Cisco ASR 5000 Series Gateway GPRS Support Node Administration Guide

Version 10.0

Last updated June 30, 2010

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-22944-01

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. 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 Gateway GPRS Support Node Administration Guide

© 2010 Cisco Systems, Inc. and/or its affiliated entities. All rights reserved.

CONTENTS

About this Guide vii
Conventions Used viii
Contacting Customer Support x
GGSN Support in GPRS/UMTS Wireless Data Services 11
Product Description 12
Product Specification 13
Licenses 13
Hardware Requirements 13
ASR 5000 Platform System Hardware Components 13
Operating System Requirements 14
Network Deployment and Interfaces 15
GGSN in the GPRS/UMTS Data Network 15
Supported Interfaces 16
Features and Functionality - Base Software 19
16,000 SGSN Support 20
AAA Server Groups 20
Access Control List Support 20
ANSI T1.276 Compliance 21
APN Support 21
Bulk Statistics Support 22
Direct Tunnel Support 23
DHCP Support 24
DSCP Marking 25
Generic Corporate APN 25
GTPP Support 25
Host Route Advertisement 26
IP Policy Forwarding 27
IP Header Compression - Van Jacobson 27
IPv6 Support 28
Management System Overview 29
Overlapping IP Address Pool Support 31
PDP Context Support 31
Per APN Configuration to Swap out Gn to Gi APN in CDRs 32
Port Insensitive Rule for Enhanced Charging Service 32
Quality of Service Support 33
RADIUS Support 33
RADIUS VLAN Support 34
Routing Protocol Support 35
Support of Charging Characteristics Provided by AAA Server 36
Support of all GGSN generated causes for partial G-CDR closure 36
Threshold Crossing Alerts (TCA) Support 37
Features and Functionality - Optional Enhanced Feature Software 38
Common Gateway Access Support 38
Converged DSL Support on the GGSN 39
Dynamic RADIUS Extensions (Change of Authorization) 39
GRE Protocol Interface Support 40

Gx Interface Support 41
Inter-Chassis Session Recovery 42
IP Security (IPSec) 44
IPv6 Support 45
L2TP LAC Support 46
L2TP LNS Support 47
Lawful Intercept 47
Mobile IP Home and Foreign Agents 48
Mobile IP NAT Traversal 49
Multimedia Broadcast Multicast Services Support 50
Overcharging Protection on Loss of Coverage 50
Proxy Mobile IP 50
Session Persistence 51
Session Recovery Support 52
Traffic Policing and Rate Limiting 52
Web Element Management System 54
How GGSN Works 56
PDP Context Processing 56
Dynamic IP Address Assignment 57
Subscriber Session Call Flows 58
Transparent Session IP Call Flow 59
Non-Transparent IP Session Call Flow 60
Network-Initiated Session Call Flow 63
PPP Direct Access Call Flow 64
Virtual Dialup Access Call Flow 66
Corporate IP VPN Connectivity Call Flow 68
Mobile IP Call Flow 70
Proxy Mobile IP Call Flows 73
IPv6 Stateless Address Autoconfiguration Flows 76
Supported Standards 78
3GPP References 78
IETF References 79
Object Management Group (OMG) Standards 82

Understanding the Service Operation 83

Terminology 84
Contexts 84
Logical Interfaces 85
Bindings 86
Services 87
How the System Selects Contexts 89
Context Selection for Subscriber Sessions 89

GGSN Configuration Example 91

Information Required 93
Source Context Configuration 93
Destination Context Configuration 96
How This Configuration Works 101
Transparent IP PDP Context Processing 101
Non-transparent IP PDP Context Processing 103
PPP PDP Context Processing 104
Network-requested PDP Context Processing 106

Mobile IP Configuration Examples 109

Example 1: Mobile IP Support Using the System as a GGSN/FA 110
Information Required 111
Source Context Configuration 111

AAA Context Configuration 114
Mobile IP Destination Context Configuration 116
Optional Destination Context Configuration 118
How This Configuration Works 119
Example 2: Mobile IP Support Using the System as an HA 122
Information Required 123
Source Context Configuration 123
Destination Context Configuration 126
How This Configuration Works 127
Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts 130
Information Required 132
Source Context Configuration 132
Destination Context Configuration 135
System-Level AAA Configuration 137
How This Configuration Works 138
GGSN and Mobile IP Service in a Single System Configuration Example 141
Using the System as Both a GGSN/FA and an HA 142
Information Required 143
Source Context Configuration 143
Destination Context Configuration 146
Mobile IP Destination Context Configuration 150
How This Configuration Works 154
GGSN Service Configuration Procedures 157
GGSN Service Configuration 158
GGSN Service Creation and Binding 158
Accounting Context and Charging Characteristics Configuration 159
SGSN and PLMN Policy Configuration 159
Network-requested PDP Context Support Configuration 160
GGSN Configuration Verification 160
GTPP Accounting Support Configuration 163
GTPP Group Creation 164
GTPP Group Configuration 164
GTPP Group Configuration Verification 165
APN Configuration 166
APN Creation and Configuration 166
Authentication, Accounting, and GTPP Group Configuration in APN 167
Authentication and Accounting Configuration in APN 167
GTPP Group Association to APN 168
IP Address Allocation Method Configuration in APN 168
Charging Characteristics Parameter Configuration in APN 169
Virtual APN Configuration 169
Other Optional Parameter Configuration in APN 170
APN Configuration Verification 171
DHCP Service Configuration 173
DHCP Service Creation 173
DHCP Server Parameter Configuration 174
DHCP Service Configuration Verification 175
IP Address Pool Configuration on the System 177
IPv4 Pool Creation 177
IPv6 Pool Creation 178
IP Pool Configuration Verification 178
FA Services Configuration 180
FA Service Creation 180
IP Interface and UDP Port Binding for Pi Interface 181
Security Parameter Index (SPI) Configuration 181

FA Agent Advertisement Parameter Configuration 182
Subscriber Registration, Authentication and Timeout Parameter Configuration 183
Revocation Message Configuration 184
FA Service Configuration Verification 184
Common Gateway Access Support Configuration 186
Diameter Endpoint Configuration 186
AAA Group Configuration 187
Authorization over S6b Configuration 187
DNS Client Configuration 188
Duplicate Call Accept Configuration 188
Common Gateway Acces Support Configuration Verification 189
Verifying and Saving Your Configuration 191
Verifying the Configuration 192
Feature Configuration 192
Service Configuration 193
Context Configuration 194
System Configuration 194
Finding Configuration Errors 194
Saving the Configuration 196
Saving the Configuration on the Chassis 197
Monitoring the Service 199
Monitoring System Status and Performance 200
Clearing Statistics and Counters 204
Troubleshooting the Service 205
Test Commands 206
Using the PPP Echo-Test Command 206
Using the GTPC Test Echo Command 207
Using the GTPU Test Echo Command 207
Using the GTPv0 Test Echo Command 208
Using the DHCP Test Command 209
Testing GTPP Accounting with a CGF 209
Testing GTPP Connectivity with a GSS 210
Engineering Rules 211
APN Engineering Rules 212
DHCP Service Engineering Rules 213
GGSN Engineering Rules 214
GRE Tunnel Interface and VRF Engineering Rules 215
GTP Engineering Rules 216
Interface and Port Engineering Rules 217
Pi Interface Rules 217
FA to HA Rules 217
HA to FA 217
GRE Tunnel Interface Rule 218
Lawful Intercept Engineering Rules 219
MBMS Bearer Service Engineering Rules 220
Service Engineering Rules 221
Subscriber Engineering Rules 222
Mobile-IP and Proxy-MIP Timer Considerations 223
Call Flow Summary 224
Timer Values and Recommendations 226
Controlling the Mobile IP Lifetime on a Per-Domain Basis 227

About this Guide

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

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required 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
[**keyword** or *variable*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
|	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). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

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
GGSN Support in GPRS/UMTS Wireless Data Services

The Cisco® ASR 5000 chassis provides wireless carriers with a flexible solution that functions as a Gateway GPRS Support Node (GGSN) in General Packet Radio Service (GPRS) or Universal Mobile Telecommunications System (UMTS) wireless data networks.

This overview provides general information about the GGSN including:

- Product Description
- Product Specification
- Network Deployment and Interfaces
- Features and Functionality - Base Software
- Features and Functionality - Optional Enhanced Feature Software
- How GGSN Works
- Supported Standards

Product Description

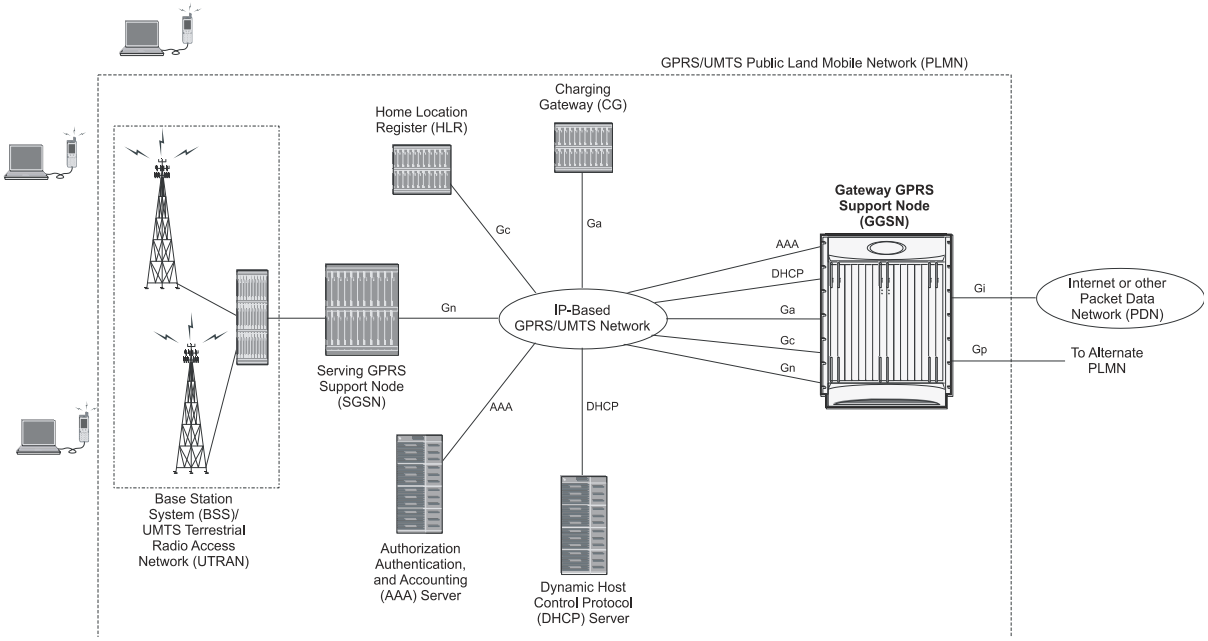
The GGSN works in conjunction with Serving GPRS Support Nodes (SGSNs) within the network to perform the following functions:

- Establish and maintain subscriber Internet Protocol (IP) or Point-to-Point Protocol (PPP) type Packet Data Protocol (PDP) contexts originated by either the mobile or the network
- Provide charging detail records (CDRs) to the charging gateway (CG, also known as the Charging Gateway Function (CGF))
- Route data traffic between the subscriber's Mobile Station (MS) and a Packet Data Networks (PDNs) such as the Internet or an intranet

PDNs are associated with Access Point Names (APNs) configured on the system. Each APN consists of a set of parameters that dictate how subscriber authentication and IP address assignment is to be handled for that APN.

In addition, to providing basic GGSN functionality as described above, the system can be configured to support Mobile IP and/or Proxy Mobile IP data applications in order to provide mobility for subscriber IP PDP contexts. When supporting these services, the system can be configured to either function as a GGSN and Foreign Agent (FA), a stand-alone Home Agent (HA), or a GGSN, FA, and HA simultaneously within the carrier's network.

Figure 1. Basic GPRS/UMTS Network Topology



In accordance with RFC 2002, the FA is responsible for mobile node registration with, and the tunneling of data traffic to/from the subscriber's home network. The HA is also responsible for tunneling traffic, but also maintains subscriber location information in Mobility Binding Records (MBRs).

Product Specification

This section describes the hardware and software requirement for GGSN service.

The following information is located in this section:

- Licenses
- Hardware Requirements
- Operating System Requirements

Licenses

The GGSN is a licensed product. A session use license key must be acquired and installed to use the GGSN service.

The following licenses are available for this product:

- GGSN Software License, 10K Sessions 600-00-7544
- GGSN Software License, 1K Sessions 600-00-7545

Apart from base software license, GGSN requires feature licenses for various enhanced features supported on ASR 5000 platform in GGSN service. The following table lists the supported licensed feature and required license part number for enhanced licensed features supported with this product:

IMPORTANT: For more information on requirement of licenses for optional enhanced features, refer to Features and Functionality - Optional Enhanced Feature Software section.

Hardware Requirements

Information in this section describes the hardware required to enable the GGSN service.

ASR 5000 Platform System Hardware Components

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

- **System Management Cards (SMCs):** Provides full system control and management of all cards within the ASR 5000 platform. Up to two SMC can be installed; one active, one redundant.
- **Packet Processing Cards (PSCs/PSC2s/PPCs):**In the ASR 5000 platform, packet processing cards provide high-speed, multi-threaded PDP context processing capabilities for GGSN services. Up to 14 packet processing cards can be installed, allowing for multiple active and/or redundant cards.

- **Switch Processor Input/Outputs (SPIO):** Installed in the upper-rear chassis slots directly behind the SMCs, SPIOs provide connectivity for local and remote management, central office (CO) alarms. Up to two SPIOs can be installed; one active, one redundant.
- **Line Cards**: The following rear-loaded line cards are currently supported by the system:
  - **Ethernet 10/100 and/or Ethernet 1000 Line Cards**: Installed directly behind packet processing cards, these cards provide the physical interfaces to elements in the LTE/SAE network. Up to 26 line cards should be installed for a fully loaded system with 13 active packet processing cards, 13 in the upper-rear slots and 13 in the lower-rear slots for redundancy. Redundant packet processing cards do not require line cards.
  - **Quad Gig-E Line Cards (QGLCs)**: The 4-port Gigabit Ethernet line card is used in the ASR 5000 system only and is commonly referred to as the Quad-GigE Line Card or the QGLC. The QGLC is installed directly behind its associated packet processing card to provide network connectivity to the packet data network.
  - **10 Gig-E Line Cards (XGLCs)**: The 10 Gigabit Ethernet Line Card is used in the ASR 5000 system only and is commonly referred to as the XGLC. The XGLC supports higher speed connections to packet core equipment, increases effective throughput between the ASR 5000 and the packet core network, and reduces the number of physical ports needed on the ASR 5000.

    The one-port XGLC supports the IEEE 802.3-2005 revision which defines full duplex operation of 10 Gigabit Ethernet.

    The XGLC is configured and monitored via the System Management Card (SMC) over the system's control bus. Both SMCs must be active to maintain maximum forwarding rates.
- **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 packet processing card in the system for redundancy. Two RCCs can be installed to provide redundancy for all line cards and packet processing cards.

IMPORTANT: Additional information pertaining to each of the application and line cards required to support GPRS/UMTS wireless data services is located in the *Hardware Platform Overview* chapter of the *Product Overview Guide*.

Operating System Requirements

The GGSN is available for ASR 5000 chassis running StarOS™ Release 7.1 or later.

Network Deployment and Interfaces

This section describes the supported interfaces and deployment scenario of GGSN in GPRS/UMPS network.

The following information is provided in this section:

- GGSN in the GPRSUMTS Data Network
- Supported Interfaces

GGSN in the GPRS/UMTS Data Network

The figures that follow display simplified network views of the GGSN in a GPRS/UMTS network and the system supporting Mobile IP and Proxy Mobile IP function both the GGSN/Foreign Agent (FA) and GGSN/FA/Home Agent (HA) combinations respectively.

Figure 2. Basic GPRS/UMTS Network Topology

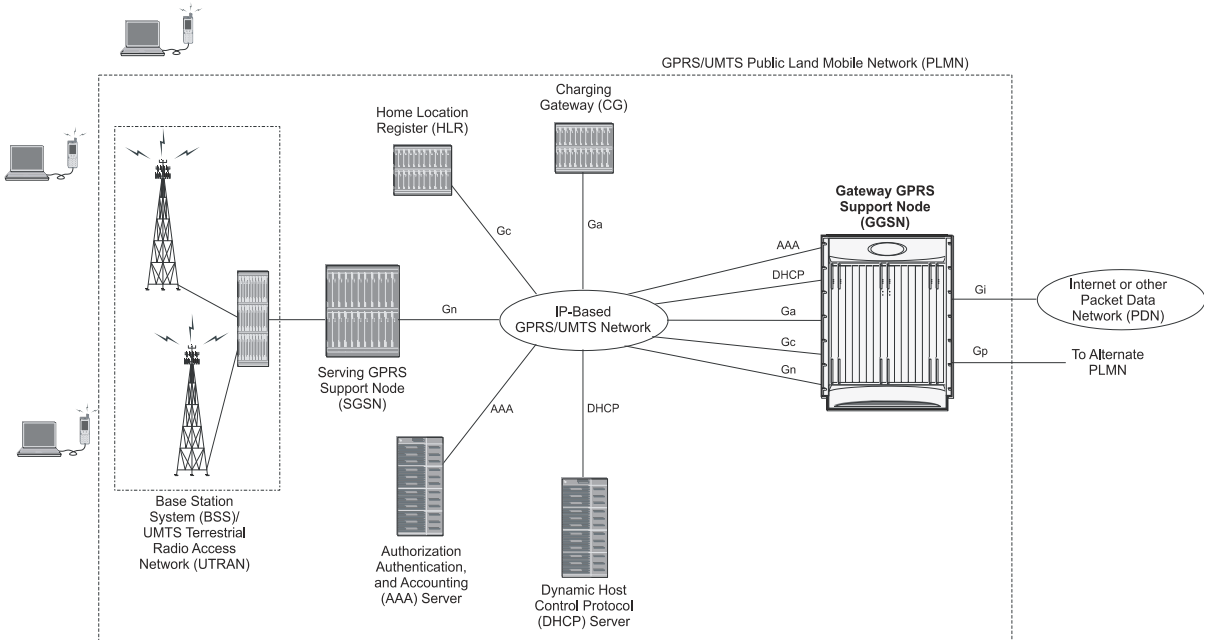


Figure 3. Combined GGSN/FA Deployment for Mobile IP and/or Proxy Mobile IP Support

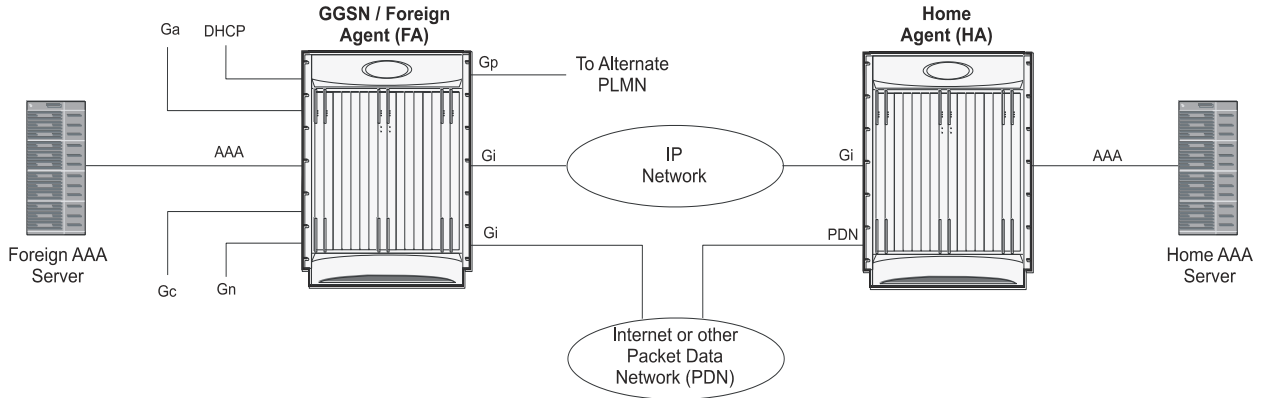
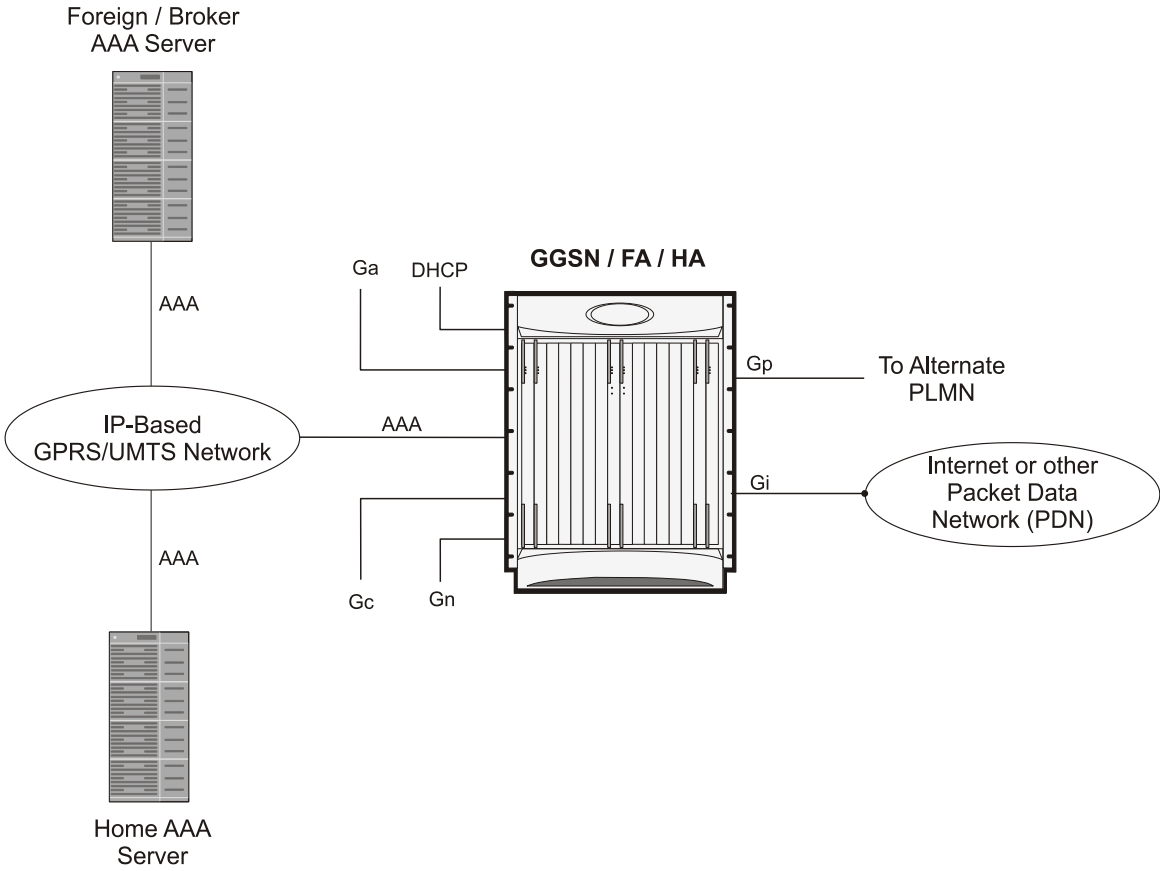


Figure 4. Combined GGSN/FA/HA Deployment for Mobile IP and/or Proxy Mobile IP Support



Supported Interfaces

In support of both mobile and network originated subscriber PDP contexts, the system GGSN provides the following network interfaces:

- **Gn**: This is the interface used by the GGSN to communicate with SGSNs on the same GPRS/UMTS Public Land Mobile Network (PLMN). This interface serves as both the signaling and data path for establishing and maintaining subscriber PDP contexts.

  The GGSN communicates with SGSNs on the PLMN using the GPRS Tunnelling Protocol (GTP). The signaling or control aspect of this protocol is referred to as the GTP Control Plane (GTPC) while the encapsulated user data traffic is referred to as the GTP User Plane (GTPU).

  One or more Gn interfaces can be configured per system context.

- **Ga**: This is the interface used by the GGSN to communicate with the Charging Gateway (CG). The charging gateway is responsible for sending GGSN Charging Data Records (G-CDRs) received from the GGSN for each PDP context to the billing system. System supports TCP and UDP as transport layer for this interface.

  The GGSN communicates with the CGs on the PLMN using GTP Prime (GTPP).

  One or more Ga interfaces can be configured per system context.

- **Gc**: This is the interface used by the GGSN to communicate with the Home Location Register (HLR) via a GTP-to-MAP (Mobile Application Part) protocol convertor. This interface is used for network initiated PDP contexts.

  For network initiated PDP contexts, the GGSN will communicate with the protocol convertor using GTP. The convertor, in turn, will communicate with the HLR using MAP over Signaling System 7 (SS7).

  One Gc interface can be configured per system context.

- **Gi**: This is the interface used by the GGSN to communicate with Packet Data Networks (PDNs) external to the PLMN. Examples of PDNs are the Internet or corporate intranets.

  Inbound packets received on this interface could initiate a network requested PDP context if the intended MS is not currently connected.

  For systems configured as a GGSN/FA, this interface is used to communicate with HAs for Mobile IP and Proxy Mobile IP support.

  One or more Gi interfaces can be configured per system context. For Mobile IP and Proxy Mobile IP, at least one Gi interface must be configured for each configured FA service. Note that when the system is simultaneously supporting GGSN, FA, and HA services, traffic that would otherwise be routed over the Gi interface is routed inside the chassis.

- **Gp**: This is the interface used by the GGSN to communicate with GPRS Support Nodes (GSNs, e.g. GGSNs and/or SGSNs) on different PLMNs. Within the system, a single interface can serve as both a Gn and a Gp interface.

  One or more Gn/Gp interfaces can be configured per system context.

- **AAA**: This is the interface used by the GGSN to communicate with an authorization, authentication, and accounting (AAA) server on the network. The system GGSN communicates with the AAA server using the Remote Authentication Dial In User Service (RADIUS) protocol.

  This is an optional interface that can be used by the GGSN for subscriber PDP context authentication and accounting.

- **DHCP**: This is the interface used by the GGSN to communicate with a Dynamic Host Control Protocol (DHCP) Server. The system can be configured as DHCP-Proxy or DHCP Client to provide IP addresses to MS on PDP contexts activation the DHCP server dynamically.

- **Gx**: This is an optional Diameter protocol-based interface over which the GGSN communicates with a Charging Rule Function (CRF) for the provisioning of charging rules that are based on the dynamic analysis of flows used for an IP Multimedia Subsystem (IMS) session. The system provides enhanced support for use of Service Based Local Policy (SBLP) to provision and control the resources used by the IMS subscriber. It also provides Flow based Charging (FBC) mechanism to charge the subscriber dynamically based on content usage.

  IMPORTANT: The Gx interface is a license-enabled support. For more information on this support, refer *Gx Interface Support* in *Features and Functionality - Optional Enhanced Feature Software* section.

- **Gy**: This is an optional Diameter protocol-based interface over which the GGSN communicates with a Charging Trigger Function (CTF) server that provides online charging data. Gy interface support provides an online charging interface that works with the ECS deep packet inspection feature. With Gy, customer traffic can be gated and billed in an “online” or “prepaid” style. Both time- and volume-based charging models are supported. In all of these models, differentiated rates can be applied to different services based on shallow or deep packet inspection.

  IMPORTANT: This interface is supported through Enhanced Charging Service. For more information on this support, refer *Enhanced Charging Service Administration Guide*.

- **GRE**: This new protocol interface in GGSN platform adds one additional protocol to support mobile users to connect to their enterprise networks: Generic Routing Encapsulation (GRE). GRE Tunneling is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSEC offers, for example).

  IMPORTANT: The GRE protocol interface is a license-enabled support. For more information on this support, refer *GRE Protocol Interface Support* in *Features and Functionality - Optional Enhanced Feature Software* section.

- **S6b**: This is an optional Diameter protocol-based interface over which the GGSN communicates with 3G AAA/HSS in LTE/SAE network for subscriber authorization.

  IMPORTANT: This interface is supported through license-enabled feature. For more information on this support, refer *Common Gateway Access Support* in guide.

IMPORTANT: GGSN Software also supports additional interfaces. For more information on additional interfaces, refer *Features and Functionality - Optional Enhanced Feature Software* section.

Features and Functionality - Base Software

This section describes the features and functions supported by default in base software on GGSN service and do not require any additional licenses.

IMPORTANT: To configure the basic service and functionality on the system for GGSN service, refer configuration examples provide in the GGSN Administration Guide.

This section describes following features:

- 16,000 SGSN Support
- AAA Server Groups
- Access Control List Support
- ANSI T1.276 Compliance
- APN Support
- Bulk Statistics Support
- Direct Tunnel Support
- DHCP Support
- DSCP Marking
- Generic Corporate APN
- GTPP Support
- Host Route Advertisement
- IP Policy Forwarding
- IP Header Compression - Van Jacobson
- Management System Overview
- Overlapping IP Address Pool Support
- Per APN Configuration to Swap out Gn to Gi APN in CDRs
- Port Insensitive Rule for Enhanced Charging Service
- Quality of Service Support
- RADIUS Support
- PDP Context Support
- RADIUS VLAN Support
- Routing Protocol Support
- Support of Charging Characteristics Provided by AAA Server

- Support of all GGSN generated causes for partial G-CDR closure
- Threshold Crossing Alerts (TCA) Support

16,000 SGSN Support

With growing roaming agreements, many more GPRS/UMTS networks support certain APNs and therefore the number of SGSNs that could connect to the GGSN increases. This feature increases the number of connected SGSNs thereby allowing a single GGSN service to support a much larger roaming network.

The GGSN service supports a maximum of 16,000 SGSN IP addresses. The chassis limit for bulk statistics collection is also limit to 16,000. No change in configuration is needed to support this feature.

AAA Server Groups

Value-added feature to enable VPN service provisioning for enterprise or MVNO customers. Enables each corporate customer to maintain its own AAA servers with its own unique configurable parameters and custom dictionaries.

This feature provides support for up to 800 AAA (RADIUS and Diameter) server groups and 800 NAS IP addresses that can be provisioned within a single context or across the entire chassis. A total of 128 servers can be assigned to an individual server group. Up to 1,600 accounting, authentication and/or mediation servers are supported per chassis and may be distributed across a maximum of 1,000 APNs. This feature also enables the AAA servers to be distributed across multiple APN within the same context.

IMPORTANT: Due to additional memory requirements, this service can only be used with 8GB minimum packet processing cards.

IMPORTANT: For more information on AAA Server Group configuration, refer *AAA Interface Administration and Reference*.

Access Control List Support

Access Control Lists provide a mechanism for controlling (i.e permitting, denying, redirecting, etc.) packets in and out of the system.

IP access lists, or Access Control Lists (ACLs) as they are commonly referred to, are used to control the flow of packets into and out of the system. They are configured on a per-context basis and consist of “rules” (ACL rules) or filters that control the action taken on packets that match the filter criteria

Once configured, an ACL can be applied to any of the following:

- An individual interface
- All traffic facilitated by a context (known as a policy ACL)

- An individual subscriber
- All subscriber sessions facilitated by a specific context

There are two primary components of an ACL:

- Rule: A single ACL consists of one or more ACL rules. As discussed earlier, the rule is a filter configured to take a specific action on packets matching specific criteria. Up to 128 rules can be configured per ACL.

  Each rule specifies the action to take when a packet matches the specifies criteria. This section discusses the rule actions and criteria supported by the system.
- Rule Order: A single ACL can consist of multiple rules. Each packet is compared against each of the ACL rules, in the order in which they were entered, until a match is found. Once a match is identified, all subsequent rules are ignored.

IMPORTANT: For more information on Access Control List configuration, refer *IP Access Control List* chapter in *System Enhanced Feature Configuration Guide*.

ANSI T1.276 Compliance

ANSI T1.276 specifies security measures for Network Elements (NE). In particular it specifies guidelines for password strength, storage, and maintenance security measures.

ANSI T1.276 specifies several measures for password security.

These measures include:

- Password strength guidelines
- Password storage guidelines for network elements
- Password maintenance, e.g. periodic forced password changes

These measures are applicable to the ASR 5000 and the Web Element Manager since both require password authentication. A subset of these guidelines where applicable to each platform will be implemented. A known subset of guidelines, such as certificate authentication, are not applicable to either product. Furthermore, the platforms support a variety of authentication methods such as RADIUS and SSH which are dependent on external elements. ANSI T1.276 compliance in such cases will be the domain of the external element. ANSI T1.276 guidelines will only be implemented for locally configured operators.

APN Support

The GGSN's Access Point Name (APN) support offers several benefits:

- Extensive parameter configuration flexibility for the APN.
- Creation of subscriber tiers for individual subscribers or sets of subscribers within the APN.
- Virtual APNs to allow differentiated services within a single APN.

Up to 1024 APNs can be configured in the GGSN. An APN may be configured for any type of PDP context, i.e., PPP, IPv4, IPv6 or both IPv4 and IPv6. Many dozens of parameters may be configured independently for each APN.

Here are a few highlights of what may be configured:

- **Accounting**: RADIUS, GTPP or none. Server group to use. Charging characteristics. Interface with mediation servers.
- **Authentication**: Protocol, such as, CHAP or PAP or none. Default username/password. Server group to use. Limit for number of PDP contexts.
- **Enhanced Charging**: Name of rulebase to use, which holds the enhanced charging configuration (e.g., eG-CDR variations, charging rules, prepaid/postpaid options, etc.).
- **IP**: Method for IP address allocation (e.g., local allocation by GGSN, Mobile IP, DHCP, DHCP relay, etc.). IP address ranges, with or without overlapping ranges across APNs.
- **Tunneling**: PPP may be tunneled with L2TP. IPv4 may be tunneled with GRE, IP-in-IP or L2TP. Load-balancing across multiple tunnels. IPv6 is tunneled in IPv4. Additional tunneling techniques, such as, IPsec and VLAN tagging may be selected by the APN, but are configured in the GGSN independently from the APN.
- **QoS**: IPv4 header ToS handling. Traffic rate limits for different 3GPP traffic classes. Mapping of R98 QoS attributes to work around particular handset defections. Dynamic QoS renegotiation (described elsewhere).

After an APN is determined by the GGSN, the subscriber may be authenticated/authorized with an AAA server. The GGSN allows the AAA server to return VSAs (Vendor Specific Attributes) that override any/all of the APN configuration. This allows different subscriber tier profiles to be configured in the AAA server, and passed to the GGSN during subscriber authentication/authorization.

The GGSN's Virtual APN feature allows the carrier to use a single APN to configure differentiated services. The APN that is supplied by the SGSN is evaluated by the GGSN in conjunction with multiple configurable parameters. Then the GGSN selects an APN configuration based on the supplied APN and those configurable parameters. The configurable parameters are the subscriber's mcc/mnc, whether the subscriber is home/visiting/roaming, the subscriber's domain name and the IP address/range of the SGSN.

IMPORTANT: For more information on APN configuration, refer *APN Configuration* in *GGSN Service Configuration*.

Bulk Statistics Support

The system's support for bulk statistics allows operators to choose to view not only statistics that are of importance to them, but also to configure the format in which it is presented. This simplifies the post-processing of statistical data since it can be formatted to be parsed by external, back-end processors.

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

The system can be configured to collect bulk statistics (performance data) and send them to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group. The individual statistics are grouped by schema.

The following schemas are supported for GGSN service:

- **System**: Provides system-level statistics
- **Card**: Provides card-level statistics

- **Port**: Provides port-level statistics
- **FA**: Provides FA service statistics
- **HA**: Provides HA service statistics
- **IP Pool**: Provides IP pool statistics
- **PPP**: Provides Point-to-Point Protocol statistics
- **GTPC**: Provides GPRS Tunneling Protocol - Control message statistics
- **GTPP**: Provides GPRS Tunneling Protocol - Prime message statistics
- **APN**: Provides Access Point Name statistics
- **RADIUS**: Provides per-RADIUS server statistics
- **ECS**: Provides Enhanced Charging Service Statistics

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

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

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

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

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

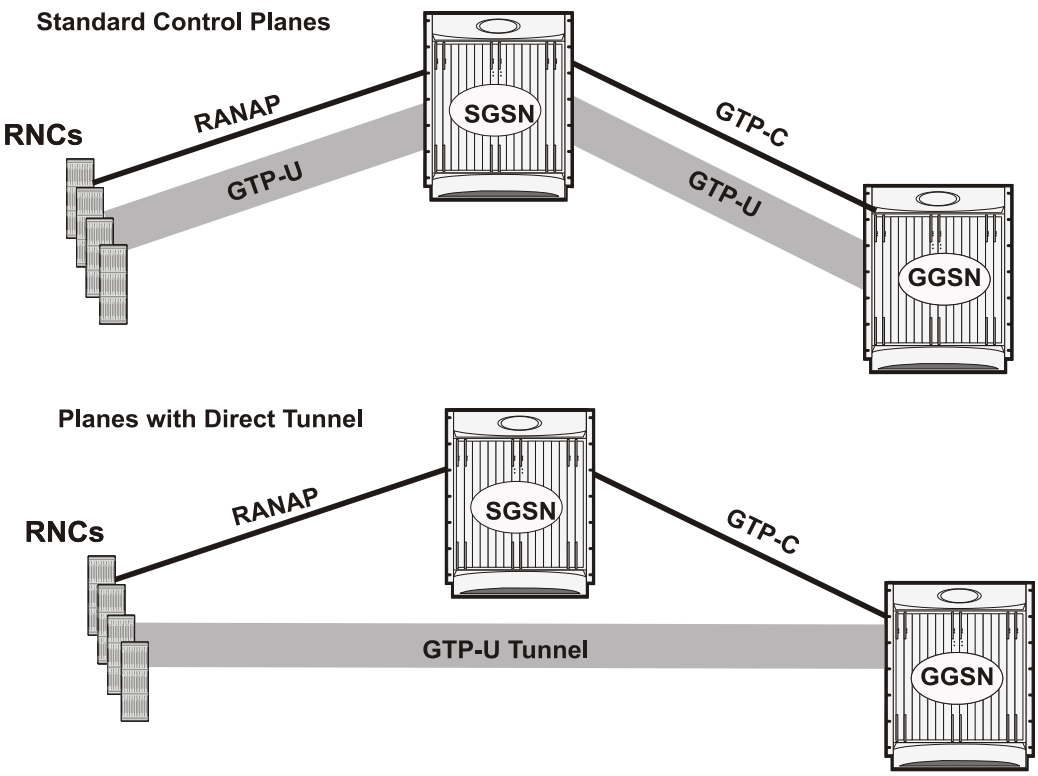
Direct Tunnel Support

Direct tunnel improves the user experience (e.g. expedited web page delivery, reduced round trip delay for conversational services, etc.) by eliminating SGSN tunnel ‘switching’ latency from the user plane. An additional advantage of Direct Tunnel from an operational and capital expenditure perspective is that direct tunnel optimizes the usage of user plane resources by removing the requirement for user plane processing on the SGSN.

The Direct Tunnel architecture allows the establishment of a direct user plane tunnel between the RAN and the GGSN, bypassing the SGSN. The SGSN continues to handle the control plane signalling and typical makes the decision to establish Direct Tunnel at PDP Context Activation. A Direct Tunnel is achieved at PDP context activation by the SGSN establishing a user plane (GTP-U) tunnel directly between RNC and GGSN (using an Update PDP Context Request towards the GGSN).

The following figure illustrates the working of Direct Tunnel between RNC and GGSN.

Figure 5. Direct Tunnel Support in GGSN



A major consequence of deploying Direct Tunnel is that it produces a significant increase in control plane load on both the SGSN and GGSN components of the packet core. It is therefore of paramount importance to a wireless operator to ensure that the deployed GGSNs are capable of handling the additional control plane loads introduced of part of Direct Tunnel deployment. The Cisco GGSN and SGSN offers massive control plane transaction capabilities, ensuring system control plane capacity will not be a capacity limiting factor once Direct Tunnel is deployed.

DHCP Support

Dynamic IP address assignment to subscriber IP PDP contexts using the Dynamic Host Control Protocol as defined by the following standards:

- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions

As described in the PDP Context Support section of this document, the method by which IP addresses are assigned to a PDP context is configured on an APN-by-APN basis. Each APN template dictates whether it will support static or dynamic addresses.

Dynamically assigned IP addresses for subscriber PDP contexts can be assigned through the use of DHCP.

The system can be configured to support DHCP using either of the following mechanisms:

- **DHCP-proxy**: The system acts as a proxy for client (MS) and initiates the DHCP Discovery Request on behalf of client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery

Request, it assigns the received IP address to the MS. This allocated address must be matched with the an address configured in an IP address pool on the system. This complete procedure is not visible to MS.

- **DHCP-relay**: The system acts as a relay for client (MS) and forwards the DHCP Discovery Request received from client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS.

IMPORTANT: For more information on DHCP service configuration, refer *DHCP Configuration* section in *GGSN Service Configuration* chapter.

DSCP Marking

Provides support for more granular configuration of DSCP marking.

For different Traffic class, the GGSN supports per-GGSN service and per-APN configurable DSCP marking for Uplink and Downlink direction based on Allocation/Retention Priority in addition to the current priorities.

Generic Corporate APN

Any operator may not be aware of the IP address that a corporation may assign to subscribers through AAA or DHCP and the traffic is sent from the GGSN to the corporation over a tunnel, this feature allows the operator to terminate such users.

Normally the GGSN validates the IP address assigned by RADIUS, however this feature removes the need for this, but does assume that the subscriber traffic is forwarded out of the GGSN through a tunnel.

When the IP address is statically assigned, i.e., either MS provided, RADIUS provided or DHCP provided, the IP address validation is not performed if the address policy is set to disable address validation.

ACL and Policy Group Info processing would still be performed.

Additionally, there is support for Virtual APN selection based on RADIUS VSA returned during Authentication.

The existing Virtual APN selection mechanism is being enhanced to select the Virtual APN based on RADIUS VSA returned during authentication.

The selected V-APN may further require AAA authentication (and accounting) with its own servers.

GTPP Support

Support for the GPRS Tunnelling Protocol Prime (GTPP) in accordance with the following standards:

- **3GPP TS 32.015 v3.12.0 (2003-12)**: 3rd Generation Partnership project; Technical Specification Group Services and System Aspects; Telecommunication Management; Charging and billing; GSM call and event data for the Packet Switched (PS) domain (Release 1999) for support of Charging on GGSN
- **3GPP TS 32.215 v5.9.0 (2005-06)**: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging data description for the Packet Switched (PS) domain (Release 4)

- **3GPP TS 29.060 v7.9.0 (2008-09)**: Technical Specification; 3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface (Release 6)

The system supports the use of GTPP for PDP context accounting. When the GTPP protocol is used, accounting messages are sent to the Charging Gateways (CGs) over the Ga interface. The Ga interface and GTPP functionality are typically configured within the system's source context. As specified by the standards, a CDR is not generated when a session starts. CDRs are generated according to the interim triggers configured using the charging characteristics configured for the GGSN, and a CDR is generated when the session ends. For interim accounting, STOP/START pairs are sent based on configured triggers.

GTPP version 2 is always used. However, if version 2 is not supported by the CGF, the system reverts to using GTPP version 1. All subsequent CDRs are always fully-qualified partial CDRs. All CDR fields are R4.

Whether or not the GGSN accepts charging characteristics from the SGSN can be configured on a per-APN basis based on whether the subscriber is visiting, roaming or, home.

By default, the GGSN always accepts the charging characteristics from the SGSN. They must always be provided by the SGSN for GTPv1 requests for primary PDP contexts. If they are not provided for secondary PDP contexts, the GGSN re-uses those from the primary.

If the system is configured to reject the charging characteristics from the SGSN, the GGSN can be configured with its own that can be applied based on the subscriber type (visiting, roaming, or home) at the APN level. GGSN charging characteristics consist of a profile index and behavior settings. The profile indexes specify the criteria for closing accounting records based specific criteria.

IMPORTANT: For more information on GTPP group configuration, refer *GTPP Accounting Configuration* in *GGSN Service Configuration*chapter.

Host Route Advertisement

When subscribers are assigned IP addresses from RADIUS or HLR, yet are allowed to connect to multiple GGSNs through the use of DNS round robin or failover, the IP addresses of the subscribers can be advertised on a per user (host) basis to the Gi network using dynamic routing, thereby providing IP reachability to these users.

IP address pools are configured on the GGSN for many reasons, although one of them is so that the pool subnets can be automatically advertised to the network. These are connected routes and are advertised for all non-tunneling pools.

A configuration **`explicit-route-advertise`** is provided to the IP pool configuration and when this option is enabled, the subnet(s) of the pool are not added to routing table and routing protocols like OSPF and BGP do not know of these addresses and hence do not advertise the subnet(s).

As calls come up, and addresses from this pool (with the “explicit-route-advertise” flag) are used, the assigned addresses are added to the routing table and these addresses can be advertised by OSPF or BGP through the network or the “redistribute connected” command.

