



Cisco ASR 5000 Series 3G Home NodeB Gateway 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-22991-01

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 3G Home NodeB Gateway Administration Guide

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

CONTENTS

About this Guide	V
Conventions Used.....	vi
Contacting Customer Support	viii
HNB Gateway in UMTS Network.....	9
Product Description	10
HNB Access Network Elements	11
Home NodeB	11
Security Gateway (SeGW).....	12
HNB Gateway (HNB-GW).....	12
HNB Management System (HMS)	12
Product Specification	13
Licenses	13
Hardware Requirements	13
Platforms	13
System Hardware Components	13
Operating System Requirements	14
Network Deployment and Interfaces.....	15
HNB Gateway in 3G UMTS Network.....	15
Supported Interfaces	15
Features and Functionality - Base Software	17
UE Management Function for Pre-Rel-8 UEs	17
UE Management Function for Rel-8 UEs	17
HNB Management Function.....	18
GTP-U Tunnels Management Support	18
Network Access Control Functions through SeGW	18
Authentication and Key Agreement (AKA)	19
3GPP AAA Server Support	19
System Management Features	19
Management System Overview	20
Bulk Statistics Support.....	21
Threshold Crossing Alerts (TCA) Support	22
ANSI T1.276 Compliance	23
Features and Functionality - Licensed Enhanced Feature Software	24
How HNB-GW Works	25
HNB Provisioning and Registration Procedure	25
UE Registration Procedure	27
UE Registration Procedure of Non-CSG UEs or Non-CSG HNBs	27
UE Registration Procedure of CSG UEs and CSG or Hybrid HNBs	29
Iu Connection Procedures.....	31
Iu Connection Establishment Procedure	31
Network Initiated Iu Connection Release Procedure	33
Supported Standards.....	36
3GPP References	36
IETF References	36
ITU-T Recommendations	39
Object Management Group (OMG) Standards	39





Understanding the Service Operation	41
Terminology	42
Contexts	42
Logical Interfaces	43
Bindings	44
Services and Networks	44
HNB-GW Service Configuration Procedures	47
Information Required to Configure the System as an HNB-GW	48
Required Local Context Configuration Information	48
Required System-Level Configuration Information	49
Required Source Context Configuration Information	51
Required Destination Context Configuration Information	53
RTP Pool Configuration	55
IPv4 RTP Pool Creation Over IuCS	55
RTP IP Pool Configuration Verification	56
HNB GW Service Configuration	58
Iuh Interface Configuration	58
SS7 Routing Domain Configuration	59
SCCP Network Instance Configuration	60
GTP-U Service Configuration	60
HNB-PS Network Configuration	61
HNB-CS Network Configuration	62
HNB-GW Service Configuration	62
Security Gateway and Crypto map Template Configuration	63
Verifying HNB-GW Configuration	64
Event IDs for HNB-GW Service	67
Verifying and Saving Your Configuration	69
Verifying the Configuration	70
Feature Configuration	70
Service Configuration	71
Context Configuration	72
System Configuration	72
Finding Configuration Errors	72
Saving the Configuration	74
Saving the Configuration on the Chassis	75
Monitoring the Service	77
Monitoring System Status and Performance	78
Clearing Statistics and Counters	80
Troubleshooting the Service	81
Test Commands	82
Using the GTPU Test Echo Command	82
Using the GTPv0 Test Echo Command	83
Using the IPsec Tunnel Test Command	83
Engineering Rules	85
DHCP Service Engineering Rules	86
HNB-GW Engineering Rules	87
Lawful Intercept Engineering Rules	88
MBMS Bearer Service Engineering Rules	89
Service Engineering Rules	90

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 <code>screen display</code>	This typeface represents displays that appear on your terminal screen, for example: Login:
Text represented as <code>commands</code>	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 <code>command variable</code>	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
{ <code>keyword</code> or <code>variable</code> }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

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

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of <http://www.cisco.com> for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

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



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

Chapter 1

HNB Gateway in UMTS Network

The Cisco® ASR 5000 Platform provides 3GPP wireless carriers with a flexible solution that functions as an Home NodeB Gateway (HNB-GW) in HNB Access Network to connect UEs with existing UMTS networks.

The Home NodeB Gateway is the HNB access network gateway used to connect the Home NodeBs (HNBs) to access the existing wireless network. The HNB-GW concentrates connections from a large amount of femtocells (HNBs) using Iuh interface and terminates the connection to existing Core Networks (CS or PS) using the standard Iu (IuCS or IuPS) interface.

This overview provides general information about the HNB Gateway including:

- [Product Description](#)
- [Product Specification](#)
- [Network Deployment and Interfaces](#)
- [Features and Functionality - Base Software](#)
- [Features and Functionality - Licensed Enhanced Feature Software](#)
- [How HNB-GW Works](#)
- [Supported Standards](#)

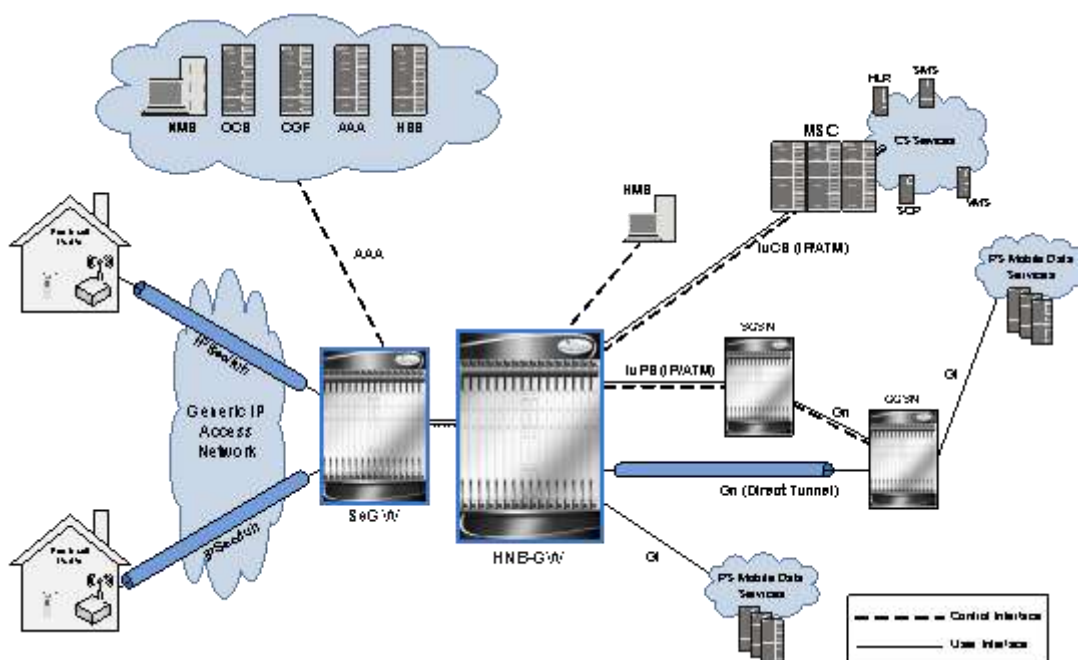
Product Description

The Home NodeB Gateway is the HNB network access concentrator used to connect the Home NodeBs (HNBs)/Femto Access Point (FAP) to access the UMTS network through HNB Access Network. It aggregates Home Node-B or Femto Access Points to a single network element and then integrates them into the Mobile Operators Voice, Data and Multimedia networks.

Femtocell is an important technology and service offering that enables new Home and Enterprise service capabilities for Mobile Operators and Converged Mobile Operators (xDSL/Cable/FFTH plus Wireless). The Femtocell network consists of a plug-n-play customer premise device generically called an Home NodeB (HNB) with limited range radio access in home or Enterprise. The HNB will auto-configure itself with the Operators network and the user can start making voice, data and multimedia calls.

The figure given describes a high level view of UMTS network with Femtocell and HNB-GW.

Figure 1. HNB-GW Deployment in 3G UMTS Network



Once a secure tunnel has been established between the HNB and the SeGW and the HNB has been configured by the HMS, the Operator has to connect the Femtocell network to their Core Network and services. There are several interworking approaches to Circuit Switch (CS) and Packet Switch (PS) domains. One approach is to make the Femtocell network appear as a standard Radio Access Network (RAN) to the Core Network. In addition to the HNB, SeGW and HMS the RAN approach requires a network element generically called a Femto Gateway (FGW/HNB-GW). The HNB-GW provides interworking and aggregation of large amount of Femtocell sessions toward standard CN interfaces (e.g. Iu-CS/PS, A1/2, A10/11, R6). In this approach services and mobility are completely transparent to CN elements (e.g. MSC, xGSN, PDSN/HA, ASN GW).

The other approach is to connect the Femtocell to an IMS Network to provide CS services to subscribers when on the Femtocell and deploy a new network element generically called a Convergence Server to provide service continuity and

mobility over standard interfaces at the MSC layer (e.g GSM-MAP, IS-41). These two approaches are clearly different in how CS based services and mobility are achieved.

In accordance with 3GPP standard, the HNB-GW provides following functions and procedures in UMTS core network:

- HNB Registration/De-registration Function
- UE Registration/De-registration Function for HNB
- Iuh User-plane Management Functions
- Iuh User plane Transport Bearer Handling
- Iu Link Management Functions



IMPORTANT: Some of the features may not be available in this release. Kindly contact your local Cisco representative for more information on supported features.

HNB Access Network Elements

This section provides the brief description and functionality of various network elements involved in the UMTS Femto access network. The HNB access network includes the following functional entities:

- [Home NodeB](#)
- [Security Gateway \(SeGW\)](#)
- [HNB Gateway \(HNB-GW\)](#)
- [HNB Management System \(HMS\)](#)

Home NodeB

A Home NodeB (HNB) is the a customer premise equipment that offers Uu interface to UE and Iuh over IPSec tunnel to HNB-GW for accessing UMTS Core Network (PS or CS) in femtocell access network.

It also provides the support to HNB registration and UE registration over Iuh with HNB-GW. Apart from these functions HNB also supports some RNC like functions as given below:

- RAB management functions
- Radio Resource Management functions
- Iu Signalling Link management
- GTP-U Tunnels management
- Buffer Management
- Iu U-plane frame protocol initialization
- Mobility management functions
- Security Functions
- Service and Network Access functions

- Paging co-ordination functions
- UE Registration for HNB
- Iuh user-plane Management functions

Security Gateway (SeGW)

Security Gateway is a logical entity in Cisco HNB-GW. Basic function of this entity are; 1) authentication of HNB and 2) providing access to HMS and HNB-GW

This entity terminates the secure tunnelling for Iuh and TR-069 between HNB and HNB-GW and HMS respectively.

In this implementation it is an optional element which is situated on HNB-GW.

HNB Gateway (HNB-GW)

The HNB-GW provides the access to Femto user to UMTS core network. It acts as an access gateway to HNB and concentrates connections from a large amount of HNBs. The Iuh interface is used between HNB and HNB-GW and HNB-GW connects with the Core Networks (CS or PS) using the generic Iu (Iu-CS or Iu-PS) or Gn interface.

It also terminates Gn and other interfaces from UMTS core networks to provide mobile data services to HNB and to interact with HMS to perform HNB authentication and authorization.

HNB Management System (HMS)

It is a network element management system for HNB access. Management interface between HNB and HMS is based on TR-069 family of standards.

It performs following functions while managing HNB access network:

- Facilitates HNB-GW discovery for HNB
- Provision of configuration data to the HNB
- Performs location verification of HNB and assigns appropriate serving elements (HMS, Security Gateway and HNB-GW)

The HNB Management System (HMS) comprises of the following functional entities:

- File Server: used for file upload or download, as instructed by TR-069 manager
- TR-069 Manager: Performs CM, FM and PM functionality to the HNB through Auto-configuration server (HMS)

Product Specification

This section describes the hardware and software requirement for HNB Gateway.

The following information is located in this section:

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

Licenses

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

The following licenses are available for this product:

- HNB-GW Software Bundle License, 10K Sessions, 600-00-9020
- HNB-GW Software Base License, 1K Sessions, 600-00-9020

For more information on supported features, refer *Features and Functionality* section.

Hardware Requirements

Information in this section describes the hardware required to enable the HNB-GW service.

Platforms

The HNB-GW service operates on the following platforms:

- ASR 5000

System Hardware Components

The following application and line cards are required to support HNB-GW services on the system:

- **System Management Cards (SMC):** 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 Services Cards (PSC/PSC2):** Within the ASR 5000 platform, PSCs/PSC2s provide high-speed, multi-threaded EPS Bearer context processing capabilities for HNB-GW services. Up to 14 PSCs/PSC2s can be installed, allowing for multiple active and/or redundant cards.
- **Switch Processor Input/Outputs (SPIOs):** Installed in the upper-rear chassis slots directly behind the SPCs/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 PSCs, 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 PSCs/PSC2, 13 in the upper-rear slots and 13 in the lower-rear slots for redundancy. Redundant PSCs/PSC2s 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 PSC/PSC2 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 SPCs/SMCs, RCCs utilize 5 Gbps serial links to ensure connectivity between Ethernet 10/100/Ethernet 1000/Quad-Gig-E/10-Gig-E line cards and every PSC/PSC2 in the system for redundancy. Two RCCs can be installed to provide redundancy for all line cards and PSCs/PSC2.



