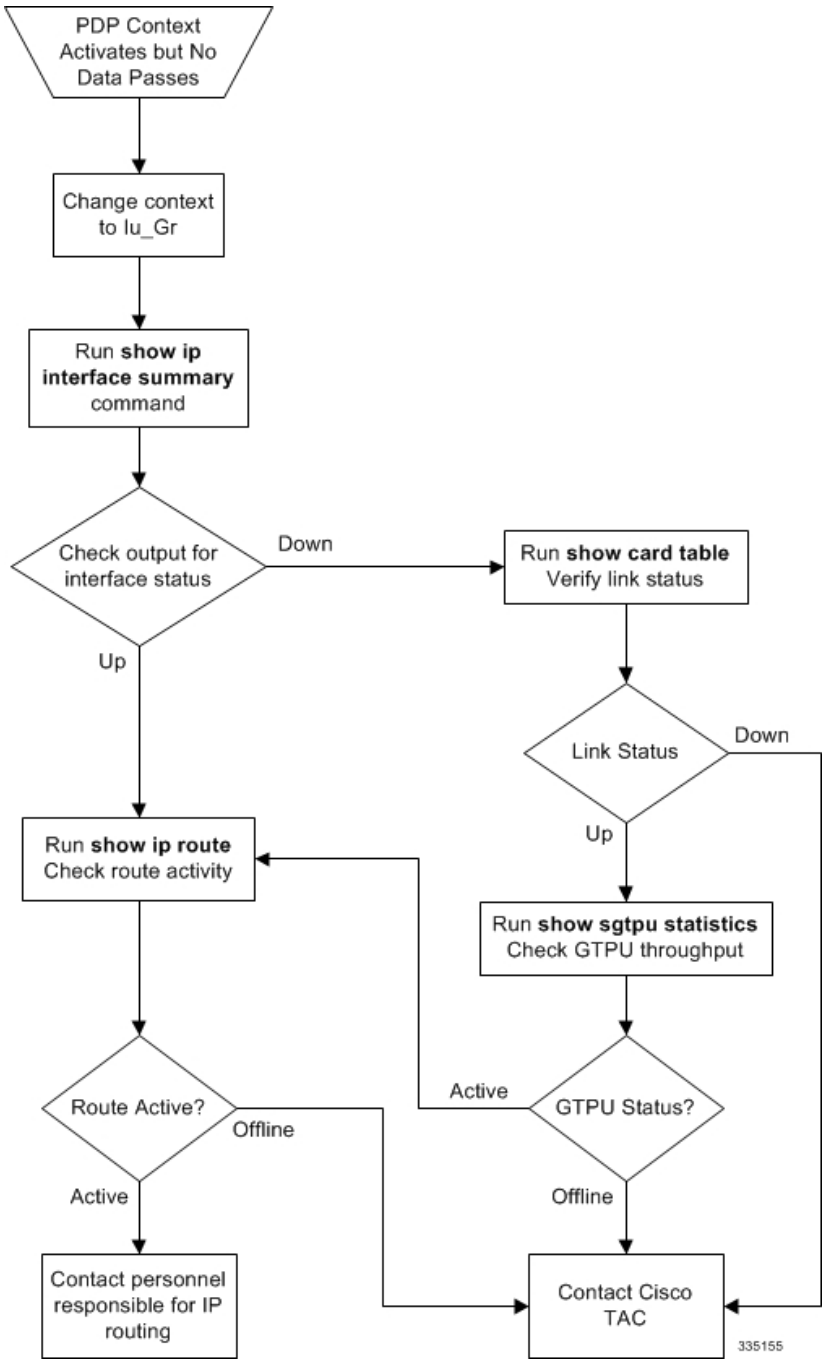
Figure 114: Troubleshooting Missing Data for Single PDP Context Activation



Mass PDP Context Activation but No Data

In many cases, this type of problem is due to a change in the configuration: hardware, interface, routing. The following will suggest commands to help run down the problem:

Figure 115: Troubleshooting Missing Data for Multiple PDP Context Activation

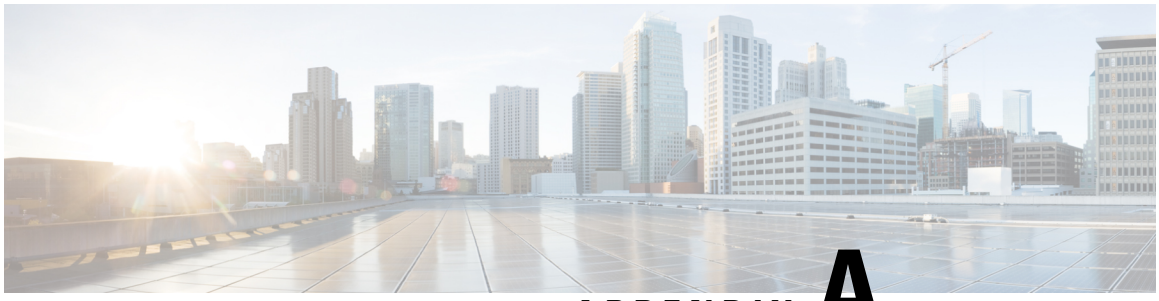


Recommendations

This section describes some recommendations and guidelines to ensure proper functioning of the system. Generic platform and system rules or limits can be found in the "Engineering Rules" appendix in the *System Administration Guide* and/or contact your Cisco account representative.

- The **task facility linkmgr** command is used to configure the maximum number of Link Managers for an SGSN. It is recommended to restrict the number of Link Managers for PSC2/PSC3 to a maximum of "4" due memory and hardware limitations. If the Link Managers are overloaded, then the number of Link Managers can be increased based on the number of cards available and associated ASP links needs to be updated. For more information on this command see *Command Line Interface Reference* document.

Note After you configure the **task facility linkmgr** command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.



APPENDIX A

Engineering Rules

- Engineering Rules, on page 635
- Service Rules, on page 635
- SGSN Connection Rules, on page 636
- Operator Policy Rules, on page 637
- SS7 Rules, on page 639
- SGSN Interface Rules, on page 641

Engineering Rules

This section provides SGSN-specific (2G, 3G, S4-SGSN related) common engineering rules or limit guidelines for the current release. These limits are hardcoded into the SGSN system and are not configurable. The limits are documented here because they should be considered prior to configuring an SGSN for network deployment.

Generic platform and system rules or limits can be found in the "Engineering Rules" appendix in the *System Administration Guide*.

Service Rules

The following engineering rules define the limits for the various services configured on the SGSN (system):

Note Maintaining a large number of services increases the complexity of management and may impact overall system performance. Therefore, we recommend that you limit the number of services that you configure and that you talk to your Cisco Service Representative for optimization suggestions and additional information on service limits.

Table 58: Service Rules for the SGSN

Features	Limits	Comments
Maximum number of (all) services (regardless of type) configurable per SGSN (system).	256	This limit includes the number of GPRS services, SGSN services, SGTP services, IuPS Services, and MAP Services.

Features	Limits	Comments
Max. number of eGTP services supported by a GPRS/SGSN service.	1	When configured for S4-SGSN. The same eGTP service should be associated with both the GPRS and the SGSN service.
Max. number of HSS peer services supported by a single GPRS or SGSN service.	1	When configured for S4-SGSN.
Max. number of Gs services supported by a single GPRS or SGSN service.	1	Although the limit is 1 Gs Service configured per GPRS Service or SGSN Service, SGSN service can access multiple Gs Services using Operator Policies.
Max. number of MAP services supported by a single GPRS (2G) or SGSN (3G) service.	1	Although the limit is 1 MAP Service configured per GPRS Service or SGSN Service, the GPRS or SGSN service can access multiple MAP Services using Operator Policies.
Max. number of Gs services supported on an SGSN (system)	12	
Maximum number of LACs per Gs service	128	
Max. number of MAP Service configurations supported by a single SCCP network.	1	
Max. number of SGTP services supported by a single GPRS or SGSN service.	1	Although the limit is 1 SGTP Service configured per GPRS Service or SGSN Service, the GPRS or SGSN service can access multiple SGTP Services using Operator Policies.

