



## **Cisco ASR 5000 Series Serving GPRS Support Node Administration Guide**

**Version 12.0**

**Last Updated September 30, 2011**

### **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

Text Part Number: OL-24828-02

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 following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://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.

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.

Cisco ASR 5000 Series Serving GPRS Support Node Administration Guide

© 2011 Cisco Systems, Inc. and/or its affiliated entities. All rights reserved.

# CONTENTS

---

<b>About this Guide .....</b>	<b>ix</b>
Conventions Used.....	x
Contacting Customer Support .....	xii
<b>Serving GPRS Support Node (SGSN) Overview .....</b>	<b>13</b>
Product Description .....	14
Product Specifications .....	15
Licenses .....	15
Hardware Requirements .....	15
Platforms .....	15
ASR 5000 System Hardware Components .....	15
Operating System Requirements .....	16
System Configuration Options .....	16
Benefits of Co-Located GSNs.....	16
Network Deployments and Interfaces .....	18
SGSN and Dual Access SGSN Deployments .....	18
SGSN/GGSN Deployments.....	20
SGSN Logical Network Interfaces .....	21
Features and Functionality - Basic .....	24
Automatic Protection Switching (APS).....	24
All-IP Network (AIPN) .....	25
SS7 Support .....	25
Gn/Gp Delay Monitoring.....	26
PDP Context Support.....	26
Mobility Management .....	27
GPRS Attach.....	27
GPRS Detach .....	27
Paging .....	28
Service Request.....	28
Authentication.....	28
P-TMSI Reallocation .....	28
P-TMSI Signature Reallocation.....	29
Identity Request .....	29
In Redundancy (ECMP over ATM).....	29
ECMP over ATM.....	29
Location Management .....	29
Session Management .....	30
PDP Context Activation.....	30
PDP Context Modification.....	31
PDP Context Deactivation .....	31
PDP Context Preservation.....	31
Charging .....	31
SGSN Call Detail Records (S-CDRs).....	31
Mobility Call Detail Records (M-CDRs).....	32
Short Message Service CDRs .....	32
VLR Pooling via the Gs Interface.....	32
HSPA Fallback .....	32
Tracking Usage of GEA Encryption Algorithms.....	33

Features and Functionality - Enhanced .....	34
APN Aliasing .....	35
Default APN .....	35
APN Resolution with SCHAR or RNC-ID .....	35
Avoiding PDP Context Deactivations .....	36
CAMEL Service Phase 3, Ge Interface .....	36
CAMEL Service .....	36
CAMEL Support .....	36
Ge Interface .....	37
CAMEL Configuration .....	37
Direct Tunnel .....	37
DSCP Template for Control and Data Packets - Gb over IP .....	38
Equivalent PLMN .....	38
GTP-C Path Failure Detection and Management .....	38
Intra- or Inter-SGSN Serving Radio Network Subsystem (SRNS) Relocation (3G only) .....	38
Lawful Intercept .....	39
Link Aggregation - Horizontal .....	39
Local DNS .....	39
Local Mapping of MBR .....	39
Local QoS Capping .....	40
Multiple PLMN Support .....	40
Network Sharing .....	40
Benefits of Network Sharing .....	41
GWCN Configuration .....	41
MOCN Configuration .....	42
Implementation .....	42
NPU FastPath .....	44
NRPCA - 3G .....	45
Operator Policy .....	45
Some Features Managed by Operator Policies .....	45
Overcharging Protection .....	46
QoS Traffic Policing per Subscriber .....	46
QoS Classes .....	46
QoS Negotiation .....	47
DSCP Marking .....	47
Traffic Policing .....	47
Reordering of SNDSCP N-PDU Segments .....	48
Session Recovery .....	49
SGSN Pooling and Iu-Flex / Gb-Flex .....	49
Gb/Iu Flex Offloading .....	50
Short Message Service (SMS over Gd) .....	50
SMS Authentication Repetition Rate .....	51
SMSC Address Denial .....	51
How the SGSN Works .....	52
First-Time GPRS Attach .....	52
PDP Context Activation Procedures .....	55
Network-Initiated PDP Context Activation Process .....	56
MS-Initiated Detach Procedure .....	58
Supported Standards .....	60
IETF Requests for Comments (RFCs) .....	60
3GPP Standards .....	60
ITU Standards .....	62
Object Management Group (OMG) Standards .....	62
<b>SGSN in a 2.5G GPRS Network .....</b>	<b>63</b>
2.5G SGSN Configuration Components .....	64

The SGSN_Ctx .....	66
The Accounting_Ctx .....	67
How the 2.5G SGSN Works .....	68
For GPRS and/or IMSI Attach .....	68
For PDP Activation .....	69
Information Required for the 2.5G SGSN .....	70
Global Configuration .....	70
SGSN Context Configuration .....	72
Accounting Context Configuration .....	73
<b>SGSN 3G UMTS Configuration .....</b>	<b>75</b>
3G SGSN Configuration Components .....	76
For GPRS and/or IMSI Attach .....	77
Information Required for 3G Configuration .....	78
Global Configuration .....	78
SGSN Context Configuration .....	80
Accounting Context Configuration .....	82
<b>SGSN Service Configuration Procedures .....</b>	<b>85</b>
2.5G SGSN Service Configuration .....	86
3G SGSN Service Configuration .....	88
Dual Access SGSN Service Configuration .....	89
Configuring an SS7 Routing Domain .....	91
Configuring an SS7 Routing Domain to Support Broadband SS7 Signaling .....	91
Example Configuration .....	91
Configuring an SS7 Routing Domain to Support IP Signaling for SIGTRAN .....	92
Example Configuration .....	93
Configuring GTT .....	95
Example Configuration .....	95
Configuring an SCCP Network .....	97
Example Configuration .....	97
Configuring a MAP Service .....	98
Example Configuration .....	98
Configuring an IuPS Service (3G only) .....	100
Example Configuration .....	100
Configuring an SGTP Service .....	101
Example Configuration .....	101
Configuring a Gs Service .....	102
Example Configuration .....	102
Configuring an SGSN Service (3G only) .....	103
Example Configuration .....	103
Configuring a GPRS Service (2.5G only) .....	105
Example Configuration .....	105
Configuring a Network Service Entity .....	107
Configure a Network Service Entity for IP .....	107
Example Configuration for a Network Service Entity for IP .....	107
Configure a Network Service Entity for Frame Relay .....	107
Example Configuration for a Network Service Entity for IP .....	108
Configuring DNS Client .....	109
Example Configuration .....	109
Configuring GTP Accounting Support .....	110
Creating GTP Group .....	110
Configuring GTP Group .....	111
Verifying GTP Group Configuration .....	112
Creating and Configuring ATM Interfaces and Ports (3G only) .....	113
Creating and Configuring Frame Relay Ports (2.5G only) .....	114
Configuring APS/MSP Redundancy .....	115

Example Configuration .....	115
<b>Operator Policy .....</b>	<b>117</b>
What Operator Policy Can Do .....	118
A Look at Operator Policy on an SGSN.....	118
The Operator Policy Feature in Detail .....	119
Call-Control Profile.....	119
APN Profile.....	120
IMEI-Profile (SGSN-only).....	121
APN Remap Table .....	121
Operator Policies .....	122
IMSI Ranges.....	123
How It Works.....	124
Operator Policy Configuration.....	125
Call-Control Profile Configuration.....	126
Configuring the Call Control Profile for an SGSN.....	126
Configuring the Call Control Profile for an MME or S-GW .....	126
APN Profile Configuration.....	127
IMEI Profile Configuration - SGSN only.....	127
APN Remap Table Configuration .....	128
Operator Policy Configuration .....	129
IMSI Range Configuration.....	129
Configuring IMSI Ranges on the MME or S-GW .....	129
Configuring IMSI Ranges on the SGSN.....	130
Operator Policy Component Associations - MME.....	130
Associating Operator Policy Components on the MME.....	130
Verifying the Feature Configuration .....	132
<b>Subscriber Overcharging Protection .....</b>	<b>133</b>
Feature Overview .....	134
Overcharging Protection - GGSN Configuration .....	136
GTP-C Private Extension Configuration .....	136
Verifying Your GGSN Configuration .....	137
Overcharging Protection - SGSN Configuration.....	138
Private Extension IE Configuration.....	138
RANAP Cause Trigger Configuration .....	139
Verifying the Feature Configuration .....	139
<b>Direct Tunnel.....</b>	<b>141</b>
Direct Tunnel Feature Overview.....	142
Direct Tunnel Configuration .....	146
Configuring Direct Tunnel Support on the SGSN.....	146
Enabling Setup of GTP-U Direct Tunnels.....	147
Enabling Direct Tunnel per APN .....	147
Enabling Direct Tunnel per IMEI.....	148
Enabling Direct Tunnel to Specific RNCs.....	149
Verifying the SGSN Direct Tunnel Configuration .....	149
Configuring S12 Direct Tunnel Support on the S-GW.....	152
<b>Verifying and Saving Your Configuration.....</b>	<b>155</b>
Verifying the Configuration.....	156
Feature Configuration.....	156
Service Configuration.....	157
Context Configuration.....	157
System Configuration.....	158
Finding Configuration Errors .....	158
Saving the Configuration .....	159

Saving the Configuration on the Chassis.....	160
<b>Monitoring and Troubleshooting.....</b>	<b>163</b>
Monitoring.....	164
Daily - Standard Health Check .....	164
Monthly System Maintenance .....	167
Every 6 Months .....	167
Troubleshooting.....	168
Problems and Issues.....	168
Troubleshooting More Serious Problems .....	168
Causes for Attach Reject.....	168
Single Attach and Single Activate Failures .....	169
Mass Attach and Activate Problems .....	170
Single PDP Context Activation without Data .....	171
Mass PDP Context Activation but No Data .....	172
<b>Engineering Rules .....</b>	<b>173</b>
Service Rules.....	174
SGSN Connection Rules .....	175
Operator Policy Rules .....	176
SS7 Rules .....	178
SS7 Routing.....	178
SIGTRAN.....	178
Broadband SS7 .....	179
SCCP .....	179
GTT .....	179
SGSN Interface Rules .....	180
System-Level.....	180
3G Interface Limits.....	180
2G Interface Limits.....	181









# About this Guide

---

This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

## Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	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.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a <code>screen display</code>	This typeface represents displays that appear on your terminal screen, for example: <code>Login:</code>
Text represented as <code>commands</code>	This typeface represents commands that you enter, for example: <code>show ip access-list</code> This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a <code>command variable</code>	This typeface represents a variable that is part of a command, for example: <code>show card slot_number</code> <code>slot_number</code> is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the <b>File</b> menu, then click <b>New</b>

Command Syntax Conventions	Description
{ <code>keyword</code> or <code>variable</code> }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

Command Syntax Conventions	Description
[ <b>keyword</b> or <i>variable</i> ]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
	<p>With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter).</p> <p>Pipe filters can be used in conjunction with required or optional keywords or variables. For example:</p> <pre>{ <b>nonce</b>   <b>timestamp</b> }</pre> <p>OR</p> <pre>[ <b>count</b> <i>number_of_packets</i>   <b>size</b> <i>number_of_bytes</i> ]</pre>

# Contacting Customer Support

Use the information in this section to contact customer support.

**For New Customers:** 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 is required to this site. Please contact your local sales or service representative for additional information.

**For Existing Customers with support contracts through Starent Networks:** Refer to the support area of <https://support.starentnetworks.com/> for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.



**Important:** For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

---

# Chapter 1

## Serving GPRS Support Node (SGSN) Overview

---

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

- [Product Description](#)
- [Product Specifications](#)
- [Network Deployments and Interfaces](#)
- [Features and Functionality - Basic](#)
- [Features and Functionality - Enhanced](#)
- [How the SGSN Works](#)
- [Supported Standards](#)

## Product Description

The ASR 5000 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.



**Important:** Throughout this chapter 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.

This chapter 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.

# Product Specifications

The following information is located in this section:

- [Licenses](#)
- [Hardware Requirements](#)
- [Operating System Requirements](#)
- [System Configuration Options](#)

## Licenses

The SGSN is a licensed product and requires the purchase and installation of the SGSN Software License.

As well, the SGSN provides several features, such as Lawful Intercept, that require license keys be acquired and installed for feature use. For more information about licenses for the SGSN, ask your Cisco Account Representative.

## Hardware Requirements

Information in this section describes the hardware required to support SGSN services.

### Platforms

The SGSN operates on an ASR 5000.

### ASR 5000 System Hardware Components

The following application and line cards are required to support GPRS/UMTS wireless data services on the SGSN:

- **System Management Cards (SMCs):** Provides full system control and management of all cards within the ASR 5000. Up to two SMCs can be installed; one active, one redundant.
- **Packet Services Cards (PSCs):** Within the chassis, PSCs (either PSC or PSC2) provide high-speed, multi-threaded PDP context processing capabilities for 2.5G SGSN, 3G SGSN, and GGSN services. Up to 14 PSCs can be installed, allowing for multiple active and/or redundant cards.
- **Switch Processor Input/Outputs (SPIOs):** Installed in the upper-rear chassis slots directly behind the SMCs, SPIOs provide connectivity for local and remote management, central office (CO) alarms, and BITS timing. Up to 2 SPIOs can be installed: 1 active, 1 redundant.
- **Line Cards:** Installed directly behind PSCs, these cards provide the physical interfaces from the SGSN to various elements in the GPRS/UMTS data network. Up to 26 line cards can be installed for a fully loaded

system with 13 active PSCs, 13 in the upper-rear slots and 13 in the lower-rear slots for redundancy. Redundant PSCs do not require line cards.

Depending on the SGSN network environment, the system supports multiple types of line cards, simultaneously if needed:

- Various types of Ethernet line cards provide IP connections:
  - Ethernet 10/100 line cards
  - Ethernet 1000 line cards
  - 4-port Quad Gig-E line cards (QGLCs)
  - 10-Gigabit Ethernet line cards (XGLCs)
- Optical (ATM over SDH/SONET) Line Cards (OLC or OLC2) - ATM/POS OC-3 Single Mode or Multi-Mode optical fiber line cards providing SS7 broadband signaling, e.g., SIGTRAN over ATM via E1/DS1 (T1) signaling
- Channelized Line Cards (CLC or CLC2) - STM-1/OC-3 provides Frame Relay over SDH/SONET signaling
- **Redundancy Crossbar Cards (RCCs):** Installed in the lower-rear chassis slots directly behind the SMCs, RCCs utilize 5 Gbps serial links to ensure connectivity between Ethernet 10/100 or Ethernet 1000 line cards/QGLCs and every PSC in the system for redundancy. Two RCCs can be installed to provide redundancy for all line cards and PSCs.

Additional information, for each of the application and line cards required to support GPRS/UMTS wireless data services, is located in the *Cisco ASR 5000 Hardware Installation and Administration Guide*.

## Operating System Requirements

The SGSN is available for all ASR 5000s running StarOS 8.0 or higher.

