Oracle® Communications HLR Router

HLR Router Online Help

E72252 Revision 01

June 2016

ORACLE®

HLR Router HLR Router Online Help

Table of Contents

List of Tables

Chapter 1

Introduction

Topics:

The chapter contains general information about the HLR Router documentation, the organization of this manual, and how to get technical assistance..

Purpose of this documentation

This documentation:

- Gives a conceptual overview of the application's purpose, architecture, and functionality
- Describes the pages and fields on the application GUI (Graphical User Interface)
- Provides procedures for using the application interface
- Explains the organization of, and how to use, the documentation

Scope and Audience

This guide is intended for trained and qualified system operators and administrators who are responsible for managing an HLR Router system.

Manual Organization

This HLR Router Online Help document is organized into the following chapters:

- *Introduction* contains general information about the HLR Router documentation, the organization of this manual, and how to get technical assistance.
- *EAGLE XG Database* describes the functions of and contains procedures for configuration and maintenance of the Network Entity, DN, IMSI, and PDBI databases.
- *Tekelec HLR Router* describes and contains procedures for configuration and maintenance of the Tekelec HLR Router.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

Icon	Description
	Danger: (This icon and text indicate the possibility of *personal injury*.)

Icon	Description
	Warning: (This icon and text indicate the possibility of *equipment damage*.)
	Caution: (This icon and text indicate the possibility of *service interruption*.)
	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Related Publications

The HLR Router documentation set includes these publications, which provide information for the configuration and use of HLR Router and related applications.

Some documents are available only through the Oracle Technical Network (OTN).

The current releases of all documents are available through the Oracle Technical Network

Getting Started includes a product overview, system architecture, and functions. It also explains the HLR Router GUI features including user interface elements, main menu options, supported browsers, and common user interface widgets.

Operation, Administration, and Maintenance (OAM) Guide provides information on system-level configuration and administration tasks for the advanced functions of the HLR Router, both for initial setup and maintenance.

HLR Router Online Help explains how to use the HLR Router GUI pages to manage the configuration and maintenance of the EAGLE XG Database and the Tekelec HLR Router.

HLR Router Administration Guide describes HLR Router architecture, functions, system and PDBI configuration; Signaling and Transport configuration; the Query Server; and PDE CSV file formats.

HLR Router Alarms, KPIs, and Measurements Reference Guide provides detailed descriptions of alarms, events, Key Performance Indicators (KPIs), and measurements; indicates actions to take to resolve an alarm, event, or unusual measurement value; and explains how to generate reports containing current alarm, event, KPI, and measurement information.

SS7/Sigtran User Guide describes HLR Router's Signaling Network Interface, which provides standard SCCP functionality, traditional MTP3 routing capabilities, and a standardM3UA interface to the external network. The SS7/Sigtran section of the documentation explains how to use the SS7/Sigtran GUI pages to perform configuration and maintenance tasks related to adjacent servers, SS7 signaling points, link sets, associations, routes, and SS7/Sigtran options.

Transport Manager User Guide describes the configuration of Transports (SCTP associations and UDP connections with remote hosts over an underlying IP network).

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, *http://docs.oracle.com*. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at *http://www.adobe.com*.

1. Access the Oracle Help Center site at *http://docs.oracle.com*.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

My Oracle Support (MOS)

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), Select **1**
   - For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Chapter 2

EAGLE XG Database

Topics:

The **EAGLE XG Database** menu options provide the ability to perform subscriber database related configuration and maintenance tasks.

The available database menu options will vary based on the type of server you are logged into and the permissions assigned to your group. If you do not see a menu option you need, please make sure you are logged into the appropriate type of server and ask your administrator to make sure the group your user ID belongs to has the appropriate permissions.

Configuration

The **EAGLE XG Database** > **Configuration** menu options allow you to manage subscriber database and PDBI related configuration. These database configuration options are only available when logged into an NOAM server.

When logged into an NOAM server you can view, add, update, and delete Network Entity, DN, and IMSI database information using the Network Entity, DN, and IMSI Database Configuration menus. The PDBI Configuration menus allow you to configure PDBI options and view, insert, edit, and delete PDBI connections, blacklist ranges, and exports.

The available database menu options will vary based on the type of server you are logged into and the permissions assigned to your group. If you do not see a menu option you need, please make sure you are logged into the appropriate type of server and ask your administrator to make sure the group your user ID belongs to has the appropriate permissions.

Network Entity database configuration

The HLR application maintains a subscriber database that associates Network Entities with IMSIs and DNs. The bulk of information in the database is provisioned through a PDBI interface, but the application GUI allows you to view database entries and make adjustments as necessary. A Network Entity is an end node that provides a voice or signaling service. In this application, the Network Entity is an HLR.

Each Network Entity record describes an HLR signal point with its E.164 number and routing data required to successfully forward an SS7 message to it. Spare point codes, indicated by an optional `s-` prefix, are supported for Network Entities with a point code type of International or National. A maximum of 512 Network Entity records are supported.

The **EAGLE XG Database** > **Configuration** > **Network Entity** page allows you to view and modify Network Entity database entries. With this page you can:

- Retrieve: look up Network Entity entires in the database and view the Network Entity's routing data
- Add: add a new Network Entity (HLR) and its routing information to the database
- Update: update a Network Entity's routing information
- Delete: delete an existing Network Entity database entry

Add Network Entity data configuration elements

The **EAGLE XG Database** > **Configuration** > **Network Entity Add** tab allows you to add routing information for a Network Entity to the database. This table describes the fields on the page.

Table 2: Add Network Entity Database Configuration Elements

Element	Description	Data Input Notes
Network Entity	Numeric identifier for the Network Entity	Format: Digits only Range: 1 - 15 digits

Element	Description	Data Input Notes
Service type	Type of service provided	Format: Pulldown menu Range: HLRR/SP Default: HLRR/SP
Point Code Type	Type of point code	Format: Pulldown menu Range: ANSI, INTL, NATL Default: ANSI
Point Code	Point code for the service. This information is used to update the CdPA of incoming messages requiring this service.	Format: Alphanumeric Range: 1 - 11 characters
Subsystem Number	Optional subsystem number for the service. This information is used to update the CdPA of incoming messages requiring this service.	Format: Digits, no value Range: blank, 2 - 255
Cancel Called Global Title	Cancel Called Global Title	Format: Pulldown menu Range: Yes, No Default: No
Routing Indicator	Routing Indicator for the service. This information is used to update the CdPA of incoming messages requiring this service.	Format: Pulldown menu Range: GT, SSN Default: GT
Translation Type	Optional translation type for the service. This information is used to update the CdPA of incoming messages requiring this service. This field cannot be specified when CCGT = Yes.	Format: Digits, no value Range: blank, 0 - 255
Numbering Plan	Optional numbering plan for the service. This information is used to update the CdPA of incoming messages requiring this service. This field cannot be specified when CCGT = Yes.	Format: Digits, no value Range: blank, 0 - 15
Nature of Address Indicator	Optional nature of address indicator for the service. This information is used to update the CdPA of incoming messages requiring this service. This field cannot be specified when CCGT = Yes.	Format: Digits, no value Range: blank, 0 - 127

Element	Description	Data Input Notes
Digit Action	Action to perform on the CdPA Global Title Address of the outgoing message. This field is ignored when CCGT = Yes.	Format: Pulldown menu Range: None, Replace, Prefix, Insert, DelCc, DelCcPrefix, Spare 1, Spare 2 Default: None

Adding a Network Entity database configuration

You can only perform this task when logged into the Active Primary NOAM.

Use this procedure to configure an HLR/SP Network Entity. To prevent creation of DN or IMSI entries, a blacklist entry is automatically generated when this Network Entity is added (if not already manually added to the blacklist table).

1. Select **EAGLE XG Database** > **Configuration** > **Network Entity**.
   The **EAGLE XG Database** > **Configuration** > **Network Entity** page appears.
2. Click the **Add** tab.
   The **Add** tab appears.
3. Enter the Network Entity you want to add in the **Network Entity** field.
4. Select the Service Type from the **Service Type** pulldown.
   The default service type for HLR Router is HLRR (HLR Routing).
5. Select the point code type from the **Point Code Type** pulldown.
6. Enter the point code for the service in the **Point Code** field.
   The point code should meet the format parameters of the point code type you selected.
7. Select **Yes** or **No** from the **Cancel Called Global Title** pulldown.
   If you select **Yes**, the Global Title is not called and the Digit Action Value is ignored.
8. Select either **GT** (Global Title) or **SSN** (Subsystem Number) from the **Routing Indicator** pulldown.
9. If you selected **No** for the Cancel Called Global Title, select a digit action from the **Digit Action** pulldown.
   If you have selected **Yes** for the Cancel Called Global Title then the value selected in this field is ignored. The default value for this field is **None**.
10. Fill out other optional fields on this page as desired. For more information about the fields on this page see *Add Network Entity data configuration elements*.
    - If the **Routing Indicator** is **SSN** you should enter an **SSN** in the **Subsystem Number** field.
    - If **Cancel Called Global Title** is set to **Yes** then the **Translation Type**, **Numbering Plan**, and **Nature of Address Indicator** values cannot be entered.
11. After you have entered all relevant information, click the **Add** button.
    A message appears on the page letting you know if the task was successful.

The Network Entity is added to the database. A corresponding blacklist entry is automatically generated for this Network Entity (if not already manually added to the blacklist table).

Retrieve Network Entity data configuration elements

The **EAGLE XG Database** > **Configuration** > **Network Entity Retrieve** tab allows you to retrieve the routing information for the specified Network Entity from the database. This table describes the fields on the page.

Table 3: Retrieve Network Entity Data Configuration Tab

Element	Description	Data Input Notes
Network Entity	Numeric identifier for the Network Entity	Format: Digits only Range: 1 - 15 digits

When you enter a valid Network Entity value and click the Retrieve tab, the page populates with a table containing the Network Entity's current database values. This table describes the fields on this page.

Table 4: Retrieve Network Entity Database Configuration Elements

Element (Fields marked with an asterisk are required)	Description
Network Entity	Network Entity number
Service type	The type of service the Network Entity provides. This is typically HLRR/SP (Home Location Register Router/ Service Provider).
PC	Point code type and number
CCGT	Indicates whether to cancel the called Global Title
RI	Routing Indicator. Specifies whether routing is based on SSN or Global Title.
SSN	Subsystem number; used to update the CdPA
TT	Translation type
NP	Numbering plan; used to update the CdPA of incoming messages requiring this service
NAI	Optional nature of address indicator
Digit Action	If Yes, changes are applied to the CdPA Global Title Address

Retrieving a Network Entity database configuration

You can only perform this task when logged into an NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **Network Entity**.
   The **EAGLE XG Database** > **Configuration** > **Network Entity** page appears.
2. Enter the Network Entity you want to view in the **Network Entity** field.

3. Click the **Retrieve** button.

The Network Entity record is shown on the page.

Update Network Entity data configuration elements

The **EAGLE XG Database** > **Configuration** > **Network Entity Update** tab allows you to update a Network Entity's routing information in the database. This table describes the fields on the page.

Table 5: Update Network Entity Database Configuration Tab

Element	Description	Data Input Notes
Network Entity	Numeric identifier for the Network Entity	Format: Digits only Range: 1 - 15 digits

When you enter a valid Network Entity value and click the Update tab, the page populates with a table containing the Network Entity's current database values. This table describes the fields on this page.

Table 6: Update Network Entity Database Configuration Elements

Element	Description	Data Input Notes
Network Entity	Numeric identifier for the Network Entity	Format: Digits only Range: 1 - 15 digits
Service type	Type of service provided	Format: Pulldown menu Range: HLRR/SP Default: HLRR/SP
Point Code Type	Type of point code	Format: Pulldown menu Range: ANSI, INTL, NATL Default: ANSI
Point Code	Point code for the service. This information is used to update the CdPA of incoming messages requiring this service.	Format: Alphanumeric Range: 1 - 11 characters
Subsystem Number	Optional subsystem number for the service. This information is used to update the CdPA of incoming messages requiring this service.	Format: Digits, no value Range: blank, 2 - 255
Cancel Called Global Title	Cancel Called Global Title	Format: Pulldown menu Range: Yes, No Default: No

Element	Description	Data Input Notes
Routing Indicator	Routing Indicator for the service. This information is used to update the CdPA of incoming messages requiring this service.	Format: Pulldown menu Range: GT, SSN Default: GT
Translation Type	Optional translation type for the service. This information is used to update the CdPA of incoming messages requiring this service. This field cannot be specified when CCGT = Yes.	Format: Digits, no value Range: blank, 0 - 255
Numbering Plan	Optional numbering plan for the service. This information is used to update the CdPA of incoming messages requiring this service. This field cannot be specified when CCGT = Yes.	Format: Digits, no value Range: blank, 0 - 15
Nature of Address Indicator	Optional nature of address indicator for the service. This information is used to update the CdPA of incoming messages requiring this service. This field cannot be specified when CCGT = Yes.	Format: Digits, no value Range: blank, 0 - 127
Digit Action	Action to perform on the CdPA Global Title Address of the outgoing message. This field is ignored when CCGT = Yes.	Format: Pulldown menu Range: None, Replace, Prefix, Insert, DelCc, DelCcPrefix, Spare 1, Spare 2 Default: None

Updating Network Entity database configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **Network Entity**.
   The **EAGLE XG Database > Configuration > Network Entity** page appears.
2. Click the **Update** tab.
   The **Update** tab appears.
3. Enter the Network Entity you want to update in the **Network Entity** field.
4. Click the **Lookup** button.
   If this is a valid Network Entity, the **Update Network Entity Database Configuration** tab will load a modifiable page. If the Network Entity does not currently exist in the database an error code will appear.
5. Update the desired fields.

For more information about the fields on this page see *Update Network Entity data configuration elements*.

6. Once you have finished updating the desired fields, click the **Update** button.
   An information message appears letting you know if the update was successful.

The Network Entity is updated.

Delete Network Entity data configuration elements

The **EAGLE XG Database** > **Configuration** > **Network Entity Delete** tab allows you to delete a Network Entity's routing information in the database. The related blacklist entry may be deleted as well. This table describes the fields on the page.

Table 7: Delete Network Entity Database Configuration Elements

Element	Description	Data Input Notes
Network Entity	Numeric identifier for the Network Entity	Format: Digits only Range: 1 - 15 digits
Delete Blacklist Entry	Delete the corresponding blacklist entry (if it exists)	Format: Selection box Range: Selected, unselected Default: Unselected

Deleting a Network Entity database configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **Network Entity**.
   The **EAGLE XG Database** > **Configuration** > **Network Entity** page appears.
2. Click the **Delete** tab.
   The **Delete** tab appears.
3. Enter the Network Entity you want to delete in the **Network Entity** field.
4. Click to check mark **Delete Blacklist Entry** to delete the blacklist entry associated with this Network Entity.
5. Click the **Delete** button.
   A pop up window appears.
6. Perform one of the following actions:
   - Click **OK** to delete the Network Entity.
   - Click **Cancel** to cancel the delete.

The Network Entity is deleted from the database.The associated blacklist entry is deleted if the selection box is check marked (and if this Network Entity address is not part of a range manually entered into the blacklist table). Any DNs or IMSIs associated with this Network Entity are not deleted, but their association with the Network Entity is removed.

DN database configuration

The **EAGLE XG Database** > **Configuration** > **DN** page allows you to view and modify DN database entries.

With this page you can:

- Retrieve: look up DN entires in the database and see what IMSI and Network Entity information is associated with the DN
- Add: add up to eight new DNs to the database and associate a Network Entity
- Update: update the Network Entity or IMSI information for a DN database entry
- Delete: delete an existing DN database entry

Add DN data configuration elements

The **EAGLE XG Database** > **Configuration** > **DN Add** tab allows you to add DNs to the database and associate them with a Network Entity. When adding DNs, you can choose to keep or change the DNs existing IMSI. If you choose to change the IMSI data with this page, then the IMSI you input will be associated with all of the DNs enter on this page. This table describes the fields on the page.