Example
A subscriber connecting to GGSN A with an IP address from a pool P1 will be assigned the IP address and the routing domain will be updated with the host route. When a subscriber connects to GGSN B with an IP address from the same pool, the subscriber will be assigned the requested IP address and the routing domain will then learn its host route. When the subscriber disconnects, the route is removed from the routing table and the routing domain is updated. The explicit-route-advertise option can be applied and removed from the pool at any time and the routing tables are updated automatically.

The overlap and resource pool behavior does not change therefore it does not make sense to configure an overlap/resource pool with the “explicit-route-advertise” option.

IP Policy Forwarding

IP Policy Forwarding enables the routing of subscriber data traffic to specific destinations based on configuration. This functionality can be implemented in support of enterprise-specific applications (i.e. routing traffic to specific enterprise domains) or for routing traffic to back-end servers for additional processing.

The system can be configured to automatically forward data packets to a predetermined network destination. This can be done in one of three ways:

- **IP Pool-based Next Hop Forwarding** - Forwards data packets based on the IP pool from which a subscriber obtains an IP address.
- **ACL-based Policy Forwarding** - Forwards data packets based on policies defined in Access Control Lists (ACLs) and applied to contexts or interfaces.
- **Subscriber specific Next Hop Forwarding** - Forwards all packets for a specific subscriber.

The simplest way to forward subscriber data is to use IP Pool-based Next Hop Forwarding. An IP pool is configured with the address of a next hop gateway and data packets from all subscribers using the IP pool are forward to that gateway.

Subscriber Next Hop forwarding is also very simple. In the subscriber configuration a nexthop forwarding address is specified and all data packets for that subscriber are forwarded to the specified nexthop destination.

ACL-based Policy Forwarding gives you more control on redirecting data packets. By configuring an Access Control List (ACL) you can forward data packets from a context or an interface by different criteria, such as; source or destination IP address, ICMP type, or TCP/UDP port numbers.

ACLs are applied first. If ACL-based Policy Forwarding and Pool-based Next Hop Forwarding or Subscriber are configured, data packets are first redirected as defined in the ACL, then all remaining data packets are redirected to the next hop gateway defined by the IP pool or subscriber profile.

IMPORTANT: For more information on IP Policy Forwarding configuration, refer *Policy Forwarding* chapter in *System Enhanced Feature Configuration Guide*.

IP Header Compression - Van Jacobson

Implementing IP header compression provides the following benefits:

- Improves interactive response time
- Allows the use of small packets for bulk data with good line efficiency
- Allows the use of small packets for delay sensitive low data-rate traffic
- Decreases header overhead
- Reduces packet loss rate over lossy links

The system supports the Van Jacobson (VJ) IP header compression algorithms by default for subscriber traffic.

The VJ header compression is supported as per RFC 1144 (CTCP) header compression standard developed by V. Jacobson in 1990. It is commonly known as VJ compression. It describes a basic method for compressing the headers of IPv4/TCP packets to improve performance over low speed serial links.

By default IP header compression using the VJ algorithm is enabled for subscribers. You can also turn off IP header compression for a subscriber.

IMPORTANT: For more information on IP header compression support, refer *IP Header Compression* chapter in *System Enhanced Feature Configuration Guide*.

IPv6 Support

Native IPv6 support allows for the configuration of interfaces/routes with IPv6 (128 bit) addressing. The increased address space allows for future subscriber growth beyond what is currently possible in IPv4. Native IPv6 support on the Gi interface allows support for packets coming from or destined to a mobile over the Gi interface. IPv6 address assignment is supported from a dynamic or static pool via standard 3GPP attributes. The GGSN can communicate using DIAMETER as the transport protocol for Gx to the AAA. Overlapping address space or resource pools are supported if they are in different VPNs. The VPN subsystem is responsible for the configuration and recovery of IP interfaces and routes. IP resources are grouped into separate routing domains know as contexts. The VPN subsystem creates and maintains each context and the resources associated with them. The existing IPv4 model of interface and route notification will be extended to support IPv6.

This feature allows IPv6 subscribers to connect via the GPRS/UMTS infrastructure in accordance with the following standards:

- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461: Neighbor Discovery for IPv6
- RFC 2462: IPv6 Stateless Address Autoconfiguration
- RFC 3314: Recommendations for IPv6 in 3GPP Standards
- RFC 3316: Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts
- RFC 3056: Connection of IPv6 domains via IPv4 clouds
- 3GPP TS 23.060: General Packet Radio Service (GPRS) Service description
- 3GPP TS 27.060: Mobile Station Supporting Packet Switched Services
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)

IP version 6 is enhanced version of IP version 4 with following modifications:

- Expanded addressing capabilities with 128 bit for address as compared to 32 bits in IPv4.
- Header format simplification
- Improved support of extensions and options
- Flow labeling capability
- Authentication and Privacy capabilities

IPv6 Neighbor Discovery protocol is used to dynamically discover the directly attached devices on IPv6 Interfaces. It facilitates the mapping of MAC addresses to IPv6 Addresses. The GGSN supports a subset of IPv6 Neighbor Discovery as defined by RFC 2461, including the following:

- The GGSN uses IPv6 Neighbor Discovery to learn the Ethernet link-layer addresses of the directly connected next-hop gateway.
- The GGSN supports configuration of the static IPv6 neighbor (next-hop gateway).
- Link-local addresses will be automatically added to Ethernet type interfaces.
- The GGSN performs Unsolicited Neighbor Advertisement on line card switchover.
- The GGSN will reply to neighbor discovery requests for the node's IPv6 addresses.

ICMPv6 is a protocol for IPv6 networks to allow error reporting and check connectivity via echo messages. The GGSN supports a subset of ICMPv6 as defined by [RFC-4443]. The GGSN replies to the link-local, configured IP address, and the all-hosts IP address.

Native IPv6 Routing allows the forwarding of IPv6 packets between IPv6 Networks. The forwarding lookup is based on a longest prefix match of the destination IPv6 address. The GGSN supports configuration of IPv6 routes to directly attached next hops via an IPv6 Interface.

Management System Overview

The system's management capabilities are designed around the Telecommunications Management Network (TMN) model for management -- focusing on providing superior quality Network Element (NE) and element management system (Web Element Manager) functions. The system provides element management applications that can easily be integrated, using standards-based protocols (CORBA and SNMPv1, v2), into higher-level management systems -- giving wireless operators the ability to integrate the system into their overall network, service, and business management systems. In addition, all management is performed out-of-band for security and to maintain system performance.

The Operation and Maintenance module of ASR 5000 offers comprehensive management capabilities to the operators and enables them to operate the system more efficiently. There are multiple ways to manage the system either locally or remotely using its out-of-band management interfaces.

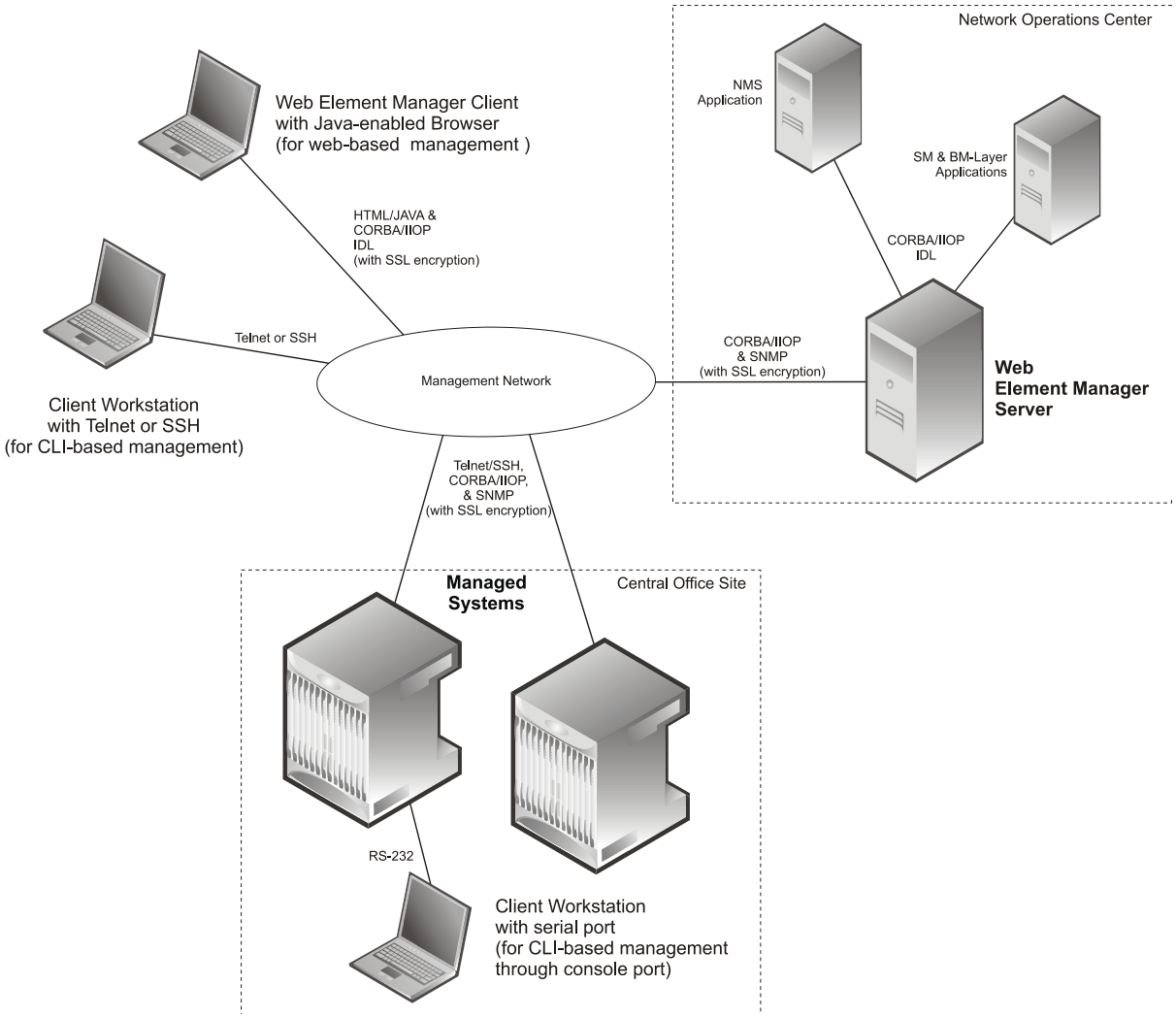
These include:

- Using the Command Line Interface (CLI)
- Remote login using Telnet, and Secure Shell (SSH) access to CLI through SPIO card's Ethernet management interfaces
- Local login through the Console port on SPIO card using an RS-232 serial connection
- Using the Web Element Manager application
- Supports communications through 10 Base-T, 100 Base-TX, 1000 Base-TX, or 1000
- Base-SX (optical gigabit Ethernet) Ethernet management interfaces on the SPIO
- Client-Server model supports any browser (i.e. Microsoft Internet Explorer v5.0 and above or Netscape v4.7 or above, and others)

- Supports Common Object Request Broker Architecture (CORBA) protocol and Simple Network Management Protocol version 1 (SNMPv1) for fault management
- Provides complete Fault, Configuration, Accounting, Performance, and Security (FCAPS) capabilities
- Can be easily integrated with higher-level network, service, and business layer applications using the Object Management Group's (OMG's) Interface Definition Language (IDL)

The following figure demonstrates these various element management options and how they can be utilized within the wireless carrier network.

Figure 6. Element Management Methods



IMPORTANT: GGSN management functionality is enabled by default for console-based access. For GUI-based management support, refer *Web Element Management System* section.

IMPORTANT: For more information on command line interface based management, refer *Command Line Interface Reference* and *GGSN Administration Guide*.

Overlapping IP Address Pool Support

Overlapping IP Address Pools provides a mechanism for allowing operators to more flexibly support multiple corporate VPN customers with the same private IP address space without the expensive investments in physically separate routers, or expensive configurations using virtual routers.

The system supports two type of overlapping pools: resource and overlap. Resource pools are designed for dynamic assignment only, and use a VPN tunnel, such as a GRE tunnel, to forward and received the private IP addresses to and from the VPN. Overlapping type pools can be used for both dynamic and static, and use VLANs and a next hop forwarding address to connect to the VPN customer.

To forward downstream traffic to the correct PDP context, the GGSN uses either the GRE tunnel ID, or the VLAN ID to match the packet. When forwarding traffic upstream, the GGSN uses the tunnel and forwarding information in the IP pool configuration, so overlapping pools must be configured in the APN for this feature to be used.

When a PDP context is created, the IP addresses is either assigned from the IP pool, in this case the forwarding rules are also configured into the GGSN at this point. If the address is assigned statically, when the GGSN confirms the IP address from the pool configured in the APN, the forwarding rules are also applied.

The GGSN can scale to as many actual overlapping pools as there are VLAN interfaces per context, and there can be multiple contexts per GGSN, or when using resource then the limit is the number of IP pools. This scalability allows operators, who wish to provide VPN services to customers using the customer's private IP address space, need not be concerned about escalating hardware costs, or complex configurations.

IMPORTANT: For more information on IP pool overlapping configuration, refer *VLANs* chapter in *System Enhanced Feature Configuration Guide*.

PDP Context Support

Support for subscriber primary and secondary Packet Data Protocol (PDP) contexts in accordance with the following standards:

- **3GPP TS 23.060 v7.4.0 (2007-9)**: 3rd Generation Partnership project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description (Release 1999) as an additional reference for GPRS/UMTS procedures
- **3GPP TS 29.061 v7.6.0 (2008-09)**: 3rd Generation Partnership Project; Technical Specification Group Core Network; Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN) (Release 4)

PDP context processing is based on the APN that the subscriber is attempting to access. Templates for all of the possible APNs that subscribers will be accessing must be configured within the system. Up to 1024 APNs can be configured on the system.

Each APN template consists of parameters pertaining to how PDP contexts are processed such as the following:

- Type (IPv4, IPv6, and/or PPP)

- Accounting protocol (GTPP or RADIUS
- Authentication protocol (CHAP, MSCHAP, PAP, MSID-based)
- Charging characteristics (use SGSN-supplied or use configured)
- IP address allocation method (static or dynamic)
- PDP Context timers
- Quality of Service

A total of 11 PDP contexts are supported per subscriber. These could be all 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 come up.

Per APN Configuration to Swap out Gn to Gi APN in CDRs

In order to allow for better correlation of CDRs with the network or application used by the subscriber, a configuration option has been added to the GGSN replace the Gn APN with the Gi (virtual) APN in emitted G-CDRs.

When virtual APNs are used, the operator can specify via EMS or a configuration command that the Gi APN should be used in the “Access Point Name Network Identifier” field of emitted G-CDRs, instead of the Gn APN.

Port Insensitive Rule for Enhanced Charging Service

This feature allows a single host or url rule to be applied to two different addresses, one with and one without the port number appended. As adding the port to the address is optional, this means that the number of rules could be halved.

Browser applications can sometimes appended the port number to the host or url when sending the host or URL fields. RFC 2616 for example states that port should be appended but if it is omitted then 80 should be assumed.

When configuring rules to define the content, as the web browser may provide the port number, even if it is the default one of 80 for HTTP, then two of each URL are needed.

Example

```
host = www.w3.org host = www.w3.org:80orhttp url =
http://213.229.187.118:80/chat/c/wel.w.wml http url =
http://213.229.187.118/chat/c/wel.w.wml
```

This feature provides a means to configure the rule such that the traffic is matched irrespective of the presence of a port number.

A new configurable has been added to the rulebase configuration that will ignore the port numbers embedded in the application headers of HTTP, RTSP, SIP, and WSP protocols.

When this feature is enabled, a single rule, such as “host = www.w3.org” would be matched even if the port number is appended and in this case the host field has the value www.w3.org:80, thereby cutting the number of rules needed by up to a half.

IMPORTANT: For more information on enhanced charging service, refer *Enhanced Charging Service Administration Guide*.

Quality of Service Support

Provides operator control over the prioritization of different types of traffic.

Quality of Service (QoS) support provides internal processing prioritization based on needs, and DiffServ remarking to allow external devices to perform prioritization.

IMPORTANT: The feature described here is internal prioritization and DiffServ remarking for external prioritization. For additional QoS capabilities of the GGSN, refer Features and Functionality - Optional Enhanced Feature Software section.

External prioritization (i.e., the value to use for the DiffServ marking) is configured for the uplink and downlink directions. In the uplink direction, each APN is configurable for the DiffServ ToS value to use for each of the 3GPP traffic classes. Alternatively, you can configure "pass-through", whereby the ToS value will pass through unchanged.

In the downlink direction, the ToS value of the subscriber packet is not changed, but you can configure what to use for the ToS value of the outer GTP tunnel. The value for ToS is configurable for each of the 3GPP traffic classes. In addition, the connections between the GGSN and one or more SGSNs can be configured as a "GGSN Service", and different values for ToS for the same 3GPP traffic class may be configured for different GGSN Services.

RADIUS Support

Provides a mechanism for performing authorization, authentication, and accounting (AAA) for subscriber PDP contexts based on the following standards:

- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000

The Remote Authentication Dial-In User Service (RADIUS) protocol is used to provide AAA functionality for subscriber PDP contexts. (RADIUS accounting is optional since GTPP can also be used.)

Within context contexts configured on the system, there are AAA and RADIUS protocol-specific parameters that can be configured. The RADIUS protocol-specific parameters are further differentiated between RADIUS Authentication server RADIUS Accounting server interaction.

Among the RADIUS parameters that can be configured are:

- **Priority**: Dictates the order in which the servers are used allowing for multiple servers to be configured in a single context.
- **Routing Algorithm**: Dictate the method for selecting among configured servers. The specified algorithm dictates how the system distributes AAA messages across the configured AAA servers for new sessions. Once a session is established and an AAA server has been selected, all subsequent AAA messages for the session will be delivered to the same server.

In the event that a single server becomes unreachable, the system attempts to communicate with the other servers that are configured. The system also provides configurable parameters that specify how it should behave should all of the RADIUS AAA servers become unreachable.

The system provides an additional level of flexibility by supporting the configuration RADIUS server groups. This functionality allows operators to differentiate AAA services for subscribers based on the APN used to facilitate their PDP context.

In general, 128 AAA Server IP address/port per context can be configured on the system and it selects servers from this list depending on the server selection algorithm (round robin, first server). Instead of having a single list of servers per context, this feature provides the ability to configure multiple server groups. Each server group, in turn, consists of a list of servers.

This feature works in following way:

- All RADIUS authentication/accounting servers configured at the context-level are treated as part of a server group named “default”. This default server group is available to all subscribers in that context through the realm (domain) without any configuration.
- It provides a facility to create “user defined” RADIUS server groups, as many as 399 (excluding “default” server group), within a context. Any of the user defined RADIUS server groups are available for assignment to a subscriber through the APN configuration within that context.

Since the configuration of the APN can specify the RADIUS server group to use as well as IP address pools from which to assign addresses, the system implements a mechanism to support some in-band RADIUS server implementations (i.e. RADIUS servers which are located in the corporate network, and not in the operator's network) where the NAS-IP address is part of the subscriber pool. In these scenarios, the GGSN supports the configuration of the first IP address of the subscriber pool for use as the RADIUS NAS-IP address.

IMPORTANT: For more information on RADIUS AAA configuration, refer *AAA Interface Administration and Reference*.

RADIUS VLAN Support

VPN customers often use private address space which can easily overlap with other customers. The subscriber addresses are supported with overlapping pools which can be configured in the same virtual routing context.

This feature now allows Radius Server and NAS IP addresses to also overlapping without the need to configure separate contexts, thereby simplifying APN and RADIUS configuration and network design.

This feature now allows Radius Server and NAS IP addresses to also overlapping without the need to configure separate contexts, thereby simplifying APN and RADIUS configuration and network design.

This feature supports following scenarios to be defined in the same context:

- Overlapping RADIUS NAS-IP address for various RADIUS server groups representing different APNs.
- Overlapping RADIUS server IP address for various RADIUS servers groups.

Previously, the above scenarios were supported, albeit only when the overlapping addresses were configured in different contexts. Moreover a static route was required in each context for IP connectivity to the RADIUS server.

The new feature utilizes the same concept as overlapping IP pools such that every overlapping NAS-IP address is giving a unique next-hop address which is then bound to an interface that is bound to a unique VLAN, thereby allowing the configuration to exist within the same context.

RADIUS access requests and accounting messages are forwarded to the next hop defined for that NAS-IP and it is then up to the connected router's forward the messages to the RADIUS server. The next hop address determines the interface and VLAN to use. Traffic from the server is identified as belonging to a certain NAS-IP by the port/VLAN combination.

The number of Radius NAS-IP addresses that can be configured is limited by the number of loopback addresses that can be configured.

IMPORTANT: For more information on VLAN support, refer *VLANs* chapter in *System Enhanced Feature Configuration Guide*.

Routing Protocol Support

The system's support for various routing protocols and routing mechanism provides an efficient mechanism for ensuring the delivery of subscriber data packets.

GGSN node supports Routing Protocol in different way to provide an efficient mechanism for delivery of subscriber data.

The following routing mechanisms and protocols are supported by the system:

- **Static Routes**: The system supports the configuration of static network routes on a per context basis. Network routes are defined by specifying an IP address and mask for the route, the name of the interface in the currant context that the route must use, and a next hop IP address.
- **Open Shortest Path First (OSPF) Protocol**: A link-state routing protocol, OSPF is an Interior Gateway Protocol (IGP) that routes IP packets based solely on the destination IP address found in the IP packet header using the shortest path first. IP packets are routed “as is”, meaning they are not encapsulated in any further protocol headers as they transit the network.

  Variable length subnetting, areas, and redistribution into and out of OSPF are supported.

  OSPF routing is supported in accordance with the following standards:

  - RFC-1850, OSPF Version 2 Management Information Base, November 1995
  - RFC-2328, OSPF Version 2, April 1998
  - RFC-3101 OSPF-NSSA Option, January 2003
- **Border Gateway Protocol version 4 (BGP-4)**: The system supports a subset of BGP (RFC-1771, A Border Gateway Protocol 4 (BGP-4)), suitable for eBGP support of multi-homing typically used to support geographically redundant mobile gateways, is supported.

  EBGP is supported with multi-hop, route filtering, redistribution, and route maps. The network command is support for manual route advertisement or redistribution.

  BGP route policy and path selection is supported by the following means:

  - Prefix match based on route access list

  - AS path access-list
  - Modification of AS path through path prepend
  - Origin type
  - MED
  - Weight
- **Route Policy**: Routing policies modify and redirect routes to and from the system to satisfy specific routing needs. The following methods are used with or without active routing protocols (i.e. static or dynamic routing) to prescribe routing policy:
  - **Route Access Lists**: The basic building block of a routing policy, route access lists filter routes based upon a specified range of IP addresses.
  - **IP Prefix Lists**: A more advanced element of a routing policy. An IP Prefix list filters routes based upon IP prefixes
  - **AS Path Access Lists**: A basic building block used for Border Gateway Protocol (BGP) routing, these lists filter Autonomous System (AS) paths.
- **Route Maps**: Route-maps are used for detailed control over the manipulation of routes during route selection or route advertisement by a routing protocol and in route redistribution between routing protocols. This detailed control is achieved using IP Prefix Lists, Route Access Lists and AS Path Access Lists to specify IP addresses, address ranges, and Autonomous System Paths.
- **Equal Cost Multiple Path (ECMP)**: ECMP allows distribution of traffic across multiple routes that have the same cost to the destination. In this manner, throughput load is distributed across multiple path, typically to lessen the burden on any one route and provide redundancy. The mobile gateway supports from four to ten equal-cost paths.

IMPORTANT: For more information on IP Routing configuration, refer *Routing* chapter in *System Enhanced Feature Configuration Guide*.

Support of Charging Characteristics Provided by AAA Server

This feature provides the ability for operators to apply Charging Characteristics (CC) from the AAA server instead of a hard coded local profile during access authentication.

The RADIUS attribute **3GPP-Chrg-Char** can be used to get the charging characteristics from RADIUS in Access-Accept message. Accepting the RADIUS returned charging characteristic profile must be enabled per APN. The CC profile returned by AAA will override any CC provided by the SGSN, the GGSN or per APN configuration. All 16 profile behaviors can be defined explicitly or the default configuration for that profile is used.

Support of all GGSN generated causes for partial G-CDR closure

Provides more detailed eG-CDR and/or G-CDR closure causes as per 3GPP TS 32.298.

System handles the GGSN generated causes for partial closure of CDRs. It supports various type of causes including Radio Access Technology Change, MS Time Zone Change, Cell update, inter-PLMN SGSN change, PLMN id change, QoS, Routing-Area update etc.

Threshold Crossing Alerts (TCA) Support

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

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

The following thresholding models are supported by the system:

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

Thresholding reports conditions using one of the following mechanisms:

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

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

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

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

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

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

IMPORTANT: For more information on threshold crossing alert configuration, refer *Thresholding Configuration Guide*.

Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions for GGSN service.

Each of the following features require the purchase of an additional license to implement the functionality with the GGSN service.

This section describes following features:

- Common Gateway Access Support
- Converged DSL Support on the GGSN
- Dynamic RADIUS Extensions (Change of Authorization)
- GRE Protocol Interface Support
- Gx Interface Support
- Inter-Chassis Session Recovery
- IP Security (IPSec)
- IPv6 Support
- L2TP LAC Support
- L2TP LNS Support
- Lawful Intercept
- Mobile IP Home and Foreign Agents
- Mobile IP NAT Traversal
- Multimedia Broadcast Multicast Services Support
- Overcharging Protection on Loss of Coverage
- Proxy Mobile IP
- Session Persistence
- Session Recovery Support
- Traffic Policing and Rate Limiting
- Web Element Management System

Common Gateway Access Support

Common Gateway Access support is a consolidated solution that combines 3G and 4G access technologies in a common gateway supporting logical services of HA, PGW, and GGSN to allow users to have the same user experience, independent of the access technology available.

In todays scenario an operator must have multiple access networks (CDMA, eHRPD and LTE) plus a GSM/UMTS solution for international roaming. Therefore, operator requires a solution to allow customers to access services with the same IP addressing behavior and to use a common set of egress interfaces, regardless of the access technology (3G or 4G).

This solution allows static customers to access their network services with the same IP addressing space assigned for wireless data, regardless of the type of connection (CDMA, eHRPD/LTE or GSM/UMTS). Subscribers using static IP addressing will be able to get the same IP address regardless of the access technology.

For more information on this product, refer *Common Gateway Access Support* section in GGSN Service Administration Guide.

Converged DSL Support on the GGSN

Digital Subscriber Line (DSL) is one of the dominant technologies used to provide wired broadband access to consumers and SOHO/ROBO today. DSL operates over copper telephone line owned by Local Exchange Carriers, who often have strong relationships to the Mobile Wireless Operators either through shared ownership or joint holdings. This feature allows Mobile Wireless Operators to provide DSL converged services with the GGSN.

Dynamic RADIUS Extensions (Change of Authorization)

Dynamic RADIUS extension support provide operators with greater control over subscriber PDP contexts by providing the ability to dynamically redirect data traffic, and or disconnect the PDP context.

This functionality is based on the RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS), July 2003 standard.

The system supports the configuration and use of the following dynamic RADIUS extensions:

- **Change of Authorization**: The system supports CoA messages from the AAA server to change data filters associated with a subscriber session. The CoA request message from the AAA server must contain attributes to identify NAS and the subscriber session and a data filter ID for the data filter to apply to the subscriber session.
- **Disconnect Message**: The DM message is used to disconnect subscriber sessions in the system from a RADIUS server. The DM request message should contain necessary attributes to identify the subscriber session.

The above extensions can be used to dynamically re-direct subscriber PDP contexts to an alternate address for performing functions such as provisioning and/or account set up. This functionality is referred to as Session Redirection, or Hotlining.

Session redirection provides a means to redirect subscriber traffic to an external server by applying ACL rules to the traffic of an existing or a new subscriber session. The destination address and optionally the destination port of TCP/IP or UDP/IP packets from the subscriber are rewritten so the packet is forwarded to the designated redirected address.

Return traffic to the subscriber has the source address and port rewritten to the original values. The redirect ACL may be applied dynamically by means of the Radius Change of Authorization (CoA) extension.

IMPORTANT: For more information on dynamic RADIUS extensions support, refer *CoA, RADIUS, And Session Redirection (Hotlining)* chapter in *System Enhanced Feature Configuration Guide*.

GRE Protocol Interface Support

GGSN supports GRE generic tunnel interface support in accordance with RFC-2784, Generic Routing Encapsulation (GRE).

GRE protocol functionality adds one additional protocol on ASR 5000 to support mobile users to connect to their enterprise networks through Generic Routing Encapsulation (GRE).

GRE tunnels can be used by the enterprise customers of a carrier 1) To transport AAA packets corresponding to an APN over a GRE tunnel to the corporate AAA servers and, 2) To transport the enterprise subscriber packets over the GRE tunnel to the corporation gateway.

The corporate servers may have private IP addresses and hence the addresses belonging to different enterprises may be overlapping. Each enterprise needs to be in a unique virtual routing domain, known as VRF. To differentiate the tunnels between same set of local and remote ends, GRE Key will be used as a differentiation.

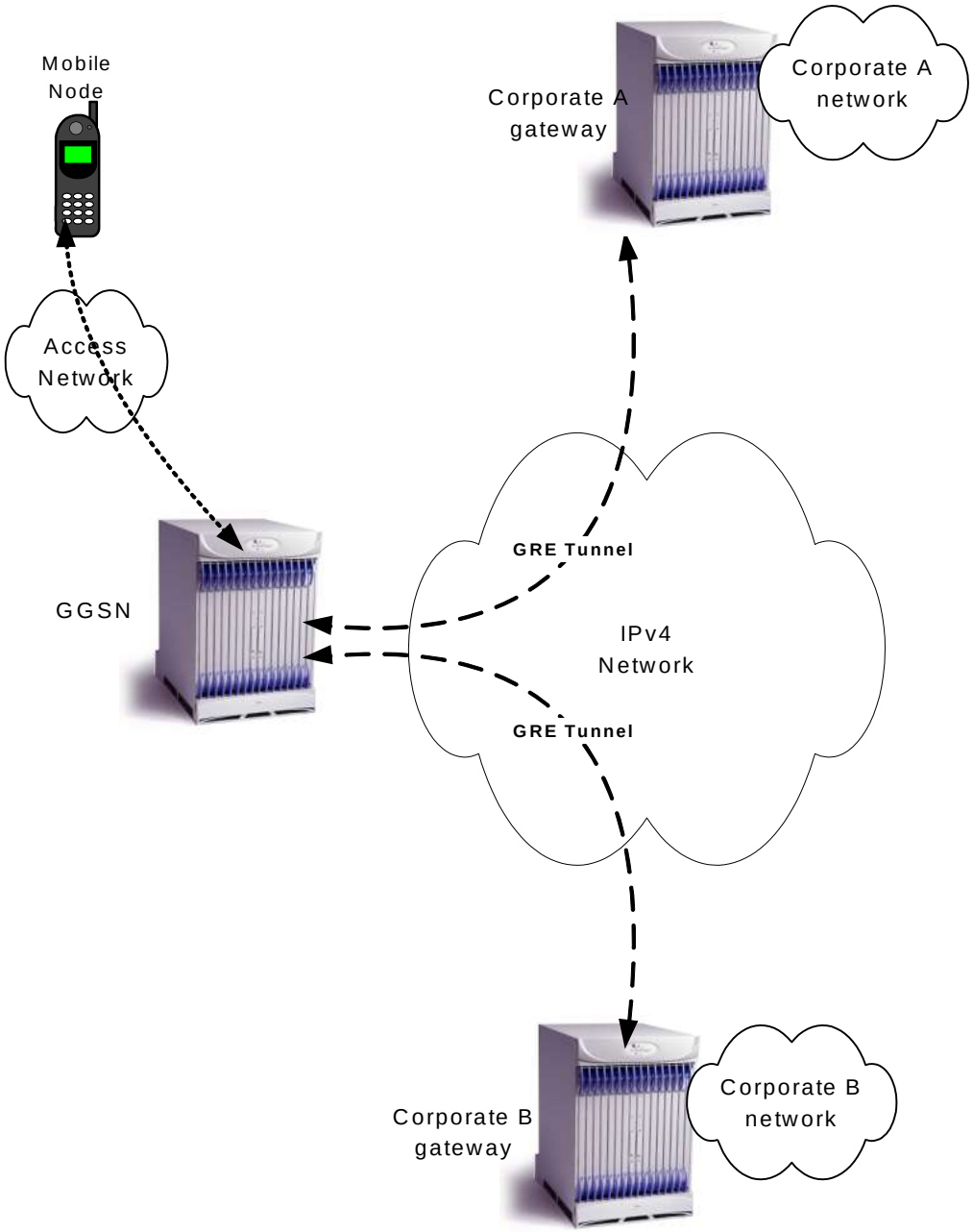
GRE Tunneling is a common technique to enable multi-protocol local networks over a single-protocol backbone, to connect non-contiguous networks and allow virtual private networks across WANs. This mechanism encapsulates data packets from one protocol inside a different protocol and transports the data packets unchanged across a foreign network. It is important to note that GRE tunneling does not provide security to the encapsulated protocol, as there is no encryption involved (like IPSEC offers, for example).

GRE Tunneling consists of three main components:

- Passenger protocol-protocol being encapsulated. For example: CLNS, IPv4 and IPv6.
- Carrier protocol-protocol that does the encapsulating. For example: GRE, IP-in-IP, L2TP, MPLS and IPSEC.
- Transport protocol-protocol used to carry the encapsulated protocol. The main transport protocol is IP.

The most simplified form of the deployment scenario is shown in the following figure, in which GGSN has two APNs talking to two corporate networks over GRE tunnels.

Figure 7. GRE Deployment Scenario



Gx Interface Support

Gx interface support on the system enables the wireless operator to:

- Implement differentiated service profiles for different subscribers

- Intelligently charge the services accessed depending on the service type and parameters

This interface is particularly suited to control and charge multimedia applications and IMS services. This interface support is compliant to following standards:

- 3GPP TS 23.203 V7.6.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 7)
- 3GPP TS 29.210 V6.2.0 (2005-06): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Charging rule provisioning over Gx interface; (Release 6)
- 3GPP TS 29.212 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)
- 3GPP TS 29.213 V7.4.0 (2008-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)
- RFC 3588, Diameter Base Protocol
- RFC 4006, Diameter Credit-Control Application

In addition to the above RFCs and standards IMS authorization partially supports 3GPP TS 29.212 for Policy and Charging Control over Gx reference point functionality.

The goal of the Gx interface is to provide network based QoS control as well as dynamic charging rules on a per bearer basis. The Gx interface is in particular needed to control and charge multimedia applications.

The Gx interface is located between the GGSN and the E-PDF / PCRF. It is a Diameter- based interface and provides the functions provided earlier by the Gx and Go interfaces:

- QoS control based on either a token-based or token-less mechanism. In the token-based mechanism, the E-PDF or PCRF dynamically assign network resources to the different bearers used by the subscriber. These resource assignments are transmitted in Tokens carried over the Gx interface. The authorization tokens are allocated by the network (E-PDF/PCRF), hence the network is in full control of the mechanism since it only authorizes resources. The token-less mechanism is for further study.
- Dynamic rules for Flexible Bearer Charging. These dynamic charging rules are carried in the resource assignment tokens and provide 5-tuple type charging rules that enables to implement a specific charging policy for each subscriber bearer. These charging rules will be applied by the FBC function of the GGSN, and produce the appropriate eG-CDRs or the appropriate messages on the Gy interface to the OCS.

IMPORTANT: For more information on Gx interface support, refer *Gx Interface Support* chapter in *System Enhanced Feature Configuration Guide*.

Inter-Chassis Session Recovery

The ASR 5000 provides industry leading carrier class redundancy. The systems protects against all single points of failure (hardware and software) and attempts to recover to an operational state when multiple simultaneous failures occur.

The system provides several levels of system redundancy:

- Under normal N+1 packet processing card hardware redundancy, if a catastrophic packet processing card failure occurs all affected calls are migrated to the standby packet processing card if possible. Calls which cannot be migrated are gracefully terminated with proper call-termination signaling and accounting records are generated with statistics accurate to the last internal checkpoint
- If the Session Recovery feature is enabled, any total packet processing card failure will cause a packet processing card switchover and all established sessions for supported call-types are recovered without any loss of session.

Even though chassis provides excellent intra-chassis redundancy with these two schemes, certain catastrophic failures which can cause total chassis outages, such as IP routing failures, line-cuts, loss of power, or physical destruction of the chassis, cannot be protected by this scheme. In such cases, the GGSN Inter-Chassis Session Recovery feature provides geographic redundancy between sites. This has the benefit of not only providing enhanced subscriber experience even during catastrophic outages, but can also protect other systems such as the RAN from subscriber re-activation storms.

The Interchassis Session Recovery feature allows for continuous call processing without interrupting subscriber services. This is accomplished through the use of redundant chassis. The chassis are configured as primary and backup with one being active and one in recovery mode. A checkpoint duration timer is used to control when subscriber data is sent from the active chassis to the inactive chassis. If the active chassis handling the call traffic goes out of service, the inactive chassis transitions to the active state and continues processing the call traffic without interrupting the subscriber session. The chassis determines which is active through a propriety TCP-based connection called a redundancy link. This link is used to exchange Hello messages between the primary and backup chassis and must be maintained for proper system operation.

- **Interchassis Communication**:

  Chassis configured to support Interchassis Session Recovery communicate using periodic Hello messages. These messages are sent by each chassis to notify the peer of its current state. The Hello message contains information about the chassis such as its configuration and priority. A dead interval is used to set a time limit for a Hello message to be received from the chassis' peer. If the standby chassis does not receive a Hello message from the active chassis within the dead interval, the standby chassis transitions to the active state. In situations where the redundancy link goes out of service, a priority scheme is used to determine which chassis processes the session. The following priority scheme is used:

  - router identifier
  - chassis priority
  - SPIO MAC address

- **Checkpoint Message**:p

  Checkpoint messages are sent from the active chassis to the inactive chassis. Checkpoint messages are sent at specific intervals and contain all the information needed to recreate the sessions on the standby chassis, if that chassis were to become active. Once a session exceeds the checkpoint duration, checkpoint data is collected on the session. The checkpoint parameter determines the amount of time a session must be active before it is included in the checkpoint message.

IMPORTANT: For more information on inter-chassis session recovery support, refer *Interchassis Session Recovery* chapter in *System Enhanced Feature Configuration Guide*.

IP Security (IPSec)

IP Security provides a mechanism for establishing secure tunnels from mobile subscribers to pre-defined endpoints (i.e. enterprise or home networks) in accordance with the following standards:

- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-3193, Securing L2TP using IPSEC, November 2001

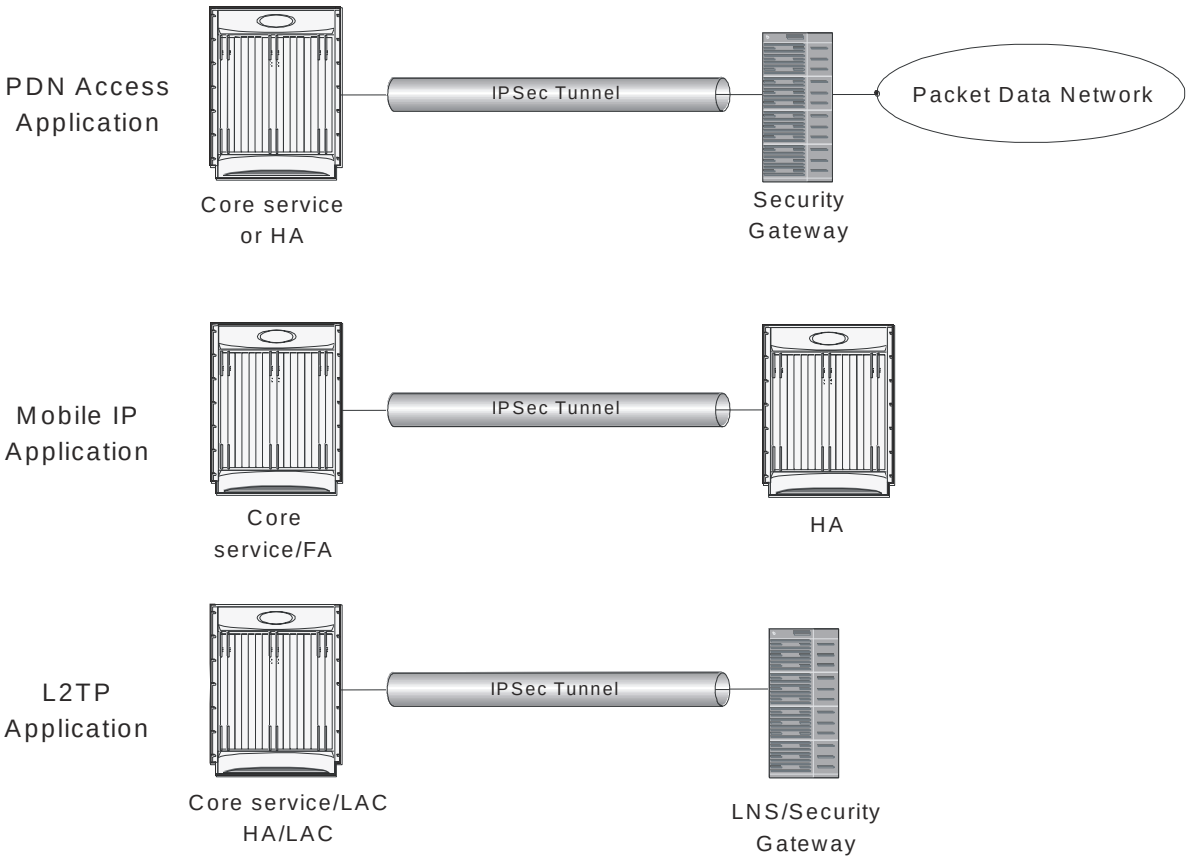
IP Security (IPSec) is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways. IPSec can be implemented on the system for the following applications:

- **PDN Access**: Subscriber IP traffic is routed over an IPSec tunnel from the system to a secure gateway on the Packet Data Network (PDN) as determined by Access Control List (ACL) criteria.
- **Mobile IP**: Mobile IP control signals and subscriber data is encapsulated in IPSec tunnels that are established between Foreign Agents (FAs) and Home Agents (HAs) over the Pi interfaces.

  IMPORTANT: Once an IPSec tunnel is established between an FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions will be unaffected.

- **L2TP**: L2TP-encapsulated packets are routed from the system to an LNS/secure gateway over an IPSec tunnel.

Figure 8. IPSec Application



IMPORTANT: For more information on IPSec support, refer IP Security chapter in System Enhanced Feature Configuration Guide.

IPv6 Support

Native IPv6 support allows for the configuration of interfaces/routes with IPv6 (128 bit) addressing. The increased address space allows for future subscriber growth beyond what is currently possible in IPv4. Native IPv6 support on the Gi interface allows support for packets coming from or destined to a mobile over the Gi interface. IPv6 address assignment is supported from a dynamic or static pool via standard 3GPP attributes. The GGSN can communicate using DIAMETER as the transport protocol for Gx to the AAA. Overlapping address space or resource pools are supported if they are in different VPNs. The VPN subsystem is responsible for the configuration and recovery of IP interfaces and routes. IP resources are grouped into separate routing domains know as contexts. The VPN subsystem creates and maintains each context and the resources associated with them. The existing IPv4 model of interface and route notification will be extended to support IPv6.

This feature allows IPv6 subscribers to connect via the GPRS/UMTS infrastructure in accordance with the following standards:

- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461: Neighbor Discovery for IPv6
- RFC 2462: IPv6 Stateless Address Autoconfiguration
- RFC 3314: Recommendations for IPv6 in 3GPP Standards
- RFC 3316: Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts
- RFC 3056: Connection of IPv6 domains via IPv4 clouds
- 3GPP TS 23.060: General Packet Radio Service (GPRS) Service description
- 3GPP TS 27.060: Mobile Station Supporting Packet Switched Services
- 3GPP TS 29.061: Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)

IP version 6 is enhanced version of IP version 4 with following modifications:

- Expanded addressing capabilities with 128 bit for address as compared to 32 bits in IPv4.
- Header format simplification
- Improved support of extensions and options
- Flow labeling capability
- Authentication and Privacy capabilities

IPv6 Neighbor Discovery protocol is used to dynamically discover the directly attached devices on IPv6 Interfaces. It facilitates the mapping of MAC addresses to IPv6 Addresses. The GGSN supports a subset of IPv6 Neighbor Discovery as defined by RFC 2461, including the following:

- The GGSN uses IPv6 Neighbor Discovery to learn the Ethernet link-layer addresses of the directly connected next-hop gateway.
- The GGSN supports configuration of the static IPv6 neighbor (next-hop gateway).
- Link-local addresses will be automatically added to Ethernet type interfaces.
- The GGSN performs Unsolicited Neighbor Advertisement on line card switchover.
- The GGSN will reply to neighbor discovery requests for the node's IPv6 addresses.