IMPORTANT: Additional information pertaining to each of the application and line cards required to support LTE/SAE services is located in the Hardware Platform Overview chapter of the Product Overview Guide.

Operating System Requirements

The HNB-GW is available for ASR 5000 running StarOS™ Release 10.0 or later.

Network Deployment and Interfaces

This section describes the supported interfaces and deployment scenario of HNB-GW in 3G Femto access network.

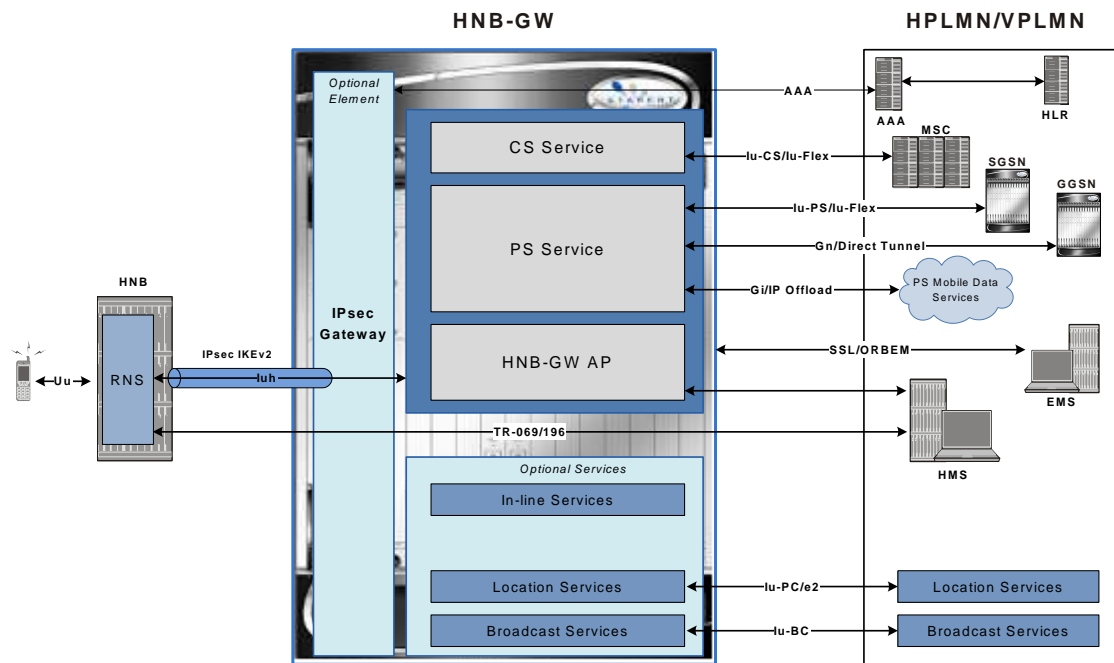
The following information is provided in this section:

- [HNB Gateway in 3G UMTS Network](#)
- [Supported Interfaces](#)

HNB Gateway in 3G UMTS Network

The following figure displays simplified network views of the HNB-GW in an Femto access network accessing UMTS PS or CS Core Network.

Figure 2. The HNB-GW in UMTS Network and Interfaces



Supported Interfaces

In support of both mobile and network originated subscriber UE contexts, the HNB-GW provides the following network interface support:

- **Iuh Interface:** This interface is the reference point for the control plane protocol between Home NodeB and HNB-GW. Iuh uses SCTP over IPsec IKEv2 tunnel as the transport layer protocol for guaranteed delivery of signaling messages between HNB-GW and Home NodeB.

This is the interface used by the HNB-GW to communicate with HNB on the same Femtocell Access Network. This interface serves as path for establishing and maintaining subscriber UE contexts.

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

- **IuCS:** This interface is the reference point in UMTS which links the HNB-GW, which acts as an RNC (Radio Network Controller), with a Mobile Switching Centre (3G MSC) in the 3G UMTS Femtocell Access Network. This interface provides an IuCS over IP or IuCS over ATM (IP over AAL5 over ATM) interface between the MSC and the RNC (HNB-GW) in the 3G UMTS Femtocell Access Network. RAN Application Part (RANAP) is the control protocol that sets up the data plane (GTP-U) between these nodes. SIGTRAN (M3UA/SCTP) or QSAAL (MTP3B/QSAAL) handle IuCS (control) for the HNB-GW.

This is the interface used by the HNB-GW to communicate with 3G MSC on the same Public Land Mobile Network (PLMN). This interface serves as path for establishing and maintaining the CS access for Femtocell UE to circuit switched UMTS core networks

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

- **IuPS:** This interface is the reference point between HNB-GW and SGSN. This interface provides an IuPS over IP or IuPS over ATM (IP over AAL5 over ATM) interface between the SGSN and the RNC (HNB-GW) in the 3G UMTS Femtocell Access Network. RAN Application Part (RANAP) is the control protocol that sets up the data plane (GTP-U) between these nodes. SIGTRAN (M3UA/SCTP) or QSAAL (MTP3B/QSAAL) handle IuPS-C (control) for the HNB-GW.

This is the interface used by the HNB-GW to communicate with SGSN on the same Public Land Mobile Network (PLMN). This interface serves as path for establishing and maintaining the PS access for Femtocell UE to packet switched UMTS core networks.

One or more Iu-PS interfaces can be configured per system context.

- **Gi:** This interface is the reference point between HNB-GW and IP Offload Gateway. It is used by the HNB-GW to communicate with Packet Data Networks (PDNs) through IP Offload Gateway in the H-PLMN/V-PLMN. Examples of PDNs are the Internet or corporate intranets.

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

- **Gn:** This interface is the reference point between HNB-GW and GGSN. It is used by the HNB-GW to communicate with GGSNs on the same GPRS/UMTS Public Land Mobile Network (PLMN).

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

- **TR-069:** This interface is an application layer protocol which is used for remote configuration of terminal devices, such as DSL modems, HNBs and STBs. TR-069 provides an auto configuration mechanism between the HNB and a remote node in the service provider network termed the Auto Configuration Server. The standard also uses a combination of security measures including IKEv2 (Internet Key Exchange v2) and IPsec (IP Security) protocols to authenticate the operator and subscriber and then guarantee the privacy of the data exchanged.

One TR-069 interface can be configured per HNB node.

Features and Functionality - Base Software

This section describes the features and functions supported by default in base software on HNB-GW service and do not require any additional license to implement the functionality with the HNB-GW service.



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

Following features and supports are discussed in this section:

- [UE Management Function for Pre-Rel-8 UEs](#)
- [UE Management Function for Rel-8 UEs](#)
- [HNB Management Function](#)
- [System Management Features](#)

UE Management Function for Pre-Rel-8 UEs

Support for Pre-Rel-8 UE registration and de-registration in 3G UMTS HNB Access Network in accordance with the following standards:

- **3GPP TS 25.467 V8.0.0. (2008-12):** 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN architecture for 3G Home NodeB; Stage 2 (Release 8)
- **3GPP TS 25.469 V8.1.0 (2009-03):** 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iuh interface Home Node B Application Part (HNBAP) signalling (Release 8)
- IETF RFC 4960, Stream Control Transmission Protocol, December 2007

The HNB-GW provides UE registration and de-registration procedure for the HNB to convey pre-Rel-8 UE identification data to the HNB-GW in order to perform access control for the UE in the HNB-GW. The UE Registration also establishes a UE specific context identifier to be used between HNB and HNB-GW. The procedure triggered when the UE attempts to access the HNB via an initial NAS message and there is no context in the HNB allocated for that UE.

UE Management Function for Rel-8 UEs

Support for Rel-8 UE registration and de-registration in 3G UMTS HNB Access Network in accordance with the following standards:

- **3GPP TS 25.467 V8.0.0. (2008-12):** 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN architecture for 3G Home NodeB; Stage 2 (Release 8)
- **3GPP TS 25.469 V8.1.0 (2009-03):** 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iuh interface Home Node B Application Part (HNBAP) signalling (Release 8)

- IETF RFC 4960, Stream Control Transmission Protocol, December 2007

The HNB-GW provides UE registration and de-registration procedure for the HNB to convey Rel-8 UE identification data to the HNB-GW in order to perform access control for the UE in the HNB-GW. The UE Registration also establishes a UE specific context identifier to be used between HNB and HNB-GW. The procedure triggered when the UE attempts to access the HNB via an initial NAS message and there is no context in the HNB allocated for that UE.

HNB Management Function

Support for HNB registration and de-registration in 3G UMTS HNB Access Network accordance with the following standards:

- **3GPP TS 25.469 V8.1.0 (2009-03)**: 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iuh interface Home Node B Application Part (HNBAP) signalling (Release 8)
- IETF RFC 4960, Stream Control Transmission Protocol, December 2007

The HNB-GW provides HNB registration and de-registration procedure to register the HNB with the HNB-GW. This procedure enables the HNB-GW to provide service and core network connectivity for the HNB. This procedure is the first HNBAP procedure triggered after the SCTP association has become operational between HNB and HNB-GW.

GTP-U Tunnels Management Support

Support to manage the GTP-U tunnels between HNB-GW and GSNs by in accordance with the following standards:

- **3GPP TS 25.467 V9.1.0 (2009-12)**: 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN architecture for 3G Home Node B (HNB); Stage 2 (Release 9)
- **3GPP TS 25.468 V9.0.0 (2009-12)**: 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iuh Interface RANAP User Adaption (RUA) signalling (Release 9)
- **3GPP TS 25.469 V9.0.0 (2009-12)**: 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iuh interface Home Node B Application Part (HNBAP) signalling (Release 9)

Network Access Control Functions through SeGW

These functions enable secure user and device level authentication between the authenticator component of the HNB-GW and a 3GPP HSS/AuC and Diameter-based Wm interface support.

This section describes following features:

- Authentication and Key Agreement (AKA)
- 3GPP AAA Server Support

Authentication and Key Agreement (AKA)

HNB-GW provides Authentication and Key Agreement mechanism for user authentication procedure over the HNB Access Network. The Authentication and Key Agreement (AKA) mechanism performs authentication and session key distribution in networks. AKA is a challenge- response based mechanism that uses symmetric cryptography.

The AKA is the procedure that take between the user and network to authenticate themselves towards each other and to provide other security features such as integrity and confidentiality protection.

In a logical order this follows the following procedure:

1. **Authentication:** Performs authentication by, identifying the user to the network; and identifying the network to the user.
2. **Key agreement:** Performs key agreement by, generating the cipher key; and generating the integrity key.
3. **Protection:** When the AKA procedure is performed it protects, the integrity of messages; confidentiality of signalling data; and confidentiality of user data

3GPP AAA Server Support

This interface between the SeGW and AAA Server provides a secure connection carrying authentication, authorization, and related information. in accordance with the following standards:

- 3GPP TS 33.320 V9.1.0 (2010-03): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security of Home Node B (HNB) / Home evolved Node B (HeNB) (Release 9)

This reference point is located between 3GPP AAA Server/Proxy and HNB-GW. The functionality of this reference point is to enable following requirements on SeGW:

- The SeGW shall be authenticated by the HNB using a SeGW certificate.
- The SeGW shall authenticate the HNB based on HNB certificate.
- The SeGW authenticates the hosting party of the HNB in cooperation with the AAA server using EAP-AKA.
- The SeGW shall allow the HNB access to the core network only after successful completion of all required authentications.
- Any unauthenticated traffic from the HNB shall be filtered out at the SeGW

System Management Features

This section describes following features:

- [Management System Overview](#)
- [Bulk Statistics Support](#)
- [Threshold Crossing Alerts \(TCA\) Support](#)
- [ANSI T1.276 Compliance](#)