## System Configuration Options

An ASR 5000 SGSN system supports multiple GPRS Support Node (GSN) service applications, in any combination, co-located within a single chassis, for example:

- 2.5G SGSN and 3G SGSN - Dual Access
- SGSN (2.5G or 3G) and GGSN

## Benefits of Co-Located GSNs

*Integrated co-location* is done without introducing proprietary protocols, thus avoiding mobility and handoff issues. Multiple network element applications, integrated as a single application within a single chassis, benefit carriers for the following reasons:



- Same hardware for all services
- Load sharing architecture ensures that all hardware is used efficiently
- Single software load
- Uniform configuration
- Optimal usage of the high capacity system
- Reduced latency in the control and data paths
- Simplification of network architecture
- Single platform-view, maintained even in the presence of multiple services
- Fewer IP addresses needed
- No internal interfaces
- Combined SGSN/GGSN serve other SGSNs and GGSNs with no loss of functionality
- Hand-offs between 2.5G and 3G networks can re-use the same SAU state; this avoids repeated exchanges with the HLR thereby reducing the number of interaction messages
- Operating as a combined SGSN/GGSN, the common processes host both SGSN and GGSN sessions resulting in optimized hardware usage and latency
- Combined with Iu-Flex and Gb-Flex, an SGSN/GGSN system enables single-hop core network routing (a given session is always routed to the same combined node)

## Network Deployments and Interfaces

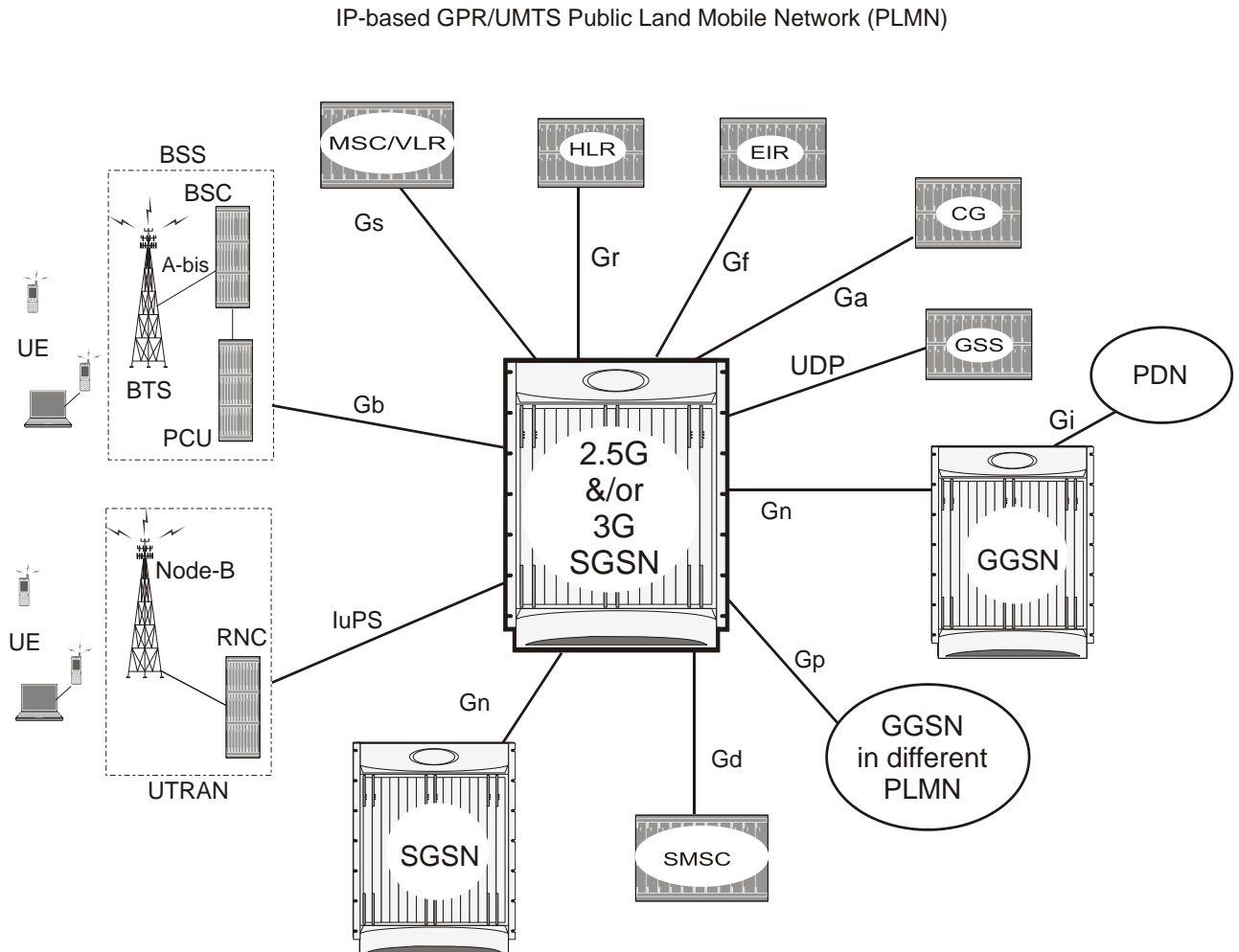
The following logical connections maps indicate the SGSN's ability to connect to both 2G (GSM BSS) and 3G (UMTS RAN) radio access networks, a mobile service center (MSC) and visitor location register (VLR), a home location register (HLR), a charging gateway (CG - sometimes referred to as a charging gateway function (CGF)), a GTPP storage server (GSS), a standalone GGSN, network devices in another PLMN, an SMS server center, and a standalone SGSN.

## 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 the ASR 5000 enables a single chassis to reduce hardware requirements by supporting integrated co-location of a variety of the GPRS/UMTS 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; or multiple instances of 3G SGSNs; or a combination of 2.5G and 3G SGSN to comprise a dual access SGSN.

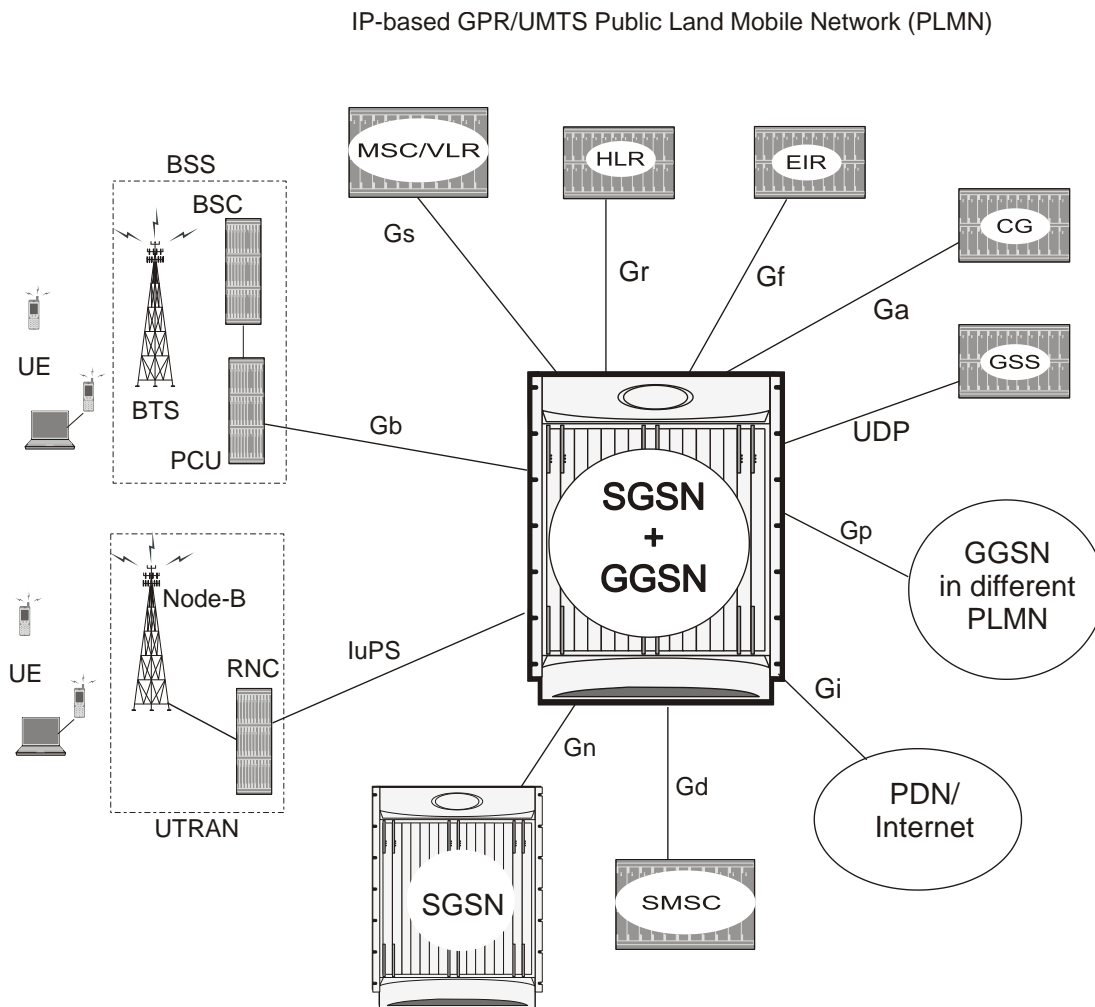
Figure 1. Dual Access 2.5G/3G SGSNs



## SGSN/GGSN Deployments

The co-location of the SGSN and the GGSN in the same chassis facilitates handover. Again, it can be any type of SGSN, 2.5G or 3G, with the GGSN.

**Figure 2. Co-located SGSN and GGSN**



## 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:

- **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
- **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) or Frame Relay (via a Channelized SDH or SONET 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 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)
- Transport over ATM/STM-1Optical, Fast Ethernet, and Ethernet 1000 line cards/QGLCs)
- 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
- **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
- **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.
- **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.
- **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
- **Ga:** The SGSN uses the Ga interface with GTP 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.

## Features and Functionality - Basic

The 2.5G and 3G SGSNs support a broad range of features and functionality. All features are either proprietary or are fully compliant with 3GPP standards. The following is a list of *some* of the features supported by the SGSN:

- [Automatic Protection Switching \(APS\)](#)
- [All-IP Network \(AIPN\)](#)
- [SS7 Support](#)
- [PDP Context Support](#)
- [Mobility Management](#)
- [Iu Redundancy \(ECMP over ATM\)](#)
- [Location Management](#)
- [Session Management](#)
- [Charging](#)
- [Tracking Usage of GEA Encryption Algorithms](#)

### 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 ASR 5000 APS/MSP supports the following 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.

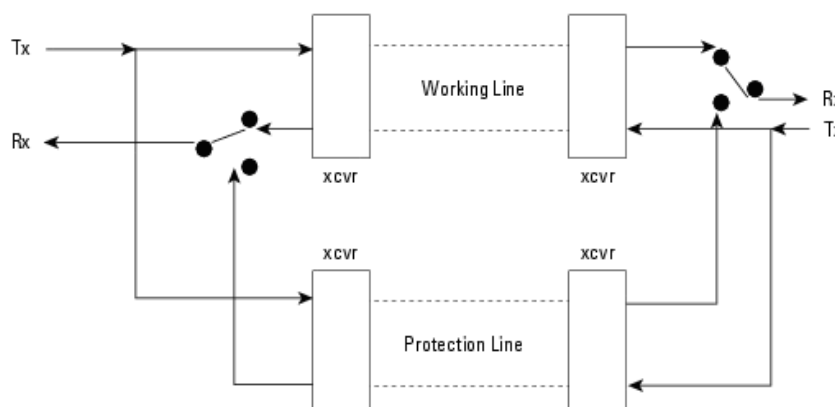
With the non-revertive option, if a signal fail condition is detected, the hardware switches to the protection line and does not automatically revert back to the working line.

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 3. SONET APS 1+1**



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

## 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.

## SS7 Support

The ASR 5000 SGSN implements SS7 functionality to communicate with the various SS7 network elements, such as HLRs and VLRs.

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

- Transport layer support includes:
  - Broadband SS7 (MTP3B/SSCF/SSCOP/AAL5)
  - Narrowband SS7 (high speed and low speed)
  - 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
  - MTP3
  - SCCP with BSSAP+ and RANAP
  - ISUP
  - TCAP and MAP

## 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.

## 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, 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" chapter in the *Cisco ASR 5000 Series 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 on configurable 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.

## Iu Redundancy (ECMP over ATM)

Iu Redundancy is the ASR 5000's implementation of equal-cost multi-path routing (ECMP) over ATM.

### 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.

## 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 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

To provide efficient and accurate billing for calls and SMS passing through the SGSN, the system:

- allows the configuration of multiple CGFs and GSSs and their relative priorities.
- implements the standardized Ga interface based on GTPP over UDP and all relevant charging information as defined in 3GPP TS.32.251 v 7.2.0.

## 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.

## 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:  $[(\text{IMSI} \div 10) \bmod 1000]$ . 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" chapter in the *Cisco ASR 5000 Series Command Line Interface Reference*.

## 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* chapter in the *Cisco ASR 5000 Series Command Line Interface Reference*.

## 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.

## Features and Functionality - Enhanced

Enhanced features add or expand the capabilities of the SGSN beyond levels of basic operation. All of these features are either proprietary or comply with relevant 3GPP specifications.

A few of these features require the purchase of an additional license to implement the functionality on the SGSN. For information about licenses, ask your Cisco Account Representative.

The following is an alphabetical list of the enhanced features:

- [APN Aliasing](#)
- [APN Resolution with SCHAR or RNC-ID](#)
- [Avoiding PDP Context Deactivations](#)
- [CAMEL Service Phase 3, Ge Interface](#)
- [Direct Tunnel](#)
- [DSCP Template for Control and Data Packets - Gb over IP](#)
- [Equivalent PLMN](#)
- [GTP-C Path Failure Detection and Management](#)
- [Intra- or Inter-SGSN Serving Radio Network Subsystem \(SRNS\) Relocation \(3G only\)](#)
- [Lawful Intercept](#)
- [Link Aggregation - Horizontal](#)
- [Local DNS](#)
- [Local Mapping of MBR](#)
- [Local QoS Capping](#)
- [Multiple PLMN Support](#)
- [Network Sharing](#)
- [NPU FastPath](#)
- [NRPCA - 3G](#)
- [Operator Policy](#)
- [Overcharging Protection](#)
- [QoS Traffic Policing per Subscriber](#)
- [Reordering of SND CP N-PDU Segments](#)
- [Session Recovery](#)
- [SGSN Pooling and Iu-Flex Gb-Flex](#)
- [Short Message Service \(SMS over Gd\)](#)
- [SMS Authentication Repetition Rate](#)
- [SMSC Address Denial](#)

## 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 an HFL-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 *Cisco ASR 5000 Series Command Line Interface Reference* for the command to configure this feature.

## 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 (enhancement CSCtr10048), and if inclusion of the profile index of the charging characteristics information is enabled (per this enhancement) 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.

## 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). By 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.

## CAMEL Service Phase 3, Ge Interface

The ASR 5000 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

ASR 5000 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 ASR 5000 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 ASR 5000 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 SIGTAN.

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 *Cisco ASR 5000 Series Serving GPRS Support Node Administration Guide* and the *Cisco ASR 5000 Series Command Line Interface Reference*.

## 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* chapter in this guide.

## DSCP Template for Control and Data Packets - Gb over IP

One or more reusable templates, setting DSCP parameter configuration for downlink control packets and data packets, can be created and associated with one or more GPRS Service configurations.

## 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.

## 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.

## 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. For additional information and documentation on the Lawful Intercept feature, contact your local Cisco Account Representative.

## Link Aggregation - Horizontal

The SGSN supports enhanced link aggregation (LAG) within ports on different side-by-side XGLCs. Ports can be from multiple XGLCs with some cards in L2 (side-by-side) redundancy. 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. With side-by-side redundancy on the XGLC, link aggregation supports horizontal ports from both XGLC cards.

## 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. For details, refer to CSCzn32233 in the CLI Syntax section of the Interface Changes section of this release note.



**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* chapter of the *Cisco ASR 5000 Series Command Line Interface Reference* for the `qos` command.