ICMPv6 is a protocol for IPv6 networks to allow error reporting and check connectivity via echo messages. The GGSN supports a subset of ICMPv6 as defined by [RFC-4443]. The GGSN replies to the link-local, configured IP address, and the all-hosts IP address.

L2TP LAC Support

The system configured as a Layer 2 Tunneling Protocol Access Concentrator (LAC) enables communication with L2TP Network Servers (LNSs) for the establishment of secure Virtual Private Network (VPN) tunnels between the operator and a subscriber's corporate or home network.

The use of L2TP in VPN networks is often used as it allows the corporation to have more control over authentication and IP address assignment. An operator may do a first level of authentication, however use PPP to exchange user name and password, and use IPCP to request an address. To support PPP negotiation between the GGSN and the corporation, an L2TP tunnel must be setup in the GGSN running a LAC service.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. The LAC service is based on the same architecture as the GGSN and benefits from dynamic resource allocation and distributed message and data processing. This design allows the LAC service to support over 4000 setups per second or a maximum of over 3G of throughput. There can be a maximum up to 65535 sessions in a single tunnel and as many as 500,000 L2TP sessions using 32,000 tunnels per system.

The LAC sessions can also be configured to be redundant, thereby mitigating any impact of hardware of software issues. Tunnel state is preserved by copying the information across processor cards.

IMPORTANT: For more information on this feature support, refer *L2TP Access Concentrator* chapter in *System Enhanced Feature Configuration Guide*.

L2TP LNS Support

The system configured as a Layer 2 Tunneling Protocol Network Server (LNS) supports the termination secure Virtual Private Network (VPN) tunnels between from L2TP Access Concentrators (LACs).

The LNS service takes advantage of the high performance PPP processing already supported in the system design and is a natural evolution from the LAC. The LNS can be used as a standalone, or running alongside a GGSN service in the same platform, terminating L2TP services in a cost effective and seamless manner.

L2TP establishes L2TP control tunnels between LAC and LNS before tunneling the subscriber PPP connections as L2TP sessions. There can be a maximum of up to 65535 sessions in a single tunnel and up to 500,000 sessions per LNS.

The LNS architecture is similar to the GGSN and utilizes the concept of a de-multiplexer to intelligently assign new L2TP sessions across the available software and hardware resources on the platform without operator intervention.

IMPORTANT: For more information on this feature support, refer *L2TP Network Server* chapter in *System Enhanced Feature Configuration Guide*.

Lawful Intercept

The system supports the Lawful Interception (LI) of subscriber session information. This functionality provides Telecommunication Service Providers (TSPs) with a mechanism to assist Law Enforcement Agencies (LEAs) in the monitoring of suspicious individuals (referred to as targets) for potential criminal activity.

The following standards were referenced for the system's LI implementation:

- TR-45 Lawfully Authorized Electronic Surveillance TIA/EIA J-STD-025 PN4465 RV 1.7
- 3GPP TS 33.106 V6.1.0 (2004-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful Interception requirements (Release 6)
- 3GPP TS 33.107 V6.2.0 (2004-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions (Release 6)
- 3GPP TS 33.108 V9.0.0 (2009-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Handover interface for Lawful Interception (LI) (Release 9)

- Technical Directive: Requirements for implementing statutory telecommunications interception measures (TR TKÜ), Version 4.0

LEAs provide one or more TSPs with court orders or warrants requesting the monitoring of a particular target. The target is identified by information such as their mobile station Integrated Services Digital Network (MSISDN) number, or their International Mobile Subscriber Identification (IMSI) number.

Once the target has been identified, the system, functioning as either a GGSN or HA, serves as an Access Function (AF) and performs monitoring for both new PDP contexts or PDP contexts that are already in progress. While monitoring, the system intercepts and duplicates Content of Communication (CC) and/or Intercept Related Information (IRI) and forwards it to a Delivery Function (DF) over an extensible, proprietary interface. Note that when a target establishes multiple, simultaneous PDP contexts, the system intercepts CC and IRI for each of them. The DF, in turn, delivers the intercepted content to one or more Collection Functions (CFs).

Lawful intercept supports TCP transport on node interfaces along with support for IPv6 address link between chassis and LI server.

On ASR 5000 or higher platforms with StarOS version 9.0 or later, this feature enhanced to allow 20,000 LI targets to be provisioned as well as monitored.

CAUTION: This capacity improvement impacts performance over various network scenario and in order to reach the full target of 20000 LI targets, it is required that the used platform have at least 12 active packet processing cards installed.

IMPORTANT: For more information on this feature support, refer *Lawful Intercept Configuration Guide*.

Mobile IP Home and Foreign Agents

Consolidation of GGSN, HA and/or FA services on the same platform eliminates CapEx and OpEx requirements for separate network elements and devices under management. Service integration also enables seamless mobility and inter-technology roaming between 1xEV-DO and UMTS/W-CDMA/GPRS/EDGE radio access networks. This shared configuration also enables common address pools to be applied across all service types. In addition, this combination of collapsed services does not create dependencies for Mobile IP client software on the user access device and consequently does not introduce additional requirements for Mobile IP signaling in the 3GPP radio access network.

This functionality provides the following benefits:

- Timely release of Mobile IP resources at the FA and/or HA
- Accurate accounting
- Timely notification to mobile node of change in service

The ASR 5000 system are capable of supporting both GGSN and Mobile IP functions on a single chassis. For Mobile IP applications, the system can be configured to provide the function of a Gateway GPRS Support Node/Foreign Agent (GGSNSN/FA) and/or a Home Agent (HA).

HA and FA components are defined by RFC 2002 in support of Mobile IP. Mobile IP provides a network-layer solution that allows Mobile Nodes (MNs, i.e. mobile phones, wireless PDAs, and other mobile devices) to receive routed IP packets from their home network while they are connected to any visitor network using their permanent or home IP

address. Mobile IP allows mobility in a dynamic method that allows nodes to maintain ongoing communications while changing links as the user traverses the global Internet from various locations outside their home network.

When configured to support HA functionality, the system is capable of supporting following enhanced features:

- **Mobile IP HA Session Rejection/Redirection**: Enables the HA service to either reject new calls or redirect them to another HA when a destination network connection failure is detected. When network connectivity is re-established, the HA service begins to accept calls again in the normal manner. This feature provides the benefit of reducing OpEx through increased operational efficiency and limiting of system downtime.
- **Mobile IP Registration Revocation**: Registration Revocation is a general mechanism whereby the HA providing Mobile IP or Proxy Mobile IP functionality to a mobile node can notify the GGSN/FA of the termination of a binding. Mobile IP Registration Revocation can be triggered at the HA by any of the following:
  - Administrative clearing of calls
  - Session Manager software task outage resulting in the loss of FA sessions (sessions that could not be recovered)
  - Session Idle timer expiry (when configured to send Revocation)
  - Any other condition under which a binding is terminated due to local policy (duplicate IMSI detected, duplicate home address requested)

IMPORTANT: For more information on Mobile IP HA service and FA service configuration, refer *HA Administration Guide* and *GGSN Administration Guide* respectively

Mobile IP NAT Traversal

This functionality enables converged WiFi-cellular data deployments in which the system is used to concentrate and switch traffic between WiFi hotspots. UDP/IP tunneling enables NAT firewalls in WLAN hotspots to maintain state information for address translation between NATed public address/UDP ports and addresses that are privately assigned for the mobile access device by a local DHCP server.

The Mobile IP protocol does not easily accommodate subscriber mobile nodes that are located behind WLAN or WAN-based NAT devices because it assumes that the addresses of mobile nodes or FA's are globally routable prefixes. However, the mobile node’s co-located care of address (CCoA/CoA) is a private address. This presents a problem when remote hosts try to reach the mobile node via the public advertised addresses. The system provides a solution that utilizes UDP tunneling subject to subscriber reservation requests. In this application, the HA uses IP UDP tunneling to reach the mobile subscriber and includes the same private address that was provided in original reservation request in the encapsulated IP payload packet header.

IMPORTANT: For more information on this feature, refer *MIP NAT Traversal* chapter in *System Enhanced Feature Configuration Guide*.

Multimedia Broadcast Multicast Services Support

Multimedia services are taking on an ever-increasing role in the wireless carriers' plans for an application centric service model. As such, any next generation GGSN platform must be capable of supporting the requirements of multimedia service delivery, including:

- Higher bandwidth requirements of streaming audio and video delivery
- Efficient broadcast and multicast mechanisms, to conserve resources in the RAN

MBMS represents the evolutionary approach to multicast and broadcast service delivery. MBMS uses spectrum resources much more efficiently than Multicast-over-Unicast by optimizing packet replication across all critical components in the bearer path. Thus, services requiring largely uni-directional multicast flows towards the UE are particularly well suited to the MBMS approach. These would include news, event streaming, suitably encoded/compressed cable/radio programs, video-on-demand, multi-chat / group-push-to-talk/video-conferencing sessions with unicast uplink and multicast downlink connections, and other applications.

For MBMS functionality, the system supports the Gmb interface, which is used signal to the BM-SC

IMPORTANT: For more information on this feature, refer *Multicast Broadcast Service* chapter in *System Enhanced Feature Configuration Guide*.

Overcharging Protection on Loss of Coverage

This solution provides the ability to configure mobile carriers to maximize their network solutions and balancing the requirements to accurately bill their customer.

Considerin a scenario where a mobile is streaming or downloading very large files from external sources and the mobile goes out of radio coverage. If this download is happening on Background/Interactive traffic class then the GGSN is unaware of such loss of connectivity as SGSN does not perform the Update PDP Context procedure to set QoS to 0kbps (this is done when traffic class is either Streaming or Conversational only). The GGSN continues to forward the downlink packets to SGSN. In the loss of radio coverage, the SGSN will do paging request and find out that the mobile is not responding; SGSN will then drops the packets. In such cases, the G-CDR will have increased counts but S-CDR will not. This means that when operators charge the subscribers based on G-CDR the subscribers may be overcharged. This feature is implemented to avoid the overcharging in such cases.

This implementation is based on Cisco-specific private extension to GTP messages and/or any co-relation of G-CDRs and S-CDRs. It also does not modify any RANAP messages.

IMPORTANT: For more information on this feature, refer *Subscriber Overcharging Protection* chapter in *System Enhanced Feature Configuration Guide*.

Proxy Mobile IP

Mobility for subscriber sessions is provided through the Mobile IP protocol as defined in RFCs 2002-2005. However, some older Mobile Nodes (MNs) do not support the Mobile IP protocol. The Proxy Mobile IP feature provides a mobility solution for these MNs.

For IP PDP contexts using Proxy Mobile IP, the MN establishes a session with the GGSN as it normally would. However, the GGSN/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber's profile) on behalf of the MN (i.e. the MN is only responsible for maintaining the IP PDP context with the GGSN, no Agent Advertisement messages are communicated with the MN).

The MN is assigned an IP address by either the HA, an AAA server, or on a static-basis. The address is stored in a Mobile Binding Record (MBR) stored on the HA. Therefore, as the MN roams through the service provider's network, each time a hand-off occurs, the MN will continue to use the same IP address stored in the MBR on the HA.

Proxy Mobile IP can be performed on a per-subscriber basis based on information contained in their user profile, or for all subscribers facilitated by a specific APN. In the case of non-transparent IP PDP contexts, attributes returned from the subscriber's profile take precedence over the configuration of the APN.

IMPORTANT: For more information on this feature, refer *Proxy Mobile IP* chapter in *System Enhanced Feature Configuration Guide*.

Session Persistence

IMPORTANT: Other licenses (i.e. IP Security and L2TP) may be additionally required depending on your network deployment and implementation.

Provides seamless mobility to mobile subscribers as they roam between WiLAN and 3G cellular access networks. This type of inter-technology roaming is ordinarily not possible as wireline access networks do not include SGSNs to permit inter-SGSN call hand-offs with cellular access networks.

The Cisco Session Persistence Solution maintains consistent user identities and application transparency for your mobile subscribers as they roam across bearer access networks. This is accomplished through the integration of Home Agent (HA) and GGSN functionality on the wireless access gateway in the packet network and the use of standards-based protocols such as Mobile IP and Mobile IP NAT Traversal. The solution also includes Session Persistence client software that runs on dual-mode WiFi/GPRS/EDGE and/or UMTS/W-CDMA access devices including cellular phones and laptop computers with wireless data cards.

The Session Persistence client is designed to permit Mobile IP tunneling over the applicable underlying network including cellular access connections and cable or XDSL broadband access networks. When the user is attached to a WiFi access network, the Session Persistence client utilizes a Mobile IP Co-located Care of Address Foreign Agent Service (CCoA FA) and establishes a MIP tunnel to the HA service in the platform. This scenario is completely transparent to the GGSN service that operates in the same system. The Mobile IP protocol requires a publicly addressable FA service; however, this is a problem when the mobile subscriber is located behind a NAT firewall. In this case, the NAT firewall has no way of maintaining state to associate the public NATed address with the private address assigned to the user by local DHCP server. Mobile IP NAT Traversal solves this problem by establishing a UDP/IP tunnel between the subscriber access device and Home Agent. The NAT firewall uses the UDP port address to build state for the subscriber session. During this Mobile IP transaction, the HA establishes a mobility binding record for the subscriber session.

When the subscriber roams to a 3GPP cellular access network, it uses the IP address from normal PDP IP context establishment as its new Mobile IP Care of Address to refresh the mobility binding record at the Home Agent. For reduced latency between access hand-offs, it is also possible to utilize a permanent 'always-on' PDP IP context with the IP address maintained in the MIP session persistence client. In this scenario, the mobile access device only needs to re-establish the dormant RAB wireless connection with the 3GPP access network prior to transmitting a new Mobile IP registration.

The system also enables network-provisioned VPNs for Session Persistence applications by permitting use of overlapping address pools on the HA and using various tunneling protocols including IPSEC, Layer 2 Tunneling Protocol (L2TP) and Ethernet IEEE 802.1Q VLANs for separation of subscriber traffic. This application may be further augmented by additional features such as 800 RADIUS Server Groups to permit use of enterprise controlled AAA servers and custom dictionaries.

Session Recovery Support

The Session Recovery feature provides seamless failover and reconstruction of subscriber session information in the event of a hardware or software fault within the system preventing a fully connected user session from being disconnected.

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), wherein they perform no processing, 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.

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

The additional hardware resources required for session recovery include a standby System Processor Card (SPC) and a standby packet processing card.

There are two modes for Session Recovery.

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

IMPORTANT: For more information on this feature, refer *Session Revocery* chapter in *System Enhanced Feature Configuration Guide*.

Traffic Policing and Rate Limiting

Allows the operator to proportion the network and support Service-level Agreements (SLAs) for customers.

The Traffic-Policing/Shaping feature enables configuring and enforcing bandwidth limitations on individual PDP contexts of a particular 3GPP traffic class. Values for traffic classes are defined in 3GPP TS 23.107 and are negotiated with the SGSN during PDP context activation using the values configured for the APN on the GGSN. Configuration and enforcement is done independently on the downlink and the uplink directions for each of the 3GPP traffic classes. Configuration is on a per-APN basis, but may be overridden for individual subscribers or subscriber tiers during RADIUS authentication/authorization.

A Token Bucket Algorithm (a modified trTCM, as specified in RFC2698) is used to implement the Traffic-Policing feature. The algorithm measures the following criteria when determining how to mark a packet.

- **Committed Data Rate (CDR)**: The guaranteed rate (in bits per second) at which packets may be transmitted/received for the subscriber during the sampling interval.
- **Peak Data Rate (PDR)**: The maximum rate (in bits per second) that packets may be transmitted/received for the subscriber during the sampling interval.
- **Burst-size**: The maximum number of bytes that may be transmitted/received for the subscriber during the sampling interval for both committed (CBS) and peak (PBS) rate conditions. This represents the maximum number of tokens that can be placed in the subscriber's "bucket". Note that the committed burst size (CBS) equals the peak burst size (PBS) for each subscriber.

Tokens are removed from the subscriber's bucket based on the size of the packets being transmitted/received. Every time a packet arrives, the system determines how many tokens need to be added (returned) to a subscriber's CBS (and PBS) bucket. This value is derived by computing the product of the time difference between incoming packets and the CDR (or PDR). The computed value is then added to the tokens remaining in the subscriber's CBS (or PBS) bucket. The total number of tokens can not be greater than the configured burst-size. If the total number of tokens is greater than the burst-size, the number is set to equal the burst-size. After passing through the Token Bucket Algorithm, the packet is internally classified with a color, as follows:

- There are not enough tokens in the PBS bucket to allow a packet to pass, then the packet is considered to be in violation and is marked "red" and the violation counter is incremented by one.
- There are enough tokens in the PBS bucket to allow a packet to pass, but not in the CBS "bucket", then the packet is considered to be in excess and is marked "yellow", the PBS bucket is decremented by the packet size, and the exceed counter is incremented by one.
- There are more tokens present in the CBS bucket than the size of the packet, then the packet is considered as conforming and is marked "green" and the CBS and PBS buckets are decremented by the packet size.

The APN on the GGSN can be configured with actions to take for red and yellow packets. Any of the following actions may be specified:

- **Drop**: The offending packet is discarded.
- **Transmit**: The offending packet is passed.
- **Lower the IP Precedence**: The packet's ToS octet is set to "0", thus downgrading it to Best Effort, prior to passing the packet.
- **Buffer the Packet**: The packet stored in buffer memory and transmitted to subscriber once traffic flow comes in allowed bandwidth.

Different actions may be specified for red and yellow, as well as for uplink and downlink directions and different 3GPP traffic classes.

IMPORTANT: For more information on this feature, refer *Traffic Policing and Shaping* chapter in *System Enhanced Feature Configuration Guide*.

Web Element Management System

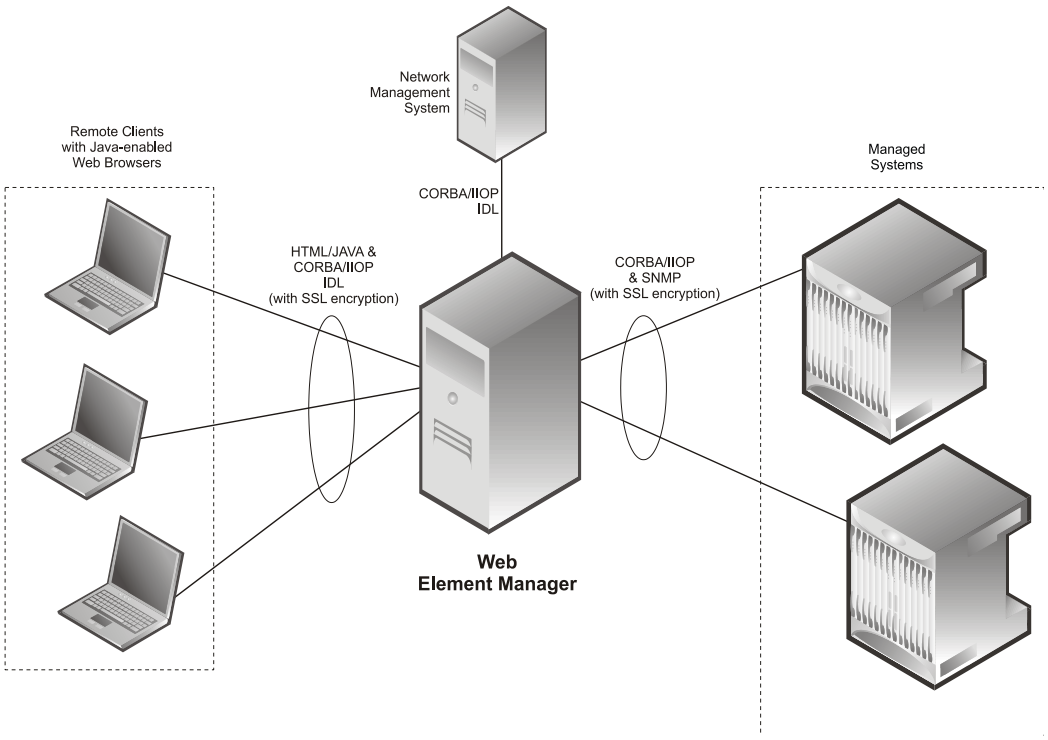
Provides a Graphical User Interface (GUI) for performing Fault, Configuration, Accounting, Performance, and Security (FCAPS) management of the ASR 5000.

The Web Element Manager is a Common Object Request Broker Architecture (CORBA)-based application that provides complete Fault, Configuration, Accounting, Performance, and Security (FCAPS) management capability for the system.

For maximum flexibility and scalability, the Web Element Manager application implements a client-server architecture. This architecture allows remote clients with Java-enabled web browsers to manage one or more systems via the server component which implements the CORBA interfaces. The server component is fully compatible with the fault-tolerant Sun® Solaris® operating system.

The following figure demonstrates various interfaces between the Cisco Web Element Manager and other network components.

Figure 9. Web Element Manager Network Interfaces



IMPORTANT: For more information on on WEM support, refer *WEM Installation and Administration Guide*.

How GGSN Works

This section provides information on the function of the GGSN in a GPRS/UMTS network and presents call procedure flows for different stages of session setup.

The following topics and procedure flows are included:

- PDP Context Processing
- Dynamic IP Address Assignment
- Subscriber Session Call Flows

PDP Context Processing

PDP context processing is based on the APN that the subscriber is attempting to access. Templates for all of the possible APNs that subscribers will be accessing must be configured within the system. Up to 1024 APNs can be configured on the system.

Each APN template consists of parameters pertaining to how PDP contexts are processed such as the following:

- **Type**: The system supports IPv4, IPv6, and PPP PDP contexts.
- **Accounting protocol**: Support is provided for using either the GTPP or Remote Authentication Dial-In User Service (RADIUS) protocols. In addition, an option is provided to disable accounting if desired.
- **Authentication protocol**: Support is provided for using any of the following:
  - Challenge Handshake Authentication Protocol (CHAP)
  - Microsoft CHAP (MSCHAP)
  - Password Authentication Protocol (PAP)
  - Mobile Station Identity (MSID)-based authentication

In addition, an option is provided to disable authentication if desired.

- **Charging characteristics**: Each APN template can be configured to either accept the charging characteristics it receives from the SGSN for a PDP context or use it's own characteristics.
- **IP address allocation method**: IP addresses for PDP contexts can be assigned using one of the following methods:
  - **Statically**: The APN template can be configured to provide support for MS-requested static IP addresses. Additionally, a static address can be configured in a subscriber's profile on an authentication server and allocated upon successful authentication.

IMPORTANT: Static IP addresses configured in subscriber profiles must also be part of a static IP address pool configured locally on the system.

  - **Dynamically** :The APN template can be configured to dynamically assign an IP address from locally configured address pools or via a Dynamic Host Control Protocol (DHCP) server. Additional information on dynamic address assignment can be found in the *Dynamic IP Address Assignment* section that follows.

- **Selection mode**: The MS's right to access the APN can be either verified or unverified. For verified access, the SGSN specifies the APN that should be used. For unverified access, the APN can be specified by either the SGSN or the MS.
- **Timeout**: Absolute and idle session timeout values specify the amount of time that an MS can remain connected.
- **Mobile IP configuration**: Mobile IP requirements, HA address, and other related parameters are configured in the APN template.
- **Proxy Mobile IP support**: Mobile IP support can be enabled for all subscribers facilitated by the APN. Alternatively, it can be enabled for individual subscribers via parameters in their RADIUS or local-user profiles.
- **Quality of Service**: Parameters pertaining to QoS feature support such as for Dynamic Renegotiation, Traffic Policing, and DSCP traffic class.

A total of 11 PDP contexts are supported per subscriber. These could be all 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 come up.

Dynamic IP Address Assignment

IP addresses for PDP contexts can either be static—an IP address is permanently assigned to the MS—or dynamic—an IP address is temporarily assigned to the MS for the duration of the PDP context.

As previously described in the *PDP Context Processing* section of this chapter, the method by which IP addresses are assigned to a PDP context is configured on an APN-by-APN basis. Each APN template dictates whether it will support static or dynamic addresses. If dynamic addressing is supported, the following methods can be implemented:

- **Local pools:** The system supports the configuration of public or private IP address pools. Addresses can be allocated from these pools as follows:
  - **Public pools:** Provided that dynamic assignment is supported, a parameter in the APN configuration mode specifies the name of the local public address pool to use for PDP contexts facilitated by the APN.
  - **Private pools:** Provided that dynamic assignment is supported, the name of the local private pool can be specified in the subscriber's profile. The receipt of a valid private pool name will override the APN's use of addresses from public pools.
- **Dynamic Host Control Protocol (DHCP):** The system can be configured to use DHCP PDP context address assignment using either of the following mechanisms:
  - **DHCP-proxy**: The system acts as a proxy for client (MS) and initiates the DHCP Discovery Request on behalf of client (MS). Once it receives an allocated IP address from DHCP server in response to

DHCP Discovery Request, it assigns the received IP address to the MS. This allocated address must be matched with the an address configured in an IP address pool on the system. This complete procedure is not visible to MS.

- **DHCP-relay**: The system acts as a relay for client (MS) and forwards the DHCP Discovery Request received from client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS.

In addition to the above methods, IP addresses for subscriber Mobile IP sessions are also dynamically assigned by the subscriber's home network upon registration. The GGSN/FA, in turn, provide the assigned address to the mobile station.

Subscriber Session Call Flows

This section provides information on how GPRS/UMTS subscriber data sessions are processed by the system GGSN. The following data session scenarios are provided:

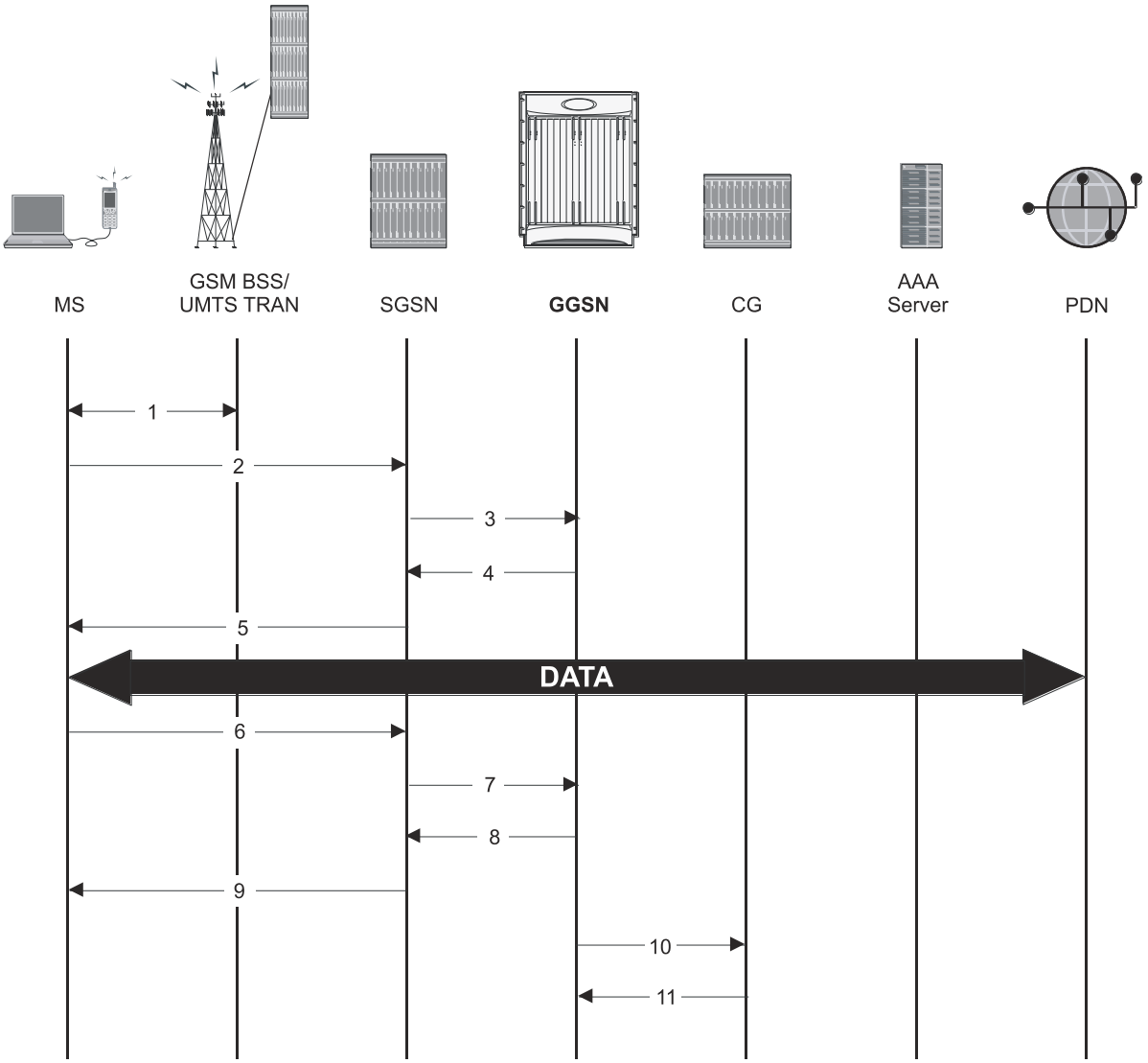
- **Transparent IP:** The subscriber is provided basic access to a PDN without the GGSN authenticating the subscriber. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Non-transparent IP**: The GGSN provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Network-initiated**: An IP Packet Data Unit (PDU) is received by the GGSN from the PDN for a specific subscriber. If configured to support network-initiated sessions, the GGSN, will initiate the process of paging the MS and establishing a PDP context.
- **PPP Direct Access**: The GGSN terminates the subscriber's PPP session and provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Virtual Dialup Access**: The GGSN functions as an LAC, encapsulates subscriber packets using L2TP, and tunnels them directly to an LNS for processing.
- **Corporate IP VPN Connectivity**: Similar to the Virtual Dialup Access model, however, the GGSN is configured to tunnel subscriber packets to a corporate server using IP-in-IP.
- **Mobile IP**: Subscriber traffic is routed to their home network via a tunnel between the GGSN/FA and an HA. The subscriber's IP PDP context is assigned an IP address from the HA.
- **Proxy Mobile IP**: Provides a mobility solution for subscribers whose Mobile Nodes (MNs) do not support the Mobile IP protocol. The GGSN/FA proxy the Mobile IP tunnel with the HA on behalf of the MS. The subscriber receives an IP address from their home network. As the subscriber roams through the network, the IP address is maintained providing the subscriber with the opportunity to use IP applications that require seamless mobility such as transferring files.
- **IPv6 Stateless Address Autoconfiguration**: The mobile station may select any value for the interface identifier portion of the address. The only exception is the interface identifier for the link-local address used by the mobile station. This interface identifier is assigned by the GGSN to avoid any conflict between the mobile station link-local address and the GGSN address. The mobile station uses the interface ID assigned by the GGSN during stateless address auto-configuration procedure (e.g., during the initial router advertisement messages). Once this is over, the mobile can select any interface ID for further communication as long as it does not conflict with the GGSN's interface ID (that the mobile would learn through router advertisement messages from the GGSN).

Additionally, this section also provides information about the process used by the system to dynamically assign IP addresses to the MS.

Transparent Session IP Call Flow

The following figure and the text that follows describe the call flow for a successful transparent data session.

Figure 10. Transparent IP Session Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.

2. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
3. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and Tunnel Endpoint Identifier (TEID, if the PDP Address was static).
4. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

   If the MS required the dynamic assignment of an IP address (i.e., the PDP Address received from the mobile was null), the GGSN will assign one. The IP address assignment methods supported by the system GGSN are described in the *Dynamic IP Address Assignment* section of this guide.

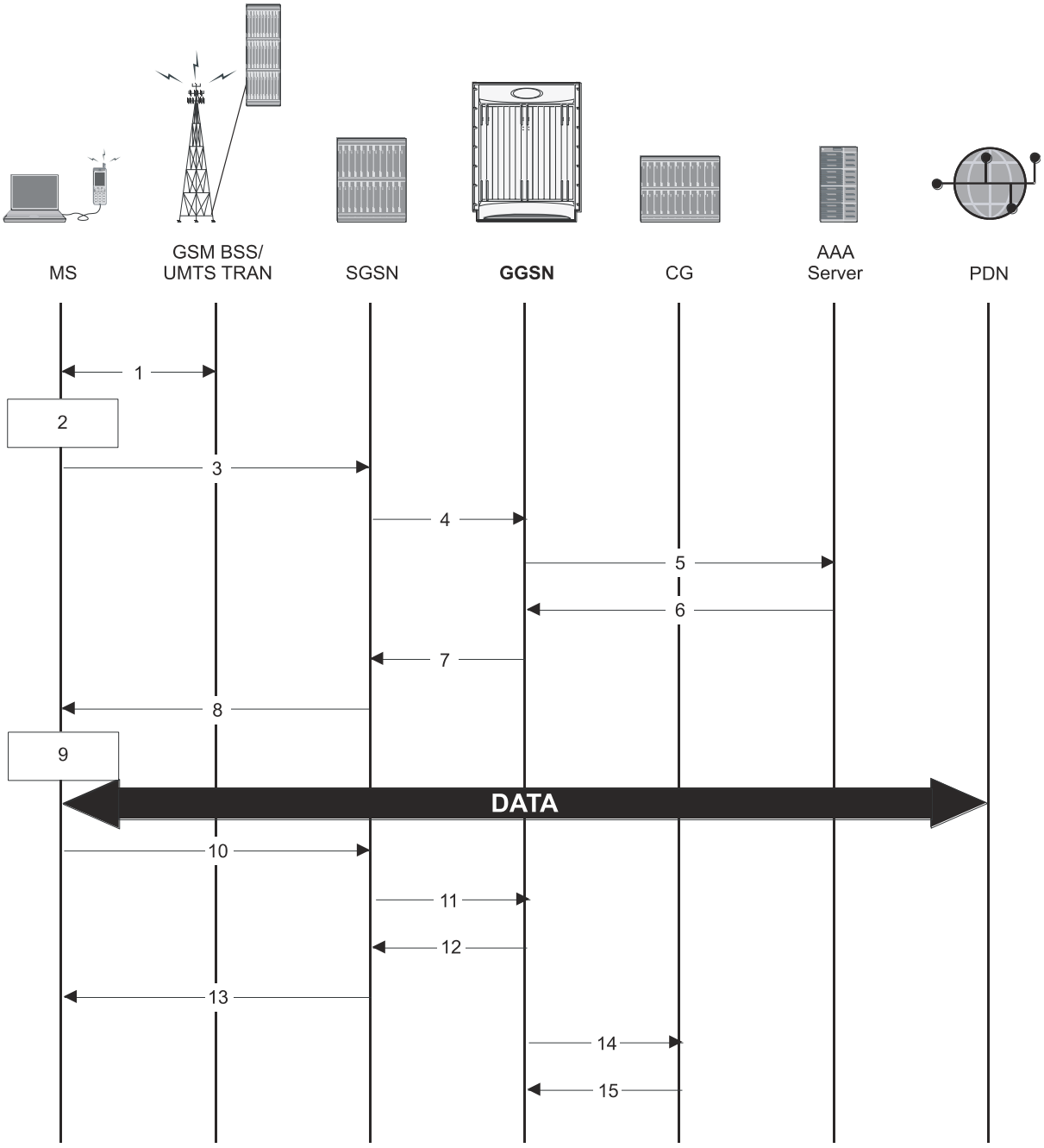
   The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.
5. The SGSN returns an Activate PDP Context Accept response to the MS.

   The MS can now send and receive data to or from the PDN until the session is closed or times out. The MS can initiate multiple PDP contexts if desired and supported by the system. Each additional PDP context can share the same IP address or use alternatives.
6. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
7. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
8. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
9. The SGSN returns a Deactivate PDP Context Accept message to the MS.
10. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
11. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Non-Transparent IP Session Call Flow

The following figure and the text that follows describe the call flow for a successful non-transparent data session.

Figure 11. Non-Transparent IP Session Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The Terminal Equipment (TE) aspect of the MS sends AT commands to the Mobile Terminal (MT) aspect of the MS to place it into PPP mode.

   The Link Control Protocol (LCP is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication

Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.

Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.

3. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
4. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and tunnel endpoint identifier (TEID, if the PDP Address was static).
5. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

   From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, how an IP address should be assigned if using dynamic allocation, and how to route the session.

   If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to an AAA server.

   If the MS required the dynamic assignment of an IP address (i.e., the PDP Address received from the mobile was null), the GGSN will assign one. The IP address assignment methods supported by the system GGSN are described in the *Dynamic IP Address Assignment* section of this chapter.
6. If the GGSN authenticated the subscriber to an AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication.
7. The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.
8. The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
9. The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message.

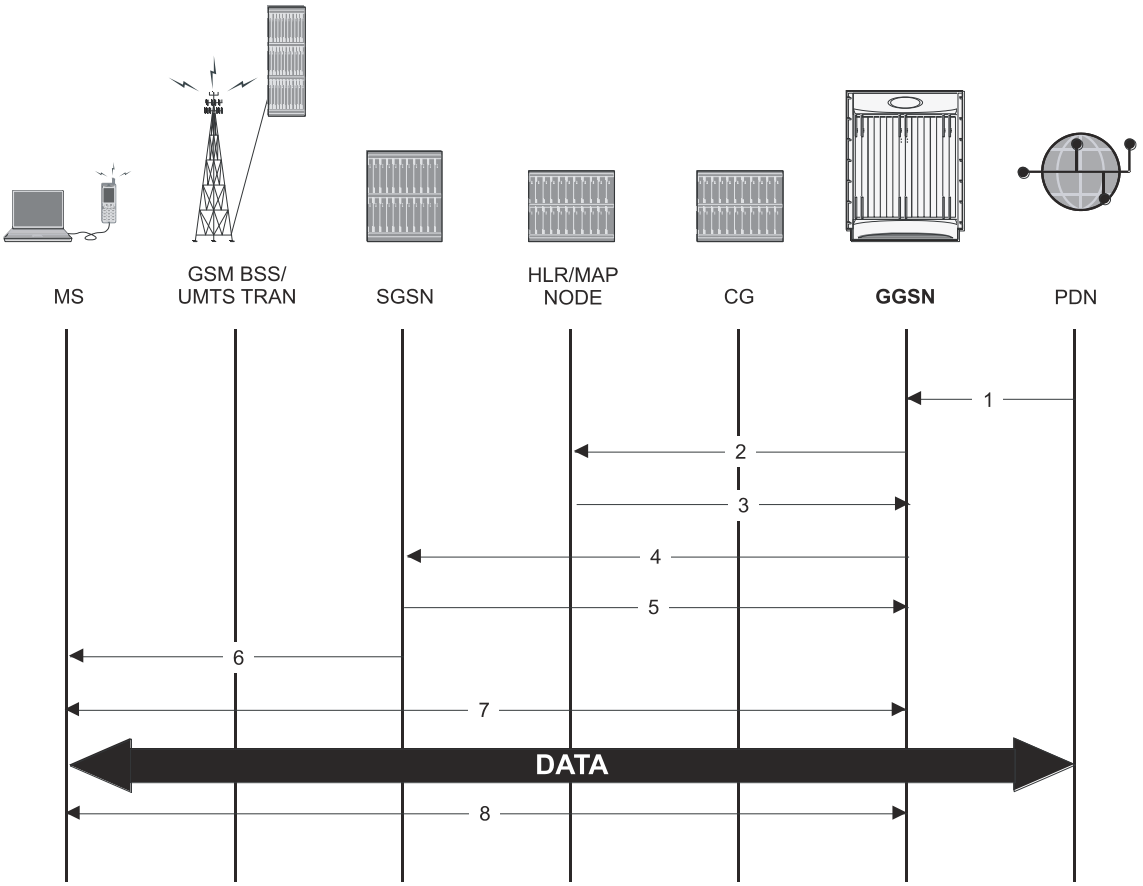
   The MS can now send and receive data to or from the PDN until the session is closed or times out. The MS can initiate multiple PDP contexts if desired and supported by the system. Each additional PDP context can share the same IP address or use alternatives.
10. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
11. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).
12. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
13. The SGSN returns a Deactivate PDP Context Accept message to the MS.

14. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
15. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Network-Initiated Session Call Flow

The following figure and the text that follows describe the call flow for a successful network-initiated data session.

Figure 12. Network-initiated Session Call Flow



1. An IP Packet Data Unit (PDU) is received by the GGSN from the PDN. The GGSN determines if it is configured to support network-initiated sessions. If not, it will discard the packet. If so, it will begin the Network-Requested PDP Context Activation procedure.
2. The GGSN may issue a Send Routing Information for GPRS request to the HLR to determine if the MS is reachable. The message includes the MS's International Mobile Subscriber Identity (IMSI).

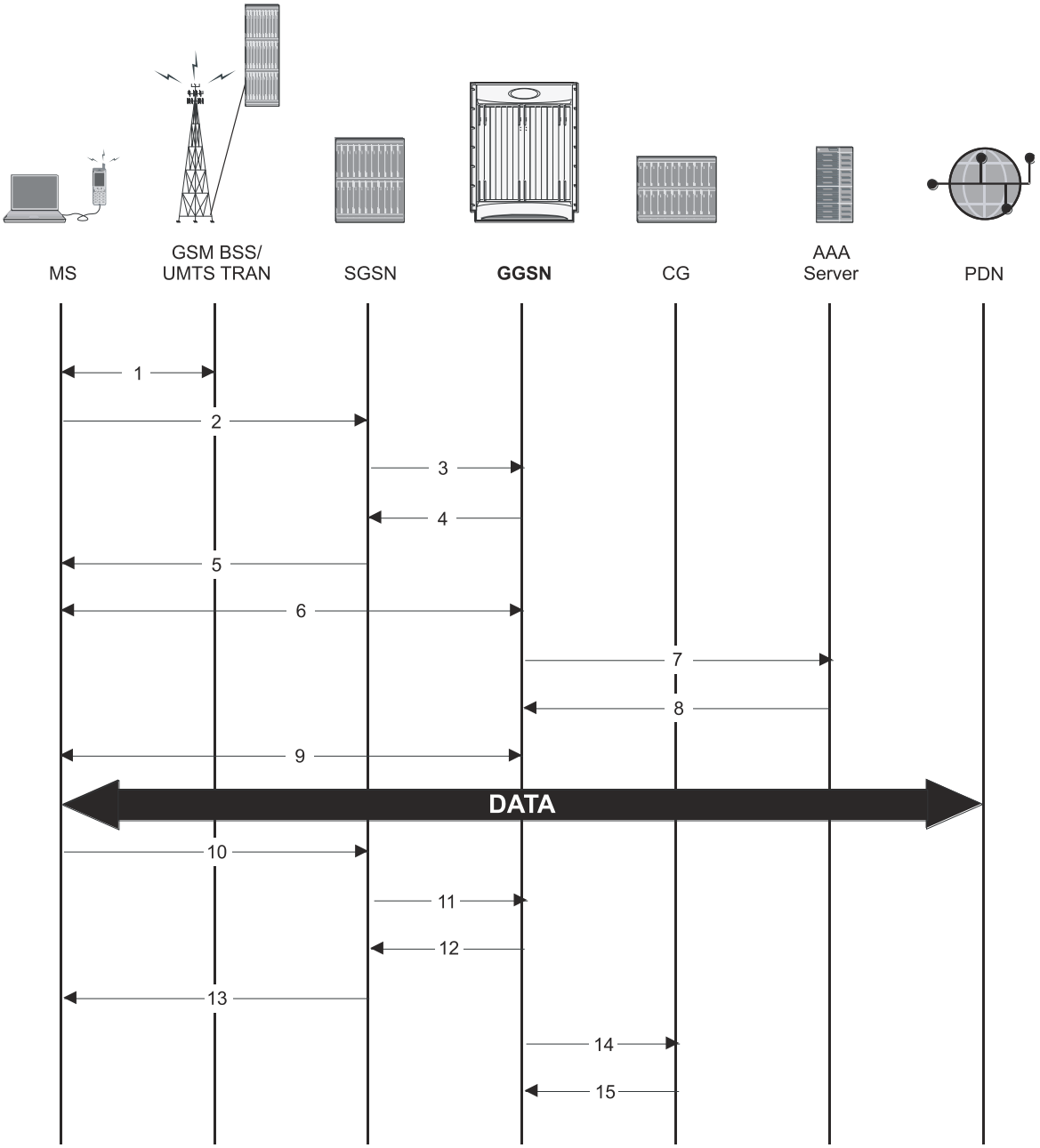
3. If the MS is reachable, the HLR returns a Send Routing Information for GPRS Ack containing the address of the SGSN currently associated with the MS's IMSI.
4. The GGSN sends a PDU Notification Request message to the SGSN address supplied by the HLR. This message contains the IMSI, PDP Type, PDP Address, and APN associated with the session.
5. The SGSN sends a PDU Notification Response to the GGSN indicating that it will attempt to page the MS requesting that it activate the PDP address indicated in the GGSN's request.
6. The SGSN sends a Request PDP Context Activation message to the MS containing the information supplied by the GGSN.
7. The MS begins the PDP Context Activation procedure as described in *step 2* through *step 5* of the *Transparent Session IP Call Flow* section of this chapter.