Management System Overview

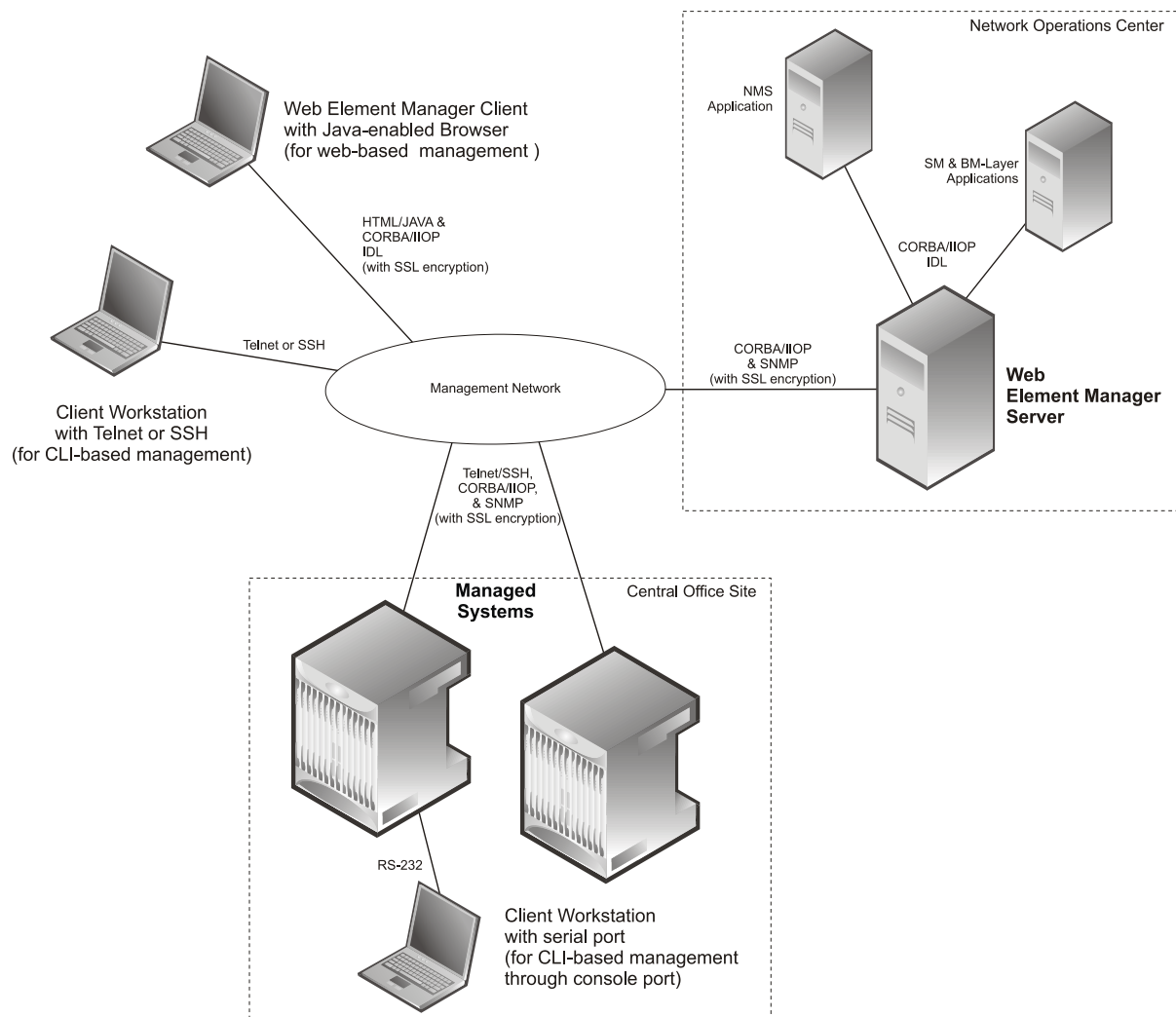
The system's management capabilities are designed around the Telecommunications Management Network (TMN) model for management - focusing on providing superior quality network element (NE) and element management system (Web Element Manager) functions. The system provides element management applications 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.

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 3. Element Management System



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

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

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. Following is a partial list of supported schemas:

- **System:** Provides system-level statistics
- **Card:** Provides card-level statistics
- **Port:** Provides port-level statistics
- **HNB-GW:** Provides HNB-GW service statistics
- **GTPU:** Provides GPRS Tunneling Protocol - User message 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 IMG 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, IMG host name, IMG 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.

Threshold Crossing Alerts (TCA) Support

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

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

The following thresholding models are supported by the system:

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

Thresholding reports conditions using one of the following mechanisms:

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

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

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

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

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

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



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

Features and Functionality - Licensed Enhanced Feature Software

How HNB-GW Works

This section provides information on the function and procedures of the HNB-GW in an wireless network and presents message flows for different stages of session setup.

The following procedures are supported in this release:

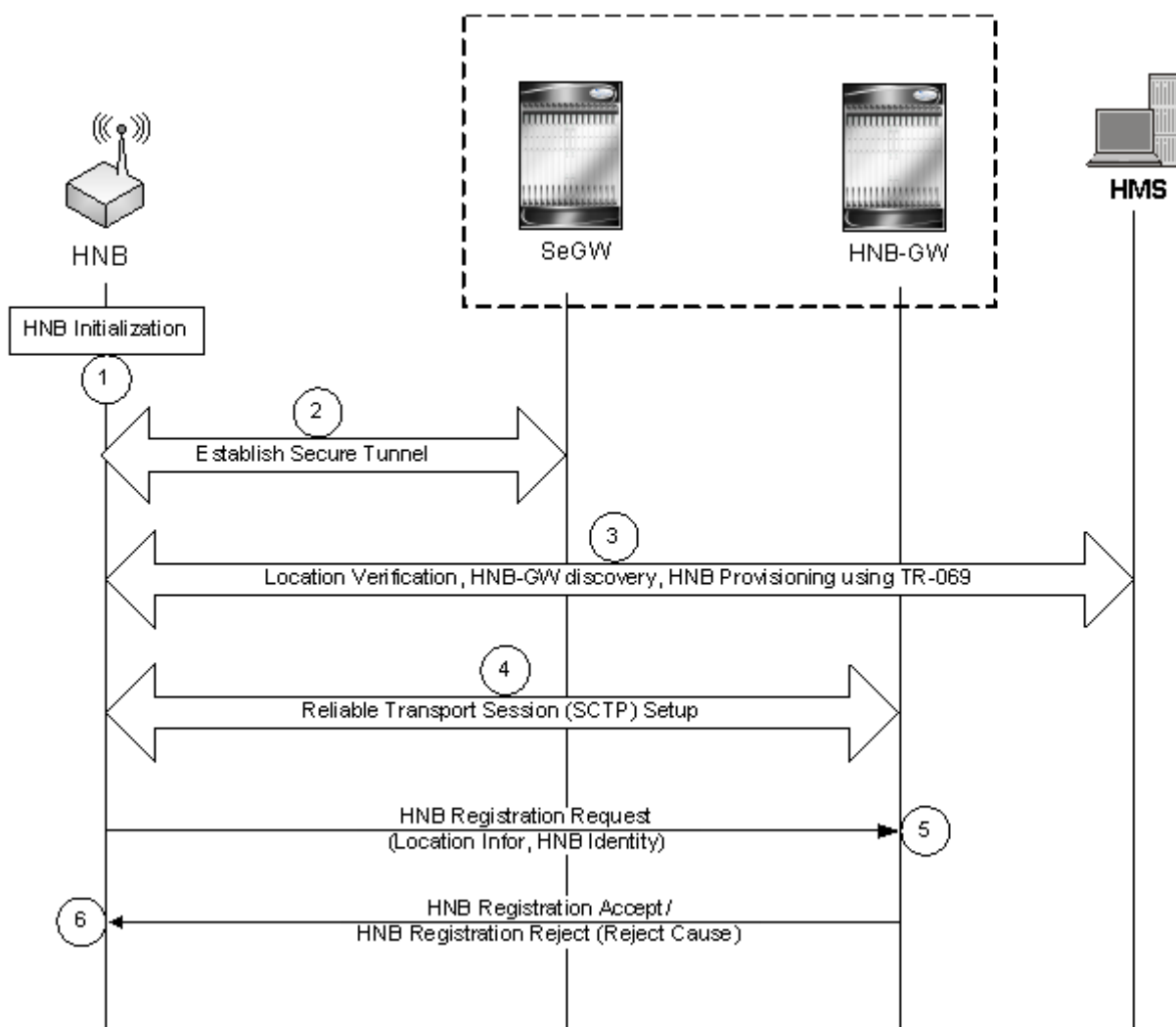
- [HNB Provisioning and Registration Procedure](#)
- [UE Registration Procedure](#)
- [Iu Connection Procedures](#)

HNB Provisioning and Registration Procedure

This section describes the call flow for HNB provisioning and registration procedure.

The following figure and the text that follows describe the message flow for HNB provisioning and registration with HNB-GW procedure.

Figure 4. HNB Provisioning and Registration Setup Call Flow



1. HNB initialization is performed to obtain HNB configuration from the HNB Management System (HMS). Similarly, HNB-GW discovery is performed to obtain the initial serving HNB-GW information.
2. A secure tunnel is established from the HNB to the Security Gateway.
3. Location verification shall be performed by the HMS based on information sent by the HNB (e.g. macro neighbor cell scans, global navigational satellite system type of information etc.). HMS determines the serving elements and provides the HNB-GW, HMS and Security Gateway to the HNB. The HMS also provisions configuration parameters to the HNB only after successful location verification in the HMS.
4. Reliable transport setup (SCTP) completed and the HNB sets up a SCTP transport session to a well-defined port on the serving HNB-GW. HNB Registration procedure started.
5. The HNB attempts to register with the serving HNB-GW using a HNB-REGISTER-REQUEST message. This message may contains:
 - **HNB Location Information:** The HNB provides location information via use of one or more of the following mechanisms:
 - detected macro coverage information (e.g. GERAN and/or UMTS cell information)
 - geographical co-ordinates (e.g. via use of GPS, etc)

- Internet connectivity information (e.g. IP address).
 - **HNB Identity:** the HNB has a globally unique and permanent identity.
 - **HNB Operating Parameters:** Such as the selected LAC, RAC, SAC, etc.
6. The HNB-GW uses the information from the HNB-REGISTER-REQUEST message to perform access control of the HNB (e.g. whether a particular HNB is allowed to operate in a given location, etc). If the HNB-GW accepts the registration attempt the PLMN-ID received in the request shall be used to lookup the PLMN to RNC id mapping table and corresponding RNC-ID shall be returned in the HNB-REGISTER-ACCEPT message else the HNB-GW may reject the registration request (e.g. due to network congestion, blacklisted HNB, unauthorized HNB location, etc). In reject case, the HNB-GW shall respond with a HNB-REGISTER-REJECT indicating the reject cause.



IMPORTANT: The HNB shall start broadcasting only after successful registration with the HNB-GW.

UE Registration Procedure

This section describes the UE registration procedure for HNB provides means for the HNB to convey UE identification data to the HNB-GW in order to perform access control for the UE in the HNB GW. The UE Registration also informs the HNB-GW of the specific HNB where the UE is located.

The UE registration procedure generally triggers when the UE attempts to access the HNB through an initial NAS message and there is no context id in the HNB for specific UE.

UE Registration procedure is described for following scenarios:

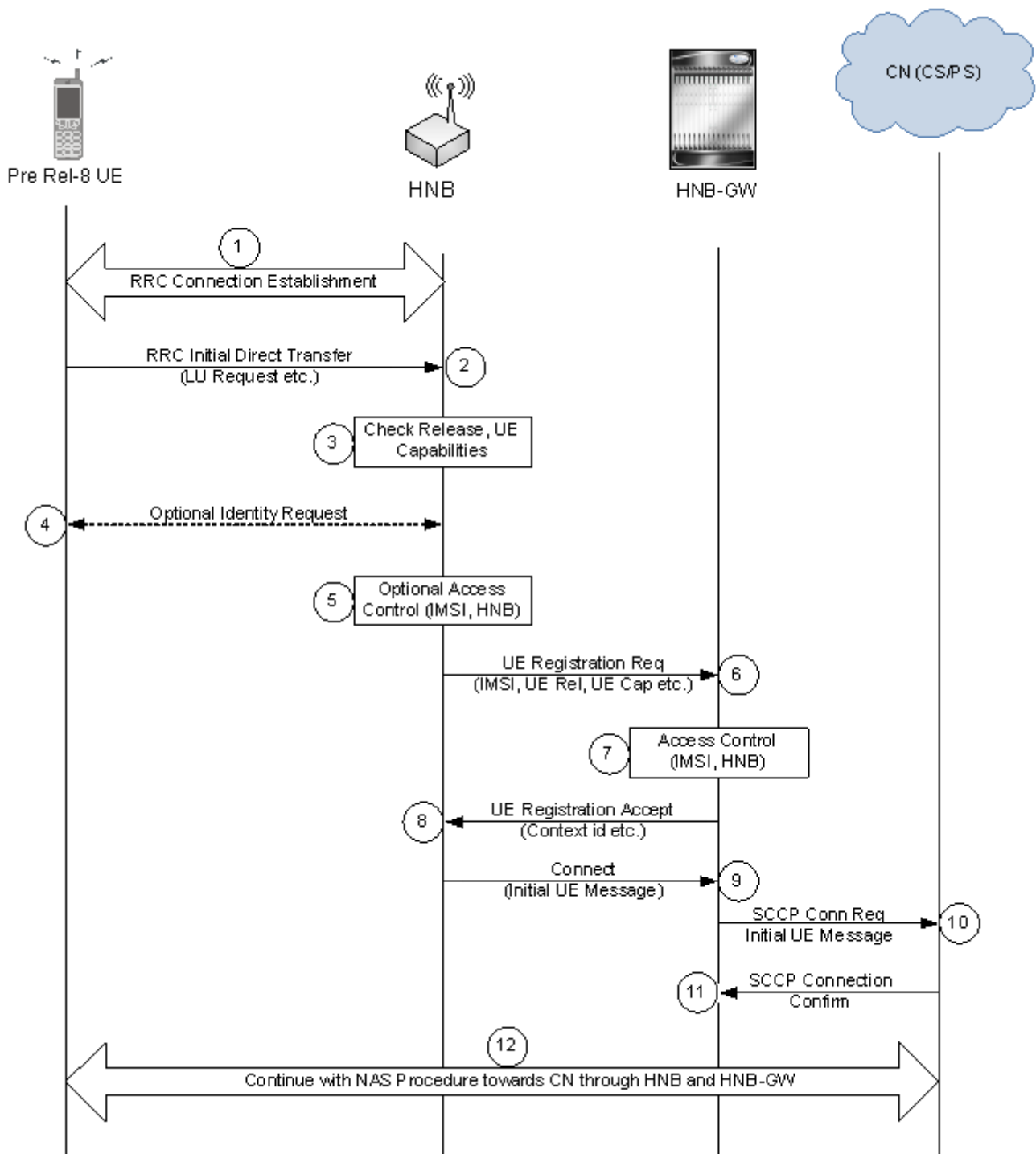
- UE Registration Procedure of Non-CSG UEs or Non-CSG HNBs
- UE Registration Procedure of CSG UEs and CSG or Hybrid HNBs

UE Registration Procedure of Non-CSG UEs or Non-CSG HNBs

This procedure is applicable for non-CSG UEs or HNBs.