## 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 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

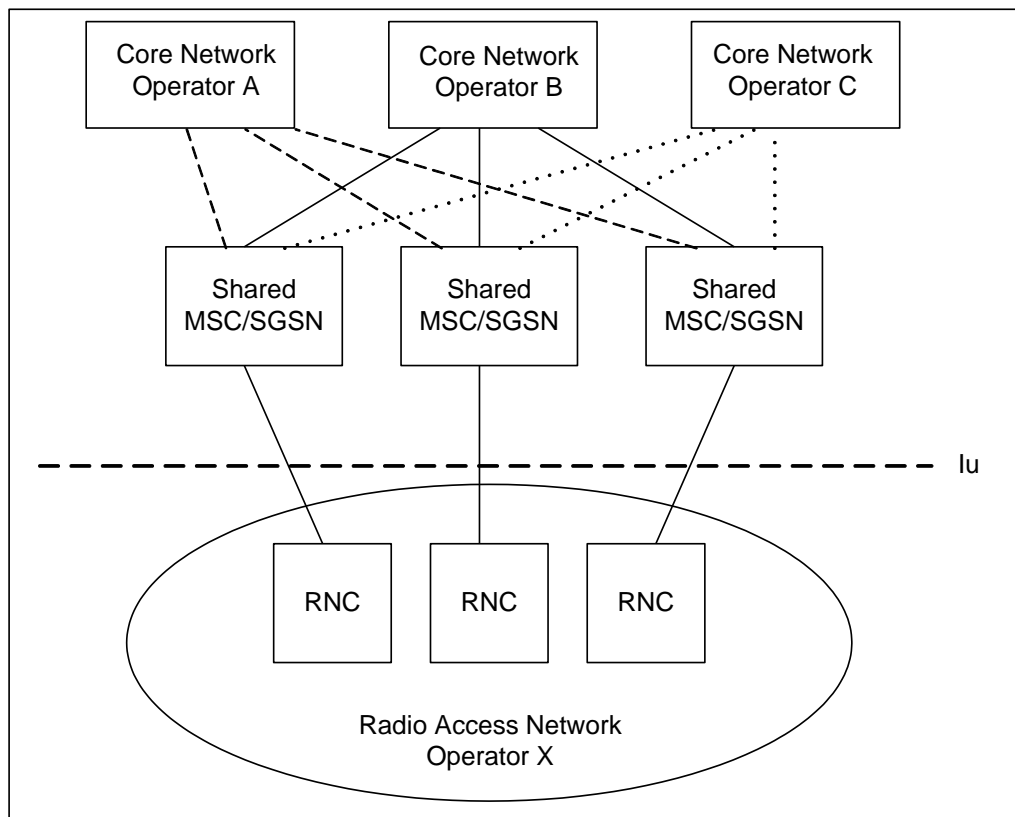
Network sharing provides operators with a range of logistical and operational benefits:

- 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

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 4. GWCN-type Network Sharing**



With the GWCN configuration, the SGSN supports two scenarios:

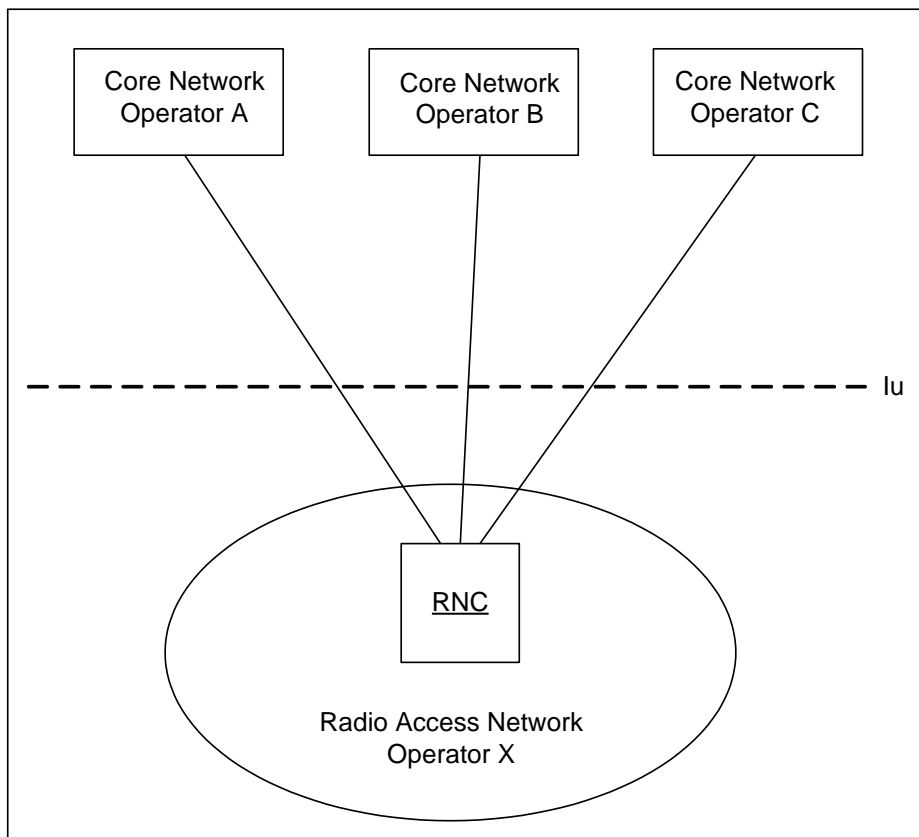
- GWCN with non-supporting UE

- 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.

**Figure 5. MOCN-type Network Sharing**



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

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

## 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 configuraiton mode.
- IMSI ranges are defined in the SGSN-Global configuration mode
- The Call-Control Profile and IMSI ranges are associated in the configuration mode.

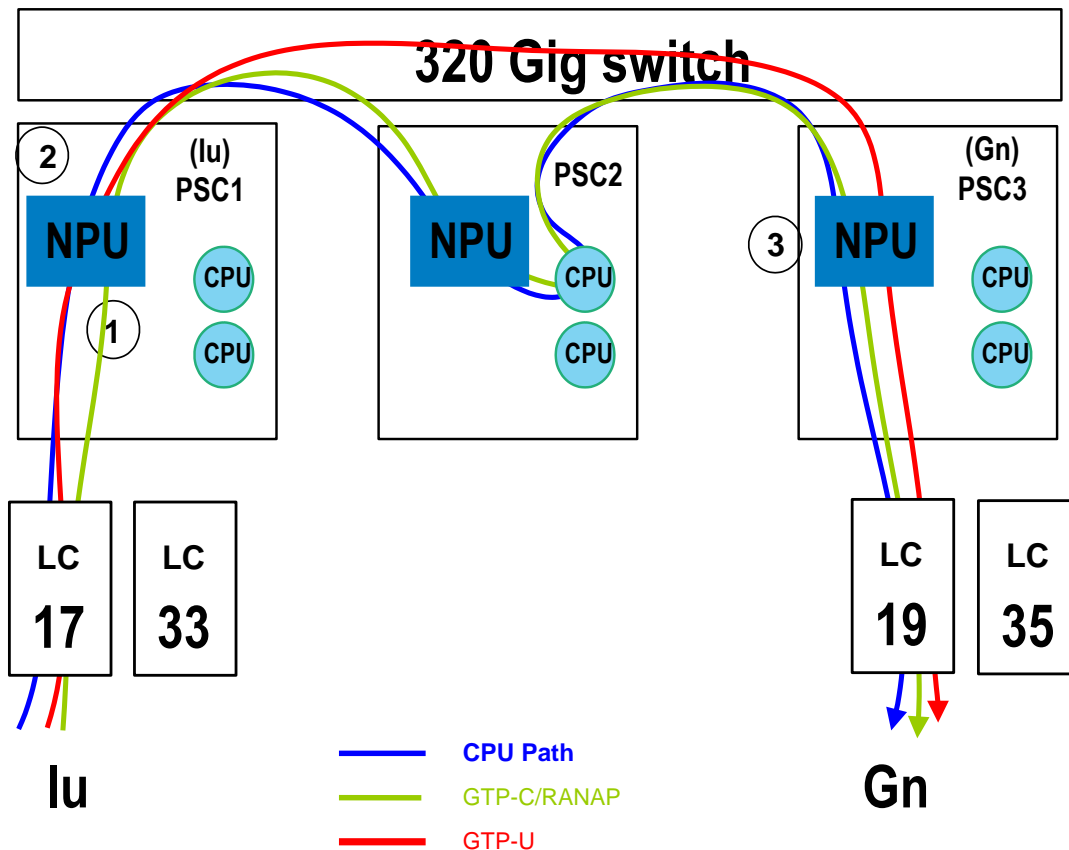
For commands and information on network sharing configuration, refer to the Service Configuration Procedures section in the *Cisco ASR 5000 Series Serving GPRS Support Node Administration Guide* and the command details in the *Cisco ASR 5000 Series Command Line Interface Reference*.

## NPU FastPath

NPU FastPath's proprietary internal direct tunnel optimizes resource usage and reduces latency when processing GTP-U packets. This proprietary feature is only available on the ASR 5000 SGSN.

Incoming traffic passes through the switch fabric and the routing headers are changed to re-route traffic from the incoming network processing unit (NPU) of the ingress PSC directly to the outgoing NPU of the egress PSC. This means that intervening NPUs and CPUs are by-passed. This provides the SGSN with router-like latency and increased node signaling capacity.

Figure 6. SGSN NPU FastPath



FastPath is established when both ends of a tunnel are available. Two FastPath flows are established, one for the uplink and one for the downlink direction for a given PDP context. FastPath will temporarily go down or be disengaged so that packets temporarily do not move through FastPath when either an Intra-SGSN RAU or an Iu-Connection Release occurs.

If FastPath cannot be established, the NPU forwards the GTP-U packets to a CPU for processing and they are processed like all other packets.

FastPath can not be established for subscriber PDP sessions if:

- Traffic Policing and Shaping is enabled.
- Subscriber Monitoring is enabled.
- Lawful Intercept (LI) is enabled,
- IP Source Violation Checks are enabled.
- GTP-v0 tunnel is established with an GGSN.

For NPU fast path configuration, refer to Enabling NPU Fast Path for GTP-U Processing section of “Service Configuration Procedures” chapter of *Cisco ASR 5000 Series Serving GPRS Support Node Administration Guide*.

## NRPCA - 3G

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

Whenever there is downlink data at the GGSN for a subscriber, but there is no valid context for the already-established PDP address, the GGSN initiates an NRPCA procedure towards the SGSN. Prior to starting the NRPCA procedure, the GGSN either obtains the SGSN address from the HLR or uses the last SGSN address of the subscriber available at the GGSN.

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 *Cisco ASR 5000 Series Command Line Interface Reference*

## Operator Policy

The non-standard feature is unique to the ASR 5000 SGSN. This feature empowers the carrier with unusual and flexible control to manage functions that aren't 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 chapter 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* chapter 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, refer to the *Subscriber Overcharging Protection* chapter in this guide.

## Overcharging Protection

Overcharging Protection enables the 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* chapter 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.

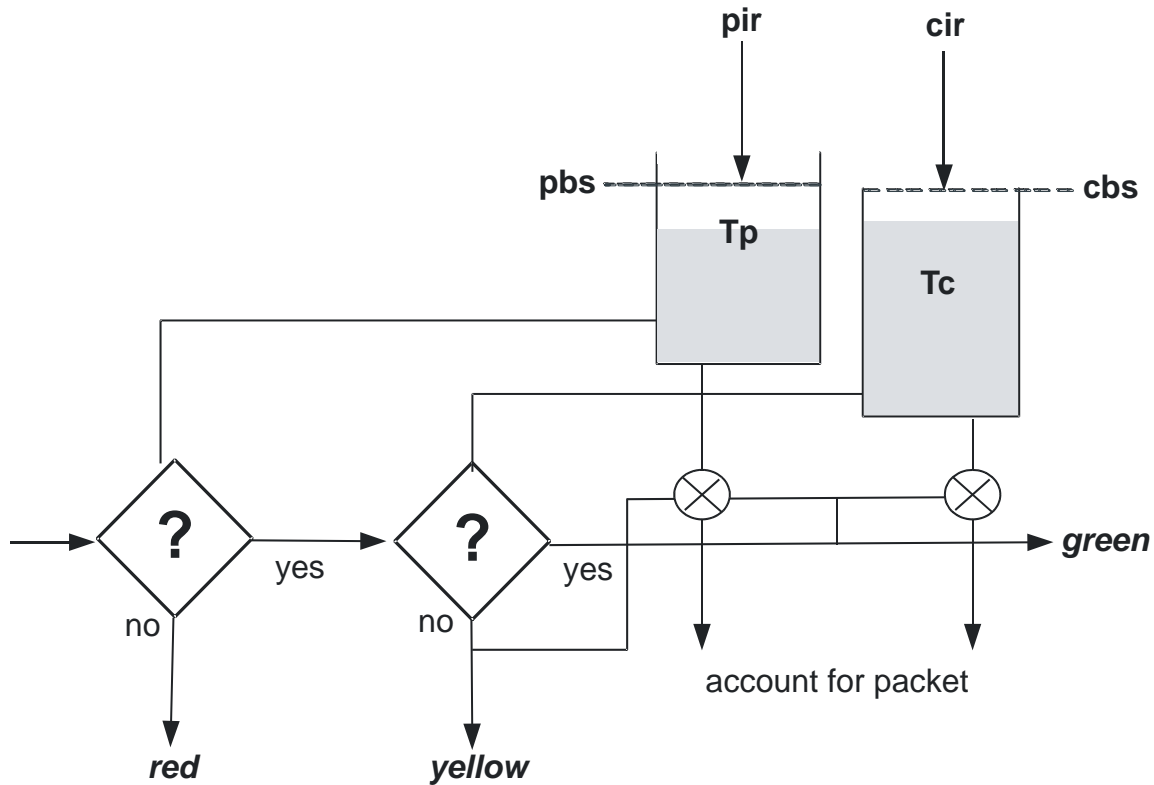
## Traffic Policing

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 trTCM algorithm:

Figure 7. TCM Algorithm Logic for Traffic Policing



For commands and more information on traffic policing configuration, refer to the *Cisco ASR 5000 Series Command Line Interface Reference*.

## Reordering of SND CP N-PDU Segments

The SGSN fully supports reordering of out-of-order segments coming from the same SND CP 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 expires, then all queued segments are dropped.



## 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 processor card (PSC or PSC2) 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 PSC 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 processor card (PSC/PSC2).

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 processor card recovery mode:** Used when a PSC/PSC2 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* chapter in the *Cisco ASR 5000 Series System Administration Guide*.

## 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.

## 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).

## 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* chapter in the *Cisco ASR 5000 Series 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.

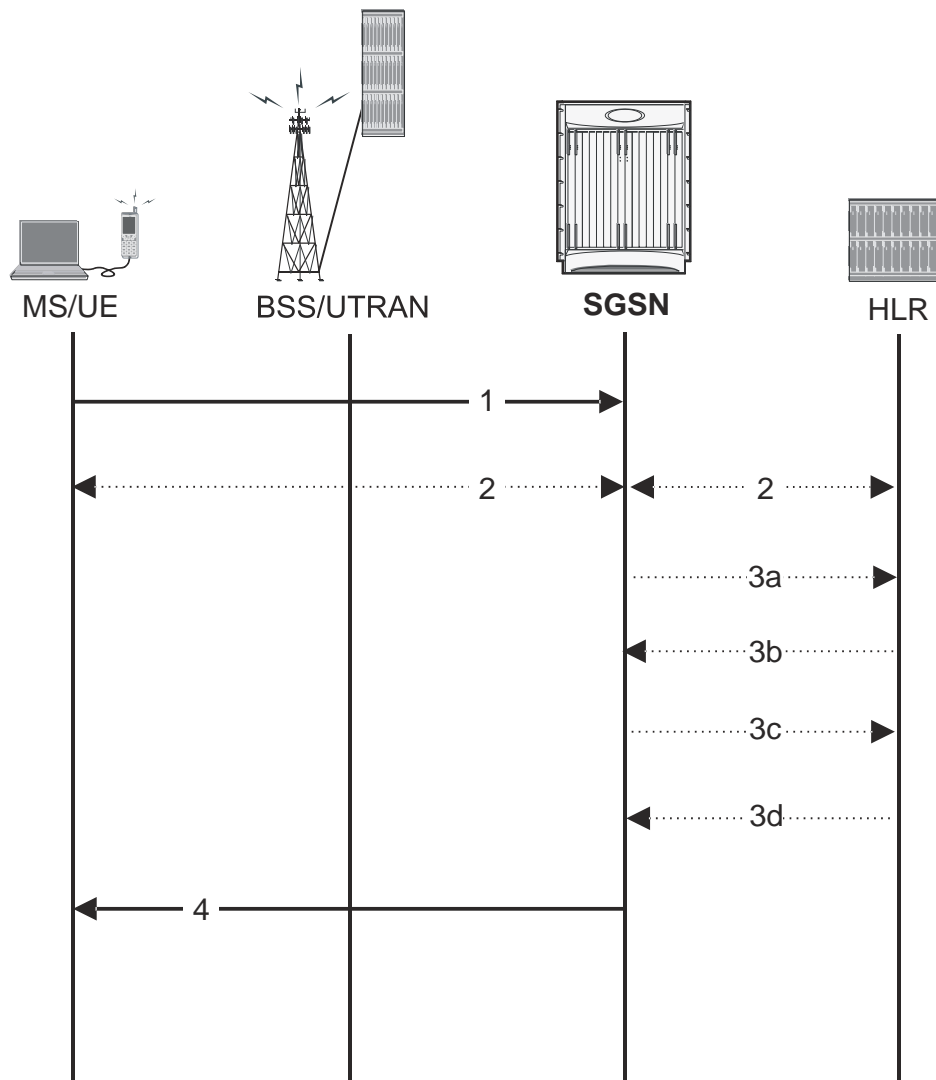
Now, the SGSN can restrict forwarding of SMS messages to specific SMSC addresses, in order to allow operators to block SMS traffic that cannot be charged for. This functionality supports multiple SMSCs and is configurable per SMSC address with a maximum of 10 addresses. It is also configurable for MO-SMS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

## 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 1. First-Time GPRS Attach Procedure**

Step	Description
1	<p>The MS/UE sends an Attach Request message to the SGSN. Included in the message is information, such as:</p> <ul style="list-style-type: none"> <li>• Routing area and location area information</li> <li>• Mobile network identity</li> <li>• Attach type</li> </ul>