   Upon PDP context establishment, the MS can send and receive data to or from the PDN until the session is closed or times out.
8. The MS can terminate the data session at any time. To terminate the session, the MS begins the PDP Context De-Activation procedure as described in *step 6* through *step 11* of the *Transparent Session IP Call Flow* section of this chapter.

PPP Direct Access Call Flow

The following figure and the text that follows describe the call flow for a successful PPP Direct Access data session.

Figure 13. PPP Direct Access Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.

3. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, and charging characteristics.
4. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. It determines that the PDP context type is PPP and based on the APN, what authentication protocol to use and how to perform IP address assignment.

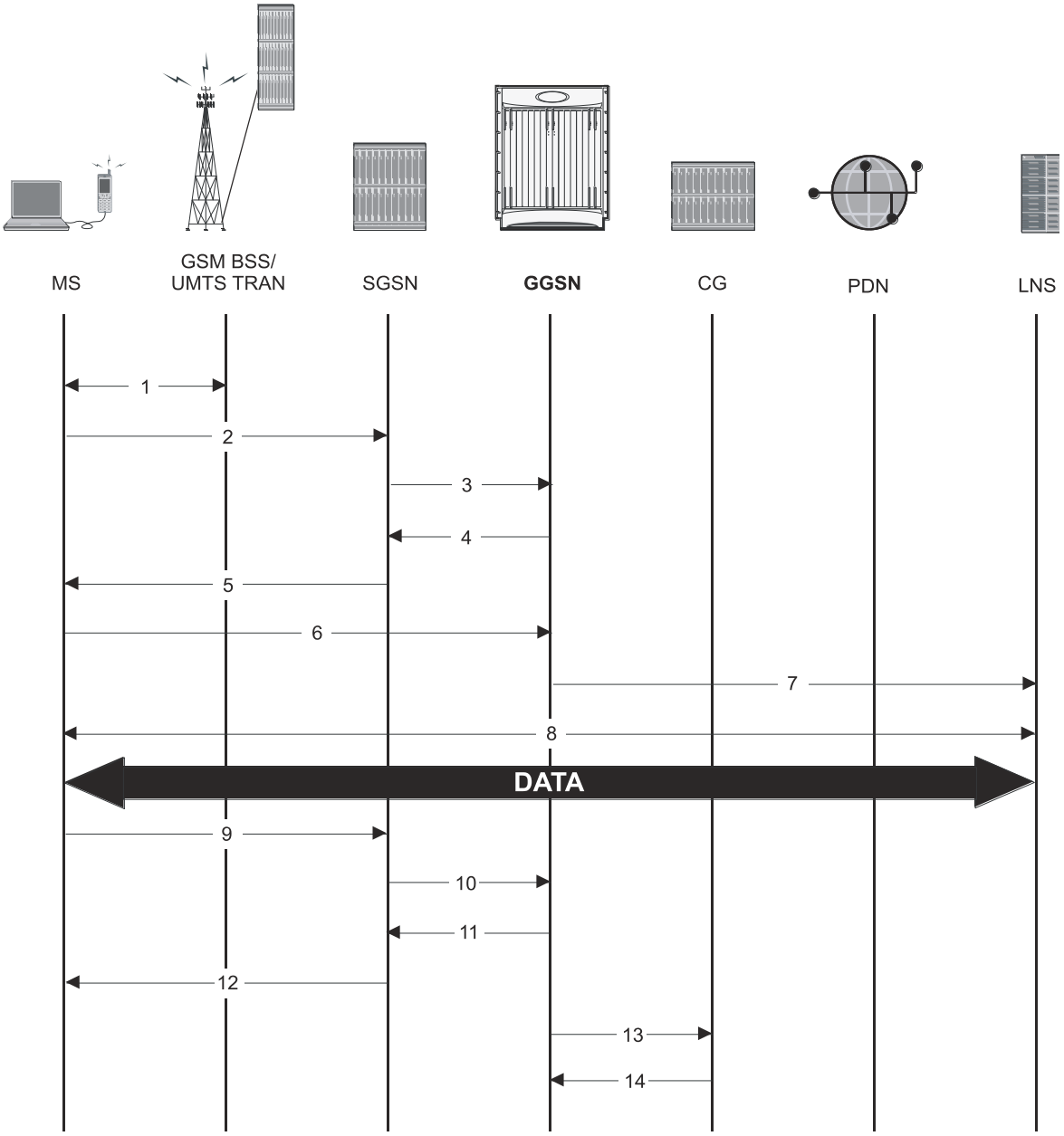
   The GGSN replies with an affirmative Create PDP Context Response using GTPC.
5. The SGSN returns an Activate PDP Context Accept response to the MS.
6. The MS and the GGSN negotiate PPP.
7. The GGSN forwards authentication information received from the MS as part of PPP negotiation to the AAA server in the form of an Access-Request.
8. The AAA server authenticates the MS and sends an Access-Accept message to the GGSN.
9. The GGSN assigns an IP address to the MS and completes the PPP negotiation process. More information about IP addressing for PDP contexts is located in the *PDP Context Processing* and *Dynamic IP Address Assignment* sections of this chapter.

   Once the PPP negotiation process is complete, the MS can send and receive data.
10. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
11. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
12. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
13. The SGSN returns a Deactivate PDP Context Accept message to the MS.
14. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
15. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Virtual Dialup Access Call Flow

The following figure and the text that follows describe the call flow for a successful VPN Dialup Access data session.

Figure 14. Virtual Dialup Access Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.
3. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The

recipient GGSN is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, and charging characteristics.

4. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. It determines the PDP context type and based on the APN, what authentication protocol to use and how to perform IP address assignment.

   The GGSN replies with an affirmative Create PDP Context Response using GTPC.

5. The SGSN returns an Activate PDP Context Accept response to the MS.
6. The MS sends packets which are received by the GGSN.
7. The GGSN encapsulates the packets from the MS using L2TP and tunnels them to the LNS.
8. The LNS terminates the tunnel and un-encapsulates the packets.

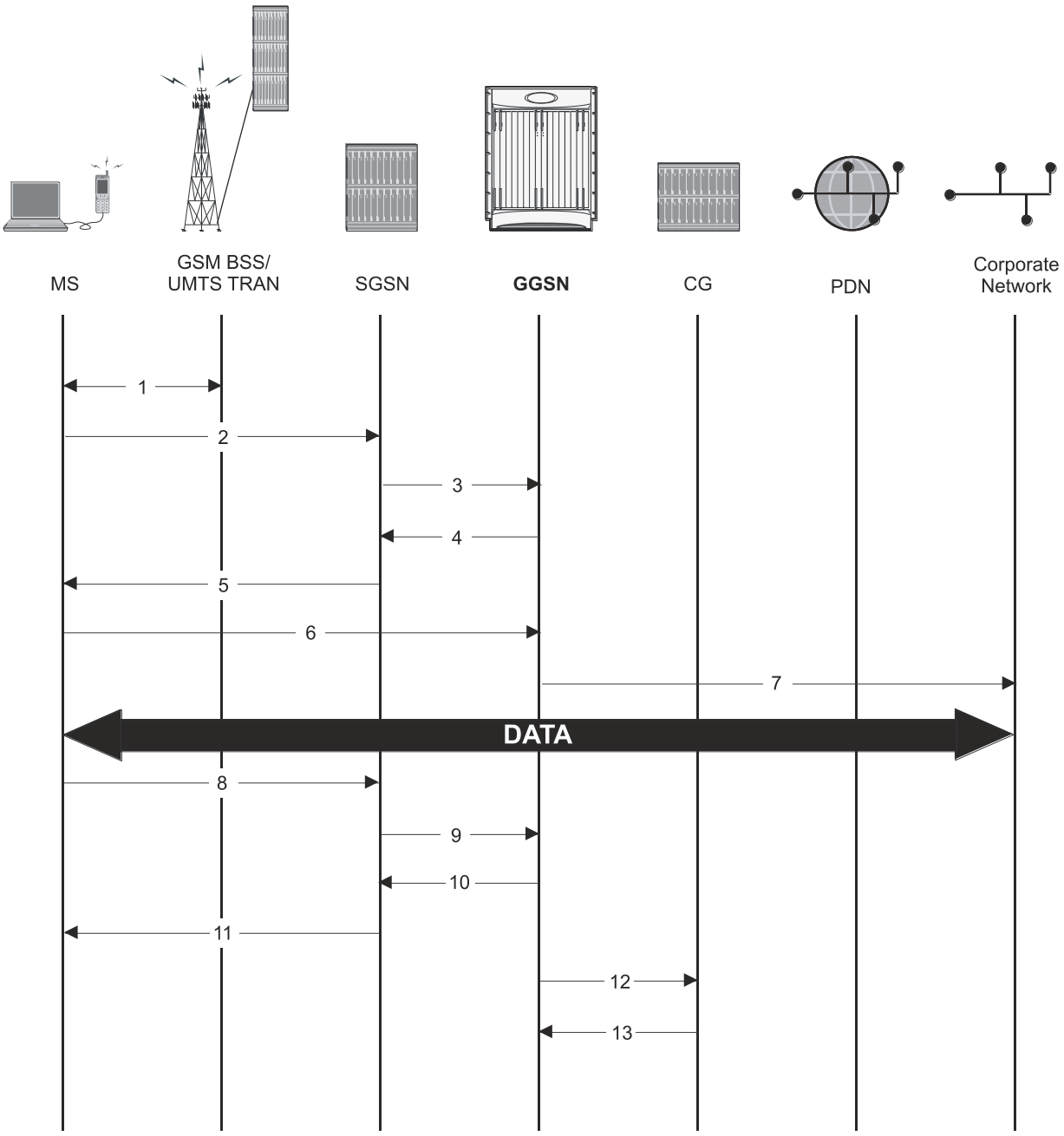
   The MS can send and receive data over the L2TP tunnel facilitated by the GGSN.

9. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
10. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
11. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
12. The SGSN returns a Deactivate PDP Context Accept message to the MS.
13. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
14. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Corporate IP VPN Connectivity Call Flow

The following figure and the text that follows describe the call flow for a successful Corporate IP Connectivity data session.

Figure 15. Corporate IP VPN Connectivity Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.

3. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, and charging characteristics.
4. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session. It determines the PDP context type and based on the APN, what authentication protocol to use and how to perform IP address assignment.

   If the MS required the dynamic assignment of an IP address (i.e., the PDP Address received from the mobile was null), the GGSN will assign one. The IP address assignment methods supported by the system GGSN are described in the *Dynamic IP Address Assignment* section of this chapter.

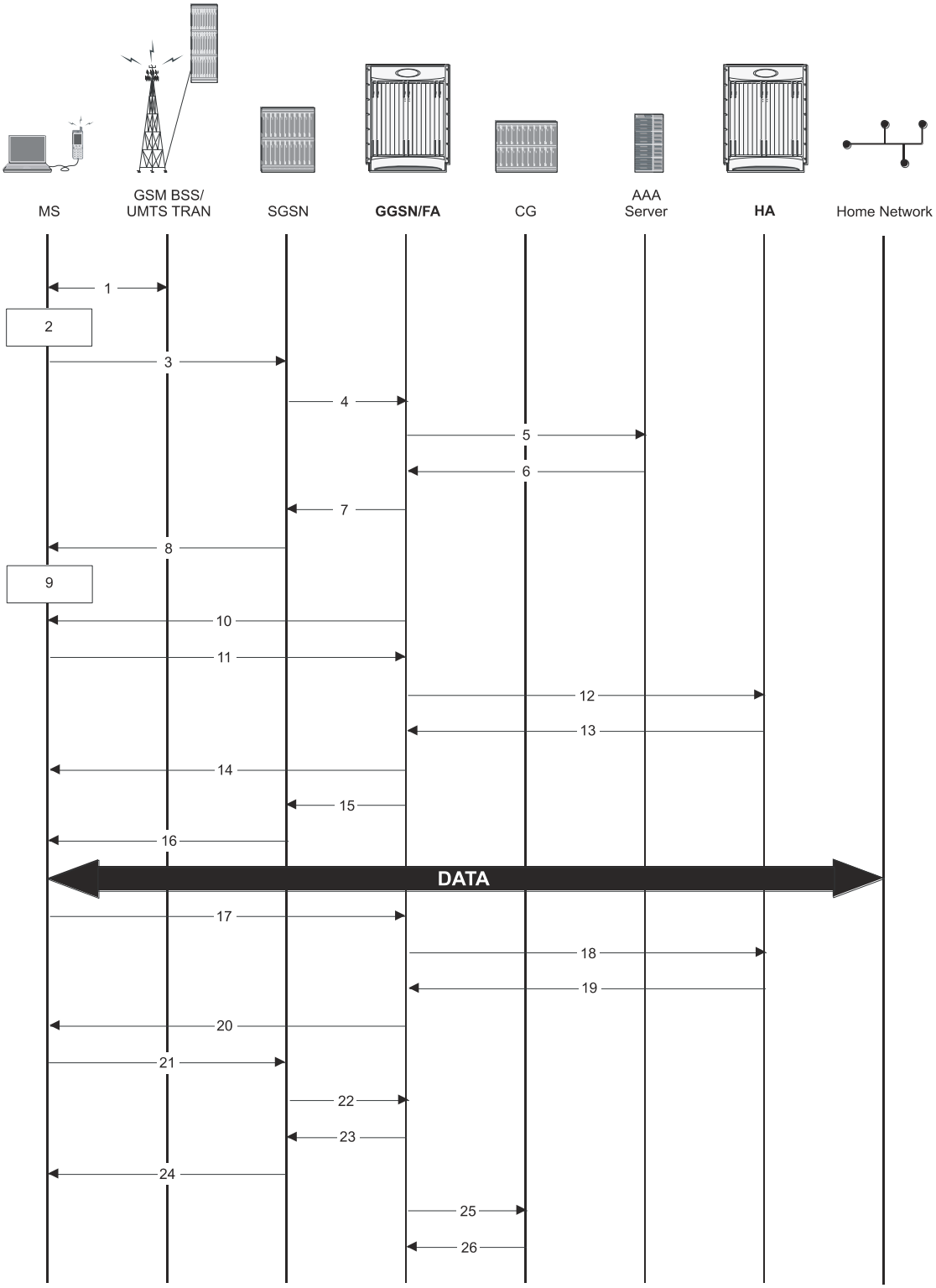
   The GGSN replies with an affirmative Create PDP Context Response using GTPC.
5. The SGSN returns an Activate PDP Context Accept response to the MS.
6. The MS sends IP packets which are received by the GGSN.
7. The GGSN encapsulates the IP packets from the MS using IP-in-IP and tunnels them to the subscriber's corporate network.

   All data sent and received by the MS over the IP-in-IP tunnel facilitated by the GGSN.
8. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.
9. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
10. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN. If the PDP context was the last associated with a particular dynamically assigned PDP Address, the GGSN will re-claim the IP address for use by subsequent PDP contexts.
11. The SGSN returns a Deactivate PDP Context Accept message to the MS.
12. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
13. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Mobile IP Call Flow

The following figure and the text that follows describe the call flow for a successful Corporate IP Connectivity data session.

Figure 16. Mobile IP Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.
2. The Terminal Equipment (TE) aspect of the MS sends AT commands to the Mobile Terminal (MT) aspect of the MS to place it into PPP mode.

   The Link Control Protocol (LCP is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.

   Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP home address to use or request that one be dynamically assigned.
3. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.

   Note that regardless of whether or not the MS has a static address or is requesting a dynamic address, the "Requested PDP Address" field is omitted from the request when using Mobile IP.
4. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, Requested PDP con, APN, charging characteristics, and Tunnel Endpoint Identifier (TEID).
5. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

   From the APN specified in the message, the GGSN determines how to handle the PDP context including whether or not Mobile IP should be used.

   If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to an AAA server.
6. If the GGSN authenticated the subscriber to an AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication.
7. The GGSN replies to the SGSN with a PDP Context Response using GTPC. The response will contain information elements such as the PDP Address, and PDP configuration options specified by the GGSN. Note that for Mobile IP, the GGSN returns a PDP Address of 0.0.0.0 indicating that it will be reset with a Home address after the PDP context activation procedure.
8. The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.
9. The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message. This ends the PPP mode between the MT and TE components of the MS.

   Data can now be transmitted between the MS and the GGSN.
10. The FA component of the GGSN sends an Agent Advertisement message to the MS. The message contains the FA parameters needed by the mobile such as one or more card-of addresses. The message is sent as an IP limited broadcast message (i.e. destination address 255.255.255.255), however only on the requesting MS's TEID to avoid broadcast over the radio interface.
11. The MS sends a Mobile IP Registration request to the GGSN/FA. This message includes either the MS's static home address or it can request a temporary address by sending 0.0.0.0 as its home address. Additionally, the request must always include the Network Access Identifier (NAI) in a Mobile-Node-NAI Extension.

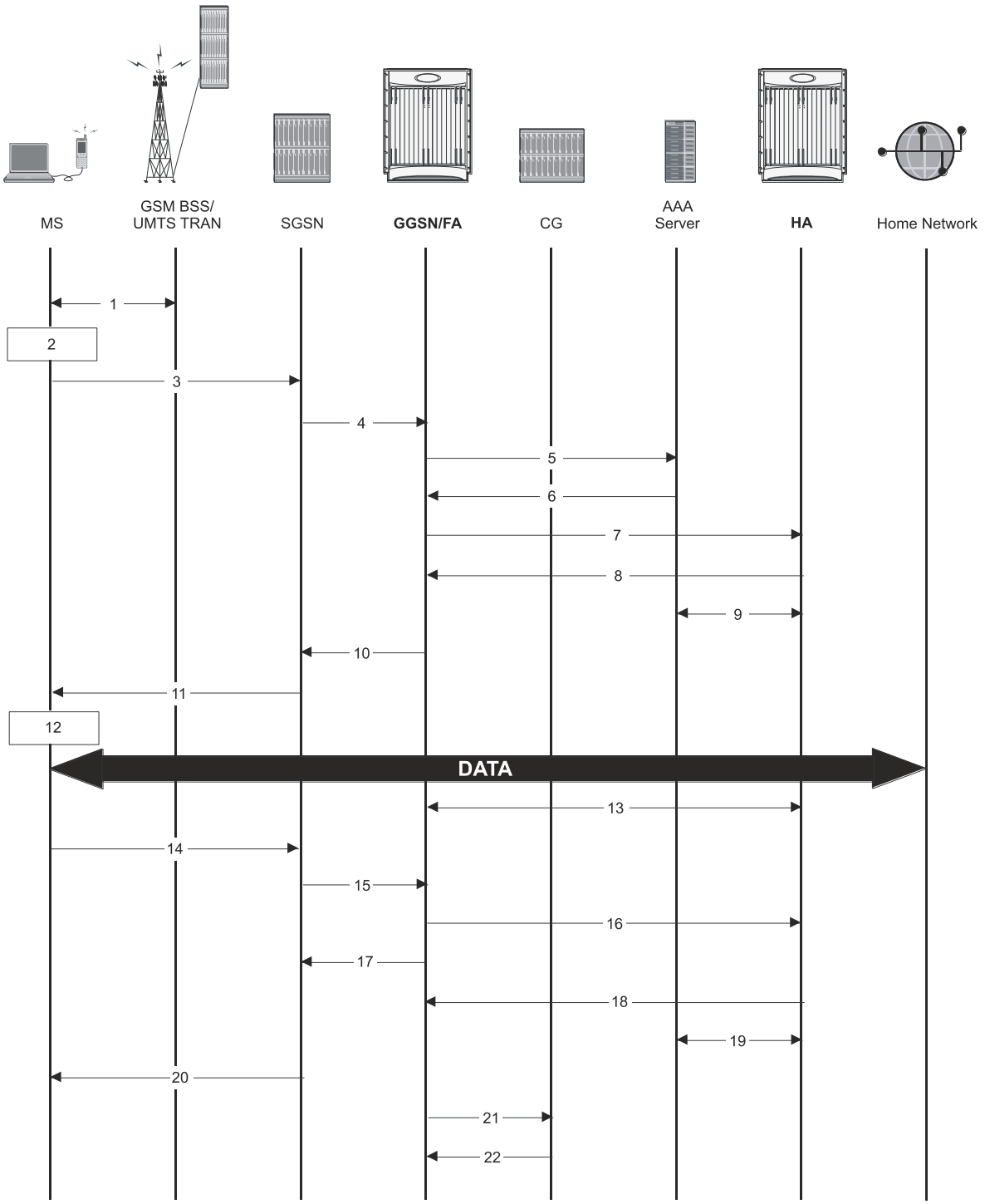
12. The FA forwards the registration request from the MS to the HA while the MS's home address or NAI and TEID are stored by the GGSN.
13. The HA sends a registration response to the FA containing the address assigned to the MS.
14. The FA extracts the home address assigned to the MS by the HA from the response and the GGSN updates the associated PDP context. The FA then forwards it to the MS (identified by either the home address or the NAI and TEID).
15. The GGSN issues a PDP context modification procedure to the SGSN in order to update the PDP address for the MS.
16. The SGSN forwards the PDP context modification message to the MS.

    The MS can now send and receive data to or from their home network until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.
17. The MS can terminate the Mobile IP data session at any time. To terminate the Mobile IP session, the MS sends a Registration Request message to the GGSN/FA with a requested lifetime of 0.
18. The FA component forwards the request to the HA.
19. The HA sends a Registration Reply to the FA accepting the request.
20. The GGSN/FA forwards the response to the MN.
21. The MS sends a Deactivate PDP Context Request message that is received by the SGSN.
22. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context.
23. The GGSN removes the PDP context from memory and returns a Delete PDP Context Response message to the SGSN.
24. The SGSN returns a Deactivate PDP Context Accept message to the MS.
25. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.
26. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

Proxy Mobile IP Call Flows

The following figure and the text that follows describe a sample successful Proxy Mobile IP session setup call flow in which the MS receives its IP address from the HA.

Figure 17. HA Assigned IP Address Proxy Mobile IP Call Flow



1. The Mobile Station (MS) goes through the process of attaching itself to the GPRS/UMTS network.

2. The Terminal Equipment (TE) aspect of the MS sends AT commands to the Mobile Terminal (MT) aspect of the MS to place it into PPP mode.

   The Link Control Protocol (LCP is then used to configure the Maximum-Receive Unit size and the authentication protocol (Challenge-Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), or none). If CHAP or PAP is used, the TE will authenticate itself to the MT, which, in turn, stores the authentication information.

   Upon successful authentication, the TE sends an Internet Protocol Control Protocol (IPCP) Configure-Request message to the MT. The message will either contain a static IP address to use or request that one be dynamically assigned.

3. The MS sends an Activate PDP Context Request message that is received by an SGSN. The message contains information about the subscriber such as the Network layer Service Access Point Identifier (NSAPI), PDP Type, PDP Address, Access Point Name (APN), Quality of Service (QoS) requested, and PDP configuration options.

4. The SGSN authenticates the request message and sends a Create PDP Context Request message to a GGSN using the GPRS Tunneling Protocol (GTPC, "C" indicates the control signaling aspect of the protocol). The recipient GGSN is selected based on either the request of the MS or is automatically selected by the SGSN. The message consists of various information elements including: PDP Type, PDP Address, APN, charging characteristics, and Tunnel Endpoint Identifier (TEID, if the PDP Address was static).

5. The GGSN determines if it can facilitate the session (in terms of memory or CPU resources, configuration, etc.) and creates a new entry in its PDP context list and provides a Charging ID for the session.

   From the APN specified in the message, the GGSN determines whether or not the subscriber is to be authenticated, if Proxy Mobile IP is to be supported for the subscriber, and if so, the IP address of the HA to contact.

   Note that Proxy Mobile IP support can also be determined by attributes in the user's profile. Attributes in the user's profile supersede APN settings.

   If authentication is required, the GGSN attempts to authenticate the subscriber locally against profiles stored in memory or send a RADIUS Access-Request message to an AAA server.

6. If the GGSN authenticated the subscriber to an AAA server, the AAA server responds with a RADIUS Access-Accept message indicating successful authentication and any attributes for handling the subscriber PDP context.

7. If Proxy Mobile IP support was either enabled in the APN or in the subscriber's profile, the GGSN/FA forwards a Proxy Mobile IP Registration Request message to the specified HA. The message includes such things as the MS's home address, the IP address of the FA (the care-of-address), and the FA-HA extension (Security Parameter Index (SPI)).

8. The HA responds with a Proxy Mobile IP Registration Response. The response includes an IP address from one of its locally configured pools to assign to the MS (its Home Address). The HA also creates a Mobile Binding Record (MBR) for the subscriber session.

9. The HA sends a RADIUS Accounting Start request to the AAA server which the AAA server responds to.

10. The GGSN replies with an affirmative Create PDP Context Response using GTPC. The response will contain information elements such as the PDP Address representing either the static address requested by the MS or the address assigned by the GGSN, the TEID used to reference PDP Address, and PDP configuration options specified by the GGSN.

11. The SGSN returns an Activate PDP Context Accept message to the MS. The message includes response to the configuration parameters sent in the initial request.

12. The MT, will respond to the TE's IPCP Config-request with an IPCP Config-Ack message.

The MS can now send and receive data to or from the PDN until the session is closed or times out. Note that for Mobile IP, only one PDP context is supported for the MS.

13. The FA periodically sends Proxy Mobile IP Registration Request Renewal messages to the HA. The HA sends responses for each request.

14. The MS can terminate the data session at any time. To terminate the session, the MS sends a Deactivate PDP Context Request message that is received by the SGSN.

15. The SGSN sends a Delete PDP Context Request message to the GGSN facilitating the data session. The message includes the information elements necessary to identify the PDP context (i.e., TEID, and NSAPI).

16. The GGSN removes the PDP context from memory and the FA sends a Proxy Mobile IP Deregistration Request message to the HA.

17. The GGSN returns a Delete PDP Context Response message to the SGSN.

18. The HA replies to the FA with a Proxy Mobile IP Deregistration Request Response.

19. The HA sends a RADIUS Accounting Stop request to the AAA server which the AAA server responds to.

20. The SGSN returns a Deactivate PDP Context Accept message to the MS.

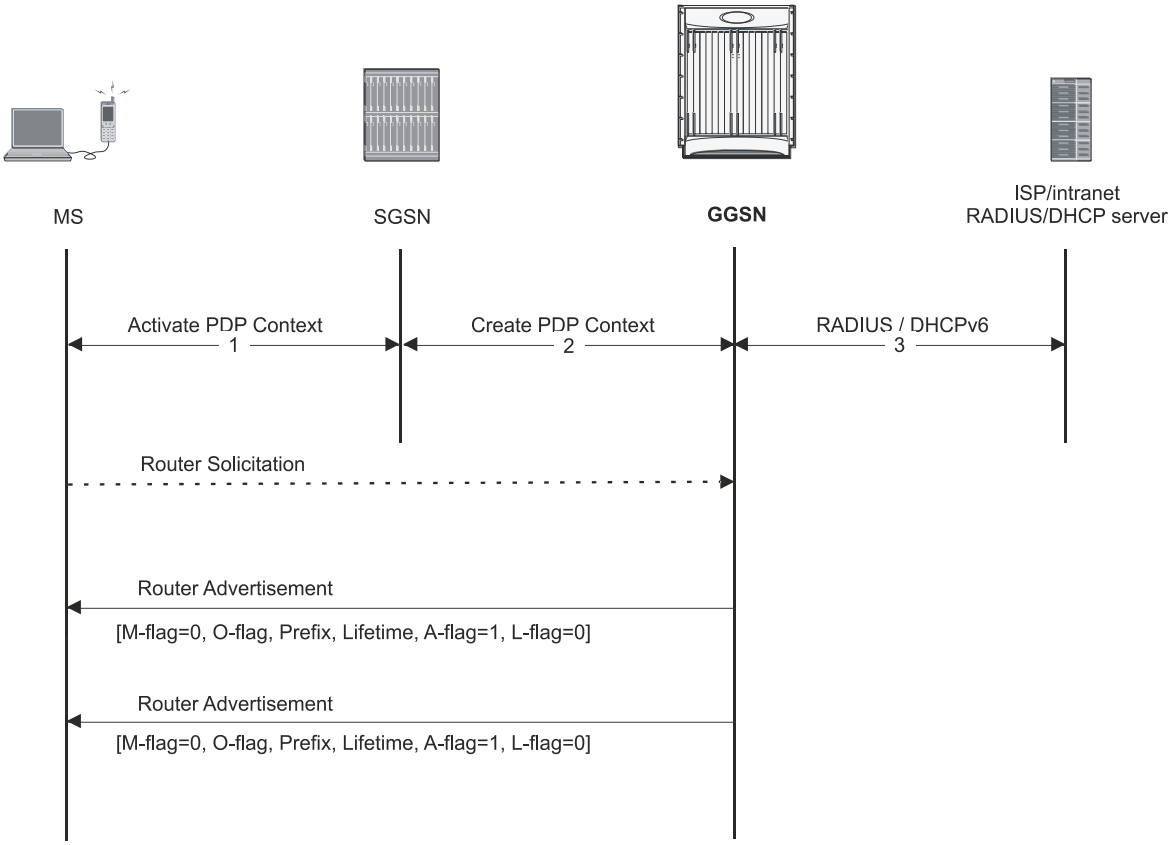
21. The GGSN delivers the GGSN Charging Detail Records (G-CDRs) to a Charging Gateway (CG) using GTP Prime (GTPP). Note that, though not shown in this example, the GGSN could optionally be configured to send partial CDRs while the PDP context is active.

22. For each accounting message received from the GGSN, the CG responds with an acknowledgement.

IPv6 Stateless Address Autoconfiguration Flows

The following figure and the text that follows describe a sample IPv6 stateless address auto configuration session setup call flow in which the MS receives its IP address from the RADIUS DHCP server.

Figure 18. IPv6 Stateless Address Autoconfiguration Flow



1. The MS uses the IPv6 interface identifier provided by the GGSN to create its IPv6 link-local unicast address. Before the MS communicates with other hosts or mobile stations on the intranet/ISP, the MS must obtain an IPv6 global or site-local unicast address.
2. After the GGSN sends a create PDP context response message to the SGSN, it starts sending router advertisements periodically on the new MS-GGSN link established by the PDP context.
3. When creating a global or site-local unicast address, the MS may use the interface identifier received during the PDP context activation or it generates a new interface identifier. There is no restriction on the value of the interface identifier of the global or site-local unicast address, since the prefix is unique.

Supported Standards

The GGSN complies with the following standards for 3GPP wireless data services.

- 3GPP References
- IETF References
- Object Management Group (OMG) Standards

3GPP References

- 3GPP TS 09.60 v7.10.0 (2001-09): 3rd Generation Partnership project; Technical Specification Group Core Network; General Packet Radio Services (GPRS); GPRS Tunneling Protocol (GTP) across the Gn and Gp Interface (Release 1998) for backward compatibility with GTPv0
- 3GPP TS 23.060 v7.6.0 (2007-9): 3rd Generation Partnership project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description (Release 1999) as an additional reference for GPRS/UMTS procedures
- 3GPP TS 23.107 v7.1.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; QoS Concept and Architecture
- 3GPP TS 23.203 V7.7.0 (2006-08): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Policy and charging control architecture (Release 7)
- 3GPP TS 23.246 v7.4.0 (2007-09): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description (Release 7)
- 3GPP TS 24.008 v7.11.0 (2001-06): Mobile radio interface layer 3 specification; Core Network Protocols- Stage 3 (Release 1999) as an additional reference for GPRS/UMTS procedures
- 3GPP TS 29.060 v7.9.0 (2008-09): 3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Services (GPRS); GRPS Tunneling Protocol (GTP) across the Gn and Gp Interface (Release 4) for the Core GTP Functionality
- 3GPP TS 29.061 v7.7.0 (2008-09): 3rd Generation Partnership Project; Technical Specification Group Core Network; Packet Domain; Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)
- 3GPP 29.212 v7.6.0 (2008-09) 3rd Generation Partnership Project, Technical Specification Group Core Network and Terminals; Policy and Charging Control over Gx reference point (Release 7)
- 3GPP TS 29.213 V7.5.0 (2005-08): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control signalling flows and QoS parameter mapping; (Release 7)
- 3GPP TR 29.846 6.0.0 (2004-09) 3rd Generation Partnership Project, Technical Specification Group Core Networks; Multimedia Broadcast/Multicast Service (MBMS); CN1 procedure description (Release 6)

- 3GPP TS 32.015 v3.12.0 (2003-12): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Telecommunication Management; Charging management; Call and event data for the Packet Switched (PS) domain (Release 1999) for support of Charging on GGSN
- 3GPP TS 32.215 v5.9.0 (2005-06): 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Telecommunication Management; Charging Management; Charging data description for the Packet Switched (PS) domain (Release 5)
- 3GPP 32.251 v7.5.1 (2007-10) 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Packet Switched (PS) domain charging (Release 7)
- 3GPP TS 32.298 v7.4.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description
- 3GPP TS 32.299 v7.7.0 (2007-10): 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Telecommunication management; Charging management; Diameter charging applications (Release 7)
- 3GPP TS 32.403 V7.1.0: Technical Specification Performance measurements - UMTS and combined UMTS/GSM
- 3GPP TS 33.106 V7.0.1 (2001-06): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful Interception requirements (Release 7)
- 3GPP TS 33.107 V7.7.0 (2007-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions (Release 7)

IETF References

- RFC-768, User Datagram Protocol (UPD), August 1980
- RFC-791, Internet Protocol (IP), September 1982
- RFC-793, Transmission Control Protocol (TCP), September 1981
- RFC-894, A Standard for the Transmission of IP Datagrams over Ethernet Networks, April 1984
- RFC-1089, SNMP over Ethernet, February 1989
- RFC-1144, Compressing TCP/IP headers for low-speed serial links, February 1990
- RFC-1155, Structure & identification of management information for TCP/IP-based internets, May 1990
- RFC-1157, Simple Network Management Protocol (SNMP) Version 1, May 1990
- RFC-1212, Concise MIB Definitions, March 1991
- RFC-1213, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, March 1991
- RFC-1215, A Convention for Defining Traps for use with the SNMP, March 1991
- RFC-1224, Techniques for managing asynchronously generated alerts, May 1991
- RFC-1256, ICMP Router Discovery Messages, September 1991
- RFC-1305, Network Time Protocol (Version 3) Specification, Implementation and Analysis, March 1992

- RFC-1332, The PPP Internet Protocol Control Protocol (IPCP), May 1992
- RFC-1398, Definitions of Managed Objects for the Ethernet-Like Interface Types, January 1993
- RFC-1418, SNMP over OSI, March 1993
- RFC-1570, PPP LCP Extensions, January 1994
- RFC-1643, Definitions of Managed Objects for the Ethernet-like Interface Types, July 1994
- RFC-1661, The Point to Point Protocol (PPP), July 1994
- RFC-1662, PPP in HDLC-like Framing, July 1994
- RFC-1701, Generic Routing Encapsulation (GRE), October 1994
- RFC-1850, OSPF Version 2 Management Information Base, November 1995
- RFC-1901, Introduction to Community-based SNMPv2, January 1996
- RFC-1902, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1903, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1904, Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1905, Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1906, Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1907, Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2), January 1996
- RFC-1908, Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework, January 1996
- RFC-1918, Address Allocation for Private Internets, February 1996
- RFC-1919, Classical versus Transparent IP Proxies, March 1996
- RFC-1962, The PPP Compression Control Protocol (CCP), June 1996
- RFC-1974, PPP STAC LZS Compression Protocol, August 1996
- RFC-2002, IP Mobility Support, May 1995
- RFC-2003, IP Encapsulation within IP, October 1996
- RFC-2004, Minimal Encapsulation within IP, October 1996
- RFC-2005, Applicability Statement for IP Mobility Support, October 1996
- RFC-2118, Microsoft Point-to-Point Compression (MPPC) Protocol, March 1997
- RFC 2131, Dynamic Host Configuration Protocol
- RFC 2132, DHCP Options and BOOTP Vendor Extensions
- RFC-2136, Dynamic Updates in the Domain Name System (DNS UPDATE)
- RFC-2211, Specification of the Controlled-Load Network Element Service
- RFC-2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999
- RFC-2290, Mobile-IPv4 Configuration Option for PPP IPCP, February 1998

- RFC-2328, OSPF Version 2, April 1998
- RFC-2344, Reverse Tunneling for Mobile IP, May 1998
- RFC-2394, IP Payload Compression Using DEFLATE, December 1998
- RFC 2401, Security Architecture for the Internet Protocol
- RFC 2402, IP Authentication Header (AH)
- RFC 2406, IP Encapsulating Security Payload (ESP)
- RFC 2409, The Internet Key Exchange (IKE)
- RFC-2460, Internet Protocol Version 6 (IPv6)
- RFC-2461, Neighbor Discovery for IPv6
- RFC-2462, IPv6 Stateless Address Autoconfiguration
- RFC-2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998
- RFC-2475, An Architecture for Differentiated Services, December 1998
- RFC-2484, PPP LCP Internationalization Configuration Option, January 1999
- RFC-2486, The Network Access Identifier (NAI), January 1999
- RFC-2571, An Architecture for Describing SNMP Management Frameworks, April 1999
- RFC-2572, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), April 1999
- RFC-2573, SNMP Applications, April 1999
- RFC-2574, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), April 1999
- RFC-2597, Assured Forwarding PHB Group, June 1999
- RFC-2598, Expedited Forwarding PHB, June 1999
- RFC-2618, RADIUS Authentication Client MIB, June 1999
- RFC-2620, RADIUS Accounting Client MIB, June 1999
- RFC-2661, Layer Two Tunneling Protocol “L2TP”, August 1999
- RFC-2697, A Single Rate Three Color Marker, September 1999
- RFC-2698, A Two Rate Three Color Marker, September 1999
- RFC-2784, Generic Routing Encapsulation (GRE) - March 2000, IETF
- RFC-2794, Mobile IP Network Access Identifier Extension for IPv4, March 2000
- RFC-2809, Implementation of L2TP Compulsory Tunneling via RADIUS, April 2000
- RFC-2845, Secret Key Transaction Authentication for DNS (TSIG), May 2000
- RFC-2865, Remote Authentication Dial In User Service (RADIUS), June 2000
- RFC-2866, RADIUS Accounting, June 2000
- RFC-2867, RADIUS Accounting Modifications for Tunnel Protocol Support, June 2000
- RFC-2868, RADIUS Attributes for Tunnel Protocol Support, June 2000
- RFC-2869, RADIUS Extensions, June 2000
- RFC-3007, Secure Domain Name System (DNS) Dynamic Update, November 2000

- RFC-3012, Mobile IPv4 Challenge/Response Extensions, November 2000
- RFC-3056, Connection of IPv6 Domains via IPv4 Clouds, February 2001
- RFC-3101 OSPF-NSSA Option, January 2003
- RFC-3143, Known HTTP Proxy/Caching Problems, June 2001
- RFC-3193, Securing L2TP using IPSEC, November 2001
- RFC-3314, Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards, September 2002
- RFC-3316, Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts, April 2003
- RFC-3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers, February 2004
- RFC-3543, Registration Revocation in Mobile IPv4, August 2003
- RFC 3588, Diameter Base Protocol, September 2003
- RFC 4006, Diameter Credit-Control Application, August 2005
- Draft, Route Optimization in Mobile IP
- Draft, Generalized Key Distribution Extensions for Mobile IP
- Draft, AAA Keys for Mobile IP

Object Management Group (OMG) Standards

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

Chapter 2
Understanding the Service Operation

The system provides wireless carriers with a flexible solution for providing Gateway GPRS Support Node (GGSN) functionality for GPRS or UMTS networks.

The system functioning as a GGSN is capable of supporting the following types of subscriber data sessions:

- **Transparent IP:** The subscriber is provided basic access to a packet data network (PDN) without the GGSN authenticating the subscriber. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Non-transparent IP:** The GGSN provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Network-initiated:** An IP Packet Data Unit (PDP) is received by the GGSN from the PDN for a specific subscriber. If configured to support network-initiated sessions, the GGSN, will initiate the process of paging the MS and establishing a PDP context.
- **PPP Direct Access:** The GGSN terminates the subscribers PPP session and provides subscriber authentication services for the data session. Either a static or dynamic IP address can be assigned to the MS in this scenario.
- **Virtual Dialup Access:** The GGSN functions as an LAC, encapsulates subscriber packets using L2TP, and tunnels them directly to an LNS for processing.
- **Corporate IP VPN Connectivity:** Similar to the Virtual Dialup Access model, however, the GGSN is configured to tunnel subscriber packets to a corporate server using a protocol such as IP-in-IP.

Prior to connecting to the command line interface (CLI) and beginning the system's configuration, there are important things to understand about how the system supports these applications. This chapter provides terminology and background information that must be considered before attempting to configure the system.

Terminology

This section defines some of the terms used in the chapters that follow.

Contexts

A context is a logical grouping or mapping of configuration parameters that pertain to various physical ports, logical IP interfaces, and services. A context can be thought of as a virtual private network (VPN).

The system supports the configuration of multiple contexts. Each is configured and operates independently from the others. Once a context has been created, administrative users can then configure services, logical IP interfaces, subscribers, etc.for that context. Administrative users would then bind the logical interfaces to physical ports.

Contexts can also be assigned domain aliases, wherein if a subscriber's domain name matches one of the configured alias names for that context, then that context is used.

Contexts on the system can be categorized as follows:

- **Source context:** Also referred to as the "ingress" context, this context provides the subscriber's point-of-entry in the system. It is also the context in which services are configured. For example, in a GPRS/UMTS network, the radio network containing the Service GPRS Support Nodes (SGSNs) would communicate with the system via Gn interfaces configured within the source context as part of the GGSN service.
- **Destination context:** Also referred to as the "egress" context, this context is where a subscriber is provided services (such as access to the Internet) as defined by access point name (APN) configuration templates. For example, the system's destination context would be configured with the interfaces facilitating subscriber data traffic to/from the Internet, a VPN, or other PDN.
- **Authentication context:** This context provides authentication functionality for subscriber PDP contexts and/or administrative user sessions and contains the policies and logical interfaces for communicating with Remote Authentication Dial In User Service (RADIUS) authentication servers.

For subscriber authentication, this functionality must be configured in the same system context as the APN template(s). Optionally, to simplify the configuration process, both subscriber RADIUS authentication functionality and APN templates can be configured in the destination context.

IMPORTANT: To ensure scalability, authentication functionality for subscriber sessions should not be configured in the local context.

For administrative users, authentication functionality can either be configured in the local context or be authenticated in the same context as subscribers.

- **Accounting context:** This context provides accounting functionality for subscriber PDP contexts and/or administrative user sessions.

The system context in which accounting functionality is configured depends on the protocol used. Accounting for subscriber PDP contexts can be performed using either the GPRS Tunneling Protocol Prime (GTPP) or RADIUS. Accounting for administrative user sessions is based on RADIUS.

When using GTPP, it is recommended that accounting functionality be configured in a system source context along with the GGSN service.

When using RADIUS for subscriber accounting, it must be configured in the same context as RADIUS authentication. To simplify the configuration process, RADIUS-based authentication and accounting can be configured in a destination context as long as the APN templates are configured there as well.

RADIUS-based accounting for administrative user sessions can either be configured in the local context or in the same context used for subscriber accounting.

IMPORTANT: To ensure scalability, accounting functionality for subscriber sessions should not be configured in the local context.

- **Local context:** This is the default context on the system used to provide out-of-band management functionality. The local context is described in the Command Line Reference.

Logical Interfaces

Prior to allowing the flow of user data, the port must be associated with a virtual circuit or tunnel called a logical interface. A logical interface within the system is defined as the logical assignment of a virtual router instance that provides higher-layer protocol transport, such as Layer 3 IP addressing. Interfaces are configured as part of the VPN context and are independent from the physical port that will be used to bridge the virtual interfaces to the network.

Logical interfaces are assigned to IP addresses and are bound to a specific port during the configuration process. Logical interfaces are also associated with services through bindings. Services are bound to an IP address that is configured for a particular logical interface. When associated, the interface takes on the characteristics of the functions enabled by the service. For example, if an interface is bound to a GGSN service, it will function as a Gn interface between the GGSN service and the SGSN. Services are defined later in this section.

There are several types of logical interfaces that must be configured to support the service as described below:

- **Gn:** This is the interface used by the GGSN to communicate with SGSNs on the same GPRS/UMTS Public Land Mobile Network (PLMN). This interface serves as both the signalling and data path for establishing and maintaining subscriber PDP contexts.

  The GGSN communicates with SGSNs on the PLMN using the GPRS Tunnelling Protocol (GTP). The signalling or control aspect of this protocol is referred to as the GTP Control Plane (GTPC) while the encapsulated user data traffic is referred to as the GTP User Plane (GTPU).

  One or more Gn interfaces can be configured per system context. Gn interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the four-port Quad Gig-E Line Card (QGLC) (ASR 5000 only).

- **Ga:** This is the interface used by the GGSN to communicate with the charging gateway (CG). The charging gateway is responsible for sending GGSN charging detail records (G-CDRs) received from the GGSN for each PDP context to the billing system.

  The GGSN communicates with the CGs on the PLMN using GTP Prime (GTPP).

One or more Ga interfaces can be configured per system context. Ga interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC (ASR 5000 only).

