CONTENTS

Preface

About this Guide vii

Conventions Used vii

Supported Documents and Resources viii

Related Common Documentation viii

Related Product Documentation viii

Obtaining Documentation ix

Contacting Customer Support ix

CHAPTER 1

HeNB Gateway in Wireless LTE Network 1

Product Description 1

Protocol Architecture 3

Deployment Scenarios for HeNB Access Network 5

HeNB Access Network Elements 8

Home eNodeB 9

Security Gateway (SeGW) 9

HeNB Gateway (HeNB-GW) 9

HeNB Management System (HeMS) 10

CSG List Server 10

Licenses 10

Qualified Platforms 11

DPC2 on ASR 5500 11

MIO Demux Card on ASR 5500 11

Network Deployment and Interfaces 11

Supported Logical Interfaces 12

Features and Functionality - Base Software 14

AAA Server Group Support 15

Access Control List Support 15
Bulk Statistics Support 16
Congestion Control and Management Support 17
DSCP Marking on S1-U Relay 17
Fault Reporting Support 18
Location Reporting Support 18
QoS Support 18
Redundancy Support 18
Troubleshooting Features Support 19
X2 Handover Procedure Support 19
MME Pool size 20
Cell Broadcast Support 20
3GPP Standard Support for Overload Control 22
DHCPv4 Proxy support for HeNBGW with IPSec 23
HeNBGW Multi Operator Core Network (MOCN) 23
s1ap-reset/partial-reset messages from HeNBGW 27
X2 Proxy Gateway support 28
Features and Functionality - Optional Enhanced Feature Software 30
Automatic Neighbor Relation (ANR) Support 30
CSG-ID Based Paging Optimization Support 31
License-based Control for No. of HeNB Connections 31
License-based Control for No. of Subscribers Allowed 31
Session Recovery Enhancements 32

**CHAPTER 2**

Understanding the Service Operation 33
Terminology 33
Contexts 33
Logical Interfaces 34
Bindings 35
Services and Networks 35

**CHAPTER 3**

HeNB-GW Service Configuration Procedures 37
Information Required to Configure the System as an HeNB-GW 38
Required Local Context Configuration Information 38
Required Source Context Configuration Information 39
Required Destination Context Configuration Information 40
CHAPTER 7  Troubleshooting the Service  69

Test Commands  69

Using the GTPU Test Echo Command  69
Using the SNMP TRAP command for debugging  70
Using the RESOURCES SESSION command for debugging  70
About this Guide

This preface describes the HeNBGW Administration Guide, how it is organized, and its document conventions. The Home eNodeB Gateway Administration Guide (HeNBGW) is a StarOS application that runs on Cisco ASR 5x00 platforms. For additional platform information, refer to the appropriate System Administration Guide and/or contact your Cisco account representative.

- Conventions Used, page vii
- Supported Documents and Resources, page viii
- Obtaining Documentation, page ix
- Contacting Customer Support, page ix

Conventions Used

The following tables describe the conventions used throughout this documentation.

<table>
<thead>
<tr>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Note</td>
<td>Provides information about important features or instructions.</td>
</tr>
<tr>
<td>Caution</td>
<td>Alerts you of potential damage to a program, device, or system.</td>
</tr>
<tr>
<td>Warning</td>
<td>Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Typeface Conventions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text represented as a screen display</td>
<td>This typeface represents displays that appear on your terminal screen, for example: Login:</td>
</tr>
</tbody>
</table>
Supported Documents and Resources

Related Common Documentation

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

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

Related Product Documentation

S-GW Administration Guide
MME Administration Guide
Obtaining Documentation

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

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

Use the following path selections to access the HNBGW documentation:

Products > Wireless > Mobile Internet> Network Functions > HeNB-GW Administration Guide.

Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.
The Home eNodeB Gateway (HeNB-GW) or Femtocell Gateway (F-GW) is the HeNB network access concentrator used to control capabilities necessary to manage large clusters of femtocells. It aggregates HeNBs or Femto Access Points (FAPs) to a single network element and then connects to Mobile Operators LTE core networks. The primary function of HeNB-GW is to enable simple, seamless, and highly secure access to subscribers as they roam between trusted/secure mobile networks and intrusted/insecure public networks.

Femtocell is an important technology and service offering that enables new Home and Enterprise service capabilities for Mobile Operators and Converged Mobile Operators. The Femtocell network consists of a plug-n-play customer premise device generically called a Home eNodeB (HeNB) with limited range radio access in home or Enterprise. Femtocells' biggest advantage is their capability to off-load traffic from the macrocell network and enable new applications, for example: location based services.
The figure given describes a high level view of LTE network with Femtocell and HeNB-GW.

**Figure 1: Home eNodeB Gateway Network Architecture**

In the above figure, the S1 interface has been defined as an interface between

- HeNB-GW and the Core Network (CN)/EPC
- HeNB and the HeNB-GW
- HeNB and the CN

An HeNB-GW provides standards-based S1-MME and S1-U network interfaces. As shown in the above high level LTE Femto network architecture diagram, the HeNB-GW appears to the MME as an eNodeB. The HeNB-GW appears to the HeNB as an MME. The S1 interface between HeNB and EPC whether the HeNB is connected to the CN/EPC via an HeNB-GW or not. The HeNB-GW connects to the EPC in a way that inbound and outbound mobility to cells served by the HeNB-GW does not necessarily require inter MME handovers.

In accordance with 3GPP LTE standards, the HeNB-GW hosts the following functions and procedures in LTE core network:

- Relaying UE-associated S1 application part messages between the MME serving the UE and the HeNB serving the UE.
- Terminating non-UE associated S1 application part procedures towards the HeNB and towards the MME.

**Important**

When an HeNB-GW is deployed, non-UE associated procedures shall be run between HeNBs and the HeNB-GW and between the HeNB-GW and MME.

- Optionally terminating S1-U interface with the HeNB and with the S-GW.
- Supporting tracking area code (TAC) and PLMN ID used by the HeNB.
- Allowing no X2 interface establishment between the HeNB-GW and other nodes.
- Optionally performing paging optimization in case the Allowed closed subscriber group (CSG) List of the paged UE is included in the PAGING message.

At the same time, the MME hosts the following functions to support HeNB-GW:

- CSG reporting to S-GW/P-GW
- Access control for UEs that are members of CSG
• Optionally performing paging optimization

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

Protocol Architecture

This section provides a brief description and pictorial representation of protocol stacks for User as well as Control planes in context to HeNB-GW.

Protocol Stacks for S1 User Plane

The S1-U data plane is defined between the HeNB, HeNB-GW and the S-GW. The figures below show the S1-U protocol stack with and without the HeNB-GW.

Figure 2: User plane for S1-U interface for HeNB with HeNB-GW

The HeNB-GW may optionally terminate the user plane towards the HeNB and towards the S-GW, and provide a relay function for relaying User Plane data between the HeNB and the S-GW.
Protocol Stacks for S1 Control Plane

The two figures below show the S1-MME protocol stacks with and without the HeNB-GW. When the HeNB-GW is not present, all the S1 procedures are terminated at the HeNB and the MME.

Figure 3: Control plane for S1-MME Interface for HeNB to MME without the HeNB-GW

The HeNB-GW terminates the non-UE-dedicated procedures: both with the HeNB, and with the MME. The HeNB-GW provides a relay function for relaying Control Plane data between the HeNB and the MME. The
scope of any protocol function associated to a non-UE-dedicated procedure lies between HeNB and HeNB-GW, and/or between HeNB-GW and MME.

Figure 4: Control plane for S1-MME Interface for HeNB to MME with the HeNB-GW

Any protocol function associated to a UE-dedicated-procedure resides within the HeNB and the MME only.

**Deployment Scenarios for HeNB Access Network**

An HeNB-GW can be deployed to provide an alternate path for the data traffic. It holds capabilities to divert the data traffic away from core and directly onto the Internet thus reducing the load on the core network.

There are following two variants of deploying an HeNB-GW solution according to the TR 23.830:
• **Variant I**: With dedicated HeNB-GW where HeNBs connect via HeNB-GW for control and data aggregation. This deployment scenario is displayed in the following figure:

*Figure 5: With Dedicated HeNB-GW*
• **Variant II**: With HeNB-GW for control plane aggregation only and directly connect to SGW for data plane. This deployment scenario is displayed in the following figure:

*Figure 6: With HeNB-GW for Control Plane*
There is another deployment scenario for HeNBs where HeNB-GW is absent. In this deployment, HeNBs connect directly to highly scalable MMEs. This deployment scenario is displayed in the following figure:

*Figure 7: Without HeNB-GW*

Cisco's LTE Femtocell network solution focuses on Variant 1 where HeNB-GW is mandatory for HeNBs to connect. Communication between the HeNB and the HeNB GW is secured by a security Gateway (SeGW) function. The SeGW function is optionally collocated or else off-loaded to external security function node.

**HeNB Access Network Elements**

This section provides the brief description and functionality of various network elements involved in the LTE Femtocell access network. The HeNB access network includes the following functional entities:

- Home eNodeB, on page 9
- Security Gateway (SeGW), on page 9
- HeNB Gateway (HeNB-GW), on page 9
- HeNB Management System (HeMS), on page 10
- CSG List Server, on page 10
Home eNodeB

A Home eNodeB (HeNB) is the a customer premise equipment that offers Uu interface to UE and S1 interface over IPSec tunnel to HeNB-GW for accessing LTE Core Network in Femtocell access network. It also provides the support to HeNB registration and UE registration over S1 interface with the HeNB-GW. Apart from these functions HeNB also supports functions as given below:

- e-RAB management functions
- Radio resource management functions
- GTP-U tunnels management
- Mobility management functions
- Security functions
- Service and Network access functions
- Paging co-ordination functions
- UE registration for HeNB
- User-plane management functions including ciphering

Using Cisco variant 1 and 2, a HENB is directly connected only to 1 HENBGW. HeNB enforces the UL (uplink) bearer level rate based on UE-AMBR and MBR via means of uplink scheduling; and does DL (downlink) bearer level rate enforcement based on UE-AMBR (Aggregate Maximum Bit Rate).

Security Gateway (SeGW)

The Security Gateway is an logical function on HeNB-GW in the LTE femtocell network deployment, however it is specified as a requirement in the Femtocell LTE network architecture. It may be implemented either as a separate physical entity or co-located with an existing entity. The SeGW secures the communication from/to the HeNBs.

Basic function of this entity are:

- Authentication of HeNBs
- Termination of encrypted IPsec data connection from the femtocells
- Providing access to HeMS and HeNB-GW

The SeGW holds capability of implementing a Denial of Service (DoS) shield to protect the EPC (S-GW and MME) by detecting and then filtering out the attack traffic while maintaining the QoS (Quality of Service) of useful traffic. In our implementation, it is an optional element which is situated on HeNB-GW.

HeNB Gateway (HeNB-GW)

The HeNB-GW provides the access to Femto user to LTE core network. It acts as an access gateway to HeNB and concentrates connections from a large amount of HeNBs. HeNB-GW serves as a control plane (C-Plane) concentrator, specifically the S1-MME interface.
The HeNB-GW may optionally terminate the user plane towards the HeNB and towards the S-GW, and may provide a relay function for relaying User Plane data between the HeNB and the S-GW. The HeNB-GW supports NAS Node Selection Function (NNSF).

**Important**

NAS Node Selection Function (NNSF) supports S1-Flex or multiple S1-MME connections towards the EPC from any one HeNB.

---

**HeNB Management System (HeMS)**

It is a network element management system for HeNB access. Management interface between HeNB and HMS is based on TR-069 family of standards. Femto access point extensions are based on standards as defined in TR-196.

It performs following functions while managing HeNB access network:

- Facilitates HeNB-GW discovery for HeNB(s)
- Provision of configuration data to the HeNB
- Performs location verification of HeNB(s) and assigns appropriate serving elements (HeMS, SeGW, and HeNB-GW)

The HeNB 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 HeNB through Auto-configuration server (HMS)

**CSG List Server**

The Closed Subscriber Group (CSG) List Server is an optional function which allows the EPC network to update the allowed CSG lists on CSG-capable UEs.

The CSG List Server hosts functions used by a subscriber to manage membership to multiple as well as different CSGs. For example, the CSG List Server includes the UE CSG provisioning functions which are responsible to manage the Allowed CSG List and the Operator CSG list stored on the UE.

**Licenses**

The HeNB-GW is a licensed Cisco product. Separate session and feature licenses may be required. Each HeNB-GW session corresponds to one IKEv2 session from an HeNB node when SeGW is integrated and enabled. The license is based on the number of sessions and enables all HeNB-GW functionality, including the following:

- IKEv2 support, including all IKEv2 and IPSEC encryption/authentication
- HeNB-GW service
- GTP-U service for S1-U data plane
Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the Managing License Keys section of the Software Management Operations chapter in the System Administration Guide.

**Qualified Platforms**

The HeNB-GW service is a StarOS™ application that is fully qualified to run on the following platforms:

- Cisco ASR 5000
- Cisco ASR 5500
- Cisco Virtualized Packet Core-Single Instance (VPC-SI)

These platforms can be configured with a variety of components to meet specific network deployment requirements.

