Oracle® Communications Tekelec HLR Router

HLR Router Administration Guide

910-6571-001 Revision B

February 2014

ORACLE®

Oracle® Communications HLR Router Administration Guide

Table of Contents

Chapter 4: Query Server..85

Chapter 5: File Formats...92

List of Figures

List of Tables

Chapter

1

Introduction

Topics:

This section describes the organization of the manual and provides other information that could be useful to the reader.

Purpose of this document

This document provides administrative information for the EAGLE XG HLR Router application including:

- A functional description of the product
- System configuration information
- Information about using Query Server
- General, provisioning, and SS7/Sigtran script commands
- File formatting information

Scope and Audience

The *HLR Router Administration Guide* and HLR Router Administration Help are intended for anyone responsible for configuring and using the EAGLE XG HLR Router.

Users of this guide must have a working knowledge of telecommunications and network installations.

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	**Danger**: (This icon and text indicate the possibility of *personal injury*.)
WARNING	**Warning**: (This icon and text indicate the possibility of *equipment damage*.)
CAUTION	**Caution**: (This icon and text indicate the possibility of *service interruption*.)

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

Document Organization

This *HLR Router Administration Guide* is organized into the following chapters:

- *Introduction* contains general information about the *HLR Router Administration Guide*, the scope, audience, and organization of this document, how to contact Tekelec for assistance, and how to locate documentation on the Customer Support Site.
- *Functional Description* describes the functions, system architecture, user interface, and distributed configuration of the HLR Router.
- *HLR Router Configuration* describes HLR Router system, PDBI, Transport Manager, and signaling configuration.
- *Query Server* describes the functions of the SQL Query Server.
- *File Formats* describes HLR Router import and export file name formats, signaling reports, and PDE CSV file formats.

Customer Care Center

The Tekelec Customer Care Center is your initial point of contact for all product support needs. A representative takes your call or email, creates a Customer Service Request (CSR) and directs your requests to the Tekelec Technical Assistance Center (TAC). Each CSR includes an individual tracking number. Together with TAC Engineers, the representative will help you resolve your request.

The Customer Care Center is available 24 hours a day, 7 days a week, 365 days a year, and is linked to TAC Engineers around the globe.

Tekelec TAC Engineers are available to provide solutions to your technical questions and issues 7 days a week, 24 hours a day. After a CSR is issued, the TAC Engineer determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, normal support procedures apply. A primary Technical Engineer is assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Tekelec Technical Assistance Centers are located around the globe in the following locations:

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

  1-888-367-8552 (toll-free, within continental USA and Canada)

1-919-460-2150 (outside continental USA and Canada)

TAC Regional Support Office Hours:

8:00 a.m. through 5:00 p.m. (GMT minus 5 hours), Monday through Friday, excluding holidays

- **Caribbean and Latin America (CALA)**

  Phone:

  +1-919-460-2150

  TAC Regional Support Office Hours (except Brazil):

  10:00 a.m. through 7:00 p.m. (GMT minus 6 hours), Monday through Friday, excluding holidays

  - **Argentina**

    Phone:

    0-800-555-5246 (toll-free)

  - **Brazil**

    Phone:

    0-800-891-4341 (toll-free)

    TAC Regional Support Office Hours:

    8:00 a.m. through 5:48 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

  - **Chile**

    Phone:

    1230-020-555-5468

  - **Colombia**

    Phone:

    01-800-912-0537

  - **Dominican Republic**

    Phone:

    1-888-367-8552

  - **Mexico**

    Phone:

    001-888-367-8552

  - **Peru**

    Phone:

    0800-53-087

  - **Puerto Rico**

    Phone:

    1-888-367-8552

- **Venezuela**

  Phone:

  0800-176-6497

- **Europe, Middle East, and Africa**

  Regional Office Hours:

  8:30 a.m. through 5:00 p.m. (GMT), Monday through Friday, excluding holidays

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**

  - **India**

    Phone:

    +91-124-465-5098 or +1-919-460-2150

    TAC Regional Support Office Hours:

    10:00 a.m. through 7:00 p.m. (GMT plus 5 1/2 hours), Monday through Saturday, excluding holidays

  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

    9:00 a.m. through 6:00 p.m. (GMT plus 8 hours), Monday through Friday, excluding holidays

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. 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 the Tekelec Customer Care Center.

Related Publications

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

Getting Started includes a product overview, system architecture, and functions. It also explains the EAGLE XG HLR Router GUI features including user interface elements, main menu options, supported browsers, and common user interface widgets. Available from the application GUI and on the documentation DVD.

Feature Notice describes new features in the current release, provides the hardware baseline for this release, and explains how to find customer documentation on the Customer Support Site. Available from the application GUI and on the documentation DVD.

Operation, Administration, and Maintenance (OAM) Guide provides information on system-level configuration and administration tasks for the advanced functions of the EAGLE XG 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 EAGLE XG HLR Router. Available from the application GUI and on the documentation DVD.

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. Available from the application GUI and on the documentation DVD.

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. Available from the application GUI and on the documentation DVD.

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. Available from the application GUI and on the documentation DVD.

Transport Manager User Guide describes the configuration of "Transports" (SCTP associations and UDP connections with remote hosts over an underlying IP network). Available from the application GUI and on the documentation DVD.

Locate Product Documentation on the Customer Support Site

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a document. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the *Tekelec Customer Support* site.

   Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.

2. Click the **Product Support** tab.
3. Use the Search field to locate a document by its part number, release number, document name, or document type. The Search field accepts both full and partial entries.
4. Click a subject folder to browse through a list of related files.
5. To download a file to your location, right-click the file name and select **Save Target As**.

Chapter
2

Functional Description

Topics:

This section provides a description of the HLR design, features, and user interfaces.

Introduction to EAGLE XG HLR Router

The Eagle XG HLR Router aids the optimization of HLR workloads over mobile networks by providing a centralized database of subscriber to HLR mappings. This allows mobile network operators to optimize the workloads of HLRs by pairing subscribers with HLRs based on their signaling activity patterns. It also optimizes capacity for each HLR by allowing subscriber ranges to be split over different HLRs and allows individual subscribers to be assigned to any HLR.

Additionally, the HLR eliminates the need to maintain subscriber routing information at every MSC in the network. When an HLR record is needed, the MSC routes the request to the HLR. The HLR uses global title translation to determine the correct HLR for the subscriber and sends the MSC request to that HLR. The HLR also provides the ability to route to mated HLRs based on SS7 network status, and to route to a default HLR if no translations exist for a given subscriber via exception routing. Not only does this eliminate the need to maintain subscriber routing information at every MSC in the network, this also allows great flexibility in distributing or redistributing subscribers across available HLRs.

This introduction will familiarize you with the basic operation, features, and components of the EAGLE XG HLR Router.

HLR Router functionality

The EAGLE XG HLR Router provides the following functionality:

- SCCP message relay functions for HLR Routing
- PDBI provisioning allowing independent information systems to add, delete, change or retrieve information about any IMSI, DN, or Network Entity association
- The ability to add an NPA to a region using NPA Splits
- On-demand ability to initiate an audit of the remote EPAP provisioning database, and flag differences found between the EPAP and the HLR databases
- Automatic provisioning of blacklist entries for new Network Entities
- Efficient and flexible MTP3-style routing of SS7 signaling between MSCs and HLRs
- A Mate Network Entities table that contains preferred and mate relationships that allows rerouting to a Mate Network Entity if the primary is not available
- Ability to throttle the amount of any GSM messages destined to the HLR
- Exception routing of messages that do not find a successful translation in the provisioning database
- The ability for a remote client to run adhoc, read-only queries on a provisioned database using Query Server
- Geographically independent Disaster Recovery NOAMP servers that can, upon activation, take over the responsibilities of the main NOAMP
- Enhanced application security via the ability to manage the administration of accounts, logins, and passwords
- Real-time alarms and alarm history availability
- The ability to capture and preserve vital collections of configured data using manual and/or automatic backups
- Automatic file-based bulk import of provisioning data on the NOAMP
- Map Layer Routing (MLR) to activate or deactivate the map layer routing feature
- On-demand ability to collect performance data on HLR Router

- Access to the Secure Active Network Environment (SANE)

System Architecture

The EAGLE XG HLR Router consists of an active/standby pair of NOAMP servers in an HA configuration, a third NOAMP server configured as a Query Server (optional), an optional DR NOAMP, redundant SOAM servers, and up to 10 MP (Message Processor SCCP Relay Point) servers per SOAM site. An EAGLE XG HLR Router can have up to 40 sites with each capable of supporting up to 512 remote signaling points.

Figure 1: EAGLE XG HLR Router System Diagram provides an overview of the EAGLE XG HLR Router architecture.
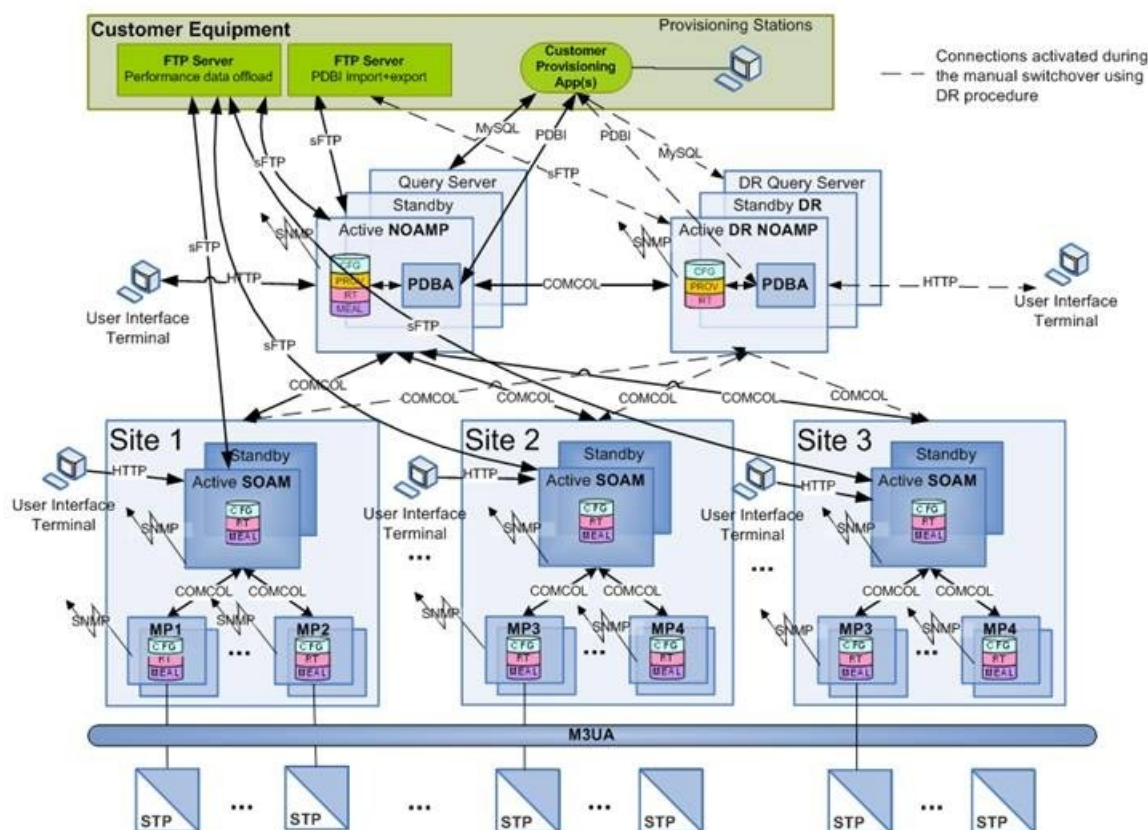
Figure 1: EAGLE XG HLR Router System Diagram

HLR Router Components

NOAMP

The NOAMP component consists of one active NOAMP and one standby NOAMP server running in a high availability configuration. It accepts subscriber data provisioned by the customer over PDBI

and replicates it to the DR NOAMP, the Query Server and all subtending SOAMs. It also provides a GUI which is used for configuration, user administration and the viewing of alarms and measurements.

NOAMP distributes all successful incoming subscriber provisioning data, independent of source, to all downstream Network Elements and the DR NOAMP at a rate of up to 200 provisioning database updates per second. In order to ensure the database levels of the Network Elements are less than the database levels of the NOAMP and DR NOAMP, the active provisioning site NOAMP provisions the DR NOAMP prior to updating the Network Elements.

DR NOAMP (Optional)

The DR NOAMP is a geographically independent NOAMP component. The DR NOAMP has the same hardware configuration and network accessibility as the NOAMP.

The DR NOAMP's databases are kept up to date through real-time replication of subscriber and application data from the Active NOAMP. Under normal operating conditions, the DR NOAMP does not provision any downstream systems but if made Active, it will take over all the functions of the Active NOAMP including the PDBI and database replication to subtending SOAMs.

SOAM

The SOAM component consists of one active SOAM and a standby SOAM server running in a high availability configuration. It accepts subscriber data replicated from the Active NOAMP and in turn replicates it to all subtending MPs located in the same physical frame. SOAM also provides a GUI used for local Signaling configuration and viewing alarms and measurements details specific to components located within the frame (SOAM, MP).

The SOAM supports up to 10 MPs.

Query Server (Optional)

The Query Server is an independent application server containing a replicated version of the PDBI database. It accepts replicated subscriber data from the NOAMP and stores it in a customer accessible MySQL database. A Query Server is located in the same physical frame as each NOAMP component (NOAMP / DR NOAMP).

Network Element

Network Elements are containers that group and create relationships between servers in the network. There are two types of Network Elements:

• NOAMP: such as the NOAMP and the DR NOAMP
• Signaling: contains a pair of SOAM servers and one or more MP servers

The system can support two NOAMP Network Elements and up to 40 Signaling Network Elements.

MPs

The MPs are servers with the HLR Router application installed that are configured for MP functionality. They accept replicated subscriber data from the local SOAM and store it in a subscriber database.

The MP is accessed as a Service Relay Point and is connected to the Eagle STPs via Sigtran M3UA interfaces. Each MP is capable of relaying real-time SCCP messages at a maximum sustained rate of 20,000 (15,000 for MLR) transactions per second for HLR routing lookups. Multiple MP servers may be deployed in a single frame in order to scale query capacity. Each site can support up to 10 MPs, but the HLR Router System can support up to a total of 96 MPs in the system.

User interface introduction

This section describes the organization and usage of the application user interface. In it you can find information about how the interface options are organized, how to use widgets and button, and how filtering and other page display options work.

User interface organization

The user interface is the central point of user interaction with the application. It is a Web-based graphical user interface (GUI) that enables remote user access over the network to the application and its functions.

Main menu options

The menu options that appear on the screen differ according to whether you are logged into an NOAMP or SOAM. This table describes all main menu user interface options. For a list of NOAMP menu options please see *Centralized configuration*. For a list of SOAM menu options please see *Decentralized configuration*.