Table 8: Add DN Data Configuration Elements

Element	Description	Data Input Notes
DNs	Mobile Subscriber ISDN (MSISDN) Numbers	Format: Digits only Range: 8 - 15 digits
Network Entity	Numeric identifier for the Network Entity providing service for this mobile subscriber	Format: Digits only Range: 1 - 15 digits
Force	Overwrite DNs if they already exist	Format: Pulldown menu Range: Yes, No Default: No

Adding DN configuration data

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **DN**.
   The **EAGLE XG Database** > **Configuration** > **DN** page appears.
2. Click the **Add** tab.
   The **Add** tab appears.
3. Enter the DN(s) you want to add to the database in the **DN** field(s).
   You can enter up to eight DNs and all DNs entered are associated with the Network Entity entered in the **Network Entity** field.
4. Enter the Network Entity to associate with the DN(s) in the **Network Entity** field.
5. Select **Yes** or **No** from the **Force** pulldown menu.

Selecting **Yes** overwrites any existing DN information in the database. If you are sure you want the DNs entered on this page to only be associated with the given Network Entity, you should select **Yes**. The default option is **No**.

6. Click the **Add** button.

The DNs are added to the database and are associated with the Network Entity.

Retrieve DN data configuration elements

The **EAGLE XG Database** > **Configuration** > **DN Retrieve** tab allows you to look up a DN and retrieve information about it from the subscriber database. This table describes the fields on the page.

Table 9: Retrieve DN Data Configuration Tab

Element	Description	Data Input Notes
DN	Mobile Subscriber Integrated Services Digital Network (MSISDN) Number	Format: Digits only Range: 8 - 15 digits

When you enter a valid DN value and click the Retrieve tab, the page populates with a table containing the DN's current database values. This table describes the fields on this page.

Table 10: Retrieve DN Data Configuration Elements

Element	Description
DNs	Mobile Subscriber International Subscriber Directory Number
Network Entity	Numeric identifier for the Network Entity providing service for this mobile subscriber
IMSI	International Mobile Subscriber Identity for this mobile subscriber

Retrieving a DN database configuration

You can only perform this task when logged into an NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **DN**.
   The **EAGLE XG Database** > **Configuration** > **DN** page appears.
2. Enter the DN you want to view the database information for in the **DN** field.
3. Click the **Retrieve** button.

The DN database record is shown on the page.

Update DN data configuration elements

The **EAGLE XG Database** > **Configuration** > **DN Update** tab allows you to update the Network Entity or IMSI in the subscriber database for the specified DN. This table describes the fields on the page.

Table 11: Update DN Data Configuration Elements

Element	Description	Data Input Notes
DN	Mobile Subscriber ISDN (MSISDN) Number	Format: Digits only Range: 8 - 15 digits
Network Entity	Numeric identifier for the Network Entity providing service for this mobile subscriber	Format: Digits only Range: 1 - 15 digits
IMSI	International Mobile Subscriber Identity for this mobile subscriber	Format: Digits only Range: 10 - 15 digits

Updating a DN database configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **DN**.
   The **EAGLE XG Database** > **Configuration** > **DN** page appears.
2. Click the **Update** tab.
   The **Update** tab appears.
3. Enter the DN you want to update in the **DN** field.
4. Enter the values associated with the DN you want to change:
   - To change the DN's Network Entity, enter a new Network Entity in the **Network Entity** field.
   - To change the DN's IMSI, enter a new IMSI in the **IMSI** field.
   - To change both the Network Entity and the IMSI, then fill out both value fields.

   If either field is left blank, the Network Entity and/or IMSI currently associated with the DN in the database do not change.
5. Click the **Update** button.

The DN database entry is updated with the values entered on this page.

Deleting a DN database configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **DN**.
   The **EAGLE XG Database** > **Configuration** > **DN** page appears.
2. Click the **Delete** tab.
   The **Delete** tab appears.
3. Enter the DN you want to delete in the **DN** field.
4. Click the **Delete** button.
   A pop up window appears.
5. Perform one of the following actions:
   - Click **OK** to delete the DN.
   - Click **Cancel** to cancel the delete.

The DN is deleted.

IMSI database configuration

The HLR application maintains a subscriber database that associates IMSIs (International Mobile Subscriber Identities) with DNs and Network Entities. The bulk of information in the database is provisioned through a PDBI interface, but the application GUI allows you to view database entires and make adjustments as necessary.

The **EAGLE XG Database** > **Configuration** > **IMSI** page allows you to view and modify IMSI database entries. With this page you can:

- Retrieve: look up IMSI entires in the database and see what DN and Network Entity information is associated with the IMSI
- Add: add a new IMSI entry to the database with an associated Network Entity, and associate up to eight DNs
- Update: update the Network Entity for the IMSI database entry
- Delete: delete an existing IMSI database entry

Add IMSI data configuration elements

The **EAGLE XG Database** > **Configuration** > **IMSI Add** tab allows you to add an IMSI to the subscriber database. While adding the IMSI you can also choose to associate DNs with it, or overwrite and existing DN information for the IMSI in the database. This table describes the fields on the page.

Table 12: Add IMSI Data Configuration Elements

Element	Description	Data Input Notes
IMSI	International Mobile Subscriber Identity for this mobile subscriber	Format: Digits only Range: 10 - 15 digits
Network Entity	Numeric identifier for the Network Entity for this mobile subscriber	An entity that provides a type of network service. This is typically the HLR.
DNs	Dialed number(s) for this mobile subscriber associated with this IMSI	Format: Digits only Range: optional; 8 - 15 digits
Force	Overwrite existing IMSI-Network Entity-DN relationships	Format: Pulldown menu Range: Yes, No Default: No

Adding IMSI configuration data

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **IMSI**.
   The **EAGLE XG Database** > **Configuration** > **IMSI** page appears.

2. Click the **Add** tab.
   The **Add** tab appears.
3. Enter the IMSI you want to add in the**IMSI** field.
4. Enter the Network Entity to associate with the IMSI in the **Network Entity** field.
5. Enter up to eight DNs you want to associate with the IMSI in the **DNs** fields.
   This is optional. If you do not want to associate any DNs with the IMSI just leave these fields blank.
6. Select **Yes** or **No** from the **Force** pulldown menu.
   Selecting **Yes** overwrites any existing IMSI information for this IMSI in the database. If you are sure you want the IMSI entered on this page to only be associated with the given Network Entity, you should select **Yes**. The default option is **No**.
7. Click the **Add** button.

The IMSI is added to the database.

Retrieve IMSI data configuration elements

The **EAGLE XG Database** > **Configuration** > **IMSI Retrieve** tab allows you to look up information about the specified IMSI in the subscriber database. This table describes the fields on the page.

Table 13: IMSI Data Configuration Retrieve Tab

Element	Description	Data Input Notes
IMSI	International Mobile Subscriber Identity	Format: Digits only Range: 10 - 15 digits

When you enter a valid IMSI value and click the Retrieve tab, the page populates with a table containing the IMSI's current database values. This table describes the fields on this page.

Table 14: Retieve IMSI Configuration Elements

Element	Description
IMSI	International Mobile Subscriber Identity for this mobile subscriber
Network Entity	Numeric identifier for the Network Entity for this mobile subscriber
DNs	Dialed number(s) for this mobile subscribers associated with this IMSI

Retrieving an IMSI database configuration

You can only perform this task when logged into an NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **IMSI**.
   The **EAGLE XG Database** > **Configuration** > **IMSI** page appears.
2. Enter the IMSI you want to retrieve in the **IMSI** field.

3. Click the **Retrieve** button.

The IMSI record is shown on the page.

Update IMSI data configuration elements

The **EAGLE XG Database** > **Configuration** > **IMSI Update** tab allows you to update the Network Entity in the subscriber database for the specified IMSI. This table describes the fields on the page.

Table 15: Update IMSI Data Configuration Elements

Element	Description	Data Input Notes
IMSI	International Mobile Subscriber Identity for this mobile subscriber	Format: Digits only Range: 10 - 15 digits
Network Entity	Numeric identifier for the Network Entity for this mobile subscriber	Format: Digits only Range: 1 - 15 digits

Updating an IMSI database configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **IMSI**.
   The **EAGLE XG Database** > **Configuration** > **IMSI** page appears.
2. Click the **Update** tab.
   The **Update** tab appears.
3. Type the IMSI you want to update in the **IMSI** field.
4. Type the new Network Entity to associate with the IMSI in the **Network Entity** field.
5. Click the **Update** button.

The IMSI database entry is updated.

Deleting an IMSI database configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **IMSI**.
   The **EAGLE XG Database** > **Configuration** > **IMSI** page appears.
2. Click the **Delete** tab.

   The **Delete** tab appears.
3. Enter the IMSI you want to delete from the database in the **IMSI** field.
4. Click the **Delete** button.
   A pop up window appears.
5. Perform one of the following actions:
   - Click **OK** to delete the IMSI.
   - Click **Cancel** to cancel the delete.

The IMSI is deleted.

PDBI database configuration

The Provisioning Database Interface (PDBI) allows one or several independent information systems, supplied and maintained by the network operator, to be used for provisioning databases and for configuring systems. Through the PDBI, client systems may add, delete, change or retrieve information about any IMSI, DN, or Network Entity association. For this application a Network Entity generally refers to an HLR (Home Location Register).

This feature allows mobile network operators to optimize the use of subscriber numbers (IMSIs and DNs) and number ranges by providing a logical link between any DN and any IMSI. This permits subscribers to be easily moved from one HLR to another. It also allows each HLR to be filled to 100 percent capacity by allowing DN/IMSI ranges to be split over different HLRs and individual DNs and IMSIs to be assigned to any HLR. This also eliminates the need to maintain subscriber routing information at every MSC in the network.

The provisioning client application is responsible for establishing the TCP/IP socket connection, creating and sending PDBI requests, receiving and processing PDBI responses, and detecting and handling socket errors.

The **EAGLE XG Database** > **Configuration** > **PDBI** menu options allow you to configure PDBI Options, allow and configure PDBI connections, set PDBI blacklist ranges, and to schedule PDBI exports.

PDBI database configuration options

The **EAGLE XG Database** > **Configuration** > **PDBI** > **Options** page allows you to configure the PDBI mechanized interface options. These options control how PDBI connections and data are managed from the application GUI.

PDBI connections options

Connections between the application and the PDBI client are set up using the **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections** page. For more information about these connections, refer to *PDBI database connections configuration*. The **EAGLE XG Database** > **Configuration** > **PDBI** > **Options** page allows you to manage configuration options for these connections. Through this page you can configure:

- whether to allow connections and the maximum number of connections allowed
- number of seconds of inactivity allowed before a connection is timed out
- whether to log PDBI messages
- number of seconds allowed between a transaction being committed and becoming durable and the course of action to take if this time limit is exceeded
- TCP and SSL listening ports
- maximum number of Ks for the response message size
- maximum number of commands allowed per transaction
- an IMSI and/or DN prefix, if desired

PDBI import options

The status of PDBI imports can be viewed using the **EAGLE XG Database** > **Maintenance** > **PDBI** > **Import Status** page. For more information about PDBI imports, refer to *PDBI import status maintenance*. PDBI imports are configured through the **EAGLE XG Database** > **Configuration** > **PDBI** > **Options** page. Through this page you can configure:

- whether PDBI imports are enabled
- remote host information, including the IP address, username, password, and import directory name
- whether the import mode is blocking or non-blocking

PDBI export options

PDBI exports are scheduled through the **EAGLE XG Database** > **Configuration** > **PDBI** > **Export Status** page and the export status can be viewed through the **EAGLE XG Database** > **Maintenance** > **PDBI** > **Export Status** page. For more information about PDBI exports, refer to *PDBI export configuration* or *PDBI export status maintenance*. The **EAGLE XG Database** > **Configuration** > **PDBI** > **Options** page allows you to configure:

- whether or not exports are allowed to be copied from this server to the remote host
- remote host information, including the IP address, username, password, and export directory name

PDBI configuration options elements

The **EAGLE XG Database** > **Configuration** > **PDBI** > **Options** page allows you to configure the options used for PDBI connections, imports, and exports. This table describes the fields on this page.

Table 16: PDBI Options Elements

Element	Description	Data Input Notes
Display PDBI Output	If checked, the PDBI commands and responses will be displayed on the GUI when provisioning data	Format: Selection box Default: Unchecked
TCP Listening Port	Port number for the unsecure listening port. This port can be disabled by setting the value to 0. **Note:** Changes to the TCP Listening port do not take effect until the client process is restarted.	Format: Digits only; port number Range: 0 - 65635 Default: 5873
TLS Listening port	TLS (unsecure) Listening Port. The TLS Listening port can be disabled by setting it to 0. **Note:** Changes the TLS listening port do not take effect until the client process is restarted.	Format: Digits only; port number Range: 0 - 65635 Default: 5874

Element	Description	Data Input Notes
Allow Connections	If checked incoming connections are allowed.	Format: Check box Range: Selected, deselected Default: Selected
Max Connections	If connections are allowed, use this to set the maximum number of connections that can occur at the same time.	Format: Digits only Range: 1 - 128 Default: 16
Connection Init Timeout	The number of seconds allowed to pass between the establishment of a network connection and a connection message being received without causing a timeout.	Format: Digits only; seconds Range: 0 - 60 Default: 5
Message Receive Timeout	The maximum number of seconds a client may take to send a PDBI request message terminated by a • NUL (NULL, 0x00) • CR (Carriage Return, 0x0d) • LF (Line Feed, 0x0a) • CR followed by LF (CR+LF, 0x0d 0x0a) control character. If the **Message Receive Timer** expires, the characters received will be considered complete for the incoming message and processed. Setting the **Message Receive Timeout** to zero disables the processing of incorrectly terminated messages.	Format: Digits only; seconds Range: 0 - 59 Default: 0 (disabled)
Max Response Message Size	Maximum number of Kilobytes for a response message.	Format: Digits only; Kilo bytes Range: 1 - 132 Default: 4
Max Transaction Size	Maximum number of database manipulation commands per transaction.	Format: Digits only Range: 10 - 1000 Default: 200

Element	Description	Data Input Notes
IMSI Prefix	International Mobile Subscriber Identity. The IMSI Prefix is automatically pre-appended to the IMSI of incoming PDBI requests and removed in outgoing PDBI responses.	Format: Digits only Range: 10 - 15 digits
DN Prefix	Mobile Subscriber International Subscriber Directory Number. The DN Prefix is automatically pre-appended to the DN(s) of incoming PDBI requests and removed in outgoing PDBI responses.	Format: Digits only Range: 8 - 15 digits
Asynchronous Database Report Frequency	Number of seconds between each asynchronous Database Report (dbrpt) message sent to the client.	Format: Digits only; seconds Range: 1 - 86400 Default: 10
Database Report Percentage	Percentage of MP servers that meet or exceed the reported level	Format: Digits only; percentage Range: 1 - 100 Default: 100
Log PDBI Messages	If checked all incoming and outgoing PDBI messages will be logged.	Format: Selection box Range: Selected, Deselected Default: Selected
Transaction Durability Timeout	Number of seconds allowed between a transaction being committed and it becoming durable.	Format: Digits only; seconds Range: 2 - 3600 Default: 5
Remote Import Enabled	If checked PDBI files can be imported.	Format: Selection box Range: Selected, Deselected Default: Deselected
Remote Import Mode	If set to Non-Blocking, updates are allowed on all PDBI connections while the remote import operation is in progress. If set to Blocking, updates are not allowed.	Format: Pulldown menu Range:Non-Blocking, Blocking Default: Non-Blocking
Remote Import Host IP Address	IP Address queried for PDBI import files.	Format: Alphanumeric Range: 0 - 39 characters

Element	Description	Data Input Notes
Remote Import User	Username for remote import host user.	Format: Alphanumeric Range: 0 - 255 characters
Remote Import Password	Password to exchange ssh keys with the remote import host. The password is cleared from this table once the keys have been exchanged.	Format: Alphanumeric Range: 0 -255 characters
Remote Import Directory	Remote import host directory where the PDBI import files are stored.	Format: Alphanumeric Range: 0 -255 characters
Export Mode	If set to Non-Blocking, updates are allowed on all PDBI connections while the remote export operation is in progress. If set to Blocking, updates are not allowed.	Format: Pulldown menu Range:Non-Blocking, Blocking Default: Non-Blocking
Remote Export Transfers Enabled	If checked PDBI export files can be copied to the remote export host.	Format: Selection box Range: Selected, Deselected Default: Deselected
Remote Export Host IP Address	IP address that PDBI export files may be sent to.	Format: Alphanumeric Range: 0 - 39 characters
Remote Export User	Username for remote export host user.	Format: Alphanumeric Range: 0 - 255 characters
Remote Export Password	Password to exchange ssh keys with the remote export host. The password is cleared from this table once the keys have been exchanged.	Format: Alphanumeric Range: 0 - 255 characters
Remote Export Directory	If PDBI export is configured, the location on the remote export directory the PDBI export files are sent to.	Format: Alphanumeric Range: 0 - 255 characters

Changing PDBI options

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Options**.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Options** page appears.
2. Modify the PDBI options you want to change by entering information in the appropriate fields.
   For a detailed explanation about the PDBI options and valid input for these fields, see *PDBI configuration options elements*.