For additional information, refer to the System Administration Guide and/or contact your Cisco account representative.

**DPC2 on ASR 5500**

The HeNB-GW services are fully qualified to run on the second generation Data Processing Card (DPC2) on the ASR 5500.

The DPC2 offers increased performance versus the first generation DPC, while maintaining backwards compatibility with other ASR 5500 cards. The raw input/output has been increased from 80Gbps (DPC/UDPC) to 150Gbps (DPC2).

The DPC2 has three CPU subsystems. Each subsystem consists of two CPUs with 24 cores each (maximum 144 cores) that are paired with a Platform Controller Hub (PCH). Each CPU is associated with 32 GB of DDR4 memory (total of 192 GB per DPC2) and a latest generation crypto offload engine.

For more information on the DPC2 card, refer the ASR 5500 System Administration Guide.

**MIO Demux Card on ASR 5500**

The HeNB-GW service is fully qualified to run on the Management Input/Output (MIO) card for demux functions. HeNB-GW can leverage on the additional card for user plane processing to increase the capacity of the chassis.

For more information on the MIO Demux card, refer the ASR 5500 System Administration Guide.

**Network Deployment and Interfaces**

This section describes the supported interfaces and Cisco supported deployment scenario of HeNB-GW in LTE access network.

As mentioned above in the section "Deployment Scenarios for HeNB Access Network", Cisco's LTE Femtocell network solution focuses on **Variant 1** where HeNB-GW is mandatory for HeNBs to connect. HeNB-GW may also be frequently deployed or co-located together with MME, S-GW/P-GW, and/or e-PDG in the same system.
These collocations are not yet supported in the Cisco ASR5x00 and virtualized platforms and are planned for future releases.

**Supported Logical Interfaces**

This section provides the brief information on supported interfaces on HeNB-GW node.

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

- **E-UTRAN Uu Interface**: The LTE Uu interface is responsible for all sort of signalling between UE and eNodeB. It carries all signalling message between the eNodeB and the MME along with the user traffic between the eNodeB and S-GW. This way the Uu interface works over both the Control as well as User planes.

  The protocols of the LTE Uu interface include:
  
  - **Radio Resource Control (RRC)**: This protocol governs the signalling between the UE and MME. Technically, the RRC governing lies between the UE and eNodeB. It terminates on the RAN access equipment and then signalling is forwarded to MME.
  
  - **Non-Access Stratum (NAS)**: This protocol also governs the signalling between UE and MME

Other than the above protocols, both the control planes (Control and User) of the Uu interface are supported by the same set of interface functions. These interface functions include Security and Header Compression. All of these functions are carried by the physical layer over the air as shown in the following figure:

*Figure 8: e-UTRAN Uu Interface Logical Representation*
The physical layer in LTE is based upon the Orthogonal Frequency Division Multiplexing (OFDM) using Orthogonal Frequency Division Multiple Access (OFDMA) in the downlink and variant of this Single Carrier Frequency Division Multiple Access (SC-FDMA) in the uplink.

- **S1 Interface**: The communication between the E-UTRAN and the EPC has been designated to the S1 interface. The S1 interface has been separated by the Control plane signalling and User plane traffic:
  - **S1-MME**: The S1 variant used for Control plane signalling is referred to as S1-MME interface.
  - **S1-U**: The S1 variant used for User plane traffic is referred to as S1-U interface.

The S1-MME interface is governed by the S1-AP protocol, whose functions include:

- **E-RAB Management Function**: This functionality is responsible for setting up, modifying and releasing evolved Radio Access Bearers (E-RABs), which are triggered by the MME. The release of E-RABs may be triggered by the eNodeB as well.

- **Initial Context Transfer Function**: This functionality is used to establish an S1-UE context in the eNodeB. It is also used to setup the default IP connectivity, to setup one or more E-RAB(s) if requested by the MME, and to transfer NAS signalling related information to the eNodeB if needed.

- **UE Capability Information Indication Function**: This functionality is used to provide the UE Capability Information when received from the UE to the MME.

- **Paging**: This functionality provides the EPC with the capability to page the UE.

- **S1 Interface Management Functions**: These functions comprise the following:
  - Reset functionality for ensuring a well defined initialization on the S1 interface.
  - Error Indication functionality for allowing a proper error reporting/handling in cases where no failure messages are defined.
  - Overload function for indicating the load situation in the control plane of the S1 interface.
  - Load balancing function for ensuring equally loaded MMEs within an MME pool area.
  - S1 Setup functionality for initial S1 interface setup for providing configuration information.
  - eNodeB and MME Configuration Update functions are to update application level configuration data needed for the eNodeB and MME to inter operate correctly on the S1 interface.

- **S1 UE context Release Function**: This functionality is responsible to manage the release of UE specific context in the eNodeB and the MME.

- **UE Context Modification Function**: This functionality allows to modify the established UE Context partly.

- **Status Transfer**: This functionality transfers Packet Data Convergence Protocol (PDCP) SN Status information from source eNodeB to target eNodeB in support of in-sequence delivery and duplication avoidance for intra LTE handover.

- **Trace Function**: This functionality is to control a trace session recording for a UE in ECM_CONNECTED or to control an MDT (Minimization of Derive Tests) session transferring MDT measurements collected by the UE.

- **Location Reporting**: This functionality allows MME to be aware of the UE's current location.
• **Warning Message Transmission Function**: This functionality provides the means to start and overwrite the broadcasting of warning message.

• **RAN Information Management (RIM) Function**: This functionality allows the request and transfer of RAN information (For example, GERAN system information) between two RAN nodes via the core network.

• **Configuration Transfer Function**: This functionality allows the request and transfer of RAN configuration information (For example, SON information) between two RAN nodes via the core network.

---

**Features and Functionality - Base Software**

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

Following features and supports are discussed in this section:

- AAA Server Group Support, on page 15
- Access Control List Support, on page 15
- Bulk Statistics Support, on page 16
- Congestion Control and Management Support, on page 17
- DSCP Marking on S1-U Relay, on page 17
- Fault Reporting Support, on page 18
- Location Reporting Support, on page 18
- QoS Support, on page 18
- Redundancy Support, on page 18
- Troubleshooting Features Support, on page 19
- X2 Handover Procedure Support, on page 19
- MME Pool size, on page 20
- Cell Broadcast Support, on page 20
- 3GPP Standard Support for Overload Control, on page 22
- DHCPv4 Proxy support for HeNBGW with IPSec, on page 23
- HeNBGW Multi Operator Core Network (MOCN), on page 23
- s1ap-reset/partial-reset messages from HeNBGW, on page 27
- X2 Proxy Gateway support, on page 28
AAA Server Group Support

It is a value-added feature to enable VPN service provisioning for enterprise or MVNO customers, however integrated SeGW is required to be enabled for this feature. It enables each corporate customer to maintain its own AAA servers with its own unique configurable parameters and custom dictionaries.

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

Important

For more information on AAA Server Group configuration, if you are using StarOS 12.3 or an earlier release, refer to the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

Access Control List Support

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

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

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

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

There are two primary components of an ACL:

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

  Each rule specifies the action to take when a packet matches the specifies criteria. This section discusses the rule actions and criteria supported by the system.

- Rule Order: A single ACL can consist of multiple rules. Each packet is compared against each of the ACL rules, in the order in which they were entered, until a match is found. Once a match is identified, all subsequent rules are ignored.
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
- **GTP-U**: Provides GPRS Tunneling Protocol - User message statistics
- **HENBGW-ACCESS**: Provides HeNB-GW access side statistics
- **HENBGW-NETWORK**: Provides HeNB-GW network side 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 chassis or sent at configured intervals. The bulk statistics are stored on the receiver(s) in files.

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

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

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

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

Congestion Control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. Session managers actually handle both the HeNB associations and UE sessions for memory utilization. However, continuous or large numbers of these conditions within a specific time interval may have an impact on the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies for addressing the situation.

Congestion control operation is based on configuring the following:

- **Congestion Condition Thresholds**: Thresholds dictate the conditions for which congestion control is enabled and establishes limits for defining the state of the system (congested or clear). These thresholds function in a way similar to operation thresholds that are configured for the system as described in the Thresholding Configuration Guide. The primary difference is that when congestion thresholds are reached, a service congestion policy and an SNMP trap, starCongestion, are generated.
  
  A threshold tolerance dictates the percentage under the configured threshold that must be reached in order for the condition to be cleared. An SNMP trap, starCongestionClear, is then triggered.
  
  - **Port Utilization Thresholds**: If you set a port utilization threshold, when the average utilization of all ports in the system reaches the specified threshold, congestion control is enabled.
  
  - **Port-specific Thresholds**: If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is enabled system-wide.

- **Service Congestion Policies**: Congestion policies are configurable for each service. These policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

---

**Important**

For more information on Congestion Control support, refer Congestion Control chapter in System Administration Guide.

---

DSCP Marking on S1-U Relay

Cisco supports the DSCP marking of S1-U traffic traversing the HeNB-GW. This functionality on HeNB-GW is supported through command line interface (CLI). CLI configuration capability has been enabled for DSCP marking for both Access and Network service.

CLIs are used for the dscp marking configuration for IP packets sent out on the S1-U interface, from the HeNB-GW to the Access/Network side. Default value used for dscp marking is the dscp value for the incoming packet.

---

**Important**

For more information on the supported CLIs for this feature, refer the CLI Reference Guide.
Fault Reporting Support

SNMP traps are used for faults and fault reporting in the system for network side S1-MME and S1-U interfaces. For these traps on the network side, some other mechanism is required, as the SCTP/S1-MME associations do not generate SNMP traps.

Location Reporting Support

Cisco HeNB-GW supports the location reporting feature for the subscribers/UE movements. Location Reporting is the procedure by which the serving MME keeps in the track of the UE change in location within the allowed tracking area list of the eNodeB.

With the HeNB-GW deployed in the Femtocell LTE network, MME does not directly connect to HeNBs, and therefore any location report message is forwarded by the HeNB-GW to and fro. When HeNB-GW receives location reporting control messages, it forwards the same to the appropriate HeNB for location reporting procedure.

QoS Support

Cisco HeNB-GW along with the SeGW supports QoS handling based on the DSCP mapping configuration. QoS support provides a foundation for contributing towards improved Quality of User Experience (QoE) by enabling deterministic end-to-end forwarding and scheduling treatments for different services or classes of applications pursuant to their requirements for committed bandwidth resources, jitter and delay. In this way, each application receives the service treatment that users expect.

Redundancy Support

To support redundancy, the HeNB-GW tasks should be started based on the following guidelines:

- **HENBGW DEMUX** - The HENBGW DEMUX task recovers and updates the relevant information regarding HeNB/UE connections by querying all the session managers (SMGRs) in the system. This task should not be started on a PSC in which SMGRs are started. Regardless of whether session recovery is enabled or not, the HENBGW DEMUX task should always be started on the Demux PSC. Upon recovery, the IPsec tunnel being preserved, the HeNB re-connects and the UE is paged via network initiated service request or transition to ECM ACTIVE state on the MME by sending uplink packets itself, but only after the HeNB has successfully re-established its association with the HeNB-GW.

<table>
<thead>
<tr>
<th>Important</th>
<th>From release 16.0 FCS Full Session Recovery on HENBGW is supported.</th>
</tr>
</thead>
</table>

- **SMGR** – The SMGRs follow the standard guidelines used for other services and are ought to recover HeNB association and UE state from its AAAMGR pair.
UE state recovery by SMGRs in Cisco HeNB-GW deployment is supported from 16.0 FCS release.

- **HENBGWMGR** – The HENBGWMGRs use the henbgw-network-service information to establish the SCTP connections towards MME(s). HENBGWMGRs are demux tasks and are started on the Demux PSC. After Henbgwmgr task recovery, it synchronises its data with the Session Managers only.

- **GTPUMGR** – GTPUMGR task(s) are started in the demux PSC. Any required state information after a task restart is fetched from the SMGR(s).

A minimum of 3 ACTIVE PSCs and 1 STANDBY PSC is required to support session recovery. One of the active PSCs works as the DEMUX PSC and runs the demux tasks.

**Troubleshooting Features Support**

HeNB-GW provides monitor protocol support for S1AP, SCTP and GTP-U.

The following logging facilities can be used for troubleshooting HENB-GW:

- henbgw
- henbgwdemux
- henbgwmgr
- hnbapp
- gtpumgr
- egtpu
- ipsec
- ikev2
- sessmgr
- henbgw-sctp-acs
- henbgw-sctp-nw

The above listed in addition to the existing facilities can be enabled to capture logs at different levels, for example: information, trace, debug etc.

**Important** For more information on troubleshooting, refer the *Troubleshooting the Service* chapter of this guide.

**X2 Handover Procedure Support**

In order to support X2 Handover between HENBs, the HeNB-GW should provide the HeNB with the MME UE S1AP ID allocated by the MME and HeNB-GW within the S1 HANDOVER REQUEST along with the
S1 INITIAL CONTEXT SETUP REQUEST messages. HeNB-GW may also inform the HeNB about any GUMMEI corresponding to the serving MME.