Note: The menu options can differ according to the permissions assigned to a user's log-in account. For example, the Administration menu options would not appear on the screen of a user who does not have administrative privileges.

Menu Item	Function
Administration	The Administration menu allows you to: • Set up and manage user accounts • Configure group permissions • View session information • Authorize IP addresses to access the user interface • Configure options including, but not limited to, password history and expiration, login message, welcome message, and the number of failed login attempts before an account is disabled • Configure SNMP services • Validate and transfer ISO files • Prepare, initiate, monitor, and complete upgrades • View the software versions report
Configuration	Provides access to configuring network elements, servers, server groups, and systems.
Alarms and Events	Lists active alarms and alarm history.
Security Log	Allows you to view and export security log data.

Menu Item	Function
Status & Manage	Allows you to monitor the statuses of server processes, both collectively and individually, as well as perform actions required for server maintenance. Also allows you to view the status of file management systems, and to manage data files on servers throughout the system.
Measurements	Allows you to view, modify, import, and export measurement data.
SS7/Sigtran	Provides maintenance and configuration options for the Signaling Network Interface. This provides standard SCCP functionality, traditional MTP3 routing capabilities, and a standard M3UA interface to the external network. **Note:** The SS7/Sigtran menu option is only available when logged into an SOAM.
Transport Manager	Enables the configuration of Transports (SCTP associations and UDP connections with remote hosts over an underlying IP network).
EAGLE XG Database	Provides maintenance and configuration options related to HLR Routing. **Note:** The EAGLE XG HLR Router options differ depending on the type of server a user is logged into.
EAGLE XG HLR Router	Provides maintenance and configuration options related to HLR **Note:** The EAGLE XG HLR Router options differ depending on whether a user is logged in to a NOAMP or SOAM.
Help	Launches the online help system for the user interface.
Logout	Allows you to log out of the user interface.

Distributed configuration

The EAGLE XG HLR Router supports centralized and decentralized configurations:

- Centralized configuration:
  - All subscriber data configuration and maintenance occurs at the NOAMP level
  - Application management, such as configuring servers, occurs at the NOAMP level

- Decentralized:

    - All signaling network configuration and maintenance occurs on the SOAM level

Due to distributed configuration:

- Most OAM Administration, Configuration, and Status & Manage tasks can only be performed when you are logged into an active NOAMP
- EAGLE XG Database and EAGLE XG HLR Router tasks related to the subscriber database are only available when logged into an active NOAMP, with the exception of querying the database
- EAGLE XG Database and EAGLE XG HLR Router tasks related to signaling are only available when logged into an active SOAM
- All SS7/Sigtran Main Menu options are only available when you are logged into an SOAM
- The available Alarms, KPIs, Measurements, and Events vary depending on whether you are logged into an NOAMP or SOAM

Centralized configuration

Subscriber provisioning data is provisioned at the active server of the Primary NOAMP cluster and replicated to all servers on the network. System configuration and subscriber data is provisioned at the active server of the Primary NOAMP cluster, replicated to all other NOAMPs, and then replicated to the active SOAM of each Network Element (NE).

PDBI

The main method of subscriber data provisioning is PDBI (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, independent information systems may add, delete, change or retrieve information about any IMSI, DN, or Network Entity association.

GUI Provisioning

Local provisioning can be done using the HLR Router GUI. The GUI can be used to manage PDBI setup, to make direct changes to the subscriber database entries, and to perform application operations, management, and provisioning.

This table shows the GUI options available when logged into an NOAMP.

Table 2: NOAMP Main Menu Options

Menu Item	Function

Administration	All options available:
	
	• Users
	• Groups
	• Sessions
	• Single Sign-On
	
	    • LDAP Servers
	    • Zones

Menu Item	Function
	• Authorized IPs • Options • SNMP • ISO • Upgrade • Software Versions • Export Server
Configuration	All options available: • Network Elements • Services • Servers • Server Groups • Network 　• Devices 　• Routes
Alarms & Events	All options available: • View Active • View History • View Trap Log
Security Log	All options available: • View History
Status & Manage	All options available: • Network Elements • Server • Replication • Collection • HA • Database • KPIs • Processes • Tasks 　• Active Tasks 　• Scheduled Tasks • Files
Measurements	All options available: • Report
EAGLE XG Database	• Configuration:

Menu Item	Function
	- Network Entity - DN - IMSI - PDBI - Options - Connections - Blacklist - Export - Maintenance: - Audit - Request - Status - Query - Network Entity - DN - IMSI - PDBI - Connections - Command Log - Import Status - Export Status - Remote Audit - Run Command - DB Status - NPA Splits
EAGLE XG HLR Router	Configuration: - Options - Service Config - Substitutions - Mated Entities - Throttling - DN Whitelist - IMSI Whitelist - MP Groups - Opcodes - Rules - Rule Test - PDE

Menu Item	Function
	• Options

Decentralized configuration

Since each Network Element may have different signaling network connectivity, different routes, etc. signaling and application site-specific configuration data is configured at the SOAM. The SOAM servers provide provisioning control over multiple Message Processors (SCCP Relay Points), for the SS7 Signaling Network Interface, and for HLR routing configuration.

The SOAM replicates system configuration, signaling and application site-specific configuration, and real-time data to the MPs. Measurements, Events, Alarms, and Logs from active/standby SOAM, and all MPs in the local Network Element, are merged to the active server of the Primary NOAMP cluster.

This table shows the GUI options available when logged into an SOAM.

Table 3: SOAM Main Menu Options

Menu Item	Function
Administration	Most **Administration** submenu functions are only permissible from an active, primary NOAMP server. However, these options may be fully utilized from an SOAM: • ISO • Software Version • Export Server
Configuration	Provisioning functions are only permissible from an active, primary NOAMP server.
Alarms & Events	All options are available: • View Active • View History • View Trap Log
Security Log	All options are available: • View History
Status & Manage	Most **Status & Manage** submenu functions are available on an SOAM. However, these options are only permissible from an active, primary NOAMP server: • Network Elements • HA
Measurements	• Report
Transport Manager	• Configuration

Menu Item	Function
	• Adjacent Node • Configuration Set • Transport • Maintenance • Transport

SS7/Sigtran	All options are available:
	
	• Configuration
	
	    • Adjacent Server Groups
	    • Local Signaling Points
	    • Local SCCP Users
	    • Remote Signaling Points
	    • Remote MTP3 Users
	    • Link Sets
	    • Links
	    • Routes
	    • SCCP Options
	    • MTP3 Options
	    • M3UA Options
	    • Local Congestion Options
	    • Capacity Constraint Options
	
	• Maintenance
	
	    • Local SCCP Users
	    • Remote Signaling Points
	    • Remote MTP3 Users
	    • Linksets
	    • Links
	
	• Command Line Interface
	
	    • Command Import

EAGLE XG Database	Maintenance:
	
	• Query
	
	    • Network Entity
	    • DN
	    • IMSI

EAGLE XG HLR Router	Configuration: • Exception Routing • MP E.164 Maintenance:

Menu Item	Function
	• Test

Chapter
3

HLR Router Configuration

Topics:

This section provides information about HLR Router application configuration.

System configuration

The system configuration section describes activities that occur after hardware installation.

Network

The Network pages allow the user to configure signaling networks, devices, and routes. Through the Network Configuration page, network IDs and subnets can be added to enable servers to communicate with the signaling networks. Route configuration allows the user to define specific routes for signaling traffic. Device configuration allows the user to configure additional interfaces on MP servers used in signaling networks.

Network Insert elements

This table describes the elements of the Network Insert page.

Table 4: Network Insert Elements

Field	Description	Data Input Notes
Network Name	The name of the Network	Format: Alphanumeric; must begin with a letter Range: 31 character maximum
VLAN ID	The VLAN ID of the Network	Format: Numeric Range: 5-4094 **Note:** VLAN IDs 1-4 are reserved for Management, XMI, and IMI. VLAN IDs that are already in use cannot be reused.
Network Address	The network address of the Network	Format: Valid network address Range: Dotted decimal (IPv4) or colon hex (IPv6)
Netmask	Subnetting to apply to servers within the Network	Range: Valid netmask for the network in prefix length (IPv4 or IPv6) or dotted quad decimal (IPv4)

Inserting a Network

Use the following procedure for inserting a network. Alternatively, you can also use the procedures included in the Network Elements topics.

1. Select **Configuration > Network**
    The **Network** page appears.
2. Click the **Insert** button.
    The **Network Insert** page appears.
3. Enter a **Network Name**.

    For more information about **Network Name**, or any field on this page, see *Network Insert elements*
    .
4. Enter a **VLAN ID**.
5. Enter a **Network Address**.
6. Enter a **Netmask**.
7. Click **OK** to submit the information and return to the Network page, or click **Apply** to submit the information and continue entering additional data.

The new network is added.

Configuration Network elements

This table describes the elements of the **Configuration Network** page.

Table 5: Configuration Network Elements

Field	Description
Network Name	The name associated with the network
VLAN	VLAN ID associated with the network
Network	The IP address associated with the network in the format: IP Address/Prefix Length

Editing a Network

Not all networks can be edited. Pre-configured networks created during the install process, for example, cannot be edited. A network that cannot be edited is distinguished using italic font.

Note: Prior to editing a network, generate a network report. The network report will serve as a record of the network's original settings. Print or save the network report for your records. For more information about generating a network report, see *Generating a Network Report*.

1. Select **Configuration > Network**
    The **Network** page appears.
2. Click to select a network and click **Edit.**

    Note: If the network cannot be edited, the **Edit** button will be disabled.

    If the network can be edited, the **Network Edit** page appears.

3. Edit the available fields as necessary.

    See *Network Insert elements* for details about the fields that appear on this page.

    Note: Fields that cannot be edited are disabled.

4. Click **OK** to submit the changes and return to the **Network** page, or click **Apply** to submit the information and continue editing additional data.

The network is changed.

Deleting a Network

Not all networks can be deleted. In-use networks and pre-configured networks created during the install process, for example, cannot be deleted. A network that cannot be deleted is distinguished using italic font.

Note: Prior to deleting a network, generate a network report. The network report will serve as a record of the network's original settings. Print or save the network report for your records. For more information about generating a network report, see *Generating a Network Report*.

1. Select **Configuration > Network.**
    The **Network** page appears.
2. Click to select the network you want to delete. Alternately, you can delete multiple networks. To delete multiple networks, press and hold **Ctrl** and click to select specific networks.

    Note: If the network cannot be deleted, the **Delete** button will be disabled.

    Note: To delete multiple networks at one time, all selected networks must be deletable.

3. Click **Delete**.
    A confirmation box appears.
4. Click **OK** to delete the network.
    The network is deleted.

Generating a Network Report

A network report provides a summary of the configuration of one or more networks. Reports can be printed or saved to a file.

1. Select **Configuration > Network**
    The **Network** page appears.
2. Click **Report** to generate a report for all networks. To generate a report for a single network, click to select the network and click **Report**. Alternately, you can select multiple networks. To generate a report for multiple networks, press and hold **Ctrl** as you click to select specific networks.
    The Network Report is generated.
3. Click **Print** to print the report.
4. Click **Save** to save the report to a file.

Devices

Device configuration allows the user to configure interfaces on MP servers used in signaling networks.

Device Insert elements

This table describes the elements of the Devices Insert page.

Table 6: Devices General Options

Field	Description	Data Input Notes
Device Type	The type of device	Format: Radio button Range: Ethernet, Bonding, VLAN, Alias **Note:** Ethernet is not selectable.
Device Monitoring	The monitoring style to use with a bonding device	Format: Pulldown list Default: MII Range: MII, ARP **Note:** Device Monitoring is disabled when the Device Type is not Bonding.
Start on Boot	When selected, this checkbox enables the device to start on boot.	Format: Checkbox Default: Enabled
Boot Protocol	The boot protocol	Format: Pulldown list Range: None, DHCP Default: None
Base Device(s)	The base device(s) for Bond, Alias, and VLAN device types **Note:** Alias and VLAN devices require one selection; bond devices require two selections.	Format: Checkbox Range: Available base devices

The **MII Monitoring Options** and **ARP Monitoring Options** tabs collect settings for MII and ARP monitoring, respectively. The **IP Interfaces** tab allows interfaces to be associated with a device.

Table 7: Devices MII Monitoring Options tab

Field	Description	Data Input Notes
Primary Interface	The preferred primary interface	Format: Pulldown list Range: None and available devices Default: None

Field	Description	Data Input Notes
Monitoring Interval	MII monitoring interval in milliseconds	Range: A positive integer Default: 100ms
Upstream Delay	MII monitoring upstream delay in milliseconds	Range: A positive integer Default: 200ms
Downstream Delay	MII monitoring downstream delay in milliseconds	Range: A positive integer Default: 200ms

Table 8: Devices ARP Monitoring Options tab

Field	Description	Data Input Notes
Primary Interface	The preferred primary interface	Format: Pulldown list Range: Available devices
Monitoring Interval	ARP monitoring interval in milliseconds	Range: A positive integer Default: 100ms
ARP Validation	The method to validate the ARP probes and replies	Format: Pulldown list Range: None, Active, Backup, All Default: None
ARP Target List	Comma-separated ARP target IP addresses	Format: Valid IP address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)

Table 9: Devices IP Interfaces tab

Field	Description	Data Input Notes
IP Address List	The IP address of the interfaces associated with the device	Format: Valid IP address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)
Add Row	Displays a textbox to add an IP Address	Format: Button **Note:** Multiple rows can be added.
IP Address textbox	Textbox for an IP address	Format: Textbox Range: Dotted quad decimal (IPv4) or colon hex (IPv6)

Field	Description	Data Input Notes
Remove	Removes the device interface IP Address on the selected row	Format: Button

Inserting a Device

Devices cannot be created which use management networks (those configured after installation and designated in the Network listing in blue italic text). This ensures continued access to the GUI via the management networks.

1. Select **Configuration > Network > Devices**.
   The **Devices** page appears.

2. Select a server.

3. Click the **Insert** button.
   The **Device Insert** page appears.

4. Select a **Device Type**.

   For more information about **Device Type**, or any field on this page, see *Device Insert elements* .

   Note: Device Type of Ethernet cannot be selected.

5. Select a **Device Monitoring** style.

   Note: Device Monitoring is only used when the Device Type is Bonding.

6. By default, **Start on Boot** is enabled. Uncheck the check box if you want to disable **Start on Boot**.

7. Select the **Boot Protocol**.

8. Select the **Base Device(s)** if the device type is one of the following: Bond, Alias, or VLAN.

   Note: Alias and VLAN devices require one selection; bond devices require two selections.

9. Click **OK** to submit the information and return to the Device page, or click **Apply** to submit the information and continue entering additional data.

The device is added. You can now update MII and ARP monitoring options and add IP interfaces, if applicable.

Inserting MII Monitoring Options

Inserting MII monitoring options is only required if the device type is Bonding. For all other device types, the **MII Monitoring Options** tab is disabled.