The following figure and the text that follows describe the message flow for UE registration procedure of Non-CSG UEs or Non-CSG HNBs:

Figure 5. UE Registration Call Flow for Non-CSG UEs or Non-CSG HNBs



1. Upon camping on the HNB, the UE initiates an initial NAS procedure (e.g. LU Procedure) by establishing an RRC connection with the HNB. UE capabilities are reported to the HNB as part of the RRC Connection establishment procedure.

2. The UE then transmits a RRC Initial Direct Transfer message carrying the initial NAS message (e.g. Location Updating Request message) with identity (IMSI or TMSI).
3. The HNB checks UE capabilities provided in step 1, if these indicate that CSG is not supported and if the identity of the UE (provided during RRC Connection Establishment) is unknown at the HNB being accessed, i.e. no Context id exists for the UE, the HNB initiates UE registration towards HNB-GW (step 6-8).
4. Before starting the UE Registration procedure, HNB optionally triggers the Identification procedure asking for the UE IMSI, if such identity is not provided during the RRC Connection Establishment. If the HNB has a context id for the UE, the UE registration procedure is not performed nor the Identification procedure.
5. The HNB may optionally perform access control based on IMSI and provided access control list.
6. The HNB attempts to register the UE on the HNB-GW by transmitting the UE-REGISTER-REQUEST. The message contains at a minimum:
 - **UE Identity:** IMSI of the (U)SIM associated with the UE and the indication about UE capabilities provided in step 1.



IMPORTANT: The UE IMSI provided in the UE-REGISTER message is unauthenticated.

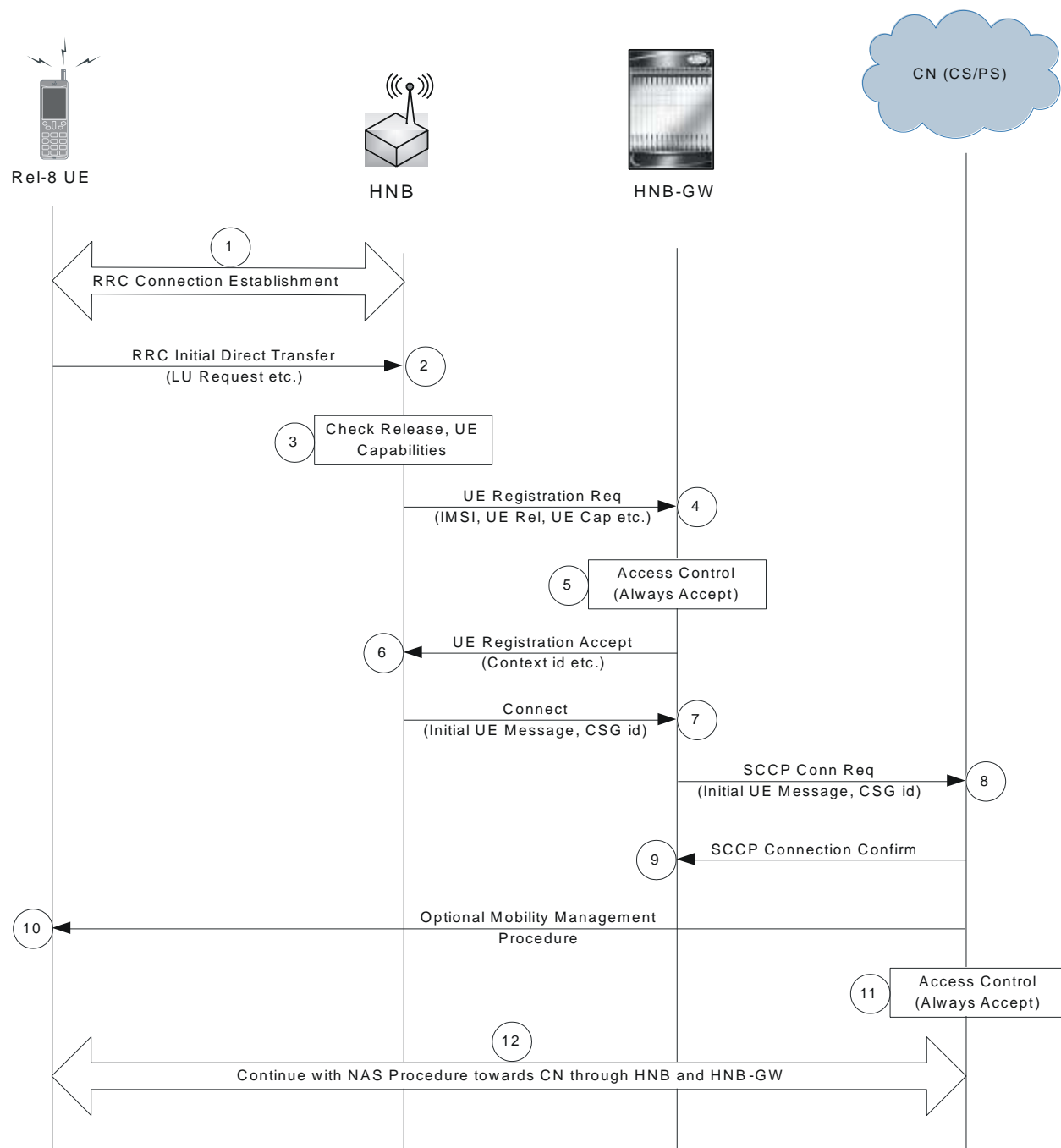
7. The HNB-GW checks UE capabilities and if these indicate that CSG is not supported the HNB-GW shall perform access control for the particular UE attempting to utilize the specific HNB.
8. If the HNB-GW accepts the UE registration attempt it shall allocate a context-id for the UE and respond with a UE-REGISTER-ACCEPT message, including the context-id, to the HNB. If the HNB-GW chooses to not accept the incoming UE registration request then the HNB-GW shall respond with a UE-REGISTRATION-REJECT message.
9. The HNB then sends a RUA (RANAP User Adaptation) CONNECT message containing the RANAP Initial UE message to HNB-GW.
10. The reception of the RUA CONNECT message at the HNB-GW triggers the setup of SCCP connection by the HNB-GW towards the CN. HNB-GW forwards the Initial UE Message to CN.
11. The CN response with a SCCP Connection Confirm message to HNB-GW.
12. The UE then continue with the NAS procedure (e.g. Location Updating procedure) towards the CN, via HNB and the HNB-GW.

UE Registration Procedure of CSG UEs and CSG or Hybrid HNBs

This procedure is applicable for CSG UEs and CSG or Hybrid HNBs.

The following figure and the text that follows describe the message flow of UE registration procedure for CSG UEs and CSG or Hybrid HNBs..

Figure 6. UE Registration Call Flow of CSG UEs and CSG or Hybrid HNBs



1. Upon camping on the HNB, the UE initiates an initial NAS procedure (e.g. LU Procedure) by establishing an RRC connection with the HNB. UE capabilities are reported to the HNB as part of the RRC Connection establishment procedure.
2. The UE then transmits a RRC Initial Direct Transfer message carrying the initial NAS message (e.g. Location Updating Request message) with identity (IMSI or TMSI).
3. The HNB checks UE capabilities provided in step 1, if these indicate that CSG is supported and if the identity of the UE (provided during RRC Connection Establishment) is unknown at the HNB being accessed, i.e. no

Context id exists for the UE, the HNB initiates UE registration towards HNB-GW (step 4-6). If the HNB has a context id for the UE neither UE registration procedure is performed nor the Identification procedure is triggered.

4. The HNB attempts to register the UE on the HNB-GW by transmitting the UE-REGISTER-REQUEST. The message contains at a minimum:
 - **UE Identity:** IMSI of the (U)SIM associated with the UE and the indication about UE capabilities provided in step 1.



IMPORTANT: The UE IMSI provided in the UE-REGISTER message is unauthenticated.

5. The HNB-GW checks UE capabilities and if these indicate that CSG is supported the HNB-GW shall accept the UE registration and allocate a context-id for the UE.
6. HNB-GW respond with a UE-REGISTER-ACCEPT message back to the HNB including a context-id allocated to the UE.
7. The HNB then sends a CONNECT message containing the RANAP Initial UE message.
8. The reception of the CONNECT message at the HNB-GW triggers the setup of SCCP connection by the HNB-GW towards the CN. HNB-GW forwards the Initial UE Message and the CSG id of HNB.
9. The CN response with a SCCP Connection Confirm message.
10. The CN may optionally perform Mobility Management procedures, e.g. Authentication procedure.
11. The CN performs access control of UE.
12. After granted access the UE then continue with the NAS procedure (e.g. Location Updating procedure) towards the CN, via HNB and the HNB-GW.

Iu Connection Procedures

This section describes call flow for Iu connection procedures on HNB-GW.

Following procedure call flows are described for Iu connection procedures between HNB, HNB-GW, and SGSN/MSC in core network:

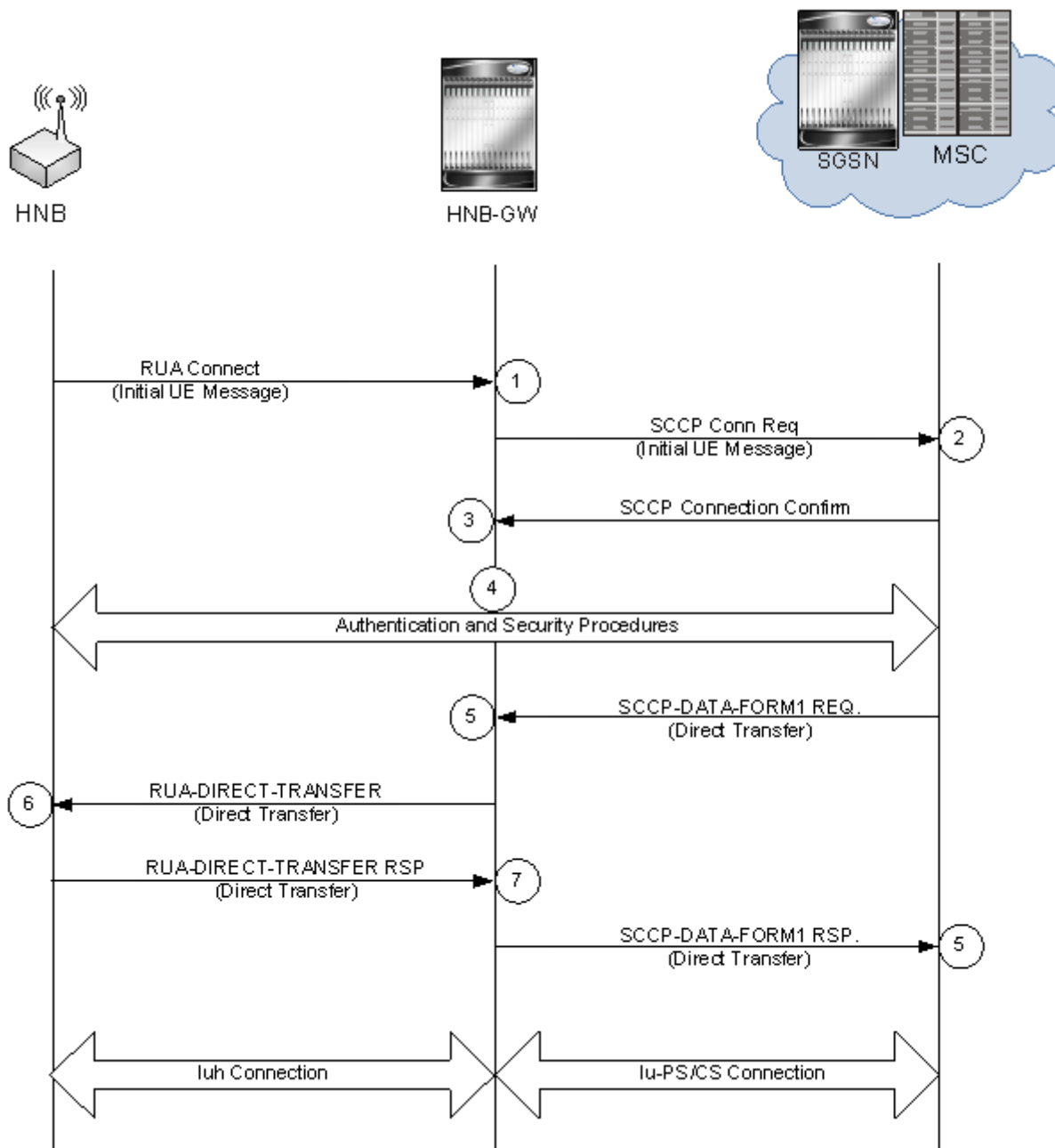
- Iu Connection Establishment Procedure
- Network Initiated Iu Connection Release Procedure

Iu Connection Establishment Procedure

This procedure is applicable for establishment of Iuh and Iu-PS/CS connection between HNB to HNB-GW and HNB-GW to SGSN/MSC in core network.