- **Gc:** This is the interface used by the GGSN to communicate with the Home Location Register (HLR) via a GTP-to-MAP (Mobile Application Part) protocol convertor. This interface is used for network initiated PDP contexts.

  For network initiated PDP contexts, the GGSN will communicate with the protocol convertor using GTP. The convertor, in turn, will communicate with the HLR using MAP over Signalling System 7 (SS7).

  One Gc interface can be configured per system context. Gc interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC (ASR 5000 only).

- **Gi:** This is the interface used by the GGSN to communicate with packet data networks (PDNs) external to the PLMN. Examples of PDNs are the Internet or corporate intranets.

  Additionally, inbound packets received on this interface could initiate a network requested PDP context if the intended MS is not currently connected.

  One or more Gi interfaces can be configured per system context. Gi interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC (ASR 5000 only).

- **Gp:** This is the interface used by the GGSN to communicate with GPRS support nodes (GSNs, e.g. GGSNs and/or SGSNs) on different PLMNs. Within the system, a single interface can serve as both a Gn and a Gp interface.

  One or more Gn/Gp interfaces can be configured per system context. Gp interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC (ASR 5000 only).

- **AAA:** This is the interface used by the GGSN to communicate with either an authentication or accounting server on the network using the Remote Authentication Dial In User Service (RADIUS) protocol.

  This is an optional interface that can be by the GGSN for subscriber PDP context authentication or accounting. AAA interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC (ASR 5000 only).

- **S6b**: This is an optional Diameter protocol-based interface over which the GGSN communicates with 3G AAA/HSS in LTE/SAE network for subscriber authorization.

  IMPORTANT: This interface is supported through license-enabled feature. For more information on this support, refer *Common Gateway Access Support* in guide.

- **DHCP:** This is the interface used by the GGSN to communicate with a Dynamic Host Control Protocol (DHCP) Server. The system can be configured to dynamically provide IP addresses for PDP contexts from the DHCP server.

  DHCP interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000 Line Cards or on the QGLC (ASR 5000 only).

Bindings

A binding is an association between “elements” within the system. There are two types of bindings: static and dynamic.

Static binding is accomplished through the configuration of the system. Static bindings are used to associate:

- A specific logical interface (configured within a particular context) to a physical port. Once the interface is bound to the physical port, traffic can flow through the context just as if it were any physically defined circuit. Static bindings support any encapsulation method over any interface and port type.
- A service to an IP address assigned to a logical interface within the same context. This allows the interface to take on the characteristics (i.e., support the protocols) required by the service. For example, a GGSN service bound to a logical interface will cause the logical interface to take on the characteristics of a Gn interface within a GPRS/UMTS network.

Dynamic binding associates a subscriber to a specific egress context based on the configuration of their profile or system parameters. This provides a higher degree of deployment flexibility as it allows a wireless carrier to support multiple services and facilitates seamless connections to multiple networks.

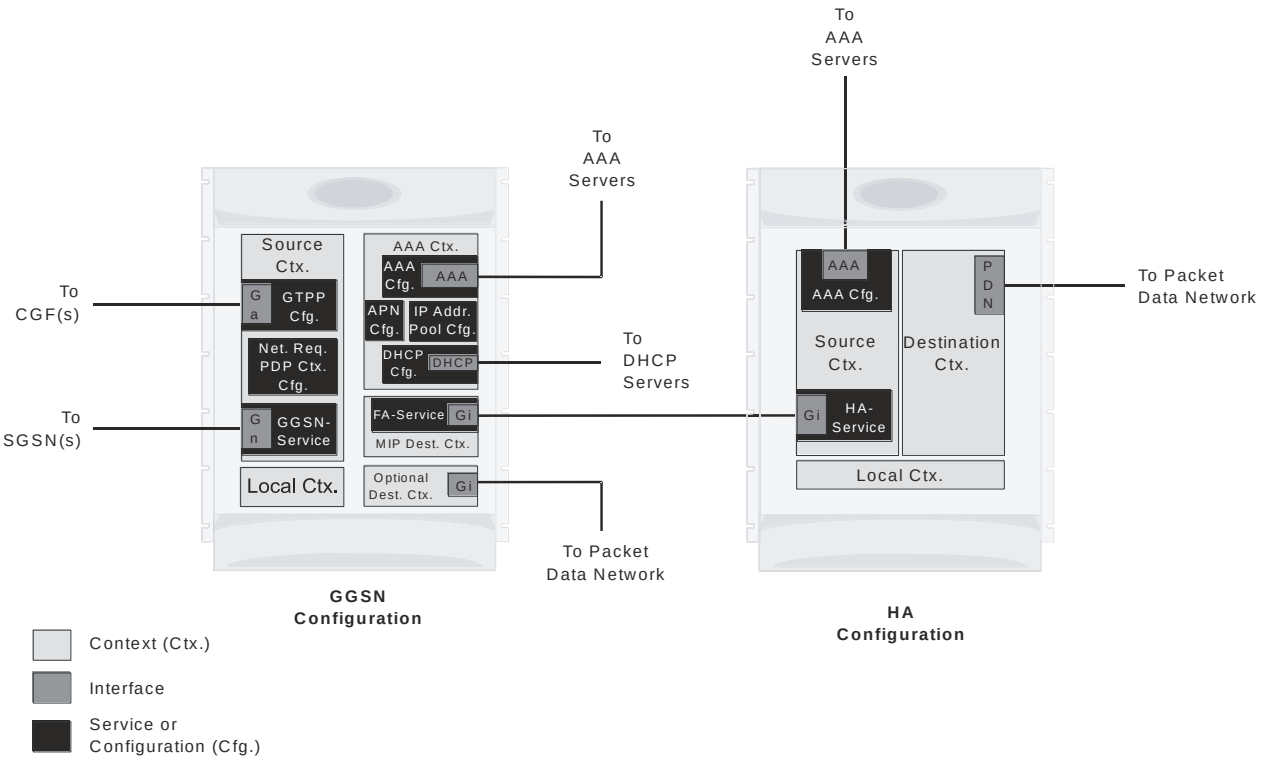
Services

Services are configured within a context and enable certain functionality. The following services can be configured on the system:

- **GGSN services:** GGSN services are configured to support both mobile-initiated and network-requested PDP contexts. The GGSN service must be bound to a logical interface within the same context. Once bound, the interface takes on the characteristics of a Gn interface. Multiple services can be bound to the same logical interface. Therefore, a single physical port can facilitate multiple Gn interfaces.
- **FA services**: FA services are configured to support Mobile IP and define FA functionality on the system.
- **LAC services:** LAC services are configured on the system to provide Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) functionality. LAC services can be configured and used within networks to provide secure tunneling to an L2TP network server (LNS) on a remote PDN.
- **DHCP services:** DHCP services are configured on a system to provide dynamic assignment of IP address to PDP contexts through the use of the Dynamic Host Configuration Protocol (DHCP).

Following figure illustrates the relationship between services, interfaces, and contexts within the system for GPRS/UMTS networks.

Figure 19. Service, Interface, and Context Relationship Within the System for GPRS/UMTS Networks



The source context used to service a subscriber session is the same as the context in which the GGSN service is configured. Each GGSN service is bound to an IP address in a source context. The SGSNs select which IP address to use, typically by using DNS. Once a subscriber has established a PDP context with a GGSN, the SGSNs continue to use that same PDP context and GGSN as the subscriber moves about the network.

Destination contexts are selected based on APN configuration. When the system receives a **Create PDP Context Request** message from the SGSN, it examines the APN that was provided. If the APN is not found on the system, the system rejects the request.

After the APN has been found, the system may choose a different APN based on the system's virtual APN configuration. In any event, a final APN is selected by the system

The system determines the destination context to use based on a parameter contained within the final APN configuration. If a valid destination context name is configured for this parameter, it is used. If the name is not valid, or if it is not configured, the system uses the context in which the APN is configured.

Once the system locates the context in which the APN is configured, it uses that context for subscriber authentication and RADIUS-based accounting (if enabled). Any parameters returned by the RADIUS server during the subscriber authentication/authorization override APN configuration parameters.

If GTPP-based accounting is enabled, the system uses the source context for accounting. That context may be overridden by configuring a different accounting context to use in the GGSN service configuration.

How the System Selects Contexts

This section provides details about the process that is used to determine which context to use for context-level administrative user and/or subscriber sessions. Understanding this process allows you to better plan your configuration in terms of how many contexts and interfaces need to be configured.

Context Selection for Subscriber Sessions

The context selection process for a subscriber session is more involved than that for the administrative users.

The source context used to service a subscriber session is the same as the context in which the GGSN service is configured. Each GGSN service is bound to an IP address in a source context. The SGSNs select which IP address to use, typically by using DNS. Once a subscriber has established a PDP context with a GGSN, the SGSNs continue to use that same PDP context and GGSN as the subscriber moves about the network.

Destination contexts are selected based on APN configuration. When the system receives a **Create PDP Context Request** message from the SGSN, it examines the APN that was provided. If the APN is not found on the system, the system rejects the request.

After the APN has been found, the system may choose a different APN based on the system's virtual APN configuration. In any event, a final APN is selected by the system

The system determines the destination context to use based on a parameter contained within the final APN configuration. If a valid destination context name is configured for this parameter, it is used. If the name is not valid, or if it is not configured, the system uses the context in which the APN is configured.

Once the system locates the context in which the APN is configured, it uses that context for subscriber authentication and RADIUS-based accounting (if enabled). Any parameters returned by the RADIUS server during the subscriber authentication/authorization override APN configuration parameters.

If GTPP-based accounting is enabled, the system uses the source context for accounting. That context may be overridden by configuring a different accounting context to use in the GGSN service configuration.

Chapter 3
GGSN Configuration Example

This chapter provides information for configuring the system to function as a Gateway GPRS Support Node (GGSN) in General Packet Radio Service (GPRS) or Universal Mobile Telecommunications System (UMTS) wireless data networks.

IMPORTANT: This chapter does not discuss the configuration of the local context. Information about the local context can be found in the *Command Line Interface Overview* chapter of the *System Administration Guide* and the *Command Line Interface Reference*.

The most simple configuration that can be implemented on the system to support GGSN functionality requires that two contexts (one source and one destination) be configured on the system as shown in the following figure.

The source context facilitates the following:

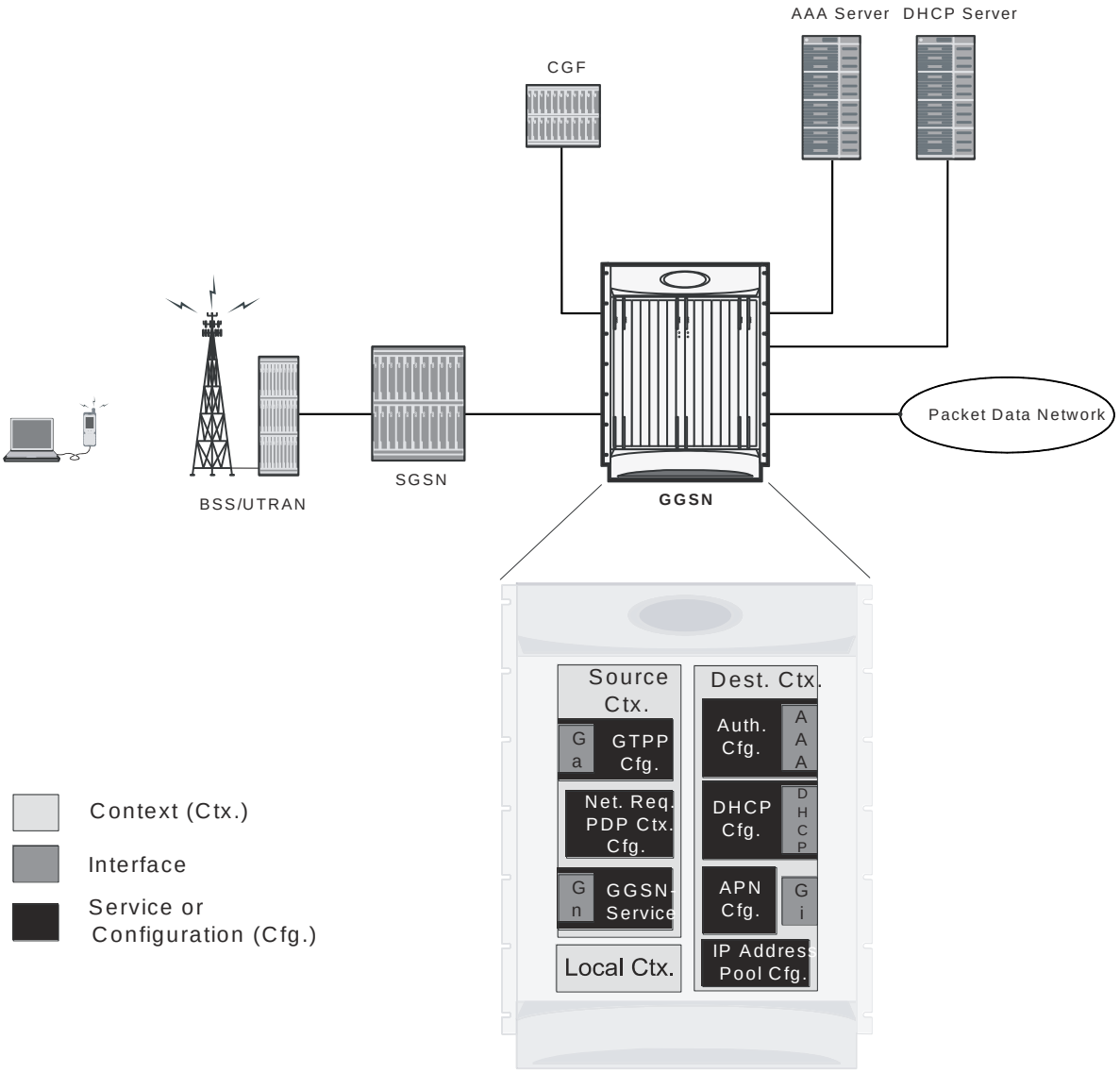
- GGSN service(s) and Gn interface to the Service GPRS Support Node (SGSN)
- GPRS Tunneling Protocol Prime (GTPP) configuration and Ga interface to the Charging Gateway Function (CGF)

The destination context facilitates the following:

- Access Point Name (APN) configuration
- RADIUS authentication configuration and the interface to the authentication server
- DHCP configuration and the interface to the DHCP server
- IP address pools
- Gi interface to the packet data network (PDN)

This configuration supports IP (transparent and non-transparent) and PPP PDP contexts as well as network requested PDP contexts.

Figure 20. GGSN Support Using a Single Source and Destination Context



Information Required

The following sections describe the minimum amount of information required to configure and make the GGSN 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 GGSN in the network. Information on these parameters can be found in the appropriate sections of the Command Line Reference.

Source Context Configuration

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

Table 1. Required Information for Source Context Configuration

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Gn Interface Configuration	
Gn interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Gn interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Gn interfaces.
Gateway IP address	Used when configuring static routes from the Gn interface(s) to a specific network.
GGSN service Configuration	
GGSN service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GGSN service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.

Required Information	Description
Accounting context	The name of the context configured on the system in which the processing of GTPP accounting records is performed. The context name is an identification string from 1 to 79 characters (alpha and/or numeric). By default, the system attempts to use the same context as the one in which the GGSN service is configured.
UDP port number for GTPC traffic	The port used by the GGSN service and the SGSN for communicating GTPC sockets for GTPv1. The UDP port number and can be any integer value from 1 to 65535. The default value is 2123.
Public Land Mobile Network (PLMN) Identifiers	**Mobile Country Code (MCC)**:The MCC can be configured to any integer value from 0 to 999.
	Mobile Network Code (MNC):The MNC can be configured to any integer value from 0 to 999.
SGSN information (optional)	The GGSN can be configured with information about the SGSN(s) that it is to communicate with. This includes the SGSN's IP address and subnet mask and whether or not the SGSN is on a foreign PLMN. Multiple SGSNs can be configured.
GGSN charging characteristics (CC) (optional)	**Behavior Bits**:If charging characteristics will be configured on the GGSN, behavior bits for the following conditions can be configured: • GGSN use of the accounting server specified by the profile index • GGSN rejection of Create PDP Context Request messages • GGSN ceases sending accounting records Each value must be a unique bit from 1 to 12 to represent the 12 possible behavior bits allowed for in the standards. The default configuration is disabled (0).
	Profile Index:If the GGSN's charging characteristics will be used for subscriber PDP contexts, profile indexes can be modified/configured for one or more of the following conditions: • The number of statistics container changes is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4. • The up and/or downlink traffic volume limits are met or exceeded within a specific time interval causing a partial record to be generated. The up and downlink volumes can be configured from 0 to 1000000 octets. The interval can be configured from 60 to 40000000 seconds. • The up and/or downlink traffic volume limits are met or exceeded causing an accounting record to be closed. The up and downlink volumes can be configured from 100000 to 4000000000 octets. • The number of SGSN switchovers is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4. • Specific tariff times within a day are reached causing an accounting record to be closed. Up to four times can be configured using the hour of the day (1-24) and the minute (1-60). • Prepaid accounting can be disabled for a specified profile index. The system supports the configuration of up to 16 profile indexes numbered 0 through 15 .

Required Information	Description
PLMN policy	The GGSN can be configured treat communications from unconfigured SGSNs in one of the following ways: • Treat the SGSN as if it is on a foreign PLMN • Treat the SGSN as if it is on a home PLMN • Reject communications from unconfigured SGSNs (default)
Ga Interface Configuration	
Ga interface name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Ga interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Ga interfaces.
Gateway IP address	Used when configuring static routes from the Ga interface(s) to a specific network.
GTPP Configuration	
Charging gateway address	The IP address of the system's GGSN interface.
CGF server information	**IP address**:The IP address of the CGF server to which the GGSN will send accounting information. Multiple CGFs can be configured.
	Priority:If more than on CGF is configured, this is the server's priority. It is used to determine the rotation order of the CGFs when sending accounting information. The priority can be configured to any integer value from 1 to 1000. The default is 1.
	Maximum number of messages:The maximum number of outstanding or unacknowledged GTPP messages allowed for the CGF. The maximum number can be configured to any integer value from 1 to 256. The default is 256.
GCDR optional fields	The following optional fields can be specified/configured in CDRs generated by the GGSN: • diagnostics • duration-ms (the time specified in the mandatory Duration field is reported in milliseconds) • local-record-sequence-number • plmn-id
Network Requested PDP Context Support Configuration (optional)	

Required Information	Description
Activation Requirements	**IP address**:The static IP address of the mobile station's for which network-requested PDP context activation will be supported. Up to 1000 addresses can be configured.
	Destination context name:The name of the destination context configured on the system that contains the IP address pool containing the mobile station's static address.
	International Mobile Subscriber Identity (IMSI):The IMSI of the mobile station.
	APN:The name of the access point that will be passed to the SGSN by the GGSN for the mobile station.
GSN-map node	Communications with the HLR from the GGSN go through a GSN-map node that performs the protocol conversion from GTPC to SS7. The IP address of the map node must be configured. Only one GSN-map node can be configured per source context.

Destination Context Configuration

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

Table 2. Required Information for Destination Context Configuration

Required Information	Description
Destination context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. **NOTE:** For this configuration, the destination context name should **not** match the domain name of a specific APN.
APN Configuration	
APN name	An identification string by which the APN will be recognized by the system. The name can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-). Multiple names are needed if multiple APNs will be used.
Accounting mode	Selects the accounting protocol. GTPP or RADIUS are supported. In addition, accounting can be completely disabled. The default is to perform accounting using GTPP. **NOTE:** The examples discussed in this chapter assumes GTPP is used.
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
APN charging characteristics (CC) (optional)	Specifies whether or not the GGSN accepts the CC from the SGSN for home, visiting, and roaming subscribers. By default the GGSN accepts the CC from the SGSN for all three scenarios. If the GGSN is to use its own CC for any of these scenarios, then each scenario requires the specification of behavior bits and a profile index to use. **NOTE:** The profile index parameters are configured as part of the GGSN service.

Required Information	Description
Domain Name Service (DNS) information (optional)	If DNS will be used for the APN, IP addresses can be configured for primary and secondary DNS servers.

IP address allocation method	Specifies how sessions facilitated by this APN will receive an IP address. IP addresses can be assigned using one of the following methods:
	• **Dynamic**: Address can be dynamically assigned from one of the sources.
	  • **Dynamic Host Control Protocol (DHCP) server**: The system can be configured to act as a DHCP proxy and receive address from the server in advance and assign them as needed or it can relay DHCP messages from the MS.
	  • **Local address pools**: The system can be configured with local address pools.
	• **Static**: MS IP addresses can be permanently assigned.
	By default, the system is configured to either dynamically assign addresses from a local pool and/or allow static addresses.

IP address pool name	If addresses will be dynamically assigned from a locally configured private pool, the name of the pool must be configured. If no name is configured, the system will automatically use any configured public pool.
IP destination context name	The name of the system destination context to use for subscribers accessing the APN. If no name is specified, the system automatically uses the system context in which the APN is configured.
Maximum number of PDP contexts	The maximum number of PDP contexts that are supported for the APN. The maximum number can be configured to any integer value from 1 to 1500000. The default is 1000000.
PDP type	The type of PDP contexts supported by the APN. The type can be IPv4, IPv6, both IPv4 and IPv6, or PPP. IPv4 support is enabled by default.
Verification selection mode	The level of verification that will be used to ensure a MS's subscription to use the APN. The GGSN uses any of the following methods: • No verification and MS supplies APN • No verification and SGSN supplies APN • Verified by SGSN (default)
DHCP Interface Configuration (optional)	
DHCP interface name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the DHCP interface and be bound to the DHCP service. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Gateway IP address	Used when configuring static routes from the DHCP interface(s) to a specific network.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

Required Information	Description
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical DHCP interfaces.
DHCP Service Configuration (optional)	
DHCP Service Name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the DHCP service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
DHCP Server Information	The IP address of each DHCP server that the system is to communicate with must be configured .Multiple servers can be configured. If multiple servers are configured, each can be assigned a priority from 1 to 1000. The default priority is 1.
Lease Duration	Specifies the minimum and maximum allowable lease times that are accepted in responses from DHCP servers. • **Minimum Lease Time**: Measured in seconds and can be configured to any integer value from 600 to 3600. The default is 600 seconds. • **Maximum Lease Time**: Measured in seconds and can be configured to any integer value from 10800 to 4294967295. The default is 86400 seconds.
AAA Interface Configuration	
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	
RADIUS Authentication server	**IP Address**: Specifies the IP address of the RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. If multiple servers are configured, each can be assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.

Required Information	Description
	UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
RADIUS Accounting server (optional)	**IP Address**: Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured.RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number:Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.
PDN Interface Configuration	
PDN interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration	
IP address pool name(s)	This is an identification string from 1 to 31 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used.

Required Information	Description
Pool addresses, subnet mask and type	The pool can consist of either of the following: • An entire subnet configured using the initial address and the subnet mask • A range of addresses configured using the first and last IP addresses in the range The pool can be configured as public, private, or static. Public pools can also be assigned a priority.

How This Configuration Works

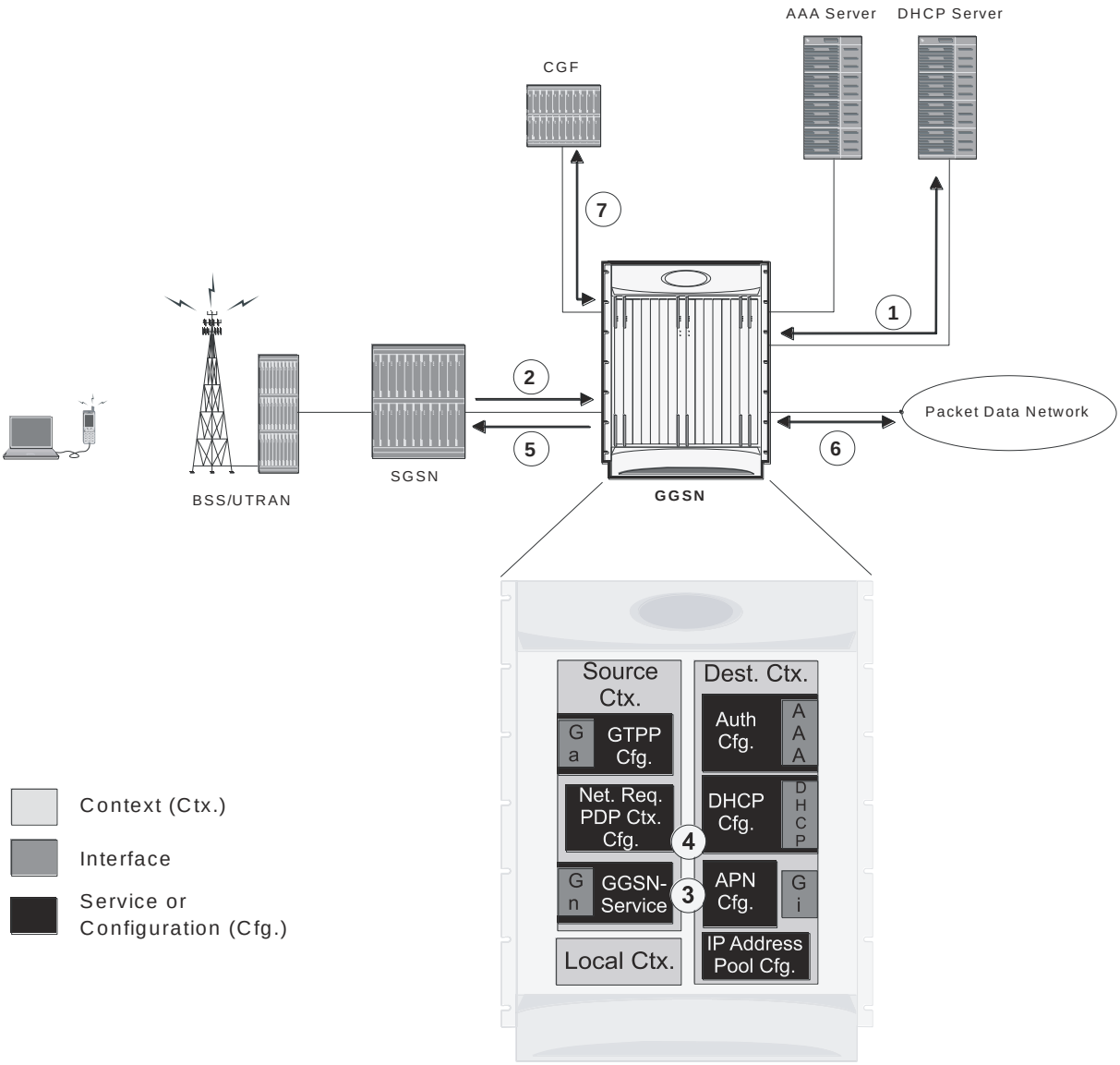
This section provides a description of how the information detailed in the previous sections of this chapter are used in the processing of the following types of subscriber sessions:

- Transparent IP PDP Context Processing
- Non-transparent IP PDP Context Processing
- PPP PDP Context Processing
- Network-requested PDP Context Processing

Transparent IP PDP Context Processing

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a transparent IP PDP context.

Figure 21. Transparent IP PDP Context Call Processing



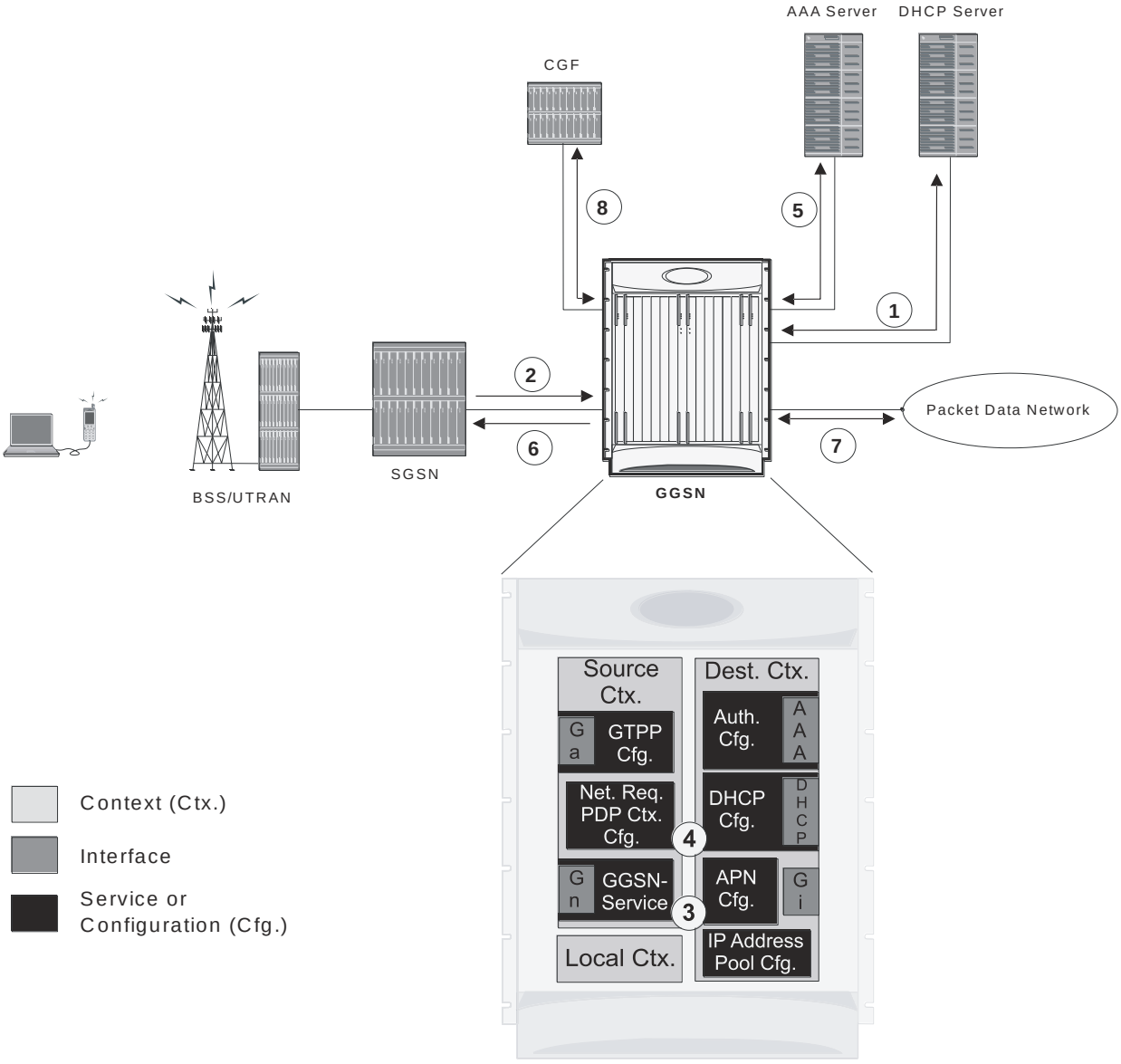
1. If the DHCP client mode is used for the dynamic assignment of IP addresses for subscriber PDP contexts, the system will retrieve addresses from the server over the DHCP interface during boot up and store them in cache memory.
2. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
3. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
4. If the MS requires a dynamically assigned address, the GGSN assigns one from those stored in its memory cache.

5. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
6. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
7. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

Non-transparent IP PDP Context Processing

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a non-transparent IP PDP context.

Figure 22. Non-transparent IP PDP Context Call Processing

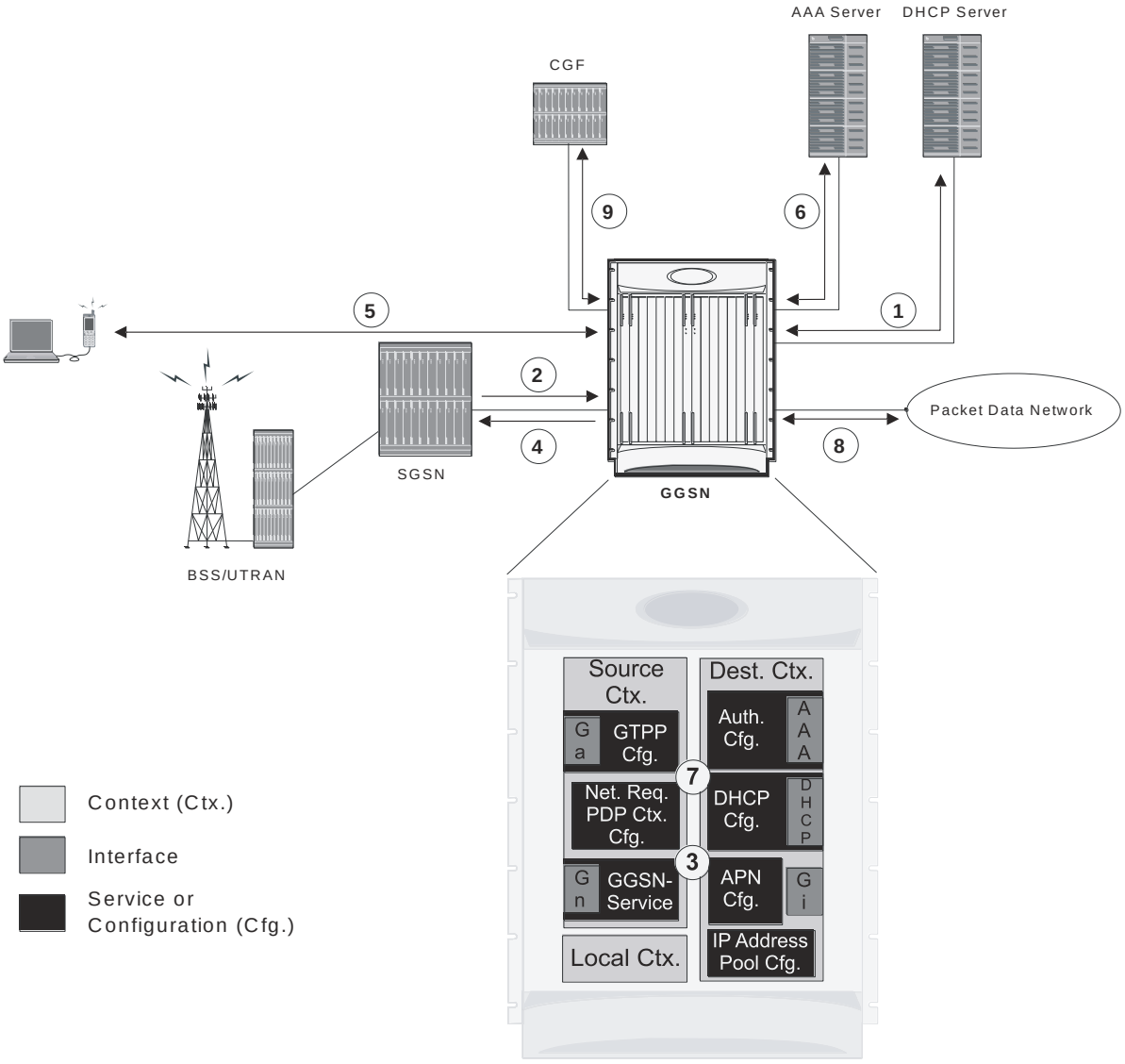


1. If the DHCP client mode is used for the dynamic assignment of IP addresses for subscriber PDP contexts, the system will retrieve addresses from the server over the DHCP interface during boot up and store them in cache memory.
2. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
3. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
4. If the MS requires a dynamically assigned address, the GGSN assigns one from those stored in its memory cache.
5. If subscriber authentication is required, the GGSN authenticates the subscriber by communicating with a RADIUS server over the AAA interface.
6. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
7. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
8. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

PPP PDP Context Processing

The following figure and the following text describe how this configuration with a single source and destination context would be used by the system to process a PPP PDP context.

Figure 23. PPP PDP Context Call Processing



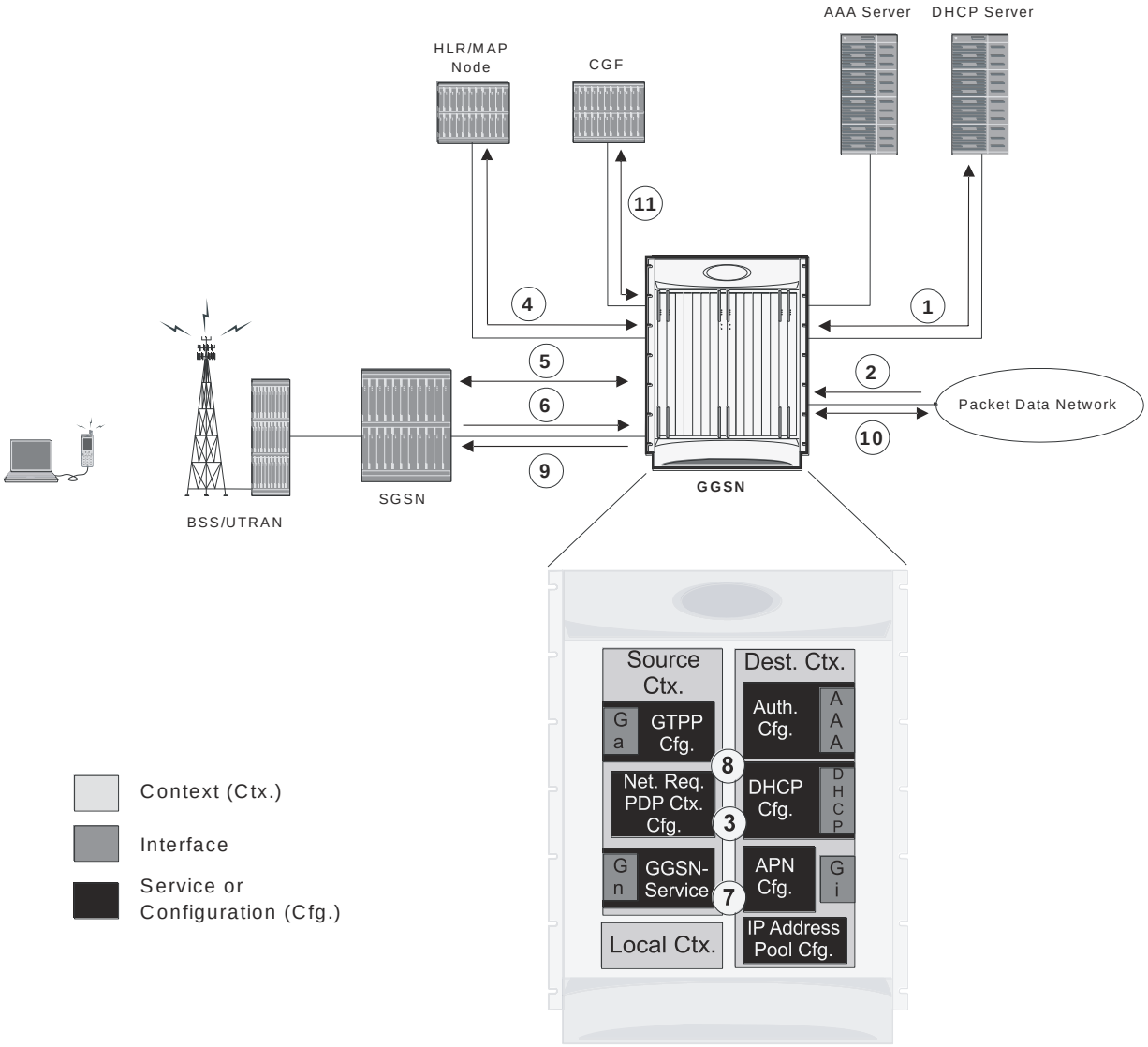
1. If the DHCP client mode is used for the dynamic assignment of IP addresses for subscriber PDP contexts, the system will retrieve addresses from the server over the DHCP interface during boot up and store them in cache memory.
2. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
3. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
4. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
5. The MS and GGSN negotiate PPP.
6. The GGSN authenticates the subscriber as part of the PPP negotiation by communicating with a RADIUS server over the AAA interface.

7. Upon successful authentication, the GGSN assigns an IP address to the MS from one of those stored in its memory cache.
8. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
9. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

Network-requested PDP Context Processing

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a network-requested PDP context.

Figure 24. Network-requested PDP Context Call Processing



1. If the DHCP client mode is used for the dynamic assignment of IP addresses for subscriber PDP contexts, the system will retrieve addresses from the server over the DHCP interface during boot up and store them in cache memory.
2. An IP packet data unit (PDU) is received by the GGSN from the PDN.
3. The GGSN determines if it is configured to support network-initiated sessions. If so, it begins the Network-Requested PDP Context Activation procedure, otherwise it discards the packet.
4. The GGSN determines if the MS is reachable by communicating with the HLR through a MAP node over one of the Gn interfaces.
5. The GGSN works with the SGSN to activate the MS.
6. Once activated, the MS initiates a PDP context resulting in the sending of a Create PDP Context Request message from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
7. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.
8. If the MS requires a dynamically assigned address, the GGSN assigns one from those stored in its memory cache.
9. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
10. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
11. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

Chapter 4
Mobile IP Configuration Examples

This chapter provides information for several configuration examples that can be implemented on the system to support Mobile IP (MIP) data services.

IMPORTANT: This chapter does not discuss the configuration of the local context. Information about the local context can be found in *Command Line Reference*.

IMPORTANT: When configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations* appendix.

Example 1: Mobile IP Support Using the System as a GGSN/FA

For Mobile IP applications, the system can be configured to perform the function of a Gateway GPRS Support Node/Foreign Agent (GGSN/FA) and/or a Home Agent (HA). This example describes what is needed for and how the system performs the role of the GGSN/FA. Examples 2 and 3 provide information on using the system to provide HA functionality.

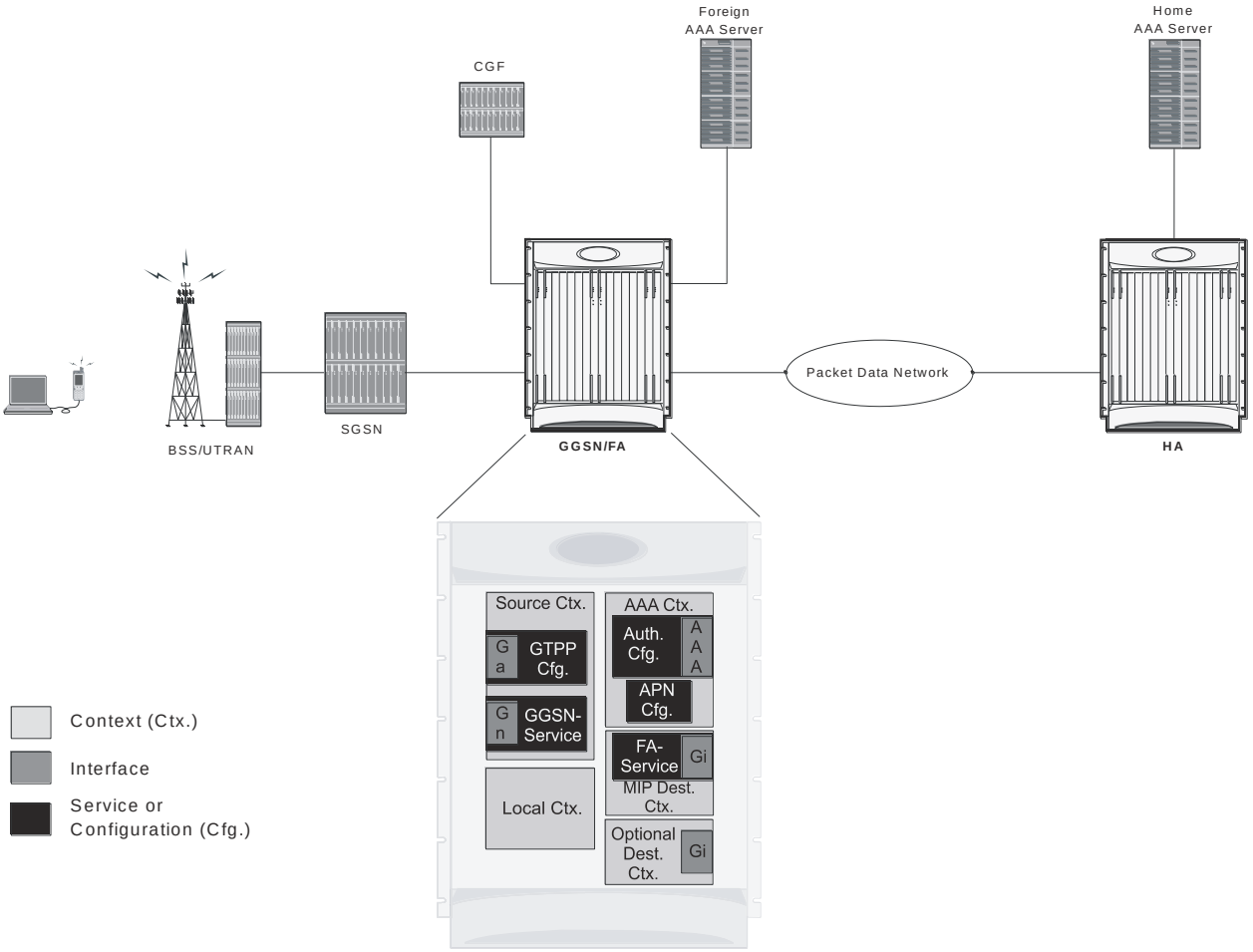
The system's GGSN/FA configuration for Mobile IP applications is best addressed with three contexts (one source, one AAA, and one Mobile IP destination) configured as shown in the figure that follows.