HENBGW have to route S1 PATH SWITCH REQUEST message from HENB towards the MME based on the GUMMEI of the source MME received from the HeNB. If HENBGW receives CSG ID IE and Cell Access Mode IE in the S1 PATH SWITCH REQUEST, the same should be forwarded to MME. In case of S1 PATH SWITCH REQUEST ACKNOWLEDGE message, HENBGW will inform the HeNB about the MME UE S1AP ID assigned by the MME and the MME UE S1AP ID assigned by the HeNB GW for the UE.

HENBGW will receive UE CONTEXT RELEASE REQUEST message with an explicit GW Context Release Indication from Source HENB at the end of X2 Handover Procedure phase. Therefore the HeNB GW terminates the S1 UE Context Release Request procedure and releases the UE context if it determines that the UE identified by the received UE S1AP IDs is no longer served by a HeNB attached to it or it ignores the message.

**MME Pool size**

HeNBGW supports 32 MMEs max per MME pool. Pool size is increased from 8 to 32 MMEs per logical eNB with which HeNBGW can interact. The maximum associations will now be 256 (8 LeNB x 32 MME).

**Cell Broadcast Support**

The Cell Broadcast Support is in compliance with the Warning system aspects of the S1-MME interface between eNodeB and MME, and the S1AP protocol defined by the 3GPP specification TS 36.413 Release 10.

**S1AP Messages supported by HeNBGW for CMAS**

- Write Replace Warning Request
- Write Replace Warning Response
Kill Request

Kill Response

All the above messages are supported in the protocol monitor trace.

On receiving a Write-Replace Warning request, HeNGBW will forward the request only to HeNBs that belong to the Tracking Area or Cell Id specified in the message.

HeNGBW will support Cell Id and TAI in the Warning Area List. Emergency Area Id will not be supported.

1. If TAI list is present in Warning Area List, HeNGBW will forward the request to all HeNBs associated with TAI in the list

2. If Cell Id list is present in Warning Area List, HeNBW will only forward the request to HeNBs belong to the cell list.

3. If no Warning Area List present, HeNBGW will forward the request to ALL HeNBs under HeNBGW.

4. HeNBGW will maintain a list of Request information (AWR) until the configured timeout. The information would be deleted after the response to the Write-Replacewarning-request is sent to MME.

5. HeNBGW will collect the responses from HeNBs for an AWR and send a single Warning Response to the MME.
   - HeNBGW will not include in its WRITE-REPLACE WARNING RESPONSE the unrecognized cells in the BroadcastCompletedAreaList IE parameter. A configurable wait for response timer will be used. When timer expires and not all HeNBs have respond to the request, HeNBGW will send response with aggregated Broadcast Completed Area List from received responses.

6. HeNBGW will detect duplicate Warning Request messages for an existing AWR (with same Message ID & Serial number from different MMEs), HeNBGW will NOT forward duplicated messages to HeNBs. HeNBGW will send the same responses to duplicated messages as the response to the first Warning Request message. If HeNBGW has NOT sent response to first request message (i.e. still waiting responses from HeNB), HeNBGW will delay sending responses to duplicated request messages until after response is sent to first request message.
   - The message will be considered duplicated only if the message matches the original message exactly.
   - If a WRWR message is received with same messageid/sequence num with changed contents in other IEs, the message will be processed and forwarded to all Henbs as per the WAL IE.
   - After response to WRWR message is sent to MME, another WRWR message with same message id/sequence number will not be considered as duplicate message. It will be processed as fresh WRWR request.

7. On receiving a Kill request for an existing AWR, HeNGBW will forward the request to all HeNB as per WAL IE in the request message
   - The HeNBGW will collect the responses from the HeNBs and send a single Kill Response to the MME from which the KILL request was received.
   - A configurable wait for response timer will be used. When timer expires and not all HeNBs have respond to the request, HeNBGW will send response with aggregated Broadcast Cancelled Area list from response received.
   - HeNBGW will detect duplicated KILL Request messages (Exactly same message from different MMEs), and will NOT forward duplicated messages to HeNBs. However, it will be forwarding for changes in WAL IE and will send to all Henbs as per the WAL IE. HeNBGW will send the same aggregated responses to duplicated messages as the response to the first KILL Request messages. If HeNBGW has NOT sent response to first request message (i.e. still waiting responses from HeNB),
HeNBGW shall delay sending responses to duplicated KILL request messages until after response is sent to first request message.

### 3GPP Standard Support for Overload Control

The Support for Overload Control is in compliance with 3GPP standards 3GPP spec 36.413 and 23.401.

On receiving MME Overload Start message, HeNBGW shall use the Traffic Load Reduction Indication IE to determine the percentage of HeNBs (attached to the same logic eNB which receives the message) to which Overload Start message need to be relayed. If Traffic Load Reduction Indication IE is not present in the message, HeNBGW will relay the message to a configurable percentage of HeNBs.

- Each HenbGW logic eNB needs to create an Overload Control HeNB List (OCHL) per MME for all HeNBs to which Overload Start message has been relayed, so subsequent overload start/stop message can be correlated.
- If HenbGW logic eNB receives another Overload start message from the same MME (before receiving any Overload Stop Message)
  1. If there is Traffic Load Reduction Indication IE and percentage is changed from previous Overload Start message, HenbGW will calculate the difference and either relay the message to more HeNBs (adding to OCHL) or send Overload Stop messages to a subset of HeNBs in OCHL. Thus the number of HeNBs in OCHL will match the new percentage.
  2. Otherwise
     a. If the newly received Overload start message has the same actions, new message will be dropped by Henbgw
     b. If actions are different, new message will be forwarded to newly adjusted HeNBs in OCHL

- GUMMEI List update will be integrated to this feature.
  - HeNBGW's logic eNB needs to maintains a list of GUMMEIs per as received in S1AP Setup Response and S1AP MME Configuration Update Request.
  - The combined GUMMEI list will be formed as follows, for each RAT in order
    - Combine the PLMN list from all MMEs and discard duplicates
    - Combine the MME Group list from all MMEs and discard duplicates
    - Combine the MME Code list from all MMEs and discard duplicates End For
  - HeNBGW's logic eNB shall populate aggregated GUMMEI list from all MMEs in a MME-pool in the S1 SETUP Response message to HeNB.
  - GUMMEI list status changes for any MME (i.e. lost SCTP connection to MME, new MME connections is up, or receive MME configuration Update message which changes GUMMEI list for a MME) shall be broadcasted to all HeNB attached to the logical eNB using MME configuration Update Message.
  - On receiving Overload Start/Stop Message from a MME, HenBGW shall re-populate GUMMEI list from received GUMMEI list in S1 SETUP RESPONSE message from that MME in Overload/Stop message before relaying to HeNBs.
• HenbgwMgr MME selection mechanism will be integrated to this feature. When receives new InitialUE message:
  ◦ If there is no GUMMEI in the message, HeNBGWMgr will NOT choose MME(s) which are congested.
  ◦ Otherwise, HeNBGWMgr will select specified GUMMEI even if the MME is congested.

• Overload Control will be integrated to session recovery feature
  ◦ eNB context in sessmgr will have overload flag be checked-pointed.
  ◦ After session recovery, there will be a sessmgr-wide global timer to send overload stop to overload flagged HeNBs unless a new Overload Start messages are sent to the overload flagged HeNBs.
  ◦ In case henbgwmgr restart, overload stops will be sent to all overload flagged HeNBs in sessmgr.

• Automatic congestion control recovery:
  ◦ For each OCHL, a configurable guard timer will be started. If there is no overload stop received from the MME before the timer expires, overload stop will be sent to all corresponding HeNBs.

• Manual congestion control recovery:
  ◦ Henbgw will provide CLI command to send overload stops to all HeNBs in a OCHL of a MME.

• SoC compliance will be updated to S1AP specifications.

### DHCPv4 Proxy support for HeNBGW with IPSec

The DHCPv4 proxy functionality on the SeGW integrated with HeNBGW is to update the DHCP messages with the HeNB Id in DHCP Option 61 (Client ID) and forward the DHCP messages to an external DHCP server.

**How DHCPv4 Proxy support for HeNBGW with IPSec works**

1. The SeGW forwards DHCP requests from a LTE FAP to an external DHCP server during IPSec Setup.
2. The SeGW adds LTE FAP Id in the Client Identifier (CID) of the DHCP messages.
3. The PNR then receives these DHCP requests maintains a mapping between the LTE FAP ID and the assigned "Inner" IP Address
4. The RMS queries the PNR to get the LTE FAP inner IP Address, to use this inner IP Address to send TR-069 Connection Requests to the LTE FAP.

### HeNBGW Multi Operator Core Network (MOCN)

MOCN is a network sharing technology that allows different core network operators to connect to a shared radio access network. One HENB can handle more than one core network operator. In this scenario HENB broadcasts a list of PLMN Ids to UE's. UE's supporting MOCN functionality decode the broadcast system information sent by HENB and are able to select a core network operator as the serving operator within a shared network.
Below diagram depicts complete radio network shared among different operators, while each operator maintains its own separate core network.

**Figure 9: Multi Operator Core Network Architecture**

---

**Limitations & Assumptions**

Below are the limitations and assumptions for HeNBGW MOCN feature.

- HENB will send list of PLMNs and TAC to the HeNBGW with S1 Setup Request message. All the PLMNs in the PLMN list and TAC received with S1 Setup message shall be configured in the HeNBGW else S1 setup will be rejected with S1 setup failure.

- Each TAIDB list associated for a logical EnodeB shall be configured with only one PLMN. If operator has multiple PLMNs then, configure different PLMNs in multiple TAIDB list and associate each to a different logical ENB.

- HeNBGW now support up to 256 TAIs per TAIDB. Given maximum of 64 logical EnodeBs, it can support up to (8*256) 2048 unique TAIs. Considering at max 6 PLMS each sharing the same TAC, the geographical area covered can be shrunk. HeNBGW cannot increase the number of TAIs per TAIDB, as s1-setup request message sent to MME can hold max of 256 TAIs.

---

**Note**

For Release 18 HeNBGW supports maximum of 8 logical EnodeBs only.

- There will be only one IPSEC tunnel for each HENB SCTP association.
S1AP Handover Request & DL NAS Transport Message with network sharing (MOCN or GWCN) the MME will generally populate the optional Handover Restriction List IE in the S1AP Initial Context Setup Request which is S1AP Handover Request & S1AP DL NAS Transport Message. These messages are transparent to the HeNBGW and no specific processing required from HeNBGW.

HENB requirements for MOCN

- With multiple TAIs (one TAC and multiple PLMNs) per HeNB, all the TAIs information has to be informed to the HeNBGW in the S1AP Setup Request and S1AP ENB Configuration Update.
- When UE’s connect to the HENB they indicate the PLMN they wish to use. Based on the UE’s choice, the HENB needs to populate the TAI corresponding to the selected PLMN in the S1AP Initial UE Message.

Configuring HeNBGW MOCN support

This section introduces configuration support details for the HeNBGW MOCN support.

ENB configuration update from HENB

- When HeNBGW validates new PLMN list and TAC, it should match all the PLMNs list & TAC received with the ENB Configuration Update message from HENB with the TAIDB list of logical EnodeBs. Otherwise HENBGW will send ENB configuration update failure message.
- If there is any change of logical EnodeB list for the new PLMN list and TAC, HeNBGW aggregates GUMMEI list for newly selected logical EnodeB from all MMEs in a MME-pool in the S1 MME Configuration Update message to HENB.
- If any of the PLMN is deleted or TAC changed with the ENB configuration update message then HENBGW will send ENB configuration update failure message.

MME configuration update from MME

- GUMMEI list status changes for any MME (i.e. lost SCTP connection to MME, new MME connections is up, or receive MME configuration Update message which changes GUMMEI list for a MME) is broadcasted to all the HeNBs attached to the logical EnodeB using MME configuration Update Message.
- If one of the MME connection goes down HeNBGW will send partial RESET message towards HENB.
- If all the MME connections for all the PLMNS goes down HeNBGW will terminate SCTP/S1AP connection for HeNB.
Initial UE Message / MME selection

**Figure 10: Modified NAS Node Selection function (NNSF)**

- HENB sends INIT UE message with UE selected PLMN

- Is the PLMN and TAC associated to the HENB?
  - Yes: Selects logical Enoddb
  - No: Send error indication to HENB and drop the message

- Select MME based on GUMMEI or S-TMSI or TAI
- Forward INIT UE message to MME
• When UE’s connect to the HeNB they indicate to the PLMN they want to connect. Based on the UE’s choice, the HeNB populates the TAI corresponding to the selected PLMN in the S1AP Initial UE Message.

• The HeNBGWs modified NAS Node Selection Function (NNSF) only routes this S1AP message to one of the MMEs of a logical HeNBs that supports the selected PLMN in their S1AP Setup Request Response or S1AP MME Configuration Update.

• The modified NNSF applies PLMN filtering to the MME list of logical EnodeB before processing any requested GUMMEI or S-TMSI.