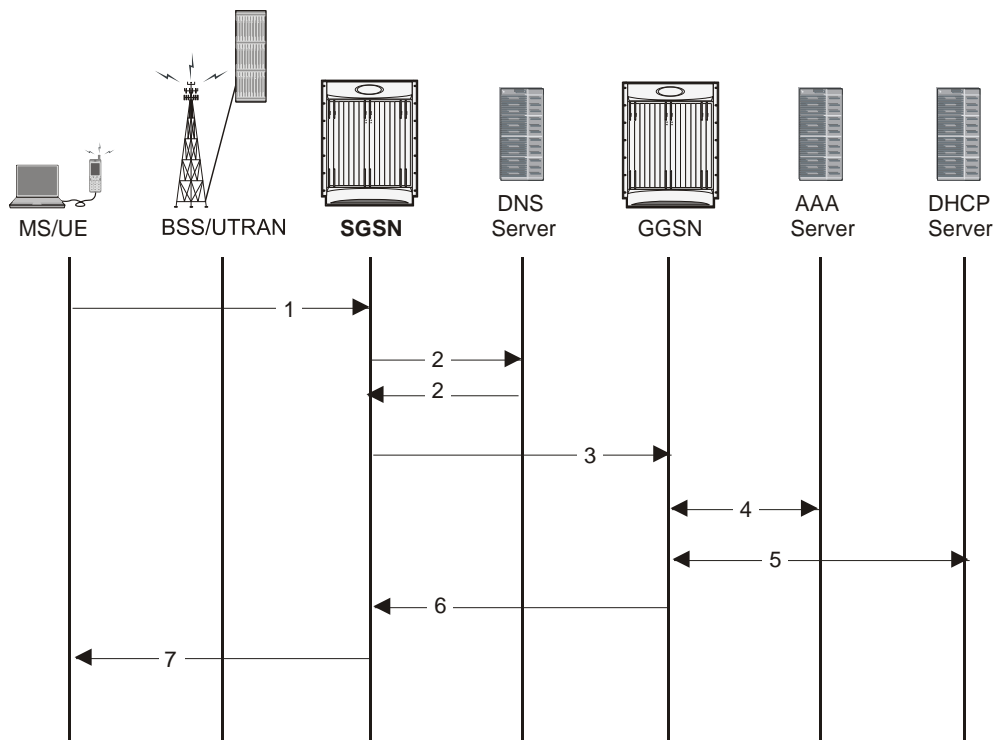
Step	Description
2	<p>Authentication is mandatory if no MM context exists for the MS/UE:</p> <ul style="list-style-type: none"> <li>• The SGSN gets a random value (RAND) from the HLR to use as a challenge to the MS/UE.</li> <li>• The SGSN sends a Authentication Request message to the UE containing the random RAND.</li> <li>• 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).</li> <li>• The MS/UE sends a Authentication Response to the SGSN containing the SRES.</li> </ul>
3	<p>The SGSN updates location information for the MS/UE:</p> <p>a) The SGSN sends an Update Location message, to the HLR, containing the SGSN number, SGSN address, and IMSI.</p> <p>b) The HLR sends an Insert Subscriber Data message to the “new” SGSN. It contains subscriber information such as IMSI and GPRS subscription data.</p> <p>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.</p> <p>d) The HLR sends a Update Location Ack to the SGSN after it successfully clears the old MM context and creates new one</p>
4	<p>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.</p> <p>At this point the GPRS Attach is complete and the SGSN begins generating M-CDRs.</p>

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 2. PDP Context Activation Procedure**

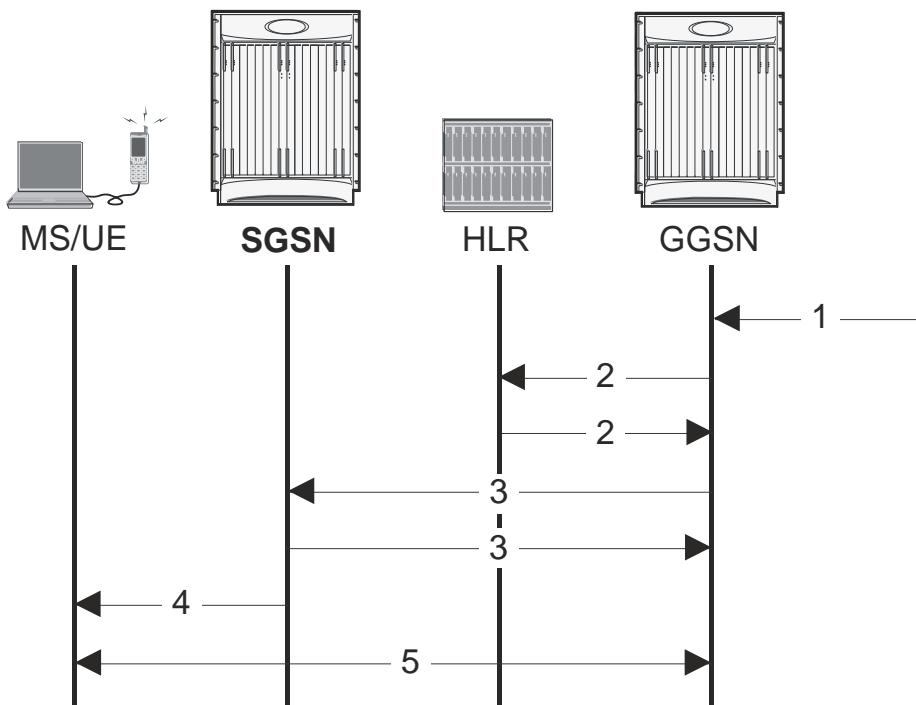
Step	Description
1	The MS/UE sends a PDP Activation Request message to the SGSN containing an Access Point Name (APN).
2	The SGSN sends a DNS query to resolve the APN provided by the MS/UE to a GGSN address. The DNS server provides a response containing the IP address of a GGSN.
3	The SGSN sends a Create 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.
5	If the MS/UE requires an IP address, the GGSN may allocate one dynamically via DHCP.

Step	Description
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.



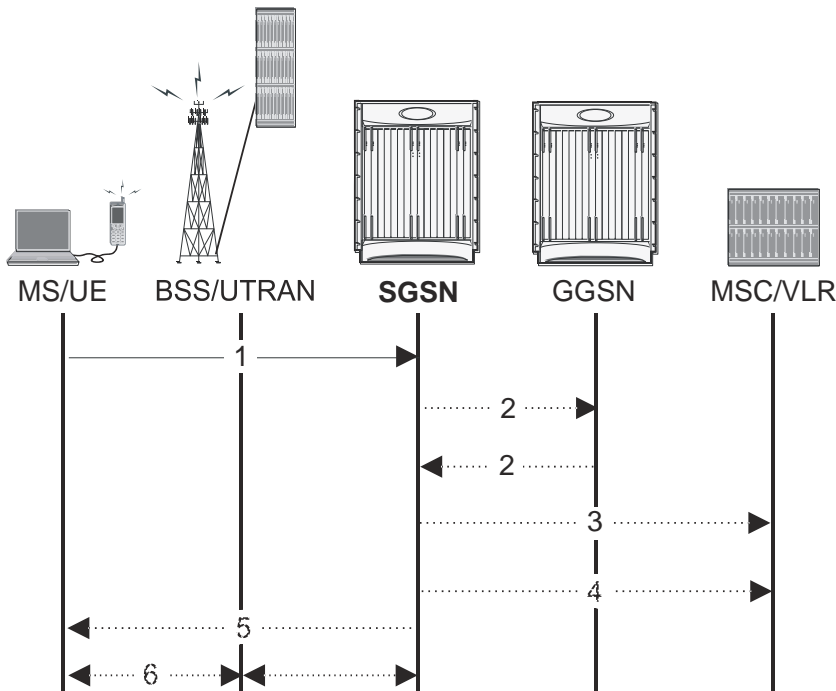
**Table 3. Network Invites MS/UE to Activate PDP Context**

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 address of the target SGSN and it may also indicate if 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 4. 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.

Step	Description
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 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

Release 6 and higher is supported for all specifications unless otherwise noted.

- **3GPP TS 22.041 v8.1.0** (2007-06), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Operator Determined Barring (ODB) (Release 8)
- **3GPP TS 23.060 v7.4.0** (2007-03), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2
- **3GPP TS 23.107 v7.0.0** (2007-06), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture
- **3GPP TS 23.236 v7.0.0** (2006-12), 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 (Release 7)
- **3GPP TS 23.251 v7.0.0** (2007-06), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Sharing; Architecture and functional description
- **3GPP TS 24.008 v6.16.0** (2007-06), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3; some features support v7.8.0 (2007-06) and v7.12.0 (2007-06)
- **3GPP TS 25.410 v6.5.0** (2006-03) and **v7.0.0** (2006-03), 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu Interface: general aspects and principles

- **3GPP TS 25.411 v7.0.0** (2006-03) and (2007-06), 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface layer 1
- **3GPP TS 25.412 v7.1.0** (2006-06), 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface signaling transport
- **3GPP TS 25.413 v6.14.0** (2007-06), 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface RANAP signaling; some features support v7.6.0 (2007-06)
- **3GPP TS 25.414 v7.1.0** (2006-06), 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface data transport and transport signaling
- **3GPP TS 25.415 v6.3.0** (2006-06), 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface user plane protocols
- **3GPP TS 29.002 v6.15.0** (2006-12), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Mobile Application Part (MAP) specification
- **3GPP TS 29.016 v6.0.0** (2004-12), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Serving GPRS Support Node SGSN - Visitors Location Register (VLR); Gs Interface Network Service Specification
- **3GPP TS 29.018 v6.5.0** (2006-12), 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
- **3GPP TS 29.060 v6.17.0** (2007-06), 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
- **3GPP TS 29.202 v8.0.0** (2007-06), 3rd Generation Partnership Project; Technical Specification Group Core Network; SS7 signaling Transport in Core Network; Stage 3
- **3GPP TS 32.215 v5.9.0** (2007-10), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging data description for the Packet Switched (PS) domain
- **3GPP TS 32.251 v7.4.0** (2007-10), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Packet Switched (PS) domain charging
- **3GPP TS 32.298 v7.4.0** (2007-10), 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- **3GPP TS 33.102 v6.5.0** (2005-12), Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture
- **3GPP TS 33.107 v6.4.0** (2004-12), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions
- **3GPP TS 44.064 v7.1.0** (2007-03), 3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile Station - Serving GPRS Support Node (MS-SGSN); Logical Link Control (LLC) layer specification
- **3GPP TS 48.014 v7.3.0** (2006-12), 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
- **3GPP TS 48.016 v7.3.0** (2006-12), 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

## ■ Supported Standards

- **3GPP TS 48.018 v7.10.0** (2007-06), 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)
- Appendix 1: SGSN-TRS\_QoS-3GPP Standards

## ITU Standards

- **Q711**; 3GPP TS 29.002 v6.15.0 (2007-12), 3GPP TS 29.016 v7.0.0 (2007-08), and 3GPP TS 25.410 v7.0.0 (2006-03)
- **Q712**; 3GPP TS 29.002 v6.15.0 (2007-12), 3GPP TS 29.016 v7.0.0 (2007-08), and 3GPP TS 25.410 v7.0.0 (2006-03)
- **Q713**; 3GPP TS 29.002 v6.15.0 (2007-12), 3GPP TS 29.016 v7.0.0 (2007-08), and 3GPP TS 25.410 v7.0.0 (2006-03)
- **Q714**; 3GPP TS 29.002 v6.15.0 (2007-12), 3GPP TS 29.016 v7.0.0 (2007-08), and 3GPP TS 25.410 v7.0.0 (2006-03)
- **Q715**; 3GPP TS 29.002 v6.15.0 (2007-12), 3GPP TS 29.016 v7.0.0 (2007-08), and 3GPP TS 25.410 v7.0.0 (2006-03)
- **Q716**; 3GPP TS 29.002 v6.15.0 (2007-12), 3GPP TS 29.016 v7.0.0 (2007-08), and 3GPP TS 25.410 v7.0.0 (2006-03)
- **Q771**; 3GPP TS 29.002 v6.15.0 (2007-12)
- **Q772**; 3GPP TS 29.002 v6.15.0 (2007-12)
- **Q773**; 3GPP TS 29.002 v6.15.0 (2007-12)
- **Q774**; 3GPP TS 29.002 v6.15.0 (2007-12)
- **Q775**; 3GPP TS 29.002 v6.15.0 (2007-12)

## Object Management Group (OMG) Standards

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

# Chapter 2

## 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

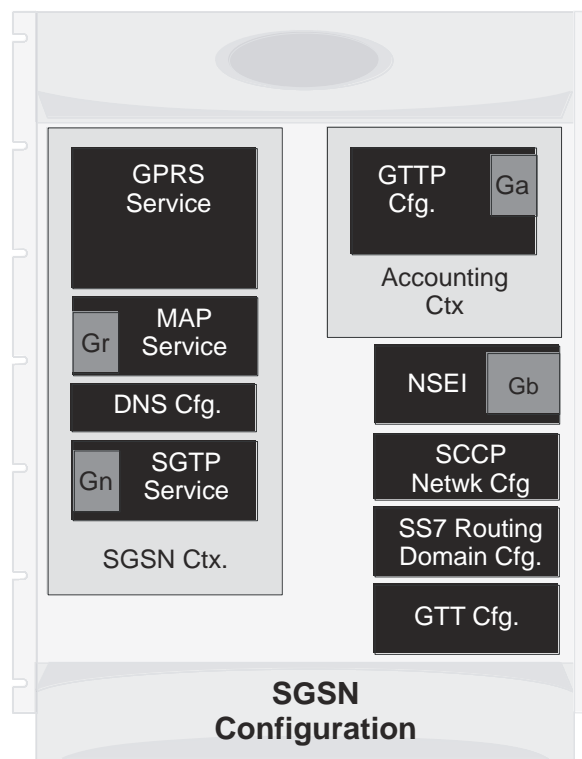
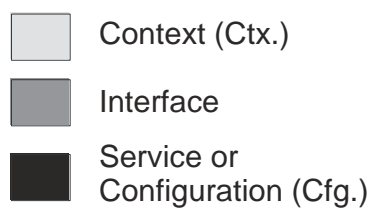
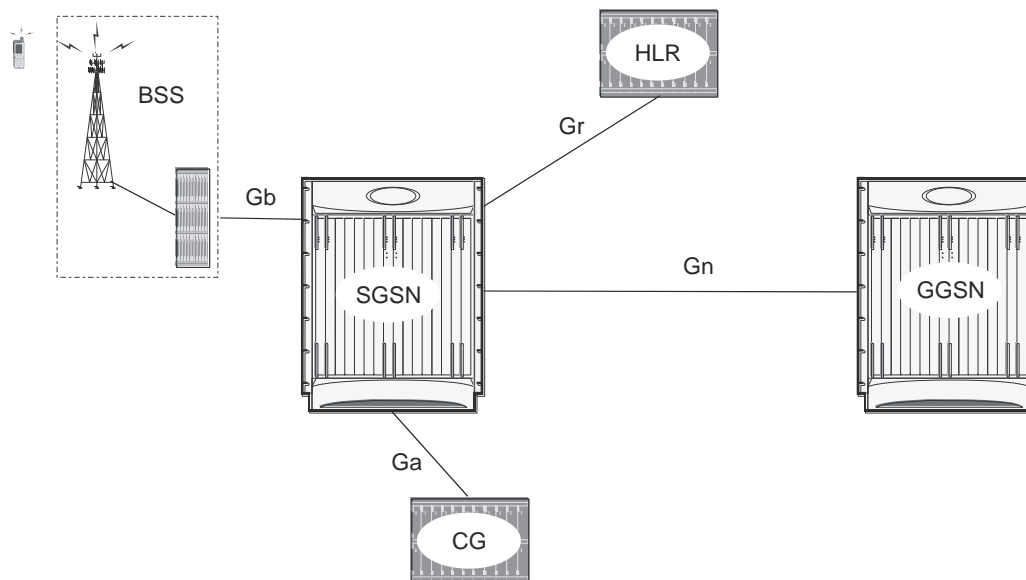
To simplify configuration management, more contexts can be created to categorize the service configuration. Each context can be named as needed. The contexts listed above can be configured as illustrated in the figure on the next page.

## 2.5G SGSN Configuration Components

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.