The following figure and the text that follows describe the message flow for an Iu connection establishment procedure.

Figure 7. Iu Connection Establishment Call Flow



1. Upon receiving of UE-REGISTER-ACCEPT message from HNB-GW, the HNB then sends a RUA CONNECT message to HNB-GW containing the RANAP Initial UE message.
2. The reception of the RUA CONNECT message at the HNB-GW triggers the setup of SCCP connection by the HNB-GW towards the CN (SGSN/MSC). HNB-GW forwards the Initial UE Message.
3. The CN responds with a SCCP Connection Confirm message.
4. The UE then continue with the authentication and security procedures towards the CN, via HNB and the HNB-GW.
5. The SGSN/MSC performs Direct Transfer procedure with HNB-GW and sends SCCP-DATA-FORM1 REQ to HNB-GW.

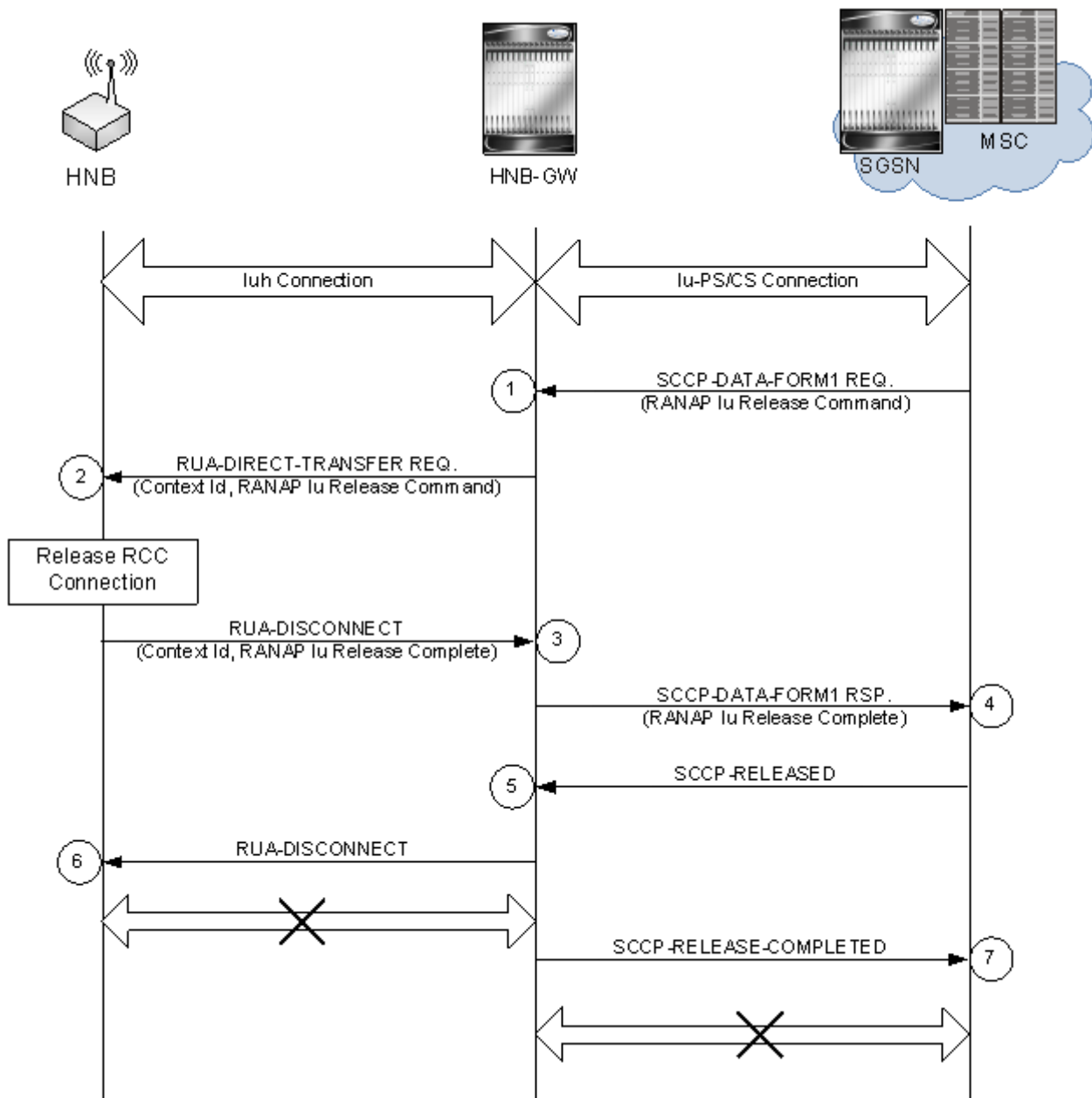
6. The HNB-GW uses the information received in Direct Transfer procedure from CN and forwards the same to HNB through RUA-DIRECT-TRANSFER message.
7. On successful acceptance of RUA-DIRECT-TRANSFER message the HNB responds to HNB-GW and sends RUA-DIRECT-TRANSFER Response message to HNB-GW.
8. On reception of successful acceptance of RUA-DIRECT-TRANSFER message from HNB, the HNB-GW sends SCCP-DATA-FORM1 (Direct Transfer) Response message to CN (SGSN/MSC). This completes the establishment of Iuh and Iu-PS/CS connection through HNB, HNB-GW, and SGSN/MSC in core network.

Network Initiated Iu Connection Release Procedure

This procedure is applicable for release of Iuh and Iu-PS/CS connection between HNB to HNB-GW and HNB-GW to SGSN/MSC in core network.

The following figure and the text that follows describe the message flow for an Iu connection release procedure initiated by CN (SGSN/MSC).

Figure 8. Network Initiated Iu Connection Release Call Flow



1. User session is established between UE and CN via HNB and HNB-GW over Iu interface and CN (SGSN/MSC) starts RANAP Iu Release procedure with HNB-GW and sends SCCP-DATA-FORM1 REQ with RANAP Iu Release command to HNB-GW.
2. The HNB-GW uses the information received in SCCP-DATA-FORM1 REQ with RANAP Iu Release procedure from CN and forwards the same to HNB through RUA-DIRECT-TRANSFER message with RANAP Iu Release command.
3. On reception of RANAP Iu Release command in RUA-DIRECT-TRANSFER message the HNB triggers the RCC Connection Release procedure and responds to HNB-GW with RANAP Iu Release Complete command in RUA-DISCONNECT Response message.

4. On reception of successful RANAP Iu Release Complete command in RUA-DISCONNECT Response message from HNB, the HNB-GW sends RANAP Iu Release Complete command in SCCP-DATA-FORM1 Response message to CN (SGSN/MSC).
5. On reception of RANAP Iu Release Complete command in SCCP-DATA-FORM1 Response message from HNB-GW, CN sends SCCP-RELEASED message to HNB-GW and triggers the associated SCCP connection.
6. On reception of SCCP-RELEASED message from CN, the HNB-GW sends RUA-DISCONNECT message to HNB and disconnect the Iuh connection with HNB.
7. After successful completion of RUA-DISCONNECT procedure and Iuh connection release, HNB-GW sends SCCP-RELEASE-COMPLETE message to CN and HNB-GW confirms the Iu-PS/CS connection released between HNB-GW and CN.

Supported Standards

The HNB-GW complies with the following standards for 3G UMTS Femto wireless data services.

- [3GPP References](#)
- [IETF References](#)
- [ITU-T Recommendations](#)
- [Object Management Group \(OMG\) Standards](#)

3GPP References

- 3GPP TS 25.467 V8.0.0. (2008-12): 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN architecture for 3G Home NodeB; Stage 2 (Release 8)
- 3GPP TS 25.467 V9.1.0 (2009-12): 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN architecture for 3G Home Node B (HNB); Stage 2 (Release 9)
- 3GPP TS 25.468 V8.0.0 (2008-12): 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iuh Interface RANAP User Adaptation (RUA) signalling (Release 8)
- 3GPP TS 25.468 V9.0.0 (2009-12): 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iuh Interface RANAP User Adaptation (RUA) signalling (Release 9)
- 3GPP TS 25.469 V8.1.0 (2009-03): 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iuh interface Home Node B Application Part (HNBAP) signalling (Release 8)
- 3GPP TS 25.469 V9.0.0 (2009-12): 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iuh interface Home Node B Application Part (HNBAP) signalling (Release 9)
- 3GPP TS 33.320 V9.1.0 (2010-03): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security of Home Node B (HNB) / Home evolved Node B (HeNB) (Release 9)

IETF References

- RFC-768, User Datagram Protocol (UDP), 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-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-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-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-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-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-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

ITU-T Recommendations

- ITU-T Recommendation Q.2630.1 - AAL type2 signalling protocol (Capability Set 1)
- ITU-T Recommendation Q.2630.2 - AAL type2 signalling protocol (Capability Set 2)
- ITU-T Recommendation I.361 B-ISDN ATM layer specification
- ITU-T Recommendation I.363.2 B-ISDN ATM Adaptation Layer (AAL) Specification: Type 2 AAL
- ITU-T Recommendation I.366.1 Segmentation and Reassembly Service Specific Convergence Sublayer for the AAL type 2
- ITU-T Recommendation Q.2150.1 AAL type 2 signaling transport converter on broadband MTP
- ITU-T Recommendation E.164 - The international public telecommunication numbering plan
- ITU-T Recommendation E.191 - B-ISDN addressing

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 Security Gateway (SeGW) and Home-NodeB Gateway (HNB-GW) functionality for 3G UMTS networks.

The system functioning as an HNB-GW is capable of supporting the following types of subscriber sessions:

- **CS Session over Iu-CS:** The subscriber is provided voice, video, and CS data service on circuit switch session through MSC in CS network.
- **PS Session over Iu-PS:** The subscriber is provided packet switch connection with different traffic class on PS session with GSN in PS.
- **Network-initiated Session:** A paging procedure initiated by MSC/SGSN/GGSN for a specific subscriber is send to HNB-GW and in turn HNB-GW initiates a paging procedure with HNBs to page the UE and establish a bearer context.

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 3G UMTS network, the HNB access radio network containing the Home-NodeBs (HNBs) would communicate with the system via Iuh interfaces configured within the source context as part of the HNB-GW service.
- **Destination context:** Also referred to as the “egress” context, this context is where a subscriber is provided connectivity to core network (such as access to the MSC, SGSN, GGSN etc.) as configured on HNB-GW service and related services. For example, the system's destination context would be configured with the Iu-CS, Iu-PS, Gn, Gi or IP offload interfaces facilitating subscriber data traffic to/from the core network (MSC, SGSN, GGSN) or other PDN (Mobile Data Service or Internet).
- **AAA context:** This context provides AAA functionality for subscriber bearer contexts and/or administrative user sessions and contains the policies and logical interfaces for communication between Security Gateway (SeGW) and a 3GPP AAA Server or 3GPP AAA proxy (OCS/CGF/AAA/HSS) over AAA interface for authentication and authentication procedures for Femto user.

In the roaming case, the 3GPP AAA Proxy can act as a stateful proxy between SeGW and 3GPP AAA Server.

The AAA server is responsible for transfer of subscription and authentication data for authenticating/authorizing user access and UE authentication. The SeGW communicates with the AAA on the PLMN using AAA interface.



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.

- **Local context:** This is the default context on the system used to provide out-of-band management functionality.

Logical Interfaces

This section describes the logical interface supported on HNB-GW.

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 an HNB-GW service, it will function as an Iuh interface between the SeGW (HNB-GW) service and the HNB. Services are defined later in this section.

In support of both mobile and network originated subscriber UE contexts, the HNB-GW provides the following network interface support:

- **Iuh Interface:** This interface is the reference point for the control plane protocol between Home NodeB and HNB-GW. Iuh uses SCTP over IPsec IKEv2 tunnel as the transport layer protocol for guaranteed delivery of signaling messages between HNB-GW and Home NodeB.

This is the interface used by the HNB-GW to communicate with HNB on the same Femtocell Access Network. This interface serves as path for establishing and maintaining subscriber UE contexts.

One or more Iuh interfaces can be configured per system context.
- **IuCS:** This interface is the reference point in UMTS which links the HNB-GW, which acts as an RNC (Radio Network Controller), with a Mobile Switching Centre (3G MSC) in the 3G UMTS Femtocell Access Network.. This interface provides an IuCS over IP or IuCS over ATM (IP over AAL5 over ATM) interface between the MSC and the RNC (HNB-GW) in the 3G UMTS Femtocell Access Network. RAN Application Part (RANAP) is the control protocol that sets up the data plane (GTP-U) between these nodes. SIGTRAN (M3UA/SCTP) or QSAAL (MTP3B/QSAAL) handle IuCS (control) for the HNB-GW.

This is the interface used by the HNB-GW to communicate with 3G MSC on the same Public Land Mobile Network (PLMN). This interface serves as path for establishing and maintaining the CS access for Femtocell UE to circuit switched UMTS core networks

One or more IuCS interfaces can be configured per system context.
- **IuPS:** This interface is the reference point between HNB-GW and SGSN. This interface provides an IuPS over IP or IuPS over ATM (IP over AAL5 over ATM) interface between the SGSN and the RNC (HNB-GW) in the 3G UMTS Femtocell Access Network. RAN Application Part (RANAP) is the control protocol that sets up the data plane (GTP-U) between these nodes. SIGTRAN (M3UA/SCTP) or QSAAL (MTP3B/QSAAL) handle IuPS-C (control) for the HNB-GW.