GUMMEI List update

• HeNBGW maintains a list of GUMMEIs per logic EnodeB as received in S1AP Setup Response and S1AP MME Configuration Update Request.

• HeNBGW populates aggregated GUMMEI list form all the selected logical EnodeB in the S1 SETUP Response message to HENB.

• GUMMEI list status changes for any MME (i.e. lost SCTP connection to MME, new MME connections is up, or receive MME configuration Update message which changes GUMMEI list for a MME), HeNBGW broadcasts MME configuration Update Message with aggregated GUMMEI list to all HeNBs, which are associated to the MME.

s1ap-reset/partial-reset messages from HeNBGW

If s1ap-reset/partial-reset messages from HeNBGW is enabled HeNBGW will forward partial or full s1-reset messages to Henb or MME and delete UE context. If it is disabled it will delete UE context and drop the message.

Partial Reset message from MME

• Delete all the UE context specified with the s1-reset message.

• Update mme_ue_s1ap IDs with local mme_ue_s1ap IDs with in the message and forwards to the corresponding HeNBs.

Full Reset message from HENB

• Deletes all the UEs corresponding to HeNB.

• Sends Partial RESET message with the list of UEs corresponding to the HeNB and forwards to the associated MMEs.

Partial Reset messages from HeNB

• Deletes all the UE context specified with the s1-reset messages.

• Update enb_ue_s1ap IDs with local enb_ue_s1ap IDs with in the messages and forwards to the corresponding MMEs.

Full/Partial Reset messages generated towards HENB

• If one of the MME connections goes down, deletes all the UEs associated to the MME.
• Sends Full/Partial RESET messages with the list of UEs associate to the MME and forwards to the corresponding HeNBs.

**Full/Partial Reset messages generated towards MME**

• If one of the HeNB association goes down, deletes all the UEs corresponding to HeNB.
• Sends Partial RESET messages with the list of UEs corresponding to the HeNB and forwards to the associated MMEs.

---

# X2 Proxy Gateway support

As part of E-UTRAN architecture a X2 Gateways are deployed to allow the indirect X2-C interface between (H)eNBs

**The X2 GW hosts the following functions:**

• Routing the X2AP X2 MESSAGE TRANSFER message to target eNB or HeNB based on the routing information received in the X2AP X2 MESSAGE TRANSFER message.
• Informing the relevant (H)eNBs upon detecting that the signalling (i.e. SCTP) connection to a (H)eNB is unavailable. The relevant (H)eNBs are the ones which had an "X2AP association" with this (H)eNB via the X2 GW when the signalling connection became unavailable.
• Mapping the TNL address(es) of a (H)eNB to its corresponding Global (H)eNB ID and maintaining the association.

---

**Note**

X2GW is implemented to support aggregation of both only X2-C interface.
This section describes the EUTRAN Architecture from 3GPP 36.300.

**Figure 11: E-UTRAN Architecture from 3GPP 36.300**

Limitations

Below are the limitations for the Proxy X2 Gateway support feature.

- Session Manager Crash/Recovery will not recover SCTP associations.
- Multi-homing not supported towards (H)enbs.
- IPv6 peers support will be part of later releases.
• Integrated IPsec/SecGW support will be part of later releases.
• X2GWDemux task recovery support will be part of later releases.

Features and Functionality - Optional Enhanced Feature Software

This section describes the optional enhanced features and functions support with HeNB-GW service.

Some of the following features may require the purchase of an additional license to implement the functionality with the HeNB-GW service.

This section describes following features:

• Automatic Neighbor Relation (ANR) Support, on page 30
• CSG-ID Based Paging Optimization Support, on page 31
• License-based Control for No. of HeNB Connections, on page 31
• License-based Control for No. of Subscribers Allowed, on page 31
• Session Recovery Enhancements, on page 32

Automatic Neighbor Relation (ANR) Support

Automatic Neighbor Relation (ANR) functionality is nothing but relieving the operator from the complexity of manually managing Neighbor Relations (NRs). In LTE deployments, the manual management of NRs becomes even more challenging, as in addition of defining intra LTE neighbor relations for eNodeBs, operator has to provision neighboring 2G, 3G, CDMA2000 cells as well.

The ANR function resides in the eNodeB and manages the conceptual Neighbor Relation Table (NRT). Located within ANR, the Neighbor Detection Function (NDF) finds new neighbors and adds them to the NRT. ANR also contains the Neighbor Removal Function (NRF) which removes outdated NRs. The NDF and the NRF functions are specific to the implementation by operator.

An existing Neighbor cell Relation (NR) from a source cell to a target cell means that eNodeB controlling the source cell knows the ECGI/CGI and Physical Cell Identifier (PCI) of the target cell and has an entry in the NRT for the source cell identifying the target cell.

For each cell that the eNodeB has, the eNodeB keeps an NRT. For each NR, the NRT contains the Target Cell Identifier (TCI), which identifies the target cell. For E-UTRAN, the TCI corresponds to the E-UTRAN Cell Global Identifier (ECGI) and Physical Cell Identifier (PCI) of the target cell.

The ANR function relies on cells broadcasting their identity on global level, ECGI and allows O&M to manage the NRT.
CSG-ID Based Paging Optimization Support

Due to the high volume and small-sized femtocell deployment, it is well-known that paging messages is a big burden for the femtocell system. In order to optimize the paging procedure by the HeNB-GW, the HeNB-GW is made aware of the CSGs supported by the connected HeNBs. This allows the HeNB-GW to identify the appropriate HeNBs supporting certain CSGs. This is known through the S1-Setup request sent by HeNBs.

In order to have a complete paging optimization solution, the allowed CSG list of the paged UE is included in the paging message. The paging message is then sent with the allowed CSG list of the paged UE to the HeNB-GW by MME.

With the help of the ACL, the HeNB filtering is done by the HeNB-GW. Finally, the paging message is only sent to the HeNBs with the allowed CSG ID.

**Important**

This feature makes dependency on MME to initiate Paging messages containing CSG list.

License-based Control for No. of HeNB Connections

Number of HeNBs connecting to the HeNB-GW are controlled/limited based on the license configuration.

**Important**

SNMP traps are generated during Over/Under License capacity situation.

There are two scenarios for HeNBs connecting to the HeNB-GW: Through IPSec and Directly HeNB-GW.

**With IPSec (Integrated HeNB-GW and SeGW)**

In case, IPSec is implemented or the Security Gateway is co-located with the HeNB-GW, IPSec Tunnel setup requests are dropped once the number of tunnels exceed the configured license limit of the number of HeNBs.

**Non-IPSec (Standalone HeNB-GW)**

HeNB-GW rejects the extra HeNB connection attempts with SCTP Abort once the license control is configured for maximum number of HeNBs to connect to the HeNB-GW.

License-based Control for No. of Subscribers Allowed

Number of subscribers/UEs connecting to the HeNB-GW are also controlled/limited based on the license configuration.

**Important**

SNMP traps are generated during Over/Under License capacity situation. For more information on SNMP Traps, refer the *Alarm and Alert Trap Configuration* section of the *HeNB-GW Service Configuration Procedures* chapter of this guide.

There are two scenarios for HeNBs connecting to the HeNB-GW: Through IPSec and Directly HeNB-GW.
With IPSec (Integrated HeNB-GW and SeGW) 0

In case, IPSec is implemented or the Security Gateway is co-located with the HeNB-GW, IPSec Tunnel setup requests are dropped once the number of tunnels exceed the configured license limit of the number of UEs. UEs limit is based on configured UE license limit and are rejected with Error Indication message and cause code.

Non-IPSec (Standalone HeNB-GW) 1

HeNB-GW rejects the extra UE connection attempts with Error Indication message with proper cause code once the license control is configured for maximum number of HeNBs to connect to the HeNB-GW.

**Important**

For troubleshooting License related issues, refer the *Troubleshooting the Service* chapter of this guide.

---

**Session Recovery Enhancements**

The HeNBGW is the concentrator of HeNBs. Session Recovery feature of HeNBGW will enable it to best-effort attempt to recover from software and hardware faults. The Session recovery will make a best-effort attempt to recover existing HeNBGW SCTP and UE sessions upon a failure and restart of session manager. Partially connected or disconnecting sessions are terminated/aborted. There will be SCTP re-establishment from HeNBGW with Sessmgr recovery. HeNB S1-AP info, UE sessions state is not impacted by SCTP re-establishment and there is no S1-Setup request from HeNB. In case of S1-Setup request from HeNB, HeNBGW will clear all the UE sessions according to 3GPP spec 36.413. It is assumed that with SCTP re-establishment, HeNB will send ENB configuration update message and this will make sure that the HENBGW will have proper HeNB context information. HeNBGW will send MME configuration update message to all the HeNB’s immediately after Sessmgr recovery, to make sure HeNB have proper MME context information.

The Boxer architecture provides session recovery infrastructure. When session recovery feature is enabled, Session Manager keeps critical session information backup with AAA Manager along with the paired AAA Manager of the same instance number, as Session Manager is started on different PSC.

On single Session Manager task failure standby Session Manager on the same PSC is renamed to the instance no. of the failed Session Manager. On PSC failure Session Managers on the standby PSC are renamed to the instance nos of the Session Managers of the failed PSC. After renaming Session Manager gets the backed up session critical information from the paired AAA Manager and recreates the session. During this process Session Manager also audits with other Managers to synchronize the session states with the current state, if it has changed after the failure.

Backed up information in AAA Manager is called as CRR. This record is created/updated during check-pointing, following information of HeNB SCTP/UE Session will be checkpointed as CRR:

- SCTP Association and HeNB specific information
- UE Specific information

The CRR List fetched from AAA Manager during recovery will have CRRs which are of mix type’s i.e having HENB SCTP Session calline details or HeNB UE calline details.

When Session Manager performs audit with HeNBGW Demux it shall from the CRR list first send SCTP Association audit request, after that UE Session audit request. With this audit strategy it shall be possible in non-creation of UE Session if the corresponding HeNB SCTP Session fails. Also if HeNB SCTP Session audit succeeds but UE Session, from the HeNBGW Demux, audit fails.
CHAPTER 2

Understanding the Service Operation

The system provides wireless carriers with a flexible solution for providing Security Gateway (SeGW) and Home-eNodeB Gateway (HeNB-GW) functionality for LTE Femtocell networks.

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

- **PS Session over S1AP**: The subscriber is provided packet switch connection with different traffic class on PS session with P-GW in PS.

- **Network-initiated Sessions**: Network-initiated session procedures include Paging, Dedicated Bearers, UE disconnections etc. from CN side on HeNB-GW for a specific subscriber session and in turn HeNB-GW initiates the required procedures with HeNBs and CNs.

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, page 33**

## 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.
In HeNB-GW service implementation, the contexts can be classified into source or destination contexts. This is because GTP-U tunnels as well as HeNB-GW Access and Network services can be created over a single context.

The IP addresses as well as interfaces can also under the defined under the same context. These IP addresses are later used to bind with different services including GTP-U, MME and Interfaces including S1-MME for HeNB-GW Access service and Network service.

**Logical Interfaces**

This section describes the logical interface supported on HeNB-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 HeNB-GW service, it will function as an S1-MME interface between the HeNB-GW/SeGW service and MME. Services are defined later in this section.

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

- **S1 Interface**: This interface is the reference point for the control plane protocol between Home eNodeB and HeNB-GW. This interface sets up S1AP association over SCTP as the transport layer protocol for guaranteed delivery of signaling messages between HeNB-GW and Home eNodeB. This is the interface used by the HeNB-GW to communicate with HeNBs on the same Femtocell Access Network. This interface serves as path for establishing and maintaining subscriber UE contexts.

- **S1-MME Interface**: This interface is the reference point for the control plane protocol between E-UTRAN and MME in the LTE Femtocell network. Protocol stack architecture for the S1-MME interface has been described in the Protocol Architecture section of the Overview chapter of this guide. The Stream Control Transmission Protocol (SCTP) guarantees the delivery of signalling messages between MME and eNodeB via HeNB-GW.

- **S1-U**: This interface is the reference point between E-UTRAN and Serving Gateway (S-GW). This interface is responsible for the per bearer user plane tunnelling and inter eNodeB path switching during handover. The HeNB-GW functions as a user-plane concentrator along with the control-plane concentration function. This allows the S-GW to view the cluster of femtocells as a single entity. The user-plane aggregation functionality provides support to GTP-U.

- **RADIUS**: This interface is the reference point between a Security Gateway (SeGW) and a 3GPP AAA Server or 3GPP AAA proxy (OCS/CGF/AAA/HSS) over RADIUS protocol for AAA procedures for Femto user.
RADIUS/AAA is only applicable when SeGW is co-located with HeNB-GW.

In the roaming case, the 3GPP AAA Proxy can act as a stateful proxy between the 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 DIAMETER protocol.

One or more RADIUS 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, HeNBs and STBs. TR-069 provides an auto configuration mechanism between the HeNB 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 HeNB 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 GTP-U service bound to a logical interface will cause the logical interface to take on the characteristics of a GTP interface within an LTE Femtocell 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 HeNB-GW to support various functionality.