1. Select **Configuration > Network > Devices**.
   The **Devices** page appears.

2. Select a server.

3. Click the **Insert** button.
   The **Device Insert** page appears.

4. Click the **MII Monitoring Options** tab.
   The **MII Monitoring Options** tab appears.

5. Click **Primary Interface** to select None (for no interface) or the preferred interface from the pulldown list.

6. Enter the **Monitoring Interval**, if you do not wish to use the default setting.

7. Enter the **Upstream Delay**, if you do not wish to use the default setting.

8. Enter the **Downstream Delay**, if you do not wish to use the default setting.

9. Click the **General Options** tab.

10. Click **OK** to submit the information and return to the Device page, or click **Apply** to submit the information and continue entering additional data.

The MII monitoring options are updated.

Inserting ARP Monitoring Options

Inserting ARP monitoring options is only required if the device type is Bonding. For all other device types, the **ARP Monitoring Options** tab is disabled.

1. Select **Configuration > Network > Devices**.
   The **Devices** page appears.

2. Select a server.

3. Click the **Insert** button.
   The **Device Insert** page appears.

4. Click the **ARP Monitoring Options** tab.
   The **ARP Monitoring Options** tab appears.

5. Click **Primary Interface** to select None (for no interface) or the preferred interface from the pulldown list.

6. Enter the **Monitoring Interval**, if you do not wish to use the default setting.

7. Click **ARP Validation** to select a validation method from the pulldown list, if you do not wish to use the default setting.

8. Enter one or more IP addresses for the target device.

   Note: Multiple IP addresses are comma separated.

9. Enter an IP Address for the device.

10. Click **OK** to submit the information and return to the Device page, or click **Apply** to submit the information and continue entering additional data.

The ARP monitoring options are updated.

Inserting IP Interfaces

The IP interfaces tab allows interfaces to be associated with a device.

1. Select **Configuration > Network > Devices**.
   The **Devices** page appears.

2. Select a server.

3. Click the **Insert** button.
   The **Device Insert** page appears.

4. Click the **IP Interfaces** tab.
   The **IP Interfaces** tab appears.

5. Click **Add Row**.
   A textbox appears in which you can enter an IP Address for the device.

6. Enter an **IP Address** for the device.

7. Select a **Network Name**.

8. For each row, only one IP Address and Network Name can be specified. To specify additional rows, select **Add Row** and following Steps 6 and 7.

9. When you are finished adding IP Addresses, click **OK** to submit the information and return to the Device page, or click **Apply** to submit the information and continue entering additional data.

The IP addresses are added.

Devices elements

This table describes the elements of the **Configuration Devices** page.

Table 10: Devices Elements

Field	Description
Server	The server host name displayed in tabbed format at the top of the table
Device Name	The name of the device
Device Type	The device type. Supported types include: • Bonding • VLAN • Alias • Ethernet
Device Options	A collection of keyword value pairs for the device options
IP Interface (Network)	IP address and network name in the format: IP Address (network name)
Configuration Status	The configuration status of the device. The possible states are: • Discovered (provisioned directly on the server) • Configured (provisioned through the GUI; server update is complete) • Pending (update in progress) • Deferred (server cannot be reached for updates) • Error (specific error text is displayed in the Configuration Status field)

Editing a Device

Not all devices can be edited. Pre-configured devices created during the install process, for example, cannot be edited. A device that cannot be edited is distinguished using italic font.

Note: Prior to editing a device, generate a device report. The device report will serve as a record of the device's original settings. Print or save the device report for your records. For more information about generating a device report, see *Generating a Device Report*.

1. Select **Configuration > Network > Devices**
   The **Devices** page appears.
2. Click to select a server.
   The device data for the selected server appears.
3. Click to select a device and click **Edit.**

   Note: If the device cannot be edited, the **Edit** button will be disabled.

If the device can be edited, the **Device Edit** page appears.

4. Edit the available fields as necessary.

   See *Device Insert elements* for details about the fields that appear on this page.

   Note: Fields that cannot be edited are disabled.

5. Click **OK** to submit the changes and return to the **Devices** page, or click **Apply** to submit the information and continue editing additional data.

The device is changed.

Deleting a Device

Not all devices can be deleted. In-use devices and pre-configured devices created during the install process, for example, cannot be deleted. A device that cannot be deleted is distinguished using italic font.

Note: Prior to deleting a device, generate a device report. The device report will serve as a record of the device's original settings. Print or save the device report for your records. For more information about generating a device report, see *Generating a Device Report*.

1. Select **Configuration > Network > Devices.**
   The **Devices** page appears.
2. Click to select a server.
   The device data for the selected server appears.
3. Click to select the device you want to delete. Alternately, you can delete multiple devices. To delete multiple devices, press and hold **Ctrl** and click to select specific devices.

   Note: If the device cannot be deleted, the **Delete** button will be disabled.

   Note: To delete multiple devices at one time, all selected devices must be deletable.

4. Click **Delete**.
   A confirmation box appears.
5. Click **OK**.
   The device is deleted.

Generating a Device Report

1. Select **Configuration > Network > Devices**
   The **Devices** page appears.
2. Click to select a server.
   The device data for the selected server appears.
3. To generate a report for all devices, click **Report**. To generate a report for a single device, click to select the device and click **Report**. Alternately, you can select multiple devices. To generate a report for multiple devices, press and hold **Ctrl** as you click to select specific devices.
   The Device Report is generated.
4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

Routes

Use the Route Configuration page to define specific routes for signaling traffic. You can specify routes for the entire network, specific servers, or specific server groups.

Routes Insert elements

This table describes the elements of the Routes Insert page. Elements are displayed for the selected server or server group.

Table 11: Routes Insert Elements

Field	Description	Data Input Notes
Route Type	The type of route	Format: Radio button Range: Default, Net, Host **Note:** The Default route option is available only if there is no default route configured on the target server. There can be no more than one IPv4 and one IPv6 default route defined.
Device	The network device name through which traffic is routed	Format: Pulldown list Range: Provisioned devices on the selected server
Destination	The destination network address **Note:** This field is disabled if the **Route Type** is default.	Format: Valid network address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)
Netmask	A valid netmask for the destination network **Note:** This field is disabled if the **Route Type** is default. This field is disabled and set to 32 (IPv4) or 128 (IPv6) if the **Route Type** is host.	Format: Valid netmask Range: Valid netmask for the network in prefix length (IPv4 or IPv6) or dotted quad decimal (IPv4) Default: 24 for IPv4; 64 for IPv6
Gateway IP	The IP Address of the gateway for the route	Format: Valid IP address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)

Inserting a Route

Routes cannot be created which use management networks (those configured after installation and designated in the Network listing in blue italic text). This ensures continued access to the GUI via the management networks.

1. Select **Configuration > Network > Routes**
    The **Routes** page appears.

2. Using the tabs, select to add a server or server group to the entire network, or a specific network group.

3. Click the **Insert** button.
    The **Routes Insert** page appears.

4. Select a **Route Type**.

    For more information about **Route Type**, or any field on this page, see *Routes Insert elements* .

5. Select a **Device**.

6. Enter a **Destination**.

    Note: This step is required only if the **Route Type** is Net or Host. The field is disabled if the **Route Type** is Default.

7. Enter the **Netmask**.

    Note: This step is required only if the **Route Type** is Net. The field is disabled if the **Route Type** is Default or Host.

8. Enter the **Gateway IP**.

9. Click **OK** to submit the information and return to the Route page, or click **Apply** to submit the information and continue entering additional data.

The route is added.

Routes elements

This table describes the elements of the **Configuration Routes** page.

Table 12: Routes Elements

Field	Description
Server/Server Group	The server host name and server groups are displayed in tabbed format at the top of the table
Route Type	The type of route
Destination	The destination network IP address and prefix length in the format: IP Address/Prefix Length
Netmask	A valid netmask for the destination network
Gateway	The IP Address of the gateway for the route
Scope Status	The current number of servers where the route was successfully configured out of the total servers in the server group. (Note: This column is only present for server group routes)

Field	Description
Configuration Status	The configuration status of the route. The possible states are: • Discovered (provisioned directly on the server) • Configured (provisioned through the GUI; server update is complete) • Pending (update in progress) • Deferred (server cannot be reached for updates) • Error (specific error text is displayed in the Configuration Status field)

Editing a Route

Not all routes can be edited. Pre-configured routes created during the install process, for example, cannot be edited. A route that cannot be edited is distinguished using italic font.

Note: Prior to editing a route, generate a route report. The route report will serve as a record of the route's original settings. Print or save the route report for your records. For more information about generating a route report, see *Generating a Route Report*.

1. Select **Configuration > Network > Routes**.
    The **Routes** page appears.
2. Click to select a server or server group using the tabs at the top of the table.
    The route data for the selected server or server group appears.
3. Click to select a route and click **Edit.**

    Note: If the route cannot be edited, the **Edit** button will be disabled.

    If the route can be edited, the **Routes Edit** page appears.
4. Edit the available fields as necessary.
    See *Routes Insert elements* for details about the fields that appear on this page.

    Note: Fields that cannot be edited are disabled.

5. Click **OK** to submit the changes and return to the **Routes** page, or click **Apply** to submit the information and continue editing additional data.

The route is changed.

Deleting a Route

Not all routes can be deleted. In-use routes and pre-configured routes created during the install process, for example, cannot be deleted. A route that cannot be deleted is distinguished using italic font.

Note: Prior to deleting a route, generate a route report. The route report will serve as a record of the route's original settings. Print or save the route report for your records. For more information about generating a route report, see *Generating a Route Report*.

1. Select **Configuration > Network > Routes.**
    The **Routes** page appears.
2. Click to select a server or server group from the tabs at the top of the table.
    The route data for the selected server or server group appears.
3. Click to select the route you want to delete. Alternately, you can delete multiple routes. To delete multiple routes, press and hold **Ctrl** and click to select specific routes.

Note: If the route cannot be deleted, the **Delete** button will be disabled.

Note: To delete multiple routes at one time, all selected routes must be deletable.

4. Click **Delete**.
   A confirmation box appears.
5. Click **OK** to delete the route
   The route is deleted.

Generating a Route Report

1. Select **Configuration > Network > Routes**
   The **Routes** page appears.
2. Click to select a server or server group from the tabs at the top of the table.
3. Click **Report** to generate a report for all routes. To generate a report for a single route, click to select the route and click **Report**. Alternately, you can select multiple routes. To generate a report for multiple routes, press and hold **Ctrl** as you click to select specific routes.
   The Route Report is generated.
4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

Devices

Device configuration allows the user to configure interfaces on MP servers used in signaling networks.

Device Insert elements

This table describes the elements of the Devices Insert page.

Table 13: Devices General Options

Field	Description	Data Input Notes
Device Type	The type of device	Format: Radio button Range: Ethernet, Bonding, VLAN, Alias **Note:** Ethernet is not selectable.
Device Monitoring	The monitoring style to use with a bonding device	Format: Pulldown list Default: MII Range: MII, ARP **Note:** Device Monitoring is disabled when the Device Type is not Bonding.

Field	Description	Data Input Notes
Start on Boot	When selected, this checkbox enables the device to start on boot.	Format: Checkbox Default: Enabled
Boot Protocol	The boot protocol	Format: Pulldown list Range: None, DHCP Default: None
Base Device(s)	The base device(s) for Bond, Alias, and VLAN device types **Note:** Alias and VLAN devices require one selection; bond devices require two selections.	Format: Checkbox Range: Available base devices

The **MII Monitoring Options** and **ARP Monitoring Options** tabs collect settings for MII and ARP monitoring, respectively. The **IP Interfaces** tab allows interfaces to be associated with a device.

Table 14: Devices MII Monitoring Options tab

Field	Description	Data Input Notes
Primary Interface	The preferred primary interface	Format: Pulldown list Range: None and available devices Default: None
Monitoring Interval	MII monitoring interval in milliseconds	Range: A positive integer Default: 100ms
Upstream Delay	MII monitoring upstream delay in milliseconds	Range: A positive integer Default: 200ms
Downstream Delay	MII monitoring downstream delay in milliseconds	Range: A positive integer Default: 200ms

Table 15: Devices ARP Monitoring Options tab

Field	Description	Data Input Notes
Primary Interface	The preferred primary interface	Format: Pulldown list Range: Available devices
Monitoring Interval	ARP monitoring interval in milliseconds	Range: A positive integer Default: 100ms

Field	Description	Data Input Notes
ARP Validation	The method to validate the ARP probes and replies	Format: Pulldown list Range: None, Active, Backup, All Default: None
ARP Target List	Comma-separated ARP target IP addresses	Format: Valid IP address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)

Table 16: Devices IP Interfaces tab

Field	Description	Data Input Notes
IP Address List	The IP address of the interfaces associated with the device	Format: Valid IP address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)
Add Row	Displays a textbox to add an IP Address	Format: Button **Note:** Multiple rows can be added.
IP Address textbox	Textbox for an IP address	Format: Textbox Range: Dotted quad decimal (IPv4) or colon hex (IPv6)
Remove	Removes the device interface IP Address on the selected row	Format: Button

Inserting a Device

Devices cannot be created which use management networks (those configured after installation and designated in the Network listing in blue italic text). This ensures continued access to the GUI via the management networks.

1. Select **Configuration > Network > Devices**.
   The **Devices** page appears.

2. Select a server.

3. Click the **Insert** button.
   The **Device Insert** page appears.

4. Select a **Device Type**.

   For more information about **Device Type**, or any field on this page, see *Device Insert elements* .

   Note: Device Type of Ethernet cannot be selected.

5. Select a **Device Monitoring** style.

   Note: Device Monitoring is only used when the Device Type is Bonding.

6. By default, **Start on Boot** is enabled. Uncheck the check box if you want to disable **Start on Boot**.

7. Select the **Boot Protocol**.

8. Select the **Base Device(s)** if the device type is one of the following: Bond, Alias, or VLAN.

   Note: Alias and VLAN devices require one selection; bond devices require two selections.

9. Click **OK** to submit the information and return to the Device page, or click **Apply** to submit the information and continue entering additional data.

The device is added. You can now update MII and ARP monitoring options and add IP interfaces, if applicable.

Inserting MII Monitoring Options

Inserting MII monitoring options is only required if the device type is Bonding. For all other device types, the **MII Monitoring Options** tab is disabled.

1. Select **Configuration > Network > Devices**.
   The **Devices** page appears.

2. Select a server.

3. Click the **Insert** button.
   The **Device Insert** page appears.

4. Click the **MII Monitoring Options** tab.
   The **MII Monitoring Options** tab appears.

5. Click **Primary Interface** to select None (for no interface) or the preferred interface from the pulldown list.

6. Enter the **Monitoring Interval**, if you do not wish to use the default setting.

7. Enter the **Upstream Delay**, if you do not wish to use the default setting.

8. Enter the **Downstream Delay**, if you do not wish to use the default setting.

9. Click the **General Options** tab.

10. Click **OK** to submit the information and return to the Device page, or click **Apply** to submit the information and continue entering additional data.