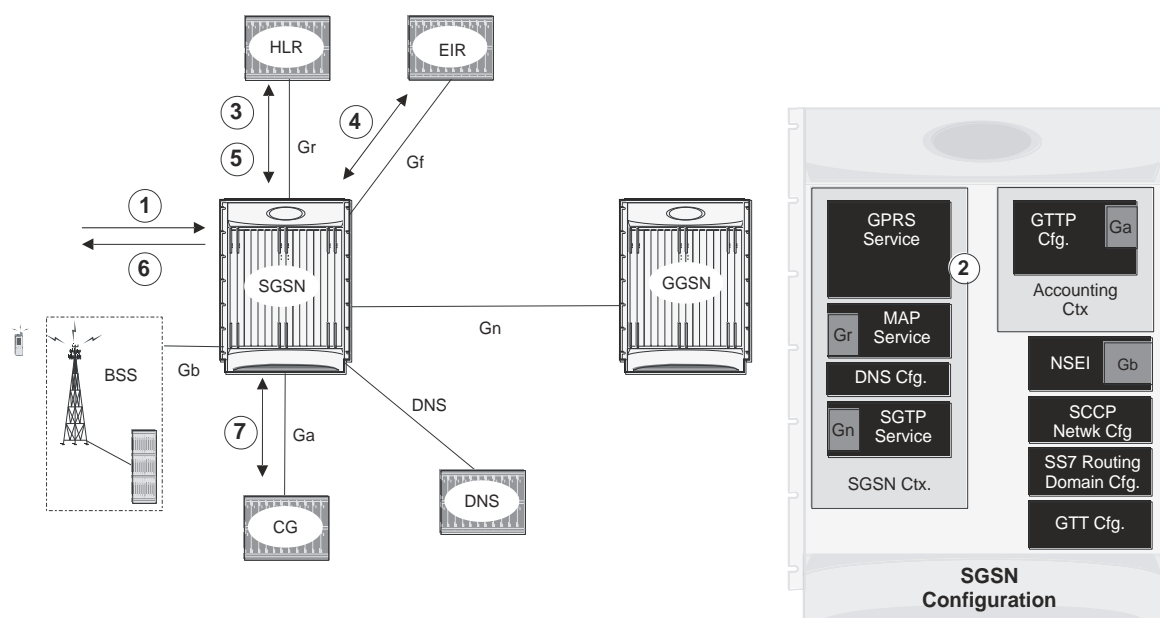
## How the 2.5G SGSN Works

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**



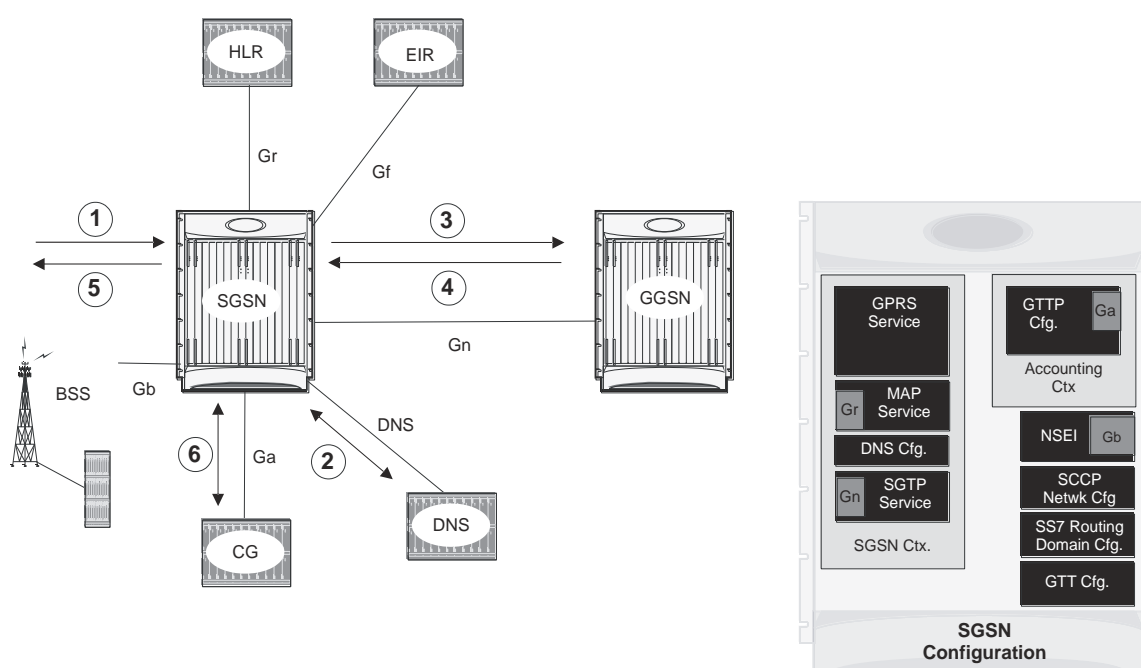
1. An Attach Request message is sent from the UE to the SGSN by the BSS over the Gb interface. This is Typically a Frame Relay connection.
2. The SGSN identifies UE and determines IMSI. Depending on whether or not the UE is already attached, this could be a simple database lookup or it could require 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

The following table lists the information that is required to be configured in Global Configuration mode.

**Table 5. 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.
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 identifies 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.

Required Information	Description
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.
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.

Required Information	Description
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 subsystem number of the SCCP entity with which to communicate.

## SGSN Context Configuration

The following table lists the information that is required to configure the SGSN context.

**Table 6. 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.
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.



Required Information	Description
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 in 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

The following table lists the information that is required to configure the Charging Context.

**Table 7. 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	
GTPP Group Name	If you are going to configure GTPP 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.
GTPP Server	The IP address and priority to use to contact the GTPP server.
GTPP Dictionary Name	The name of the GTPP dictionary to use.



# Chapter 3

## 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:

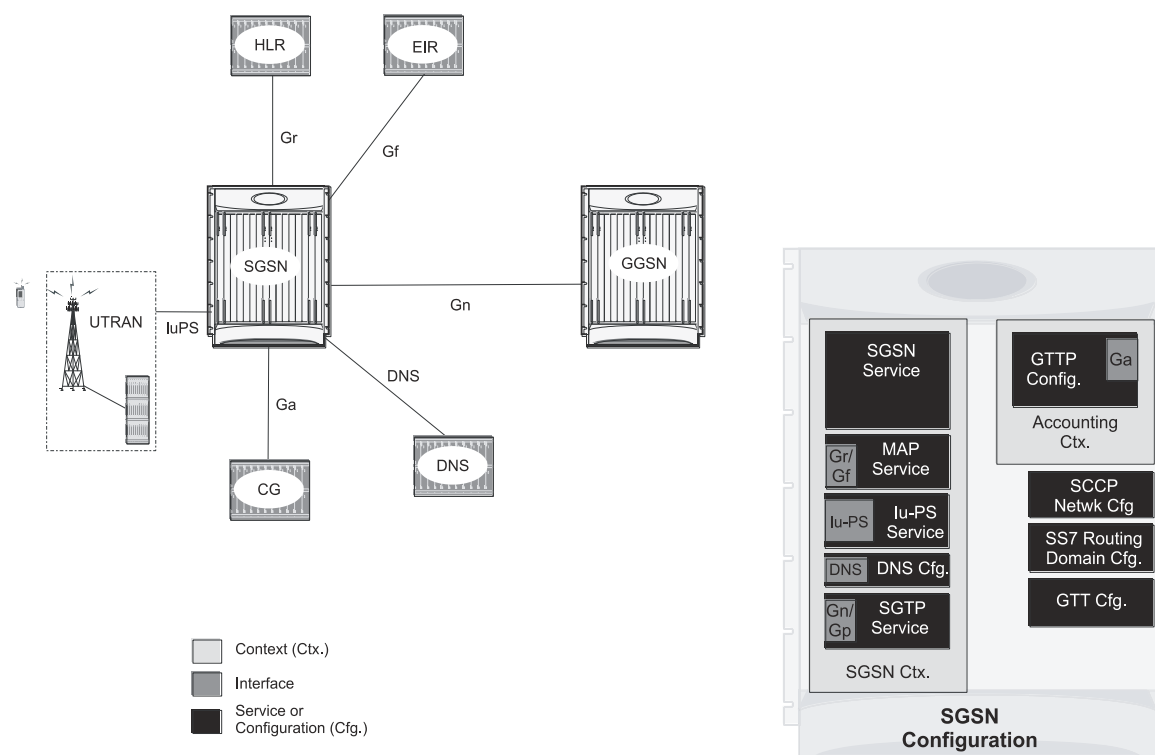
- SCCP (Signalling Connection Control Part) network configuration
- SS7 (Signaling System 7) connectivity configuration
- GTT (Global Title Translation) configuration

To simplify 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.

## 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**

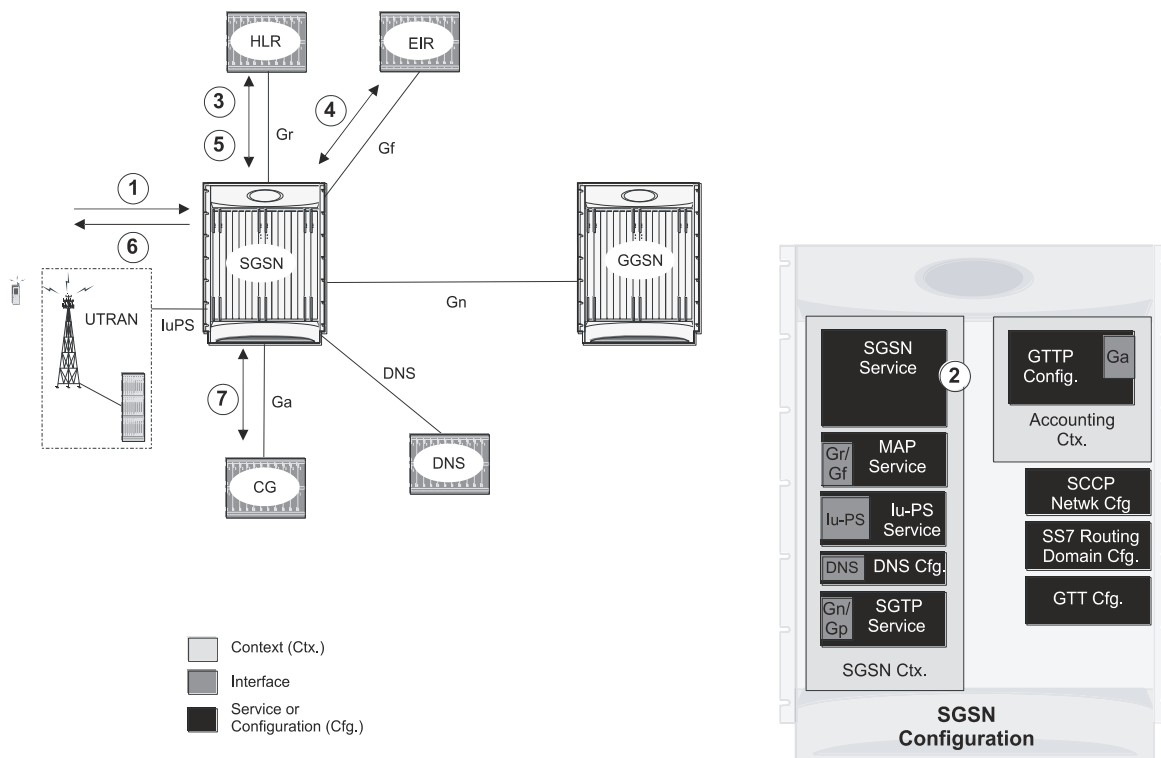


This configuration uses two contexts:

- 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 (3G)



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

The following table lists the information that is required to be configured in Global Configuration mode.

**Table 8. 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.
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

Required Information	Description
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

The following table lists the information that is required to configure the SGSN context.

**Table 9. 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.



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.
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	
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.

Required Information	Description
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

The following table lists the information that is required to configure the Accounting Context.

**Table 10. 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	
GTPP Group Name	If you are going to configure GTPP 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.

Required Information	Description
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 Service Configuration Procedures


---

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

High level step-by-step service configuration procedures are provided for the following:

- [2.5G SGSN Service Configuration](#)
- [3G SGSN Service Configuration](#)
- [Dual Access SGSN Service Configuration](#)

---

 **Important:** At least one Packet Services Card (PSC) must be activated prior to configuring the first service. PSC configuration procedures can be found in the *System Administration Guide*.

---

Detailed procedures are provided for the following:

- [Configuring an SS7 Routing Domain](#)
  - [Configuring an SS7 Routing Domain to Support Broadband SS7 Signaling](#)
  - [Configuring an SS7 Routing Domain to Support IP Signaling for SIGTRAN](#)
- [Configuring GTT](#)
- [Configuring an SCCP Network](#)
- [Configuring a MAP Service](#)
- [Configuring an IuPS Service \(3G only\)](#)
- [Configuring an SGTP Service](#)
- [Configuring a Gs Service](#)
- [Configuring a GPRS Service \(2.5G only\)](#)
- [Configuring an SGSN Service \(3G only\)](#)
- [Configuring a Network Service Entity](#)
  - [Configure a Network Service Entity for IP](#)
  - [Configure a Network Service Entity for Frame Relay](#)
- [Configuring DNS Client](#)
- [Configuring GTP Accounting Support](#)
- [Creating and Configuring ATM Interfaces and Ports \(3G only\)](#)
- [Creating and Configuring Frame Relay Ports \(2.5G only\)](#)
- [Configuring APS/MSP Redundancy](#)

## 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](#). 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](#).
- 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](#).
- 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-IW MSC. 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](#).
- 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](#).
- 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 SGSN services. Use the procedure in [Configuring an SGSN Service \(3G only\)](#).
- Step 9** Configure the GPRS service. All of the parameters needed for the system to perform as 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 \(2.5G only\)](#).
- 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](#).
- 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](#).
- Step 12** Configure GTPP Accounting. This configures GTPP-based accounting for subscriber PDP contexts. Use the procedure in [Configuring GTPP Accounting Support](#).

- 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 *SystemAdministration Guide*.
- Step 14** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

## 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](#).
- 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](#).
- 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](#).
- 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](#).
- 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 \(3G only\)](#).
- 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](#).
- 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 configurations like MAP and IuPS to communicate with other elements in the network. The system can support multiple SGSN services. Use the procedure in [Configuring an SGSN Service \(3G only\)](#).
- 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](#).
- Step 11** Configure GTP Accounting. This configures GTP-based accounting for subscriber PDP contexts. Use the procedure in [Configuring GTP Accounting Support](#).
- Step 12** 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 13** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.



# 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*.
- Step a** For IP (broadcast Ethernet) interfaces, refer to *Creating and Configuring Ethernet Interfaces and Ports* in the *System Administration Guide*.
- Step b** For ATM interfaces (3G) refer to *Creating and Configuring ATM Interfaces and Ports* in the *System Administration Guide*.
- Step 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](#).
- 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](#).
- 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](#).
- 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-IW MSC. 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](#).
- 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 \(3G only\)](#).
- 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](#).
- Step 9** Configure the GPRS service. All of the parameters needed for the system to perform as 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 \(2.5G only\)](#).
- 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](#).

- 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](#).
- Step 12** Configure GTPP Accounting. This configures GTPP-based accounting for subscriber PDP contexts. Use the procedure in [Configuring GTPP Accounting Support](#).
- 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 *SystemAdministration 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 *SystemAdministration Guide*.
- Step 15** Save your configuration as described in the Verifying and Saving Your Configuration section.

## 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
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 configurations like MAP and IuPS to communicate with other elements in the network. The system can support multiple SGSN services.

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:** GTP-U Direct Tunneling must be enabled in both the SGSN service and in the Call-Control Profile. Otherwise a direct tunnel will never be established.

- 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; *<keyword>* and *<keyword>*. Refer to the SGSN Service Configuration Mode chapter in the 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 <map_name> context <map_context>

  ran-protocol iups-service <iups_svc_name> context <iups_context>

  sgtp-service <svc_name> context <name>

    accounting cdr-types [ mcdr | scdr ]

    accounting context <acct_context>

    cc profile <profile_number> interval <seconds>

    gs-service context <ctxt> service <gs_service_name>

  end
```



## 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>
```

```
associate-service <service_type> <service_id> context <service_ctxt>
```

```
peer-nsei <peer_nsei_id> lac <lac_id> rac <rac_id>
```

```
sgsn-number <sgsn_isdn_number>
```

```
cc profile <id> buckets <value>
```

## ■ Configuring a GPRS Service (2.5G only)

```
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)#
```

## ■ Configuring a Network Service Entity

**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 DSN 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 GTPP 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 as described in the *Verifying and Saving Your Configuration* chapter.