This is the interface used by the HNB-GW to communicate with SGSN on the same Public Land Mobile Network (PLMN). This interface serves as path for establishing and maintaining the PS access for Femtocell UE to packet switched UMTS core networks.

One or more Iu-PS interfaces can be configured per system context.
- **Gi:** This interface is the reference point between HNB-GW and IP Offload Gateway. It is used by the HNB-GW to communicate with Packet Data Networks (PDNs) through IP Offload Gateway in the H-PLMN/V-PLMN. Examples of PDNs are the Internet or corporate intranets.

One or more Gi interfaces can be configured per system context.
- **Gn:** This interface is the reference point between HNB-GW and GGSN. It is used by the HNB-GW to communicate with GGSNs on the same GPRS/UMTS Public Land Mobile Network (PLMN).

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

- **TR-069:** This interface is an application layer protocol which is used for remote configuration of terminal devices, such as DSL modems, HNBs and STBs. TR-069 provides an auto configuration mechanism between the HNB and a remote node in the service provider network termed the Auto Configuration Server. The standard also uses a combination of security measures including IKEv2 (Internet Key Exchange v2) and IPsec (IP Security) protocols to authenticate the operator and subscriber and then guarantee the privacy of the data exchanged.

One TR-069 interface can be configured per HNB node.

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 and Networks

This section describes the services configured on HNB-GW to support various functionality.

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

- **HNB-GW services:** HNB-GW services are configured in Context configuration mode to support both mobile-initiated and network-requested user contexts. The HNB-GW service must be bound to a logical interface within the same context. Once bound, the interface takes on the characteristics of an Iuh interface. Multiple services can be bound to the same logical interface. Therefore, a single physical port can facilitate multiple Iuh interfaces.
- **Radio Network PLMN:** The Radio Network PLMN is configured in HNB-GW service is required to associate PLMNs with HNB-GW. The PLMN specific configuration e.g. RNC id and association of CS or PS network shall be configured under this configuration mode.
- **CS Network:** CS Network is a context independent configuration to define circuit switched networks. This circuit switched network configuration provides parameters for one or more MSCs where CS-domain Iu-connections shall be routed. In a typical deployment HNB-GW is connected to only one MSC.

CS network configured at the system level need to be associated with a Radio Network PLMN configured within HNB-GW service with desired granularity; PLMN level or location-area in that PLMN.

- **PS Network:** PS Network is a context independent configuration to define packet switched networks . This packet switched network configuration provides parameters for one or more SGSN where PS-domain Iu-connections shall be routed. In a typical deployment HNB-GW is connected to only one SGSN.

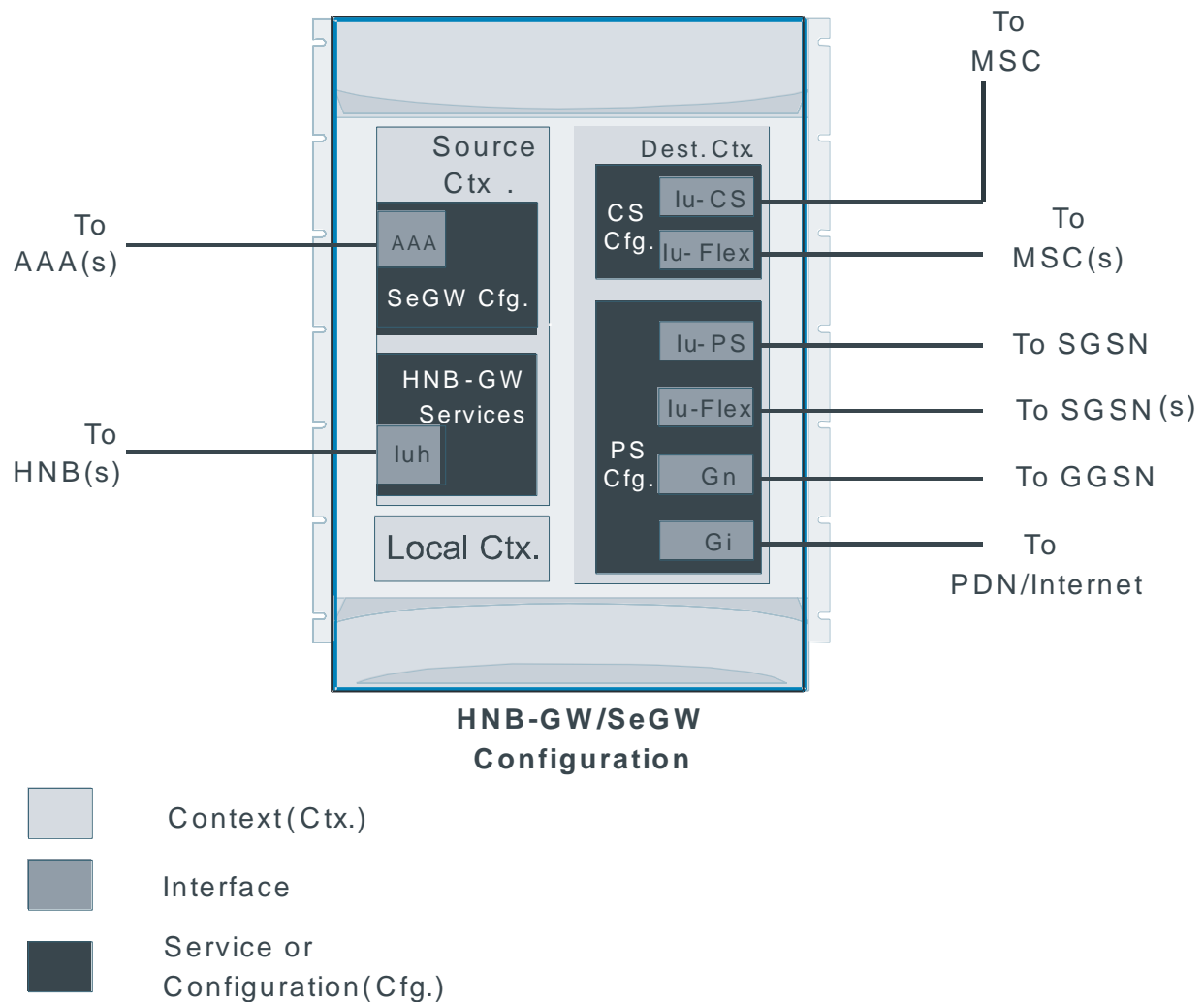
PS network configured at the system level need to be associated with a Radio Network PLMN configured within HNB-GW service with desired granularity.

- **GTP-U services:** GTP-U services are configured in Context configuration mode in pair of two services; one for GTP-U tunnel support towards HNB on Iuh interface and another for GTP-U tunnel support towards the core network on IuPS interface to communicate with SGSN respectively.

The system supports multiple GTP-U interface connections over this service. Although this service can be configured in any independent context, but for Iuh interface it must be configured in the same context as HNB-GW; i.e. source context.

Following figure illustrates the relationship between services, interfaces, and contexts within the HNB-GW system for HNB access 3G UMTS networks.

Figure 9. Service, Interface, and Context Relationship Within the System



The source context used to service a subscriber session is the same as the context in which the HNB-GW service is configured. Each HNB-GW service is bound to an IP address in a source context. The HNBs select which IP address to use, typically by using DNS. Once a UE has established a bearer context with an HNB-GW, the HNBs continue to use the same context as the subscriber anchored to that HNB-GW.

The destination contexts used to service a subscriber session to connect with CN.

The system determines the configuration used in destination context based on the parameter contained within the information received from HNB and also the configuration in HNB-GW service.

The AAA context or AAA configuration in source context uses that context for subscriber authentication.

Chapter 3

HNB-GW Service Configuration Procedures

This chapter is meant to be used in conjunction with the other chapters that describes the information needed to configure the system to support HNB-GW functionality for use in HNB access 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.

This chapter describes following:

- [Information Required to Configure the System as an HNB-GW](#)
- [RTP Pool Configuration](#)
- [HNB GW Service Configuration](#)
- [Event IDs for HNB-GW Service](#)



IMPORTANT: At least one Packet Services Card (PSC/PSC2) must be made active prior to service configuration. Information and instructions for configuring PSCs/PSC2s 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.

Information Required to Configure the System as an HNB-GW

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an HNB-GW node in a test environment. Information provided in this section includes the following:

- [Required Local Context Configuration Information](#)
- [Required System-Level Configuration Information](#)
- [Required Source Context Configuration Information](#)
- [Required Destination Context Configuration Information](#)

Required Local Context Configuration Information

The following table lists the information that is required to configure the local context on an HNB-GW.

Table 1. Required Information for Local Context Configuration

Required Information	Description
Management Interface Configuration	
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	IPv4 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
Security administrator name	The name or names of the security administrator with full rights to the system.
Security administrator password	Open or encrypted passwords can be used.
Remote access type(s)	The type of remote access that will be used to access the system such as telnetd, sshd, and/or ftpd.

Required System-Level Configuration Information


The following table lists the information that is required to configure at the system-level Global configuration mode (context independent) to support 3G UMTS Femto support.

Table 2. Required Information for System Configuration

Required Information	Description
SS7 Routing Domain Configuration	
SS7 Routing Domain id and variant	<p>An identification for SS7 routing domain and must be an integer between 1 and 12 by which the SS7 routing domain will be identified and configured.</p> <p>A variant can be configured for the SS7 routing domain. some of them are:</p> <ul style="list-style-type: none"> • ansi: American National Standards Institute (U.S.A.) • bici: Broadband Inter-carrier Interface standard • china: Chinese standard • itu: International Telecommunication Union (ITU-T) Telecommunication Standardization Sector • ntt: Japanese standard • ttc: Japanese standard
Sub Service Field (SSF)	<p>A network indicator in the subservice field for SS7 message signal units (MSUs). It can be configured with any of the following indicators:</p> <ul style="list-style-type: none"> • International • National • Reserved • Spare
Application Server Process (ASP) instance	<p>An M3UA Application Server Process (ASP) instance identified from 1 through 4. This instance needs to configure end point address as well.</p>
Peer server id	<p>Specifies a peer server instance to setup a SIGTRAN peer for sending and receiving M3UA traffic. Up to 49 peer servers can be defined.</p> <p>A peer server id configuration may contain:</p> <ul style="list-style-type: none"> • Routing context for peer server to use • Self point code in SS7 type address • Operational Mode • Peer Server Process (PSP) instance

■ Information Required to Configure the System as an HNB-GW

Required Information	Description
Peer Server Process (PSP) instance	<p>Specifies the peer server process instance in peer server id. The instance must be an integer from 1 to 4. A PSP instance configuration need to define:</p> <ul style="list-style-type: none"> • PSP mode: client or server • Exchange mode: double ended or single ended • End point address in SS7 address format • Association of ASP instance
Signaling Connection Control Part (SCCP) Network Instance Configuration	
SCCP Network Instance and variant	<p>An identification for SCCP network instance and must be an integer between 1 and 12 by which the SCCP network instance will be identified and configured. A variant can be configured for the SS7 routing domain. some of them are:</p> <ul style="list-style-type: none"> • ansi: American National Standards Institute (U.S.A.) • china: Chinese standard • itu: International Telecommunication Union (ITU-T) Telecommunication Standardization Sector • ntt: Japanese standard • ttc: Japanese standard
SS7 Routing Domain id and variant	An identification for SS7 routing domain and must be an integer between 1 and 12 by which the SS7 routing domain will be identified and associated with this SCCP network instance.
Destination point code	Specifies the destination point code (DPC) in SS7 address format along with SSN and SCCP version.
Circuit Switched Network Configuration	
Circuit Switched Network instance	<p>An identification string between 1 and 63 characters (alpha and/or numeric) by which the Circuit Switched Core Networks instance which needs to be associated with HNB Radio Network PLMN id. An HNB-CS network instance is required for Femto UMTS access over IuCS/IuFlex interface between HNB-GW service and CS networks elements; i.e. MSC/VLR. Multiple CS network instances (maximum 8) can be configured on a system.</p>
SCCP Network id	Specifies a predefined Signaling Connection Control Part (SCCP) network id in at system level in Global configuration mode to be associated with the CS network instance in order to route the messages towards MSC/VLR over IuCS interface.
RTP IP Pool name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the RTP pool is configured and associated with CS network configuration to allocate RTP IP address over IuCS towards CS core networks.
Default MSC point code	Specifies the default MSC point-code with HNB-CS network instance. This MSC point code (SS7 address) is used when HNB-GW is to be connected to only one MSC with in a CS network or as default MSC for all HNBs connected through specific HNB-CS network instance.
Packet Switched Network Configuration	

Required Information	Description
Packet Switched Network instance	An identification string between 1 and 63 characters (alpha and/or numeric) by which the Packet Switched Core Networks instance which needs to be associated with HNB Radio Network PLMN id. An HNB-CS network instance is required for Femto UMTS access over IuPS/IuFlex interface between HNB-GW service and PS networks elements; i.e. SGSN. Multiple PS network instances (maximum 8) can be configured on a system.
SCCP Network id	Specifies a predefined Signaling Connection Control Part (SCCP) network id in at system level in Global configuration mode to be associated with the PS network instance in order to route the messages towards SGSN over IuPS interface.
GTP-U service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service can be associated with HNB-GW system in PS network instance for GTP-U tunnel towards core network. It is preconfigured in destination context. Multiple names are needed if multiple GTP services is used. <div style="border: 1px solid black; padding: 5px; margin: 10px 0;">  IMPORTANT: One GTP-U service can be associated in PS network instance to provide GTP-U tunnel over IuPS interface towards PS core network and another GTP-U service needs to be associated in HNB-GW service instance for GTP-U tunnel over Iuh interface towards HNB. </div>
Default SGSN point code	Specifies the default SGSN point-code with HNB-CS network instance. This SGSN point code (SS7 address) is used when HNB-GW is to be connected to only one SGSN with in a PS network or as default SGSN for all HNBs connected through specific HNB-PS network instance.