The MII monitoring options are updated.

Inserting ARP Monitoring Options

Inserting ARP monitoring options is only required if the device type is Bonding. For all other device types, the **ARP Monitoring Options** tab is disabled.

1. Select **Configuration > Network > Devices**.
   The **Devices** page appears.

2. Select a server.

3. Click the **Insert** button.
   The **Device Insert** page appears.

4. Click the **ARP Monitoring Options** tab.
   The **ARP Monitoring Options** tab appears.

5. Click **Primary Interface** to select None (for no interface) or the preferred interface from the pulldown list.

6. Enter the **Monitoring Interval**, if you do not wish to use the default setting.

7. Click **ARP Validation** to select a validation method from the pulldown list, if you do not wish to use the default setting.

8. Enter one or more IP addresses for the target device.

    Note: Multiple IP addresses are comma separated.

9. Enter an IP Address for the device.

10. Click **OK** to submit the information and return to the Device page, or click **Apply** to submit the information and continue entering additional data.

The ARP monitoring options are updated.

Inserting IP Interfaces

The IP interfaces tab allows interfaces to be associated with a device.

1. Select **Configuration > Network > Devices**.
    The **Devices** page appears.

2. Select a server.

3. Click the **Insert** button.
    The **Device Insert** page appears.

4. Click the **IP Interfaces** tab.
    The **IP Interfaces** tab appears.

5. Click **Add Row**.
    A textbox appears in which you can enter an IP Address for the device.

6. Enter an **IP Address** for the device.

7. Select a **Network Name**.

8. For each row, only one IP Address and Network Name can be specified. To specify additional rows, select **Add Row** and following Steps 6 and 7.

9. When you are finished adding IP Addresses, click **OK** to submit the information and return to the Device page, or click **Apply** to submit the information and continue entering additional data.

The IP addresses are added.

Devices elements

This table describes the elements of the **Configuration Devices** page.

Table 17: Devices Elements

Field	Description
Server	The server host name displayed in tabbed format at the top of the table
Device Name	The name of the device
Device Type	The device type. Supported types include: • Bonding • VLAN • Alias • Ethernet
Device Options	A collection of keyword value pairs for the device options

Field	Description
IP Interface (Network)	IP address and network name in the format: IP Address (network name)
Configuration Status	The configuration status of the device. The possible states are: • Discovered (provisioned directly on the server) • Configured (provisioned through the GUI; server update is complete) • Pending (update in progress) • Deferred (server cannot be reached for updates) • Error (specific error text is displayed in the Configuration Status field)

Editing a Device

Not all devices can be edited. Pre-configured devices created during the install process, for example, cannot be edited. A device that cannot be edited is distinguished using italic font.

Note: Prior to editing a device, generate a device report. The device report will serve as a record of the device's original settings. Print or save the device report for your records. For more information about generating a device report, see *Generating a Device Report*.

1. Select **Configuration > Network > Devices**
   The **Devices** page appears.
2. Click to select a server.
   The device data for the selected server appears.
3. Click to select a device and click **Edit.**

   Note: If the device cannot be edited, the **Edit** button will be disabled.

   If the device can be edited, the **Device Edit** page appears.
4. Edit the available fields as necessary.

   See *Device Insert elements* for details about the fields that appear on this page.

   Note: Fields that cannot be edited are disabled.

5. Click **OK** to submit the changes and return to the **Devices** page, or click **Apply** to submit the information and continue editing additional data.

The device is changed.

Deleting a Device

Not all devices can be deleted. In-use devices and pre-configured devices created during the install process, for example, cannot be deleted. A device that cannot be deleted is distinguished using italic font.

Note: Prior to deleting a device, generate a device report. The device report will serve as a record of the device's original settings. Print or save the device report for your records. For more information about generating a device report, see *Generating a Device Report*.

1. Select **Configuration > Network > Devices.**

The **Devices** page appears.

2. Click to select a server.
   The device data for the selected server appears.

3. Click to select the device you want to delete. Alternately, you can delete multiple devices. To delete multiple devices, press and hold **Ctrl** and click to select specific devices.

   Note: If the device cannot be deleted, the **Delete** button will be disabled.

   Note: To delete multiple devices at one time, all selected devices must be deletable.

4. Click **Delete**.
   A confirmation box appears.

5. Click **OK**.
   The device is deleted.

Generating a Device Report

1. Select **Configuration > Network > Devices**
   The **Devices** page appears.

2. Click to select a server.
   The device data for the selected server appears.

3. To generate a report for all devices, click **Report**. To generate a report for a single device, click to select the device and click **Report**. Alternately, you can select multiple devices. To generate a report for multiple devices, press and hold **Ctrl** as you click to select specific devices.
   The Device Report is generated.

4. Click **Print** to print the report.

5. Click **Save** to save the report to a file.

Routes

Use the Route Configuration page to define specific routes for signaling traffic. You can specify routes for the entire network, specific servers, or specific server groups.

Routes Insert elements

This table describes the elements of the Routes Insert page. Elements are displayed for the selected server or server group.

Table 18: Routes Insert Elements

Field	Description	Data Input Notes
Route Type	The type of route	Format: Radio button
		Range: Default, Net, Host
		Note: The Default route option is available only if there is no default

Field	Description	Data Input Notes
		route configured on the target server. There can be no more than one IPv4 and one IPv6 default route defined.
Device	The network device name through which traffic is routed	Format: Pulldown list Range: Provisioned devices on the selected server
Destination	The destination network address **Note:** This field is disabled if the **Route Type** is default.	Format: Valid network address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)
Netmask	A valid netmask for the destination network **Note:** This field is disabled if the **Route Type** is default. This field is disabled and set to 32 (IPv4) or 128 (IPv6) if the **Route Type** is host.	Format: Valid netmask Range: Valid netmask for the network in prefix length (IPv4 or IPv6) or dotted quad decimal (IPv4) Default: 24 for IPv4; 64 for IPv6
Gateway IP	The IP Address of the gateway for the route	Format: Valid IP address Range: Dotted quad decimal (IPv4) or colon hex (IPv6)

Inserting a Route

Routes cannot be created which use management networks (those configured after installation and designated in the Network listing in blue italic text). This ensures continued access to the GUI via the management networks.

1. Select **Configuration > Network > Routes**
   The **Routes** page appears.
2. Using the tabs, select to add a server or server group to the entire network, or a specific network group.
3. Click the **Insert** button.
   The **Routes Insert** page appears.
4. Select a **Route Type**.

   For more information about **Route Type**, or any field on this page, see *Routes Insert elements* .

5. Select a **Device**.

6. Enter a **Destination**.

    Note: This step is required only if the **Route Type** is Net or Host. The field is disabled if the **Route Type** is Default.

7. Enter the **Netmask**.

    Note: This step is required only if the **Route Type** is Net. The field is disabled if the **Route Type** is Default or Host.

8. Enter the **Gateway IP**.

9. Click **OK** to submit the information and return to the Route page, or click **Apply** to submit the information and continue entering additional data.

The route is added.

Routes elements

This table describes the elements of the **Configuration Routes** page.

Table 19: Routes Elements

Field	Description
Server/Server Group	The server host name and server groups are displayed in tabbed format at the top of the table
Route Type	The type of route
Destination	The destination network IP address and prefix length in the format: IP Address/Prefix Length
Netmask	A valid netmask for the destination network
Gateway	The IP Address of the gateway for the route
Scope Status	The current number of servers where the route was successfully configured out of the total servers in the server group. (Note: This column is only present for server group routes)
Configuration Status	The configuration status of the route. The possible states are: • Discovered (provisioned directly on the server) • Configured (provisioned through the GUI; server update is complete) • Pending (update in progress) • Deferred (server cannot be reached for updates) • Error (specific error text is displayed in the Configuration Status field)

Editing a Route

Not all routes can be edited. Pre-configured routes created during the install process, for example, cannot be edited. A route that cannot be edited is distinguished using italic font.

Note: Prior to editing a route, generate a route report. The route report will serve as a record of the route's original settings. Print or save the route report for your records. For more information about generating a route report, see *Generating a Route Report*.

1. Select **Configuration > Network > Routes**.
   The **Routes** page appears.

2. Click to select a server or server group using the tabs at the top of the table.
   The route data for the selected server or server group appears.

3. Click to select a route and click **Edit.**

   Note: If the route cannot be edited, the **Edit** button will be disabled.

   If the route can be edited, the **Routes Edit** page appears.

4. Edit the available fields as necessary.
   See *Routes Insert elements* for details about the fields that appear on this page.

   Note: Fields that cannot be edited are disabled.

5. Click **OK** to submit the changes and return to the **Routes** page, or click **Apply** to submit the information and continue editing additional data.

The route is changed.

Deleting a Route

Not all routes can be deleted. In-use routes and pre-configured routes created during the install process, for example, cannot be deleted. A route that cannot be deleted is distinguished using italic font.

Note: Prior to deleting a route, generate a route report. The route report will serve as a record of the route's original settings. Print or save the route report for your records. For more information about generating a route report, see *Generating a Route Report*.

1. Select **Configuration > Network > Routes.**
   The **Routes** page appears.

2. Click to select a server or server group from the tabs at the top of the table.
   The route data for the selected server or server group appears.

3. Click to select the route you want to delete. Alternately, you can delete multiple routes. To delete multiple routes, press and hold **Ctrl** and click to select specific routes.

   Note: If the route cannot be deleted, the **Delete** button will be disabled.

   Note: To delete multiple routes at one time, all selected routes must be deletable.

4. Click **Delete**.
   A confirmation box appears.

5. Click **OK** to delete the route
   The route is deleted.

Generating a Route Report

1. Select **Configuration > Network > Routes**
   The **Routes** page appears.
2. Click to select a server or server group from the tabs at the top of the table.
3. Click **Report** to generate a report for all routes. To generate a report for a single route, click to select the route and click **Report**. Alternately, you can select multiple routes. To generate a report for multiple routes, press and hold **Ctrl** as you click to select specific routes.
   The Route Report is generated.
4. Click **Print** to print the report.
5. Click **Save** to save the report to a file.

PDBI configuration

While it is possible to add or change subscriber database information through GUI provisioning, the main method of subscriber data provisioning is PDBI (Provisioning Database Interface). Through the PDBI, independent information systems may add, delete, change or retrieve information about any IMSI, DN, or Network Entity association. PDBI does this by:

- allowing connections to clients that can write to the database
- importing .pdbi files from a remote directory and populating the values within the files to the database

The steps to setting up PDBI configuration are:

1. Configure PDBI connections
2. Configure PDBI options
3. Configure PDBI import files
4. Configure PDBI exports

For additional information about PDBI see the Provisioning Database Application and Interface Manual included on the documentation DVD or the HLR Router online help.

Configuring PDBI connections

PDBI Connections are managed through the HLR Router GUI. This task describes how to set up PDBI connections. For additional information about PDBI connections see the HLR Router online help.

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

1. Select **Eagle XG Database > Configuration > PDBI > Options**.

   The **PDBI Options Configuration** page appears.

2. Enter the port number for the unsecure listening port in the **TCP Listening Port** field.

   This port can be disabled by setting the value to 0. Changes to the TCP Listening port do not take affect until the client process is restarted.

3. Enter the port number for the SSL (Secure Socket Layer) listening port in the **SSL Listening Port** field.

This port can be disabled by setting the value to 0. Changes to the SSL Listening port do not take affect until the client process is restarted.

4. If not already checked, select Allow Connections.

5. Enter the maximum number of simultaneous connections you want to allow in the **Max Connections** field.

   This value can be set between 1 and 128 connections.

6. Enter the number of seconds you want to allow to pass between the establishment of a network connection and a connection message being received without causing a timeout in the **Connection Init Timeout** field.

   This value can be set between 0 and 60 seconds.

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

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

9. Click on **Insert** located below the table.
   The **Insert PDBI Connections** page appears.

10. Enter the System ID in the **System ID** field.

    This is a 1 - 8 character identifier for the connection.

11. Enter the IP address for the connection in the **IP Address** field.

    This must match the IP address for the client.

12. 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.

13. 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.

PDBI options configuration

PDBI options are configured using the **EAGLE XG Database Configuration PDBI Options** page of the HLR Router GUI. These include:

- PDBI connection options: connections are added using the **EAGLE XG Database Configuration PDBI Connections** page. The **EAGLE XG Database Configuration PDBI Options** page allows you to manage configuration options for connections. For information about configuring PDBI connections see *Configuring PDBI connections*.
- General PDBI options: For more information about configuring general PDBI options see *Configuring general PDBI options*.
- PDBI import options: import settings are configured using the **EAGLE XG Database Configuration PDBI Options** page. For more information about configuring PDBI import options see *Configuring PDBI import options*.

- PDBI export options: exports are scheduled through the **EAGLE XG Database Configuration PDBI Export** page. The **EAGLE XG Database Configuration PDBI Options** page allows you to manage settings for exports. For more information about configuring PDBI exports see *Configuring PDBI exports*.

If you would like to configure all PDBI options at once see the HLR Router online help documentation for instructions.

Configuring general PDBI options

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

1. Select **Eagle XG Database > Configuration > PDBI > Options**.
   The **PDBI Options Configuration** page appears.

2. Choose if you want to **Display PDBI Output**.

   If checked, the PDBI commands and responses will be displayed on the GUI when provisioning data.

3. Enter the maximum number of Kilobytes you want to allow for response messages in the **Max Response Message Size** field.

   This value can be set between 1 and 132 kilobytes.

4. Enter the maximum number of database manipulation commands you want to allow per transaction in the **Max Transaction Size** field.

5. Enter an **IMSI Prefix**.

   The IMSI Prefix must be between 10 and 15 digits and is automatically pre-appended to the IMSI of incoming PDBI requests and removed in outgoing PDBI responses.

6. Enter a **DN Prefix**.

   The DN Prefix must be between 8 and 15 digits and is automatically pre-appended to the DN(s) of incoming PDBI requests and removed in outgoing PDBI responses.

7. Enter the number of seconds you want to allow between each asynchronous Database Report (dbrpt) message sent to the client in the **Asynchronous Database Report Frequency** field.
   The value can be set between 1 and 86400 seconds.

8. Enter the percentage of MP servers that you want to allow to meet or exceed the reported level before triggering an alarm in the **Database Report Percentage** field.
   This value can be set between 1 and 100 percent.

9. Choose if you want to **Log PDBI Messages**.

   If checked all incoming and outgoing PDBI messages will be logged.

10. Enter the number of seconds you want to allow between a transaction being committed and it becoming durable in the **Transaction Durability Timeout** field.

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

The PDBI configuration options are applied.

Configuring PDBI import options

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

1. Select **Eagle XG Database > Configuration > PDBI > Options**.
   The **PDBI Options Configuration** page appears.

2. If not already checked, select **Remote Import Enabled**.

3. Set the **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.

4. Enter the IP address of the server that contains the files you want to import in the **Remote Import Host IP Address** field.