IMPORTANT: A fourth context that serves as a destination context must also be configured if Reverse Tunneling is disabled in the FA service configuration. Reverse Tunneling is enabled by default.

The source context will facilitate the GGSN service(s), and the Ga and Gn interfaces. The AAA context will be configured to provide foreign AAA functionality for subscriber PDP contexts and facilitate the AAA interfaces. The MIP destination context will facilitate the FA service(s) and the Gi interface(s) from the GGSN/FA to the HA.

The optional destination context will allow the routing of data from the mobile node to the packet data network by facilitating a packet data network (PDN) interface. This context will be used only if reverse tunneling is disabled.

Figure 25. Mobile IP Support using the system as a GGSN/FA



Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

Source Context Configuration

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

Table 3. Required Information for Source Context Configuration

Required Information	Description

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system. **NOTE**: The name of the source context should be the same as the name of the context in which the FA-context is configured if a separate system is being used to provide GGSN/FA functionality.
Gn Interface Configuration	
Gn interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Gn interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Gn interfaces.
Gateway IP address	Used when configuring static routes from the Gn interface(s) to a specific network.
GGSN service Configuration	
GGSN service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GGSN service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
Accounting context	The name of the context configured on the system in which the processing of GTPP accounting records is performed. The context name is an identification string from 1 to 79 characters (alpha and/or numeric). By default, the system attempts to use the same context as the one in which the GGSN service is configured.
UDP port number for GTPC traffic	The port used by the GGSN service and the SGSN for communicating GTPC sockets for GTPv1. The UDP port number and can be any integer value from 1 to 65535. The default value is 2123.
Public Land Mobile Network (PLMN) Identifiers	**Mobile Country Code (MCC)**: The MCC can be configured to any integer value from 0 to 999.
	Mobile Network Code (MNC): The MNC can be configured to any integer value from 0 to 999.
SGSN information (optional)	The GGSN can be configured with information about the SGSN(s) that it is to communicate with. This includes the SGSN's IP address and subnet mask and whether or not the SGSN is on a foreign PLMN.Multiple SGSNs can be configured.

Required Information	Description
GGSN charging characteristics (CC) (optional)	**Behavior Bits**: If charging characteristics will be configured on the GGSN, behavior bits for the following conditions can be configured: • GGSN use of the accounting server specified by the profile index • GGSN rejection of Create PDP Context Request messages • GGSN ceases sending accounting records Each value must be a unique bit from 1 to 12 to represent the 12 possible behavior bits allowed for in the standards. The default configuration is disabled (0).
	Profile Index:If the GGSN's charging characteristics will be used for subscriber PDP contexts, profile indexes can be modified/configured for one or more of the following conditions: • The number of statistics container changes is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4. • The up and/or downlink traffic volume limits are met or exceeded within a specific time interval causing a partial record to be generated. The up and downlink volumes can be configured from 0 to 1000000 octets. The interval can be configured from 60 to 40000000 seconds. • The up and/or downlink traffic volume limits are met or exceeded causing an accounting record to be closed. The up and downlink volumes can be configured from 100000 to 4000000000 octets. • The number of SGSN switchovers is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4. • Specific tariff times within a day are reached causing an accounting record to be closed. Up to four times can be configured using the hour of the day (1-24) and the minute (1-60). The system supports the configuration of up to 16 profile indexes numbered 0 through 15.
PLMN policy	The GGSN can be configured treat communications from unconfigured SGSNs in one of the following ways: • Treat the SGSN as if it is on a foreign PLMN • Treat the SGSN as if it is on a home PLMN • Reject communications from unconfigured SGSNs (default)
Ga Interface Configuration	
Ga interface name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Ga interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

Required Information	Description
Physical port description	An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Ga interfaces.
Gateway IP address	Used when configuring static routes from the Ga interface(s) to a specific network.
GTPP Configuration	
Charging gateway address	The IP address of the system's GGSN interface.
CGF server information	**IP address**:The IP address of the CGF server to which the GGSN will send accounting information .Multiple CGFs can be configured.
	Priority:If more than on CGF is configured, this is the server's priority. It is used to determine the rotation order of the CGFs when sending accounting information. The priority can be configured to any integer value from 1 to 1000. The default is 1.
	Maximum number of messages:The maximum number of outstanding or unacknowledged GTPP messages allowed for the CGF. The maximum number can be configured to any integer value from 1 to 256. The default is 256.
GCDR optional fields	The following optional fields can be specified/configured in CDRs generated by the GGSN: • diagnostics • duration-ms : the time specified in the mandatory Duration field is reported in milliseconds • local-record-sequence-number • plmn-id

AAA Context Configuration

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

Table 4. Required Information for AAA Context Configuration

Required Information	Description
AAA context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the AAA context will be recognized by the system. **NOTE**: If a separate system is used to provide HA functionality, the AAA context name should match the name of the context in which the AAA functionality is configured on the HA machine.
APN Configuration	
APN name	An identification string by which the APN will be recognized by the system. The name can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-). Multiple names are needed if multiple APNs will be used.

Required Information	Description
Accounting mode	Selects the accounting protocol. GTPP or RADIUS are supported. In addition, accounting can be completely disabled. The default is to perform accounting using GTPP. **NOTE:** The examples discussed in this chapter assumes GTPP is used.
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
APN charging characteristics (CC) (optional)	Specifies whether or not the GGSN accepts the CC from the SGSN for home, visiting, and roaming subscribers. By default the GGSN accepts the CC from the SGSN for all three scenarios. If the GGSN is to use its own CC for any of these scenarios, then each scenario requires the specification of behavior bits and a profile index to use. **NOTE:** The profile index parameters are configured as part of the GGSN service.
Domain Name Service (DNS) information (optional)	If DNS will be used for the APN, IP addresses can be configured for primary and secondary DNS servers.
IP destination context name	The name of the system destination context to use for subscribers accessing the APN. If no name is specified, the system automatically uses the system context in which the APN is configured.
Maximum number of PDP contexts	The maximum number of PDP contexts that are supported for the APN. The maximum number can be configured to any integer value from 1 to 1500000. The default is 1000000.
PDP type	The type of PDP contexts supported by the APN. The type can be IPv4, IPv6, both IPv4 and IPv6, or PPP. IPv4 support is enabled by default.
Verification selection mode	The level of verification that will be used to ensure a MS's subscription to use the APN. The GGSN uses any of the following methods: • No verification and MS supplies APN • No verification and SGSN supplies APN • Verified by SGSN (default)
Mobile IP Configuration	**Home Agent IP Address**: The IP address of an HA with which the system will tunnel subscriber Mobile IP sessions. Configuring this information tunnels all subscriber Mobile IP PDP contexts facilitated by the APN to the same HA unless an individual subscriber profile provides an alternate HA address. Parameters stored in individual profiles supersede parameters provided by the APN.
	Mobile IP Requirement: The APN can be configured to require Mobile IP for all sessions it facilitates. Incoming PDP contexts that do/can not use Mobile IP are dropped.
AAA Interface Configuration	
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.

Required Information	Description
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Foreign RADIUS Server Configuration	
Foreign RADIUS Authentication server	**IP Address**: Specifies the IP address of the Foreign RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers. Foreign RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
Foreign RADIUS Accounting server (optional)	**IP Address**: Specifies the IP address of the foreign RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured.RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the foreign RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the foreign RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.

Mobile IP Destination Context Configuration

The following table lists the information that is required to configure the Mobile IP destination context.

Table 5. Required Information for Mobile IP Destination Context Configuration

Required Information	Description
Mobile IP Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the Mobile IP destination context will be recognized by the system. **NOTE**: For this configuration, the destination context name should **not** match the domain name of a specific domain. It should, however, match the name of the context in which the HA service is configured if a separate system is used to provide HA functionality.
Gi Interface Configuration	
Gi interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Gi interfaces.
Gateway IP address(es)	Used when configuring static routes from the Gi interface(s) to a specific network.
FA Service Configuration	
FA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the FA service will be recognized by the system .Multiple names are needed if multiple FA services will be used. FA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the FA service and the HA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Security Parameter Index (indices) Information	**HA IP address**: Specifies the IP address of the HAs with which the FA service communicates. The FA service allows the creation of a security profile that can be associated with a particular HA.
	Index: Specifies the shared SPI between the FA service and a particular HA. The SPI can be configured to any integer value between 256 and 4294967295.Multiple SPIs can be configured if the FA service is to communicate with multiple HAs.
	Secrets: Specifies the shared SPI secret between the FA service and the HA. The secret can be between 1 and 127 characters (alpha and/or numeric).An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default is hmac-md5.A hash-algorithm is required for each SPI configured.

Required Information	Description
FA agent advertisement lifetime	Specifies the time (in seconds) that an FA agent advertisement remains valid in the absence of further advertisements. The time can be configured to any integer value between 1 and 65535. The default is 9000.
Number of allowable unanswered FA advertisements	Specifies the number of unanswered agent advertisements that the FA service will allow during call setup before it will reject the session. The number can be any integer value between 1 and 65535. The default is 5.
Maximum mobile-requested registration lifetime allowed	Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node. The lifetime is expressed in seconds and can be configured between 1 and 65534. An infinite registration lifetime can be configured by disabling the timer. The default is 600 seconds.
Registration reply timeout	Specifies the amount of time that the FA service will wait for a Registration Reply from an HA. The time is measured in seconds and can be configured to any integer value between 1 and 65535. The default is 7.
Number of simultaneous registrations	Specifies the number of simultaneous Mobile IP sessions that will be supported for a single subscriber. The maximum number of sessions is 3. The default is 1. **NOTE**: The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The FA service can be configured to always require authentication or not. If not, the initial registration and de-registration will still be handled normally.
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.

Optional Destination Context Configuration

The following table lists the information required to configure the optional destination context. As discussed previously, this context is required if: 1) reverse tunneling is disabled in the FA service, or 2) if access control lists (ACLs) are used

IMPORTANT: If ACLs are used, the destination context would only consist of the ACL configuration. Interface configuration would not be required.

Table 6. Required Information for Destination Context Configuration

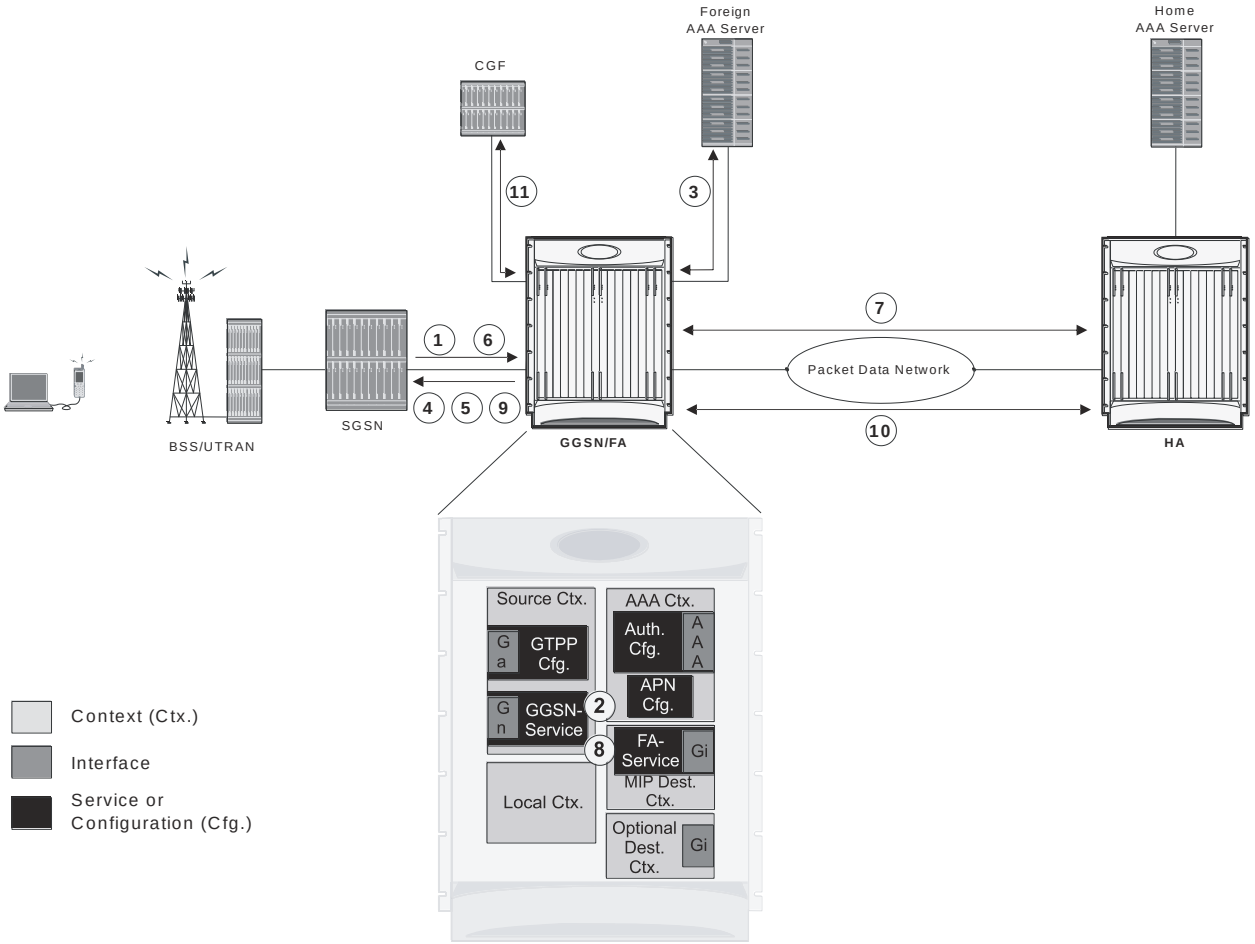
Required Information	Description

Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. **NOTE**: For this configuration, the destination context name should **not** match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.

How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

Figure 26. Call Processing When Using the system as a GGSN/FA



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN. In this case, it is determined that Mobile IP must be used. From the APM configuration, the system also determines the context in which the FA service is configured.
3. If subscriber authentication is required, the GGSN authenticates the subscriber by communicating with a RADIUS server over the AAA interface.
4. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface. The home address assigned to the mobile as part of the response is 0.0.0.0 indicating that it will be reset with a Home address after the PDP context activation procedure.
5. The FA component of the GGSN sends a Agent Advertisement message to the MS. The message contains the FA parameters needed by the mobile such as one or more card-of addresses. The message is sent as an IP limited broadcast message (i.e. destination address 255.255.255.255), however only on the requesting MS's TEID to avoid broadcast over the radio interface.

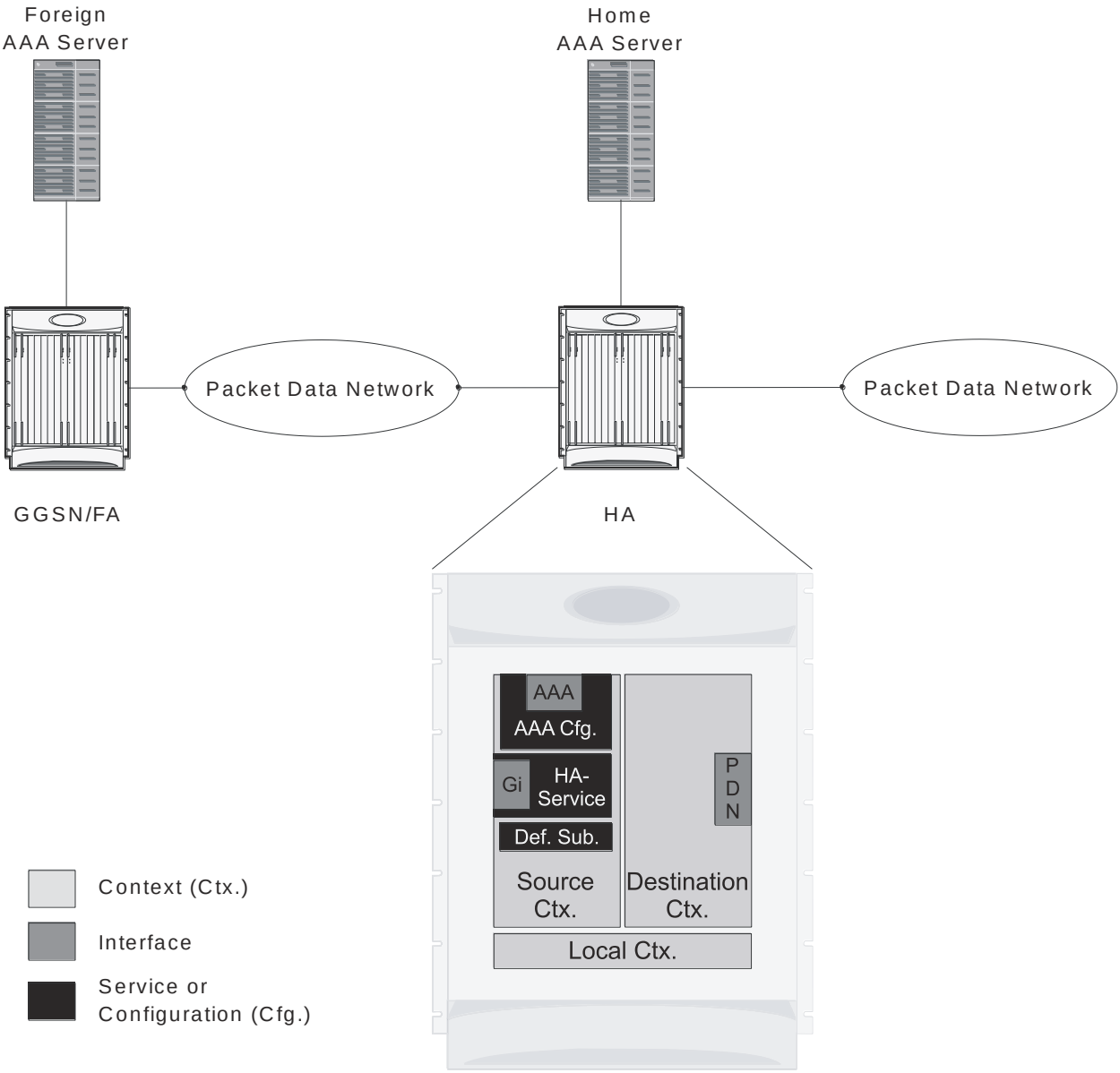
6. The MS sends a Mobile IP Registration request to the GGSN/FA. This message includes either the MS's static home address or it can request a temporary address by sending 0.0.0.0 as its home address. Additionally, the request must always include the Network Access Identifier (NAI) in a Mobile-Node-NAI Extension.
7. The FA forwards the registration request from the MS to the HA while the MS's home address or NAI and TEID are stored by the GGSN. In response the HA sends a registration response to the FA containing the address assigned to the MS.
8. The FA extracts the home address assigned to the MS by the HA from the response and the GGSN updates the associated PDP context. The FA then forwards it to the MS (identified by either the home address or the NAI and TEID).
9. The GGSN issues a PDP context modification procedure to the SGSN in order to update the PDP address for the MS.
10. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
11. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

Example 2: Mobile IP Support Using the System as an HA

The system supports both Simple and Mobile IP. For Mobile IP applications, the system can be configured to perform the function of a GGSN/FA and/or a HA. This example describes what is needed for and how the system performs the role of the HA. Example number 1 provides information on using the system to provide GGSN/FA functionality.

The system's HA configuration for Mobile IP applications requires that at least two contexts (one source and one destination) be configured as shown in the following figure.

Figure 27. Mobile IP Support Using the system as an HA



The source context will facilitate the HA service(s), the Gi interfaces from the FA, and the AAA interfaces. The source context will also be configured to provide Home AAA functionality for subscriber sessions. The destination context will facilitate the PDN interface(s).

Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

Source Context Configuration

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

Table 7. Required Information for Source Context Configuration

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Gi Interface Configuration	
Gi interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Gi interfaces.
Gateway IP address	Used when configuring static routes from the Gi interface(s) to a specific network.
HA service Configuration	
HA service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	The port used by the HA service and the FA for communications. The UDP port number and can be any integer value from 1 to 65535. The default value is 434.

Required Information	Description
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations.The HA service can be configured as follows: • Always require authentication • Never require authentication **NOTE**: The initial registration and de-registration will still be handled normally) • Never look for mn-aaa extension • Not require authentication but will authenticate if mn-aaa extension present.
FA-to-HA Security Parameter Index Information	**FA IP address**: The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is **hmac-md5**. A hash-algorithm is required for each SPI configured.
Mobile Node Security Parameter Index Information	**Index**: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is **hmac-md5**. A hash-algorithm is required for each SPI configured.
	Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each mobile node-to-HA SPI configured.
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.
AAA Interface Configuration	

Required Information	Description
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	
Home RADIUS Authentication server	**IP Address**: Specifies the IP address of the home RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers. Home RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
Home RADIUS Accounting server (optional)	**IP Address**: Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured.RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the home RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.

Required Information	Description
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.
Default Subscriber Configuration	
"Default" subscriber's IP context name	Specifies the name of the egress context on the system that facilitates the Gi interfaces. **NOTE**: For this configuration, the IP context name should be identical to the name of the destination context.

Destination Context Configuration

The following table lists the information required to configure the destination context.

Table 8. Required Information for Destination Context Configuration

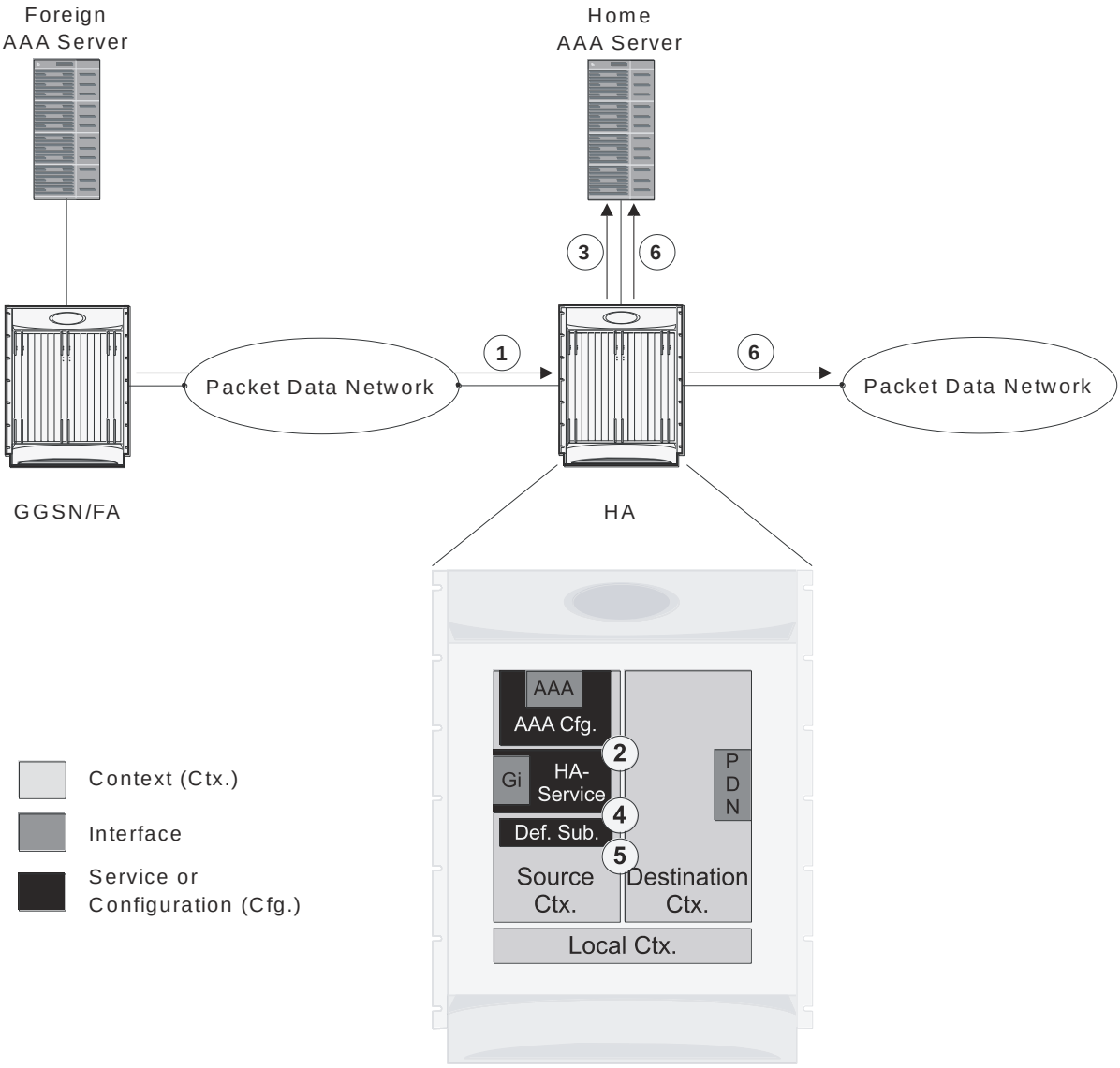
Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. **NOTE**: For this configuration, the destination context name should **not** match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration	
IP address pool name	Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.

Required Information	Description
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.

How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

Figure 28. Call Processing When Using the system as an HA



1. A subscriber session from the FA is received by the HA service over the Gi interface.
2. The HA service determines which context to use to provide AAA functionality for the session. This process is described in the How the System Selects Contexts section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.

   For this example, the result of this process is that the HA service determined that AAA functionality should be provided by the *Source* context.
3. The system then communicates with the Home AAA server specified in the Source context's AAA configuration to authenticate the subscriber.

4. Upon successful authentication, the *Source* context determines which egress context to use for the subscriber session. This process is described in the *How the System Selects Contexts section* located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.

   For this example, the system determines that the egress context is the Destination context based on the configuration of the *Default* subscriber.

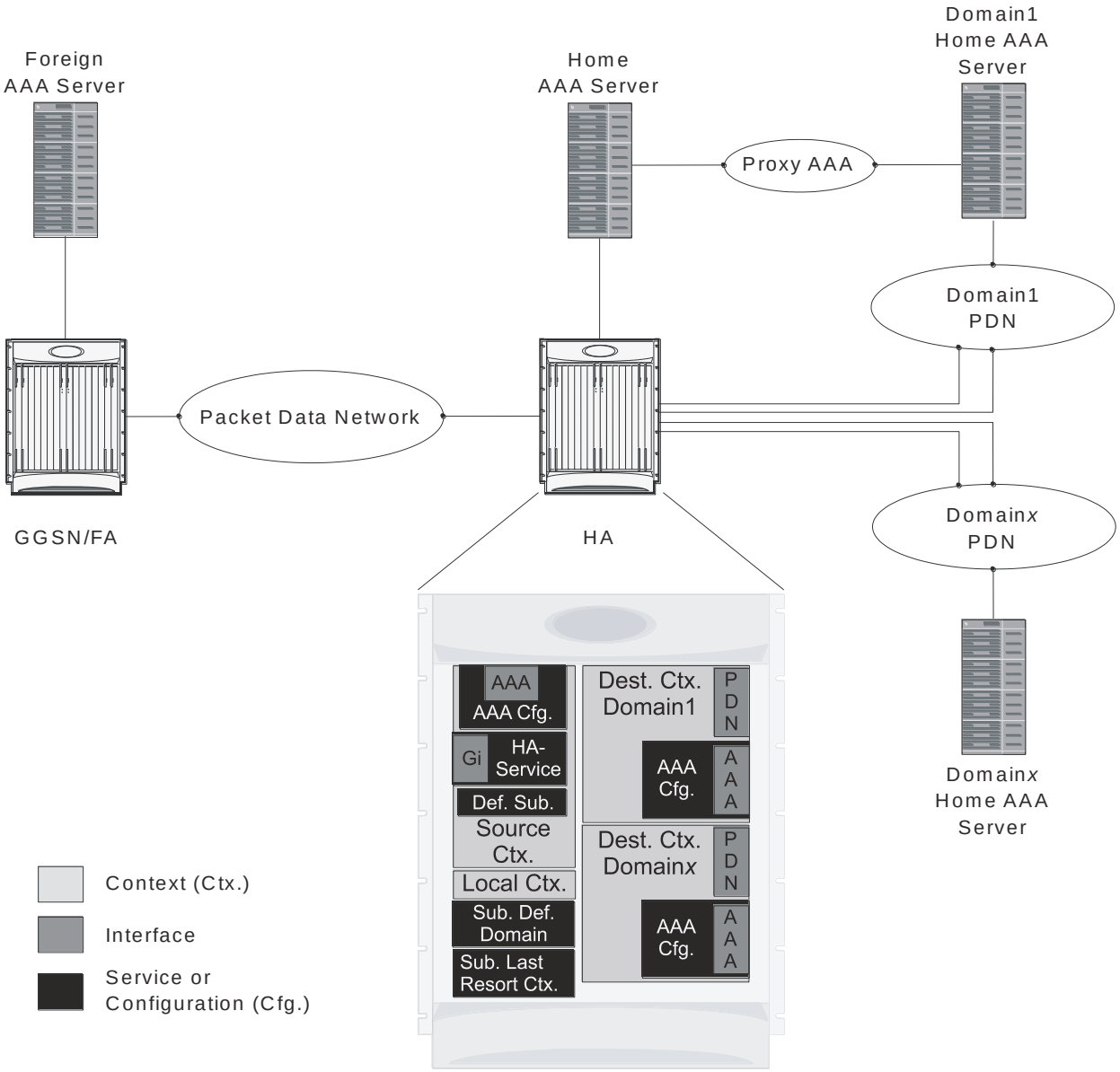
5. An IP address is assigned to the subscriber's mobile node from an IP address pool configured in the destination context. This IP address is used for the duration of the session and then be returned to the pool.
6. Data traffic for the subscriber session is then routed through the PDN interface in the *Destination* context.
7. Accounting messages for the session are sent to the AAA server over the AAA interface.

Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts

The system allows the wireless carrier to easily generate additional revenue by providing the ability to configure separate contexts that can then be leased or outsourced to various enterprises or ISPs, each having a specific domain.

In order to perform the role of an HA and support multiple outsourced domains, the system must be configured with at least one source context and multiple destination contexts as shown in the following figure. The AAA servers could by owned/maintained by either the carrier or the domain. If they are owned by the domain, the carrier will have to receive the AAA information via proxy.

Figure 29. The system as an HA Using a Single Source Context and Multiple Outsourced Destination Contexts



The source context will facilitate the HA service(s), and the Gi interface(s) to the FA(s).The source context will also be configured with AAA interface(s) and to provide Home AAA functionality for subscriber sessions. The destination contexts will each be configured to facilitate PDN interfaces. In addition, because each of the destination contexts can be outsourced to different domains, they will also be configured with AAA interface(s) and to provide AAA functionality for that domain.

In addition to the source and destination contexts, there are additional system-level AAA parameters that must be configured.

Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

Source Context Configuration

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

Table 9. Required Information for Source Context Configuration

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Gi Interface Configuration	
Gi interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Gn interfaces.
Gateway IP address	Used when configuring static routes from the Gi interface(s) to a specific network.
HA service Configuration	
HA service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	The port used by the HA service and the FA for communications. The UDP port number and can be any integer value from 1 to 65535. The default value is 434.

Required Information	Description
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations.The HA service can be configured as follows: • Always require authentication • Never require authentication **NOTE**: The initial registration and de-registration will still be handled normally) • Never look for mn-aaa extension • Not require authentication but will authenticate if mn-aaa extension present.
FA-to-HA Security Parameter Index Information	**FA IP address**: The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is **hmac-md5**. A hash-algorithm is required for each SPI configured.
Mobile Node Security Parameter Index Information	**Index**: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is **hmac-md5**. A hash-algorithm is required for each SPI configured.
	Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each mobile node-to-HA SPI configured.
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.
AAA Interface Configuration	

Required Information	Description
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	
Home RADIUS Authentication server	**IP Address**: Specifies the IP address of the home RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers. Home RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
Home RADIUS Accounting server (optional)	**IP Address**: Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured.RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the home RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.

Required Information	Description
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.
Default Subscriber Configuration	
"Default" subscriber's IP context name	Specifies the name of the egress context on the system that facilitates the Gi interfaces. **NOTE**: For this configuration, the IP context name should be identical to the name of the destination context.

Destination Context Configuration

The following table lists the information required to configure the destination context. This information will be required for each domain.

Table 10. Required Information for Destination Context Configuration

Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system.**NOTE:** For this configuration, the destination context name should **not** match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.Multiple names are needed if multiple interfaces will be configured.PDN interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface.Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.Multiple descriptions are needed if multiple ports will be used.Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration (optional)	
IP address pool name	Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.

Required Information	Description
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet , or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.
AAA Interface Configuration	
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	
RADIUS Authentication server	**IP Address**: Specifies the IP address of the RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers. Foreign RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
RADIUS Accounting server (optional)	**IP Address**: Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured.RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.

Required Information	Description
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.

System-Level AAA Configuration

The following table lists the information that is required to configure the system-level AAA parameters.

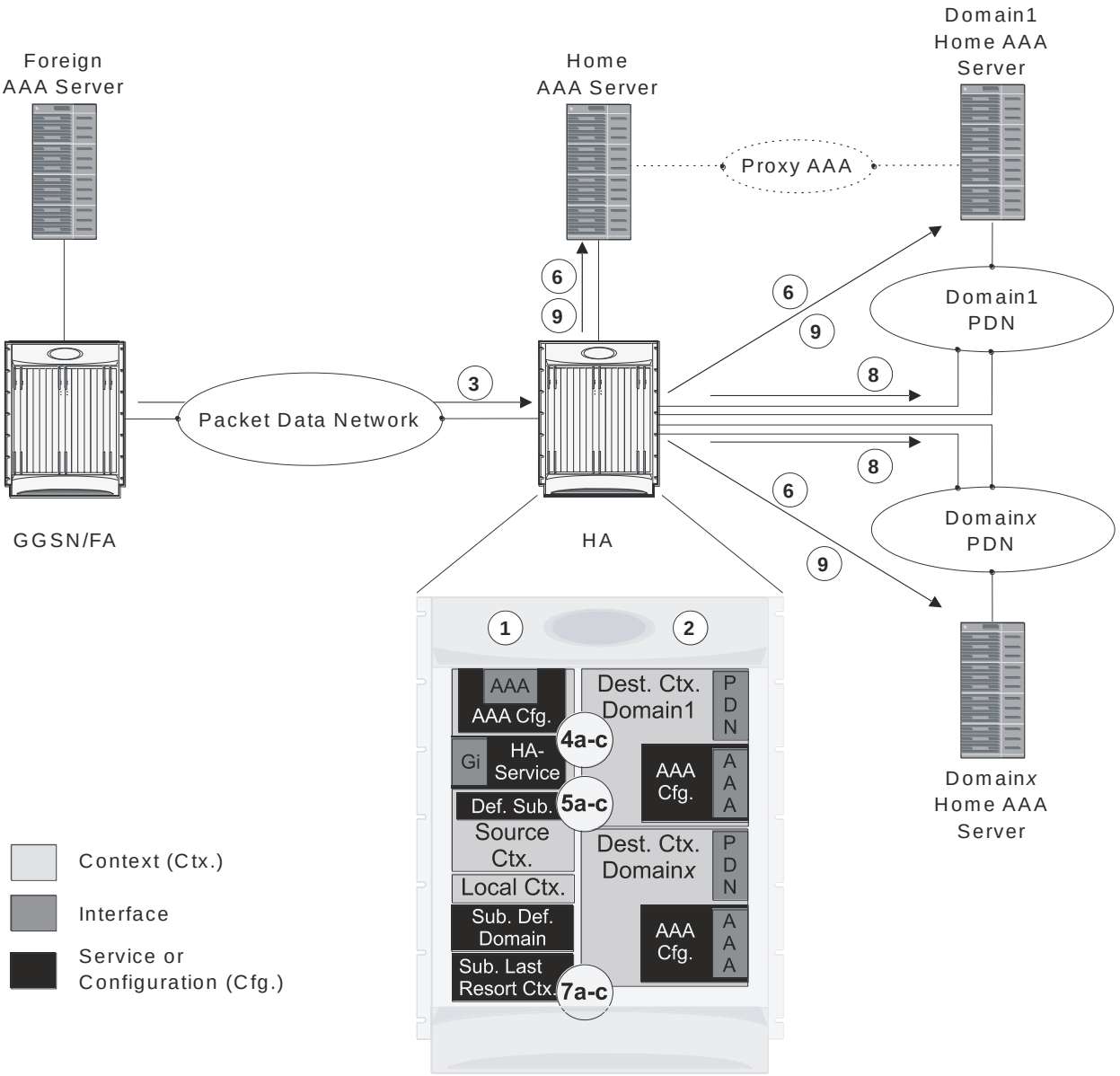
Table 11. Required Information for System-Level AAA Configuration

Required Information	Description
Subscriber default domain name	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username is missing or poorly formed. This parameter will be applied to all subscribers if their domain can not be determined from their username regardless of what domain they are trying to access. **NOTE**: The default domain name can be the same as the source context.
Subscriber Last-resort context	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username was present but does not match the name of a configured destination context .This parameter will be applied to all subscribers if their specified domain does not match a configured destination context regardless of what domain they are trying to access. **NOTE**: The last-resort context name can be the same as the source context.
Subscriber username format	Specifies the format of subscriber usernames as to whether or not the username or domain is specified first and the character that separates them. The possible separator characters are: • @ • % • - • \ • # • / Up to six username formats can be specified. The default is `username@`. **NOTE**: The username string is searched from right to left for the separator character. Therefore, if there is one or more separator characters in the string, only the first one that is recognized is considered the actual separator. For example, if the default username format was used, then for the username string *user1@enterprise@isp1*, the system resolves to the username *user1@enterprise* with domain *isp1*.

How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

Figure 30. Call Processing When Using the system as an HA with a Single Source Context and Multiple Outsourced Destination Contexts



1. The system-level AAA settings were configured as follows:
    - Subscriber default domain name = *Domainx*

- Subscriber username format = `username@`
- No subscriber last-resort context name was configured

2. The subscriber IP context names were configured as follows:
   - Within the *Source* context, the IP context name was configured as `Domainx`
   - Within the *Domainx* context, the IP context name was configured as `Domainx`
3. Sessions are received by the HA service from the FA over the Gi interface for *subscriber1@Domain1*, *subscriber2*, and *subscriber3@Domain37*.
4. The HA service attempts to determine the domain names for each session.
   - For *subscriber1*, the HA service determines that a domain name is present and is *Domain1*.
   - For *subscriber2*, the HA service determines that no domain name is present.
   - For *subscriber3*, the HA service determines that a domain name is present and is *Domain37*.
5. The HA service determi nes which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
   - For *subscriber1*, the HA service determines that a context was configured with a name (*Domain1*) that matches the domain name specified in the username string. Therefore, *Domain1* is used.
   - For *subscriber2*, the HA service determines that *Domainx* is configured as the default domain name. Therefore, *Domainx* is used.
   - For *subscriber3*, the HA service determines that no context is configured that matches the domain name (*Domain37*) specified in the username string. Because no **last-resort** context name was configured, the *Source* context is used.
6. The system then communicates with the Home AAA server specified in the Source context's AAA configuration to authenticate the subscriber.
7. Upon successful authentication of all three subscribers, the HA service determines which destination context to use for each of the subscriber sessions. This process is described in the *How the System Selects Context*s section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
   - For *subscriber1*, the HA service receives the *SN-VPN-NAME* or *SN1-VPN-NAME* attribute equal to *Domain1* as part of the Authentication Accept message from the AAA server on *Domain1*'s network. Therefore, *Domain1* is used as the destination context.
   - For *subscriber2*, the HA service determines that the *SN-VPN-NAME* or *SN1-VPN-NAME* attribute was not returned with the Authentication Accept response, and determines the subscriber IP context name configured within the *Domainx* context. Therefore, the *Domainx* context is used as the destination context.
   - For *subscriber3*, the HA service determines that the *SN-VPN-NAME* or *SN1-VPN-NAME* attribute was not returned with the Authentication Accept response, and determines the subscriber IP context name configured within the *Source* context. Therefore, the *Source* context is used as the destination context.
8. Data traffic for the subscriber session is then routed through the PDN interface in the each subscriber's destination context.
9. Accounting messages for the session are sent to the AAA server over the appropriate AAA interface.

Chapter 5
GGSN and Mobile IP Service in a Single System Configuration Example

This chapter provides information for several configuration examples that can be implemented on the system to support GGSN and Mobile IP data services in a single system.

IMPORTANT: This chapter does not discuss the configuration of the local context. Information about the local context can be found in *System Administration Guide*.

IMPORTANT: When configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations*.

Using the System as Both a GGSN/FA and an HA

The system supports both GGSN and Mobile IP functionality. For Mobile IP applications, the system can be configured to perform the function of a Gateway GPRS Support Node/Foreign Agent (GGSNSN/FA) and/or a Home Agent (HA). This example describes what is needed for and how a single system simultaneously supports both of these functions.

In order to support GGSN, FA, and HA functionality, the system must be configured with at least one source context and at least two destination contexts as shown in the following figure.

The source context facilitates the following:

- GGSN service(s) and Gn interface to the Service GPRS Support Node (SGSN)
- GPRS Tunneling Protocol Prime (GTPP) configuration and Ga interface to the Charging Gateway Function (CGF)

The destination context facilitates the following:

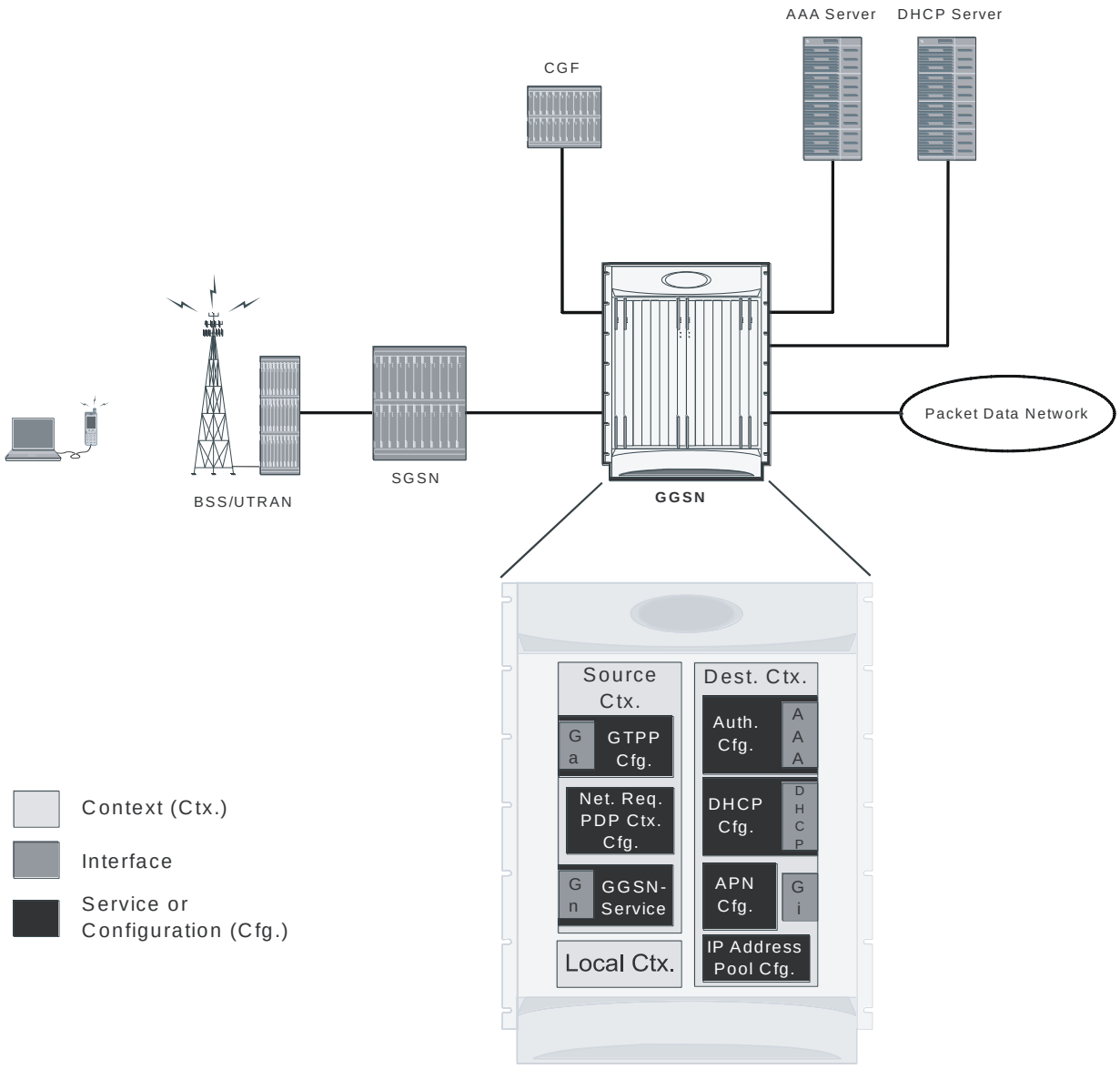
- Access Point Name (APN) configuration
- RADIUS authentication configuration and the interface to the authentication server
- DHCP configuration and the interface to the DHCP server
- IP address pools
- Gi interface to the packet data network (PDN)

The Mobile IP destination context facilitates the following:

- FA Service(s)
- HA Service(s)
- Gi interface to the packet data network (PDN)
- ICC interface facilitating communication between the FA and HA services.