3. Click the **Apply** button.
   A successful update message appears.

The PDBI configuration options modifications are made.

PDBI database connections configuration

The **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections** page allows you to manage the configuration for servers permitted to establish a connection to the local database. Only the specified servers will be allowed to connect to the NOAM remotely and to execute PDBI commands.

HLR Router allows up to 128 simultaneous PDBI connections and supports secure and unsecured connections. While the application is capable of supporting 128 connections, the maximum number of connections allowed can be limited using the **EAGLE XG Database** > **Configuration** > **PDBI** > **Options** page. For more information about connection, see *PDBI database configuration options*.

With this **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections** page you can:

- View the list of allowed servers and each servers permissions
- Configure the HLR to allow connection requests from remote servers
- Modify the System ID, IP address, or permissions for listed servers
- Delete servers from the connections list

Multiple session connections

PDBI supports multiple simultaneous client connections and read transactions, but only one client can open a write transaction at a time. Requests are answered in the order they are received. If more than one authorized system requests a write transaction the first system to submit a write request is granted access.

If a second system submits a write request while the first transaction is still open, it will either be immediately rejected or queued for a specified time out period to wait on the first client's write transaction to complete. The time out period can be specified in the write transaction request, and can be any value from 0 to 3600 seconds. If the value is not included or is set to 0, the second write request will be immediately rejected. If the time out value is set to any non-zero value, the second request will be held for that time period before being rejected. If the first user releases the write transaction before the second user's time out period has expired, the second user will then be granted write access.

If a third user submits a write request after the second user with a specified time out period, the third user's request will be queued behind the second user's request. Once the first user releases the transaction, the second user is granted access. After the second user releases the transaction, the third user is granted access and so forth. If any user's time out period expires the request will be immediately rejected. If the third user sets a time out period longer than the second user, and the second user's time out period expires before the first user releases the transaction, the second user's request will be dropped from the queue and the third user will move up in the queue. If the first user then releases the transaction before the third user's time out has expired; the third user will be granted access.

The application interface operates as clients and provisioning for both is locked if there is an active write connection from another client.

PDBI connections configuration elements

The **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections** page allows you to view, edit, and delete existing PDBI connections and to add new PDBI connections. This table describes the fields on the page.

Table 17: PDBI Connections Configuration Elements

Element	Description
Action	The action that can be performed to the existing PDBI connections. Actions include: • Edit • Delete
System ID	Identifying text for this system
IP Address	The IP address (either an IPv4 or IPv6 address) of the client that will connect to the PDBA
Permission	Database permission group for this client

Insert or Edit PDBI connections configuration elements

The **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections [Insert]** page allows you to add new PDBI connections and the **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections [Edit]** page allows you to edit existing PDBI connections. This table describes the fields on the **Insert** and **Edit** pages.

Table 18: Insert or Edit PDBI Connections Configuration Elements

Element	Description	Data Input Notes
System ID	Identifying text for this system	Format: Alphanumeric Range: 1 - 32 characters
IP Address	The IP address (either an IPv4 or IPv6 address) of the client that will connect to the PDBA	Format: Valid IP
Permissions	Database permission group for this client	Format: Pulldown menu Range: Read Only, Read Write

Inserting PDBI connections

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections**.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections** page appears.
2. Click on **Insert** located below the table.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections [Insert]** page appears.
3. Enter the System ID in the **System ID** field.
   This is a 1 - 8 character identifier for the connection.
4. Enter the IP address for the connection in the **IP Address** field.
   This must match the IP address for the client.
5. Select the permissions level for the connection from the **Permissions** pulldown menu.

- Select **READ_ONLY** to grant read only access for the client with this connection. This is the default.
- Select **READ_WRITE** to grant read and write access for the client with this connection.

6. Perform one of the following:
   - Click **OK** to save the PDBI connection and exit this page.
   - Click **Apply** to save the PDBI connection and remain on this page.

PDBI client connection requests are now allowed for the configured PDBI connection.

Viewing PDBI connections

You can only perform this task when logged into an NOAM.

Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections**.
The **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections** page appears.

The currently allowed PDBI connections are listed in the table.

Filtering using the Display Filter

Use this procedure to perform a filtering operation. This procedure assumes that you have a data table displayed on your page. This process is the same for all data tables. However, all filtering operations are not available for all tables.

1. Select a field name from the **Display Filter** pulldown menu.

   This selection specifies the field in the table that you want to filter on. The default is **None**, which indicates that you want all available data displayed.

   The selected field name displays in the **Display Filter** field.

2. Select an operator from the operation selector pulldown menu.

   The selected operator appears in the field.

3. Enter a value in the value field.

   This value specifies the data that you want to filter on. For example, if you specify **Filter=Severity** with the equals (**=**) operator and a value of MINOR, the table would show only records where Severity=MINOR.

4. Click **Go** to filter on the selection, or click **Reset** to clear the selection.

Records are displayed according to the specified criteria.

Editing PDBI connections

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections**.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections**page appears.
2. Locate the PDBI connection you want to edit and click the corresponding **Edit** action.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections [Edit]** page appears.
3. Edit the System ID, IP Address, and/or Permission for the connection.

   For more information about these fields, see *Insert or Edit PDBI connections configuration elements*.

4. Perform one of the following:
   - Click **OK** to save the changes to the PDBI connection and exit this page.
   - Click **Apply** to save the changes to the PDBI connection and remain on this page.

The PDBI connection is changed.

Deleting PDBI connections

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections**.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Connections** page appears.
2. Locate the PDBI connection you want to delete and click the corresponding **Delete** action.
   A pop up window appears.
3. Perform one of the following actions:
   - Click **OK** to delete the PDBI connection.
   - Click **Cancel** to cancel the delete.

The PDBI connection is deleted.

PDBI blacklist database configuration

E.164 addresses of all HLRs can be reserved by using the **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist** page. This page allows you to configure number ranges reserved for HLRs that cannot be used for IMSIs or DNs. Any attempt to create a DN or an IMSI that uses a number that falls within a blacklist will be rejected.

Blacklist entries only impacts future PDBI data from the moment of the blacklist entry creation; any existing DNs or IMSIs that fall within the blacklist range are not impacted.

PDBI blacklist configuration elements

The **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist** page allows you to view, delete, and edit existing PDBI blacklist ranges and insert new PDBI blacklist ranges. This table describes the fields on the page.

Table 19: PDBI Blacklist Configuration Elements

Element	Description
Action	The actions that can be performed on the existing address range. Actions include: • Edit • Delete
Start of Range	Start of a range of addresses reserved for HLRs
End of Range	End of a range of addresses reserved for HLRs

Insert or Edit PDBI blacklist configuration elements

The **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist [Insert]** page allows you to add new PDBI blacklist ranges and the **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist [Edit]** page allows you to edit existing PDBI blacklist ranges. This table describes the fields on the Insert and Edit pages.

Table 20: PDBI Blacklist Insert or Edit Configuration elements

Element	Description	Data Input Notes
Start of Range	Start of a range of addresses reserved for HLRs	Format: Digits only Range: 8 - 15 digits
End of Range	End of a range of addresses reserved for HLRs	Format: Digits only Range: 8 - 15 digits

Inserting PDBI blacklist

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist**.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist** page appears.
2. Click on **Insert** located below the table.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist [Insert]** page appears.
3. Enter the lowest number of the reserved number range in the **Start of Range** field.
4. Enter the highest number of the reserved range in the **End of Range** field.
5. Perform one of the following:
   - Click **OK** to save the PDBI blacklist and exit this page.
   - Click **Apply** to save the PDBI blacklist and remain on this page.

The PDBI blacklist is created and the numbers within the range are reserved and can only be used for the HLR Router.

Viewing PDBI blacklist

You can only perform this task when logged into an NOAM.

Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist**.
The **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist** page appears.

The currently configured PDBI blacklists are listed in the table. For information about how to filter this information, see *Filtering using the Display Filter*.

Editing PDBI blacklist

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist**.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist** page appears.
2. Locate the PDBI blacklist you want to edit and click the corresponding **Edit** action.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist [Edit]** page appears.
3. Change either the start or the end of the range by entering a new number in the appropriate **Range** field.
4. Perform one of the following:
   - Click **OK** to save the PDBI blacklist changes and exit this page.
   - Click **Apply** to save the PDBI blacklist changes and remain on this page.

The PDBI blacklist range is changed and a new range of numbers is reserved.

Deleting PDBI blacklist

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist**.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Blacklist** page appears.
2. Locate the range you want to delete and click the corresponding **Delete** action.
   A pop up window appears.
3. Perform one of the following actions:
   - Click **OK** to delete the PDBI blacklist.
   - Click **Cancel** to cancel the delete.

The PDBI blacklist is deleted.

PDBI export configuration

The **EAGLE XG Database** > **Configuration** > **PDBI** > **Export** page allows you to schedule exports of files containing Network Entity, DN, or IMSI data from the local subscriber database. Each type of data can be exported individually, or DN, IMSI, and Network Entity data can all be exported in a single file.

Data is exported to an ASCII text file in either PDBI or CSV format. The export can be initiated immediately or scheduled to occur daily, weekly, monthly, or yearly. Data can only be scheduled to be exported a maximum of once a day, seven days a week.

The export file is stored locally on the NOAM in the file management storage area unless the option to automatically transfer files to a remote server is set up. For more information about setting up this option, see *PDBI database configuration options*.

Export operation status is viewable up to seven days unless it is manually removed.

PDBI export file names

Export files are stored locally on the NOAM in the file management storage area using the naming convention:

```
export_<id>.<datatype>.<yyyymmdd><hhmm>.<format>
```

So, a PDBI export file name might look like:

```
export_datafeednotesfortesting.dn.200908152058.pdbi
```

This table describes the variables that make up a file name.

Table 21: PDBI Export File Names

Variable	Description
<id>	A string of 1 - 100 characters that identifies the file. This value is user configured.
<datatype>	Provisioning data type exported (Scheduled exports only). Possible values: • all: All data types

Variable	Description
	• ne: Network Entities • imsi: IMSIs • dn: DNs
<yyyymmdd>	Date the export was started (Scheduled exports only). Values: • yyyy: 1970+ (year) • mm: 01-12 (month) • dd 01-31 (day of month)
<hhmm>	Time the export was started (Scheduled exports only). Values: • hh: 00-23 (hours) • mm: 00-59 (minutes)
<format>	Export file format. Values: • pdbi: (PDBI format) • csv: (comma-separated values format)

PDBI export configuration elements

The **EAGLE XG Database** > **Configuration** > **PDBI** > **Export** page allows you to view, edit, and delete currently schedule PDBI data exports and to schedule new PDBI data exports. This table describes the fields on the page.

Table 22: PDBI Export Configuration Elements

Element	Description
Action	Actions that can be performed on an existing scheduled PDBI export. Actions include: • Edit • Delete
Identifier	Identifying string for this scheduled report
File Format	Format of the export file (PDBI or CSV)
Delimiter	Field delimiter used in the export file (applies to CSV file format only)
Export Data	Type of data to export
First Export	The initial date on which the export should run
Next Export	The initial time at which this export should run
Repeat	How often this export should be repeated
Comment	Optional text that may be used to describe the purpose of this report

Insert or Edit PDBI export configuration elements

The **EAGLE XG Database** > **Configuration** > **PDBI** > **Export [Insert]** page allows you to schedule new PDBI exports and the **EAGLE XG Database** > **Configuration** > **PDBI** > **Export [Edit]** page allows you to edit already scheduled PDBI exports. This table describes the fields on the **Insert** and **Edit** pages.

Table 23: Insert or Edit PDBI Export Configuration Elements

Elements	Description	Data Input Notes
Identifier	Identifying string for this scheduled report	Format: Alphanumeric Range: 4 - 12 characters
File Format	Format of the export file (PDBI or CSV)	Range: csv, pdbi Default: csv
Delimiter	Field delimiter used in the export file (applies to CSV file format only)	Format: Pulldown menu Range: Comma, Pipe, Colon, Semicolon, Space Default: Comma
Export Data	Type of data to export	Format: Pulldown menu Range: All, DN, IMSI, Network Entity Default: All
Date	The initial date on which the export should run	Format: Pulldown menus Range: • Valid months • Valid days: The range of available days is dependant upon the month selected • Next two years Default: Current date
Time	The initial time at which this export should run	Format: Pulldown menus Values include: • Hours in 24 hour format • Minutes in five minute increments, starting with 00 and ending with 55 Default: Five minutes after the page is initially displayed

Elements	Description	Data Input Notes
Repeat	How often this export should be repeated	Range: none, daily, weekly, monthly Default: none
Comment	Optional text that may be used to describe the purpose of this report	Format: Alphanumeric Range: 0 - 255 characters

Inserting PDBI export configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Export**.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Export** page appears.
2. Click on**Insert** located below the table.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Export [Insert]** page appears.
3. Enter a name for the export in the **Identifier** field.
4. Select one of the **File Formats**:
   - **csv**: to export a CSV file. This is the default value.
   - **pdbi**: to export a file in PDBI format.
5. Select the type of value separator to be used in the export file from the **Delimiter** pulldown menu.
   This option is only available for CSV files. The default value is a comma.
6. Select the type(s) of data to include in the export file from the **Export Data** pulldown menu.
   The default value is **All**.
7. Select the month, day, and year you initially want the report to run from the **Date** pulldown menus.
   The default is the current day.
8. Select the time you initially want the report to run from the **Time** pulldown menu.
   The default value is the time the **Insert** button was clicked rounded up to the next five minute interval.
9. Select how often you would like to repeat this export from the **Repeat** options.
10. If desired, add a comment in the **Comment** field.
    The comment provides context for someone viewing the **EAGLE XG Database** > **Configuration** > **PDBI** > **Export** page. It is not included in the export file.
11. Perform one of the following:
    - Click **OK** to save the PDBI export and exit this page.
    - Click **Apply** to save the PDBI export and remain on this page.

The PDBI export is scheduled and should run at the set date and time.

Viewing PDBI export configuration

You can only perform this task when logged into an NOAM.

Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Export**.

The **EAGLE XG Database** > **Configuration** > **PDBI** > **Export** page appears.

The currently configured PDBI exports are listed in the table. For information about how to filter this information, see *Filtering using the Display Filter*.

Editing PDBI export configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Export**.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Export** page appears.
2. Locate the PDBI export you want to edit and click the corresponding **Edit** action.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Export [Edit]**page appears.
3. Change the desired fields.
   For more information about these fields, see *Insert or Edit PDBI export configuration elements*.
4. Perform one of the following:
   - Click **OK** to save the changes to the PDBI export and exit this page.
   - Click **Apply** to save the changes to the PDBI export and remain on this page.

The PDBI export is changed and should run of the specified date and time.

Deleting PDBI export configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **EAGLE XG Database** > **Configuration** > **PDBI** > **Export**.
   The **EAGLE XG Database** > **Configuration** > **PDBI** > **Export** page appears.
2. Locate the scheduled export you want to delete and click the corresponding **Delete** action.
   A pop up window appears.
3. Perform one of the following actions:
   - Click **OK** to delete the PDBI export.
   - Click **Cancel** to cancel the delete.

The PDBI export is deleted.

Maintenance

The **EAGLE XG Database** > **Maintenance** menu options allow you to view data and perform tasks related to subscriber database maintenance. The available menu options vary depending on the type of server you are logged into.

When you are logged into an NOAM you can perform database audits; query the database for specified DN, IMSI, or Network Entity ranges; run PDBI commands from the GUI; view PDBI connections, command logs, and the status of imports and exports; and configure and manage NPA Splits.