5. Enter a username used to log into the server in the **Remote Import User** field.

6. Enter a password used to exchange ssh keys with the remote import host in the **Remote Import Password** field.

   The password is cleared from this table once the keys have been exchanged.

7. Enter the name of the directory where the import files are stored in the **Remote Import Directory** field.

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

The PDBI configuration import options are configured. Import files that are placed in the Remote Import directory on the specified 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 NOAMP.

PDBI import file configuration

Import files that are placed in the **Remote Import Directory** on the remote server specified in the **Remote Import Host IP Address** field on the PDBI options page 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 NOAMP. For a file to be imported it must:

- be properly named following the naming convention. For more information about PDBI import file names see *File name formats*.
- 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.

Configuring PDBI exports

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

1. Select **Eagle XG Database > Configuration > PDBI > Options**.
   The **PDBI Options Configuration** page appears.

2. Select an **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.

3. If not already checked, select the **Remote Export Transfers Enabled** field.

4. Enter the IP address for the server you want to send export files to in the **Remote Export Host IP Address** field.

5. Enter a username for the server in the **Remote Export User** field.

6. Enter a password used to exchange ssh keys with the remote export host in the **Remote Export Password** field.

   The password is cleared from this table once the keys have been exchanged.

7. Enter the name of the directory you want export files sent to in the **Remote Export Directory** field.

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

9. Select **Eagle XG Database > Configuration > PDBI > Export**.
   The **PDBI Export** page appears.

10. Click on **Insert** located below the table.

    The **Insert PDBI Export** page appears.

11. Type a name for the export in the **Identifier** field.

12. Select one of the **File Formats**:

    - **csv**: to export a CSV file. This is the default value.
    - **pdbi**: to export a file in PDBI commands format.

13. 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.

14. Select the type(s) of data to include in the export file from the **Export Data** pulldown menu.

    The default value is **All**.

15. Select the month, day, and year you initially want the report to run from the **Date** pulldown menus.

    The default is the current day.

16. 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.

17. Select how often you would like to repeat this export from the **Repeat** options.

18. If desired, add a comment in the **Comment** field.

    The comment provides context for someone viewing the **PDBI Export** page. It is not included in the export file.

19. 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.

PDBI exports are configured and will begin at the next scheduled interval.

Transport Manager configuration

Transport Manager acts as an interface between the User Adapter Layer and IP Transport layer (UDP/Linux SCTP) for EAGLE XG applications. It supports both SCTP and UDP (User Datagram) protocols.

Adjacent Node

An Adjacent Node is a server acting as a signaling peer on a network. An Adjacent Node connects to one or more MP (message processing) Servers using reliable IP transport sessions, such as SCTP associations. In short, the Adjacent Node represents the far-end of an SCTP association. In the case of Eagle 5 ISS STP, an Adjacent Node is an E5-ENET card.

The Adjacent Nodes table lists all servers configured for direct connection to this SS7 node. An Adjacent Node is associated with the IP address on which the Adjacent Node will listen for M3UA signaling.

Safeguard to prevent service impact from configuration changes:

* The software will not allow you to delete an Adjacent Node that is referenced by an Adjacent Server Group.

Adjacent Node elements

This information appears on the **Adjacent Node** page:

Table 20: Adjacent Node Elements

Element	Description	Data Input Notes
Signaling Network Element Name	Identifies the Signaling Network Element to which the Transport is being added.	Format: Pulldown list Range: All configured Signaling Network Elements. This field is required. Note: When the Adjacent Node configuration is mastered from the System OAM and this Insert screen is viewed from System OAM server, the Signaling Network Element Name drop down is disabled and contains the NE name of the connected System OAM server.
Adjacent Node Name	Unique identifier used to label an Adjacent Node. An adjacent node is a remote node serving as the far end of a Transport.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string.

Element	Description	Data Input Notes
		This field is required.
IP Address 1	IP address 1 of an adjacent node. By default this will be configured as Primary IP address of an Adjacent Node.	Range: A valid IPv4 address: xxx.xxx.xxx.xxx This field is required.
IP Address 2	IP address 2 of an adjacent node. If this is configured then Adjacent Node can be configured as Multihomed if both the IP Addresses are selected in *Transport Configuration*	Range: A valid IPv4 address: xxx.xxx.xxx.xxx This field is required.

Viewing Adjacent Nodes

Use this procedure to view a list of defined Adjacent Nodes.

Select **Transport Manager>Configuration>Adjacent Nodes.**

The **Adjacent Nodes** page appears. For field definitions, see *Adjacent Node elements*.

To filter the information on this page, see *Filtering using the display filter*.

The page appears with the defined Adjacent Nodes listed.

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 **Display Filter: Signaling Network Element Name** with the equals (**=**) operator and a value of **SO_ONE**, the table would show only records where the **Signaling Network Element Name=SO_ONE**.

4. Click **Go** to filter on the selection or set the **Display Filter** to **None** to clear the selection.

Records are displayed according to the specified criteria.

Inserting an Adjacent Node

1. Select **Transport Manager>Configuration>Adjacent Node**

   The **Adjacent Nodes** page appears.

2. Click **Insert**.

   The **Insert Adjacent Node** page appears.

3. Populate the fields with data (for field definitions, see *Adjacent Node elements*).

4. Perform one of these actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.

The Adjacent Node is added to the configuration.

Deleting an Adjacent Node

Deleting an Adjacent Node removes the Adjacent Node from the configuration.

The software will not allow you to delete an Adjacent Node that is referenced by an Adjacent Server Group. If necessary, perform remove the Adjacent Node from the Adjacent Server Group.

1. Select **Transport Manager>Configuration>Adjacent Node**.

   The **Adjacent Node** page appears.

2. Click on the row of the Adjacent Node you want to remove.

   A delete confirmation message appears.

3. Click the Delete button at the bottom of the page.

4. Click **OK** to confirm the deletion.

The Adjacent Node is deleted from the table.

Configuration Sets

The **Transport Manager > Configuration > Configuration Sets** page shows all configured sets of SCTP association parameter values and lets you create new Configuration Sets.

A Default Configuration Set is provided with the software. The Default Configuration Set is pre-populated with values appropriate for a typical signaling network. The pre-populated values are shown in *Transport Manager Configuration Set elements*.

Transport Manager Configuration Set elements

Table 21: Transport Manager Configuration Set Elements describes the fields on the **Transport Manager > Configuration > Configuration Set** pages.

Many of the fields in the table use the value configured in the Default Configuration Set as their default. If the defaults have been modified, the new values are shown on the **Transport Manager >**

Configuration > Configuration Set pages. The original default values are shown in *Table 21: Transport Manager Configuration Set Elements*.

Table 21: Transport Manager Configuration Set Elements

Element	Description	Data Input Notes
Configuration Set Name	A name that uniquely identifies the SCTP Transport Manager Configuration Set. The name is case sensitive.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string. This field is required and must be unique.
Retransmit Initial Timeout	The expected average network round-trip time in milliseconds. This value is used to initialize the round-trip time value when an association is first started and the round-trip time has not yet been measured. The round-trip time is used by SCTP in calculating when to retransmit chunks.	Format: Numeric Range: 10 - 5000 msec Default: 120 This field is required.
Retransmit Minimum Timeout	The minimum amount of time to wait for an acknowledgment for a message sent. This value prevents the retransmit timeout from becoming too small in networks with a very short round-trip time.	Format: Numeric Range: 10 - 1000 msec Default: 120 This field is required.
Retransmit Maximum Timeout	The maximum amount of time to wait for an acknowledgment for a message sent. This value places an upper bound on the exponential back-off algorithm used by SCTP for retransmission timing. Once this retransmit interval is reached, retransmits will be sent at a constant rate until an ACK is received or the maximum attempt is reached.	Format: Numeric Range: 10-10000 msec Default: 120 This field is required.
Number of Retransmits Triggering Association Failure	Number of consecutive retransmits that will cause an SCTP Association to be marked as failed. This value indicates how many SCTP retransmission attempts should be made to all	Format: Numeric Range: 1- 12 Default: 5 This field is required.

Element	Description	Data Input Notes
	destinations for an SCTP association before marking the association as failed. This value should not be greater than the sum of the retransmit attempts for all destinations within the association.	
Number of Retransmits Triggering Init Failure	Number of consecutive retransmits for INIT and COOKIE-ECHO chunks that will cause an SCTP Association to be marked as failed. This value indicates how many retransmission attempts should be made to the primary SCTP address for INIT and COOKIE-ECHO chunks before marking the association as failed.	Format: Numeric Range: 1 - 12 Default: 8 This field is required.
SACK Delay (ms)	The number of milliseconds to delay after receiving a DATA chunk and prior to sending a SACK. A non-zero value for SACK Delay gives the application time to bundle DATA chunks in the same SCTP datagram with the SACK, thereby reducing the number of packets in the network. Setting SACK Delay to zero disables this delay so that SACKs are sent as quickly as possible.	Format: Numeric Range: 0 - 200 msec Default: 10 This field is required.
SCTP Heartbeat Interval (ms)	The interval in milliseconds between sending SCTP HEARTBEAT messages to a peer. HEARTBEAT messages are only sent when no user data has been sent for the duration of the heartbeat interval. Setting the heartbeat interval to zero disables heartbeating (not recommended).	Format: Numeric Range: 0, 100 - 300000 msec Default: 1000 This field is required.
Connection Retry Interval (sec)	The interval in seconds between connection attempts when the connection is unsuccessful.	Format: Numeric Range: 5 - 60 sec Default: 10 This field is required.

Element	Description	Data Input Notes
Socket Send Buffer Size (bytes)	The socket send buffer size for outgoing SCTP messages. The send buffer size should be greater than or equal to the product of the bandwidth and the round trip delay for the Association.	Format: Numeric Range: 65535 - 5000000 bytes Default: 2000000 This field is required.
Socket Receive Buffer Size (bytes)	The socket receive buffer size for incoming SCTP messages. The receive buffer size should be greater than or equal to the product of the bandwidth and the round trip delay for the Association.	Format: Numeric Range: 65535 - 5000000 bytes Default: 2000000 This field is required.
SCTP Multihoming Mode	The SCTP Multihoming mode allows the user to configure remote host validation mode setting for SCTP. If the Adjacent Node is Multihomed for a specified Transport, Adjacent Node IP Addresses received in INIT/INIT-ACK chunk will be validated based on this parameter. SCTP Multihoming Mode = **Relax**: One of the IP Address received from Adjacent Node in an INIT/INIT-ACK chunk must match any of the configured Adjacent Node IP Address associated with that Transport. SCTP Multihoming Mode = **Match**: All of the IP Address received from Adjacent Node in an INIT/INIT-ACK chunk must match all of the configured Adjacent Node IP Address associated with that Transport.	Default: Relax Allowed Values: Relax, Match This field is required.

Viewing Transport Manager Configuration Sets

Select **Transport Manager>Configuration>Configuration Sets.**

The **Transport Manager Configuration Sets** page appears (for field definitions, see *Transport Manager Configuration Set elements*).

To filter the information on this page, see *Filtering using the display filter*.

The **Transport Manager Configuration Sets** page appears with the Configuration Sets listed.

Inserting Transport Manager Configuration Set

1. Select **Transport Manager>Configuration>Configuration Sets.**

    The **Transport Manager Configuration Sets** page appears.

2. Click **Insert**.

    The **Insert Transport Manager Configuration Sets** page appears.

    The default values that appear on the Transport Manager Configuration Set page match whatever values are configured in the default Transport Manager Configuration Set. The original default values are shown in *Transport Manager Configuration Set elements*.

3. Populate the fields with data. For field definitions, see *Transport Manager Configuration Set elements*.
4. Perform one of these actions:

    - Click **OK** to save the data and exit this page.
    - Click **Apply** to save the data and remain on this page.

The Transport Manager Configuration Set is added.

Editing a Transport Manager Configuration Set

Note: Although the software provides the capability to edit the Default Transport Manager Configuration Set, any changes to the default values should be evaluated carefully. The Default values shown in *Transport Manager Configuration Set elements* are recommended.

The software will not allow you to edit a configuration set that is referenced by an active Transport.

1. Select **Transport Manager>Configuration>Configuration Sets**.

    The **Transport Manager Configuration Sets** page appears.

2. Click **Edit** next to the Transport Manager Configuration Set you wish to modify. Note that you cannot change a Configuration Set Name.

    The **Edit Transport Manager Configuration Sets** page appears.

3. Make the desired changes. For field definitions, see *Transport Manager Configuration Set elements*.
4. Perform one of these actions:

    - Click **OK** to save the data and exit this page.
    - Click **Apply** to save the data and remain on this page.

The Transport Managers Configuration Set is updated. For the changes to take effect, the disabled Transport Manager must be placed back in service.

Deleting a Transport Manager Configuration Set

Deleting an Transport Manager Configuration Set removes the configuration set from the database.

The software will not let you remove an Transport Manager Configuration Set that is referenced by an active Transport.

The *Default* Transport Manager Configuration Set cannot be deleted.

1. Select **Transport Manager>Configuration>Configuration Sets.**

   The **Transport Manager Configuration Sets** page appears (for field definitions, see *Transport Manager Configuration Set elements*).

2. Click **Delete** in the row you want to remove.
   A Delete confirmation message appears.

3. Click **OK** to remove the configuraiton set.

The Transport Manager Configuration Set is removed from the table.

Transport Configuration

The **Transport Configuration** page lists all SCTP Transports for all MP servers and Adjacent Nodes.

The **Transport Configuration** page also provides a link to the **Transport Maintenance** page where you can view the status of an Transport.

Safeguards to prevent service impact from configuration changes:

• The software will not let you edit or delete an Transport unless it is in the **Disabled** administrative state.
• The software will not let you specify an MP Server IP Address and Local SCTP Port combination that already exists as a Transport.
• The software will not let you delete an Transport referenced by a Link.

Note: There is dependency between the Transport Manager and ENUM UDP Adapter managed objects that dictate the order of Transport provisioning. When configuring a listening Transport for ENUM, the order of provisioning and the object dependencies are defined in the following: *Table 22: Order of Managed Object Provisioning*.