Required Source Context Configuration Information


The following table lists the information that is required to configure the Source context on an HNB-GW.

Table 3. 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 is recognized by the system. Generally it is identified as source context.
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.

■ Information Required to Configure the System as an HNB-GW

Required Information	Description
Iuh Interface Configuration (To/from Home-NodeB)	
HNB-GW service Name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the HNB-GW service can be identified on the system. It is configured in Context configuration mode. Multiple names are needed if multiple HNB-GW services will be configured.
HNB-GW Service Configuration	
Iuh interface IP address	IPv4 addresses assigned to the Iuh interface as SCTP bond address. This address will be used for binding the SCTP (local bind address(es)) to communicate with the HNBs using GTP-U. The HNB-GW passes this IP address during setting up the SCTP association with the HNB. Multiple addresses and subnets are needed if multiple interfaces will be configured.
Iuh SCTP Port	The physical port to which the Iuh interface will be bound. The local SCTP port used to communicate with the HNBs over Iuh interface.
RTP IP address	This is the IP address of HNB-GW which is configured as RTP address and sent to HNB to map the RTP streams with this IP address on HNB-GW. This configuration is required at HNB-GW to communicate with MSC/VLR over IuCS-over-IP tunnel.
Optional Security Gateway Configuration	
Security Gateway IP address	This is the IP Address where the SeGW service is bound and shall be provided to HNB during SeGW-Discovery. Only one SeGW IP address can be configured.
IPsec Crypto-map Template Configuration	
EAP profile	This is the profile to be used to provide authenticator modes for incoming packets on Security Gateway. Only one EAP profile can be configured.
IP Pool for IPsec Tunnel	Specifies the IP pool to assign IP address for IPsec traffic to use.
IKEv2 Transform set	IKEv2 transform set for IKE security association.
IPsec Crypto-map Template	Specifies the Crypto-map template to be used for IPsec IKEv2 tunneling for the interface configured as an Iuh. This crypto-map template is to be associated with HNB-GW service if SeGW is enabled and bind with HNB-GW service. Only one IPsec Crypto-map Template can be configured.
AAA Server Group Context name	Specifies the name of the context in which a AAA server group is configured for association with SeGW for AAA parameters during subscriber authentication phases.
AAA Server Group name	Specifies the AAA server group already configured in a context and is to be used for first/second phase of authentication of subscriber while using SeGW functionality in an HNB-GW service.
Radio Network PLMN Configuration	
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.

Required Information	Description
Radio Network Controller (RNC) identifier	Specify the RNC id which shall be provided to HNB during HNB-REGISTRATION procedure. Depending upon the requirement the RNC-ID can be provided at the desired granularity as given below follows: <ul style="list-style-type: none"> • LAC id: Location Area identifier • RAC id: Routing Area identifier • Cell id: Cell identifier
GTP-U service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service can be associated with HNB-GW system in HNB-GW service for GTP-U tunnel towards HNB access network (HNB). It is preconfigured in Context configuration mode. Multiple names are needed if multiple GTP-U services is used. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  IMPORTANT: One GTP-U service can be associated with HNB-GW service instance to provide GTP-U tunnel over Iuh interface towards HNB access network (HNB) and another GTP-U service needs to be associated with PS network instance for GTP-U tunnel over IuPS interface towards PS core network to GSNs. </div>
GTP-U Tunnel Innerves Configuration	
GTP-U service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service can be associated with HNB-GW system for GTP-U tunnel towards HNB access network (HNB). Various control parameters can be configured for GTP-U packet transmission. Multiple names are needed if multiple GTP services is used.
GTP-U Tunnel interface IP address	IPv4 addresses assigned to the interface as GTP-U bond address. This address will be used for binding the GTP-U service (local bind address(es)) for sending/receiving GTP-U packets from/to HNB using GTP-U tunnel. Multiple addresses and subnets are needed if multiple interfaces will be configured.
GTP-U Tunnel interface Port	The physical port to which the Iuh interface will be bound. The local GTP-U port used to communicate with the HNB over GTP-U tunnel interface.

Required Destination Context Configuration Information

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

Table 4. 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.

■ Information Required to Configure the System as an HNB-GW

Required Information	Description
Interface name	An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface is recognized by the system. Multiple names are needed if multiple interfaces will be configured.
IP address and subnet	IPv4 addresses assigned to the interface. Multiple addresses and 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 followed by the number of the physical connector on the card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Gateway IP address	Used when configuring static IP routes from the management interface(s) to a specific network.
GTP-U Tunnel Interface Configuration	
GTP-U service name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the GTP-U service can be associated with HNB-GW system in PS network instance for GTP-U tunnel towards core network. Various control parameters can be configured for GTP-U packet transmission. Multiple names are needed if multiple GTP services is used.
GTP-U Tunnel interface IP address	IPv4 addresses assigned to the interface as GTP-U bond address. This address will be used for binding the GTP-U service (local bind address(es)) for sending/receiving GTP-U packets from/to PS core network using GTP-U tunnel. Multiple addresses and subnets are needed if multiple interfaces will be configured.
GTP-U Tunnel interface Port	The physical port to which the Iuh interface will be bound. The local GTP-U port used to communicate with the PS core network over GTP-U tunnel interface.
RTP Pool Configuration	
RTP IP Pool name	An identification string from 1 to 63 characters (alpha and/or numeric) by which the RTP pool can be identified on the system to allocate RTP IP address over IuCS towards CS core networks. It is to be associated with PS network configuration.

RTP Pool Configuration

One of the steps in establishing a RTP session between the UE and the core network through HNB and HNB-GW service running on the system is that upon successful authentication, the UE is assigned an RTP IP address. The IP address could be dynamically assigned from a pool that is configured on the system. It may also be an address that is statically configured in the user profile or even one that is requested by the subscriber.

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: Note that setting different priorities on each individual pool can cause addresses in some pools to be used more frequently.

To configure the RTP IP pool:

- Step 1** Create the RTP IP pool for IPv4 addresses in source context for RTP pool allocation over Iuh interface by applying the example configuration in the *IPv4 RTP Pool Creation Over IuCS* section.
- Step 2** Create the RTP IP pool for IPv4 addresses in destination context for RTP pool allocation over IuCS interface by applying the example configuration in the *IPv4 RTP Pool Creation Over Iuh* section.
- Step 3** Verify your RTP IP pool configuration by applying the example configuration in the *RTP IP Pool Configuration Verification* section.
- Step 4** Save your configuration as described in the *Saving Your Configuration* chapter.

IPv4 RTP Pool Creation Over IuCS

Use the following example to create the IPv4 address RTP pool for RTP address allocation over IuCS interface towards CS core network.

```
configure
  context <dest_ctxt_name>
    ip pool <cs_ip_pool_name> <ip_address/mask>
  end
```

Notes:

- <cs_ip_pool_name> is name of the IP pool configured in destination context named <dest_ctx_name> and to be associated with CS Network Configuration to allocate RTP end point address towards CS network over IuCS interface.

- To ensure proper operation with CS network configuraiton, RTP 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 PSCs/PSC2s 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 **ip pool** command section in *Context Configuration Mode Commands* chapter of *Command Line Interface Reference*.

RTP 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 will 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				

HNB GW Service Configuration

HNB-GW services are configured within source contexts and allow the system to function as an HNB-GW in the 3G UMTS wireless data network.



IMPORTANT: This section provides the minimum instruction set for configuring an HNB-GW service that allows the system to process bearer contexts with IPsec authentication on SeGW. Commands that configure additional HNB-GW service properties are provided in the different chapters 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 HNB-GW service with SeGW enabled:

- Step 1** Create an interface in source context for Iuh interface by applying the example configuration in the *Iuh Interface Configuration* section.
- Step 2** Configure SS7 routing domain by applying the example configuration in the *SS7 Routing Domain Configuration* section.
- Step 3** Configure SCCP network id with national variant by applying the example configuration in the *SCCP Network Instance Configuration* section.
- Step 4** Configure CS network parameters by applying the example configuration in the *HNB-CS Network Configuration* section.
- Step 5** Configure PS network parameters by applying the example configuration in the *HNB-PS Network Configuration* section.
- Step 6** Configure GTP-U service parameters by applying the example configuration in the *GTP-U Service Configuration* section.
- Step 7** Create and configure the HNB-GW service and associate related parameters with HNB-GW by applying the example configuration in the *HNB-GW Service Configuration* section.
- Step 8** *Optional.* Configure Security Gateway parameters with Crypto-template and enable SeGW by associating it with HNB-GW to enabling SeGW by applying the example configuration in the *Security Gateway and Crypto Template Configuration* section.
- Step 9** Verify your HNB-GW configuration by following the steps in the *HNB-GW Service Configuration Verification* section.
- Step 10** Save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Iuh Interface Configuration

Use the following example to configure the Iuh interfaces in source context:

```
configure
```

```
context <vpn_ctxt_name> -noconfirm
  interface <intf_name>
    ip address <ip_address>
  end
```

Notes:

- <vpn_ctxt_name> is name of the source context in which HNB-GW service is to configure.
- <intf_name> is name of the interface which is to be used for Iuh reference between HNB-GW and HNB.

SS7 Routing Domain Configuration

Use the following example to configure the SS7 routing domain id for HNB-GW service on system:

configure

```
ss7-routing-domain <ss7rd_id> variant <v_type> -noconfirm
  ssf {international | national | reserved | spare}
  asp instance <asp_instance>
    end-point address <end_point_address> context <end_ctx_name>
    end-point bind
  exit
peer-server id <peer_server_id>
  name <peer_name>
  mode {loadshare | standby}
  routing-context <routing_ctx_id>
  self-point-code <ss7_pointcode>
  psp instance <psp_instance_id>
    psp-mode {client | server}
    exchange-mode [double-ended | single-ended]
    end-point address <end_point_address>
    associate asp instance <asp_instance>
  end
```

Notes:

- `<end_point_address>` is IP address of the end point associated with application server process for M3UA end-point parameters in a specific SS7 routing domain instance.
- `<end_ctx_name>` is name of the context which is associated with end point IP address for application server process for M3UA end-point parameters in a specific SS7 routing domain instance.

SCCP Network Instance Configuration

Use the following example to configure the SCCP network instance to be associated with HNB-GW service on system:

```
configure
```

```
sccp-network <sccp_id> variant <v_type> -noconfirm
  self-point-code <ss7_pointcode>
  associate ss7-routing-domain <ss7rd_id>
  destination dpc <dpc_code> name <dpc_route_name>
  destination dpc <dpc_code> version <sccp_variant>
  destination dpc <dpc_code> ssn <dest_subsystem_num>
end
```

Notes:

- `<sccp_id>` is SCCP network identifier to be associated with HNB-GW.
- `<v_type>` is type of variant to be used for SCCP network instance.

GTP-U Service Configuration

Use the following example to configure the GTP-U service parameters to provide GTP-U tunnel over Iuh and IuPS interface. Separate instances of this service need to be configured for Iuh and IuPS interfaces.

```
configure
```

```
context <dest_ctxt_name> -noconfirm
  gtpu-service <gtpu_ps_svc_name> -noconfirm
  bind address {ipv4-address | ipv6-address} <ip_address>
  path-failure detection-policy gtp echo
end
```

```

configure
context <vpn_ctxt_name> -noconfirm

  gtpu-service <gtpu_iuh_svc_name> -noconfirm

    bind address {ipv4-address | ipv6-address} <ip_address>

    path-failure detection-policy gtp echo

  end

```

Notes:

- <dest_ctxt_name> is name of the destination context in which GTP-U service configured to provide GTP-U tunnel over IuPS interface towards core network.
- <gtpu_ps_svc_name> is name of the GTP-U service configured to provide GTP-U tunnel over IuPS interface towards core network.
- <vpn_ctxt_name> is name of the source context in which HNB-GW service is to be configured. The same context must be used for GTP-U service configuration to provide GTP-U tunnel over Iuh interface towards HNB.
- <gtpu_iuh_svc_name> is name of the GTP-U service configured to provide GTP-U tunnel over Iuh interface towards HNB.

HNB-PS Network Configuration

Use the following example to configure the packet switched network parameters to be associated with HNB-GW service on system:

```

configure

ps-network <ps_network_name> -noconfirm

  associate sccp-network <sccp_network_id>

  associate gtpu-service <gtpu_ps_svc_name> context <dest_ctx_name>

  sgsn point-code <sgsn_ss7_point_code>

end

```

Notes:

- <ps_network_name> is name of the packet switched network to be associated with HNB-GW for PS call.
- <sgsn_ss7_point_code> is address of the SGSN in SS7 point code format to be used for packet switched traffic through HNB-GW.
- <gtpu_svc_name> is name of the GTP-U service configured in <gtpu_ctx_name> to provide GTP-U tunnel over IuPS interface for packet switched traffic towards PS-CN.