When you are logged into an SOAM you can only query the database for information relating to a specified DN, Network Entity, and IMSI ranges.

The available database menu options will vary based on the type of server you are logged into and the permissions assigned to your group. If you do not see a menu option you need, please make sure

you are logged into the appropriate type of server and ask your administrator to make sure the group your user ID belongs to has the appropriate permissions.

Database query

The **EAGLE XG Database** > **Maintenance** > **Query** menu optinos allow you to query database information for a single PDBI database entry, or for a range of the same type of PDBI database entries, on an available server. For example, you can query a specified server for information about a range of DNs.

Querying a server for PDBI data allows you to see if data is being replicated correctly to each server, and allows you to see if adjustments to data management or to the subscriber database need to be made.

Network entity database query

The **EAGLE XG Database** > **Maintenance** > **Query** > **Network Entity** page allows you to query database information for a single Network Entity, or a range of Network Entities, on an available server.

Network entity query elements

Use the **EAGLE XG Database** > **Maintenance** > > **Network Entity > > Query >** page to set elements for a Network Entity Query. This table describes fields on this page.

Table 24: Network Entity Query Elements

Element	Description	Data Input Notes
Start of Range	Lowest number in the range for the type of data you want to audit. If the **End of Range** field is left blank, then only the value entered into the **Start of Range** field will be queried.	Format: Digits only Range: 1 - 15 digits
End of Range	Highest number in the range for the type of data you want to audit. This field is optional.	Format: Digits only Range: blank, 1 - 15 digits Default: blank
Hostname	Hostname of the server the query is run on. The pulldown menu lists the possible servers.	Format: Pulldown menu Range: Available servers Default: Servers are listed in alphabetical order

Running a Network Entity query

1. Select **EAGLE XG Database** > **Maintenance** > **Query** > **Network Entity**.
   The **EAGLE XG Database** > **Maintenance** > **Query** > **Network Entity** page appears.
2. Enter the lowest number in the Network Entity range in the **Start of Range** field.

3. Enter the highest number in the Network Entity range in the **Start of Range** field.
4. Select the hostname you want to run the Query on from the **Hostname** pulldown menu.
5. Click **Query**.

The query is run and any relevant Network Entity data is displayed on the page.

DN database query

The **EAGLE XG Database** > **Maintenance** > **Query** > **DN** page allows you to query database information for a single DN, or a range of DNs, on an available server.

DN query elements

Use the **EAGLE XG Database** > **Maintenance** > **Query** > **DN** page to set elements for a DN Query. This table describes fields on this page.

Table 25: DN Database Query Elements

Element	Description	Data Input Notes
Start of Range	Lowest number in the range for the type of data you want to audit. If the **End of Range** field is left blank, then only the value entered into the **Start of Range** field will be queried.	Format: Digits only Range: 8 -15 digits
End of Range	Highest number in the range for the type of data you want to audit. This field is optional.	Format: Digits only Range: blank, 8 - 15 digits Default: blank
Hostname	Hostname of the server the query is run on. The pulldown menu lists the possible servers.	Format: Pulldown menu Range: Available servers Default: Servers are listed in alphabetical order

Running a DN query

1. Select **EAGLE XG Database** > **Maintenance** > **Query** > **DN**.
   The **EAGLE XG Database** > **Maintenance** > **Query** > **DN** page appears.
2. Enter the lowest number in the DN range in the **Start of Range** field.
3. Enter the highest number in the DN range in the **Start of Range** field.
4. Select the hostname you want to run the Query on from the **Hostname** pulldown menu.
5. Click **Query**.

The query is run and any relevant DN data is displayed on the page.

IMSI database query

The **EAGLE XG Database** > **Maintenance** > **Query** > **IMSI** page allows you to query database information for a single IMSI, or a range of IMSIs, on an available server.

IMSI query elements

Use the **EAGLE XG Database** > **Maintenance** > **Query** > **IMSI** page to set elements for an IMSI Query. This table describes fields on this page.

Table 26: IMSI Database Query Elements

Element	Description	Data Input Notes
Start of Range	Lowest number in the range for the type of data you want to audit. If the **End of Range** field is left blank, then only the value entered into the **Start of Range** field will be queried.	Format: Digits only Range: 10 - 15 digits
End of Range	Highest number in the range for the type of data you want to audit. This field is optional.	Format: Digits only Range: blank, 10 - 15 digits Default: blank
Hostname	Hostname of the server the query is run on. The pulldown menu lists the possible servers.	Format: Pulldown menu Range: Available servers Default: Servers are listed in alphabetical order

Running an IMSI query

1. Select **EAGLE XG Database** > **Maintenance** > **Query** > **IMSI**.
   The **EAGLE XG Database** > **Maintenance** > **Query** > **IMSI** page appears.
2. Enter the lowest number in the IMSI range in the **Start of Range** field.
3. Enter the highest number in the IMSI range in the **Start of Range** field.
4. Select the hostname you want to run the Query on from the **Hostname** pulldown menu.
5. Click **Query**.

The query is run and any relevant IMSI data is displayed on the page.

PDBI maintenance

The **EAGLE XG Database** > **Maintenance** > **PDBI** menu options provide maintenance information related to PDBI connections and data. With this page you can monitor PDBI connections; view every PDBI message exchanged between provisioning systems in the command log, view the status of imports and exports; open import and export files and import result logs; compare (or audit) provisioning on the HLR Router and the EPAP-based G-flex systems; and run PDBI commands from the GUI.

All PDBI maintenance tasks are only available when logged into an NOAM.

PDBI connections maintenance

The **EAGLE XG Database** > **Maintenance** > **PDBI** > **Connections** page allows you to view external PDBI connections that are currently in use. PDBI connections used by the NOAM GUI are not shown or counted towards the maximum number of connections.

PDBI connections status elements

Use the **EAGLE XG Database** > **Maintenance** > **PDBI** > **Connections** page to view the status of PDBI connections. This table describes fields on this page.

Table 27: PDBI External Connections Status Elements

Field	Definition	Data Notes
Timestamp	Time the connection was established	Format: Year-Month-Day Hour-Minute-Second
CID	Connection ID	N/A
Remote IP	IP address for the remote client	Format: Valid IP address
Remote Port	Port used for the remote client connection	Format: Valid port number
Version	Version of PDBI API this client application is using. This determines the applications ability to successfully communicate with the PDBA	Default: 1.0
Mode	Database transaction mode	Range: • normal: All updates must be sent inside a transaction explicitly begun and ended by begin_txn and end_txn/abort_txn requests respectively. • single: Transactions are implicitly begun and ended for individual update requests Default: normal
Idle Timeout	Number of minutes the connection can be idle before it is automatically terminated by PDBA	Range: • 0 (the connection is never terminated) • 1 - 44640 minutes Default: 0

Field	Definition	Data Notes
Resp Max Size	The maximum size (in K bytes) of responses that the PDBA will send back. This ensures that retrieve requests resulting in a large number of returned instances come back in manageable sized responses.	Range: 1 - 32 Default: 4
Resp End Character	Character that PDBA uses to terminate responses	Range: • null: Terminate responses with a NULL (or \0) character • newline: Terminate responses with a newline (or \n) character Default: null
Async Report	If set to Yes the client is sent asynchronous database report messages	Range: Yes, No Default: No
Async Report Freq	How often (in seconds) to send the client asynchronous database report messages. This overrides the system wide, configurable default database report frequency value for a connection. If Async Report is set to No, then the value in this field is irrelevant.	Range: 1 - 86400 seconds
Async Report %	Percentage to use in the database report. This will override the system wide, configurable default for database report percent value for the specified connection. If Async Report is set to No, then the value in this field is irrelevant.	Range: 1 - 100 percent

Viewing external PDBI connections status

You can only perform this task when logged into an NOAM.

Select **EAGLE XG Database** > **Maintenance** > **PDBI** > **Connections**.
The **EAGLE XG Database** > **Maintenance** > **PDBI** > **Connections** page appears.

The information about external PDBI connections currently in use are shown on the page. For more information about these fields, see *PDBI connections status elements*. For information about how to filter this information, see *Filtering using the Display Filter*.

PDBI command log maintenance

Every PDBI message exchanged between provisioning systems is written to the command log and is stored for up to seven days. The command log on the active server of the primary NOAM contains a complete log of PDBI command activity that has occurred on all NOAM servers. This information is available even after a server switchover.

Each day a command log file is created and automatically exported to a remote FTP server. The **EAGLE XG Database** > **Maintenance** > **PDBI** > **Command Log** page allows you to view the PDBI command log entries through the GUI.

PDBI command log maintenance elements

Use the **EAGLE XG Database** > **Maintenance** > **PDBI** > **Command Log** page to view the PDBI command log. This table describes fields on this page.

Table 28: PDBI Command Log Maintenance Elements

Element	Description
Timestamp	Date and time the PDBI message was logged
System ID	Hostname of the PDBI client. Possible values: • GUI: local system GUI • Import: local system import process • <SystemId>: System identifier for the remote system the provisioning client is running
CID	Client's connection identifier
Text	PDBI command and/or response message

Viewing PDBI maintenance command logs history

You can only perform this task when logged into an NOAM.

Select **EAGLE XG Database** > **Maintenance** > **PDBI** > **Command Log**.
The **EAGLE XG Database** > **Maintenance** > **PDBI** > **Command Log**page appears.

The command history box holds the last 10 commands run during the login session. For information about how to filter this information, see *Filtering using the Display Filter*.

PDBI import status maintenance

Data can be imported from a PDBI import file to add new, or update existing, data in the database. Imports are not scheduled through the user interface but import settings are configured with the PDBI options page. For more information, see *PDBI database configuration options*.

Import files that are placed in a specific location on a remote server are detected within five minutes and automatically downloaded via SSH File Transfer Protocol (SFTP) to the file management storage area on the active server of the Primary NOAM. For a file to be imported it must:

- be properly named following the naming convention. For more information, see the *HLR Administration Manual*.
- have been placed in the remote directory after the time when PDBI import last ran

- must not have been previously imported. A file that has already been imported into the local directory will not be imported again, even if its status is Failed.

  Note: To import a previously Failed file, correct the file as necessary, rename the file, and then place the renamed file in the remote directory.

Once fully downloaded, each file is automatically imported into the Provisioning Database sequentially in the order in which their download completed. The PDBI import file is an ASCII text file that contains a series of database manipulation requests in PDBI format.

The **EAGLE XG Database** > **Maintenance** > **PDBI** > **Import Status** page allows you to view the status of PDBI imports. Import records with a status of Completed or Failed can be deleted from this table.

PDBI import status elements

Use the **EAGLE XG Database** > **Maintenance** > **PDBI** > **Import Status** page to view the status of PDBI imports. This table describes fields on this page.

Table 29: PDBI Import Status Maintenance Elements

Field	Description
Import File	Name of import file
Time Queued	Time the import was queued
Time Started	Time the import started
Time Completed	Time the import completed
Progress	Percentage of import progress
Result Log	Name/heading of result log
Pass Count	The number of successful import commands
Fail Count	The number of unsuccessful import commands
Status	Status of the import

Viewing PDBI import files

You can only perform this task when logged into an NOAM.

Select **EAGLE XG Database** > **Maintenance** > **PDBI** > **Import Status**.
The **EAGLE XG Database** > **Maintenance** > **PDBI** > **Import Status** page appears.

The imports are shown in the table. For information about how to filter this information, see *Filtering using the Display Filter*.

PDBI export status maintenance

Provisioning data can be exported to an ASCII file in either PDBI or CVS format using the application user interface. For more information about how to do PDBI exports see *PDBI export configuration*. The **EAGLE XG Database** > **Maintenance** > **PDBI** > **Export Status** page allows you to view the status, progress, and data count information for scheduled PDBI exports.

PDBI export status elements

Use the **EAGLE XG Database** > **Maintenance** > **PDBI** > **Export Status** page to view the status of PDBI exports. This table describes fields on this page.

Table 30: PDBI Export Status Maintenance Elements

Field	Description
Export File	Name of export file
Time Queued	Time the export was queued
Time Started	Time the export started
Time Completed	Time the export completed
NE Count	Number of Network Entities exported
IMSI Count	Number of IMSIs exported
DN Count	Number of DNs exported
Status	Status of export
Comment	Descriptive text about export. This field is optional, so it may be blank.

Viewing PDBI export status

You can only perform this task when logged into an NOAM.

Select **EAGLE XG Database** > **Maintenance** > **PDBI** > **Export Status**.
The **EAGLE XG Database** > **Maintenance** > **PDBI** > **Export Status** page appears.

The exports are shown in the table. For information about how to filter this information, see *Filtering using the Display Filter*.

PDBI run command maintenance

The **EAGLE XG Database** > **Maintenance** > **PDBI** > **Run Command** page allows you to run PDBI commands from the application GUI. For a full list of available PDBI commands and their descriptions see the Provisioning Database Application (PDBA) and Interface (PDBI) manual.

Note: You can also display the database status using the DB Status menu option. See *DB Status* for more information.

PDBI run command maintenance elements

Use the **EAGLE XG Database** > **Maintenance** > **PDBI** > **Run Command** page to enter a command to be run. This table describes fields on this page.

Table 31: PDBI Run Commands Elements

Element	Description	Data Input Notes
Command input line	Text box for entering PDBI commands. Only valid PDBI commands will run successfully.	Format: alphanumeric Range: up to 256 characters
Command history box	Contains the last ten commands run during the current users login session. Single clicking on any command will populate the Command line input with the selected command. You can also use the up and down keys on your keyboard to cycle through the available commands.	N/A

Viewing PDBI maintenance command logs history

You can only perform this task when logged into an NOAM.

Select **EAGLE XG Database** > **Maintenance** > **PDBI** > **Command Log**.
The **EAGLE XG Database** > **Maintenance** > **PDBI** > **Command Log**page appears.

The command history box holds the last 10 commands run during the login session. For information about how to filter this information, see *Filtering using the Display Filter*.

Running PDBI maintenance run commands

You can only perform this task when logged into an NOAM.

1. Select **EAGLE XG Database** > **Maintenance** > **PDBI** > **Command Log**.
   The **EAGLE XG Database** > **Maintenance** > **PDBI** > **Command Log**page appears.
2. Enter the PDBI command in the **Command** box or select a command from the **Command History** box.

   For a full list of available PDBI commands see the Provisioning Database Application (PDBA) and Interface (PDBI) manual.
3. Click the **Go** button.
   The command is run and the command is added to the command history.

The PDBI command is run. For more information about the resulting response of the command see the Provisioning Database Application (PDBA) and Interface (PDBI) manual. Also, the command is added to the top of the command history list.

DB Status

The **EAGLE XG Database** > **Maintenance** > **PDBI** > **DB Status** page allows you to automatically display PDBI capacity/utilization. This page's output is also exported by PDE in a PDBI status file with the measurements information PDEs so that the IMSI, DN, and NE counts can be collected automatically also.

DB Status elements

Table 32: DB Status Elements

Element	Description
DB Level	The database level.
Birthdate	The time that the database was created in standard date notation.
IMSIs	The number of International Mobile Subscriber Identities configured.
DNs	The number of directory numbers configured.
NEs	The number of network elements configured.

Viewing DB Status

You can only perform this task when logged into an NOAM.

Select **EAGLE XG Database** > **Maintenance** > **PDBI** > **DB Status**.
The **EAGLE XG Database** > **Maintenance** > **PDBI** > **DB Status** page appears.

The page automatically displays database status elements for the PDBI.

NPA splits

The NPA Split feature accommodates a growing number of subscribers and the need for new area codes (new NPA). NPA Split refers to the telephone-numbering scheme that subdivides an old area code (old NPA) by the creation of a new NPA. This is necessary when the number of telephone numbers in an old NPA grows to an excessive number. As new NPAs are defined, some existing exchanges (NXX) may be assigned to the new NPA from the old NPA. This feature allows an NPA split to be scheduled in advance of a Permissive Dialing Period (PDP). The split is in the Pending state until it becomes Active on the Start date of the PDP. While in the Active state, Dialed Numbers (DN) in the split's NXX can use either the old NPA or the new NPA. After the split becomes complete on the End date of the PDP, only the new NPA can be used in a DN.

In order to manage NPA splits through the GUI, you must have group permission access to the **EAGLE XG Database** > **Maintenance** > **NPA Splits** menu item.