## Creating GTPP Group

Use the following example to create the GTPP group to support GTPP accounting:

```
configure
```

```
context <vpn_ctxt_name>
```

```
gtp group <gtp_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>

  gtp group <gtp_group_name>

    gtp charging-agent address <ip_address> [ port <port> ]

    gtp server <ip_address> [ max <msgs >] [ priority <priority>]

    gtp dictionary <dictionaries>

    gtp max-cdrs <number_cdrs> [ wait-time <dur_sec> ]

    gtp 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 **gtp charging-agent** is optional and configuring gtp 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 in addition to referring Command Line Interface Reference, refer AAA Interface Administration and Reference.
- For better performance, it is recommended to configure maximum number of CDRs as 255 with **gtp max-cdrs** command.
- You can select transport layer protocol as TCP or UDP for Ga interface with **gtp 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

**Step 1** Verify that your CGFs were configured properly by entering the following command in Exec Mode:

```
show gtp 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



## 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 Procedures* 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 ASR 5000 Series 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 5

## 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 5000. 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)
- S-GW (Serving Gateway - LTE)

This document includes the following information:

- [What Operator Policy Can Do](#)
- [The Operator Policy Feature in Detail](#)
  - [Call-Control Profile](#)
  - [APN Profile](#)
  - [IMEI-Profile \(SGSN-only\)](#)
  - [APN Remap Table](#)
  - [Operator Policies](#)
  - [IMSI Ranges](#)
- [How It Works](#)
- [Operator Policy Configuration](#)
- [Operator Policy Component Associations - MME](#)
- [Verifying the Feature Configuration](#)

## 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.

## 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 (PSCs), 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 cprofile.
  - 15 - maximum number of supported equivalent PLMNs for 3G per cprofile.
- 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.
- 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 PSCs 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 PSCs, 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 (SGSN only).
- 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.

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 PSCs, 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 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 PSCs, 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.
- 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.

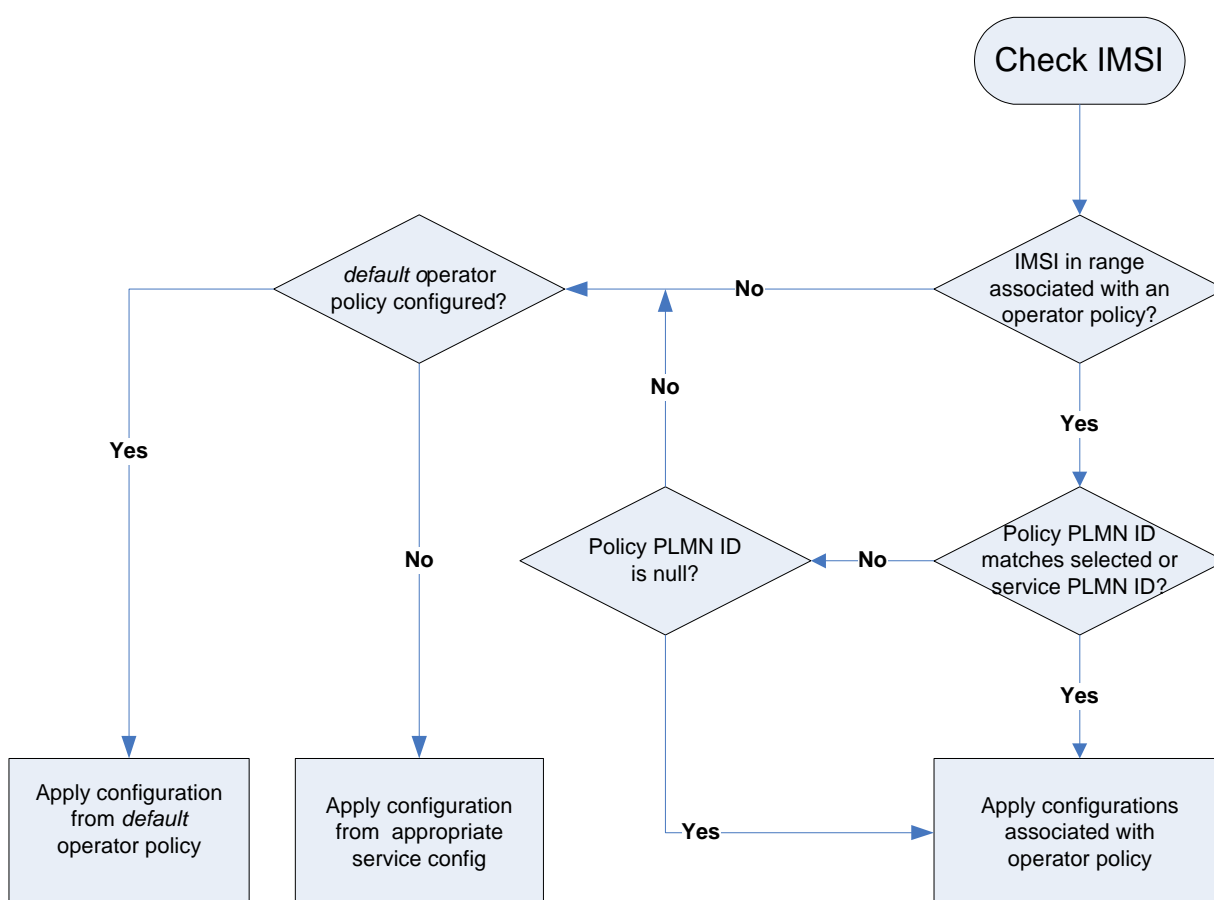
IMSI ranges are defined differently for each product supporting the operator policy feature.

## 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 17. 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.

---

 **Important:** 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.

---

- Step 3** Create and configure an IMEI profile by applying the example configuration presented in the *IMEI Profile Configuration* section.
- 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 the changes to a configuration.cfg file by applying the example configuration found in the *Saving the Configuration* section of the *Verifying and Saving Your Configuration* chapter in this book.
- Step 9** Verify the configuration for each component separately by following the instructions provided the *Verifying the Feature Configuration* section.

## 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
```

Note:

- Refer to the *Call-Control Profile Configuration Mode* chapter in the *Cisco ASR 5000 Series 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
```

Note:

- 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
```

Note:

- 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
```

Note:

- 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 (MME-only)

wildcard-apn pdp-type ipv4 network-identifier <apn_net_id>

blank-apn network-identifier <apn_net_id> (SGSN only)

end
```

Note:

- 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.

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
```

Note:

- 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>

  precedence <number> match-criteria imsi mcc <mcc_number> mnc <mnc_number>
msin first <start_range> last <end_range> operator-policy-name <policy_name>
```

```
end
```

Note:

- 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
```

Note:

- Operator policies are not valid until IMSI ranges are associated with them.

## Operator Policy Component Associations - 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.

### Associating Operator Policy Components on the MME

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.

## 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.

**Step 1** 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.

```
[local]asr5000# 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                                         : imeiprofl
```

```
Include/Exclude                                          : Include
```

```
Validity                                                : Valid
```

```
APN NI homers1
```

```
APN Profile Name                                         : apn-  
profile1
```

```
Validity                                                : Valid
```

Note:

- 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 6

## 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 the Cisco ASR 5000 Gateway GPRS Support Node (GGSN) and the Cisco ASR 5000 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:** The feature described in this chapter is an enhanced feature and implementation may require a feature license. Refer to your product's administration guide or ask your Cisco account representative for more information about feature licensing.

---

This chapter covers the following topics in support of the Subscriber Overcharging Protection feature:

- [Feature Overview](#)
- [Overcharging Protection - GGSN Configuration](#)
- [Overcharging Protection - SGSN Configuration](#)

## 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 11. 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

Condition	Triggered by	SGSN Action	LORC Intimation IE - private extension payload
PDP deactivated during LORC	GGSN	Send DPCR to GGSN Stop counting unsent packets/bytes	Unsent packet/byte counts

## 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 *Cisco ASR 5000 Series Command Line Interface Reference*.

These instructions assume that you have already configured the system-level configuration as described in *Cisco ASR 5000 Series System Administration Guide* and the *Cisco ASR 5000 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 the changes to a configuration .cfg file by applying the example configuration found in *Saving the Configuration* section of the *Verifying and Saving Your Configuration* chapter in this book.
- 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 *Cisco ASR 5000 Gateway GPRS Support Node Administration Guide*.
- *<ggsn\_svc\_name>* is 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 *Cisco ASR 5000 Series Command Line Interface Reference*.

These instructions assume that you have already completed:

- the system-level configuration as described in the *Cisco ASR 5000 Series System Administration Guide*,
- the SGSN service configuration as described in the *Cisco ASR 5000 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.



**Important:** 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 the changes to a configuration *.cfg* file by applying the example configuration found in the *Saving the Configuration* section of the *Verifying and Saving Your Configuration* chapter in this book.
- 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
```

Note:

- `<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).

## 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 7

## Direct Tunnel

---

This chapter briefly describes the 3G/4G 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)
- LTE devices (per 3GPP TS 23.401 v8.3.0):
  - Serving Gateway (S-GW)
  - PDN Gateway (P-GW)



**Important:** Direct tunnel is an enhanced feature and some products may require a feature implementation license. Refer to your product's administration guide for feature licensing information.

---

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.

This chapter provides the following information:

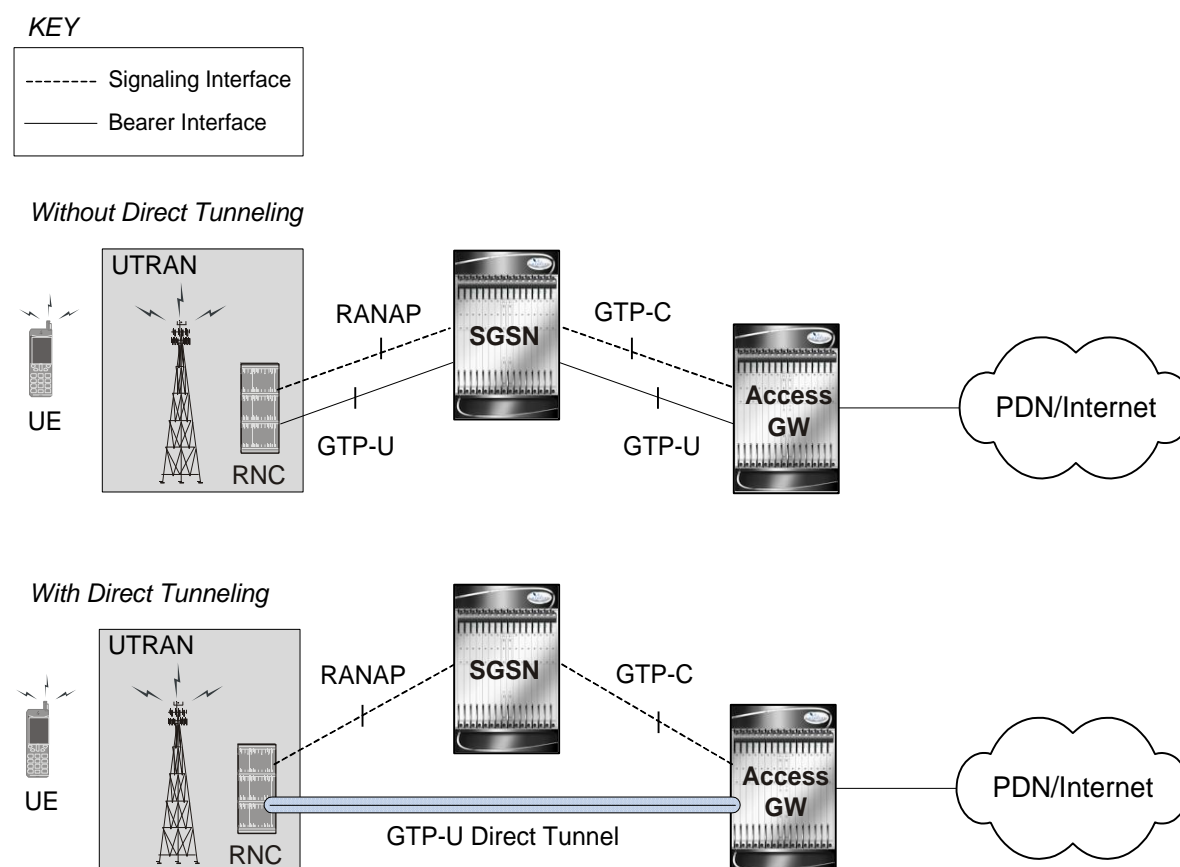
- [Direct Tunnel Feature Overview](#)
- [Direct Tunnel Configuration](#)

## 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 the GGSN/P-GW.

Once a direct tunnel is established, the 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 PDN context activation.

Figure 18. 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/S-GW to handle the user plane processing.

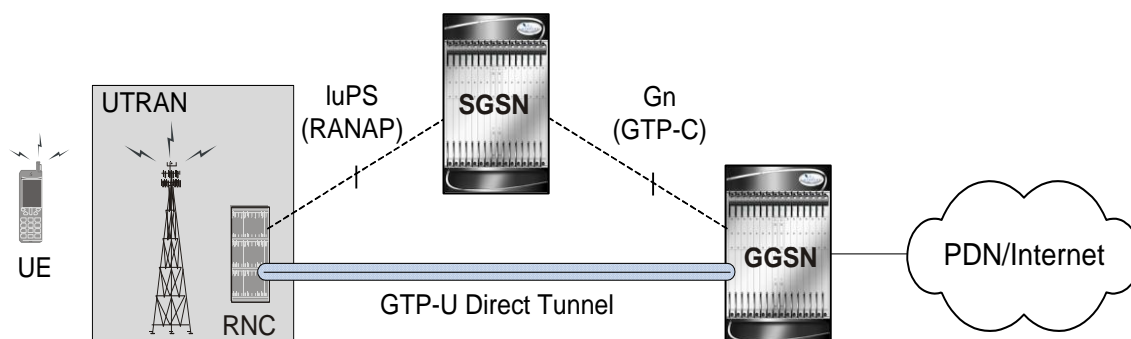
A direct tunnel is achieved upon PDN context activation in the following ways:

- **3G network:** The SGSN establishes a user plane (GTP-U) tunnel directly between the RNC and the GGSN, using an Updated PDN Context Request toward the GGSN.

- **Direct Tunneling - 3G Network**

## KEY

----- Signaling Interface  
 ——— Bearer Interface

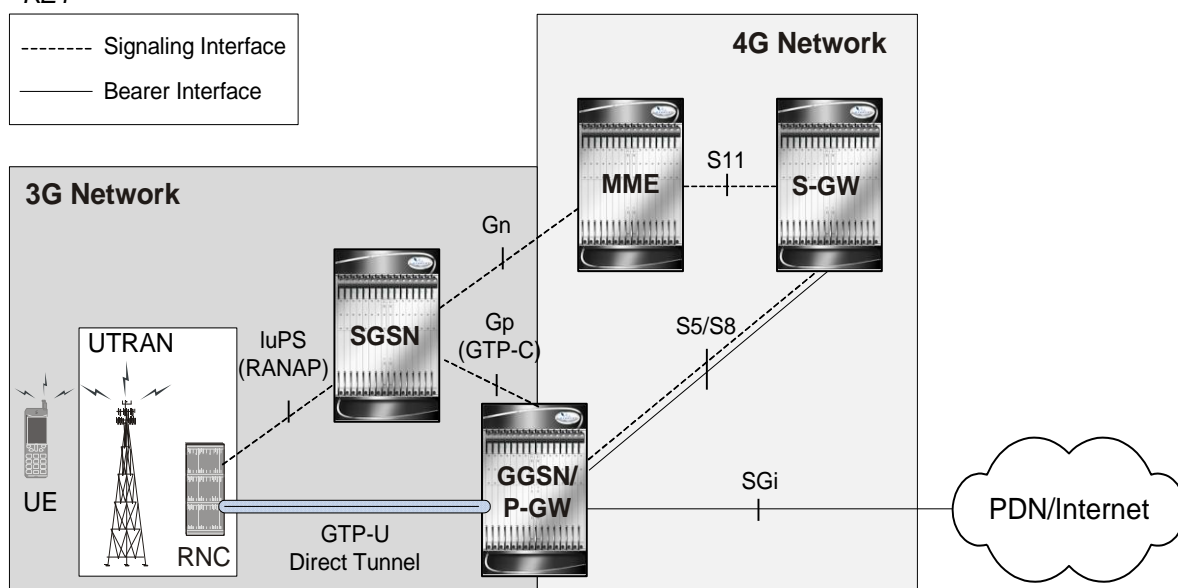


- **LTE network:** When Gn/Gp interworking with pre-release 8 (3GPP) SGSNs is enabled, the GGSN service on the P-GW supports direct tunnel functionality. The SGSN establishes a user plane (GTP-U) tunnel directly between the RNC and the GGSN/P-GW, using an Update PDN Context Request toward the GGSN/P-GW.

- **Direct Tunneling - LTE Network, GTP-U Tunnel**

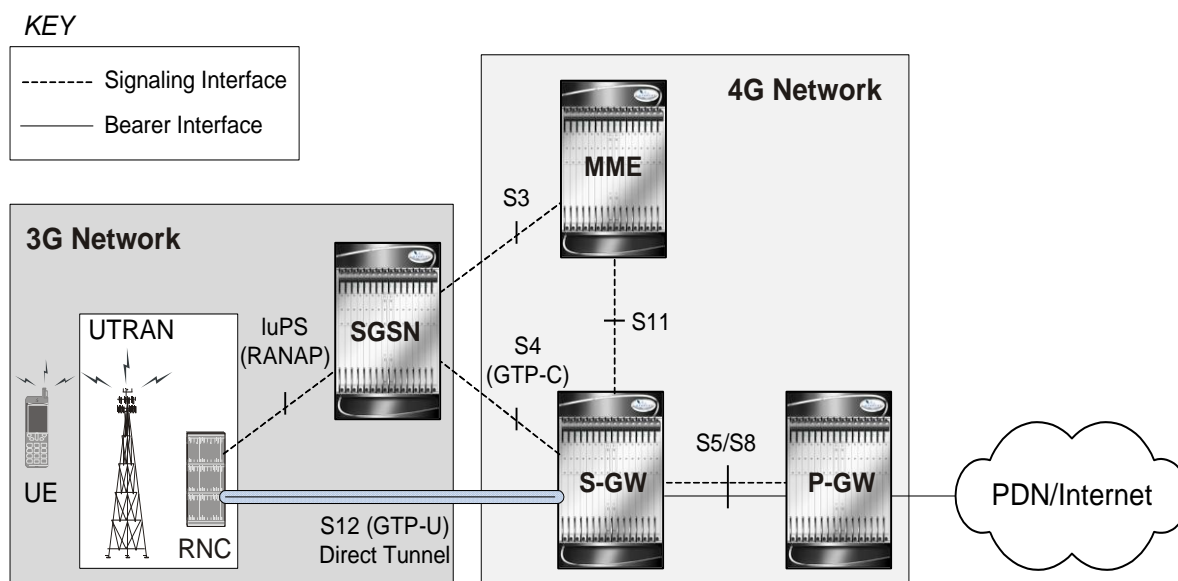
## KEY

----- Signaling Interface  
 ——— Bearer Interface



- **LTE network:** The SGSN establishes a user plane tunnel (GTP-U tunnel over an S12 interface) directly between the RNC and the S-GW, using an Update PDN Context Request toward the S-GW.

- *Direct Tunneling - LTE Network, S12 Interface*

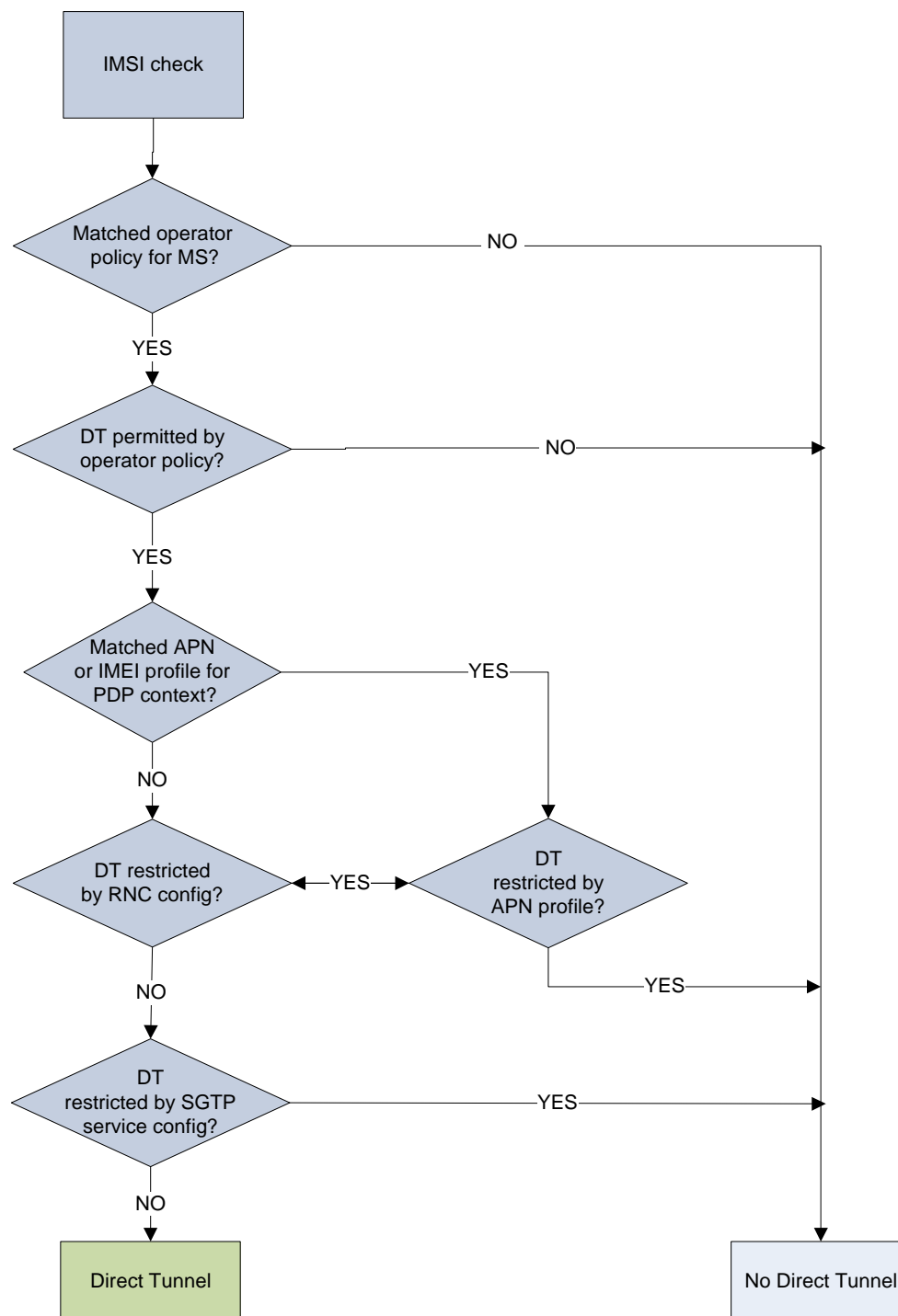


A major consequence of deploying a direct tunnel is that it produces a significant increase in control plane load on both the SGSN/S-GW and GGSN/P-GW components of the packet core. Hence, deployment requires highly scalable GGSNs/P-GWs since the volume and frequency of Update PDP Context messages to 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.

The following figure illustrates the logic used within the SGSN/S-GW to determine if a direct tunnel will be setup.



Figure 19. Direct Tunneling - Establishment Logic



# Direct Tunnel Configuration

The following configurations are provided in this section:

- [Configuring Direct Tunnel Support on the SGSN](#)
- [Configuring S12 Direct Tunnel Support on the S-GW](#)

## Configuring Direct Tunnel Support on the SGSN

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 system operator policy named *default*.

For more information about operator policies and configuration details, refer to the *Operator Policy* chapter also in this guide.



**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*.

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 5000 Series 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.

8. 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* section below.
9. 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* section below.



**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.

10. 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* section below.
11. 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* section below.

12. (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 Cisco ASR 5000 Series Command Line Interface Reference.
13. Save the changes to the system configuration by applying the sample configuration found in the *Saving the Configuration* section of the *Verifying and Saving Your Configuration* chapter in this guide.
14. Check that your configuration changes have been saved by using the sample configuration found in the *Verifying the SGSN Direct Tunnel Configuration* section in this chapter.

## 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
    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.
- Direct tunnel is now 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 *Cisco ASR 5000 Series Command Line Interface Reference*.

## 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.