Table 22: Order of Managed Object Provisioning

Order of Managed Object Provisioning	Must be Available Beforehand	
1. Local Node	Server Group	
3. Configuration Set	Default is configured through initialization loaders	
3. Listening Transport for ENUM	**Steps for Listening Transport:**	a. Signaling Network Element b. Local MP server HostName c. Local MP Server IP Address/port

Transport Configuration elements

This information appears on the **Transport Configuration** page:

Table 23: Transport Configuration elements

Element	Description	Data Input Notes
Signaling Network Element Name	Identifies the Signaling Network Element to which the Transport is being added.	Format: Pulldown list Range: All configured Signaling Network Elements. This field is required.
Adapter	Identifies the Transport User for which the Transport is being added.	Default: n/a Options: ENUM, M3UA This field is required.
Transport Name	A name that uniquely identifies the Transport.	Format: Valid characters are alphanumeric and underscore. Must contain at least one alpha and must not start with a digit. Range: A 32-character string. This field is required and must be unique.
Transport Protocol	Identifies the Tranport protocol to be used by this Transport.	Format: Pulldown list Default: n/a This field is required.
Transport Type	Identifies the Transport type to be used by this Transport.	Format: Pulldown list Default: n/a This field is required.
MP Server Hostname	The hostname of the MP server that will host the local end of the Transport.	Format: Pulldown list Default: n/a This field is required.
MP Server IP Address (Primary)	The Primary IP Address hosted by the MP Server that will be bound to this Transport. If the MP Server is configured with more than one signaling network IP address, this field allows selection of the desired IP address to be used for this Transport.	Format: Pulldown list Default: n/a This field is required.

Element	Description	Data Input Notes
MP Server IP Address (Secondary)	The Secondary IP Address hosted by the MP Server that will be bound to this Transport. If the MP Server is configured with more than one signaling network IP address, this field allows the Transport to be Multihomed.	Format: Pulldown list Default: n/a This field is required.
MP Server Listen Port	Listen port number of the MP Server for this Transport. This port will be used if the Transport Type is configured as "Listener". If the MP server hosts multiple "Listener" Transports, each Transport must listen on a different port.	Default: 5060; Range: 1024 - 65535
MP Server Initiate Port	Initiate port number of the MP Server for this Transport. This port will be used if the Transport Type is configured as "Initiator". If the MP server hosts multiple Transports, a unique initiate port number must be configured for each IP address.	Default: 2905; Range: 1024 - 65535
Adjacent Node	The Adjacent Node that will host the remote end of this Transport.	Format: Pulldown list Default: n/a
Adjacent Node IP Address (Primary)	The Primary IP Address configured for the Adjacent Node to host the remote end of the Transport.	This is a display-only field populated automatically when the Adjacent Node is selected. Format: Pulldown list Default: n/a
Adjacent Node IP Address (Secondary)	The Secondary IP Address configured for the Adjacent Node to host the remote end of the Transport. This field allows the Adjacent Node of a Transport to be Multihomed.	This is a display-only field populated automatically when the Adjacent Node is selected. Format: Pulldown list Default: n/a
Adjacent Node Port	Adjacent Node port number for this Transport. This port number must match the port number configured on the Adjacent Node as the listening or initiator port as per the Transport Type	Format: Numeric Default: 2905 Range: 1024 - 65535

Element	Description	Data Input Notes
	configured. If the Adjacent Node hosts multiple Transports, each Transport may listen on a different Remote port number.	
Configuration Set Name	The configuration parameter set to be sused for this Transport. Configuraton sets are defined on the **Configuration Sets** page (see *Configuration Sets*).	Format: Pulldown list Range: All Configuration Set names Default: Default

Viewing Transports

Select **Transport Manager>Configuration>Transport>.**

The **Transport Configure** page appears. For field definitions, see *Transport Configuration elements*.

To filter the information on this page, see *Filtering using the display filter*.

The page appears with the configured Transports listed.

Inserting a Transport

1. Select **Transport Manager>Configuration>Transport.**

    The **Transport** page appears.

2. Click **Insert**.

    The **Insert Transport** page appears.

3. Populate the fields with data. For field definitions, see *Transport Configuration elements*.
4. Perform one of these actions:

    *   Click **OK** to save the data and exit this page.
    *   Click **Apply** to save the data and remain on this page.

The Transport is added.

Editing a Transport

The **Edit** operation lets you change the following parameters on the **Transport** page:

*   Transport Type
*   MP Server IP Address
*   MP Server Listen Port
*   MP Server Initiate Port
*   Adjacent Node
*   Adjacent Node Port
*   Configuration Set Name

The remaining parameters are grayed-out and cannot be edited.

Note: The software will not let you edit an Transport unless it is in the **Disabled** administrative state. For instructions on disabling the Transport, see *Transport Manager maintenance*.

1. Select **Transport Manager>Configuration>Transport.**

   The **Transports** page appears.

2. Click **Edit**.

   The **Edit Transports** page appears.

3. Make the desired changes. For field definitions, see *Transport Configuration elements*.

4. Perform one of the following actions:

   - Click **OK** to save the data and exit this page.
   - Click **Apply** to save the data and remain on this page.

The edited Transport data is written to the database. The Transport remains in the **Disabled** administrative state. To view or enable the Transport, see *Viewing Transports* and *Enabling a Transport*.

Deleting a Transport

Deleting an Transport removes the Transport from the configuration.

The software will not let you delete an Transport unless it is in the **Disabled** administrative state.

1. Select **Transport Manager>Configuration>Transport>**.

   The **Transports** page appears.

2. Click **Delete** in the row you want to remove.

   A delete confirmation message appears.

3. Click **OK** to confirm the deletion.

The Transport is deleted from the table.

Generating a Report on Transports

1. Select **Transport Manager>Configuration>Transports>.**

   The **Transports** page appears.

2. Click the **Report** link at the bottom of the table to generate a report on all entries.

The report opens listing all of the transports and associated parameters. Click **Print** or **Save** to print a copy of the report or save the report as a text file.

Viewing the Status of a Transport

You can use the Transport Maintenance page to view the administrative status of transports.

   Select **Transport Manager>Maintenance>Transport.**

   The **Transport Maintenance** page appears listing all transports and their operational status.

Note: To see the IP addresses of the Adjacent Node, click on the "+" button in the Adjacent Node field.

Transport Manager maintenance

The **Transport Maintenance** page shows the administrative state and operational status of each Transport. The administrative state may be **Enabled**, **Blocked**, or **Disabled**. The operational status may be **Up** or **Down**.

Each MP server reports status only for Transports hosted by that MP server.

Colored cells may indicate the need for maintenance activity. When the active server's collection status is **Unknown**, cells with gray text indicate the last known information about the Transport.

The **Maintenance** menu options are helpful under alarm conditions as a starting point for gathering additional information. For example, the maintenance options record the timestamp when a Transport goes down. The timestamp can then be used to narrow the search in the event history log and measurements reports.

Errors, warnings, and the possible need for maintenance activity are shown in the GUI in colored cells so that the conditions are readily identifiable.

Once rudimentary information for troubleshooting has been obtained, the network operator can continue investigating under the **Alarms & Events** and **Measurements** options on the GUI.

The menu also enables you to perform maintenance-related tasks such as:

- Enabling and disabling Transports.
- Blocking Transports.

Status information is obtained on the system through the collection process, whereby the SOAM server collects data from the MP servers. You can monitor the system's data collection functions under **Status & Manage>Collection**.

A user group must have permissions to view or execute any of the procedures on the **Transport Manager Maintenance** menu. If a group does not have permissions for the **Maintenance** menu options for **Transport**, this option will not appear in the GUI.

Transport maintenance is allowed from both the NOAMP and the SOAM. When the configuration is allowed from the SOAM, configuration and maintenance from the NOAMP is not allowed. All maintenance links are active whether the user is connected to the NOAMP or the SOAM. Maintenance data can be written to the standby NOAMP server.

Transport Maintenance Elements

This information appears on the **Transport Maintenance** page:

Table 24: Transport Maintenance elements

Element	Description
Signaling Network Element Name	Identifies the Signaling Network Element to which the Transport is being added.
MP Server Hostname	The hostname of the MP server that will host the local end of the Transport.
Adapter	Identifies the Transport User for which the Transport is being added.
Transport Name	A name that uniquely identifies this Transport.
Transport Protocol	Identifies the Transport protocol to be used by this Transport.
Transport Type	Identifies the Transport type to be used by this Transport.
Adjacent Node	The Adjacent Node to host the remote end of the Transport. Note: clicking on the "+" button in the Adjacent Node field shows the IP addresses for the Adjacent Node.
Admin State	The administrative state of the Transport. Transports can be either enabled, disabled, or blocked.
Operational Status	The operational status of the Transport: **Up** or **Down**.
Operational Reason	The reason a given operational status is shown. For information on a value listed in this field, see *Transport Operational Status and Reason*.
Up/Down Since	The date and time that the Transport came up or went down. For a newly added Transport, the time is when the Transport was configured. After a database restart, reboot, or initial startup before the Transports and Links are initialized, the value is the time when the application initialization runs.

Transport Administrative State

This list shows the possible values that may appear in the **Admin State** field of the **Transport Maintenance** page. A description of each state is also provided.

- **Enabled**- the MP server associated with the Transport begins attempts to bring the Transport to the SCTP Established state and the ASP-UP Operational State.
- **Blocked**-the SCTP connection should be up, but no M3UA signaling is allowed. The MP server associated with the Transport begins attempts to bring the Transport to the SCTP Established state

and the ASP-DOWN state. The **Blocked** administrative state is useful for cases in which the network operator wishes to verify IP network connectivity without allowing any M3UA signaling.

- **Disabled**-the MP server associated with the Transport begins attempts to bring the Transport to the SCTP Closed state and the ASP-DOWN states.

The relationship between the **Admin State** and the protocol state is reflected in the **Transport Status** (*Viewing the Status of a Transport*).

Orange color in the **Admin State** field highlights the value when the value is anything other than **Enabled**.

When a new Association is configured, the Association is in the **Disabled** administrative state and must be manually placed in the **Enabled** administrative state.

Admin State Relationships

This section provides additional details about the **Admin State** field on the **Transport Maintenance** page.

The **Admin State** tells the MP server what protocol state the Transport should be in. If the Transport protocol state does not match what is expected for the **Admin State**, the MP server actively tries to resolve the problem until the **Admin State** and the protocol state match. The relationship between the **Admin State** and the protocol state is reflected in the **Transport Status**.

Table 25: Transport Admin State Relationships

Admin State	Operational Status	Operational Reason	Description
Enabled	Down	Connecting	Trying establishing the SCTP connection in Initiator mode.
	Down	Listening	Trying establishing the SCTP connection or opening UDP socket in Listener mode.
	Down	Up Pending	**Valid only for M3UA :** SCTP Transport has been established & ASP-UP has been sent, Waiting for ASP-UP-ACK.
	Up	Normal	**SIP :** • For SCTP Transports, SCTP Connection is established after exchanging SCTP Init handshake methods.

Admin State	Operational Status	Operational Reason	Description
			• For UDP Transports, UDP Socket binds and opened for Listen mode. **M3UA** : • For SCTP Transport, it has reached the ASP-UP state and is available for enabling links. **ENUM** : For UDP Transports, UDP Socket binds and opened for Listen mode.
	Up	Abnormal	If one of the Local IP address goes down in SCTP Transport for Multihomed Adjacent nodes.
	Down	BindFail	**Valid only for SIP/ENUM :** Socket bound fail.
	Down	Application Disabled	Application is down.
	Down	Forced Standby	If the application process was gracefully stopped and the server's HA status is set to Forced Standby.
Disabled	Down	Disabled	Transport is Disabled
Disabled	Down	Connecting	**Valid only for M3UA :** Trying establishing the SCTP connection. But ASP-UP will not be sent afterwards.
	Down	Blocked	**Valid only for M3UA :** SCTP Transport has been established. But is has been blocked for any M3UA traffic.

Transport Operational Status and Reason

This list shows the possible values that may appear in the **Operational Status** and **Reason** fields of the Transport Maintenance page. The **Operational Status** is either **Up** or **Down**. **Up** indicates that the Transport is ready for M3UA signaling. **Down** indicates that the Transport is not ready for M3UA signaling. If the **Status** is **Down**, the **Operational Reason** provides information about why it is down.

Possible values of the **Operational Reason** field where **Status=Down** are:

- **Disabled**-the Transports's administrative state is **Disabled**.This is the initial operational status and reason for a newly configured Transport. This reason is also shown when an Transport is manually disabled.
- **Application Disabled**-the Transport's administrative state is **Enabled** or **Blocked**, and the application state has been manually **Disabled** via the **Server Status** page.
- **Connecting**-the administrative state is **Enabled** or **Blocked**, but the SCTP 4-way handshake has not yet completed xxxxxxxxxxxxxxx.
- **Up Pending**-the administrative state is **Enabled**, but the ASP-UP has not yet been acknowledged.
- **Blocked**-the administrative state is **Blocked**, and the SCTP 4-way handshake has completed successfully.
- **Forced Standby**-the administrative state is **Enabled** or **Blocked**, and the MP server's HA state has been manually set to **Forced Standby** via the **HA Status** page. All signaling is inhibited for MP servers that are in the **Forced Standby** state.

Possible values of the **Operational Reason** field where **Status=Up** are:

- **Normal**-this is the desired status. This status occurs when the administrative state is **Enabled** and the ASP-UP has been ACKed.

Viewing the Status of a Transport

You can use the Transport Maintenance page to view the administrative status of transports.

Select **Transport Manager>Maintenance>Transport.**

The **Transport Maintenance** page appears listing all transports and their operational status.

Note: To see the IP addresses of the Adjacent Node, click on the "+" button in the Adjacent Node field.

For a description of the operational status and reason, see *Transport Operational Status and Reason*.

For a descripton of the administrative state relationships, see *Admin State Relationships*.

Enabling a Transport

When a Transport is put in the **Enabled** administrative state, the MP server associated with the Transport begins attempts to bring the Transport to the SCTP Established state and the ASP-UP state.

You can enable multiple transports at the same time.

1. Select **Transport Manager>Maintenance>Transport**.

   The **Transport Maintenance** page appears.

2. Click on the row with the Transport you wish to enable to highlight it.

   The **Enable** link is not grayed out if the Transport's administrative state is already **Enabled**. Also if collection on the server is not working, all actions (**Enable**, **Block**, and **Disable**) are active to give the user control when the status is unknown. The MP server will simply disregard the command if the Transport is already in the selected administrative state.

3. Click the **Enable**button at the bottom of the screen.

   A confirmation message appears.

4. Click **OK** to confirm.

   The **Operational Status** field shows **Up**. The **Up/Down Since** column now indicates when the Transport transitioned into the **Up** status. The orange color is removed from the **Admin State** field. The **Enable** action is now grayed out.

The Transport is enabled.

Disabling a Transport

⚠️ **Caution:** Disabling an Transport causes an Transport alarm, and possibly, alarms for Links, Link Sets, Routes, or node isolation.

CAUTION

When an Transport is put in the **Disabled** administrative state, the MP server begins attempts to bring the Transport to the SCTP Closed state and the ASP-DOWN states.

1. Select **Transport Manager>Maintenance>Transports**.

   The **Transports Maintenance** page appears.

2. Click on the **Pause Updates** checkbock for the page (lower right corner) so you can view the results of your selections during this procedure. You can also click the menu option on the main menu to manually update the page.