SGSN Connection Rules

The following limitations apply to both 2G and 3G SGSNs.

Table 59: Connection Rules for the SGSN

Features	Limits	Comments
Maximum number of entry authentication triplets (RAND, SRES, and KC) and quintuplets stored per MM context	5	5 (unused) + 5 (used) Triplets/Quituplets
Maximum number of logically connected SMSCs	no limit	Limit would be based on the number of routes if directly connected. No limit if GT is used.
Maximum number of logically connected HLRs	no limit	Limit would be based on the number of routes if directly connected. No limit if GT is used.
Maximum number of logically connected EIRs	1	SGSN will be connected to only 1 EIR.
Maximum number of logically connected MSCs	see comment	System supports a max of 128 LACs per Gs service and a max of 12 Gs service.
Maximum number of concurrent PDP contexts per active user	11	
Maximum number of logically connected GGSNs per Gn/Gp interface	20000	
Maximum number of packets buffered while other engagement Maximum number of packets buffered in suspended state Maximum number of packets buffered during RAU	see comment	- Minimum of 2KB/subscriber. - Maximum of 10KB/subscriber -- if buffers are available in the shared pool*. (*SGSN provides a common buffer pool for 2G and 3G subscribers of 10M per session manager buffers to be shared by all subscribers "belonging" to that session manager.) - Additional 2G subscriber buffer pool in BSSGP.

Operator Policy Rules

The following engineering rules apply for the entire system when the system is configured as an SGSN.

The limits listed in the table below are applicable for a standalone SGSN application . Limits may be lower when using a PSC1 or in combo nodes, such as SGSN+GGSN.

Table 60: Operator Policy Limits Applicable to the SGSN

Features	Limits	Comments
Maximum number of Operator Policies	1000	Includes the 1 default policy.
Maximum number of Call-Control Profiles	1000	
Maximum number of APN Profiles	1000	
Maximum number of IMEI Profiles	1000	
Maximum number of APN Remap Tables	1000	
Maximum number of APN remap entries per APN Remap Table	300	
Maximum number of IMSI ranges under SGSN mode	1000	
Maximum number of IMEI ranges per operator policy	128	
Maximum number of APN profile associations per operator policy	128	
Maximum number of Call-Control Profiles per Operator Policy	1	
Maximum number of APN remap tables per Operator Policy	1	
Maximum number of EIR Profiles	16	
Maximum number of congestion-action-profiles	16	
Call-Control Profiles		
Maximum number of equivalent PLMN for 2G and 3G	15	Mandatory to configure the IMSI range. Limit per call-control profile.
Maximum number of equivalent PLMN for 2G	15	Limit per call-control profile.
Maximum number of equivalent PLMN for 3G	15	Limit per call-control profile.
Maximum number of static SGSN addresses	256	Limit per PLMN.
Maximum number of location area code lists	5	

Features	Limits	Comments
Maximum number of LACs per location area code list	100	
Maximum number of allowed zone code lists	10	
Maximum number of allowed zone code lists	no limit	For Release 12.2
Maximum number of LACs per allowed zone code list	100	
Maximum number of integrity algorithms for 3G	2	
Maximum number of encryption algorithms for 3G	3	
APN Profiles		
Maximum number of APN profiles	1000	
Maximum number of gateway addresses per APN profile	16	

SS7 Rules

SS7 Routing

Table 61: SS7 Routing Rules for SGSN

Features	Limits	Comments
Maximum number of SS7 routing domains supported by an SGSN	12	
Maximum number of SS7 routes supported by an SGSN	2048	This includes the self point code of the peer-server.
Maximum number of routes possible via a link-set	2048	
Maximum number of routes possible via peer-server	2048	This includes one route for the peer-server and 2047 indirect routes.
Maximum number of different levels of priority for link sets used in a single route set	16	