This configuration supports IP (transparent and non-transparent) and PPP PDP contexts as well as network requested PDP contexts. In addition, Mobile IP and Proxy Mobile IP are supported for IP PDP contexts.

Figure 31. Simple and Mobile IP Support Within a Single System



Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the required information to configure the source and destination contexts.

Source Context Configuration

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

Table 12. Required Information for Source Context Configuration

Required Information	Description
Source context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Gn Interface Configuration	
Gn interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Gn interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Gn interfaces.
Gateway IP address	Used when configuring static routes from the Gn interface(s) to a specific network.
GGSN service Configuration	
GGSN service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GGSN service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
Accounting context	The name of the context configured on the system in which the processing of GTPP accounting records is performed. The context name is an identification string from 1 to 79 characters (alpha and/or numeric). By default, the system attempts to use the same context as the one in which the GGSN service is configured.
UDP port number for GTPC traffic	The port used by the GGSN service and the SGSN for communicating GTPC sockets for GTPv1. The UDP port number and can be any integer value from 1 to 65535. The default value is 2123.
Public Land Mobile Network (PLMN) Identifiers	**Mobile Country Code (MCC)**: The MCC can be configured to any integer value from 0 to 999.
	Mobile Network Code (MNC): The MNC can be configured to any integer value from 0 to 999.
SGSN information (optional)	The GGSN can be configured with information about the SGSN(s) that it is to communicate with. This includes the SGSN's IP address and subnet mask and whether or not the SGSN is on a foreign PLMN. Multiple SGSNs can be configured.

Required Information	Description
GGSN charging characteristics (CC) (optional)	**Behavior Bits**:If charging characteristics will be configured on the GGSN, behavior bits for the following conditions can be configured: • GGSN use of the accounting server specified by the profile index • GGSN rejection of Create PDP Context Request messages • GGSN ceases sending accounting records Each value must be a unique bit from 1 to 12 to represent the 12 possible behavior bits allowed for in the standards. The default configuration is disabled (0).
	Profile Index:If the GGSN's charging characteristics will be used for subscriber PDP contexts, profile indexes can be modified/configured for one or more of the following conditions: • The number of statistics container changes is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4. • The up and/or downlink traffic volume limits are met or exceeded within a specific time interval causing a partial record to be generated. The up and downlink volumes can be configured from 0 to 1000000 octets. The interval can be configured from 60 to 40000000 seconds. • The up and/or downlink traffic volume limits are met or exceeded causing an accounting record to be closed. The up and downlink volumes can be configured from 100000 to 4000000000 octets. • The number of SGSN switchovers is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4. • Specific tariff times within a day are reached causing an accounting record to be closed. Up to four times can be configured using the hour of the day (1-24) and the minute (1-60). • Prepaid accounting can be disabled for a specified profile index. The system supports the configuration of up to 16 profile indexes numbered 0 through 15
PLMN policy	The GGSN can be configured treat communications from unconfigured SGSNs in one of the following ways: • Treat the SGSN as if it is on a foreign PLMN • Treat the SGSN as if it is on a home PLMN • Reject communications from unconfigured SGSNs (default)
Ga Interface Configuration	
Ga interface name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the Ga interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.

Required Information	Description
Physical port description	An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical Ga interfaces.
Gateway IP address	Used when configuring static routes from the Ga interface(s) to a specific network.
GTPP Configuration	
Charging gateway address	The IP address of the system's GGSN interface.
CGF server information	**IP address**:The IP address of the CGF server to which the GGSN will send accounting information. Multiple CGFs can be configured.
	Priority:If more than on CGF is configured, this is the server's priority. It is used to determine the rotation order of the CGFs when sending accounting information. The priority can be configured to any integer value from 1 to 1000. The default is 1.
	Maximum number of messages:The maximum number of outstanding or unacknowledged GTPP messages allowed for the CGF. The maximum number can be configured to any integer value from 1 to 256. The default is 256.
GCDR optional fields	The following optional fields can be specified/configured in CDRs generated by the GGSN: • diagnostics • duration-ms (the time specified in the mandatory Duration field is reported in milliseconds) • local-record-sequence-number • plmn-id
Network Requested PDP Context Support Configuration (optional)	
Activation Requirements	**IP address**:The static IP address of the mobile station's for which network-requested PDP context activation will be supported. Up to 1000 addresses can be configured.
	Destination context name:The name of the destination context configured on the system that contains the IP address pool containing the mobile station's static address.
	International Mobile Subscriber Identity (IMSI): The IMSI of the mobile station.
	APN: The name of the access point that will be passed to the SGSN by the GGSN for the mobile station.
GSN-map node	Communications with the HLR from the GGSN go through a GSN-map node that performs the protocol conversion from GTPC to SS7. The IP address of the map node must be configured. Only one GSN-map node can be configured per source context.

Destination Context Configuration

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

Table 13. Required Information for Destination Context Configuration

Required Information	Description
Destination context name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. **NOTE:** For this configuration, the destination context name should **not** match the domain name of a specific APN.
APN Configuration	
APN name	An identification string by which the APN will be recognized by the system. The name can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots (.) and/or dashes (-). Multiple names are needed if multiple APNs will be used.
Accounting mode	Selects the accounting protocol. GTPP or RADIUS are supported. In addition, accounting can be completely disabled. The default is to perform accounting using GTPP. **NOTE:** The examples discussed in this chapter assumes GTPP is used.
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
APN charging characteristics (CC) (optional)	Specifies whether or not the GGSN accepts the CC from the SGSN for home, visiting, and roaming subscribers. By default the GGSN accepts the CC from the SGSN for all three scenarios. If the GGSN is to use its own CC for any of these scenarios, then each scenario requires the specification of behavior bits and a profile index to use. **NOTE:** The profile index parameters are configured as part of the GGSN service.
Domain Name Service (DNS) information (optional)	If DNS will be used for the APN, IP addresses can be configured for primary and secondary DNS servers.

IP address allocation method	Specifies how sessions facilitated by this APN will receive an IP address. IP addresses can be assigned using one of the following methods:
	• **Dynamic**: Address can be dynamically assigned from one of the sources:
	  • **Dynamic Host Control Protocol (DHCP) server**: The system can be configured to act as a DHCP proxy and receive address from the server in advance and assign them as needed or it can relay DHCP messages from the MS.
	  • **Local address pools** The system can be configured with local address pools.
	• **Static:** MS IP addresses can be permanently assigned.
	By default, the system is configured to either dynamically assign addresses from a local pool and/or allow static addresses.

IP address pool name	If addresses will be dynamically assigned from a locally configured private pool, the name of the pool must be configured. If no name is configured, the system will automatically use any configured public pool.
IP destination context name	The name of the system destination context to use for subscribers accessing the APN. When supporting Mobile IP, this is the name of the context containing the FA service configuration. If no name is specified, the system automatically uses the system context in which the APN is configured.
Maximum number of PDP contexts	The maximum number of PDP contexts that are supported for the APN.The maximum number can be configured to any integer value from 1 to 1000000. The default is 1000000.

Required Information	Description
PDP type	The maximum number of PDP contexts that are supported for the APN. The maximum number can be configured to any integer value from 1 to 1500000. The default is 1000000.
Verification selection mode	The level of verification that will be used to ensure a MS's subscription to use the APN. The GGSN uses any of the following methods: • No verification and MS supplies APN • No verification and SGSN supplies APN • Verified by SGSN (default)
Mobile IP Configuration	**Home Agent IP Address**: The IP address of an HA with which the system will tunnel subscriber Mobile IP sessions. Configuring this information tunnels all subscriber Mobile IP PDP contexts facilitated by the APN to the same HA unless an individual subscriber profile provides an alternate HA address. Parameters stored in individual profiles supersede parameters provided by the APN.
	Mobile IP Requirement: The APN can be configured to require Mobile IP for all sessions it facilitates. Incoming PDP contexts that do/can not use Mobile IP are dropped.
DHCP Interface Configuration (optional)	
DHCP interface name	An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the DHCP interface and be bound to the DHCP service. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Gateway IP address	Used when configuring static routes from the DHCP interface(s) to a specific network.
Physical port number	The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical DHCP interfaces.
DHCP Service Configuration (optional)	
DHCP Service Name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the DHCP service will be recognized by the system. Multiple names are needed if multiple GGSN services will be used.
DHCP Server Information	The IP address of each DHCP server that the system is to communicate with must be configured .Multiple servers can be configured. If multiple servers are configured, each can be assigned a priority from 1 to 1000. The default priority is 1.

Required Information	Description
Lease Duration	Specifies the minimum and maximum allowable lease times that are accepted in responses from DHCP servers. • **Minimum Lease Time**: Measured in seconds and can be configured to any integer value from 600 to 3600. The default is 600 seconds. • **Maximum Lease Time**: Measured in seconds and can be configured to any integer value from 10800 to 4294967295. The default is 86400 seconds.
AAA Interface Configuration	
AAA interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	
RADIUS Authentication server	**IP Address**:Specifies the IP address of the RADIUS authentication server the system will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. If multiple servers are configured, each can be assigned a priority.
	Shared Secret:The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number:Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
RADIUS Accounting server (optional)	**IP Address**: Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured.RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number:Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.

Required Information	Description
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.
Gi Interface Configuration	
Gi interface name	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Gi interfaces.
Gateway IP address(es)	Used when configuring static routes from the Gi interface(s) to a specific network.
IP Address Pool Configuration	
IP address pool name(s)	his is an identification string from 1 to 31 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used.
Pool addresses, subnet mask and type	The pool can consist of either of the following: • An entire subnet configured using the initial address and the subnet mask • A range of addresses configured using the first and last IP addresses in the range The pool can be configured as public, private, or static. Public pools can also be assigned a priority.

Mobile IP Destination Context Configuration

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

Table 14. Required Information for Mobile IP Destination Context Configuration

Required Information	Description

Required Information	Description
Mobile IP Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the Mobile IP destination context will be recognized by the system. **NOTE:** For this configuration, the destination context name should **not** match the domain name of a specific domain. It should, however, match the name of the context in which the HA service is configured if a separate system is used to provide HA functionality.
ICC Interface Configuration	
ICC interface name	The intra-context communication (ICC) interface is configured to allow FA and HA services configured within the same context to communicate with each other. The ICC interface name is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. ICC interface(s) are configured in the same destination context as the FA and HA services.
IP address and subnet	These will be assigned to the ICC interface(s). Multiple addresses (at least one per service) on the same subnet will be needed to assign to the same ICC interface.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical ICC interfaces.
Gi Interface Configuration	
Gi interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. Gi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Gi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical Gi interfaces.
Gateway IP address(es)	Used when configuring static routes from the Gi interface(s) to a specific network.
IP Address Pool Configuration (optional)	

Required Information	Description
IP address pool name(s)	If IP address pools will be configured in the destination context(s), names or identifiers will be needed for them. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive.
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.
FA Service Configuration	
FA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the FA service will be recognized by the system .Multiple names are needed if multiple FA services will be used. FA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the FA service and the HA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Security Parameter Index (indices) Information	**HA IP address**: Specifies the IP address of the HAs with which the FA service communicates. The FA service allows the creation of a security profile that can be associated with a particular HA.
	Index: Specifies the shared SPI between the FA service and a particular HA. The SPI can be configured to any integer value between 256 and 4294967295.Multiple SPIs can be configured if the FA service is to communicate with multiple HAs.
	Secrets: Specifies the shared SPI secret between the FA service and the HA. The secret can be between 1 and 127 characters (alpha and/or numeric).An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default is hmac-md5.A hash-algorithm is required for each SPI configured.
FA agent advertisement lifetime	Specifies the time (in seconds) that an FA agent advertisement remains valid in the absence of further advertisements. The time can be configured to any integer value between 1 and 65535. The default is 9000.
Number of allowable unanswered FA advertisements	Specifies the number of unanswered agent advertisements that the FA service will allow during call setup before it will reject the session. The number can be any integer value between 1 and 65535. The default is 5.
Maximum mobile-requested registration lifetime allowed	Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node. The lifetime is expressed in seconds and can be configured between 1 and 65534. An infinite registration lifetime can be configured by disabling the timer. The default is 600 seconds.
Registration reply timeout	Specifies the amount of time that the FA service will wait for a Registration Reply from an HA. The time is measured in seconds and can be configured to any integer value between 1 and 65535. The default is 7.
Number of simultaneous registrations	Specifies the number of simultaneous Mobile IP sessions that will be supported for a single subscriber. The maximum number of sessions is 3. The default is 1. **NOTE**: The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address.

Required Information	Description
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The FA service can be configured to always require authentication or not. If not, the initial registration and de-registration will still be handled normally.
HA service Configuration	
HA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the HA service and the FA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations.The HA service can be configured as follows: • Always require authentication • Never require authentication **NOTE**: The initial registration and de-registration will still be handled normally) • Never look for mn-aaa extension • Not require authentication but will authenticate if mn-aaa extension present.
FA-to-HA Security Parameter Index Information	**FA IP address**: The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	Index: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is **hmac-md5**. A hash-algorithm is required for each SPI configured.
Mobile Node Security Parameter Index Information	**Index**: Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is **hmac-md5**. A hash-algorithm is required for each SPI configured.

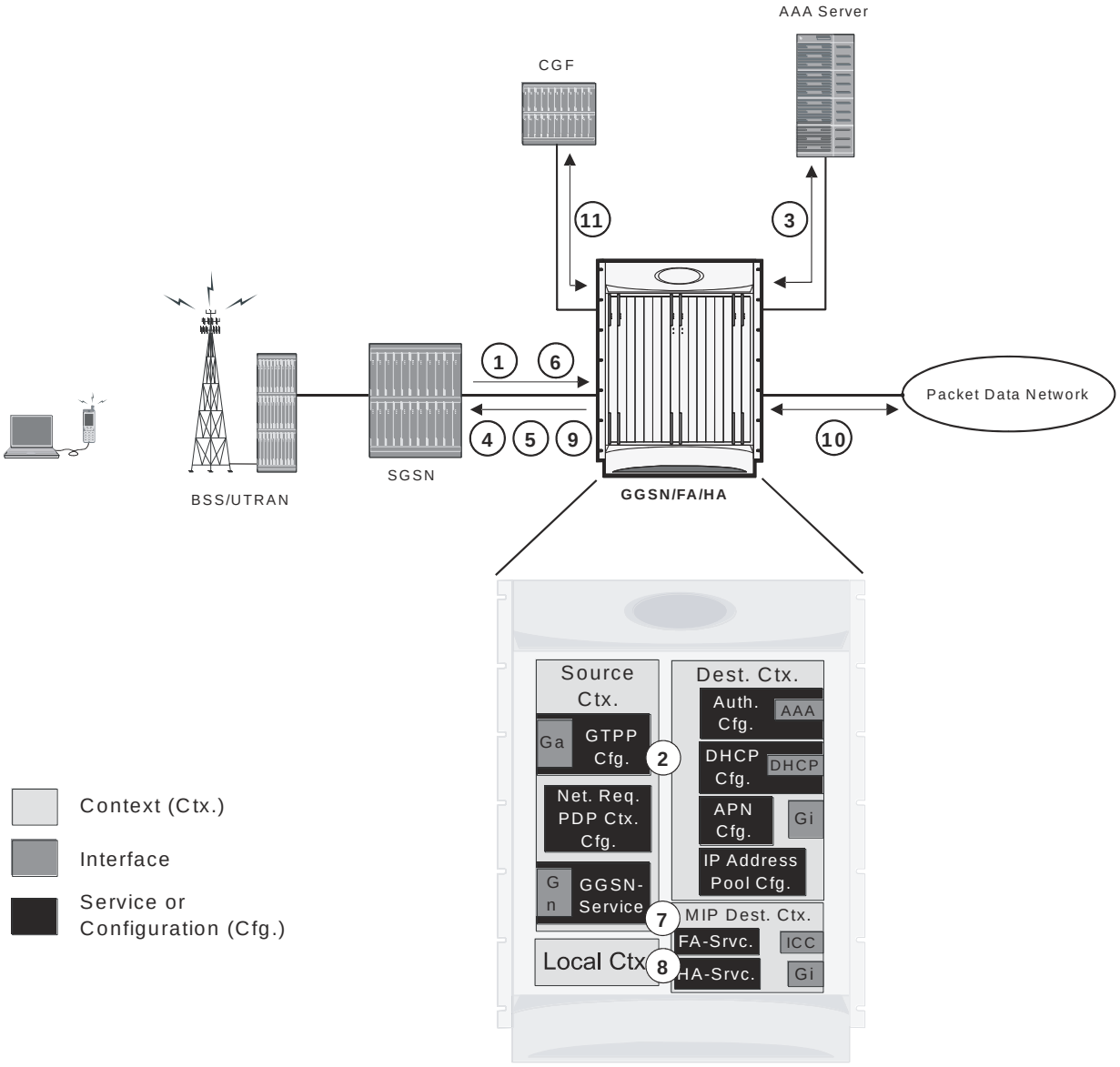
Required Information	Description
	Replay-protection process: Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds. A replay-protection process is required for each mobile node-to-HA SPI configured.
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.
Default Subscriber Configuration	
"Default" subscriber's IP context name	Specifies the name of the egress context on the system that facilitates the Gi interfaces. **NOTE**: For this configuration, the IP context name should be identical to the name of the destination context.

How This Configuration Works

This system configuration supports typical GGSN and Mobile IP functionality.

System operation for typical GGSN functionality behaves as described in *GGSN Configuration Example* chapter of this guide for each of the various call types. This section focusses on how this system configuration functions to process a Mobile IP session. The following figure and the text that follows describe how this configuration works to process calls

Figure 32. Call Processing When Using the System as a GGSN, FA, and HA



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN. In this case, it is determined that Mobile IP must be used. From the APM configuration, the system also determines the context in which the FA service is configured.
3. If subscriber authentication is required, the GGSN authenticates the subscriber by communicating with a RADIUS server over the AAA interface.
4. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface. The home address assigned to the mobile as part of the response is 0.0.0.0 indicating that it will be reset with a Home address after the PDP context activation procedure.

5. The FA component of the GGSN sends a Agent Advertisement message to the MS. The message contains the FA parameters needed by the mobile such as one or more card-of addresses. The message is sent as an IP limited broadcast message (i.e. destination address 255.255.255.255), however only on the requesting MS's TEID to avoid broadcast over the radio interface.
6. The MS sends a Mobile IP Registration request to the GGSN/FA. This message includes either the MS's static home address or it can request a temporary address by sending 0.0.0.0 as its home address. Additionally, the request must always include the Network Access Identifier (NAI) in a Mobile-Node-NAI Extension.
7. The FA forwards the registration request from the MS to the HA while the MS's home address or NAI and TEID are stored by the GGSN. The FA service communicates with the required HA service configured in the same context over the ICC interface. In response the HA sends a registration response to the FA containing the address assigned to the MS.
8. The FA extracts the home address assigned to the MS by the HA from the response and the GGSN updates the associated PDP context. The FA then forwards it to the MS (identified by either the home address or the NAI and TEID).
9. The GGSN issues a PDP context modification procedure to the SGSN in order to update the PDP address for the MS.
10. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
11. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

Chapter 6
GGSN Service Configuration Procedures

This chapter is meant to be used in conjunction with the previous chapter that describes the information needed to configure the system to support GGSN functionality for use in GPRS/UMTS networks.

It is recommended that you identify the options from the previous chapters that are required for your specific deployment. You can then use the procedures in this chapter to configure those options.

Procedures are provided for the following tasks:

- GGSN Service Configuration
- GTPP Accounting Support Configuration
- APN Configuration
- DHCP Service Configuration
- IP Address Pool Configuration on the System
- FA Services Configuration
- Common Gateway Access Support Configuration

IMPORTANT: At least one Packet Accelerator Card (PAC) or Packet Services Card (PSC) must be made active prior to service configuration. Information and instructions for configuring PACs/PSCs to be active can be found in the Configuring System Settings chapter of the System Administration Guide.

CAUTION: While configuring any base-service or enhanced feature, it is highly recommended to take care of conflicting or blocked IP addresses and port numbers for binding or assigning. In association with some service steering or access control features, like *Access Control List* configuration, use of inappropriate port number may result in communication loss. Refer respective feature configuration document carefully before assigning any port number or IP address for communication with internal or external network.

GGSN Service Configuration

GGSN services are configured within contexts and allow the system to function as a GGSN in the either a GPRS or UMTS wireless data network.

IMPORTANT: This section provides the minimum instruction set for configuring a GGSN service that allows the system to process PDP contexts. Commands that configure additional GGSN service properties are provided in the GGSN Service Configuration Mode Commands chapter of Command Line Interface Reference.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide*.

To configure the system to work as GGSN service:

Step 1 Create the GGSN service, local User Datagram Protocol (UDP) port for the Gn interfaces' IP socket, and bind it to an IP address by applying the example configuration in the *GGSN Service Creation and Binding* section.

Step 2 Associate the accounting context for the GGSN service and configure charging characteristic profile parameters for GGSN service by applying the example configuration in the *Accounting Context and Charging Characteristics Configuration* section.

Step 3 Configure the SGSN and PLMN related policy and session setup timeout for the GGSN service by applying the example configuration in the *SGSN and PLMN Policy Configuration* section.

Step 4 Optional. Configure the GGSN service to support network-requested PDP contexts by applying the example configuration in the *Network-requested PDP Context Support Configuration* section.

Step 5 Verify your GGSN configuration by following the steps in the *GGSN Configuration Verification* section.

Step 6 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

GGSN Service Creation and Binding

Use the following example to create the GGSN service and bind it to an IP address:

```
configure
      context <vpn_ctxt_name> -noconfirm
        ggsn-service <ggsn_svc_name>
          end
```

Notes:

- A maximum of 256 services (regardless of type) can be configured per system.
- Bind address should not conflict with any other GTP-based service.

Accounting Context and Charging Characteristics Configuration

Use the following example to configure a GTPP accounting context and charging characteristics parameters for GGSN service.

```
configure
      context <vpn_ctxt_name>
        ggsn-service <ggsn_svc_name>
          accounting context <aaa_ctxt_name>
          cc profile <cc_prof_index>
          end
```

Notes:

- Charging characteristics behavior and profile index can be configured for multiple CC profile indexes. For more options and keywords like **buckets**, **interval**, , **sgsns**, **tariff**, **volume** etc., refer cc profile section in Command Line Interface Reference.
- This command works in conjunction with the **cc-sgsn** command located in the APN configuration mode that dictates which CCs should be used for subscriber PDP contexts. Refer to the *APN Configuration* section in this chapter.

SGSN and PLMN Policy Configuration

Use the following example to configure the SGSN and PLMN related policy and session setup timeout for the GGSN service:

```
configure
      context <vpn_ctxt_name>
        ggsn-service <ggsn_svc_name>
          plmn id mcc <mcc_number> mnc <mnc_number> [primary]
          sgsn address <ip_address> / <subnet_mask>
          plmn unlisted-sgsn {foreign | home | reject]
          setup-timeout <dur_sec>
          end
```

Notes:

- SGSN or PLMN related policy can be defined for multiple SGSNs or PLMN.
- For optional configuration parameters of SGSN address, refer Command Line Interface Reference.

IMPORTANT: The GGSN only communicates with the SGSNs configured using this command unless a PLMN policy is enabled to allow communication with unconfigured SGSNs. PLMN policies are configured using the **plmn unlisted-sgsn** command.

Network-requested PDP Context Support Configuration

Use the following example to configure the GGSN to support the network-requested PDP context:

```
configure

      context <vpn_ctxt_name>

        network-requested-pdp-context activate <ip_address> dst-context
<dst_ctxt_name> imsi <imsi> apn <apn_name>

        network-requested-pdp-context gsn-map <ip_address>

        end
```

Notes:

- It is recommended that this functionality be configured in the system source context(s) along with the GGSN service(s).
- Up to 1000 IP address can be configured for network request PDP context support.
- Only one GSN-MAP node can be configured per system context.

GGSN Configuration Verification

Step 1 Verify that your GGSN services were created and configured properly by entering the following command in Exec Mode:

```
show ggsn-service name <ggsn_svc_name>}
```

The output of this command given below is a concise listing of GGSN service parameter settings as shown in the sample output displayed. In this example, a GGSN service called *ggsn1* was configured and you can observe some parameters configured as default.

```
Service name:                ggsn1

Context:                      ggsn1

Accounting Context Name: ggsn1
```

```
Bind:                     Done
Local IP Address:         192.168.70.1         Local IP Port: 2123
Self PLMN Id.:            MCC:  450, MNC:   06
Retransmission Timeout:   20 (secs)
Max Retransmissions:      4
Restart Counter:          16
Echo Interval:            60 (secs)
GTPU Echo Interval:       60 (secs)
GTPU Sequence Numbers:    Disabled
GTPU re-order:            Disabled
GTP re-order timeout:     100 (milliseconds)
Guard Interval:           100 (secs)
Setup Timeout:            60 (secs)
PLMN Policy:              Reject unlisted SGSN
Max IP sessions:          1000000
Max PPP sessions:         500000
Max sessions:             1000000
Service Status:           Started
Newcall Policy:           None
Session license limit:    OK
3GPP Qos to DSCP Mapping (for G-PDUs):
GTPC messages:            be
Conversational:           ef
    Streaming:                 af11
    Interactive (TP 1):        ef
    Interactive (TP 2):        af21
    Interactive (TP 3):        af21
    Background:                be
Charging Characteristics(CC) Profiles:
```

```
        Profile 0:
         Buckets: 4                          SGSN changes: 4
        Profile 1:
         Buckets: 4                          SGSN changes: 4
    SGSN Configuration List:
        sgsn address 2.2.2.2/32 mcc 111 mnc 999 description aaa-ggsn
```

Step 2 Verify configuration for errors by entering the following command in Exec Mode:

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

GTPP Accounting Support Configuration

This section provides instructions for configuring GTPP-based accounting for subscriber PDP contexts. GTPP-based accounting for a subscriber can be configured by CGF server configuration in a GTPP group. Additionally individual CGF server can be configured with this example.

IMPORTANT: To configure RADIUS and Diameter AAA functionality, refer *AAA Interface Administration and Reference*.

When the GTPP protocol is used, accounting messages are sent to the charging gateways (CGs) over the Ga interface. The Ga interface and GTPP functionality are typically configured within the system's source context. CDRs are generated according to the interim triggers configured using the charging characteristics configured for the GGSN, and a CDR is generated when the session ends.

GTPP version 2 is used by default. However, if version 2 is not supported by the CGF, the system reverts to using GTPP version 1. All subsequent CDRs are always fully-qualified partial CDRs. For CDR encoding different dictionaries are supported. For more information on GTPP dictionaries, refer AAA Interface Administration and Reference.

Whether or not the GGSN accepts charging characteristics from the SGSN can be configured on a per-APN basis based on whether the subscriber is visiting, roaming or, home.

By default, the GGSN always accepts the charging characteristics from the SGSN. However it accepts charging characteristics from RADIUS too, they must always be provided by the SGSN for GTPPv1 requests for primary and secondary PDP contexts.

If the system is configured to reject the charging characteristics from the SGSN, the GGSN can be configured with its own that can be applied based on the subscriber type (visiting, roaming, or home) at the APN level (refer to the *APN Configuration* section of this chapter for more information). GGSN charging characteristics consist of a profile index and behavior settings (refer to the *GGSN Service Configuration* section of this chapter for more information). The profile indexes specify the criteria for closing accounting records based specific criteria (refer to the *GGSN Service Configuration* section of this chapter for more information).

IMPORTANT: This section provides the minimum instruction set for configuring a GTPP accounting support in a GGSN service. Commands that configure additional GTPP accounting properties are provided in the *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in System Administration Guide and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the GTPP accounting support for a GGSN service:

Step 1 Create the GTPP group in accounting context by applying the example configuration in the *GTPP Group Creation* 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 *GTPP Group Configuration* section.

Step 3 Verify your GTPP group and accounting configuration by following the steps in the *GTPP Group Configuration Verification* section.

Step 4 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

GTPP Group Creation

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

```
configure
      context <vpn_ctxt_name>
        gtpp group <gtpp_group_name> -noconfirm
        end
```

Notes:

- In addition to one default GTPP group “default” a maximum of 8 GTPP groups can be configured with this command in a context.
- In case no GTPP group is configured in this context, system creates a default GTPP group named “default” and all the CGF servers and their parameters configured in this context are applicable to this “default” GTPP group.

GTPP Group Configuration

Use the following example to configure the GTPP server parameters, GTPP dictionary, and optionally CGF to support GTPP accounting:

```
configure
      context <vpn_ctxt_name>
        gtpp group <gtpp_group_name>
          gtpp charging-agent address <ip_address> [port <port>]
          gtpp server <ip_address> [max <msgs >] [priority <priority>]
          gtpp dictionary <dictionaries>
          gtpp max-cdrs <number_cdrs> [wait-time <dur_sec>]
          gtpp transport-layer {tcp | udp}
          end
```

Notes:

- In addition to one default GTPP group “default” a maximum of 8 GTPP groups can be configured with this command in a context.
- In case no GTPP group is configured in this context, system creates a default GTPP group named “default” and all the CGF servers and their parameters configured in this context are applicable to this “default” GTPP group.

- Command for CGF **gtpp charging-agent** is optional and configuring gtpp charging-agent on port 3386 may interfere with ggsn-service configured with the same ip address. Multiple interfaces can be configured within a single context if needed.
- For more information on GTPP dictionary encoding 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 **gtpp max-cdrs** command.
- Operator can select transport layer protocol as TCP or UDP for Ga interface with **gtpp transport-layer** command.
- 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.

GTPP Group Configuration Verification

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

```
show gtpp accounting servers
```

This command produces an output similar to that displayed below:

```
context: source
Preference IP               Port   Priority   State         Group
---------- --------------- ----- -------- ---------------- ----------
Primary   192.168.32.135    3386    1          Active        default
Primary   192.168.89.9      3386    100        Active        default
```

Step 2 Verify configuration for errors by entering the following command in Exec Mode:

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

APN Configuration

This section provides instructions for configuring the APN templates that are used to determine how PDP contexts should be processed. APNs are configured in system authentication contexts.

IMPORTANT: This section provides the minimum instruction set for configuring APNs in a GGSN service. Commands that configure additional APN properties are provided in APN Configuration Mode Commands chapter of Command Line Interface Reference.

These instructions assume that you have already configured the system level configuration as described in System Administration Guide and GGSN service as described in the GGSN Service Configuration section of this guide.

To configure the APN properties for a GGSN service:

Step 1 Create the APN in system context and specify the support of PDP contexts and selection mode by applying the example configuration in the APN Creation and Configuration section.

Step 2 Configure the authentication and accounting parameters in APN by applying the example configuration in the Authentication, Accounting, and GTPP Group Configuration in APN section.

Step 3 Configure the IP allocation method in APN by applying the example configuration in the IP Address Allocation Method Configuration in APN section.

Step 4 Optional. Configure the charging characteristics related parameters for the APN by applying the example configuration in the Charging Characteristics Parameter Configuration in APN section.

Step 5 Optional. Configure virtual APNs by applying the example configuration in the Virtual APN Configuration section.

Step 6 Optional. Configure other optional parameters for the APN by applying the example configuration in the Other Optional Parameter Configuration in APN section.

Step 7 Verify your APN configuration by following the steps in the APN Configuration Verification section.

Step 8 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

APN Creation and Configuration

Use the following example to create and configure the APNs:

```
configure
      context <vpn_ctxt_name>
        apn <apn_name> -noconfirm
          max-contexts primary <number> total <total_number>
          pdp-type {ipv4 [ipv6] | ipv6 [ipv4] | ppp}
          selection-mode {sent-by-ms | chosen-by-sgsn | subscribed}
```

```
ip context-name <dst_ctxt_name>
end
```

Notes:

- Up to 1000 APNs can be configured on a system.
- APN templates should be created/configured within system authentication contexts or destination context.
- Selection mode parameter's setting must be identical to the selection mode setting on the SGSN(s) that the GGSN communicates with. The GGSN rejects attempts to establish PDP contexts from any SGSN having a different setting.
- If the APN supports Mobile IP for subscriber PDP contexts, then ip context-name command is used to indicate the context in which the FA service is configured.
  - If no context name is specified, the system uses the context in which the APN is configured.
  - If Mobile IP is supported and no name is specified, the system uses the context in which the GGSN service facilitating the PDP context is located.

Authentication, Accounting, and GTPP Group Configuration in APN

This section describes the procedure to configure the authentication and accounting parameters for an APN. It also specify the procedure to attach a GTPP group with an APN.

Step 1 Configure the authentication and accounting parameters by applying the example configuration in the *Authentication and Accounting Configuration in APN* section.

Step 2 Attach a GTPP group with APN by applying the example configuration in the *GTPP Group Association to APN* section.

Authentication and Accounting Configuration in APN

Use the following example to configure the accounting mode and authentication parameter for APN:

```
configure
      context <dst_ctxt_name>
        apn <apn_name>
          accounting-mode {none | gtpp | radius [no-interims] [no-early-pdus]}
          default authentication
          end
```

Notes:

- APNs are configured in system authentication contexts or destination context.
- The authentication process varies depending on whether the PDP context is of type IP or PPP. The **authentication** command provides **msid-auth**, **msi-auth**, **msisdn-auth**, **allow-noauth**,

chap, mschap, and **pap** options. For more information on type of authentication, refer authentication section in APN Configuration Mode Commands chapter of Command Line Interface Reference.

GTPP Group Association to APN

After configuring GTPP group at context-level, an APN within the same context can be configured to use the user defined GTPP group.

Refer section GTPP Accounting Support Configuration for GTPP group configuration.

```
configure
      context <vpn_ctxt_name>
        apn <apn_name>
          gtpp group <gtpp_group_name> [accounting-context <aaa_ctxt_name>]
          end
```

Notes:

- GTPP group must be configured before associating with APN or "default" GTPP group can be used.

IP Address Allocation Method Configuration in APN

Use the following example to configure the IP address allocation method for APN:

IMPORTANT: Additional charging characteristics parameters are configurable as part of the GGSN service. Refer to the *GGSN Service Configuration* section of this chapter for more information.

```
configure
      context <dst_ctxt_name>
        apn <apn_name>
          ip address allocation-method {dhcp-proxy | dhcp-relay | local | no-
dynamic} [allow-user-specified]
          end
```

Notes:

- The process used by the system to determine how the address should be allocated. For detail information on IP address allocation, refer Usage section of **ip address allocation-method** command in *APN Configuration Mode Commands* chapter of Command Line Interface Reference.
- If DHCP-Proxy and DHCP-Relay method is selected for IP address allocation, a DHCP service must be configured on the system as described in *DHCP Service Configuration* section and specified the name of

DHCP Service by entering the **dhcp service-name** command as described in APN Configuration Mode Commands chapter of Command Line Interface Reference.

- If local pool is selected for IP address allocation, a local pool must be configured on the system as described in *IP Address Pool Configuration on the System* section and specified the name of a private IP address pool by entering the **ip address pool** command as described in APN Configuration Mode Commands chapter of Command Line Interface Reference.

Charging Characteristics Parameter Configuration in APN

Use the following example to configure the charging characteristics parameter for APN:

IMPORTANT: Additional charging characteristics parameters are configurable as part of the GGSN service. Refer to the *GGSN Service Configuration* section of this chapter for more information.

```
configure

      context <dst_ctxt_name>

        apn <apn_name>

          cc-sgsn {home-subscriber-use-GGSN | roaming-subscriber-use-GGSN |
visiting-subscriber-use-GGSN}+

          cc-home behavior <bit> profile <index>

          cc-roaming behavior <bit> profile <index>

          cc-visiting behavior <bit> profile <index>

        end
```

Notes:

- If multiple behavior bits are configured for a single profile index, the variable bits is achieved by “Or”ing the bit strings and converting the result to hexadecimal.

Example
If behavior bits 5 (0000 0001 0000) and 11 (0100 0000 0000) are both being assigned to profile index 5 for a home subscriber, the appropriate command is **cc-home behavior** *410* **profile** *5*.

Virtual APN Configuration

Virtual APNs are references (or links) to alternative APNs to be used for PDP context processing based on properties of the context. Use the following example to configure the virtual APNs.

```
configure

      context <dst_ctxt_name>
```

```
        apn <apn_name>

          virtual-apn preference <priority > apn <apn_name> {domain <domain_name
> | mcc <mcc_number> mnc <mnc_number> / roaming-mode {home | visiting | roaming}

          end
```

Notes:

- Up to 1023 references can be configured per APN. Additional information about “virtual” APNs and their operation can be found in the *Command Line Interface Reference*.

Other Optional Parameter Configuration in APN

Use the following example to configure various optional parameter for APN:

```
configure

      context <dst_ctxt_name>

        apn <apn_name>

          dns {primary | secondary} {<dns_ip_address>}

          mobile-ip required

          mobile-ip home-agent <ha_ip_address>

          ip source-violation {ignore | check [drop-limit <limit>]} [exclude-
from-accounting]

          restriction-value <value>

          timeout {absolute | idle | qos-renegotiate} <timeout_dur>

          timeout long-duration <ldt_dur> [inactivity-time <inact_dur>]

          long-duration-action detection

          long-duration-action disconnection [suppress-notification] [dormant-
only] +

          end
```

Notes:

- Mobile is supported for IP PDP contexts only. Mobile IP configuration attributes returned as part of a successful authentication during the GTP authentication phase (for non-transparent IP PDP contexts) supersede the APN configuration. Any attributes returned during the FA authentication phase are ignored.
- If mobile-ip required option is enabled, the system deletes any PDP context using the APN that can not establish a Mobile IP session.

APN Configuration Verification

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

show apn all

This command produces an output similar to that displayed below is an excerpt from a sample output. In this example, an APN called apn1 was configured.

```
access point name (APN):   apn1
authentication context:     test
pdp type:  ipv4
Selection Mode:  subscribed
ip source violation:  Checked              drop limit:  10
accounting mode: gtpp                      No early PDUs: Disabled
max-primary-pdp-contexts:  1000000         total-pdp-contexts:  1000000
primary contexts: not available            total contexts: not available
local ip:  0.0.0.0
primary dns:  0.0.0.0                      secondary dns:  0.0.0.0
ppp keep alive period :  0                 ppp mtu :  1500
absolute timeout :  0                      idle timeout :  0
long duration timeout:  0                  long duration
action:  Detection
ip header compression:  vj
data compression:  stac mppc deflate       compression mode:  normal
min compression size:  128
ip output access-group:                    ip input access-group:
ppp authentication:
allow noauthentication:  Enabled           imsi authentication:Disabled
```

Step 2 Verify configuration for errors in APN configuration by entering the following command in Exec Mode:

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

DHCP Service Configuration

The system can be configured to use the Dynamic Host Control Protocol (DHCP) to assign IP addresses for PDP contexts. IP address assignment using DHCP is done using one of two methods as configured within an APN:

- **DHCP-proxy**: The system acts as a proxy for client (MS) and initiates the DHCP Discovery Request on behalf of client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS. This allocated address must be matched with the an address configured in an IP address pool on the system. This complete procedure is not visible to MS.

  As the number of addresses in memory decreases, the system solicits additional addresses from the DHCP server. If the number of addresses stored in memory rises above the configured limit, they are released back to the DHCP server.
- **DHCP-relay**: The system acts as a relay for client (MS) and forwards the DHCP Discovery Request received from client (MS). Once it receives an allocated IP address from DHCP server in response to DHCP Discovery Request, it assigns the received IP address to the MS.

Regardless of the DHCP method, there are parameters that must first be configured that specify the DHCP servers to communicate with and how the IP address are handled. These parameters are configured as part of a DHCP service.

IMPORTANT: This section provides the minimum instruction set for configuring a DHCP service on system for DHCP-based IP allocation. For more information on commands that configure additional DHCP server parameters and working of these commands, refer DHCP Service Configuration Mode Commands chapter of Command Line Interface Reference.

These instructions assume that you have already configured the system level configuration as described in System Administration Guide and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the DHCP service:

Step 1 Create the DHCP service in system context and bind it by applying the example configuration in the *DHCP Service Creation* section.

Step 2 Configure the DHCP servers and minimum and maximum allowable lease times that are accepted in responses from DHCP servers by applying the example configuration in the *DHCP Server Parameter Configuration* section.

Step 3 Verify your DHCP Service configuration by following the steps in the *DHCP Service Configuration Verification* section.

Step 4 Save your configuration as described in the*Verifying and Saving Your Configuration* chapter.

DHCP Service Creation

Use the following example to create the DHCP service to support DHCP-based address assignment:

```
configure
      context <dest_ctxt_name>
```

```
        dhcp-service <dhcp_svc_name>

          bind address <ip_address> [nexthop-forwarding-address
<nexthop_ip_address> [mpls-label input <in_mpls_label_value> output
<out_mpls_label_value1> [out_mpls_label_value2]]]

          end
```

Notes:

- To ensure proper operation, DHCP functionality should be configured within a destination context.
- Optional keyword **nexthop-forwarding-address** *<nexthop_ip_address>* **[mpls-label input** *<in_mpls_label_value>* **output** *<out_mpls_label_value1>* **[** *out_mpls_label_value2* **]]** applies DHCP over MPLS traffic.

DHCP Server Parameter Configuration

Use the following example to configure the DHCP server parameters to support DHCP-based address assignment:

```
configure

      context <dest_ctxt_name>

        dhcp-service <dhcp_svc_name>

          dhcp server <ip_address> [priority <priority>

          dhcp server selection-algorithm {first-server | round-robin}

          lease-duration min <minimum_dur> max <max_dur>

          dhcp deadtime <max_time>

          dhcp detect-dead-server consecutive-failures <max_number>

          max-retransmissions <max_number>

          retransmission-timeout <dur_sec>

          end
```

Notes:

- Multiple DHCP can be configured by entering **dhcp server** command multiple times. A maximum of 20 DHCP servers can be configured.
- The **dhcp detect-dead-server** command and **max-retransmissions** command work in conjunction with each other.
- The retransmission-timeout command works in conjunction with **max-retransmissions** command.

DHCP Service Configuration Verification

Step 1 Verify that your DHCP servers configured properly by entering the following command in Exec Mode:

```
show dhcp service all
```

This command produces an output similar to that displayed below where DHCP name is *dhcp1*:

```
Service name:                dhcp1
Context:                     isp
Bind:                        Done
Local IP Address:            150.150.150.150
Service Status:              Started
Retransmission Timeout:      3000 (milli-secs)
Max Retransmissions:         2
Lease Time:                  600 (secs)
Minimum Lease Duration:      600 (secs)
Maximum Lease Duration:      86400 (secs)
DHCP Dead Time:              120 (secs)
DHCP Dead consecutive Failure:5
DHCP T1 Threshold Timer:     50
DHCP T2 Threshold Timer:     88
DHCP Client Identifier:      Not Used
DHCP Algorithm:              Round Robin
DHCP Servers configured:
 Address: 150.150.150.150    Priority: 1
Next Hop Address:            192.179.91.3
MPLS-label:
     Input:                  5000
     Output:                 1566  1899
```

Step 2 Verify the DHCP service status by entering the following command in Exec Mode:

```
show dhcp service status
```

IP Address Pool Configuration on the System

Before an MS is able to access data services, they must have an IP address. As described previously, the GGSN supports static or dynamic addressing (through locally configured address pools on the system, DHCP client-mode, or DHCP relay-mode). Regardless of the allocation method, a corresponding address pool must be configured.

IP addresses can be dynamically assigned from a single pool/a group of IP pools/a group of IP pool groups. The addresses/IP pools/ IP pool groups are placed into a queue in each pool or pool group. An address is assigned from the head of the queue and, when released, returned to the end. This method is known as least recently used (LRU).

When a group of pools have the same priority, an algorithm is used to determine a probability for each pool based on the number of available addresses, then a pool is chosen based on the probability. This method, over time, allocates addresses evenly from the group of pools.

IMPORTANT: Setting different priorities on each individual pool can cause addresses in some pools to be used more frequently.

IMPORTANT: This section provides the minimum instruction set for configuring local IP address pools on the system. For more information on commands that configure additional parameters and options, refer ip pool command section in *Context Configuration Mode Commands* chapter of *Command Line Interface Reference*.

These instructions assume that you have already configured the system level configuration as described in System Administration Guide and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the IP pool:

Step 1 Create the IP pool for IPv4 addresses in system context by applying the example configuration in the *IPv4 Pool Creation* section.

Step 2 Optional. Configure the IP pool for IPv6 addresses in system context by applying the example configuration in the *IPv6 Pool Creation* section.

Step 3 Verify your IP pool configuration by following the steps in the *IP Pool Configuration Verification* section.