3. Click on the row that contains the transport to highlight it. **Disable** in the row of the appropriate Transport.

   The **Disable** link is not grayed out if the Transport's administrative state is already **Disabled**. Also if collection on the server is not working, all actions (**Enable**, **Block**, and **Disable**) are active to give the user control when the status is unknown. The MP server will simply disregard the command if the Transport is already in the selected administrative state.

4. Click **Disable**

   A confirmation message appears.

5. Click **OK** to confirm.

   The **Operational Status** field shows **Down**. The The **Admin State** field shows **Disabled**. The **Disable** button at the bottom of the page is now grayed out.

The Transport is disabled.

Blocking a Transport

Note: Blocking an Transport causes an Transport alarm, and possibly, alarms for Links, Link Sets, Routes, or node isolation.

When a Transport is put in the **Blocked** administrative state, the MP server begins attempts to bring the Transport to the SCTP Established protocol state and the ASP-DOWN state. The MP server does not attempt to send ASP-UP.

1. Select **Transport Manager>Maintenance>Transports**.

   The **Transports Maintenance** page appears.

2. Click the **Pause Updates** checkbox (lower right corner) so that you can view the results of your selection during this procedure. You can also click the menu option on the main menu to update the page.

3. Click on the row containing the transport you wish to block to highlight it.

4. Click the **Block** button.

   The **Block** button is not grayed out if the Transport's administrative state is already **Blocked**. Also if collection on the server is not working, all actions (**Enable**, **Block**, and **Disable**) are active to give the user control when the status is unknown. The MP server will simply disregard the command if the Transport is already in the selected administrative state.

   A confirmation message appears.

5. Click **OK** to confirm.

   The **Operational Status** field shows **Blocked**. The **Admin state** column now indicates when the Transport transitioned into the **Blocked** status. The **Block** button is no longer available.

The Transport is blocked.

Signaling configuration

Signaling configuration consists of setting up the SS7/Sigtran data for each signaling Network Element, or site. This requires completing several tasks that fall into four main categories:

1. *Site topology configuration*
2. *Adjacent server configuration*
3. *SS7 address configuration*
4. *Routing Configuration*

Site topology is configured using the Configuration menu of a GUI hosted on the active NOAMP server. The remaining steps are configured using the SS7/Sigtran Configuration menu on GUIs hosted on the active SOAM for each site.

Site topology configuration

Site topology configuration is done from a GUI hosted on the active NOAMP server. Site topology consists of defining signaling network elements, assigning MP servers to each signaling network element, and creating server groups for the servers.

The steps for setting up site topology are:

1. Create a signaling Network Element
2. Add servers to each signaling Network Element

   a. two servers for the SOAM pair
   b. one server for each MP at the site

3. Place all servers into server groups

   a. one server group for the SOAM pair
   b. one server group for each MP server

Creating a signaling network element

HLRR network elements can be created by using an XML configuration file. Users are required to create individual XML files for each of your HLRR network elements.

Signaling network elements are created using the GUI hosted by the active NOAMP. A maximum of 40 signaling network elements can be configured. A signaling network element should be configured for each site that will independently manage its SS7/Sigtran network.

1. Select **Configuration > Network Elements**.

   The **Network Elements** page appears.

   Note: You can use the **Filter** dropdown to narrow the results.

2. Click **Browse**. Navigate to the location of XML configuration file. This assumes that the required configuration files have already been created.
3. Select the configuration file.
4. Select **Upload File**.

   If the selected file passes the validation rules, a successful banner is displayed.

The network element is added to the topology database tables, and the GUI displays the updated Network Elements table.

Adding servers to each signaling network element

After the signaling network element has been provisioned you can add servers to the network element using the active NOAMP GUI to **Insert** new servers. Each signaling network element requires two servers for the SOAM pair, plus enough MP servers to support the required Sigtran traffic. The number of MP servers configured for each site must be sufficient to process the Sigtran traffic when an MP has failed or is down for maintenance.

Note: XSI does not need to be configured for HLR Router.

Use this procedure to insert a server:

1. Select **Configuration > Servers**.
2. Click **Insert** at the bottom of the table.

   The **Adding a new server** page appears.

3. Enter a **Host Name**.

   This is a user-defined name for the server and must be unique. The Hostname can be 1 - 20 alphanumeric characters, but must start with a letter.

4. Select a role from the **Role** pulldown menu.

   - If the server is being added for the SOAM, select **SOAM**.
   - If the server is not being added to the SOAM select **MP**.

5. Select the name of the signaling network element the server belongs to from the **Network Element Name** pulldown menu.

6. Enter a **Location**.

   This is an optional field that allows you to enter text to identify the physical location of the server.

7. If the Role of the server being added is **SOAM**, enter the IP address of the external management interface in the **XMI** field.

   Note: If the Role is MP, this field should be left blank.

8. Enter the IP address of the internal management interface in the **IMI** field.
9. Enter the Server console RMM Address in the **RMM** field.
10. Click **OK** to submit the information and return to the Servers Configuration page.
11. Repeat this task for every server that needs to be added to the signaling network element.

Placing servers into server groups

After the servers have been assigned to signaling network elements you must create server groups using the active NOAMP GUI. Placing servers into a server group gives the servers a Function and Redundancy Model. One server group is needed for the SOAM pair in each signaling network element. One server group is needed for each MP server.

1. Select **Configuration > Server Groups**.
2. Click **Insert**.

   The **Insert Server Groups** page appears.

3. Enter the **Server Group Name.**

   The name can be up to 32 alphanumeric characters. It must contain one letter.

4. Select a role from the **Role** pulldown menu.

   - If the server group is for the SOAM pair, select **SYSTEM OAM** from the **Role** pulldown menu.
   - If the server group is for an MP server, select **MP** from the **Role** pulldown menu.

5. Select a **Function** from the pulldown menu.

   - If the server group is for the SOAM pair, select **NONE** from the **Function** pulldown menu.
   - If the server group is for an EXHR MP server, select **EAGLE XG HLR Router** from the **Function** pulldown menu.

6. Select a **Redundancy Model** from the pulldown menu.

   - If the server group is for the SOAM pair, select **Active/Standby with VIP** from the **Redundancy Model** pulldown menu.
   - If the server group is for an EXHR MP server, select **Stateless Cluster** from the **Redundancy Model** pulldown menu.

7. If the server group is for the SOAM pair, enter the **Virtual IP Address** for the server group.

8. If the server group is for the SOAM pair, enter the **Subnet Mask** for the server group.

9. Click **OK** to submit the information and return to the Server Groups page.

10. Select the server group just added and click **Edit**.

    The **Server Groups Edit** screen appears.

11. If the server group is for the SOAM pair

    a) select two servers from the Available Servers in Network Element list (using ctrl or shift-click as desired)

    b) drag the selected servers to the Existing Servers in Server Group list

12. If the server group is for an MP server, drag one server from the Available Servers in Network Element list to the Existing Servers in Server Group list.

13. Repeat this task until all servers have been added to server groups.

Each site will have two SOAM servers and from two to ten MP servers. Each MP server is in its own server group.

Adjacent server configuration

Adjacent server configuration is done from a GUI hosted on the active SOAM server for each site. Adjacent servers represent the servers (E5Enet cards for example) on the Sigtran Signaling Gateway (for example EAGLE IPSG) that will host M3UA associations. These adjacent servers are grouped into adjacent server groups that share an SS7 point code. For example, all the adjacent server used to carry Sigtran traffic for a given SS7 point code are grouped into one adjacent server group.

The steps for Adjacent server configuration are:

1. Configure an adjacent server for each IP address that will host the SG side of an M3UA association

2. Create adjacent server groups for each SS7 point code that will be adjacent to your MP servers (i.e. connected via M3UA associations)

Creating Adjacent Servers

You should create an Adjacent Server for every IP card on each EAGLE. You can only perform this task when logged into an SOAM.

1. Select **SS7/Sigtran>Configuration>Adjacent Servers**

   The **Adjacent Servers** page appears.

2. Click **Insert**.

   The **Insert Adjacent Servers** page appears.

3. Enter a name for the adjacent server in the **Adjacent Server Name** field.

4. Enter the IP address of the adjacent server in the **Primary IP Address** field.

   This IP address is the one on which the adjacent server is listening for M3UA associations.

5. Click **OK** to insert the server and exit this page.

6. Repeat steps 2 through 5 until you have created an adjacent server for every IP card on each EAGLE.

Creating Adjacent Server Groups

You should create Adjacent Server Groups for each EAGLE. You can only perform this task when logged into an SOAM.

1. Select **SS7/Sigtran>Configuration>Adjacent Server Groups**.

   The **Adjacent Server Groups** page appears.

2. Click **Insert**.

   The **Insert Adjacent Server Groups** page appears.

3. Enter a name for the Adjacent Server Group in the **Adjacent Server Group Identifier** field.

   The name should encompass all of the adjacent servers that share an SS7 true point code. This name generally represents an entire IP signaling gateway.

4. The **Unassigned Adjacent Servers** field contains the Adjacent Servers you have created and any other Adjacent Servers on the system that have not yet been assigned to a group. Assign the relevant Adjacent Servers to this Adjacent Server Group by moving them from **Unassigned Adjacent Servers** to **Adjacent Servers in the Adjacent Server Group**. You can

   - Add one server at a time by clicking on the server then clicking the **Add** button
   - Add multiple servers at once by holding down **ctrl** while clicking each Adjacent Server name then clicking the **Add** button
   - Add all servers at once by clicking the Add All button

5. Once you have added all of the relevant Adjacent Servers to this group click **OK** to save the Adjacent Server Group and exit this page.

6. Repeat this task as necessary to create additional Adjacent Server Groups.

   An Adjacent Server Group represents a set of one or more adjacent servers that share a point code on the signaling gateway. If you have multiple EAGLES then you should have multiple Adjacent Server Groups with the Adjacent Servers assigned to the appropriate group.

SS7 address configuration

The next step is to configure SS7 addresses for each MP server, each adjacent signaling gateway, each remote destination you wish to route to, and each remote subsystem you with to communicate with. The steps are as follows:

The steps for SS7 address configuration are:

1. Configure a local SS7 true point code for each MP server group
2. Configure an SS7 point code for each adjacent signaling gateway
3. Configure an SS7 point code for each remote destination to which you need to route M3UA signaling
4. Configure remote subsystems for each remote SCCP peer that you want to communicate with

Local SS7 point code configuration

Each HLR Router MP server must have a local point code by which it can be addressed in the SS7 network. This unique point code is known as the true point code of the MP server. MP servers can also share an alias point code called the capability point code. These point codes are configured on the SS7/Sigtran Local Signaling Points configuration GUI hosted by the active SOAM server for each site.

Configuring local SS7 point codes

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

1. Select **SS7/Sigtran>Configuration>Local Signaling Points.**

   The **Local Signaling Points** page appears.

2. Click **Insert**.

   The Insert Local Signaling Points page appears.

3. Enter a unique name in the **Local Signaling Point Name** field.
   The Local Signaling Point name must start with a letter and can contain up to 32 alphanumeric characters. Underscores are also allowed.

4. Select the type of SS7 domain the node resides in from the **SS7 Domain** pulldown menu.

5. Enter the unique point code for this local signaling point in the **MTP True Point Code** field.

6. If this local signaling point shares a point code with one or more other local signaling points then check the **MTP Capability Point Code** box and enter the point code.

7. The **Unassigned Server Groups** field contains the server groups you have created and any other server groups on the system that have not yet been assigned to a group. Assign a server group to this Local Signaling Point by moving one from **Unassigned Server Groups** to **Server Groups included in this Local Signaling Point**. :

8. Once you have added the server group to this Local Signaling Point click **OK** to save the Local Signaling Point and exit this page.

9. Repeat steps 2 through 8 as necessary to create additional Local Signaling Points.

Remote SS7 point code configuration

Remote signaling points must be created for:

- adjacent point codes
- non-adjacent point codes

Since both adjacent point codes and non-adjacent point codes are classified as remote SS7 point codes, the same procedure is used to configure adjacent and non-adjacent point codes, with the only difference being that the adjacent server group field can be left blank for non-adjacent point codes.

Configuring Remote SS7 point codes

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

1. Select **SS7/Sigtran>Configuration>Remote Signaling Points.**

The **Remote Signaling Points** page appears.

2. Click **Insert**.

   The **Insert Remote Signaling Points** page appears.

3. Enter a unique name in the **Remote Signaling Point Name** field.

   The Remote Signaling Point name must start with a letter and can contain up to 32 alphanumeric characters. Underscores are also allowed.

4. Select the type of SS7 domain the remote signaling point resides in from the **SS7 Domain** pulldown menu.

5. Enter the unique point code for this remote signaling point in the **MTP True Point Code** field.

6. Select the relevant Adjacent Server Group from the **Adjacent Server Group** pulldown menu.

   This is the adjacent signaling gateway you are assigning the remote signaling point code to.

   - A Remote Signaling Point that the application communicates directly with is called an Adjacent Remote Signaling Point and should be assigned an Adjacent Server Group
   - A Remote Signaling Point that the application communicates with via an STP is called a Non-adjacent Remote Signaling Point and should not be assigned an Adjacent Server Group

7. Click **OK** to save the Remote Signaling Point and exit this page.

8. Repeat steps 2 through 7 as necessary to create additional Remote Signaling Points.

The Remote Signaling Points are created.

Remote subsystem configuration

Each remote subsystem that must be communicated with from a site must be configured as a Remote MTP3 User. This is accomplished by using the SS7/Sigtran Remote MTP3 Users GUI hosted by the active SOAM server of a site.

Creating Remote MTP3 Users

You need to configure a remote MTP3 user for each destination that the application routes to using SCCP addressing. You do not need to configure a remote MTP3 user for destinations the application routes to using global title routing. You can only perform this task when logged into an SOAM.

1. Select **SS7/Sigtran>Configuration>Remote MTP3 Users.**

   The **Remote MTP3 Users** page appears.

2. Click **Insert** .

   The **Insert Remote MTP3 Users** page appears.

3. Enter a unique name in the **Remote MTP3 User Name** field.

   The Remote MTP3 User Name must start with a letter and can contain up to 32 alphanumeric characters. Underscores are also allowed.

4. Select the Remote Signaling Point to associate with this Remote MTP3 User from the **Remote Signaling Point** pulldown menu.
   When you select a Remote Signaling Point the **Remote Point Code** field will automatically populate with the associated point code.

5. Enter the subsystem number used to track the status of the RMU in the **Remote SSN** field.

6. Click **OK** to save the Remote MTP3 User Configuration and exit this page.

7. Repeat steps 2 through 6 as necessary to create additional Remote MTP3 Users.

Routing Configuration

Routing configuration connects the local and remote signaling network elements and can only occur after all local and remote signaling network tasks have been completed. Once you have finished the routing configuration tasks the application is ready to perform signaling activities.