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

- **HeNB-GW services**: HeNB-GW services are configured in Context Configuration Mode to support both mobile-initiated and network-requested user contexts. The HeNB-GW services must be bound to a logical interface within the same context. There are two HeNB-GW services:
**HeNB-GW Access Service**: This service is configured under the Context Configuration Mode in order to initialize the HeNB-GW functionality. The configuration of this service controls the functionality of S1-MME interface between HeNB-GW and the HeNBs. This service is bound to a local SCTP end-point address (IP address) to listen the incoming SCTP associations from HeNBs.

**HeNB-GW Network Service**: This service is also configured in the Context configuration mode to support the HeNB-GW functionalities. The configuration of this service controls the functionality of S1-MME interface between HeNB-GW and MME. One-to-one mapping is maintained between the HeNB-GW Access service and HeNB-GW Network service. It is the HeNB-GW Network service where enabling of logical eNodeBs is configured within the HeNB-GW. The Logical eNodeB configuration can be used to support load balancing among different TAI Lists. Each Logical eNodeB can connect up to 8 MMEs from the MME pool and therefore 64 connections are possible to be established between HeNB-GW and MME.

**Important**

At least one logical eNodeB configuration is required to start the HeNB-GW Network service. Up to 8 logical eNodeBs can be configured per HeNB-GW Network service.

- **Radio Network PLMN**: The Radio Network PLMN is configured in HeNB-GW Access service to associate PLMNs with HeNB-GW. PLMN configuration is also required at the time of configuring Logical eNodeBs for the HeNB-GW Network service.

- **GTP-U services**: GTP-U services are configured in Context configuration mode in pair of two services; one for GTP-U tunnel support towards HeNB on S1 interface and another for GTP-U tunnel support towards the core network on S1-U interface to communicate with the S-GW respectively. These two GTP-U services are called Access GTP-U service and Network GTP-U service. GTP-U service comes in picture specially when the S1-U Relay option is enabled. S1-U relay activation actually allows the data to flow through the GTP-U tunnel via HeNB-GW, otherwise it directly travels from HeNBs to S-GW.

  When S1-U relay is enabled, the HeNB-GW Access service has to be associated with the Network GTP-U service and Access GTP-U service. Also the HeNB-GW Access service has to be associated with the HeNB-GW Network service.

**Important**

S1-U Relay is disabled by default. Also when S1-U relay is enabled, both Access and Network GTP-U services need to be in STARTED state for the HeNB-GW access service to be STARTED.
HeNB-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 HeNB-GW functionality for use in HeNB 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.

Important
At least one packet card must be made active prior to service configuration. Information and instructions for configuring the packet cards 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.

This chapter includes the following:

- Information Required to Configure the System as an HeNB-GW, page 38
- HeNB-GW Service Configuration, page 44
- Logging Facility Configuration, page 50
- Alarm and Alert Trap Configuration, page 51
- SNMP MIB Traps for HeNB-GW Service, page 52
- Event IDs for HeNB-GW Service, page 53
- DHCP Configuration, page 54
Information Required to Configure the System as an HeNB-GW

This section provides a high-level series of steps and the associated configuration file examples for configuring the system to perform as an HeNB-GW node in a test environment.

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

Important

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

Required Local Context Configuration Information

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Interface Configuration</td>
<td></td>
</tr>
<tr>
<td>Interface name</td>
<td>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.</td>
</tr>
<tr>
<td>IP address and subnet</td>
<td>IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>Physical port number</td>
<td>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.</td>
</tr>
<tr>
<td>Gateway IP address</td>
<td>Used when configuring static IP routes from the management interface(s) to a specific network.</td>
</tr>
<tr>
<td>Security administrator name</td>
<td>The name or names of the security administrator with full rights to the system.</td>
</tr>
<tr>
<td>Security administrator password</td>
<td>Open or encrypted passwords can be used.</td>
</tr>
<tr>
<td>Remote access type(s)</td>
<td>The type of remote access that will be used to access the system such as telnetd, sshd, and/or ftpd.</td>
</tr>
</tbody>
</table>
## Required Source Context Configuration Information

### Table 2: Required Information for Source Context Configuration

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source context name</td>
<td>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.</td>
</tr>
<tr>
<td>Interface name</td>
<td>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.</td>
</tr>
<tr>
<td>IP address and subnet</td>
<td>IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>Physical port number</td>
<td>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.</td>
</tr>
<tr>
<td>Gateway IP address</td>
<td>Used when configuring static IP routes from the management interface(s) to a specific network.</td>
</tr>
<tr>
<td>Ingress and Egress GTP-U Services</td>
<td></td>
</tr>
<tr>
<td>Ingress GTP-U service Name</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the Ingress GTP-U service can be identified on the system. It is configured in Context Configuration Mode. When S1-U Relay is enabled, the Ingress GTP-U service configuration is critical as it has to be associated with the HeNB-GW Access Service. It is also called access-side GTP-U service for the HeNB-GW ACCESS service.</td>
</tr>
<tr>
<td>Egress GTP-U service Name</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the Egress GTP-U service can be identified on the system. It is configured in Context Configuration Mode. When S1-U Relay is enabled, the Egress GTP-U service configuration is critical as it has to be associated with the HeNB-GW Access Service. It is also called network-side GTP-U service for the HeNB-GW ACCESS service.</td>
</tr>
<tr>
<td>GTP-U Tunnel interface IP address</td>
<td>IP 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 HeNB using GTP-U tunnel. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
</tbody>
</table>
### Required Destination Context Configuration Information

**Table 3: Required Information for Destination Context Configuration**

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination context name</td>
<td>An identification string from 1 to 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system.</td>
</tr>
<tr>
<td>Interface name</td>
<td>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.</td>
</tr>
<tr>
<td>IP address and subnet</td>
<td>IPv4 addresses assigned to the interface. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>Physical port number</td>
<td>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.</td>
</tr>
<tr>
<td>Gateway IP address</td>
<td>Used when configuring static IP routes from the management interface(s) to a specific network.</td>
</tr>
</tbody>
</table>

**HeNB-GW Access Service Configuration**
<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1-MME interface IP address</td>
<td>IPv4/IPv6 addresses assigned to the S1-MME interface as SCTP bond address. This address will be used for binding the SCTP (local bind address(es)) to communicate with the MME using eGTP. The HeNB-GW passes this IP address during setting up the association with the MME. Multiple addresses and subnets are needed if multiple interfaces will be configured.</td>
</tr>
<tr>
<td>Public Land Mobile Network (PLMN) Identifiers</td>
<td>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.</td>
</tr>
<tr>
<td>S1-MME SCTP Port</td>
<td>The physical port to which is used to communicate with the HeNBs over S1-MME interface. It is usually an integer value ranging from 1 to 65535.</td>
</tr>
<tr>
<td>MME ID Group ID</td>
<td>MME Group ID to be configured for the HeNB-GW Access Service. This is a required parameter since the HeNB-GW acts as an MME to the HeNB(s) and this ID is filled in the S1-SETUP response sent to the HeNB(s). It is an integer ranging from 32768..65535.</td>
</tr>
<tr>
<td>MME Code</td>
<td>MME Code is also part of the MME ID configuration. MME Group ID and MME Code both are required for MME Identifier configuration for the HeNB-GW Access service. It is an integer which ranges from 0..255.</td>
</tr>
<tr>
<td>S1-U Relay</td>
<td>Enables the S1-U relay functionality for the HeNB-GW Access Service. Once S1-U Relay is enabled, the association to Ingress and Egress GTP-U services is considered as critical configuration for the HeNB-GW Access service.</td>
</tr>
<tr>
<td>Associate HeNB-GW Network Service</td>
<td>A pre-configured HeNB-GW Network Service is required to be associated to the HeNB-GW Access Service. User can enter a desired HeNB-GW Network service name even if it is not pre-configured, but it will be required to be configured in later course for this HeNB-GW Access service to come up.</td>
</tr>
<tr>
<td>Optional Security Gateway Configuration</td>
<td></td>
</tr>
<tr>
<td>Security Gateway IP address</td>
<td>This is the IP Address where the SeGW service is bound and shall be provided to HeNB during SeGW-Discovery. This security gateway is associated with the HeNB-GW Access Service. Only one SeGW IP address can be configured.</td>
</tr>
<tr>
<td>Diameter Endpoint</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the Diameter endpoint configuration is recognized by the system. This Diameter Endpoint is required by the SeGW to communicate with the AAA server.</td>
</tr>
</tbody>
</table>

| Diameter Endpoint Configuration                |                                                                                 |
### Required Information

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Name</td>
<td>An identification string from 1 to 63 characters (alpha and/or numeric) by which the Diameter endpoint configuration is recognized by the system. This Diameter Endpoint is required by the SeGW to communicate with the AAA server.</td>
</tr>
<tr>
<td>Origin realm name</td>
<td>An identification string between 1 through 127 characters. The realm is the Diameter identity. The originator.s realm is present in all Diameter messages and is typically the company or service name.</td>
</tr>
<tr>
<td>Origin host name</td>
<td>An identification string from 1 to 255 characters (alpha and/or numeric) by which the origin host is recognized by the system.</td>
</tr>
<tr>
<td>Origin host address</td>
<td>The IP address of the interface.</td>
</tr>
<tr>
<td>Peer name</td>
<td>The endpoint name described above.</td>
</tr>
<tr>
<td>Peer realm name</td>
<td>The interface origin realm name described above.</td>
</tr>
<tr>
<td>Peer address and port number</td>
<td>The IP address and port number of the OCS.</td>
</tr>
</tbody>
</table>

### IPsec Crypto-map Template Configuration

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP profile</td>
<td>This is the profile to be used to provide authenticator modes for incoming packets on Security Gateway. Only one EAP profile can be configured.</td>
</tr>
<tr>
<td>IP Pool for IPsec Tunnel</td>
<td>Specifies the IP pool to assign IP address for IPsec traffic to use.</td>
</tr>
<tr>
<td>IKEv2 Transform set</td>
<td>IKEv2 transform set for IKE security association.</td>
</tr>
<tr>
<td>IPsec Crypto-map Template</td>
<td>Specifies the Crypto-map template to be used for IPsec IKEv2 tunneling for the interface configured.</td>
</tr>
<tr>
<td>AAA Server Group Context</td>
<td>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.</td>
</tr>
<tr>
<td>AAA Server Group name</td>
<td>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 HeNB-GW service.</td>
</tr>
</tbody>
</table>

### HeNB-GW Network Service Configuration
**Required Information** | **Description**
--- | ---
Logical eNodeB | The Logical eNodeB configuration option enables the configuration of one or more logical eNodeBs within the HeNB-GW. The Logical eNodeB configuration is usually used to support load balancing within a pool of TAIs. At least one logical eNodeB configuration is required to START an HeNB-GW Network service. 8 Logical eNodeBs are supported per HeNB-GW Network service. **Caution** Deleting or modifying any of the parameters for a fully configured logical eNodeB results in the termination of SCTP connections to MMEs from that logical eNodeb.

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.

| | **Macro eNodeB ID:** Macro eNodeB identifier, required as a parameter for the Logical eNodeB configuration. It is an option to the Home eNodeB identifier.

| | **Home eNodeB ID:** Home eNodeB identifier, required as a parameter for the Logical eNodeB configuration. It is an option to the Macro eNodeB identifier.

| | **S1-MME interface IP address:** IPv4 addresses assigned to the S1-MME interface as SCTP bond address. This address will be used for binding the SCTP (local bind address(es)) to communicate with the MME using eGTP. The HeNB-GW passes this IP address during setting up the association with the MME. Multiple addresses and subnets are needed if multiple interfaces will be configured.

| | **S1-MME SCTP Port:** The physical port to which is used to communicate with the HeNBs over S1-MME interface. It is usually an integer value ranging from 1 to 65535.

Logical eNodeB Configuration | **MME Pool:** A pre-configured MME pool to be associated with the Logical eNodeB. An MME pool is configured in the LTE Policy Configuration Mode. Only one MME Pool instance can be associated with a Logical eNodeB instance. All MMEs in the pool are assumed to support all TAIs in the associated TAI List DB object. One Logical eNodeB can connect up to 8 MMEs and therefore a max of 64 associations can be established between HeNB-GW and MME.

| | **TAI List DB:** A pre-configured list of tracking area identity (TAIs) pool to be associated with the Logical eNodeB. A TAI List database is configured in the LTE Policy Configuration Mode. Only one TAI list DB can be associated with the Logical eNodeB instance. The tai-list-db contains a list of TAIs. These are sent in the S1 Setup message to the MME to indicate the list of TAIs supported by the eNodeB. The TAI database which can be associated to each logical EnodeB can accommodate 256 configuration of TACs.

TAI List DB Configuration
### Required Information

<table>
<thead>
<tr>
<th>Description</th>
<th>Required Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Country Code (MCC): The MCC can be configured to any integer value from 0 to 999.</td>
<td>MCC</td>
</tr>
<tr>
<td>Mobile Network Code (MNC): The MNC can be configured to any integer value from 0 to 999.</td>
<td>MNC</td>
</tr>
<tr>
<td>TAC is an integer value ranging from 0..65535. The HeNB-GW Network service searches these TACs for establishing UE connections.</td>
<td>Tracking Area Code (TAC)</td>
</tr>
</tbody>
</table>

---

## HeNB-GW Service Configuration

HeNB-GW services are configured within source contexts and allow the system to function as an HeNB-GW in the 4G LTE wireless data network.