NPA splits elements

Use the **EAGLE XG Database** > **Maintenance** > **NPA Splits** page to manage NPA splits. This table describes fields on this page.

Table 33: NPA Splits Elements

Element	Description	Data Input Notes
Old NPA	The old Numbering Plan Area that the DNs will be split from.	Format: Integer Range: 200 - 999, 3-digit number

Element	Description	Data Input Notes
		Default: blank
New NPA	The new Numbering Plan Area that the DNs will be split to.	Format: Integer Range: 200 - 999, 3-digit number Default: blank
NXX	The Central Office (exchange) code. On the **Modify** and **Delete** tabs, an **All** selection box is also available. If this box is check marked (the default) when the **Modify** or **Delete** button is clicked, all NXXs are modified or deleted.	Format: Integer Range: 000 - 999, 3-digit number Default: blank
PDP Start	The start date of the Permissive Dialing Period. Can only be changed if NPA split is Pending. This date cannot be in the past, and must be before the PDP End date. Activation occurs within the first 15 minutes of the PDP Start date. If today's date is entered, activation occurs within 15 minutes of the **Create** or **Modify** button being clicked. This field only appears on the **Create** and **Modify** tabs.	Format: Pulldown menus Range: Valid date Default: blank
PDP End	The end date of the Permissive Dialing Period. This date cannot be in the past, and must be after the PDP Start date. Termination occurs within the first 15 minutes of the PDP End date. The date cannot be changed once the NPA split is complete. This field only appears on the **Create** and **Modify** tabs.	Format: Pulldown menus Range: Valid date Default: blank

Viewing NPA splits

You can only perform this task when logged into an NOAM.

From the View Tab, all NPA Split information can be displayed. Each field can be used as a filter option when viewing NPA splits.

If you click **View** while all three fields are empty, the GUI displays all NPA splits found in the PDB database. If the **Save Results** checkbox is check marked, the results are also saved to a CSV file named NpaSplitReport.guiadmin.<timestamp>.csv. This file can then be viewed and downloaded in the HLR file management area (The **Network Element Name** field on the **Status & Manage** > **Network Elements** page).

1. Select **EAGLE XG Database** > **Maintenance** > **NPA Splits**.
   The **EAGLE XG Database** > **Maintenance** > **NPA Splits** page appears, with the **View** tab displayed.
2. Add search criteria to the fields in the **Value** column, as desired.
3. To save results of NPA split information to a file for further viewing and/or processing, click to check mark **Save Results**.
4. Click **View**.

The NPA splits in the PDB database that match the criteria entered are shown on the bottom of the page. For information about how to filter this information see *Filtering using the Display Filter*.

If **Save Results** was check marked, the CSV file is generated.

Creating an NPA split

You can only perform this task when logged into the Active Primary NOAM.

Use this procedure to create an NPA split and define its characteristics, including the old NPA code, the new NPA code, the central office (exchange) NXX code(s) to be transferred to the new NPA, and the beginning and ending dates of the Permissive Dialing Period (PDP).

1. Select **EAGLE XG Database** > **Maintenance** > **NPA Splits**
   The **EAGLE XG Database** > **Maintenance** > **NPA Splits** page appears.
2. Click to select the **Create** tab.
   The NPA Splits **Create** table appears.
3. Enter data to provision an NPA split. Values must be entered for **Old NPA**, **New NPA**, and **NXX**. If dates are entered in the **PDP Start** and/or **PDP End** dates, these dates must be greater than today's date.

   For more information about these fields please see *NPA splits elements*.
4. Click **Create**.

The NPA Split record is provisioned. Its state is initialized to Pending.

Modifying an NPA split

You can only perform this task when logged into the Active Primary NOAM.

Use this procedure to modify the Permissive Dialing Period (PDP) start and or end dates for one or more existing NPA splits.

1. Select **EAGLE XG Database** > **Maintenance** > **NPA Splits**.
   The **EAGLE XG Database** > **Maintenance** > **NPA Splits** page appears.
2. Click the **Modify** tab.
   The **Modify** tab appears.

3. Enter the **Old NPA**, **New NPA**, and **NXX** fields to select the NPA to modify. To modify all **NXX**, leave the **All** selection box check marked.
4. Enter the **PDP Start** and/or **PDP End** dates, as needed.

   Both the **PDP Start** and **PDP End** dates can be modified for pending splits. Only the **PDP End** date can be modified for active splits. Neither can be modified for completed splits. The **PDP End** date must be greater than today's date.

   For more information about these fields please see *NPA splits elements*.
5. Click **Modify.**

The NPA splits are updated.

Deleting an NPA split

You can only perform this task when logged into an NOAM.

Use this procedure to delete NPA splits that are pending or completed.

1. Select **EAGLE XG Database** > **Maintenance** > **NPA Splits**.
   The **EAGLE XG Database** > **Maintenance** > **NPA Splits** page appears.
2. Click the **Delete** tab.
   The **Delete** tab appears.
3. Enter values into the fields to select the NPA splits you want to delete. To delete all **NXX**, leave the **All** selection box check marked.
4. Click the **Delete** button.
   A warning pop up window appears, asking if you are sure you want to delete this NPA split.
5. Click **OK** to continue with the deletion.

The selected NP splits are deleted, and a Delete successful message is displayed.

Chapter 3

Tekelec HLR Router

Topics:

The **Tekelec HLR Router** menu options provide the ability to perform signaling and/or HLR Router related configuration and maintenance tasks.

The available HLR Router menu options will vary based on the type of server you are logged into and the permissions assigned to your group. If you do not see a menu option you need, please make sure you are logged into the appropriate type of server and ask your administrator to make sure the group your user ID belongs to has the appropriate permissions.

Tekelec HLR Router configuration

The **Tekelec HLR Router** > **Configuration** menu options allow you to perform signaling and/or HLR related configuration tasks. The available database menu options will vary based on the type of server you are logged into and the permissions assigned to your group.

When you are logged into an NOAM, you can set up signaling options and view, insert, edit, and delete service configurations, substitutions, mated entities, and throttling.

When you are logged into an SOAM you can view, insert, edit, and delete exception routing rules.

If you do not see a menu option you need, please make sure you are logged into the appropriate type of server and ask your administrator to make sure the group your user ID belongs to has the appropriate permissions.

Signaling options configuration

The **Tekelec HLR Router** > **Configuration** > **Options** page allows you to update signaling-specific configuration values that convert the CdPA digits into INTL format, so that they can be used in the DN/IMSI lookup.

All DNs and IMSIs in the database are stored in INTL (International) format. However, the address digits of the CdPA from the incoming message, which are used in the DN/IMSI lookup, will not always be in INTL format. To be in INTL format the address digits must contain:

- A CC (Country Code)
- An NDC (Network Destination Code)
- A subscriber number

The **Tekelec HLR Router** > **Configuration** > **Options** page allows you to supply E.214 and E.212 Country and Network Destination Codes that can be used when converting numbers to INTL format.

This page also allows you to specify whether the subscriber digits should be obtained from the SCCP or MAP layer when performing database look-ups. This applies to messages which have SCCP CdPA GTA encoded with entity address, and the message includes IMSI or MSISDN in the MAP layer.

Signaling options configuration elements

The **Tekelec HLR Router** > **Configuration** > **Options** page allows you to edit signaling options. This table describes fields on this page.

Table 34: Signaling Options Configuration Elements

Element	Description	Data Input Notes
Default Country Code	Default Country Code (CC) used when converting a E.214 number into international format	Format: Alphanumeric Range: 0 - 5 characters

Element	Description	Data Input Notes
Default Network Destination Code	Default Network Destination Code (NDC) used when converting a E.214 number into international format	Format: Alphanumeric Range: 0 - 5 characters
Default Mobile Country Code	Default Mobile Country Code (MCC) used when converting a E.212 number into international format	Format: Alphanumeric Range: 0 - 5 characters
Default Mobile Network Code	Default Mobile Network Code (MNC) used when converting a E.212 number into international format	Format: Alphanumeric Range: 0 - 5 characters
Throttling Disabled	Activates or deactivates the throttling disabled feature.	Format: Check mark
Exception Routing Override	Activates or deactivates the exception routing override feature.	Format: Check mark
Map Layer Routing	Activates or deactivates the map layer routing feature.	Format: Check mark

Changing HLR configuration options

You can only perform this task when logged into the Active Primary NOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Options**
   The **Tekelec HLR Router** > **Configuration** > **Options** page appears.
2. Edit the relevant fields.
   For more information about these fields, see *Signaling options configuration elements*.
3. Click **Apply**.
   The values entered are changed.

The changes are applied to the signaling configuration.

Service configuration

The **Tekelec HLR Router** > **Configuration** > **Service Config** page allows you to associate a TT (Translation Type) and SSN (Sub System Number) combination with a specific NP (Numbering Plan) and type of service. This relationship is used by the signaling application to determine the associated NP for a signaling message and to provide proper treatment of a message for the duration of the signaling message process.

In order to determine which database to query the application must know if the incoming message's CdPA address digits contain a DN or an IMSI. The NP describes the contents of the address digits. The supported NPs are:

- E.164 – The address digits contain a DN. Perform number conditioning on the address digits and query the DN database with the conditioned number.
- E.212 – The address digits contain an IMSI. Perform number conditioning on the address digits and query the IMSI database with the conditioned number.
- E.214 – The address digits contain a Mobile GT. Perform number conditioning on the address digits, convert the conditioned number to an E.212 number, then query the IMSI database with the converted number.

Service configuration elements

The **Tekelec HLR Router** > **Configuration** > **Service Config** page allows you to view, insert, edit, and delete service configurations. This table describes fields on this page.

Table 35: Service Configuration Elements

Element	Description
Action	The action that can be performed to the existing PDBI connections. Actions include: • Edit • Delete
TT	The Called Party Address Translation Type of the incoming message.
SSN	The Called Party Address Subsystem Number of the incoming message.
NP	The Numbering plan to use for an incoming with this TT/SSN combination. For E.164 numbers, the lookup will be performed in the DN table. For all others, the lookup will be performed in the IMSI table.
NAI	The Nature of Address Indicator to use for an incoming message with this TT/SSN combination.
Type of Service	The type of service to be performed for an incoming message with this TT/SSN combination.

Insert and Edit service configuration elements

The **Tekelec HLR Router** > **Configuration** > **Service Config [Insert]** page allows you to add new service configurations and the **Tekelec HLR Router** > **Configuration** > **Service Config [Edit]** page allows you to edit existing service configurations. This table describes fields on the **Insert** and **Edit** pages.

Table 36: Insert and Edit Service Configuration Elements

Element	Description	Data Input Notes
TT	The Called Party Address Translation Type of the incoming message	Format: Digits only Range: between 1 - 255
SSN	The Called Party Address Subsystem Number of the incoming message	Format: Digits only Range: between 2 - 255
NP	The Numbering Plan to use for an incoming message with this TT/SSN combination. For E.164 numbers, the lookup will be performed in the DN table. For all others, the lookup will be performed in the IMSI table.	Format: Pulldown menu Range: E164, E212, E214 Default: E164
NAI	The Nature of Address Indicator to use for an incoming message with TT/SSN combination.	Format: Pulldown menu Range: INTL, NATL, SUBS Default: INTL
Type of Service	The type of service to be performed for an incoming message with this TT/SSN combination.	Format: Pulldown menu Range: HLRR Default: HLRR

Inserting a service configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Service Config**
   The **Tekelec HLR Router** > **Configuration** > **Service Config** page appears.
2. Click on **Insert** located below the table.
   The **Tekelec HLR Router** > **Configuration** > **Service Config [Insert]** page appears.
3. Enter the trasnalation type in the **TT** field.
4. Enter the subsystem number in the **SSN** field.
5. Select the numbering plan from the **NP** pulldown.
6. Select the nature of address from the **NAI** pulldown.
7. Select the type of service from the **Type of Service** pulldown.
   For HLR, the **Type of Service** is always **HLRR** (HLR Routing).
8. Perform one of the following:
   - Click **OK** to save the signaling service configuration and exit this page.
   - Click **Apply** to save the signaling service configuration and remain on this page.

The service configuration is added and can now be used by the HLR to determine the associated numbering plan and provide proper treatment of a message for the duration of signaling message processing.

Viewing a service configuration

You can only perform this task when logged into an NOAM.

Select **Tekelec HLR Router** > **Configuration** > **Service Config**.
The **Tekelec HLR Router** > **Configuration** > **Service Config** page appears.

The current signaling service configurations are shown on the page. For information about how to filter this information, see *Filtering using the Display Filter*.

Editing a service configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Service Config**
   The **Tekelec HLR Router** > **Configuration** > **Service Config** page appears.
2. Click the **Edit** that corresponds to the service configuration you want to change.
   The **Tekelec HLR Router** > **Configuration** > **Service Config [Edit]** page appears.
3. Edit the fields you want to change.
   For more information about these fields, see *Insert and Edit service configuration elements*.
4. Perform one of the following:
   - Click **OK** to save the signaling service configuration and exit this page.
   - Click **Apply** to save the signaling service configuration and remain on this page.

The service configuration is updated and can now be used by the HLR to determine the associated numbering plan and provide proper treatment of a message for the duration of signaling message processing.

Deleting a service configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Service Config**
   The **Tekelec HLR Router** > **Configuration** > **Service Config** page appears.
2. Locate the Service Config you want to delete and click the corresponding **Delete** action.
   A pop up window appears.
3. Perform one of the following actions:
   - Click **OK** to delete the Service Config.
   - Click **Cancel** to cancel the delete.

The signaling service configuration is deleted.

Substitutions configuration

The **Tekelec HLR Router** > **Configuration** > **Substitutions** page allows you to associate a Country Code and Network Destination Code combination with a Mobile Country Code and Mobile Network Code combination. This association allows the translation of E.214 numbers to E.212 (IMSI) format, used for looking up IMSIs in the subscriber database..

Substitutions configuration elements

The **Tekelec HLR Router** > **Configuration** > **Substitutions** page allows you to view, insert, edit, and delete substitutions. This table describes fields on this page.

Table 37: Substitutions Configuration Elements

Element	Description
Action	The action that can be performed to the existing PDBI connections. Actions include: • Edit • Delete
CC	The Country Code of the incoming E.214 message.
NDC	The Network Destination Code of the incoming E.214 message.
MCC	The Mobile Country Code of the translated E.212 message.
MNC	The Mobile Network Code of the translated E.212 message.

Insert and Edit substitutions configuration elements

The **Tekelec HLR Router** > **Configuration** > **Substitutions [Insert]** page allows you to add new signaling substitutions and the **Tekelec HLR Router** > **Configuration** > **Substitutions [Edit]** page allows you to edit existing substations. This table describes fields on the **Insert** and **Edit** pages.

Table 38: Substitutions Insert and Edit Elements

Element	Description	Data Input Notes
CC	The Country Code of the incoming E.214 message	Format: Alphanumeric Range: 1 - 5 characters
NDC	The Network Destination Code of the incoming E.214 message	Format: Alphanumeric Range: 1 - 5 characters
MCC	The Mobile Country Code of the translated E.212 message	Format: Alphanumeric Range: 1 - 5 characters

Element	Description	Data Input Notes
MNC	The Mobile Network Code of the translated E.212 message	Format: Alphanumeric Range: 1 - 5 characters

Inserting substitutions configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Substitutions**
   The **Tekelec HLR Router** > **Configuration** > **Substitutions** page appears.
2. Click on **Insert** located below the table.
   The **Tekelec HLR Router** > **Configuration** > **Substitutions [Insert]** page appears.
3. Enter the country code in the **CC** field.
4. Enter the network destination code in the **NDC** field.
5. Enter the mobile country code in the **MCC** field.
6. Enter the mobile network code in the **MNC** field.
7. Perform one of the following:
   - Click **OK** to save the substitution configuration and exit this page.
   - Click **Apply** to save the substitution configuration and remain on this page.

The substitution is added and can now be used to translate E.214 numbers to IMSI format.

Viewing substitutions configuration

You can only perform this task when logged into the Active Primary NOAM.

Select **Tekelec HLR Router** > **Configuration** > **Substitutions**
The **Tekelec HLR Router** > **Configuration** > **Substitutions** page appears.

The current substitutions configurations are shown on the page. For information about how to filter this information, see *Filtering using the Display Filter*.