```
[local]asr5000# show operator-policy full name oppolicy1
```

```

Operator Policy Name = oppolicy1

Call Control Profile Name                               : ccprofile1

Validity                                                : Valid

IMEI Range 999999999999990 to 999999999999995

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
```

## Configuring S12 Direct Tunnel Support on the S-GW

The example in this section configures an S12 interface supporting direct tunnel bypass of the release 8 SGSN for inter-RAT handovers.

The direct tunnel capability on the S-GW is enabled by configuring an S12 interface. The R8 SGSN is then responsible for creating the direct tunnel by sending an FTEID in a control message to the MME over the S3 interface. The MME forwards the FTEID to the S-GW over the S11 interfaces. The S-GW responds with its own U-FTEID providing the SGSN with the identification information required to set up the direct tunnel over the S12 interface.

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.



# Chapter 8

## Verifying and Saving Your Configuration

---

This chapter describes how to save your system configuration.

## Verifying the Configuration

You can use a number of commands to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of, or specific lines in, the configuration file.

### Feature Configuration

In many configurations, you have to set and verify specific features. An example includes IP address pool configuration. Using this example, enter the following commands to verify proper feature configuration:


Enter the following command to display the IP address pool configuration:

**show ip pool**

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```
context : isp1:
+-----Type: (P) - Public (R) - Private
|
| (S) - Static (E) - Resource
|
|+-----State: (G) - Good (D) - Pending Delete (R)-Resizing
||
||+---Priority: 0..10 (Highest (0) .. Lowest (10))
||||
||||+--Busyout: (B) - Busyout configured
|||| ||||| vvvvv Pool Name Start Address Mask/End Address Used Avail
-----
PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00
pool1 10.10.0.0 255.255.0.0 0 65534 SG00
vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5
```

---

 **Important:** To configure features on the system, use the *show* commands specifically for these features. Refer to the *Cisco Systems ASR 5000 Command Line Interface Reference* for more information.

---

## Service Configuration

Verify that your service was created and configured properly by entering the following command:

```
show <service_type> <service_name>
```

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a P-GW service called *pgw* is configured.

```
Service name : pgw1
Service-Id : 1
Context : test1
Status : STARTED
Restart Counter : 8
EGTP Service : egtpl
LMA Service : Not defined
Session-Delete-Delay Timer : Enabled
Session-Delete-Delay timeout : 10000(msecs)
PLMN ID List : MCC: 100, MNC: 99
Newcall Policy : None
```

## Context Configuration

Verify that your context was created and configured properly by entering the following command:

```
show context name <name>
```

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named *test1* is configured.

Context Name	ContextID	State
-----	-----	-----
test1	2	Active

## System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

```
show configuration
```

This command displays the entire configuration including the context and service configurations defined above.

## Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

```
show configuration errors
```

This command displays errors it finds within the configuration. For example, if you have created a service named “service1”, but entered it as “srv1” in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

```
show configuration errors section ggsn-service
```

or

```
show configuration errors section aaa-config
```

If the configuration contains no errors, an output similar to the following is displayed:

```
#####  
  
Displaying Global  
AAA-configuration errors  
#####  
  
Total 0 error(s) in this section !
```

## Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network. You can use this configuration file on any other systems that require the same configuration.

Files saved locally can be stored in the CompactFlash or a PCMCIA memory card on the SMC. Files that are saved to a remote network node can be transmitted through FTP or TFTP.

# Saving the Configuration on the Chassis

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

To save your current configuration, enter the following command:

```
save configuration url [-redundant] [-noconfirm] [showsecrets] [verbose]
```

Table 12. Command Syntax for Saving the Configuration

Keyword/Variable	Description
<i>url</i>	<p>Specifies the path and name to which the configuration file is to be stored. <i>url</i> may refer to a local or a remote file. <i>url</i> must be entered using one of the following formats:</p> <ul style="list-style-type: none"> <li><code>{ /flash   /pcmcia1   /pcmcia2 } [ /dir ] /file_name</code></li> <li><code>file://{ /flash   /pcmcia1   /pcmcia2 } [ /dir ] /file_name</code></li> <li><code>tftp://{ ipaddress   host_name [ :port# ] } [ /directory ] /file_name</code></li> <li><code>ftp://{ username [ :pwd ] @ } { ipaddress   host_name } [ :port# ] [ /directory ] /file_name</code></li> <li><code>sftp://{ username [ :pwd ] @ } { ipaddress   host_name } [ :port# ] [ /directory ] /file_name</code></li> </ul> <p><code>/flash</code> corresponds to the CompactFlash on the SMC.  <code>/pcmcia1</code> corresponds to PCMCIA slot 1.  <code>/pcmcia2</code> corresponds to PCMCIA slot 2.  <i>ipaddress</i> is the IP address of the network server.  <i>host_name</i> is the network server's <i>hostname</i>.  <i>port#</i> is the network server's logical port number. Defaults are:</p> <ul style="list-style-type: none"> <li>tftp: 69 - data</li> <li>ftp: 20 - data, 21 - control</li> <li>sftp: 115 - data</li> </ul> <p>Note: <i>host_name</i> can only be used if the <b>networkconfig</b> parameter is configured for DHCP and the DHCP server returns a valid nameserv er.dx  <i>username</i> is the username required to gain access to the server if necessary.  <i>password</i> is the password for the specified username if required.  <i>/directory</i> specifies the directory where the file is located if one exists.  <i>/file_name</i> specifies the name of the configuration file to be saved.  Note: Configuration files should be named with a .cfg extension.</p>
-redundant	<p>Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the <i>url</i> variable, and then automatically copy that same file to the like device on the Standby SMC, if available.  Note: This keyword will only work for like local devices that are located on both the active and standby SMCs. For example, if you save the file to the /pcmcia1 device on the active SMC, that same type of device (a PC-Card in Slot 1 of the standby SMC) must be available. Otherwise, a failure message is displayed.  Note: When saving the file to an external network (non-local) device, the system disregards this keyword.</p>



Keyword/Variable	Description
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).
showsecrets	Optional: This keyword saves the CLI configuration file with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies to display every parameter that is being saved to the new configuration file.



**Important:** The **-redundant** keyword is only applicable when saving a configuration file to local devices. This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SMC, you must synchronize the local file system on both SMCs.

To save a configuration file called *system.cfg* to a directory that was previously created called *cfgfiles* on the CompactFlash in the SMC, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called *simple\_ip.cfg* to a directory called *host\_name\_configs*, using an FTP server with an IP address of *192.168.34.156*, on which you have an account with a username of *administrator* and a password of *secure*, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called *init\_config.cfg* to the root directory of a TFTP server with a hostname of *config\_server*, enter the following command:

```
save configuration tftp://config_server/init_config.cfg
```



# Chapter 9

## Monitoring and Troubleshooting

---

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 13. 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.	<code>show snmp trap history</code>
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.	<code>show power chassis</code>
Check the power status of an individual chassis.	<code>show power all</code>
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.	<code>show fans</code>
View the LED status for all installed cards. All LEDs for active cards should be green.	<code>show leds all</code>
Checking the temperatures confirms that all cards and fan trays are operating within safe ranges to ensure hardware efficiency.	<code>show temperature</code>

**Table 14. Physical Layer Status Check**

To Do This:	Enter This Command:
View mapping of the line cards-to-controlling application cards.	<code>show card mappings</code>
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.	<code>show card table</code> <code>show card table all</code>
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.	<code>show linecard table</code>
View the number and status of physical ports on each line card. Output indicates Link and Operation state for all interfaces -- UP or down.	<code>show port table all</code>
Verify CPU usage and memory.	<code>show cpu table</code> <code>show cpu information</code>

**Health Check - System & Performance**

Most of these commands are useful for both maintenance and diagnostics, and if the system supports a “combo” (a co-located SGSN and GGSN), then these commands can be used for either service.

**Table 15. System & Performance Checks**

To Do This:	Enter This Command:
Check a summary of CPU state and load, memory and CPU usage.	<code>show cpu table</code>
Check availability of resources for sessions.	<code>show resources session</code>
Review session statistics, such as connects, rejects, hand-offs, collected in 15-minute intervals.	<code>show session counters historical</code>
View duration, statistics, and state for active call sessions.	<code>show session duration</code> <code>show session progress</code>
Display statistics for the Session Manager.	<code>show session subsystem facility sessmgr all</code>
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.	<code>show system uptime</code>
Verify the status of the configured NTP servers. Node time should match the correct peer time with minimum jitter.	<code>show ntp status</code>
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.	<code>show clock universal</code>
View both active and inactive system event logs.	<code>show logs</code>

To Do This:	Enter This Command:
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.	<b>show snmp trap history</b>
Check the crash log. Use this command to determine if any software tasks have restarted on the system.	<b>show crash list</b>
Check current alarms to verify system status.	<b>show alarm outstanding all</b> <b>show alarm all</b>
View system alarm statistics to gain an overall picture of the system's alarm history.	<b>show alarm statistics</b>

Daily - Health Check- SGSN-Specific Status and Performance

These commands are useful for both maintenance and diagnostics.