**Important**

This section provides the minimum instruction set for configuring an HeNB-GW service that allows the system to process bearer contexts with IPsec authentication on SeGW. Commands that configure additional HeNB-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 HeNB-GW service with SeGW enabled:

---

**Step 1** Configure a system context in the Global Configuration Mode, as shown in the Context Configuration section of the HeNB-GW Service Configuration example. Using this step, the user enters in the Context Configuration Mode.

**Step 2** Create an interface and enter the interface configuration mode for newly created interface to add IP addresses along with the subnet mask for this interface, as shown in the Interface and IP Address Configuration section of the HeNB-GW
Service Configuration example. These IP addresses are used to bind to different services including GTP-U Access and Network services and even interfaces like S1-MME.

**Step 3**
Configure the Access and Network GTP-U services, as shown in the *Access and Network GTP-U Services Configuration* section of the *HeNB-GW Service Configuration* example. These services are bound individually to the IP addresses configured in the Step 2.

**Step 4**
Configure the HeNB-GW Network service, as shown in the *HeNB-GW Network Service Configuration* section of the *HeNB-GW Service Configuration* example. Using this step, the user enters in the HeNB-GW Network Service Configuration Mode.

**Step 5**
Configure the logical eNodeB for the HeNB-GW Network service created in step4, as shown in the *Logical eNodeB Configuration* section of the *HeNB-GW Service Configuration* example.

**Step 6**
Bind the S1-MME using IP address of this interface to the Logical eNodeB created in Step 5. Enter the IP address in dotted decimal notation.

**Step 7**
Specify the SCTP port for the S1-MME interface bound in step 6.

**Step 8**
Associate the MME pool name to the Logical eNodeB. This MME pool can be created in the LTE Policy configuration mode, as shown in the *LTE Policy Configuration* example.

**Step 9**
Associate the TAI List database to the Logical eNodeB. This TAI List database can be configured in the LTE Policy configuration mode, as shown in the *LTE Policy Configuration* example.

**Step 10**
Configure the HeNB-GW Access service, as shown in the *HeNB-GW Access Service Configuration* section of the *HeNB-GW Service Configuration* example. Using this step, the user enters in the HeNB-GW Access Service Configuration Mode.

**Step 11**
Bind the S1-MME using IP address of this interface to the HeNB-GW service created in Step 10. Enter the IP address in dotted decimal notation.

**Step 12**
Specify the SCTP port for the S1-MME interface bound in Step 11.

**Step 13**
Configure the MME Group Identifier for the HeNB-GW Access service. As part of this configuration, group ID as well as the MME code has to be configured. MME ID is used as part of S1 setup procedure during HeNB association. It is an integer value ranging from 0 to 255.

**Step 14**
Associate the HeNB-GW Network service configured in the step 4 to this HeNB-GW Access Service.

**Step 15**
Configure the Public Land Mobile Network Identifiers MMC and MNC for this HeNB-GW Access Service.

**Step 16**
Enable the S1-U Relay for this HeNB-GW Access service. Using this step, the user enters in the S1-U Relay Configuration Mode. This is an optional step.

**Step 17**
Associate the Access and Network GTP-U services created in the Step 3 to this HeNB-GW Access service. Association of the GTP-U services is mandatory in case S1-U Relay is enabled.

---

**HeNB-GW Service Configuration**

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

```configure
------------------ Context Configuration ------------------
context <ingress_ctxt_name>

----------- Interface and IP addresses Configuration -----------
interface <interface_name>
  ip address <ipv4_addr> 255.255.255.0
```
ip address <ipv4_addr> 255.255.255.0 secondary
exit

-------- Access and Network GTP-U Services Configuration --------
gtpu-service <gtpu_svc_access> -noconfirm
   bind ipv4-address <secondary1_ipv4_addr>
exit
gtpu-service <gtpu_svc_network> -noconfirm
   bind ipv4-address <secondary2_ipv4_addr>
exit

------------ HeNB-GW Network Service Configuration -------------
henbgw-network-service <henb_network_svc_name> -noconfirm

--------- Logical eNodeB Configuration ------------------------
   logical-enb global-enb-id plmn id mcc <mcc_id> mnc <mnc_id> macro-enb-id <macro_enodeb_id>
   -n
   bind s1-mme { ipv4-address | ipv6-address } <ip_addr>
   s1-mme scpt port <scpt_port_no>
   associate henbgw mme-pool <mme_pool_name>
   associate tai-list-db <lte_policy_tai_db>
exit

------------ HeNB-GW Access Service Configuration --------------
henbgw-access-service <henb_access_svc_name> -n
   bind s1-mme { ipv4-address | ipv6-address } <ip_addr>
   s1-mme scpt port <scpt_port_no>
   mme-id group-id <mme_id> mme-code <mme_code>
   associate henbgw-network-service <henb_network_svc_name>
   plmn id mcc <mcc_id> mnc <mnc_id>

---------- S1-U Relay Configuration -----------------------------
s1u-relay
   associate access-gtpu-service <gtpu_svc_access> context ingress
   associate network-gtpu-service <gtpu_svc_network> context ingress
exit

Notes:

• <ingress_ctxt_name> is name of the source context in which HeNB-GW service is configured.

• <interface_name> is the name of the interface under which primary and secondary IP addresses are to be defined for different services to bind including GTP-U and HeNB-GW Access and Network services.

• <gtpu_svc_access> is the name of the GTP-U service configured in the <ingress_ctxt_name> context mode to provide GTP-U tunnel for HeNB-GW Access service. This GTP-U service will be used as Access GTP-U service and will be associated with the HeNB-GW Access Service in case s1-U relay is enabled.

• <gtpu_svc_network> is the name of the second GTP-U service configured in the <ingress_ctxt_name> context mode to provide GTP-U tunnel for HeNB-GW Network service. This GTP-U service will be used as Network GTP-U service and will be associated with the HeNB-GW Access Service in case s1-U relay is enabled.

• <secondary1_ipv4_addr> is the IPV4 type address defined under the <interface_name> interface and being bound to the <gtpu_svc_name1> GTP-U service.

• <secondary2_ipv4_addr> is the IPV4 type address defined under the <interface_name> interface and being bound to the <gtpu_svc_name2> GTP-U service.

• <henb_network_svc_name> is the HeNB-GW Network service name
• `<secondary3_ipv4_addr>` is the IPv4 type address used to bind with the S1-MME interface.
• `<mme_pool_name>` is the MME pool name as defined while the LTE policy configuration.

**Important**
This MME pool is associated with the HeNB-GW network service.

• `<lte_policy_tai_db>` is the tracking area information database name as defined while the LTE policy configuration.

**Important**
This tracking area information database is associated with the HeNB-GW network service.

• `<henb_access_svc_name>` is the name of the HeNB-GW Access service name.
• `<primary_ipv4_addr>` is the IPv4 type primary address used to bind with the S1-MME interface for this HeNB-GW access service.

• **s1u-relay** enables the S1-U relay functionality by the HeNB-GW service. When configured, user enters into S1-U relay configuration mode. In this mode user has to configure associations to the Access and Network GTP-U services for S1-U relay. When s1-u relay is enabled, the association to ingress and egress GTP-U services is considered as a critical configuration for the HeNB-GW Access service. When S1-U relay is enabled, both Access and Network GTP-Uu services need to be in STARTED state for the HeNB-GW Access service to START.

**Important**
Changing the S1-U Relay configuration is a disruptive operation. The HeNB-GW Service is re-started.

### IPSec Configuration

Use the following example to configure the IPSec configuration which goes with the Security Gateway (SeGW) configuration on the HeNB-GW Access Service.

**For EAP-AKA Authentication Only**

Configure

```plaintext
context <ctxt_name>
    eap-profile <eap_profile_name>
    mode authenticator-pass-through
    exit
ipsec transform-set <ipsec_transform_set_name>
    exit
ikev2-ikesa transform-set <ikesa_transform_set_name>
    exit
crypto template <crypto_template_name> ikev2-dynamic
    authentication remote eap-profile <eap_profile_name>
    ikev2-ikesa transform-set list <ikesa_transform_set_name>
    payload <crypto_template_payload_name> match childsa match ipv4
    ipsec transform-set list <ipsec_transform_set_name>
```

HeNB-GW Administration Guide, StarOS Release 21.2
For Certificate Based Authentication Only

Configure

- **certificate name**: `<cert_name>`
  - pem url `<url format>`
  - private-key pem|der url|data `<url or data format>`
- **ca-cert name**: `<cacert_name>`
- **context**: `<ctxt_name>`
- **ipsec transform-set**: `<ipsec_transform_set_name>`
- **ikev2-ikesa transform-set**: `<ikesa_transform_set_name>`
- **crypto template**: `<crypto_template_name>`
  - ikev2-dynamic
  - authentication remote certificate
  - authentication local certificate
  - ikev2-ikesa transform-set `<ikesa_transform_set_name>`
  - payload `<crypto_template_payload_name>`
    - match childsa match ipv4
  - ipsec transform-set list `<ipsec_transform_set_name>`
- **certificate**: `<cert_name>`
- **ca-certificate list**: ca-cert-name `<cacert_name>`

For Simultaneous support of Multiple Authentication schemes (EAP-AKA & Certificate)

Configure

- **certificate name**: `<cert_name>`
  - pem url `<url format>`
  - private-key pem|der url|data `<url or data format>`
- **ca-cert name**: `<cacert_name>`
- **context**: `<ctxt_name>`
- **eap-profile**: `<eap_profile_name>`
- **mode**: authenticator-pass-through
- **ipsec transform-set**: `<ipsec_transform_set_name>`
- **ikev2-ikesa transform-set**: `<ikesa_transform_set_name>`
- **ikev2-ikesa auth-method-set**: `<auth_profile_name1>`
  - authentication remote eap-profile `<eap_profile_name>`
  - authentication local certificate
  - ikev2-ikesa transform-set `<ikesa_transform_set_name>`
  - payload `<crypto_template_payload_name>`
    - match childsa match ipv4
  - ipsec transform-set list `<ipsec_transform_set_name>`
- **certificate**: `<cert_name>`
- **ca-certificate list**: ca-cert-name `<cacert_name>`
Notes:

• `<ctxt_name>` is the context name on which unique EAP name is to configured.

• `<eap_profile_name>` is a string of size 1 to 128 which configure the context level unique Extensible Authentication Profile (EAP) Name.

• `<ipsec_transform_set_name>` configures the context level name to be used for the IKEv2 IKE Security Association Transform Set. It is a string of size 1 to 127.

• `<crypto_template_name>` configures the name of the Crypto Template. It is a string of size 1 to 104.

• `<crypto_template_payload_name>` is the name of the Crypto Template Payload being configured. This name is unique to the Crypto Template. It is a string of size 1 to 127.

**GTP-U Service Configuration**

Use the following example to configure the GTP-U service parameters to provide GTP-U tunnel over S1-U interface. The two GTP-U

```plaintext
configure
  context <dest_ctxt_name> -noconfirm
gtpu-service <gtpu_svc_access>-noconfirm
  bind address { ipv4-address | ipv6-address } <ip_address>
end

configure
  context <dest_ctxt_name> -noconfirm
gtpu-service <gtpu_svc_network>-noconfirm
  bind address ipv4-address <ip_address>
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_svc_access>` is name of the GTP-U service configured to provide GTP-U tunnel over S1-U interface towards S-GW or core network. This service has to be associated with the HeNB-GW Access Service in case S1-U Relay is enabled.

• `<gtpu_svc_network>` is name of the GTP-U service configured to provide GTP-U tunnel over towards HeNB. This service has to be associated with the HeNB-GW Access Service in case S1-U Relay is enabled.

**LTE Policy Configuration**

Use the following example to configure the LTE Policy. Other configurations done under this config include MME pool and tracking area information list (TAI list) database.

```plaintext
configure
  lte-policy
    hembgw mme-pool <mme_pool_name> -noconfirm
      mme <mme-name> { ipv4-address | ipv6-address } <ip_addr> sctp port <sctp_port_no>
    exit
  tai-list-db <lte_policy_tai_db>
```
Verifying HeNB-GW Configuration

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

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

```
show henbgw-access-service name <henbgw_access_svc_name>
show henbgw-network-service name <henbgw_network_svc_name>
```

The output of these command display concise listing of HeNB-GW Access and Network service parameter settings as configured on system.

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

```
show configuration errors section henbgw-network-service
```

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

Logging Facility Configuration

Use the following example to configure the HeNB-GW system to enable the logging and debug facilities for HeNB-GW subscriber and related protocols.
This section provides the minimum instruction set for configuring logging facilities for system monitoring that allows the user to monitor the events and logging. Commands that configure additional logging facilities are provided in the Exec Mode Command chapter of Command Line Interface Reference.