Editing substitutions configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Substitutions**
   The **Tekelec HLR Router** > **Configuration** > **Substitutions** page appears.
2. Click the **Edit** that corresponds to the substitution you want to change.
   The **Tekelec HLR Router** > **Configuration** > **Substitutions [Edit]** page appears.
3. Edit the fields you want to change.
   For more information about these fields please see *Insert and Edit substitutions configuration elements*.
4. Perform one of the following:
   - Click **OK** to save the substitution configuration and exit this page.
   - Click **Apply** to save the substitution configuration and remain on this page.

The substitution is updated and can now be used to translate E.214 numbers to IMSI format.

Deleting substitutions configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Substitutions**.
   The **Tekelec HLR Router** > **Configuration** > **Substitutions** page appears.
2. Locate the exception you want to delete and click the corresponding **Delete** action.
   A pop up window appears.
3. Perform one of the following actions:
   - Click **OK** to delete the signaling substitutions.
   - Click **Cancel** to cancel the delete.

The substitution is deleted.

Mated entities configuration

HLR supports a Mated Network Entities table that contains preferred and mated relationships. When a Network Entity is unavailable, HLR sends traffic to its mated Network Entity. The **Tekelec HLR Router** > **Configuration** > **Mated Entities** page allows you to manage the Mated Network Entities table data by associating Network Entities with a mate.

Mated entities configuration elements

The **Tekelec HLR Router** > **Configuration** > **Mated Entities** page allows you to view, delete, edit and insert mated entity associations. This table describes fields on this page.

Table 39: Mated Entities Configuration Elements

Element	Description
Action	The action that can be performed to the existing PDBI connections. Actions include: • Edit • Delete
Network Entity A	Identification string for a Network Entity
Network Entity B	Identification string for a Network Entity

Insert and Edit mated entities configuration elements

The **Tekelec HLR Router** > **Configuration** > **Mated Entities [Insert]** page allows you to add new mated entity associations and the **Tekelec HLR Router** > **Configuration** > **Mated Entities [Edit]** page allows you to edit current mated entity associations. This table describes fields on the **Insert** and **Edit** pages.

Table 40: Insert and Edit Mated Entities Configuration

Element	Description	Data Input Notes
Network Entity A	Identification string for a Network Entity	Format: Digits only Range: 1 - 15 digits
Network Entity B	Identification string for a Network Entity	Format: Digits only Range: 1 - 15 digits

Inserting mated entities configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Mated Entities**
   The **Tekelec HLR Router** > **Configuration** > **Mated Entities** page appears.
2. Enter the preferred network entity in the **Network Entity A** field.
3. Enter the mated network entity in the **Network Entity B** field.
4. Perform one of the following:
   - Click **OK** to save the mated entity configuration and exit this page.
   - Click **Apply** to save the mated entity configuration and remain on this page.

The mated entity relationship is added to the table.

Viewing mated entities configuration

You can only perform this task when logged into an NOAM.

Select **Tekelec HLR Router** > **Configuration** > **Mated Entities**
The **Tekelec HLR Router** > **Configuration** > **Mated Entities** page appears.

The currently configured mated entities are shown on the page. For information about how to filter this information, see *Filtering using the Display Filter*.

Editing mated entities configuration

You can only perform this task when logged into the Active Primary NOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Mated Entities**
   The **Tekelec HLR Router** > **Configuration** > **Mated Entities** page appears.
2. Click the **Edit** that corresponds to the service configuration you want to change.
   The **Tekelec HLR Router** > **Configuration** > **Mated Entities [Edit]** page appears.
3. Edit the fields you want to change.
   For more information about these fields, see *Insert and Edit mated entities configuration elements*.
4. Perform one of the following:
   - Click **OK** to save the mated entity configuration and exit this page.
   - Click **Apply** to save the mated entity and remain on this page.

The mated entity relationship is updated.

Deleting mated entities configuration

You can only perform this task when logged into an NOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Mated Entities**.
   The **Tekelec HLR Router** > **Configuration** > **Mated Entities** page appears.
2. Locate the exception you want to delete and click the corresponding **Delete** action.
   A pop up window appears.
3. Perform one of the following actions:
   - Click **OK** to delete the signaling mated entity.
   - Click **Cancel** to cancel the delete.

The mated entity is deleted.

Throttling configuration

The throttling feature is a powerful tool used to protect an HLR from peak overload. Throttling helps regulate the amount of traffic going to a particular HLR.

The throttling rule is a highly configurable and flexible algorithm used to select incoming messages going to the HLR. The throttling rule consists of a set of configurable criteria (conditions) on which the HLR selects the incoming message for further throttling treatment. Up to one thousand throttling rules can be defined, in any combination and configuration, depending on the reason and the purpose for the throttling. The HLR selects an incoming message; if it matches one of the active throttling rules, it applies the throttling treatment specified by the rule. Throttling treatment can include discarding the selected incoming message and not sending it to the HLR.

Any updates to throttling rules have an immediate impact on message processing, and there is no need to stop/re-start the application.

Use the **Tekelec HLR Router** > **Configuration** > **Throttling** menu options to configure and modify criteria used to determine on which messages to apply throttling. These include:

- DN Whitelists - specify which subscriber DN ranges to exempt from throttling
- IMSI Whitelists - specify which subscriber IMSI ranges to exempt from throttling
- MP Groups - specify a group of servers that share a throttling rule
- Opcodes - specify which opcodes in incoming messages to throttle
- Rules - specify when to apply throttling on a message

Throttling DN whitelists

The DN Whitelist consists of one or more subscriber DN ranges that are exempt from HLR throttling.

The DN Whitelist option allows you to view, add, modify, and delete a range. A DN whitelist range can also be imported from a CSV text file.

Throttling DN whitelist elements

The **Tekelec HLR Router** > **Throttling** > **DN Whitelist** page allows you to view, add, import, edit, and delete ranges of whitelisted subscriber DNs. This table describes fields on this page.

Table 41: Throttling DN Whitelist Configuration Elements

Element	Description	Data Input Notes
Start of Range	Start of a range of DNs immune to throttling	Format: Integer Range: 8 - 15 digits Default: blank
End of Range	End of a range of DNs immune to throttling	Format: Integer Range: 8 - 15 digits Default: blank

Viewing throttling DN whitelists

You can only perform this task when logged into an NOAM.

Use this procedure to view existing ranges of whitelisted subscriber DNS values.

Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist**.
The **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist** page appears.

All DN subscriber ranges being whitelisted are shown on the page. For information about how to filter this information, see *Filtering using the Display Filter*.

Adding a new range of subscriber DNs

You can only perform this task when logged into the Active Primary NOAM.

Use this procedure to add a new subscriber DN range to be whitelisted. Subscriber DNS specified in this range must not be included in any existing whitelisted subscriber DNs. Your attempt to add the range will fail if any do. Also, both range values entered here must be of equal length.

Note: A maximum of 1,000,000 subscriber DN ranges can be excluded from throttling using the DN Whitelist feature. Once the maximum number has been defined, no additional DN ranges can be added.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist** page appears.
2. Click **Insert** at the bottom of the page.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist [Insert]** page appears.
3. Enter the DN start range value in the **Start of Range** field. This field is required. This value cannot be the same as the start value defined in an existing range.
4. Enter the DN end range value in the **End of Range** field. This field is required.
5. Perform one of the following:
   - Click **OK**to save the new subscriber DN whitelist range and exit this page.
   - Click **Apply**to save the new subscriber DN whitelist range and remain on this page.

The subscriber DN whitelist range is added to the table, and a success message is displayed.

Importing one or more DN whitelists

You can only perform this task when logged into the Active Primary NOAM.

DN whitelists can be provisioned by importing a CSV text file that contains one or more subscriber DN ranges. This provides a quick method of specifying multiple DN ranges to be whitelisted at one time.

The valid CSV test file must contain comma-delimited ranges of DNs with each record on a separate line. This file cannot exceed 100,000 lines. Note that entries that exist prior to the import are not removed. However, if a record exists with the same start range as one being imported, it is replaced with the imported record.

Note: A maximum of 1,000,000 subscriber DN ranges can be excluded from throttling using the DN Whitelist feature. Once the maximum number has been defined, no additional DN ranges can be added.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist** page appears.
2. Click **Import** at the bottom of this page.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist [Import]** page appears.
3. Specify the **File Format** by clicking to select either **Dos** or **Unix**.
4. Enter the path to the file and the CSV filename in the **Filename** field, or click **Browse** to pop up a browse window to select the file.
5. Click **Import**.

The subscriber DN whitelist ranges defined in the text file are added to the table, and an **import successful** message is displayed.

Throttling DN whitelist import elements

The **Tekelec HLR Router** > **Throttling** > **DN Whitelist [Import]** page allows you to import a file containing DN whitelist ranges. This table describes fields on this page.

Table 42: Throttling DN Whitelist Import Configuration Elements

Element	Description	Data Input Notes
Filename	The import file containing comma-delimited data with each record on a separate line. This file should not exceed 100,000 times	Format: Alphanumeric, **Browse** button Range: Existing CSV files Default: Blank
File Format	Format of file	Format: Radio button Range: Dos, Unix Default: Dos

Modifying a DN whitelist range

You can only perform this task when logged into the Active Primary NOAM.

The start and/or end of a subscriber DN whitelist range can be modified using this procedure.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist** page appears.
2. Click the **Edit** that corresponds to the DN whitelist you want to change.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist [Edit]** page appears.

3. Edit the beginning and/or ending range fields as needed.
   For more information about these fields please see *Throttling DN whitelist elements*.
4. Perform one of the following:
   - Click **OK** to save the updated range and exit this page.
   - Click **Apply** to save the updated range and remain on this page.

The selected DN whitelist range is updated, and an Update successful message is displayed.

Deleting a DN whitelist range

You can only perform this task when logged into an NOAM.

Use this procedure to delete an existing subscriber DN range from the DN whitelist table.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **DN Whitelist** page appears.
2. Locate the range you want to delete and click the corresponding **Delete** action.
   A warning pop up window appears, asking if you are sure you want to delete this row.
3. Click **OK** to continue with the deletion.

The subscriber DN range is deleted, and a Delete successful message is displayed.

Throttling IMSI whitelists

The IMSI Whitelist consists of one or more subscriber IMSI ranges that are exempt from HLR throttling.

The IMSI Whitelist option allows you to view, add, modify, and delete a range. An IMSI whitelist range can also be imported from a CSV text file.

Throttling IMSI whitelist elements

IMSI Whitelist is a list of whitelisted subscriber IMSI ranges on which throttling is not enforced.

The **Tekelec HLR Router** > **Throttling** > **IMSI Whitelist** page allows you to view, add, import, edit, and delete ranges of whitelisted subscriber IMSIs. This table describes fields on this page.

Table 43: Throttling IMSI Whitelist Configuration Elements

Element	Description	Data Input Notes
Start of Range	Start of a range of IMSIs immune to throttling	Format: Integer Range: 10 - 15 digits Default: blank
End of Range	End of range of IMSIs immune to throttling	Format: Integer Range: 10 - 15 Default: blank

Viewing throttling IMSI whitelists

You can only perform this task when logged into an NOAM.

Use this procedure to view all configured IMSI whitelists.

Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist.**
The **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist.** page appears.

All IMSI subscriber ranges being whitelisted are shown on the page. For information about how to filter this information, see *Filtering using the Display Filter*.

Adding a new range of subscriber IMSIs

You can only perform this task when logged into the Active Primary NOAM.

Use this procedure to add a new subscriber IMSI range to be whitelisted. The subscriber IMSI range must not be included in any existing whitelisted IMSIs; your attempt to add the range will fail if any IMSIs are in an existing range. Also, both range values entered here must be of equal length.

Note: A maximum of 1,000,000 subscriber IMSI ranges can be excluded from throttling using the IMSI Whitelist feature. Once the maximum number has been defined, no additional IMSI ranges can be added.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist** page appears.
2. Click **Insert** at the bottom of the page.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist [Insert]** page appears.
3. Enter the IMSI start range value in the **Start of Range** field. This field is required. This value cannot be included in any existing IMSI whitelist ranges.
4. Enter the IMSI end range value in the **End of Range** field. This field is required. Note that the value in the **Start of Range** field and the value in the **End of Range** field must contain the same number of digits.
5. Perform one of the following:
   - Click **OK**to save the new subscriber IMSI whitelist range and exit this page.
   - Click **Apply**to save the new subscriber IMSI whitelist range and remain on this page.

The subscriber IMSI whitelist range is added to the table, and an Insert successful message is displayed.

Importing one or more IMSI whitelists

You can only perform this task when logged into the Active Primary NOAM.

IMSI whitelists can be provisioned by importing a CSV text file that contains one or more subscriber IMSI ranges. This provides a quick method of specifying multiple IMSI ranges to be whitelisted at one time.

A valid CSV text file must contain comma-delimited ranges of IMSIs with each record on a separate line. This file cannot exceed 100,000 lines. Entries that exist prior to the import are not removed. However, if a record exists with the same start range as one being imported, it is replaced with the imported record.

Note: A maximum of 1,000,000 subscriber IMSI ranges can be excluded from throttling using the IMSI Whitelist feature. Once the maximum number has been defined, no additional IMSI ranges can be added.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist** page appears.
2. Click **Import** at the bottom of this page.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist [Import]** page appears.
3. Specify the **File Format** by clicking to select either **Dos** or **Unix**.

4. Enter the path to the file and the CSV filename in the **Filename** field, or click **Browse** to pop up a browse window to select the file.
5. Click **Import**.

The subscriber IMSI whitelist ranges defined in the text file are added to the table, and an **import successful** message is displayed.

Throttling IMSI whitelist import elements

The **Tekelec HLR Router** > **Throttling** > **IMSI Whitelist [Import]** page allows you to import IMSI ranges to whitelist. This table describes fields on this page.

Table 44: Throttling IMSI Whitelist Import Configuration Elements

Element	Description	Data Input Notes
Filename	The import file containing comma-delimited data with each record on a separate line	Format: Integer **Browse** button Range: Existing CSV files Default: Blank
End of Range	Format of file (DOS or Unix)	Format: Radio button Range: Dos, Unix Default: Dos

Modifying an IMSI whitelist range

You can only perform this task when logged into the Active Primary NOAM.

The start and/or end of a subscriber IMSI whitelist range can be modified using this procedure.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist** page appears.
2. Click the **Edit** that corresponds to the IMSI whitelist you want to change.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist [Edit]** page appears.
3. Edit the beginning and/or ending range fields as needed. All range values entered must be unique IMSI whitelist values.

   For more information about these fields please see *Throttling IMSI whitelist elements*.
4. Perform one of the following:
   - Click **OK** to save the updated range and exit this page.
   - Click **Apply** to save the updated range and remain on this page.

The selected IMSI whitelist range is updated, and an Update successful message is displayed.

Deleting an IMSI whitelist range

You can only perform this task when logged into an NOAM.

Use this procedure to delete an existing IMSI whitelist range from the IMSI whitelist table.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **IMSI Whitelist** page appears.
2. Locate the IMSI whitelist you want to delete and click the corresponding **Delete** action.
   A pop up window appears, asking if you are sure you want to delete this row.

3. Click **OK** to continue with the deletion.

The IMSI whitelist is deleted, and a Delete successful message is displayed.

Throttling MP groups

An MP group is a collection of MP servers that shares one or more throttling rules; HLR enforces the throttling mechanism on all MPs listed in a group. Note that an MP server can be a member of more than one MP group. The **Tekelec HLR Router** > **Configuration** > **Throttling** > **MP Groups** page allows you to view, add, edit, and delete MP groups.

Throttling MP groups elements

The **Tekelec HLR Router** > **Throttling** > **MP Groups** page allows you to view, add, edit, and delete MP groups. This table describes fields on this page.

Table 45: Throttling MP Groups Elements

Element	Description	Data Input Notes
Group Name	Descriptive name for this collection of MP servers	Format: Alphanumeric string Range: 1 - 20 Default: Blank
Group Members	Highlight one or more MPs to be included in this group (hold the Ctrl key down to select multiple hostnames). MPs may be included in more than one group.	Format: Selection box Range: All configured MPs Default: Blank

Viewing throttling MP groups

You can only perform this task when logged into an NOAM.

Use this procedure to view the list of existing throttling MP groups.

Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **MP Groups**
The **Tekelec HLR Router** > **Configuration** > **Throttling** > **MP Groups** page appears.

All configured MP groups are shown on the page. For information about how to filter this information, see *Filtering using the Display Filter*.

Adding an MP group

You can only perform this task when logged into the Active Primary NOAM.

Use this procedure to add a new MP group to share one or more throttling rules. A maximum of 100 MP groups can be added.

Note: A maximum of 100 MP groups can be configured. Once the maximum number has been defined, no additional MP groups can be added.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **MP Groups**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **MP Groups** page appears.
2. Click **Insert** at the bottom of the page.

The **Tekelec HLR Router** > **Configuration** > **Throttling** > **MP Groups [Insert]** page appears.

3. Enter a name for the new MP group in the **Group Name** field. This name must be unique among MP group names.
4. In the **Group Members** field, click to select the MPs to include in this group. Hold down the **Ctrl** key to select more than one server. Note that an MP can be in more than one MP group.
5. Perform one of these options:
   - Click **OK** to save the new MP group configuration and exit this page.
   - Click **Apply** to save the new MP group configuration and remain on this page.

The MP server group is added to the MP groups table, and an Insert successful message is displayed.

Modifying an MP group

You can only perform this task when logged into the Active Primary NOAM.

Use this procedure to change the Group Name and/or Group Members for an MP group.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **MP Groups**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **MP Groups** page appears.
2. Click the **Edit** that corresponds to the MP group you want to change.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **MP Groups [Edit]** page appears.
3. Edit the fields you want to change.
4. Perform one of the following:
   - Click **OK**to save the MP group configuration and exit this page.
   - Click **Apply**to save the MP group and remain on this page.

The MP server group is updated, and an Update successful message is displayed.

Deleting a throttling MP group

You can only perform this task when logged into an NOAM.

Use this procedure to delete an existing MP group from the MP group table.

Note: Any MP group currently in use by the throttling rule cannot be deleted.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **MP Groups**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **MP Groups** page appears.
2. Locate the MP group you want to delete and click the corresponding **Delete** action.
   A warning pop up window appears, asking if you are sure you want to delete this row.
3. Click **OK** to continue with the deletion.

The MP group is deleted, and a Delete successful message is displayed.

Throttling opcodes

All messages destined to HLR are GSM messages, and the GSM opcode is a field within the GSM message. Use the throttling opcode GUI option to associate a GSM opcode value with an Opcode Name. The Opcode Name can be used in a throttling rule to select messages for throttling. Use this option to also view, edit, and delete opcodes.

Throttling opcodes elements

The **Tekelec HLR Router** > **Throttling** > **Opcodes** page allows you to view, add, edit, and delete GSM opcodes. This table describes fields on this page.

Table 46: Throttling Opcodes Configuration Elements

Element	Description	Data Input Notes
Opcode Value	GSM Opcode value on which to filter messages for throttling purposes	Format: Integer Range: 1 - 3 digit number (2 - 255) Default: blank
Opcode Name	Descriptive name to help identify this opcode	Format: Alphanumeric string Range: 1 - 32 characters Default: blank

Viewing throttling opcodes

You can only perform this task when logged into an NOAM.

Use this procedure to view the list of existing throttling GSM opcodes.

Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **Opcodes**.
The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Opcodes** page appears.

The currently configured throttling GSM opcodes are shown on the page. For information about how to filter this information, see *Filtering using the Display Filter*.

Adding a throttling opcode

You can only perform this task when logged into the Active Primary NOAM.

Use this procedure to add a new GSM opcode used in throttling rules.

Note: A maximum of 100 GSM opcodes can be configured. Once the maximum number has been defined, no additional opcodes can be added.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **Opcodes**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Opcodes** page appears.
2. Click **Insert** at the bottom of the page.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Opcodes [Insert]** page appears.
3. Enter a value in the **Opcode Value** field. This value must be unique and cannot exist in another opcode.
4. Enter a new name in the **Opcode Name** field. This name must be unique and cannot exist in another opcode.
5. Perform one of these options:
   - Click **OK**to save the opcode configuration and exit this page.
   - Click **Apply** to save the opcode configuration and remain on this page.

The opcode is added to the table, and an Insert successful message is displayed.

Editing opcodes

You can only perform this task when logged into the Active Primary NOAM.

Use this procedure to modify the name of an existing GSM opcode that is used in throttling rules. The Opcode Value field cannot be modified.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **Opcodes**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Opcodes** page appears.
2. Click the **Edit** that corresponds to the opcode configuration you want to change.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Opcodes [Edit]** page appears.
3. Edit the **Opcode Name**.
4. Perform one of these options:
   - Click **OK** to save the updated opcode configuration and exit this page.
   - Click **Apply** to save the updated opcode configuration and remain on this page.

The GSM opcode is updated, and an Update successful message appears.

Deleting a throttling opcode

You can only perform this task when logged into an NOAM.

Use this procedure to delete an existing GSM opcode from the opcode table.

Note: Any GSM opcode currently in use by a throttling rule cannot be deleted.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **Opcodes**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Opcodes** page appears.
2. Locate the GSM opcode you want to delete and click the corresponding **Delete** action.
   A warning pop up window appears, asking if you are sure you want to delete this row.
3. Click **OK** to continue with the deletion.

The GSM opcode is deleted, and a Delete successful message is displayed.

Throttling rules

Throttling rules are used to determine when to select an incoming message for throttling, and what type of throttling to perform. The number of servers affected by a throttling rule can range from one MP to all MPs in the entire HLR system. Note that each rule can only be applied to one MP group.

Throttling rules elements

The **Tekelec HLR Router** > **Throttling** > **Rules** page allows you to view, add, edit, and delete throttling rules. This table describes fields on this page.

Table 47: Throttling Rules Elements

Element	Description	Data Input Notes
Name	Text to identify rule	Format: Alphanumeric string Range: 1 - 20 characters Default: blank

Element	Description	Data Input Notes
Opcode	The GSM Opcode on which to filter	Format: Pull-down menu Range: Configured opcodes Default: blank
Destination Address Prefix	The E.164 destination address on which to filter. The matching algorithm uses Longest Prefix Matching, so a value of 1919 will match all destination addresses beginning with those digits.	Format: Integer Range: 1 to 15 digit number Default: blank
Source Address Prefix	The E.164 source address on which to filter. The matching algorithm uses Longest Prefix Matching, so a value of 1919 will match all source addresses beginning with those digits.	Format: Integer Range: 1 to 15 digit number Default: blank
MP Group	Group of Message Processors on which this filter is to be applied.	Format: Pull-down menu Range: Configured MP groups Default: blank
Shed Rate	The percentage of matching messages to discard.	Format: Pull-down menu Range: 10, 25, 33, 50, 66, 75, 90, 100 Default: 10
Apply Whitelist	Whether or not to apply the whitelist to this rule. If checked, the DN and IMSI whitelists will be consulted when a match occurs. Numbers contained in those whitelists are immune to throttling.	Format: Pull-down menu Range: Yes, No Default: Yes
Mode	Current mode of this rule. Simulation mode will peg measurements related to the messages matching the rule, but will not discard any messages. It is highly recommended that a rule be first placed into Simulation mode before being made Active.	Format: Pull-down menu Range: Inactive, Active, Simulation Default: Inactive
Match Action	Action to be performed on matches.	Format: Pull-down menu

Element	Description	Data Input Notes
		Range: Discard, Discard w/UDTS, Discard w/TCAP Error Default: Discard
Error Code	The error code to be returned when Match Action is set either to Discard with UDTS or Discard with TCAP Error. This field is disabled when Match Action is set to **Discard.**	Format: Integer Range: 3 digit number (0 - 255) Default: blank

Viewing throttling rules

You can only perform this task when logged into an NOAM.

Use this procedure to view all configured throttling rules.

Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **Rules**
The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Rules** page appears.

The currently configured throttling rules are shown on the page. For information about how to filter this information, see *Filtering using the Display Filter*.

Adding a throttling rule

You can only perform this task when logged into the Active Primary NOAM.

Use this procedure to configure a new throttling rule.

Note that the Opcode and MP group selected in a throttling rule must be provisioned prior to configuring this rule. Also, a new rule cannot share its combination of Opcode, Source Address Prefix, and Destination Address Prefix with any existing throttling rule.

Note: A maximum of 1,000 rules can be configured. Once the maximum number has been defined, no additional rules can be added.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **Rules**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Rules** page appears.
2. Click **Insert** at the bottom of the page.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Rules [Insert]** page appears.
3. Enter values into the required fields: **Name**, **Opcode**, **Destination Address Prefix**, **Source Address Prefix**, and **MP Group**.
4. Enter values into the optional fields, as needed.
5. Perform one of these options:
   - Click **OK** to save the throttling rule configuration and exit this page.
   - Click **Apply** to save the throttling rule configuration and remain on this page.

The throttling rule is added to the table, and an Insert success message is displayed.

Editing rules

You can only perform this task when logged into the Active Primary NOAM.

Use this procedure to modify the criteria of an existing throttling rule. The only fields that can be modified for a rule are Shed Rate, Apply Whitelist, Mode, Match Action, and Error Code.

Note: A modified rule cannot share its combination of Opcode, Source Address Prefix, and Destination Address Prefix with any other existing throttling rule.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **Rules**
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Rules** page appears.
2. Click the **Edit**that corresponds to the throttling rule you want to change.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Rules [Edit]** page appears.
3. Edit the fields you want to change.
   For more information about these fields please see *Throttling rules elements*.
4. Perform one of the these options:
   - Click **OK** to save the throttling rule configuration and exit this page.
   - Click **Apply** to save the throttling rule configuration and remain on this page.

The throttling rule is updated, and an Update successful message appears.

Deleting a throttling rule

You can only perform this task when logged into an NOAM.

Use this procedure to delete an existing rule configuration from the rule table.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **Rules**.
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Rules** page appears.
2. Locate the rule configuration you want to delete and click the corresponding **Delete** action.
   A warning pop up window appears, asking if you are sure you want to delete this row.
3. Click **OK** to continue with the deletion.

The rule configuration is deleted, and a Delete successful message is displayed.

Throttling rule test

Use this option to quickly determine whether or not an incoming message matches a throttling rule. The values that affect the test are the message's opcode, destination address, source address, and MP server.

After the test is performed, the resulting output appears at the bottom of the **Rule Test** page.

Throttling rules test elements

The **Tekelec HLR Router** > **Throttling** > **Rule Test** page allows you to determine if there is a matching throttling rule for a particular type of incoming message. This table describes fields on this page.

Table 48: Throttling Rule Test Elements

Element	Description	Data Input Notes
Opcode	The opcode on the incoming GSM message	Format: Pull-down menu Range: Configured opcodes Default: Blank

Element	Description	Data Input Notes
Destination Address	E.164 address that identifies the destination signaling point (HLR)	Format: Integer Range: 8 to15-digit number Default: Blank
Source Address	E.164 address that identifies the originating MSC	Format: Integer Range: 8 to 15-digit number Default: Blank
MP	Message Processor on which to test the rule matching logic	Format: Pull-down menu Range: Configured MPs Default: Blank

Testing a throttling rule

You can only perform this task when logged into the Active Primary NOAM.

Use this procedure to enter criteria for checking if there is a matching throttling rule for a particular type of incoming message.

1. Select **Tekelec HLR Router** > **Configuration** > **Throttling** > **Rule Test**
   The **Tekelec HLR Router** > **Configuration** > **Throttling** > **Rule Test** page appears.
2. Specify the **Opcode**, **Destination Address**, **Source Address**, and **MP** to be tested. All fields are required.
3. Click **Test**

Results of the rule test appear at the bottom of the page. If a matching throttling rule is found, the following information is displayed: Name, Opcode, Destination Prefix, Source Prefix, Applied to MPs, Apply Whitelist, Mode, Action, and Shed Rate. If no matching active rule is found, then the message "No match was found" appears instead.

Exception routing configuration

Normal routing consists of querying the DN database (for E.164 numbers) or IMSI database (for E.212 numbers), then routing the message to the preferred or mated Network Entity for the DN or IMSI that was queried. If normal routing fails, exception routing is performed. Exception routing consists of querying the Exception Routing table and routing the message based on the CdPA TT, the CdPA SSN, and the DPC of the incoming message.

HLR supports up to 256 exception routing records. When normal and exception routing fail HLR Router is unable to route a message.

The **Tekelec HLR Router** > **Configuration** > **Exception Routing** page allows you to view the current rules provisioned for routing a request when that subscriber is not found in the database, edit or delete an existing exception routing rule, or to insert a new exception routing rule.

This page is only available when logged into an SOAM.

Exception routing configuration elements

The **Tekelec HLR Router** > **Configuration** > **Exception Routing** page allows you to view current mated entity associations. This table describes fields on this page.

Table 49: Exception Routing Configuration Elements

Element	Description
Action	The action that can be performed to the existing PDBI connections. Actions include: • Edit • Delete
TT	The Called Party Address Translation Type of the incoming message
NP	The Called Party Address Numbering plan of the incoming message
DPC	Destination Point Code of incoming message. This will be called the True Point Code or the Capability Point Code of the MP processing the message
Network Entity	Network Entity identification string. This value identifies the preferred entity for the associated TT/NP/DPC combination.

Insert and Edit exception routing configuration elements

The **Tekelec HLR Router** > **Configuration** > **Exception Routing [Insert]** page allows you to add exception routing rules and the **Tekelec HLR Router** > **Configuration** > **Exception Routing [Edit]** page allows you to edit existing exception routing rules. This table describes fields on the **Insert** and **Edit** pages.

Table 50: Insert and Edit Exception Routing Configuration

Element	Description	Data Input Notes
TT	The Called Party Address Translation Type of the incoming message	Format: Digits only Range: between 1 - 255
NP	The Called Party Address Numbering plan of the incoming message	Format: Pulldown menu Range: E164, E212, E214, NA Default: E164
DPC	Destination Point Code of incoming message. This will be called the True Point Code or the	Format: Alphanumeric Range: 1 - 11 characters

Element	Description	Data Input Notes
	Capability Point Code of the MP processing the message	
Network Entity	Network Entity identification string. This value identifies the preferred entity for the associated TT/NP/DPC combination.	Format: Digits only Range: 1 - 15 digits

Inserting exception routing configuration

You can only perform this task when logged into an SOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Exception Routing**.
   The**Tekelec HLR Router** > **Configuration** > **Exception Routing** page appears.
2. Click **Insert**, located below the table.
   The**Tekelec HLR Router** > **Configuration** > **Exception Routing [Insert]** page appears.
3. Enter the Translation Type of the incoming message in the **TT** field.
4. Select the CdPA Numbering Plan of the incoming message from the **NP** pulldown menu.
5. Enter the Destination Point Code of the incoming message in the **DPC** field.
6. Enter the Network Entity identifier in the **Network Entity** field.
7. Perform one of the following:
   - Click **OK** to save the signaling exception configuration and exit this page.
   - Click **Apply** to save the signaling exception and remain on this page.

The signaling exception is added to the database.

Viewing exception routing configuration

You can only perform this task when logged into an SOAM.

Select **Tekelec HLR Router** > **Configuration** > **Exception Routing**.
The**Tekelec HLR Router** > **Configuration** > **Exception Routing** page appears.

The configured exceptions are shown in the table. For information about how to filter this information, see *Filtering using the Display Filter*.

Editing signaling exception configuration

You can only perform this task when logged into an SOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Exception Routing**.
   The**Tekelec HLR Router** > **Configuration** > **Exception Routing** page appears.
2. Locate the exception you want to edit and click the corresponding **Edit** action.
   The**Tekelec HLR Router** > **Configuration** > **Exception Routing [Edit]** page appears.
3. Edit the fields you want to change.
   For more information about these fields, see *Insert and Edit exception routing configuration elements*.

4. Perform one of the following:
   - Click **OK** to save the signaling exception configuration and exit this page.
   - Click **Apply** to save the signaling exception and remain on this page.

The signaling exception configuration is updated.

Deleting exception routing configuration

You can only perform this task when logged into an SOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **Exception Routing**.
   The **Tekelec HLR Router** > **Configuration** > **Exception Routing** page appears.
2. Locate the exception you want to delete and click the corresponding **Delete** action.
   A pop up window appears.
3. Perform one of the following actions:
   - Click **OK** to delete the signaling exception routing
   - Click **Cancel** to cancel the delete

The exception routing is deleted.