SIGTRAN

Table 62: SIGTRAN Rules for SGSN

Features	Limits	Comments
Maximum number of peer servers per LinkMgr	512	
Maximum number of peer servers per SS7RD	256	
Maximum number of PSPs per peer server	12	
Maximum number of ASPs per SS7RD	12	
Maximum number of SCTP endpoints per ASP	2	
Maximum number of of SCTP endpoints per PSP	2	
Maximum number of SCTP endpoints per PSP (dynamically learnt)	5	

Broadband SS7

Table 63: Broadband SS7 Rules for SGSN

Features	Limits	Comments
Maximum number of MTP3 linksets	512	
Maximum number of MTP3 linksets per SS7RD	256	
Maximum number of MTP3 links per linkset	16	
Maximum number of MTP3 links per combined linkset	256	

SCCP

Table 64: SCCP Rules for SGSN

Features	Limits	Comments
Maximum number of SCCP networks	12	
Maximum number of destination point codes (DPCs)	2048	
Maximum number of SSNs per DPC	3	

GTT

Table 65: GTT Rules for SGSN

Features	Limits	Comments
Maximum number of associated GTTs	16	
Maximum number of actions per association	15	
Maximum number of address maps	4096	
Maximum number of out-addresses per address map	20	

SGSN Interface Rules

The following information relates to the virtual interfaces supported by the SGSN:

System-Level

Table 66: System Rules on the SGSN

Features	Limits	Comments
Maximum supported size for IP packets (data)	1480	
Maximum recovery/reload time	17 mins.	

3G Interface Limits

Table 67: 3G Interface Rules for SGSN

Features	Limits	Comments
Maximum number of RNCs	See comment	Supports upto 256 directly connected RNC and 1024 indirectly connected through gateways.
Maximum number of RNCs controlling the same RA	no limit	
Maximum number of RAIs per SGSN	16K	16K is the recommended max RAI per SGSN, however, there is no hard limit imposed. Adding more RAIs may lead to memory issues.
Maximum number of RAIs per RNC	2.5K	
Maximum number of GTPU addresses per SGTP service	12	

2G Interface Limits

Table 68: 2G Interface Rules - Gb over Frame Relay

Features	Limits	Comments
Maximum number of NSEs	2048	Limit is total of FR + IP
Maximum number of RAIs per SGSN	16K	16K is the recommended max RAI per SGSN, however, there is no hard limit imposed. Adding more RAIs may lead to memory issues.
Maximum number of RAIs per NSE	2.5K	
Maximum number of NSEs controlling the same RA	no limit	
Maximum number of NSVCs per NSE	128	
Maximum number of BVCs per NSE	max / SGSN is 64000	Whether or not Gb Flex is enabled.
Maximum number of cell sites supported	64,000	

Table 69: 2G Interface Rules - Gb over IP

Features	Limits	Comments
Maximum number of NSEs	2048	Limit is total of FR + IP
Maximum number of Local NSVLs per SGSN	4	
Maximum number of Peer NSVLs per NSE	128	
Maximum number of RAIs per SGSN	16K	16K is the recommended max RAI per SGSN, however, there is no hard limit imposed. Adding more RAIs may lead to memory issues.
Maximum number of RAI per NSE	2.5K	
Maximum number of NSE controlling the same RA	no limit	
Maximum number of NSVCs per NSE	512	
Maximum number of BVCs per NSE	max / SGSN is 64000	
Maximum number of cell sites supported	64000	
Maximum number of 802.1q VLANs per Gb interface	1024	
Maximum number of RAIs per SGSN	2.5K	2.5k is the recommended max RAI per SGSN, however, there is no hard limit imposed. Adding more RAIs may lead to memory issues

Engineering Rules