```
logging filter active facility henbapp level { critical | error | warning | unusual | info | trace | debug }
logging filter active facility henbgw level { critical | error | warning | unusual | info | trace | debug }
logging filter active facility henbgwdemux level { critical | error | warning | unusual | info | trace | debug }
logging filter active facility henbgwmgmr level { critical | error | warning | unusual | info | trace | debug }
configure
  logging console
  logging display event-verbosity {min | concise | full}
  logging filter runtime facility henb-gw level { critical | error | warning | unusual | info | trace | debug }
  logging filter runtime facility henbapp level { critical | error | warning | unusual | info | trace | debug }
  logging filter runtime facility henbgwdemux level { critical | error | warning | unusual | info | trace | debug }
  logging filter runtime facility henbgwmgmr level { critical | error | warning | unusual | info | trace | debug }
  logging filter runtime facility sctp { critical | error | warning | unusual | info | trace | debug }
  logging filter runtime facility threshold { critical | error | warning | unusual | info | trace | debug }
```

Refer System Administration Guide for more information on logging facility configuration.

### Displaying Logging Facility

This section shows the logging facility event logs for logging facilities enabled on HeNB-GW node.

Verify the logging facilities configured on HeNB-GW system node by entering the following command in Exec Mode:
```
show logging [active | verbose]
```
The output of this command provides the display of event logs for all configured logging facilities.

### Alarm and Alert Trap Configuration

To enable and configure the SNMP Traps to generate alarms and alerts from system for various events and thresholds in HeNB-GW service, apply the following example configuration:

```
configure
  snmp trap enable ThreshHENBGWHenbSessions target [ target <trap_collector>]
  snmp trap enable ThreshHENBGPagingMessages target <trap_collector>]
  snmp trap enable ThreshHENBGWUeSessions target <trap_collector>]
  snmp trap { enable | suppress} HenbgwAccessServiceStart [ target <trap_collector>]
```
snmp trap { enable | suppress} HenbgwAccessServiceStart [ target <trap_collector>]

snmp trap { enable | suppress} HenbgwAccessServiceStop [ target <trap_collector>]

snmp trap { enable | suppress} HenbgwMMESCTPAAllAssocDown [ target <trap_collector>]

snmp trap { enable | suppress} HenbgwNetworkServiceStart [ target <trap_collector>]

snmp trap { enable | suppress} HenbgwNetworkServiceStop [ target <trap_collector>]

Notes:

• <trap_collector> is the name of the 1st trap target. It is a string of size 1 to 31.

• There are several additional SNMP Traps which can be configured. Refer Global Configuration Mode chapter of the Command Line Interface Reference for more information.

• For more information on SNMP Traps, refer System SNMP-MIB Reference.

• Repeat this configuration as needed for additional traps.

SNMP MIB Traps for HeNB-GW Service

SNMP traps are used to manage and monitor the service on HeNB-GW node.

Supported SNMP traps and its id are indicated in the following table.

Table 4: SNMP Traps and Object Ids

<table>
<thead>
<tr>
<th>Traps</th>
<th>Object Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>starThreshHENBGWHenbSessions</td>
<td>starentTraps 513</td>
</tr>
<tr>
<td>starThreshClearHENBGWHenbSessions</td>
<td>starentTraps 514</td>
</tr>
<tr>
<td>starThreshHENBGWUeSessions</td>
<td>starentTraps 515</td>
</tr>
<tr>
<td>starThreshClearHENBGWUeSessions</td>
<td>starentTraps 516</td>
</tr>
<tr>
<td>starThreshHENBGWPagingMessages</td>
<td>starentTraps 517</td>
</tr>
<tr>
<td>starThreshClearHENBGWPagingMessages</td>
<td>starentTraps 518</td>
</tr>
<tr>
<td>starHenbgwAccessServiceStart</td>
<td>starentTraps 1193</td>
</tr>
<tr>
<td>starHenbgwAccessServiceStop</td>
<td>starentTraps 1194</td>
</tr>
<tr>
<td>starHenbgwNetworkServiceStart</td>
<td>starentTraps 1195</td>
</tr>
<tr>
<td>starHenbgwNetworkServiceStop</td>
<td>starentTraps 1196</td>
</tr>
<tr>
<td>starHenbgwMMESCTPAassocUp</td>
<td>starentTraps 1227</td>
</tr>
<tr>
<td>starHenbgwMMESCTPAassocDown</td>
<td>starentTraps 1228</td>
</tr>
<tr>
<td>starHenbgwMMESCTPAAllAssocDown</td>
<td>starentTraps 1229</td>
</tr>
<tr>
<td>starHenbgwMMESCTPAAllAssocDownClear</td>
<td>starentTraps 1230</td>
</tr>
</tbody>
</table>
For more information on SNMP trap configuration and supported object ids, refer System SNMP-MIB Reference.

### Event IDs for HeNB-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. Following table lists HeNB-GW specific and other required facilities and corresponding Event ID Ranges:

**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**

<table>
<thead>
<tr>
<th>Facility</th>
<th>Event ID Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>HeNB-GW Manager Facility Events</td>
<td>193000-193999</td>
</tr>
<tr>
<td>HeNB-GW Facility Events</td>
<td>195000-195999</td>
</tr>
<tr>
<td>HeNB-GW DEMUX Facility Events</td>
<td>194000-194999</td>
</tr>
<tr>
<td>SCTP Protocol Facility Events</td>
<td>87300-87499</td>
</tr>
<tr>
<td>AAA Client Facility Events</td>
<td>6000-6999</td>
</tr>
<tr>
<td>Alarm Controller Facility Events</td>
<td>65000-65999</td>
</tr>
<tr>
<td>Card/Slot/Port (CSP) Facility Events</td>
<td>7000-7999</td>
</tr>
<tr>
<td>Command Line Interface Facility Events</td>
<td>30000-30999</td>
</tr>
<tr>
<td>Event Log Facility Events</td>
<td>2000-2999</td>
</tr>
<tr>
<td>Threshold Facility Events</td>
<td>61000-61999</td>
</tr>
</tbody>
</table>
DHCP Configuration

To configure DHCP Proxy interface support on chassis for HeNB-GW service:

**Step 1**
Create a DHCP service specific to HeNB-GW service by applying the example configuration in the Configuring DHCP Service section.

**Step 2**
Create a subscriber template for HeNB clients session and associate the DHCP service with created subscriber template by applying the example configuration in the Configuring Subscriber Template for HeNB section.

**Step 3**
Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command `save configuration`. For additional information on how to verify and save configuration files, refer to the System Administration Guide and the Command Line Interface Reference.

---

**Configuring DHCP Service**

Configure a DHCP service for DHCP interface support in the HeNB-GW service by applying the following example configuration:

```bash
configure
    context <vpn_ctxt_name>
    dhcp-service <dhcp_svc_name> -noconfirm
       dhcp client-identifier ike-id
       dhcp server selection-algorithm use-all
       dhcp server <dhcp_server_ip>
       dhcp server port 67
    end
```

**Notes:**
- `<vpn_ctxt_name>` is name of the source context for DHCP service.
- `<dhcp_svc_name>` is name of the DHCP service configured in Context Configuration mode for DHCP interface support in HeNB-GW service.
- `<dhcp_server_ip>` IP address of the DHCP server associated with DHCP service for DHCP interface support in HeNB-GW service.
- For more commands and keyword options, refer Command Line Interface Reference.

---

**Configuring Subscriber Template for HeNB**

Configure the subscriber template to associate the DHCP service for HeNB clients by applying the following example configuration:

```bash
configure
    context <vpn_ctxt_name>
    subscriber default
       dhcp service <dhcp_svc_name> context <vpn_ctxt_name>
    end
```

---
Notes:

- `<vpn_ctxt_name>` is name of the source context in which Security gateway is configured.
- `<dhcp_svc_name>` is name of the pre-configured DHCP service configured in Context Configuration mode for DHCP interface support in HeNB-GW service.
- For more commands and keyword options, refer Command Line Interface Reference.

**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.
CHAPTER 4

Multi HeNBGW Access Services support

This chapter describes Multi HeNBGW Service support, below are the links to the main sections of the document:

- Feature Description, page 57
- How It Works, page 58

Feature Description

Currently a single HeNBGW Access service is supported in StarOS. As part of this feature, multiple HeNBGW Access services will be supported. There will be no change in the number of HeNBGW Network services. All HeNBGW Access services will continue to interface with the single HeNBGW Network service instance.

Overview

Below are the features of the Multi HeNBGW Service support.

Upto 16 Henbgw Access services in the same or different VPN contexts can be configured. Each Henbgw Access service will have a unique SCTP IP address and port combination.

Each HENBGW Access service have a provision to configure a DSCP value per QCI value. Separate values can be specified in uplink and downlink direction. This DSCP value shall be applied to GTPU packets of eRABs with the given QCI value.

GTPU packets of eRABs coming from or sent to HENBs registering with a particular HENBGW Access service are treated as per the DSCP configuration of that HENBGW Access service.

In scenarios where HENBGW does not know the QCI value for a particular eRAB, a configurable default DSCP value is used. Also configurable pass through mode is available where the DSCP marking will be unaltered by the HENBGW before relaying the packet to the other side.

No additional license is required to enable this feature on StarOS.
How It Works

Configuring Multiple Access Services

An HENBGW Access service is defined in a VPN context. A minimum of the following critical parameters must be configured in an access service to move the service to started state:

- SCTP bind address
- SCTP bind port
- MME group id and PLMN ID
- HENBGW Network service
- GTPU services if S1U is enabled

A maximum of 16 HENBGW Access services in the same or different VPN contexts can be configured. There will be a single instance of HENBGW Network service. All the access services share all the logical ENodeB’s configured in the HENBGW Network service. The logical ENodeB will be selected based on the TAI sent by the HENB.

Each HENBGW Access service will have its own unique SCTP bind address and port combination. Any attempt to reuse these parameters across Access Services will be rejected while validating the configuration from CLI commands.

Each HENBGW Access service will have its own unique security gateway bind address. Any attempt to reuse this address across access services shall be rejected while validating the configuration from CLI commands.

Configuring QCI to DSCP Mapping Templates

User can now define QCI to DSCP marking mapping templates under the lte-policy configuration mode. A maximum of 32 such templates can be defined.

HENBGW Access service can refer to two such mapping templates, one for DSCP marking of uplink GTPU packets and other for downlink GTPU packets.

The template also has a provision to configure a default DSCP marking to be used in case DSCP marking is not defined for a particular QCI value or if QCI value is not known for a particular eRAB.

If no QCI to DSCP mapping template is referenced in an HENBGW Access service, then HENBGW acts in a pass through mode where it does not alter the DSCP marking of GTPU packets before forwarding to the peer node.
IPv6 and Dual Stack IP Support for HeNB-GW Access Service

Feature Information

Summary Data

<table>
<thead>
<tr>
<th>Status</th>
<th>New Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduced-In Release</td>
<td>21.2</td>
</tr>
<tr>
<td>Modified-In Release(s)</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Applicable Product(s)</td>
<td>HeNB-GW, SecGW</td>
</tr>
<tr>
<td>Applicable Platform(s)</td>
<td>ASR 5000 ASR 5500 VPC-SI VPC-DI</td>
</tr>
<tr>
<td>Default Setting</td>
<td>Disabled</td>
</tr>
<tr>
<td>Related CDETS ID(s)</td>
<td>CSCvb74765</td>
</tr>
<tr>
<td>Related Changes in This Release</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>
**Feature Description**

With this feature, HeNB-GW supports IPv6 addressing on the core network, and dual-stack IP addressing on the access side when HeNB-GW is integrated with a Security Gateway (SecGW). An IPv6 address can be used in the crypto template associated with the HeNB-GW access service, and in the bind address of the HeNB-GW access service. Different or similar crypto templates can be configured with both IPv4 and IPv6 addresses, and associated with the same HeNB-GW service.

IPsec tunnels can be initialized, authenticated and established between HeNB and HeNB-GW using IPSec IKEv2 protocols over IPv6.

The configuration parameter IE in the IKE_Auth message directs the type of internal IP address allocated for the IPsec tunnel. The HeNB-GW access service can be configured to allocate a single or dual IP address, when a dual IP address is requested in the IKEv2 Auth request. When configured to allocate a single IP address, priority is given to IPv6. If the IPv6 address pool is not available or exhausted, then address from IPv4 pool will be allocated if available. When configured to allocate dual IP addresses, the SecGW will allocate both IPv4 and IPv6 address when available.

**Limitation**

Currently, only IPv4 address is supported when the IP for HeNB is allocated using a DHCP server.

**Configuring IPv6 and Dual Stack IP for HeNB-GW Access Service**

Use the following configuration to:

- bind multiple IP addresses (dual stack) to an S1-MME interface.
- bind both IPv4 and IPv6 SecGW addresses to the HeNB-GW access service (when HeNBG​​W and SecGW are co-located)
- specify the IP allocation mode when a HeNB requests for dual IP.