Step 4 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

IPv4 Pool Creation

Use the following example to create the IPv4 address pool:

```
configure

      context <dest_ctxt_name>

        ip pool <pool_name> <ip_address/mask> [{private| public}[priority]] |
static]

        end
```

Notes:

- To ensure proper operation, IP pools should be configured within a destination context.
- Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, the number of pools may need to be limited depending on the number of addresses to be configured and the number of PACs/PSCs installed.
- Setting different priorities on individual pools can cause addresses in some pools to be used more frequently.
- For more information on commands/keywords that configure additional parameters and options, refer ipv6 pool command section in Context Configuration Mode Commands chapter of Command Line Interface Reference.

IPv6 Pool Creation

Use the following example to create the IPv6 address pool:

```
configure

      context <dest_ctxt_name>

        ipv6 pool <pool_name> 6to4 local-endpoint
<ip_address>[private][public][shared][static]

        end
```

Notes:

- To ensure proper operation, IP pools should be configured within a destination context.
- Each address in the pool requires approximately 24 bytes of memory. Therefore, in order to conserve available memory, the number of pools may need to be limited depending on the number of addresses to be configured and the number of PACs/PSCs installed.
- Setting different priorities on individual pools can cause addresses in some pools to be used more frequently.
- For more information on commands/keywords that configure additional parameters and options, refer ipv6 pool command section in Context Configuration Mode Commands chapter of Command Line Interface Reference.

IP Pool Configuration Verification

Step 1 Verify that your IPv4 address pool configured properly by entering the following command in Exec Mode:

```
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
RG00  pool3      30.30.0.0        255.255.0.0          0        65534
SG00  pool2      20.20.0.0        255.255.0.0          10       65524
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
```

Step 2 Verify that your IPv6 address pools configured properly by entering the following command in Exec Mode:

```
show ipv6 pools
```

The output from this command should look similar to the sample shown above except IPv6 addresses.

FA Services Configuration

FA services are configured within contexts and allow the system to function as an FA in the 3G wireless data network.

IMPORTANT: This section provides the minimum instruction set for configuring an FA service that allows the system to process data sessions. Commands that configure additional FA service properties are provided in the Command Line Interface Reference. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations*.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the FA service:

Step 1 Create the FA service in the system context created to facilitate FA service by applying the example configuration in the *FA Service Creation* section.

Step 2 Bind the configured FA service to a local IP address interface with UDP port and specify the maximum number of subscribers that can access this service for the Pi interfaces' IP socket by applying the example configuration in the *IP Interface and UDP Port Binding for Pi Interface* section.

Step 3 Configure the security parameter index (SPI) between FA service and HA by applying the example configuration in the *Security Parameter Index (SPI) Configuration* section.

Step 4 Specify the FA agent advertisement related parameters like lifetime, number of advertisements, and registration lifetime by applying the example configuration in the *FA Agent Advertisement Parameter Configuration* section.

Step 5 Configure the number of registration per subscriber, authentication procedure, and registration timeout parameters for this FA service by applying the example configuration in the *Subscriber Registration, Authentication and Timeout Parameter Configuration* section.

Step 6 Optional. Configure the FA service for controlling the negotiation and sending of the I-bit in revocation messages by applying the example configuration in the *Revocation Message Configuration* section.

Step 7 Verify your FA service configuration by following the steps in the *FA Service Configuration Verification* section.

Step 8 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

FA Service Creation

Use the following example to create the FA service:

IMPORTANT: A maximum of 256 services (regardless of type) can be configured per system.

```
configure
      context <fa_ctxt_name> -noconfirm
        fa-service <fa_svc_name> -noconfirm]
```

```
end
```

Notes:

- <*fa_ctxt_name*> is name of the context to use for FA service configuraiton. Generally FA should be configured within a destination context.
- <*fa_svc_name*> is name of the FA service where other parameters have to configure for FA functionality.

IP Interface and UDP Port Binding for Pi Interface

Use the following example to bind the FA service to an local IP interface and specify the maximum number of subscribers that can access this service. Binding an interface to the FA service causes the interface to take on the characteristics of a Pi interface.

```
configure
      context <fa_ctxt_name>
        fa-service <fa_svc_name>
          bind address <fa_ip_address> max-subscribers <max_subs>
          ip local-port <udp_port_num>
          end
```

Notes:

- <*fa_svc_name*> is name of the FA service which is created to configure FA functionality.
- <*fa_ip_address*> is the local IP address in IPv4/IPv6 notation for providing Pi interfae characteristics.
- <*max_subs*> is the maximum number of subscribers that can access this service on this interface. This can be configured to any integer value from 0 to 500,000. The default is 500,000.

  IMPORTANT: The maximum number of subscribers supported is dependant on the session capacity license installed and the number of active PACs/PSCs installed in the system. For more information on session capacity license, refer to the Software Management Operations chapter of the System Administration Guide.

- <*udp_port_num*> is the UDP port number from 1 through 65535 to be used for Pi interface. Default port number is 434.
- For more information on commands/keywords that configure additional parameters and options, refer *FA Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

Security Parameter Index (SPI) Configuration

Use the following example to configure the security parameter index (SPI) between FA service and HA:

IMPORTANT: A maximum of 2048 FA-HA SPIs can be configured for a single FA service.

```
configure

      context <fa_ctxt_name>

        fa-service <fa_svc_name>

          fa-ha-spi remote-address <ha_ip_address> spi-number <spi_num>
{encrypted secret <enc_secret_key> | secret <secret_key>}  [description
<desc_string>]

          end
```

Notes:

- <*fa_svc_name*> is name of the FA service which is created to configure FA functionality.
- <*ha_ip_address*> is the IP address in IPv4/IPv6 notation of HA to which this FA service will interact.
- <*spi_num*> specifies the SPI number which indicates a security context between the FA and the HA in accordance with RFC 2002 amd can be configured to any integer value from 256 through 4294967295.
- <*enc_secret_key*> specifies the encrypted shared key between the FA and the HA services. It must be from 1 to 127 alpha and/or numeric characters and is case sensitive.

  IMPORTANT: The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the **secret** keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

- <*secret_key*> specifies the secret shared key between the FA and the HA services. It must be from 1 to 127 alpha and/or numeric characters and is case sensitive.
- <*desc_string*> is the description for this SPI and must be from 1 to 31 alpha and/or numeric characters.
- For more information on commands/keywords that configure additional parameters and options, refer FA Service Configuration Mode Commands chapter of Command Line Interface Reference.

FA Agent Advertisement Parameter Configuration

Use the following example to configure the agent advertisement parameters for this FA service:

```
configure

      context <fa_ctxt_name>

        fa-service <fa_svc_name>

          advertise adv-lifetime <advt_dur>

          advertise num-adv-sent <advt_num>
```

```
advertise reg-lifetime <reg_dur>

end
```

Notes:

- <*fa_svc_name*> is name of the FA service which is created to configure FA functionality.
- <*advt_dur*> is the amount of time that an FA agent advertisement remains valid in the absence of further advertisements. It is measured in seconds and can be configured to any integer value from 1 to 65535. The default is 9000.
- <*advt_num*> is the number of unanswered agent advertisements that the FA service allows during call setup before it rejects the session. It can be any integer value from 1 to 65535. The default is 3.
- <*reg_dur*> specify the longest registration lifetime that the FA service allows in any Registration Request message from the mobile node. It is measured in seconds and can be configured to any integer value from 1 to 65534. The default is 600.

Subscriber Registration, Authentication and Timeout Parameter Configuration

Use the following example to configure the number of subscriber registration, authentication procedure and registration timeout parameters for this FA service:

```
configure

      context <fa_ctxt_name>

        fa-service <fa_svc_name>

          multiple-reg <reg_num>

          reg-timeout <timeout_dur>

          authentication mn-aaa {always | ignore-after-handoff | init-reg |
init-reg-except-handoff | renew-and-dereg-noauth | renew-reg-noauth} [optimize-
retries]

          end
```

Notes:

- <*fa_svc_name*> is name of the FA service which is created to configure FA functionality.
- <*reg_num*> is the number of simultaneous Mobile IP sessions that are to be supported for a single subscriber. It can be configured to any integer value from 1 to 3. The default value is 1.

> ***IMPORTANT:*** The system supports multiple Mobile IP sessions per subscriber only if the subscriber's mobile node has a static IP address. The system only allows a single Mobile IP session for mobile nodes that receive a dynamically assigned home IP address.
>
> ***IMPORTANT:*** In addition, because only a single Mobile IP or proxy-Mobile IP session is supported for IP PDP contexts, this parameter must remain at its default configuration.

- *<timeout_dur>* is the maximum amount of time that the FA service waits for a Registration Rely message from the HA. It is measured in seconds and can be configured to any integer value from 1 to 65535. The default value is 45.
- For more information on authentication mn-aaa commands/keywords that configure additional parameters and options, refer FA Service Configuration Mode Commands chapter of Command Line Interface Reference.

Revocation Message Configuration

Use the following example to configure the FA service for controlling the negotiation and sending of the I-bit in revocation messages:

```
configure
      context <fa_ctxt_name>
        fa-service <fa_svc_name>
          revocation negotiate-i-bit
          end
```

Notes:

- By default the system will not send the I-bit in the revocation message.

FA Service Configuration Verification

Step 1 Verify that your FA service is configured properly by entering the following command in Exec Mode:

```
show fa-service all
```

The output from this command should look similar to the sample shown below. In this example an FA service named fa1 was configured in the isp1 context.

```
Service name:       fa1
   Context:          isp1
   Bind:             Done               Max Subscribers:      500000
   Local IP Address: 195.20.20.3        Local IP Port         434
   Lifetime:         00h10m00s          Registration Timeout: 45 (secs)
   Advt Lifetime     02h30m00s          Advt Interval:        5000 (msecs)
   Num Advt:         5
```

```
   Advt Prefix Length Extn: NO
   Reverse Tunnel:    Enabled            GRE Encapsulation:     Enabled
SPI(s):
  FAHA: Remote Addr: 195.30.30.3/32
   Hash Algorithm:    HMAC_MD5           SPI Num:  1000
   Replay Protection: Timestamp          Timestamp Tolerance: 60
IPSEC Crypto Map(s):
   Peer HA Addr:          195.30.30.2
      Crypto Map:         test
   Registration Revocation:    Enabled   Reg-Revocation I bit:   Enabled
   Reg-Revocation Max Retries: 3         Reg-Revocation Timeout: 3 (secs)
   Reg-Rev on InternalFailure: Enabled
```

Step 2 Verify configuration for errors in FA service by entering the following command in Exec Mode:

show configuration errors section fa-service verbose

Common Gateway Access Support Configuration

This section describes some advance feature configuration to support multiple access networks (CDMA, eHRPD and LTE) plus a GSM/UMTS for international roaming with the same IP addressing behavior and access to 3GPP AAA for subscriber authorization. Subscribers using static IP addressing will be able to get the same IP address regardless of the access technology.

This configuration combines 3G and 4G access technologies in a common gateway supporting logical services of HA, PGW, and GGSN to allow their customers to have the same user experience, independent of the access technology available.

IMPORTANT: This feature is a license-enabled support and you may need to install a feature specific session license on your system to use some commands related to this configuration.

These instructions assume that you have already configured the system level configuration as described in *System Administration Guide* and GGSN service as described in *GGSN Service Configuration* section of this chapter.

To configure the S6b and other advance features:

Step 1 Configure Diameter endpoint by applying the example configuration in the *Diameter Endpoint Configuration* section.

Step 2 Create or modify AAA group by applying the example configuration in the *AAA Group Configuration* section.

Step 3 Modify GGSN service to allow authorization with HSS by applying the example configuration in the *Authorization over S6b Configuration* section.

Step 4 *Optional*. Create and associate DNS client parameters by applying the example configuration in the *DNS Client Configuration* section.

Step 5 *Optional*. Modify GGSN service to accept duplicate calls when received with same IP address by applying the example configuration in the *Duplicate Call Accept Configuration* section.

Step 6 Verify your S6b configuration by following the steps in the *Common Gateway Access Support Configuration Verification* section.

Step 7 Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Diameter Endpoint Configuration

Use the following example to configure the Diameter endpoint:

```
configure
  context <ggsn_ctxt_name> -noconfirm
    diameter endpoint <s6b_endpoint_name>
      origin host <host_name> address <ip_address>
       peer <peer_name> realm <realm_name> address <ip_address> port <port_num>
```

```
    end
```

Notes:

- <*ggsn_ctxt_name*> is name of the context which contains GGSN service on system.

AAA Group Configuration

Use the following example create/modify the AAA group for this feature.

```
configure
  context <fa_ctxt_name>
    aaa group <aaa_grp_name>
      diameter authentication dictionary aaa-custom15
      diameter authentication endpoint <s6b_endpoint_name>
      diameter authentication server <server_name> priority <priority>
      end
```

Notes:

- <*s6b_endpoint_name*> is name of the existing Diamtere endpoint.

Authorization over S6b Configuration

Use the following example to enable the S6b interface on GGSN service with 3GPP AAA/HSS:

```
configure
  context <ggsn_ctxt_name>
    ggsn-service <ggsn_svc_name>
      plmn-unlisted-sgsn home
      authorize-with-hss
      fqdn host <host_name> realm <realm_name>
      end
```

Notes:

- <*ggsn_svc_name*> is name of the GGSN service which is already created on the system.

DNS Client Configuration

Use the following example to enable the S6b interface on GGSN service with 3GPP AAA/HSS:

```
configure
  context <ggsn_ctxt_name>
     ip domain-lookup
     ip name-servers <ip_address/mask>
     dns-client <dns_name>
       bind address <ip_address>
       resolver retransmission-interval <duration>
       resolver number-of-retries <retrie>
       cache ttl positive <ttl_value>
       exit
    ggsn-service <ggsn_svc_name>
       default dns-client context
       end
```

Notes:

- <*ggsn_svc_name*> is name of the GGSN service which is already created on the system.

Duplicate Call Accept Configuration

Use the following example to configure GGSN service to accept the duplicate session calls with request for same IP address:

```
configure
  context <ggsn_ctxt_name>
    ggsn-service <ggsn_svc_name>
      newcall duplicate-subscriber-requested-address accept
      end
```

Notes:

- <*ggsn_svc_name*> is name of the GGSN service which is already created on the system.

Common Gateway Acces Support Configuration Verification

Step 1 Verify that your common gateway access supprot is configured properly by entering the following command in Exec Mode:

```
show ggsn-service all
```

The output from this command should look similar to the sample shown below. In this example GGSN service named *GGSN1* was configured in the *vpn1* context.

```
Service name:           ggsn1
Context:                cn1
Associated PGW svc:      None
Associated GTPU svc:     None
Accounting Context Name:cn1
dns-client Context Name:cn1
Authorize:              hss
Fqdn-name:              xyz.abc@starent.networks.com
Bind:                   Not Done
Local IP Address:       0.0.0.0          Local IP Port:          2123
Self PLMN:              Not defined
Retransmission Timeout: 5 (secs)
```

Chapter 7
Verifying and Saving Your Configuration

This chapter describes how to save the system configuration.

Verifying the Configuration

You can use a number of command 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, specific features are set and need to be verified. Examples include APN and IP address pool configuration. Using these examples, enter the following commands to verify proper feature configuration:

show apn all

The output displays the complete configuration for the APN. In this example, an APN called apn1 is configured.

```
access point name (APN): apn1

authentication context: test

pdp type: ipv4

Selection Mode: subscribed

ip source violation: Checked drop limit: 10

accounting mode: gtpp No early PDUs: Disabled

max-primary-pdp-contexts: 1000000 total-pdp-contexts: 1000000

primary contexts: not available total contexts: not available

local ip: 0.0.0.0

primary dns: 0.0.0.0 secondary dns: 0.0.0.0

ppp keep alive period : 0 ppp mtu : 1500

absolute timeout : 0 idle timeout : 0

long duration timeout: 0 long duration action: Detection

ip header compression: vj

data compression: stac mppc deflate compression mode: normal

min compression size: 128

ip output access-group: ip input access-group:

ppp authentication:

allow noauthentication: Enabled imsi

 authentication:Disabled
```

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: Many features can be configured on the system. There are show commands specifically for these features. Refer to the *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 : egtp1

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 SPC's/SMC's CompactFlash or on an installed PCMCIA memory card on the SPC/SMC. Files that are saved to a remote network node can be transmitted using either 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]
```

Keyword/Variable	Description
url	Specifies the path and name to which the configuration file is to be stored. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats: • **{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **file:/{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **tftp://**{ *ipaddress*|*host_name*[*:port#*]} [*/directory*] */file_name* • **ftp://**[*username*[*:pwd*] *@*] { *ipaddress*|*host_name*} [*:port#*] [*/directory*] */file_name* • **sftp://**[*username*[:*pwd*] *@*] { *ipaddress*|*host_name*} [*:port#*] [*/directory*] */file_name* **/flash** corresponds to the CompactFlash on the SPC/SMC. **/pcmcia1** corresponds to PCMCIA slot 1. **/pcmcia2** corresponds to PCMCIA slot 2. *ipaddress* is the IP address of the network server. *host_name* is the network server's *hostname*. *port#* is the network server's logical port number. Defaults are: • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data Note: *host_name* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserv er.dx *username* is the username required to gain access to the server if necessary. *password* is the password for the specified username if required. */directory* specifies the directory where the file is located if one exists. */file_name* specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.
-redundant	Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the url variable, and then automatically copy that same file to the like device on the Standby SPC/SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SPCs/SMCs. For example, if you save the file to the /pcmcia1 device on the active SPC/SMC, that same type of device (a PC-Card in Slot 1 of the standby SPC/SMC) must be available. Otherwise, a failure message is displayed. Note: If saving the file to an external network (non-local) device, the system disregards this keyword.

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 causes the CLI configuration file to be saved with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies that every parameter that is being saved to the new configuration file should be displayed.

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 SPC/SMC, then you must synchronize the local file system on both SPCs/SMCs.

To save a configuration file called system.cfg to a directory that was previously created called cfgfiles on the SPC's/SMC's CompactFlash, 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 8
Monitoring the Service

This chapter provides information for monitoring service status and performance using the **show** commands through the Command Line Interface (CLI).

These command have many related keywords that allow them to provide useful information on all aspects of the system ranging from current software configuration through call activity and status.

The selection of keywords described in this chapter is intended to provided the most useful and in-depth information for monitoring the system. For additional information on these and other **show** command keywords, refer to the *Command Line Interface Reference*.

In addition to the CLI, the system supports the sending of Simple Network Management Protocol (SNMP) traps that indicate status and alarm conditions. Refer to the *SNMP MIB Reference Guide* for a detailed listing of these traps.

Monitoring System Status and Performance

This section contains commands used to monitor the status of tasks, managers, applications and other software components in the system.

Output descriptions for most of the commands are located in the *Statistics and Counters Reference*.

Table 15. System Status and Performance Monitoring Commands

To do this:	Enter this command:
View Subscriber Information	
Display Session Resource Status	
View session resource status	**show resources session**
Display Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	**show subscribers configuration username** *subscriber_name*
View remotely configured subscriber profile settings	**show subscribers aaa-configuration username** *subscriber_name*
View Subscribers Currently Accessing the System	
View a listing of subscribers currently accessing the system	**show subscribers all**
View information for all ggsn-only subscriber sessions	show subscribers ggsn-only all
View information for a specific subscriber	**show subscribers full username** *username*
View Subscriber Counters	
View counters for a specific subscriber	**show subscribers counters username** *subscriber_name*
View Recovered Session Information	
View session state information and session recovery status	**show subscriber debug-info { callid | msid | username }**
View Session Statistics and Information	
Display Historical Session Counter Information	
View all historical information for all sample intervals	**show session counters historical**
Display Session Duration Statistics	
View session duration statistics	**show session duration**
Display Session State Statistics	
View session state statistics	**show session progress**

To do this:	Enter this command:
Display Session State PCF Statistics	
View session state PCF statistics	**show session progress pcf all**
Display Session Subsystem and Task Statistics ***IMPORTANT:*** Refer to the *System Software Task and Subsystem Descriptions* of the *System Administration Guide* for additional information on the Session subsystem and its various manager tasks.	
View AAA Manager statistics	**show session subsystem facility aaamgr all**
View FA Manager statistics	**show session subsystem facility famgr all**
View GTPC Manager statistics	**show session subsystem facility gtpcmgr all**
View L2TP demux manager statistics	**show session subsystem facility l2tpdemux all**
View L2TP Manager statistics	**show session subsystem facility l2tpmgr all**
View Session Manager statistics	**show session subsystem facility sessmgr all**
Display Session Disconnect Reasons	
View session disconnect reasons with verbose output	**show session disconnect-reasons**
View Point-to-Point Protocol Statistics	
Display a Summary of PPP Counter Status	
View cumulative subscriber session PPP counters	**show ppp**
Display PPP Counters for a Specific Subscriber	
View individual subscriber session PPP counters	**show ppp username** *subscriber_name*
View individual subscriber session PPP error and data counters	**show ppp counters username** *subscriber_name*
View individual subscriber session detailed PPP counters	**show ppp full username** *subscriber_name*
View Mobile IP Foreign Agent Statistics	
Display Mobile IP FA Information for a Specific Subscriber	
View Mobile IP FA counters for a specific subscriber	**show mipfa full username** *subscriber_name*
Display Mobile IP Statistics for FA Services	
View statistics for a specific FA service	**show mipfa statistics fa-service** *service_name*

To do this:	Enter this command:
Display Mobile IP FA Counters	
View Mobile IP FA counters for individual subscriber sessions	**show mipfa counters**
View APN Statistics	
view statistics for all APNs within a context	**show apn statistics**
view statistics for an individual APN	**show apn statistics name** *isp2*
View DHCP Information and Counters	
Display DHCP Counter Information	
View DHCP counter information for a specific DHCP service	**show dhcp dhcp-service** *svc_name*
View DHCP counter information for a specific DHCP user	**show dhcp counter user-address** *address*
Display DHCP Server Statistics	
View statistics for all configured DHCP servers within the context	**show dhcp statistics**
Display DHCP Status	
View status for all configured DHCP services and servers within the context	**show dhcp status**
View GTPC Statistics	
View verbose GTP statistics	**show gtpc statistics verbose**
View GTPP Statistics	
View GTPP statistics for all CGFs	**show gtpp statistics**
View GTPP statistics for a specific CGF	**show gtpp statistics cgf-address** *ip_address*
View L2TP Information	
Display L2TP Session Information	
View cumulative statistics for all sessions processed within the current contextIf this command is executed from within the local context, cumulative session information is displayed for all contexts.	**show l2tp sessions**
View all information pertaining to the L2TP session of a specific subscriber	**show l2tp session full username** *subscriber_name*
Display L2TP Statistics	
View statistics for a specific LAC serviceIf this command is executed from within the local context, cumulative session information is displayed for all contexts.	**show l2tp statistics lac-service** *service_name*
Display L2TP Tunnel Information	
View all tunnels currently being facilitated by LAC services within a specific context	**show l2tp tunnels all**
Display IPSec Security Association Statistics	

To do this:	Enter this command:
View IPSec security association statistics for crypto maps in the current context	`show crypto ipsec security-associations statistics`
Display Pre-shared ISAKMP Keys	
View pre-shared keys received from peer security gateways as part of the Diffie-Hellman exchange	`show crypto isakmp keys`
Display IPSec Statistics	
View cumulative IPSec statistics for the current context	`show crypto statistics`

Clearing Statistics and Counters

It may be necessary to periodically clear statistics and counters in order to gather new information. The system provides the ability to clear statistics and counters based on their grouping (PPP, MIPHA, MIPFA, etc.).

Statistics and counters can be cleared using the CLI **clear** command. Refer to *Command Line Interface Reference* for detailed information on using this command.

Chapter 9
Troubleshooting the Service

This chapter provides information and instructions for using the system command line interface (CLI) for troubleshooting issues that may arise during service operation.

Test Commands

In the event that an issue was discovered with an installed application or line card, depending on the severity, it may be necessary to take corrective action.

The system provides several redundancy and fail-over mechanisms to address issues with application and line cards in order to minimize system downtime and data loss. These mechanisms are described in the sections that follow.

Using the PPP Echo-Test Command

The system provides a mechanism to verify the Point-to-Point Protocol session of a particular subscriber by sending Link Control Protocol (LCP) packets to the mobile node. This functionality can be extremely useful in determining the quality of the air link and delays that may occur.

The command has the following syntax:

```
ppp echo-test { callid call_id | ipaddr ip_address | msid ms_id |
username subscriber_name }
```

Keyword/Variable	Description
callid *call_id*	Specifies that the test is executed for a subscriber with a specific call identification number (callid). *call_id* is the specific call identification number that you wish to test.
ipaddr *ip_address*	Specifies that the test is executed for a subscriber with a specific IP address. ip_address is the specific IP address that you wish to test.
msid *ms_id*	Specifies that the test is executed for a subscriber with a specific mobile station identification (MSID) number. *ms_id* is the specific mobile station identification number that you wish to test.
username *subscriber_name*	Specifies that the test is executed for a subscriber with a specific username. *subscriber_name* is the specific username that you wish to test.

The following figure displays a sample of this command's output showing a successful PPP echo-test to a subscriber named user2@aaa.

```
USERNAME: user2@aaa MSID: 0000012345 CALLID: 001e8481

 Tx/Rx 1/0 RTT(min/max/avg) 0/0/0

USERNAME: user2@aaa MSID: 0000012345 CALLID: 001e8481

 Tx/Rx 1/1 RTT(min/max/avg) 77/77/77 (COMPLETE)
```

Using the GTPC Test Echo Command

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol control plane (GTP-C) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

The test is performed by the system sending GTP-C echo request messages to the specified SGSN(s) and waiting for a response.

IMPORTANT: This command must be executed from within the context in which at least one GGSN service is configured.

The command has the following syntax:

gtpc test echo src-address *gn_address* **{ all | sgsn-address** *ip_address* **}**

Keyword/Variable	Description
echo src-address *gn_address*	Specifies the IP address of a Gn interface configured on the system. **NOTE**: The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.
all	Specifies that GTP-C echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.
sgsn-address *ip_address*	Specifies that GTP-C echo requests will be sent to a specific SGSN.*ip_address* is the address of the SGSN receiving the requests.

The following example displays a sample of this command's output showing a successful GTPC echo-test from a GGSN service bound to address 192.168.157.32 to an SGSN with an address of 192.168.157.2.

```
GTPC test echo

--------------

SGSN: 192.168.157.2 Tx/Rx: 1/1 RTT(ms): 1 (COMPLETE)Recovery:202 (0xCA)
```

Using the GTPU Test Echo Command

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol user plane (GTP-U) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

The test is performed by the system sending GTP-U echo request messages to the specified SGSN(s) and waiting for a response.

IMPORTANT: This command must be executed from within the context in which at least one GGSN service is configured.

The command has the following syntax:

gtpu test echo src-address *gn_address* **{ all | sgsn-address** *ip_address* **}**

Keyword/Variable	Description
src-address *gn_address*	Specifies the IP address of a Gn interface configured on the system. **NOTE:** The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.
all	Specifies that GTP-U echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.
sgsn-address *ip_address*	Specifies that GTP-U echo requests will be sent to a specific SGSN.*ip_address* is the address of the SGSN receiving the requests.

The following figure displays a sample of this command's output showing a successful GTPU echo-test from a GGSN service bound to address 192.168.157.32 to an SGSN with an address of 192.168.157.2.

```
GTPU test echo

--------------

SGSN: 192.168.157.2 Tx/Rx: 1/1 RTT(ms): 24 (COMPLETE)
```

Using the GTPv0 Test Echo Command

This command tests the GGSN's ability to exchange GPRS Tunneling Protocol version 0 (GTPv0) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

The test is performed by the system sending GTPv0 echo request messages to the specified SGSN(s) and waiting for a response.

IMPORTANT: This command must be executed from within the context in which at least one GGSN service is configured.

The command has the following syntax:

gtpv0 test echo src-address *gn_address* **{ all | sgsn-address** *ip_address* **}**

Keyword/Variable	Description
src-address *gn_address*	Specifies the IP address of a Gn interface configured on the system. **NOTE**: The IP address of the system's Gn interface must be bound to a configured GGSN service prior to executing this command.
all	Specifies that GTPv0 echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.
sgsn-address *ip_address*	Specifies that GTPv0 echo requests will be sent to a specific SGSN.*ip_address* is the address of the SGSN to receiving the requests.

The following figure displays a sample of this command's output showing a successful GTPv0 echo-test from a GGSN service bound to address 192.168.157.32 to an SGSN with an address of 192.168.157.2.

```
GTPv0 test echo

--------------

SGSN: 192.168.157.2 Tx/Rx: 1/1 RTT(ms):14 (COMPLETE)Recovery: 210(0xD2)
```

Using the DHCP Test Command

This command tests the system's ability to communicate with a Dynamic Host Control Protocol (DHCP) server. Testing is performed on a per-DHCP service basis for either a specific server or all servers the DHCP service is configured to communicate with. This functionality is useful for troubleshooting and/or monitoring.

Once executed, the test attempts to obtain an IP address from the DHCP server(s) and immediately release it.

IMPORTANT: This command must be executed from within the context in which at least one GGSN service is configured.

The command has the following syntax:

dhcp test dhcp-service *svc_name* [**all** | **server** *ip_address*]

Keyword/Variable	Description
dhcp-service *svc_name*	The name of the DHCP service. *svc_name* can be from 1 to 63 alpha and/or numeric characters in length and is case sensitive.
all	Tests DHCP functionality for all servers.
server *ip_address*	Tests DHCP functionality for the server.

The following figure displays a sample of this command's output showing a successful DHCP test for a DHCP service called DHCP-Gi to a server with an IP address of 192.168.16.2. The IP address provided during the test was 192.168.16.144.

```
DHCP test status for service <DHCP-Gi>:

 Server address: 192.168.16.2 Status: Tested

 Lease address: 192.168.16.144 Lease Duration: 600 secs.
```

Testing GTPP Accounting with a CGF

When used to test a CGF, this tool causes the system to send GTPP echo packets to the specified CGF(s).

IMPORTANT: This tool must be executed from the context in which GTPP functionality is configured.

To execute the GTPP accounting test tool enter the following command:

gtpp test accounting { all | cgf-server *ip_address* **}**

Keyword/Variable	Description
all	Tests all CGFs configured within the given context.
cgf-server*ip_address*	Tests a specific CGF configured within the given context.

The command's response will display whether the CGF is active or unreachable.

Testing GTPP Connectivity with a GSS

When used to test a GTPP Storage Server, this tool causes the system to send GTPP echo packets to the specified GSS for checking connectivity and provide round trip time.

IMPORTANT: This tool must be executed from the context in which GTPP functionality is configured.

To execute the GSS connectivity test tool enter the following command:

gtpp test storage-server [address *ip-address* **port** *udp-port***]**

Keyword/Variable	Description
storage-server	Tests configured GSS within the given context.
address *ip_address* **port** *udp_port*	Tests connectivity with GSS having *ip_address* and *udp_port* before configuring it within the given context.

The command's response will display whether the GSS is active or unreachable.

Appendix A
Engineering Rules

This section provides engineering rules or guidelines that must be considered prior to configuring the system for your network deployment.

This appendix describes following engineering rules for GGSN service:

- APN Engineering Rules
- DHCP Service Engineering Rules
- GGSN Engineering Rules
- GRE Tunnel Interface and VRF Engineering Rules
- GTP Engineering Rules
- Interface and Port Engineering Rules
- Lawful Intercept Engineering Rules
- MBMS Bearer Service Engineering Rules
- Service Engineering Rules
- Subscriber Engineering Rules

APN Engineering Rules

The following engineering rules apply to APNs:

- APNs must be configured within the context used for authentication.
- A maximum of 1,024 APNs per system can be configured.

DHCP Service Engineering Rules

The following engineering rule applies to the DHCP Service:

- Up to 8 DHCP servers may be configured per DHCP service.
- A maximum of 3 DHCP server can be tried for a call.

GGSN Engineering Rules

The following engineering rules apply when the system is configured as a GGSN:

- Gn/Gp interfaces can be configured. That is, if a system context is configured with a GGSN service, then all interfaces in that context may be used.
- Gi interfaces can be configured. That is, if a system context is configured as a destination context for an APN, then all interfaces in that context may be used.
- Ga interfaces. That is, if a system context is configured for GTPP accounting, then all interfaces in that context may be used.
- One GSN-MAP node may be configured per system context (in lieu of Gc).
- Up to 1000 network requested PDP contexts may be configured.
- Up to 8 GTPP groups (excluding the default GTPP group) can be configured per chassis.
- Up to 4 GTPP Storage Servers can be configured per GTPP group.
- Up to 32 GTPP Storage Servers can be configured per system context.
- Up to 511 GRE tunnel interface can be configured per context.

GRE Tunnel Interface and VRF Engineering Rules

The following engineering rules apply to GRE tunnel interface and VRF contexts:

- A maximum of 511 GRE tunnels are allowed to configure in a context but subject to maximum of 2048 GRE tunnels per chassis.
- A maximum of 100 virtual routing and forwarding tables are allowed to configure in a context but subject to a maximum of 1024 VRFs per chassis.
- A maximum of 10000 IP routes in Release 9.0 and 16384 IP routes in Release 10.0 onward are supported in a VRF context configuration mode.

GTP Engineering Rules

The following engineering rules apply to GTP on GGSN:

- A maximum of 11 primary (no secondary) PDP context per subscriber can be configured.
- A maximum of 1 primary and 10 secondary PDP context per subscriber can be configured.

Interface and Port Engineering Rules

The rules discussed in this section pertain to both the Ethernet 10/100 and Ethernet 1000 Line Cards and the four-port Quad Gig-E Line Card (QGLC; ASR 5000 only) and the type of interfaces they facilitate.

Pi Interface Rules

FA to HA Rules

When supporting Mobile IP, the system can be configured to perform the role of a FA, an HA, or both. This section describes the engineering rules for the Pi interface when using the system as a FA.

The following engineering rules apply to the Pi interface between the FA and HA:

- A Pi interface is created once the IP address of a logical interface is bound to an FA service.
- The logical interface(s) that will be used to facilitate the Pi interface(s) must be configured within the egress context.
- FA services must be configured within the egress context.
- If the system is configured as a FA is communicating with a system configured as an HA, then it is recommended that the name of the context in which the FA service is configured is identical to the name of the context that the HA service is configured in on the other system.
- Each FA service may be configured with the Security Parameter Index (SPI) of the HA that it will be communicating with over the Pi interface.
- Multiple SPIs can be configured within the FA service to allow communications with multiple HAs over the Pi interface. It is best to define SPIs using a netmask to specify a range of addresses rather than entering separate SPIs. This assumes that the network is physically designed to allow this communication.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the Pi interface can be limited.

HA to FA

The following engineering rules apply to the Pi interface between the HA and FA:

- When supporting Mobile IP, the system can be configured to perform the role of a FA, an HA or both. This section describes the engineering rules for the Pi interface when using the system as an HA.
- A Pi interface is created once the IP address of a logical interface is bound to an HA service.

- The logical interface(s) that will be used to facilitate the Pi interface(s) must be configured within an ingress context.
- HA services must be configured within an ingress context.
- If the system configured as an HA is communicating with a system configured as a FA, then it is recommended that the name of the context in which the HA service is configured is identical to the name of the context that the FA service is configured in on the other system.
- Each HA service may be configured with the Security Parameter Index (SPI) of the FA that it will be communicating with over the Pi interface.
- Multiple SPIs can be configured within the HA service to allow communications with multiple FAs over the Pi interface. It is best to define SPIs using a netmask to specify a range of addresses rather than entering separate SPIs. This assumes that the network is physically designed to allow this communication.
- Each HA service must be configured with a Security Parameter Index (SPI) that it will share with mobile nodes.
- Depending on the services offered to the subscriber, the number of sessions facilitated by the Pi interface can be limited in order to allow higher bandwidth per subscriber.

GRE Tunnel Interface Rule

The following engineering rules apply to the GRE tunnel interface between two GRE tunnel nodes:

- A maximum of 512 IP tunnels (511 GRE tunnels + 1 not tunnel interfaces) are allowed to configure in a context but subject to a maximum of 2048 GRE tunnels per chassis.

Lawful Intercept Engineering Rules

The following engineering rules apply to Lawful Intercept on supported AGW service:

- A maximum of 1000 Lawful Intercepts can be performed simultaneously.

MBMS Bearer Service Engineering Rules

The following engineering rules apply to MBMS bearer services:

- A maximum 225 downlink SGSNs per MBMS bearer service are supported on ASR 5000.
- A maximum of 2 BMSC (1 primary and 1 secondary) supported per MBMS bearer service.

Service Engineering Rules

The following engineering rules apply to services configured within the system:

- A maximum of 256 services (regardless of type) can be configured per system.

  CAUTION: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

- Up to 2,048 MN-HA and 2048 FA-HA SPIs can be supported for a single HA service.
- Up to 2,048 FA-HA SPIs can be supported for a single FA service.
- The system supports unlimited peer FA addresses per HA.
- The system maintains statistics for a maximum of 8192 peer FAs per HA service.
- If more than 8192 FAs are attached, older statistics are identified and overwritten.
- The system maintains statistics for a maximum of 4096 peer HAs per FA service.
- The total number of entries per table and per chassis is limited to 256.
- Up to 10,000 LAC addresses can be configured per LNS service.

CAUTION: Even though service names can be identical to those configured in different contexts on the same system, this is not a good practice. Having services with the same name can lead to confusion, difficulty in troubleshooting the problems, and make it difficult to understand outputs of **`show`** commands.

Subscriber Engineering Rules

The following engineering rule applies to subscribers configured within the service:

- Default subscriber templates may be configured on a per FA service basis.

Appendix B
Mobile-IP and Proxy-MIP Timer Considerations

This appendix is intended to provide a brief explanation of the considerations for lifetime, idle, and absolute timer settings that must be understood when setting up a system in a Mobile-IP or Proxy-MIP environment. The focus of the document is to understand the call flow and understand the timer values that must be applied to make the system function in the most efficient manner.

Call Flow Summary

IMPORTANT: Commands used in the examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the Command Line Interface Reference for complete information regarding all commands.

The following steps describe the call flow as regards the timers that affect a call initiated by the Mobile Node (MN).

1. (or L2TP, for Closed RP interfaces) The GGSN receives a Create PDP Context Request Message from the SGSN. The call arrives at the system, the subscriber
2. The system determines the properties to apply to the call from the APN template used. The APN provides such information as the authentication and accounting methods, and whether or not to use Mobile IP.
3. The system still does not know the username and password at this point, so it looks at the default APN template for 3GPP technology subscribers and subscriber profile for other technology subscribers. If the idle or absolute timeouts are configured, the system compares the settings for the idle and absolute timeout to the setting for the advertised registration lifetime in the FA-service.
   - Use the following example to set absolute and idle timeout for the default subscriber in non-3GPP network:

```
configure
   context <context_name>
      subscriber default
         timeout idle <value>
         timeout absolute <value>
         end
```

   - Use the following example to set absolute and idle timeout for the APN template in 3GPP network:

```
config
   context <context_name>
      apn <apn_name>
         timeout idle <value>
         timeout absolute <value>
         end
```

   - The following example can be used to set FA agent reg-lifetime in the FA service:

```
configure
```

```
context <context_name>
   fa-service <fa_service_name>
      advertise reg-lifetime <value>
      end
```

4. The new RRQ is accepted by the FA and sent to the HA. The HA authenticates the user and compares the requested lifetime to the configured MIP lifetime in the HA-service and the subscriber idle and absolute timeouts. If the MIP lifetime is lower it is be sent back to the mobile; if the MIP lifetime is higher the system sends back an RRQ accept with the lifetime set to 5 seconds less than the lower of the idle or absolute timeout for the user.

   The following CLI command sequence is used to configure the Mobile IP reg-lifetime in the HA service:

```
configure
   context <host_name>
      ha-service <ha_service_name>
         reg-lifetime <value>
         end
```

Timer Values and Recommendations

The following table shows values that would be populated under a number of different configured scenarios.

Table 16. Sample Call Flow Timer Scenarios

Scenario	1	2	3	4	5	6	7
Mobile Sub. MIP Lifetime	600	600	600	600	600	600	600
APN Template Timeout Absolute	300	300	300	300	300	300	300
APN Template Timeout Idle	300	300	300	300	300	300	300
FA-Service Advertise Reg-Lifetime	400	400	400	400	400	400	400
Mobile Sub. Profile AAA Context Timeout idle	500	500	500	500	500	500	500
HA-Service MIP Lifetime	400	400	400	400	400	400	400
Agent Advertisement Reg-Lifetime	295	295	295	295	295	295	295
Mobile Sub. MIP RRQ requested lifetime	295	295	295	295	295	295	295
FA MIP RRP Lifetime	295	295	295	295	295	295	295
FA MIP RRP	success	success	success	success	success	success	Lifetime too long

Based on the table above, the recommended guidelines are as follows:

- If you are going to use timeout idle settings for subscribers/APNs, it is recommended that you configure the timeout idle parameter in the source context default subscriber to a value that is less than or equal to the lowest timeout idle for any subscriber/APN.
- If you are going to use timeout absolute settings for subscribers/APNs, it is recommended that you configure the timeout absolute in the source context default subscriber to a value that is less than or equal to the lowest timeout idle for any subscriber/APN.
- The FA-service advertise reg-lifetime parameter should be configured to a value less than the source context default subscriber in non-3GPP networks and APN timeout idle parameter for 3GPP networks.

Failure to follow these recommendations could result in lifetime too long failures when the FA processes the subscriber profileAPN template and finds an idle timeout that is less than the proposed MIP lifetime in the mobile RRQ.

Controlling the Mobile IP Lifetime on a Per-Domain Basis

The system does not support the configuration of the MIP lifetime timer on per- domain (context) basis. However, a domain-wide lifetime timer can be achieved by configuring the idle-timeout attribute for the default subscriber for each domain.

IMPORTANT: Mobile IP lifetime settings can be controlled on a per-domain basis **only** in deployments for which the idle timeout attribute for individual subscriber profiles is **not** used during operation.

In this configuration, the value of the registration lifetime sent by the system in Agent Advertisements is selected by comparing the configured FA Agent Advertisement lifetime setting, and the idle and/or absolute timeout settings configured for the domain's default subscriber. If the value of the idle and/or absolute timeout parameter is less than the Agent Advertisement lifetime, then the system provides a registration lifetime equal to 5 seconds less than the lowest timer value.

If the idle timeout attribute is configured in individual subscriber profiles, per-domain lifetime control is not possible. In this case, the registration lifetime configured for the FA must be the lower of the two values.

IMPORTANT: Commands used in the examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the Command Line Interface Reference for complete information regarding all commands.

The following is an example CLI command sequence used to configure the Mobile IP lifetime on a per-domain basis.

```
configure
   context <aaa_context_name>
      subscriber default
         ip context-name <abc>
         exit
      subscriber name <ptt.bigco.com>
         timeout idle <3605>
         ip context-name <abc>
         exit
      subscriber name <bigco.com>
         timeout idle <7205>
         ip context-name <abc>
         exit
```

```
      domain <ptt.bigco.com> default subscriber <ptt.bigco.com>
      domain <bigco.com> default subscriber <bigco.com>
         end
configure
   context <ha_context_name>
      subscriber default
      exit   ha-service <ha>
      idle-timeout-mode normal      reg-lifetime <7200>
      end
configure
   context <fa_context_name>
      fa-service <fa>
         advertise reg-lifetime <7200>
         end
```

In the example above, two domains (ptt.bigco.com and bigco.com) are configured. The default subscribers are defined for the two domains respectively. The desired operation requires a Mobile IP lifetime of 1 hour (3600 secs) for the ptt.bigco.com domain, and a lifetime of 2 hours (7200 secs) for the bigco.com domain.

Whenever a subscriber session belonging to the ptt.bigco.com domain arrives, the system uses a Mobile IP lifetime timer value equal to 5 seconds less than the idle timeout configured for the default subscriber because the configured value is less than the registration lifetime value configured for the Agent Advertisement. 5 seconds less than the configured value of 3605 seconds equals 3600 seconds which meets the desired operation.

Whenever a subscriber session belonging to the bigco.com domain arrives, the system uses the configured registration lifetime value as the Mobile IP lifetime in Agent Advertisements because it is less than the configured idle timeout in the default subscriber's profile.

As a general rule, the registration lifetime value on the agent **must** be configured as the highest Mobile IP lifetime that is desired for a subscriber. (In the above example, it would be the subscriber bigco.com.)

Another important factor to consider is that the idle timeout value should be reset on receipt of a renewal request. To support this operation, the system provides the **idle-timeout-mode** configurable in the HA service. The following modes are supported:

- **normal**: Resets the idle timeout value on receipt of Mobile IP user data and control signaling
- **aggressive**: Resets the idle timeout value on receipt of Mobile IP user data only (this is the default behavior)
- **handoff**: Resets the idle timeout value on receipt of Mobile IP user dataand upon inter-AGW handoff

The following optional modifier is also supported:

- **upstream-only**: Only upstream user data (data from the mobile node) resets the idle timer for the session. This is disabled by default.