HNB-CS Network Configuration

Use the following example to configure the circuit switched network parameters to be associated with HNB-GW service on system:

```
configure
```

```
cs-network <cs_network_name> -noconfirm

  associate rtp-pool <cs_ip_pool_name> context <dest_ctx_name>

  associate sccp-network <sccp_network_id>

  msc point-code <msc_ss7_point_code>

end
```

Notes:

- *<cs_network_name>* is name of the packet switched network to be associated with HNB-GW for CS session.
- *<msc_ss7_point_code>* is address of the MSC in SS7 point code format to be used for circuit switched call through HNB-GW.
- *<cs_ip_pool_name>* is name of the IP pool configured in destination context named *<dest_ctx_name>* to allocate RTP end point address in this CS network over IuCS interface.

HNB-GW Service Configuration

Use the following example to configure the HNB-GW service on system in source context to provide access to HNBs towards core networks:

```
configure
```

```
context <vpn_ctxt_name>

  hnbgw-service <hnbgw_svc_name> -noconfirm

  sctp bind address <ip_address>

  sctp bind port <sctp_port>

  ranap reset hnbgw-initiated

  ranap reset max-retransmissions <max_retrans>

  ranap reset guard-timeout <timeout_dur>

  rtp address <rtp_ip_address>

  rtp mux
```

```

associate rtp-pool <ip_pool_name>

associate gtpu-service <gtpu_iuh_svc_name>

radio-network-plmn mcc <mcc> mnc <mnc_code>

rnc-id <rnc_id>

associate ps-network <cs_network_name>

associate cs-network <cs_network_name>

end

```

Notes:

- *<vpn_ctxt_name>* is name of the source context in which HNB-GW service is configured.
- *<hnbgw_svc_name>* is name of the HNB-GW service which is to be configured for used for Iuh reference between HNB-GW and HNB.
- *<ip_address>* is the SCTP IP address on which is HNB will communicate with HNB-GW and has characteristics of Iuh interface.
- *<gtpu_iuh_svc_name>* is name of the GTP-U service configured in *<vpn_ctxt_name>* to provide GTP-U tunnel over Iuh interface towards HNB.
- *<rtp_ip_address>* is the same as *ip_address* which is mapped by HNB with RTP streams for connectivity with HNB-GW over Iuh. This is a mandatory command to use to make HNB-GW communicating with MSC/VLR through IuCS-over-IP tunnel.
- *<ip_pool_name>* is name of the IP pool configured in source context named *<vpn_ctxt_name>* to allocate RTP end point address in HNB-GW service over Iuh interface.

Security Gateway and Crypto map Template Configuration

Use the following example to configure the IPsec profile and Crypto map template enabling SeGW on HNB-GW for IPsec tunneling.

```

configure

context <vpn_ctxt_name>

  eap-profile <eap_prof_name>

  mode authentication-pass-through

  exit

  ip pool ipsec <ip_address> <subnetmask>

  ipsec transform-set <ipsec_trans_set>

  exit

```

```

ikev2 transform-set <ikev2_trans_set>
    exit
crypto template <crypto_template>
    authentication eap-profile <eap_prof_name>
    exit
ikev2-ikesa transform-set list <ikev2_trans_set>
payload <crypto_payload_name> match childsa [match {ipv4 | ipv6}]
    ip-address-alloc dynamic
    ipsec transform-setlist <ipsec_trans_set>
    exit
ikev2-ikesa keepalive-user-activity
end
configure
context <vpn_ctxt_name>
    hnbgw-service <hnbgw_svc_name>
        security-gateway bind address <segw_ip_address> crypto-template
        <crypto_template>
    end

```

Notes:

- <vpn_ctxt_name> is name of the source context in which HNB-GW service is configured.
- <hnbgw_svc_name> is name of the HNB-GW service which is to be configured for used for Iuh reference between HNB-GW and HNB.

Verifying HNB-GW Configuration

This section shows the configuration parameters configured for HNB-GW service.

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

```
show hnbgw-service hnbgw-service <hnbgw_svc_name>}
```


The output of this command given below is a concise listing of HNB-GW service parameter settings as shown in the sample output displayed. In this example, an HNB-GW service called *hnbgw_svc_name* was configured and you can see some parameters configured as default.

```

Service name                : hnbgw1
Context                     : ingress
SCTP IP Address             : 172.16.60.1
SCTP Port                   : 5000
GTP-U Service               : Not defined
RTP IP Address              : Not defined
RTP Port Min                : Not defined
RTP Port Max                : Not defined
RTP MUX                     : Disabled
HNBGW Initiated Ranap Reset : Enabled
Ranap Reset Back Timer      : 10 secs
Ranap Reset Maximum Retransmissions : 1
Ranap Reset Guard Timer     : 10 secs
Available Radio Network PLMN:
    MCC                     : 123
    MNC                     : 456
    RNC-Id                  : 200
    Lac                     : 4660
    Rac                     : 18
    PS Network Name         : ps1
    CS Network Name         : cs1
Service Status              : Started
Security GW service Address : 192.168.1.23
Crypto-template             : crypt1

```

Step 2 Verify configuration errors of your HNB-GW services by entering the following command in Exec Mode:

```
show configuration errors section hnbgw-service}
```

The output of this command displays current configuration errors and warning information for the target configuration file as specified for HNB-GW service

Event IDs for HNB-GW Service

Identification numbers (IDs) are used to reference events as they occur when logging is enabled on the system. Logs are collected on a per facility basis.

Each facility possesses its own range of event IDs as indicated in the following table.



IMPORTANT: Not all event IDs are used on all platforms. It depends on the platform type and the license(s) running.

For more information on logging facility configuration and event id, refer *Configuring and Viewing System Logs* chapter in *System Administration Guide*.

Table 5. System Event Facilities and ID Ranges

Facility	Event ID Range
AAA Client Facility Events	6000-6999
Active Charging Service (ACS) Controller Events	90000-90999
Active Charging Service (ACS) Manager Events	91000-91999
Alarm Controller Facility Events	65000-65999
Card/Slot/Port (CSP) Facility Events	7000-7999
Command Line Interface Facility Events	30000-30999
Event Log Facility Events	2000-2999
HNB-GW Events	151000-151999
Lawful Intercept Log Facility Events	69000-69999
Mobile Access Gateway Manager Facility Events	137500-137999
Mobile IPv6 Facility Events	129000-129999
Network Access Signaling Facility Events	153000-153999
Statistics Facility Events	31000-31999
System Facility Events	1000-1999
System Initiation Task (SIT) Main Facility Events	4000-4999
Threshold Facility Events	61000-61999
Virtual Private Network Facility Events	5000-5999

Chapter 4

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

Keyword/Variable	Description
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).
showsecrets	Optional: This keyword 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 5

Monitoring the Service

This chapter provides information for monitoring service status and performance using the **show** commands found in 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 Counters and Statistics Reference.

Table 6. System Status and Performance Monitoring Commands

To do this:	Enter this command:
View Subscriber Information	
Display Session Resource Status	
View session resource status	<code>show resources session</code>
Display Subscriber Configuration Information	
View locally configured subscriber profile settings (must be in context where subscriber resides)	<code>show subscribers configuration username subscriber_name</code>
View remotely configured subscriber profile settings	<code>show subscribers aaa-configuration username subscriber_name</code>
View Subscribers Currently Accessing the System	
View a listing of subscribers currently accessing the system	<code>show subscribers all</code>
View information for all ggsn-only subscriber sessions	<code>show subscribers ggsn-only all</code>
View information for a specific subscriber	<code>show subscribers full username username</code>
View Subscriber Counters	
View counters for a specific subscriber	<code>show subscribers counters username subscriber_name</code>
View Recovered Session Information	
View session state information and session recovery status	<code>show subscriber debug-info { callid msid username }</code>
View Session Statistics and Information	
Display Historical Session Counter Information	
View all historical information for all sample intervals	<code>show session counters historical</code>
Display Session Duration Statistics	
View session duration statistics	<code>show session duration</code>
Display Session State Statistics	
View session state statistics	<code>show session progress</code>
Display Session State PCF Statistics	
View session state PCF statistics	<code>show session progress pcf all</code>

To do this:	Enter this command:
Display Session Subsystem and Task StatisticsRefer to the System Software Task and Subsystem Descriptions appendix of the System Administration Guide for additional information on the Session subsystem and its various manager tasks.	
View GTPU Manager statistics	show session subsystem facility gtpumgr all
View HNB-GW Manager statistics	show session subsystem facility hnbmgr all
View Session Manager statistics	show session subsystem facility sessmgr all
View Demux Manger status showing detailed statistics for IMSI Manager	show demux-mgr statistics imsimgr full
View HNB-GW Manager facility statistics	show logs facility hnb-gw
View HNB Manager facility statistics	show logs facility hnbmgr
View GTPU Manager Instance statistics	show gtpu statistics gtpumgr-instance gtpu_instance
Display Session Disconnect Reasons	
View session disconnect reasons with verbose output	show session disconnect-reasons
View HNB-GW Service Configuration	
Display a HNB-GW Service Status	
View all configured HNB-GW services configuration in detail	show hnbgw-service all verbose
View configuration errors in HNB-GW section in detail	show configuration errors section hnbgw-service verbose
View HNB-GW Related Statistics	
View HNB-GW service coutners filtered on an HNB-GW service	show hnbgw counters hnbgw-service hnb_gw_svc_name
View HNB-GW service coutners filtered by an HNB id	show hnbgw counters hnbid hnb_identifier
View HNB-GW service statistics filtered on an HNB-GW service	show hnbgw statistics hnbgw-service hnb_gw_svc_name verbose
View HNB-GW service statistics filtered by an HNB id	show hnbgw statistics hnbid hnb_identifier
View GTP-U Service Statistics	
View GTP-U peer information	show gtpu statistics peer-address ip_address
View GTP-U Service information	show gtpu statistics gtpu-service gtpu_svc_name

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 (HNB, HNB-GW, GTP-U, 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 6

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 GTPU Test Echo Command

This command tests the HNB-GW's ability to exchange GPRS Tunneling Protocol user plane (GTP-U) packets with the specified peer nodes which can be useful in troubleshooting and/or monitoring.

The test is performed by the system sending GTP-U echo request messages to the specified node(s) and waiting for a response.



IMPORTANT: This command must be executed from within the context in which at least one HNB-GW service is configured.

The command has the following syntax:

```
gtpu test echo src-address src_ip_address{ all | sgsn-address ip_address }
```

Keyword/Variable	Description
src-address <i>src_ip_address</i>	Specifies the IP address of an interface configured on the system. NOTE: The IP address of the system's interface must be bound to a configured HNB-GW service prior to executing this command.
all	Specifies that GTP-U echo requests will be sent to all Nodes that currently have sessions with the HNB-GW service.

The following figure displays a sample of this command's output showing a successful GTPU echo-test from an HNB-GW 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 HNB-GW'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 HNB-GW service is configured.

The command has the following syntax:

```
gtpv0 test echo src-address src_ip_address { all | sgsn-address
ip_address }
```

Keyword/Variable	Description
src-address <i>src_ip_address</i>	Specifies the IP address of an interface configured on the system. NOTE: The IP address of the system's interface must be bound to a configured HNB-GW service prior to executing this command.
all	Specifies that GTP-U echo requests will be sent to all Nodes that currently have sessions with the HNB-GW service.
sgsn-address <i>ip_address</i>	Specifies that GTPv0 echo requests will be sent to a specific SGSN. <i>ip_address</i> 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 an HNB-GW 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 IPsec Tunnel Test Command

This command tests the system's ability to communicate through an IPsec Tunnel. This functionality is useful for troubleshooting and/or monitoring.

The command has the following syntax:

```
test ipsec tunnel ip-pool ip_pool_name destination-ip des_ip_address
source-ip src_ip_address
```

Keyword/Variable	Description
<i>ip_pool_name</i>	The name of the IP pool configured for IPsec Tunnel. <i>ip_pool_name</i> can be from 1 to 63 alpha and/or numeric characters in length and is case sensitive.

■ Test Commands

Keyword/Variable	Description
<i>des_ip_address</i>	The IP address of destination node of IPsec tunnel.
<i>src_ip_address</i>	The IP address of source node of IPsec tunnel.

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 HNB-GW service:

- [DHCP Service Engineering Rules](#)
- [HNB-GW Engineering Rules](#)
- [Lawful Intercept Engineering Rules](#)
- [MBMS Bearer Service Engineering Rules](#)
- [Service Engineering Rules](#)

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.

HNB-GW Engineering Rules

The following engineering rules apply when the system is configured as an HNB-GW:

- A maximum of 8 HNB-GW service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.
- A maximum of 8 HNB-CS network instance can be configured on a system but limited to only one CS network instance can be associated with an HNB-GW service.
- A maximum of 8 HNB PS network instance can be configured on a system but limited to only one PS network instance can be associated with an HNB-GW service.
- A maximum of 16 radio PLMN id can be configured in an HNB-GW service.
- A maximum of one SeGW IP address can be associated with an HNB-GW service.

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 servicePNs:

- A maximum 225 downlink nodes on ASR 5000 are supported per MBMS bearer service.
- A maximum of two 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.
