HeNB Gateway in Wireless LTE Network

eNode B is the node with radio access capabilities in LTE radio access network (RAN) that is responsible for radio transmission and reception from UEs in absence of Radio Network Controller (RNC) in LTE. The functionality of eNode B is enhanced to handle the tasks which were handled by the RNC in the 3G network. The Home eNode B (HeNB) provides LTE radio coverage for LTE devices/handsets within a home residential or enterprise coverage area. An HeNB incorporates the capabilities of a standard eNode B.

The Cisco® ASR5x00 provides LTE wireless carriers with a flexible solution that functions as a Home eNode B Gateway (HeNB-GW) in HeNB Access Network to connect UEs with existing LTE networks.

The Home eNodeB Gateway works as a gateway for HeNBs to access the core networks. The HeNB-GW concentrates connections from a large amount of HeNBs through S1 interface and terminates the connection to existing Core Networks using standard interface.

This overview provides general information about the HeNB Gateway including:

- Product Description, page 1
- Network Deployment and Interfaces, page 11
- Features and Functionality - Base Software, page 14
- Features and Functionality - Optional Enhanced Feature Software, page 30

Product Description

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)
- Cisco Virtualized Packet Core-Distributed Instance (VPC-DI)

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 18
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.

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 specified criteria. This section discusses the rule actions and criteria supported by the system.

• Rule Order: A single ACL can consist of multiple rules. Each packet is compared against each of the ACL rules, in the order in which they were entered, until a match is found. Once a match is identified, all subsequent rules are ignored.

**Important**

For more information on Access Control List configuration, refer to the *IP Access Control List* chapter in *System Administration Guide*.

---

### 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 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.

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 HeNBGW 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.

Important

From release 16.0 FCS Full Session Recovery on HENBGW is supported.

• 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.

Important

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
• hENBM
• GTPuMGR
• gTPu
• 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.

![Diagram of X2 Handover Procedure Support](image)

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, HeNBGW will forward the request only to HeNBs that belong to the Tracking Area or Cell Id specified in the message.

HeNBGW 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, HeNBGW will forward the request to all HeNBs associated with TAI in the list.
2. If Cell Id list is present in Warning Area List, HeNBGW 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.

a. The message will be considered duplicated only if the message matches the original message exactly.

b. 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.

c. 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, HeNBGW 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 HenBW 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 HenBW 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 henbgwmgmgr 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)*

1. HENB sends INIT UE message with UE selected PLMN
2. Is the PLMN and TAC associated to the HENB?
   - No
   - Yes
3. Selects logical Enodb
4. Select MME based on GUMMEI or S-TMSI or TAI
5. Forward INIT UE message to MME
6. Send error indication to HENB and drop the message

404840
• 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**

**Figure 12: X2 GW logical 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.
Features and Functionality - Optional Enhanced Feature Software

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

Important
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.
Session Recovery Enhancements

The HeNB GW is the concentrator of HeNBs. Session Recovery feature of HeNB GW 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 HeNB GW 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 HeNB GW will have proper HeNB context information. HeNB GW will send MME configuration update message to all the HeNBs 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 callline details or HeNB UE callline details.

When Session Manager performs audit with HeNB GW 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 HeNB GW Demux, audit fails.
Extension of Peer Certificate Disabled

The CRL Distribution Point (CDP) feature is CLI controlled. A new command ikev2-ikesa cdp is available in the Crypto Template IKEv2-Dynamic Payload Configuration mode to enable or disable the CDP feature. The ikev2-ikesa cdp command is disabled by default.

Configuring CDP

This section describes the download CDP Extension of Peer Certificated Disable configuration.

Use the following configuration to enable or disable the CDP feature:

```
configure
  context context_name
    crypto template template_name ikev2-dynamic
    [ no ] ikev2-ikesa cdp
  end
```

Notes:

- The **no** command prefix disables the CDP feature configuration.
- The **ikev2-ikesa** command configures the configuration parameters for the IKEv2 Security Associations derived from the Crypto Template.
- The **cdp** command configures the CDP from the peer certificate for CRL download.
Extension of Peer Certificate Disabled