Exception routing override

Exception Routing Override enables an MP to directly return an unknown subscriber message to the initiating node when normal routing fails (similar to what HLR's do when an IMSI or DN is not found in their database).

If normal routing fails and the Exception Routing Override option is not set, Exception Routing is performed regardless of whether the MP E.164 number is being set or not. The MP E.164 number must be set for Exception Routing Override to be performed. If the option is set and the MP E.164 number is missing, an event is issued on the GUI and exception routing is performed.

When an MP receives a message and the E.164 DN or E.212 IMSI is not found in MP's database, the MP will first check if the Exception Routing Override flag is set and an E.164 number is configured in the MP Configuration table (see *Exception routing configuration*). If these conditions are met, the MP responds back to the MC with a well-formatted UDT message.

The following will apply to the response UDT message:

- The UDT will contain a TCAP END message.
- The DPC is assigned the OPC of the received request message.
- The OPC is assigned the MP's self point code.
- Called Party and Calling Party information will be transposed with one exception:
  - The Calling Party address digit information is assigned the E.164 of the MP. See *Exception routing configuration* for the MP E.164 Configuration.
- TCAP Component Type (Return Error).
- The SCCP error flag in the header shall be set to TRUE.
- The Dialog component of the TCAP message will be the basic Unknown Subscriber template with Destination Transaction ID recovered from the Originating Transaction ID of the initiating TCAP request.

- The dialogue PDU and version also need to be retrieved from the initiating TCAP request.

- For the Component Portion of the TCAP message, the Invoke Id will need to be recovered from the initiating TCAP request.

Note: If the Exception Override Flag and/or E.164 number is not configured, then the MP will send the request message to Exception Routing.

1. Select **Tekelec HLR Router** > **Configuration** > **Options**.
   The**Tekelec HLR Router** > **Configuration** > **Options** page appears.
2. Specify the exception you want to override and click the **Exception Routing Override** box.
3. Perform one of the following actions:
   - Click the **Exception Routing Override** box to override the signaling exception routing.
   - Click **Exception Routing Override** box to deactivate the exception routing override.

The exception routing activated or deactivated as indicated by the checkbox.

MP E.164 options configuration

The **Tekelec HLR Router** > **Configuration** > **MP E.164** page allows you to configure the hostname and E.164 numbers for MP servers.

Note: This page is available on SOAM sites only.

An MP configuration table contains hostnames and E.164 node addresses for MP servers. The hostname maps to an MP hostname in the Servers table and it must be configured in the Servers table before it can be entered.

When Exception Routing Override feature is activated and the MP's E.164 is populated, the Exception Routing Override feature will use the specified E.164 number. This E.164 number is assigned to the SCCP Calling Party address digits in TCAP END Response messages from an MP. Refer to *Exception routing override* for more details.

Note: You must restart the MP application after an E.164 address is assigned to or deleted from an MP.

MP E.164 configuration elements

The **EAGLE XG Database** > **Configuration** > **MP E.164** page allows you to assign an E.164 address to an MP for use in the SCCP Calling Party Address of a TCAP End Response message sent by the MP.

Table 51: MP E.164 Configuration Elements

Element	Description	Required Permissions
Display	Allows a user to retrieve MP Servers hostname and E.164 numbers. **Note:** The **Go** is disabled until a selection is made from the Display dropdown menu.	HLRR Configuration

Element	Description	Required Permissions
Insert	Opens a page where a user can add or configure MP Configuration information.	Insert application data, HLRR Configuration
Delete	Opens a warning pop up appears, asking if you are sure that you want to delete this item.	Delete application data, HLRR Configuration

MP E.164 insert elements

The **EAGLE XG Database** > **Configuration** > **MP E.164 [Insert]** page allows you to add and configure MP Configuration information.

The following rules apply to this page:

- A Hostname must be configured in the MP Servers table before it can be entered.
- A Hostname and E.164 number must be provided when adding MP information.
- Hostnames must be unique.
- An E.164 address must be between 8-15 digits in length.

Note: The **Apply** and **OK** buttons are disabled until a Hostname or E.164 value is selected.

Table 52: MP E.164 Insert Configuration Elements

Element	Description	Required Permissions
Hostname	Hostname assigned to MP	Insert application data, HLRR Configuration
E.164	E.164 Node Address	Insert application data, HLRR Configuration

MP E.164 edit elements

The **EAGLE XG Database** > **Configuration** > **MP E.164 [Edit]** page allows you to update and edit MP Configuration information.

The following rules apply to this page:

- A Hostname must be configured in the MP Servers table before it can be entered.
- An E.164 address must be between 8-15 digits in length.

Note: The **Apply** and **OK** buttons are disabled until a Hostname or E.164 value is selected.

Table 53: MP E.164 Edit Configuration Elements

Element	Description	Required Permissions
Hostname	Use this field to edit a MP Hostname value.	Edit application data, HLRR Configuration
E.164	Use this field to edit an E.164 value.	Edit application data, HLRR Configuration

PDE options configuration

PDE feature collects performance data on the HLR Router system, generates report files in CSV format, and then exports the CSV files to the remote customer SFTP server. Performance data provides information about system performance, workload, issues, and/or issues experienced by the system at the given period.

The PDE feature collects performance data for the following purposes:

- application performance monitoring
- hardware performance monitoring
- system workload monitoring
- network connectivity monitoring
- user activity monitoring
- signal traffic monitoring

PDE collects the following types of performance data:

- Active Alarms
- Alarms/Events
- Measurements
- KPI
- PDBI logs
- PDBI Status
- Security logs
- SS7/HLR Router Configuration

On SOAMP servers, PDE collects the following SS7/Sigtran/HLR Router configuration data:

- Associations
- Link
- Linkset
- Route
- RMU
- Mated HLR
- Exception Routing
- Adjacent Servers and groups
- Local Signaling Points
- Remote Signaling Points
- Association Configuration Sets
- SCCP Options
- MTP3 Options
- M3UA Options
- Local Congestion Options

The type of performance data that is collected cannot be limited to a subset of data.

The **Tekelec HLR Router** > **Configuration** > **PDE** > **Options** page allows you to enable and disable PDE and to specify the remote server, remote server login information, and the exported file storage location on the remote server. When the PDE export is enabled the PDE process will start at the next

15 minute interval. The PDE process will continue to run automatically every 15 minutes - at :00, :15, :30, and :45 - until it is disabled through the GUI.

PDE options configuration elements

The **Tekelec HLR Router** > **Configuration** > **PDE** > **Options** page allows you to apply or edit PDE options. This table describes fields on this page.

Table 54: PDE Configuration Options Elements

Element	Description	Data Input Notes
Hostname	Hostname of the remote server that receives periodic performance data exports. Update password when changing hostname.	Format: Alphanumeric Range: 1 - 24 characters
User Name	Login user name for the remote server that receives periodic performance data exports. Update password when changing hostname.	Format: Alphanumeric Range: 0 - 255 characters
User Password	Login user password for the remote server that receives periodic performance data exports. After successful key exchange, the password is no longer needed unless a new hostname and/or username is entered.	Format: Alphanumeric Range: 0 - 255 characters
Storage Path	Storage path on the remote server that receives periodic performance data exports.	Format: Alphanumeric Range: 1 - 255 characters
PDE Enabled	Whether or not PDE will collect and export selected performance data	Format: Selection box Range: Checked, unchecked Default: Unchecked
Measurement Export Enabled	Whether or not to create and transfer measurement CSV fies	Format: Selection box Range: Checked, unchecked Default: Checked
KPI Export Enabled	Whether or not to create and transfer KPI CSV fies	Format: Selection box Range: Checked, unchecked Default: Checked

Element	Description	Data Input Notes
PDBI Log Export Enabled	Whether or not to create and transfer PDBI log CSV fies	Format: Selection box Range: Checked, unchecked Default: Checked
Security Log Export Enabled	Whether or not to create and transfer security log CSV fies	Format: Selection box Range: Checked, unchecked Default: Checked
Active Alarms Export Enabled	Whether or not to create and transfer active alarms CSV fies	Format: Selection box Range: Checked, unchecked Default: Checked
Alarms and Events Export Enabled	Whether or not to create and transfer alarms and events CSV fies	Format: Selection box Range: Checked, unchecked Default: Checked
SS7 Config Export Enabled	Whether or not to create and transfer SS7 config CSV fies	Format: Selection box Range: Checked, unchecked Default: Unchecked

Changing PDE options

You can only perform this task when logged into the Active Primary NOAM.

1. Select **Tekelec HLR Router** > **Configuration** > **PDE** > **Options**
   The **Tekelec HLR Router** > **Configuration** > **PDE** > **Options**page appears.
2. Edit the fields you want to change.
   For more information about these fields, see *PDE options configuration elements*.
3. Perform one of the following:
   - Click **OK** to save the PDE options configuration and exit this page.
   - Click **Apply** to save the PDE options and remain on this page.

The PDE options are updated.

Tekelec HLR Router maintenance

The **Tekelec HLR Router** > **Maintenance** menu option allows you to run tests on the signaling logic of specified message processors. The menu option is only available when you are logged into an SOAM.

Signaling test maintenance

The **Tekelec HLR Router** > **Maintenance** > **Test** page allows you to test signaling logic on the specified Message Processor. This allows you to see what would happen if a message was received with arbitrary MTP/SCCP parameter values without actually initiating network traffic. The Message can be routed via SCCP or Map Layer Routing.

To run a test you input an OPC, DPC, CdPA TT, CdPA SSN, CdPA/Map Layer NAI, Map Layer Digit Type, CdPA GTA/Map Layer Digits and then select the MP to run the test on. The test runs the application routing logic on the selected MP. This is not the live routing logic, so no measurements or alarms are triggered, but the test makes the same decisions as the live routing logic based on the configuration of the HLR Router.

After the test is run the following information is displayed on the GUI:

- An explanation of its routing decisions including what values it based the decisions on.
- The result of all database lookups, including the inputs to the lookup.
- The destination to which the output message would have been sent.

This page is only available when logged into an SOAM.

Signaling maintenance test

Table 55: Tekelec HLR Router Maintenance Test

Element	Description	Data Input Notes
Originating Point Code	Numeric address that identifies the originating signaling point	Format: alphanumeric Range: 1 - 11 characters
Destination Point Code	Numeric address that identifies the destination signaling point	Format: alphanumeric Range: 1 - 11 characters
CdPA Translation Type	Called Party Translation Type	Format: numeric Range: between 1 and 255
CdPA Subsystem Number	Called Party Subsystem Number	Format: numeric Range: between 0 and 255
CdPA / MAP layer NAI	Called Party NAI or NAI of digits carried in the MAP layer	Format: Pulldown menu Range: National, International Default: National
Map Layer DT	Type of digits carried in the MAP Layer.	Format: Pulldown menu Range: N/A, IMSI, ND Default: N/A

Element	Description	Data Input Notes
CdPA GTA / Map Layer Digits	Called Party Global Title Address or Map Layer Digits	Format: numeric Range: 8 - 15 digits IMSI 10-15 or DN 8-15 Digits
MP	Message Processor on which to test the signaling logic	Format: Pulldown menu Range: Available Message processors

Running a signaling maintenance test

You can only perform this task when logged into an SOAM.

1. Select **Tekelec HLR Router** > **Maintenance** > **Test**
   The **Tekelec HLR Router** > **Maintenance** > **Test** page appears.
2. Enter the originating point code in the **Originating Point Code** field.
3. Enter the destination point code in the **Destination Point Code** field.
4. Enter the called party translation type in the **CdPA Translation Type** field.
5. Enter the called party subsystem number in the CdPA Subsystem Number field.
6. Select the called party or map layer nature of address indicator from the CdPA/Map layer NAI pulldown.
7. Select the Map Layer Digit Type from the Map Layer Digit Type pulldown. Select IMSI or DN for Map Layer Routing only.
8. Enter the called party global title address or Map Layer Digits in the **CdPA Global Title Address/Map Layer Digits** field.
9. Select the message processor to test the signaling logic on from the **MP** pulldown.
10. Click **Test**.
    The signaling test results are displayed on the page.

The signaling test is run and the results are displayed on the page.

C

CC	Country Code
CSV	Comma-Separated Values The comma-separated value file format is a delimited data format that has fields separated by the comma character and records separated by newlines (a newline is a special character or sequence of characters signifying the end of a line of text).

D

DN	Directory number A DN can refer to any mobile or wireline subscriber number, and can include MSISDN, MDN, MIN, or the wireline Dialed Number.
DPC	Destination Point Code - DPC refers to the scheme in SS7 signaling to identify the receiving signaling point. In the SS7 network, the point codes are numeric addresses which uniquely identify each signaling point. This point code can be adjacent to the EAGLE, but does not have to be.

G

GSM	Global System for Mobile Communications A second generation digital PCS mobile phone standard used in many parts of the world.

G

GT	Global Title Routing Indicator
GUI	Graphical User Interface The term given to that set of items and facilities which provides you with a graphic means for manipulating screen data rather than being limited to character based commands.

H

HLR	Home Location Register A component within the Switching Subsystem of a GSM network. The HLR database is the central database within the GSM architecture. This is where information about the mobile communications subscribers who are assigned to a specific location area is stored. The subscriber data is used to establish connections and control services. Depending on the network size, the number of subscribers and the network organization, a number of HLRs can exist within a GSM network.

I

IMSI	International Mobile Station Identity A unique internal network ID identifying a mobile subscriber.
IP	Internet Protocol - IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides

I

packet routing, fragmentation and re-assembly through the data link layer.

M

MCC

Mobile Country Code

A three-digit number that uniquely identifies a country served by wireless telephone networks. The MCC is part of the International Mobile Subscriber Identity (IMSI) number, which uniquely identifies a particular subscriber. See also MNC, IMSI.

MNC

Mobile Network Code

A number that identifies a mobile phone carrier. Used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator/carrier. See also MCC.

MP

Message Processor - The role of the Message Processor is to provide the application messaging protocol interfaces and processing. However, these servers also have OAM components. All Message Processors replicate from their Signaling OAM's database and generate faults to a Fault Management System.

MSC

Mobile Switching Center

An intelligent switching system in GSM networks. This system establishes connections between mobile communications subscribers.

The primary service delivery node for GSM/CDMA, responsible for

M

	routing voice calls and SMS as well as other services (such as conference calls, FAX and circuit switched data).
MTP	Message Transfer Part The levels 1, 2, and 3 of the SS7 protocol that control all the functions necessary to route an SS7 MSU through the network

N

NDC	Network Data Collection
NE	Network Element An independent and identifiable piece of equipment closely associated with at least one processor, and within a single location. In a 2-Tiered DSR OAM system, this includes the NOAM and all MPs underneath it. In a 3-Tiered DSR OAM system, this includes the NOAM, the SOAM, and all MPs associated with the SOAM. The devices, servers, or functions within a wireless network with which Policy Management systems interact.
NOAM	Network Operations, Administration, and Maintenance
NPA	Number Plan Area The North American “Area Codes.” (3 digits: 2- to-9, 0 or 1, 0-to-9. Middle digit to expand soon).

O

OPC	Within an SS7 network, the point codes are numeric addresses which uniquely identify each signaling point. The OPC identifies the sending signaling point.
Opcode	Operation Code An identification of the operation performed by the GSM message.

P

PDBI	Provisioning Database Interface The interface consists of the definition of provisioning messages only. The customer must write a client application that uses the PDBI request/response messages to communicate with the PDBA.
PDP	Permissive Dialing Period

S

SCCP	Signaling Connection Control Part The signaling connection control part with additional functions for the Message Transfer Part (MTP) in SS7 signaling. Messages can be transmitted between arbitrary nodes in the signaling network using a connection-oriented or connectionless approach.
SOAM	System Operations, Administration, and Maintenance

T

TCAP	Transaction Capabilities Application Part

T

	A protocol in the SS7 protocol suite that enables the deployment of advanced intelligent network services by supporting non-circuit related information exchange between signaling points using the Signaling Connection Control Part connectionless service. TCAP also supports remote control - ability to invoke features in another remote network switch.
Throttling	A mechanism to limit the number of messages being routed to a particular destination based on the various factors, like Event Type, Event Origination, Event Destination, and Shed Rate.

U

UDT	Unitdata Transfer