**Table 16. 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.	<b>show iups-service all</b>
Check the configuration for the MAP services features and some of the HLR and EIR configuration. In the display, ensure the "state" is "STARTED" for the Gr interface.	<b>show map-service all</b>
Check the configuration for the SGSN services in the current context. In the display, ensure the "state" is "STARTED" for the SGSN.	<b>show sgsn-service all</b>
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.	<b>show sccp-network all status all</b>
Check the configuration and IDs for SS7 routing domains	<b>show ss7-routing-domain all</b>
Check the connection status on SS7 routes.	<b>show ss7-routing-domain &lt;#&gt; routes</b>
Snapshot subscriber activity and summary of PDP context statistics.	<b>show subscribers sgsn-only</b>
Check the configured services and features for a specific subscriber.	<b>show subscribers sgsn-only full msid</b> <b>&lt;msid_number&gt;</b>

## Monthly System Maintenance

Depending upon system usage and performance, you may want to perform these tasks more often than once-per-month.

**Table 17. Irregular System Maintenance**

To Do This:	Enter This Command:
Check for unused or unneeded file on the CompactFlash.	<b>dir /flash</b>
Delete unused or unneeded files to conserve space using the delete command. Recommend you perform next action in list	<b>delete /flash/&lt;filename&gt;</b>
Synchronise the contents of the CompactFlash on both SMCs to ensure consistency between the two.	<b>card smc synchronize filesystem</b>
Generate crash list (and other "show" command information) and save the output as a tar file.	show support details <to location and filename> <ul style="list-style-type: none"> <li>• [file: ] { /flash   /pcmcia1   /hd } [ /directory ] /file_name</li> <li>• tftp://{ host[ :port# ] } [ /directory ] /file_name</li> <li>• [ ftp:   sftp: ]/[ username[ :password ]@ ] { host } [ :port# ] [ /directory ] /file_name</li> </ul>

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 18. 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.	<b>show hardware card</b> <b>show hardware inventory</b> <b>show hardware system</b>
View all cards installed in the chassis with hardware revision, and the firmware version of the on-board Field Programmable Gate Array (FPGAs).	<b>show hardware version board</b>

# 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 19. 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.
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:

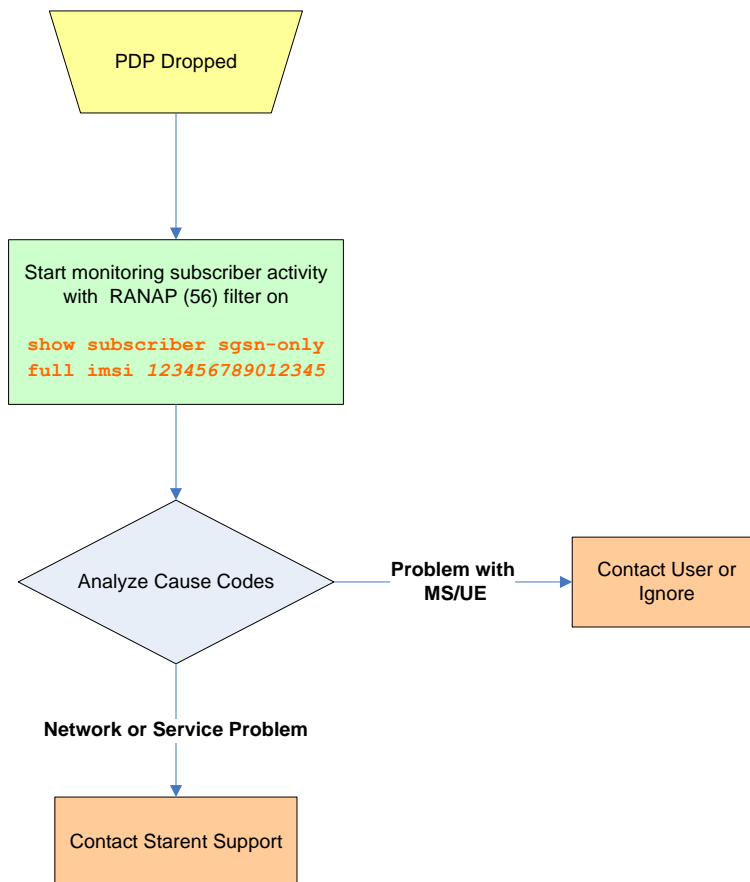
```
monitor subscriber IMSI
```



## 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:

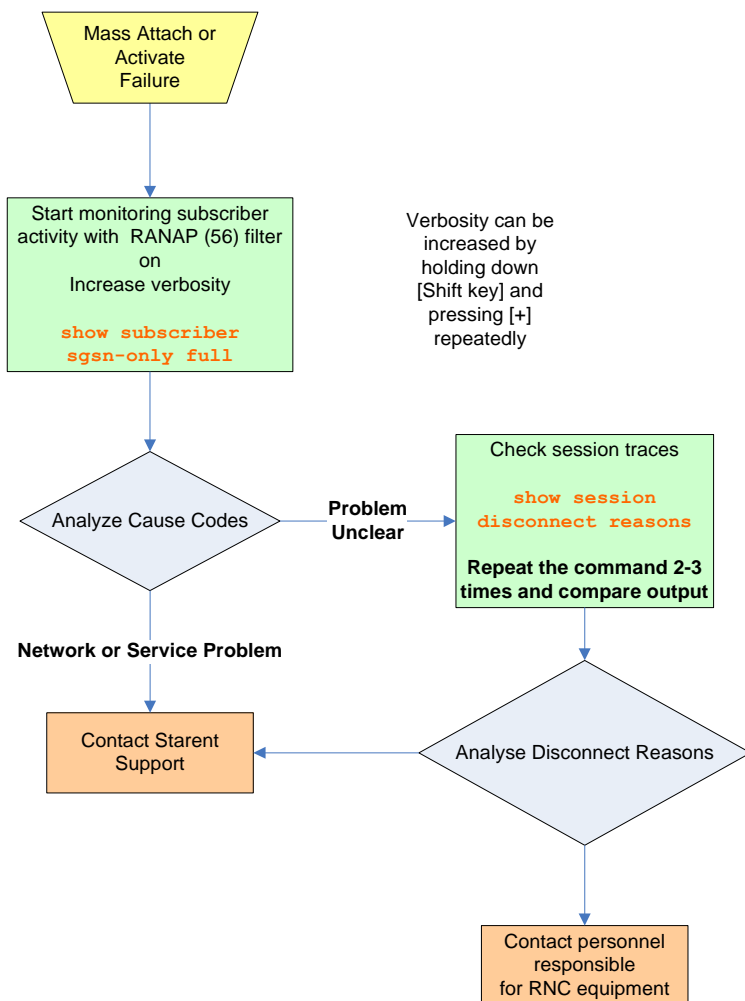
**Figure 20. Troubleshooting Single Attach/Activate Failures**



## Mass Attach and Activate Problems

The following flow chart is intended to help you diagnose the problem and determine an appropriate response:

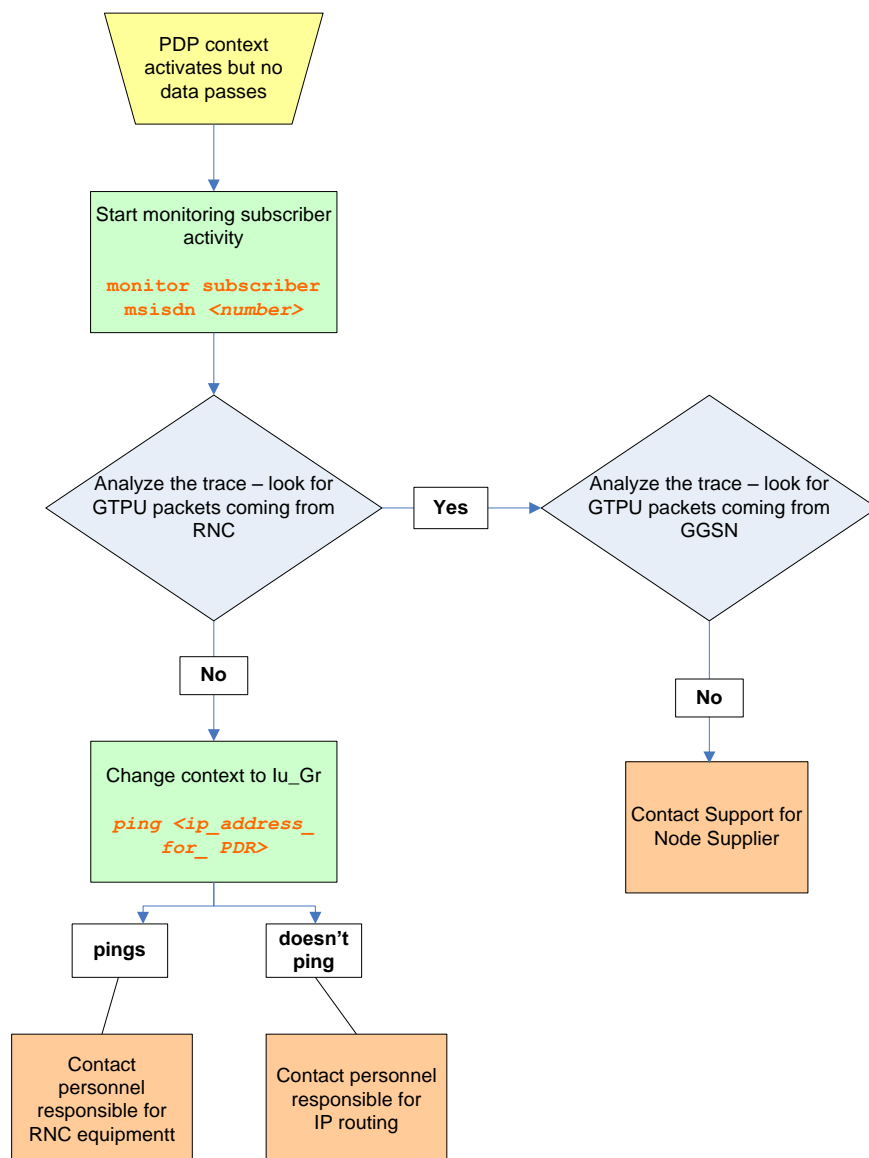
**Figure 21. Troubleshooting Multiple Attach/Activate Failures**



## 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.

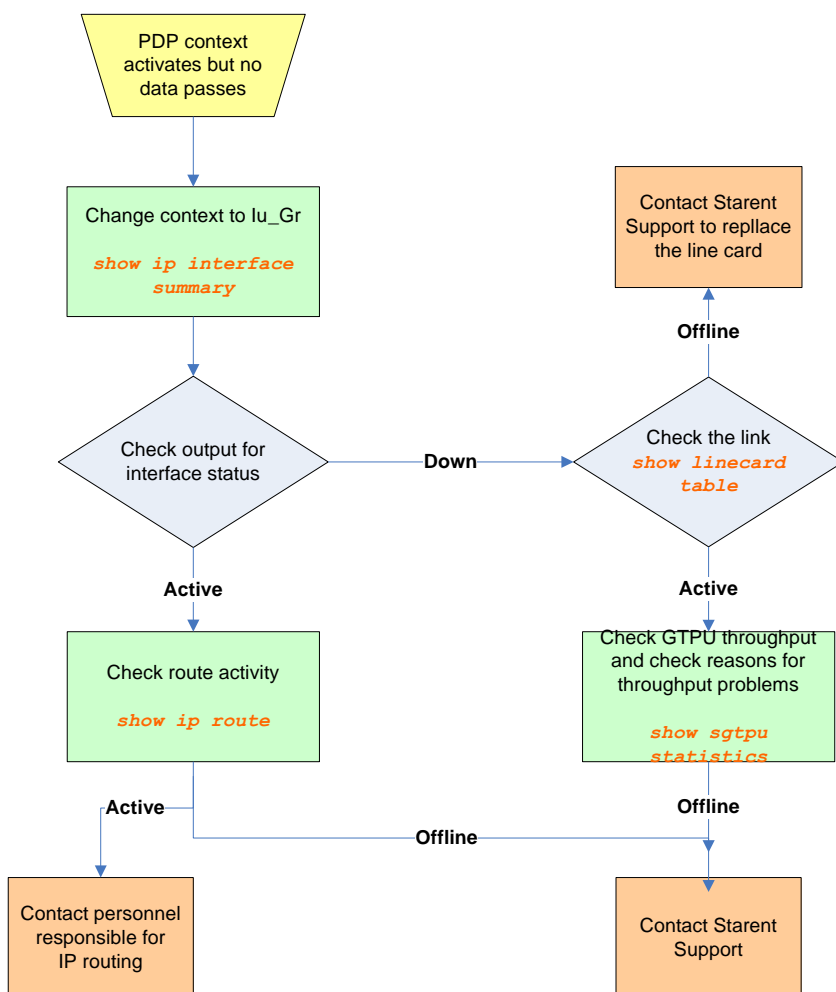
**Figure 22. Troubleshooting Missing Data for Single PDP Context Activation**



## 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 23. Troubleshooting Missing Data for Multiple PDP Context Activation**



# Appendix A

## Engineering Rules

---

This section provides SGSN-specific 2.5G, 3G , and 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):

**Table 20. 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 SGTP services, IuPS Services, and MAP Services.
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 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.
Max. number of Gs services supported by a single GPRS or SGSN service.	12	
Max. number of SCCP network configurations supported by a single MAP service.	1	
Max. number of Gs services supported on an SGSN (system)	12	
Maximum number of LACs per Gs service	128	

## SGSN Connection Rules

The following limitations apply to both 2G and 3G SGSNs.

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/Quintuplets
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 buffer pool of 10M per session manager - buffers to be shared by all subscribers “belonging” to that session manager.)

## 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 an ASR 5000 running a standalone SGSN application on a PSC2/PSC3. Limits may be lower when using a PSC1 or in combo nodes, such as SGSN+GGSN.

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	100	
Maximum number of IMSI ranges under SGSN mode	1000	
Maximum number of IMEI ranges per operator policy	10	
Maximum number of APN profile associations per operator policy	50	
Maximum number of call-control profiles per operator policy	1	
Maximum number of APN remap tables per operator policy	1	
<b>Call-Control Profiles</b>		
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	
Maximum number of LACs per location area code list	100	
Maximum number of allowed zone code lists	10	For Release 12.0
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	



Features	Limits	Comments
<b>APN Profiles</b>		
Maximum number of APN profiles	1000	
Maximum number of gateway addresses per APN profile	16	

## SS7 Rules

### SS7 Routing

*Table 21. 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, 1 per link-set and 1 per peer-server
Maximum number of routes possible via a link-set	2048	This includes the self point code of the peer, 1 per link-set and 1 per peer-server
Maximum number of routes possible via peer-server	2048	This includes the self point code of the peer, 1 per link-set and 1 per peer-server
Maximum number of different levels of priority for link sets used in a single route set	16	

## SIGTRAN

*Table 22. SIGTRAN Rules for SGSN*

Features	Limits	Comments
Maximum number of peer servers	144	
Maximum number of peer servers per SS7RD	144	
Maximum number of PSPs per peer server	4	
Maximum number of ASPs per SS7RD	4	
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 23. Broadband SS7 Rules for SGSN

Features	Limits	Comments
Maximum number of MTP3 linksets	256	
Maximum number of MTP3 linksets per SS7RD	144	
Maximum number of MTP3 links per linkset	16	
Maximum number of MTP3 links per combined linkset	16	

## SCCP

Table 24. 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 25. GTT Rules for SGSN

Features	Limits	Comments
Maximum number of associated GTTs	16	
Maximum number of actions per association	8	For Release 12.0
Maximum number of address maps	4096	
Maximum number of out-addresses per address map	5	

## SGSN Interface Rules

The following information relates to the virtual interfaces supported by the SGSN:

### System-Level

*Table 26. 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 27. 3G Interface Rules for SGSN*

Features	Limits	Comments
Maximum number of RNCs	See comment	Supports upto 144 directly connected RNC and 1024 indirectly connected through gateways.
Maximum number of RNCs controlling the same RA	no limit	
Maximum number of RAIs per RNC	2500	
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
Maximum number of GTPU addresses per SGTP service	12	

## 2G Interface Limits

**Table 28. 2G Interface Rules - Gb over Frame Relay**

Features	Limits	Comments
Maximum number of NSEs	2048	
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
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	
Maximum number of cell sites supported	64,000	

**Table 29. 2G Interface Rules - Gb over IP**

Features	Limits	Comments
Maximum number of NSEs	2048	
Maximum number of Local NSVLs per SGSN	4	
Maximum number of Peer NSVLs per NSE	128	
Maximum number of RAI per NSE	2500	
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