```
config
  context context_name
```
**henbgw-access-service**

**bind s1-mme** ipv4-address ipv4_access_address ipv6-address ipv6_access_address
**s1-mme sctp port** port_num
**associate henbgw-network-service** nw_service_name
**associate sctp-param-template** template_name
**security-gateway ip alloc-mode** { single | dual }
**security-gateway bind ipv4-address** ipv4_address crypto-template template_name
**security-gateway bind ipv6-address** ipv6_address crypto-template template_name
**s1-relay**
**associate access-gtpu-service** access_gtpu_svc [ context context_name ]
**associate network-gtpu-service** network_gtpu_svc [ context context_name ]
**end**

**Notes:**

- Use the **bind s1-mme** command to bind the pre-configured HeNB-GW Access Service to the IP address of the S1-MME interface.
- Use the **associate** command to associate a pre-configured HeNB-GW network service and SCTP parameter template to the HeNB-GW access service.
- Use the **security-gateway bind** command to configure the IPv4 and IPv6 address to be used as the connection point for establishing IKEv2 sessions, and to specify the crypto template to use for the security gateway (SecGW) for the HeNB-GW access service.
- Use the **security-gateway ip alloc-mode** command to assign a single or dual-stack IP for the HeNB.
  - When **ip alloc-mode** is **single** and a HeNB requests for a dual IP, the HeNB-GW access service will try to allocate an IPv6 address to HeNB. If the IPv6 address is unavailable, an IPv4 address will be allocated. This is the default behaviour.
  - When **ip alloc-mode** is **dual** and a HeNB requests for a dual IP, the HeNB-GW access service will allocate both IPv6 and IPv4 addresses to HeNB based on availability.
- Use the **s1u-relay** command to associate a pre-configured Access GTP-U service as well as the Network GTP-U service to this HeNB-GW Access Service for S1-U relay service functionality.

**Monitoring and Troubleshooting**

**Show Command(s) and/or Outputs**

The show command(s) in this section are available in support of IPv6 and Dual Stack IP for HeNB-GW services.

**show henbgw-access-service**

The following fields are available in the output of the **show henbgw-access-service** { name henb_svc_name | all } command in support of this feature:

- **Service name** : foo
- **Context name** : ingress
- **Status** : STARTED
- **SCTP IPv4 Address** : 1.1.1.1
- **SCTP IPv6 Address** : 1::1
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service name</td>
<td>Name of the HeNB-GW access service.</td>
</tr>
<tr>
<td>Context name</td>
<td>Indicates the context under which the HeNB-GW access service is configured.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates the current status of the HeNB-GW access service.</td>
</tr>
<tr>
<td>SCTP IPv4 Address</td>
<td>The IPv4 address of the local Stream Control Transmission Protocol (SCTP)</td>
</tr>
<tr>
<td></td>
<td>associated with the HeNB-GW access service.</td>
</tr>
<tr>
<td>SCTP IPv6 Address</td>
<td>The IPv6 address of the local Stream Control Transmission Protocol (SCTP)</td>
</tr>
<tr>
<td></td>
<td>associated with the HeNB-GW access service.</td>
</tr>
<tr>
<td>Security GW service IPv4</td>
<td>The IPv4 address used as the connection point for establishing IKEv2 session</td>
</tr>
<tr>
<td>Address</td>
<td>for the SecGW associated with the HeNB-GW access service.</td>
</tr>
<tr>
<td>Security GW Context</td>
<td>The SecGW context associated with the HeNB-GW access service.</td>
</tr>
<tr>
<td>Crypto-Template</td>
<td>Name of the crypto template used by SecGW that is associated with the HeNB-</td>
</tr>
<tr>
<td></td>
<td>GW access service.</td>
</tr>
<tr>
<td>Security GW IP Allocation</td>
<td>The IP allocation mode configured for the HeNB-GW access service.</td>
</tr>
<tr>
<td>Mode</td>
<td></td>
</tr>
<tr>
<td>Service in IPSec</td>
<td>Current status of the IPSec service.</td>
</tr>
<tr>
<td>Security GW service IPv6</td>
<td>The IPv6 address used as the connection point for establishing IKEv2 session</td>
</tr>
<tr>
<td>Address</td>
<td>for the SecGW associated with the HeNB-GW access service.</td>
</tr>
<tr>
<td>Security GW Context</td>
<td>The SecGW context associated with the HeNB-GW access service.</td>
</tr>
<tr>
<td>Crypto-Template</td>
<td>Name of the crypto template used by SecGW that is associated with the HeNB-</td>
</tr>
<tr>
<td></td>
<td>GW access service.</td>
</tr>
<tr>
<td>Service in IPSec</td>
<td>Current status of the IPSec service.</td>
</tr>
</tbody>
</table>
Monitoring the HeNB-GW Service

This chapter provides information for monitoring service status and performance using the `show` commands found in the Command Line Interface (CLI). These commands 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, page 63
- Monitoring Logging Facility, page 66
- Clearing Statistics and Counters, page 67

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 7: System Status and Performance Monitoring Commands**

<table>
<thead>
<tr>
<th>To do this:</th>
<th>Enter this command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>View HeNB-GW Service Information</td>
<td><code>show henbgw session all</code></td>
</tr>
<tr>
<td>View HeNB-GW services running on chassis</td>
<td><code>show henbgw session summary</code></td>
</tr>
<tr>
<td>View summary of HeNB-GW sessions running on chassis</td>
<td><code>show henbgw session full</code></td>
</tr>
<tr>
<td>View detailed information of HeNB-GW sessions</td>
<td></td>
</tr>
</tbody>
</table>
To do this: | Enter this command:
---|---
View HeNB-GW session information specific to an S1 peer | show hengw session s1-peer ipv4-addr

### Monitoring HeNB and UE by Protocol Monitoring

- **Monitor HeNB through Protocol Monitoring**
  - Command: `monitor protocol`
  - Use following protocol options for HeNB monitoring:
    - S1-AP
    - SCTP
    - GTP-U

- **Monitor UE through Protocol Monitoring**
  - Command: `monitor protocol`
  - Use following protocol options for HeNB monitoring:
    - S1-AP
    - SCTP
    - GTP-U

### View Subscriber Information

- **Display Session Resource Status**
  - Command: `show resources session`

- **Display Subscriber Configuration Information**
  - View locally configured subscriber profile settings (must be in context where subscriber resides)
    - Command: `show subscribers configuration username subscriber_name`
  - View remotely configured subscriber profile settings
    - Command: `show subscribers aaa-configuration username subscriber_name`

- **View Subscribers Currently Accessing the System**
  - View a listing of subscribers currently accessing the system
    - Command: `show subscribers henbgw-only all`
  - View information for a specific subscriber
    - Command: `show subscribers henbgw-only full username username`

- **View Subscriber Counters**
  - View counters for a specific subscriber
    - Command: `show subscribers counters username subscriber_name`

- **View Recovered Session Information**
  - View session state information and session recovery status
    - Command: `show subscriber debug-info { callid | msid | username }`
To do this: | Enter this command:
---|---
View Session Statistics and Information | Enter this command:
Display Historical Session Counter Information | show session counters historical
View all historical information for all sample intervals | show session counters historical
Display Session Duration Statistics | show session duration
View session duration statistics | show session duration
Display Session State Statistics | show session progress
View session state statistics | show session progress

**Display Session Subsystem and Task Statistics**
Refer 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 HeNB-GW Manager statistics | show session subsystem facility henbgwmgmgr all
View HeNB-GW Demux Manager statistics | show session subsystem facility henbgwdemux all
View Session Manager statistics | show session subsystem facility sessmgr all
View HeNB-GW Manager facility statistics | show logs facility henbgw
View HeNB Manager facility statistics | show logs facility henbgwmgmgr
View HeNB App facility statistics | show logs facility henbapp
View HeNB-GW Demux facility statistics | show logs facility henbgwdemux
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 HeNB-GW Access Service Configuration**

Display an HeNB-GW Access Service Status
View all configured HeNB-GW access services configuration in detail | show henbgw-access-service all

**View HeNB-GW Network Service Configuration**

Display an HeNB-GW Network Service Status
View all configured HeNB-GW Network services configuration in detail | show henbgw-network-service all
View configuration errors in HeNB-GW Network Service section in detail | show configuration errors section
| henbgw-network-service verbose
### To do this: | Enter this command:
--- | ---
**View HeNB-GW Access Service Related Statistics**
View HeNB-GW Access service statistics filtered on an HeNB-GW Access service | show henbgw-access-service statistics
tenbgw-access-service henbgw_access-svc_name verbose

View HeNB-GW Access service statistics filtered by a peer id | show henbgw-access-service statistics peer-id peer_identifier

View HeNB-GW Access service S1AP statistics | show henbgw-access-service statistics s1ap verbose

View HeNB-GW Access service SCTP statistics | show henbgw-access-service statistics sctp [ buffer | verbose ]

**View HeNB-GW Network Service Related Statistics**
View HeNB-GW Network service statistics filtered on an HeNB-GW Network service | show henbgw-network-service statistics
tenbgw-network-service henbgw_network-svc_name verbose

View HeNB-GW Network service statistics filtered by a peer id | show henbgw-network-service statistics peer-id peer_identifier

View HeNB-GW Network service S1AP statistics | show henbgw-network-service statistics s1ap verbose

View HeNB-GW Network service SCTP statistics | show henbgw-network-service statistics sctp [ buffer | verbose ]

**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

---

### Monitoring Logging Facility

**Table 8: Logging Facility Monitoring Commands**

<table>
<thead>
<tr>
<th>To do this:</th>
<th>Enter this command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor logging facility for specific session based on Call-id on system</td>
<td>logging trace callid call_id</td>
</tr>
</tbody>
</table>

| Monitor logging facility based on IP address used in session on system | logging trace ipaddr ip_address |

| Monitor logging facility based on MS Identity used in session on system | logging trace msid ms_identifier |
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 (HeNBGW-Access-Service, HeNBGW-Network-Service, 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.
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, page 69

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 HeNB-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 HeNB-GW service is configured.

The command has the following syntax:

gtpu test echo gtpu-service gtpu_svc_name { all | peer-address ip_addr } gtpu-version { 0 | 1 }

<table>
<thead>
<tr>
<th>Keyword/Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gtpu-service gtpu_svc_name</td>
<td>Specifies the GTP-U service configured on the system and associated with the HeNB-GW Network service.</td>
</tr>
</tbody>
</table>
Specifies the IP address of the HeNB node.

**NOTE:** The IP address of the system's interface must be bound to a configured HeNB-GW service prior to executing this command.

<table>
<thead>
<tr>
<th>Keyword/Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-address ip_addr</td>
<td>Specifies the IP address of the HeNB node.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that GTP-U echo requests will be sent to all Nodes that currently have sessions with the HeNB-GW service.</td>
</tr>
<tr>
<td>gtpu-version { 0</td>
<td>1 }</td>
</tr>
</tbody>
</table>

### Using the SNMP TRAP command for debugging

Once the thresholds are configured, then notifications get generated on reaching the limit in the configured interval and are then shown in the SNMP trap.

The SNMP traps for HeNB-GE service can be configured using the following command syntax:

```plaintext
snmp trap enable { ThreshHENBGWHenbSessions | ThreshHENBGWPagingMessages | ThreshHENBGWUESessions } target trap_target
```

<table>
<thead>
<tr>
<th>Keyword/Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ThreshHENBGWHenbSessions</td>
<td>Enables the threshold configuration for HeNB-GW HeNB sessions.</td>
</tr>
<tr>
<td>ThreshHENBGWPagingMessages</td>
<td>Enables the threshold configuration for HeNB-GW paging messages.</td>
</tr>
<tr>
<td>ThreshHENBGWUESessions</td>
<td>Enables the threshold configuration for HeNB-GW UE sessions.</td>
</tr>
<tr>
<td>trap_target</td>
<td>Specifies that these trap(s) should be sent to this trap target.</td>
</tr>
</tbody>
</table>

### Using the RESOURCES SESSION command for debugging

The `show resources session` command is ideal for debugging the license-controlled number of HeNBs and subscribers/UEs connecting to the HeNB-GW.

The license status for all sort of resources can be viewed using the following command syntax:

```plaintext
show resources session
```

In case, the number of sessions are within the acceptable limits, the output of the above command looks as the following sample (only HeNB-GW related sessions have been shown):

```
HENBGW Service:
    In Use : 1161
    Max Used : 1161 ( Monday May 06 05:22:00 IST 2013 )
    Limit : 2000
    License Status : Within Acceptable Limits
HENBGW UE Service:
    In Use : 1700
    Max Used : 1700 ( Monday May 06 05:20:10 IST 2013 )
    Limit : 2000
    License Status : Within Acceptable Limits
```
In case, the number of sessions are over the license capacity, the output of this command looks as the following sample (only HeNB-GW related sessions have been shown):

HENBGW Service:
  In Use : 2000
  Max Used : 2000 ( Monday May 06 05:22:00 IST 2013 )
  Limit : 2000
  License Status : Over License Capacity (Rejecting Excess Calls)

HENBGW UE Service:
  In Use : 2000
  Max Used : 2000 ( Monday May 06 05:20:10 IST 2013 )
  Limit : 2000
  License Status : Over License Capacity (Rejecting Excess Calls)
Using the RESOURCES SESSION command for debugging