The steps to setting up routing configuration are:

1. Create link sets to connect each MP server to the appropriate signaling gateways. In other words, a link set creates a relationship between a local signaling point and an adjacent remote signaling point

2. Configure IP interfaces for each network interface on each MP server in the site

3. Configure IP routes to each customer network for each IP interface

4. For each MP server, create an association to each adjacent server that the MP must signal through

5. Create Links that reference each Association and Link Set

6. Create routes for each Remote Signaling Point and Link Set

7. Enable the Associations

8. Enable the Links

Creating Link Sets

You need to configure a link set for pairs of Local Signaling Points and Adjacent Remote Signaling Points. You can only perform this task when logged into an SOAM.

1. Select **SS7/Sigtran>Configuration>Link Sets**.

    The **Link Sets** page appears.

2. Click **Insert** .

    The **Insert Link Sets** page appears.

3. Enter a unique name in the **Link Set Name** field.

    The Link Set Name must start with a letter and can contain up to 32 alphanumeric characters. Underscores are also allowed.

4. Define the desired relationship between the local and remote peer for this Link Set by selecting a value in the **Mode** pulldown menu.

    AS->SG mode is the only mode supported. AS->SG mode defines the relationship between the local and remote ends of the link set.

5. Select the Local Signaling Point served by this Link Set from the **Local Signaling Point** pulldown menu.

6. Select the point code of the Local Signaling Point to be served by this Link Set.

    If the local signaling point selected for the link set has a capability point code, the link set can receive signaling sent from the SS7 network to either the true point code or the capability point code. The default choice of "All" indicates that both, or all, point codes are acceptable. If no capability

point code is configured for the local signaling point, only signaling sent from the network to the LSP true point code will be processed.

7. Select the Adjacent Remote Signaling Point representing the Adjacent Signaling Gateway to be served by this Link Set from the **Adjacent Remote Signaling Point** pulldown menu.

8. Select **Yes** if a routing context applies to this Link Set or **No** if it does not from the **Assign Routing Context** pulldown menu.

    Routing Context must be specified if links from this Link Set will share an association with links from at least one other Link Set.

9. If the **Assign Routing Context** is set to **Yes** enter a value in the **Routing Context** field.

    This **Routing Context** must be configured to match the Routing Context value configured for this Link Set at the signaling gateway.

10. Click **OK** to save the Link Set and exit this page.

11. Repeat steps 2 through 10 as necessary to create additional Link Sets.

The Link Sets are configured.

Creating Links

You create links to map associations to link sets. You can only perform this task when logged into an SOAM.

1. Select **SS7/Sigtran>Configuration>Links.**
    The **Links** page appears.

2. Click **Insert**.

    The **Insert Links** page appears.

3. Enter a unique name in the **Link Name** field.

    The Link Name must start with a letter and can contain up to 32 alphanumeric characters. Underscores are also allowed.

4. Select the relevant link set from the **Link Set** pulldown menu.

5. Select the relevant association from the **Association** pulldown menu.

6. Click **OK** to save the Link and exit this page.

7. Repeat steps 2 through 6 as necessary to create additional Links.

The Link is created and is in the **Disabled** administrative state.

Route configuration

Routes represent a signaling path from a local signaling point to a remote signaling point using a given link set. Routes are needed for both adjacent and non-adjacent remote signaling points.

Creating Routes

Routes represents a signaling path from a local signaling points to a remote signaling point codes using a given link set. Routes are needed for adjacent remote signaling points to route network management signaling. You can only perform this task when logged into an SOAM.

1. Select **SS7/Sigtran>Configuration>Routes**.

The **Routes** page appears.

2. Click **Insert** .

   The **Insert Routes** page appears.

3. Enter a unique name in the **Route Name** field.

   The Route Name must start with a letter and can contain up to 32 alphanumeric characters. Underscores are also allowed.

4. Select the Remote Signaling Point that identifies the destination of this Route from the **Remote Signaling Point** pulldown menu.
   Selecting a **Remote Signaling Point** automatically populates the **Remote Point Code** field.

5. Select the Link Set for this Route from the **Link Set** pulldown menu.
   Selecting a **Link Set** automatically populates the **Adjacent Point Code** field.

6. Enter a relative cost in the **Relative Cost** field.

   The cost can be set between 0 and 99. The application attempts to route signaling over the routes that have the lowest cost. If two routes have the same cost, signaling is load-shared across both routes.

7. Click **OK** to save the Route and exit this page.

8. Repeat steps 2 through 7 as necessary to create additional Links.

The Routes are created.

Enabling a Link

When a Link is put in the **Enabled** administrative state, the MP server begins attempts to bring the Link to the ASP-ACTIVE state on an active MP server or the ASP-INACTIVE state on a standby MP server.

Links must be enabled one Link at a time.

1. Select **SS7/Sigtran>Maintenance>Links**.

   The **Links Maintenance** page appears.

2. Set the **Auto Refresh** for the page (upper right corner) to **15** so that you can view the results of your selections during this procedure. You can also click the menu option on the main menu to manually update the page.

3. Click **Enable** in the row of the appropriate Link.

   The MP server will disregard the command if the Link is already in the selected administrative state.

   If the link you wish to enable is missing or displayed in gray text, it indicates a management network problem between the MP server and the SOAM server from which your GUI session is hosted.

   A confirmation message appears.

4. Click **OK** to confirm.

   The **Operational Status** field shows **Up**. The **Up/Down Since** column now indicates when the Link transitioned into the **Up** status. The **Enable** action is now grayed out.

The Link is enabled.

Chapter

4

Query Server

Topics:

This section provides information about using a MySQL client to perform free format PDBI database queries.

Query Server access

The Query Server is an independent application server containing a replicated version of the PDBI database. It accepts replicated subscriber data from the NOAMP and stores it in an accessible MySQL database. A Query Server is located in the same physical frame as each NOAMP component (NOAMP / DR NOAMP).

For information about configuring the Query Server see the EAGLE XG HLR Router online help.

To connect to the Query Server you need:

- a MySQL client that is compatible with MySQL 5.0.84
- Query Server IP Address: same as the XMI IP Address. You can find the XMI Address by logging into the HLR Router GUI and selecting **Configuration > Servers**.
- Query Server Port: 15616
- username:

  - qsuser
  - qsadmin - all administrative tasks are done using this login

- user password: qspass
- database name: exhr

The username, password, and database name are all case sensitive.

Once connected you can use select statements and complex queries to examine information within these exhr database tables:

- *Dn table*
- *Dn2Imsi table*
- *Imsi table*
- *Imsi2Dn table*
- *Service table*

Sample queries

Any valid, relevant SQL query can be used to examine Query Server information; provided are some sample queries as an example of the types of queries you may want to run.

Table 26: Sample Queries

Query	Description
SELECT * FROM Imsi2Dn WHERE dn='18000000000'	Find the specified record in a given table
SELECT dn,service FROM exhr.Service JOIN exhr.Dn ON (exhr.Dn.serviceID=exhr.Service.id) WHERE dn='19194602167'	Find E.164 of HLR serving a given DN

Query	Description
SELECT imsi,service FROM exhr.Service JOIN exhr.Imsi ON (exhr.Imsi.serviceID=exhr.Service.id) WHERE imsi='18008888888'	Find E.164 of HLR serving a given IMSI
SELECT imsi FROM exhr.Dn2Imsi WHERE dn='19194602164'	Find IMSI associated with a DN
SELECT dn FROM exhr.Imsi2Dn WHERE imsi='18008888888'	Find DN associated with a IMSI
SELECT exhr.Dn.dn,imsi,service FROM exhr.Service JOIN exhr.Dn JOIN exhr.Dn2Imsi ON (exhr.Dn.serviceID=exhr.Service.id AND exhr.Dn.dn=exhr.Dn2Imsi.dn) WHERE exhr.Dn.dn='19194602164'	Find IMSI and HLR for given Dn
SELECT exhr.Imsi.imsi,dn,service FROM exhr.Service JOIN exhr.Imsi JOIN exhr.Imsi2Dn ON (exhr.Imsi.serviceID=exhr.Service.id AND exhr.Imsi.imsi=exhr.Imsi2Dn.imsi) WHERE exhr.Imsi.imsi='18008888888'	Find DNs and HLR for given IMSI

Dn table

Table 27: Query Server Dn Table Elements

Element	Description
dn	Mobile Subscriber International Subscriber Directory Number
serviceId	Identifier for the service

Dn2Imsi table

Table 28: Query Server Dn2Imsi Table Elements

Element	Description
dn	Mobile Subscriber International Subscriber Directory Number
imsi	International Mobile Subscriber Identity

Imsi table

Table 29: Query Server Imsi Table Elements

Element	Description
imsi	International Mobile Subscriber Identity
serviceId	Identifier for the service

Imsi2Dn table

Table 30: Query Server Imsi2Dn Table Elements

Element	Description
imsi	International Mobile Subscriber Identity
dupId	Multiple DNs can be associated with a single IMSI, which can cause more than one IMSI entry in this table. The dupId field is a unique field used to keep entires with the same IMSI from overwriting each other.
dn	Mobile Subscriber International Subscriber Directory Number

Service table

Table 31: Query Server Service Table Elements

Element	Description
id	Identifier for the service
service	An entity that provides a type of network service; typically the HLR
type	The type of service the Network Entity provides. This is typically HLRR/SP (Home Location Register Router/ Service Provider).
isSsnPresent	Yes indicates a subsystem number is present; No indicates it is not

Element	Description
isTtPresent	Yes indicates a translation type is present; No indicates it is not
isNpPresent	Yes indicates a numbering plan is present; No indicates it is not
isNaiPresent	Yes indicates a nature of address indicator is present; No indicates it is not
ri	The Routing Indicator specifies whether routing is based on SSN or Global Title. If routing is based on the GT, the GT in the address is used for routing. If routing is based on SSN, the SSN in the CdPA is used.
ccgt	Indicates if whether to cancel the called Global Title
pcType	Type of point code for the service
pc	Point code for the service, format should match Point Code Type selected: • ANSI Format: Network-Cluster-Member • INTL Format: ITU international point code. Zone-Area/Network-Signaling Point • NATL Format: ITU national point code. 14 bits interpreted as a single identifier, often referred to as a structureless Point Code
ssn	Optional subsystem number for the service; used to update the CdPA
tt	Optional translation type for the service
np	Optional numbering plan for the service; used to update the CdPA of incoming messages requiring this service
nai	Optional nature of address indicator for the service
da	Determines what changes, if any, should be applied to the CdPA Global Title Address

Logging into the Query Server

Before you perform this task you must have a valid MySQL client set up.

1. Start your MySQL client.
2. Type **`mysql -h <hostname> -P 15616 -u qsuser -p exhr`**

The hostname is the same as the XMI IP Address. You can find the XMI Address by logging into the HLR Router GUI and selecting **Configuration > Servers**.

3. When prompted for a password type **qspass**

You are now logged into the Query Server.

Creating a new user with Query Server access

This task can only be performed when logged in as qsadmin.

1. Start your MySQL client.
2. Type mysql -h <hostname> -P 15616 -u qsadmin -p exhr
3. When prompted for a password type **qspass**
4. Type **CREATE USER '<user>' IDENTIFIED BY '<password>';** then press Enter.
5. When a new prompt appears type **GRANT SELECT ON exhr.Dn TO '<user>';** then press Enter.
6. When a new prompt appears type **GRANT SELECT ON exhr.Imsi TO '<user>';** then press Enter.
7. When a new prompt appears type **GRANT SELECT ON exhr.Dn2Imsi TO '<user>';** then press Enter.
8. When a new prompt appears type **GRANT SELECT ON exhr.Imsi2Dn TO '<user>';** then press Enter.
9. When a new prompt appears type **GRANT SELECT ON exhr.Service TO '<user>';** then press Enter.

A new MySQL user with Query Server access has been created.

Changing a Query Server user's password

Query Server users can only update their own password. To change the password of a user without knowledge of that user's password, login as 'qsadmin', delete the user and re-create the user.

1. Start your MySQL client.
2. Type **mysql -h <hostname> -P 15616 -u <username> -p exhr**
3. When prompted for a password type qspass
4. Type **SET PASSWORD = PASSWORD('<newpassword>');** then press Enter.

The user's password has been changed.

Deleting an existing user with Query Server access

This task can only be performed when logged in as qsadmin.

1. Start your MySQL client.
2. Type `mysql -h <hostname> -P 15616 -u qsadmin -p exhr`
3. When prompted for a password type `qspass`
4. Type `DROP USER '<username>';`

The user has been deleted.

Chapter

5

File Formats

Topics:

This section provides a description of HLR Router files formats including:

*   FIle name formats
*   Signaling Reports
*   Performance Data Export CSV file formats

File name formats

This table describes the file name formats for HLR Router import and export files. These variables are used in the file name formats:

- **<server name>** or **<hostname>** is the server hostname from which the file is generated.
- **<application name>** is the name of the application.
- **<groupname>** is the type of data stored in the backup file.
- **<NodeType>** specifies whether the backup was generated on an NOAMP or SOAM.
- **<time_date>** or **<YYYYMMDD_HHMMSS>** is the date and time that the file was generated.
- **(AUTO | MAN)** indicates whether the backup was automatically or manually generated.

Table 32: File Name Formats

File Type	File Name	Description
Backup	**Backup.<application name>.<hostname>.<groupname> [And<groupname>… [And <groupname>]] .<NodeType>.YYYYMMDD_HHMMSS.(AUTO | MAN).tbz2**	A BZIP2 compressed tar file (tape archive format). This format can contain a collection of files in each tbz2 file. This file must be unzipped before it can be viewed.
Logs	**Logs.<application name>.<server name>.<time_date>.tgz**	Log file. This is a g-zipped (GNU zip) tar file (tape archive format). This format can contain a collection of files in each tgz file. This file must be unzipped before it can be viewed.
Measurements	**Meas.<application name>.<server name>.<time_date>.csv**	Comma-separated value file format used for storing tabular data. Measurement reports can be exported to the file management storage area, and are stored in csv format.
PDBI Export	export_<id>.<datatype>.<yyyymmdd><hhmm>.<format>	PDBI export files are stored locally on the NOAMP in the file management storage area. Provisioning data type exported

File Type	File Name	Description
		(Scheduled exports only) possible values: • all: All data types • ne: Network Entities • imsi: IMSIs • dn: DNs Export file format possible values: • pdbi: (PDBI format) • csv: (comma-separated values format)
PDBI Import	**import_<filename>.pdbi**	Import file names on the remote server must be prefixed with "import_" and suffixed with ".pdbi" to be automatically downloaded and imported into the EXHR system's provisioning database.
PDBI Import Log File	**import_<filename>.pdbi.log**	An import log file is created for each file that is imported and a copy is automatically uploaded to the same location the import file was downloaded from on the remote server. The log file has the same name as its corresponding import file with ".log" appended.
PDE CSV Files	AlarmsEvents_<timestamp>.csv	Alarms and events collected on active NOAMP and SOAMs
	ActiveAlarms_<timestamp>.csv	Active alarms (critical, major, minor) collected on active NOAMP and SOAMs

File Type	File Name	Description
	Meas_<timestamp>.csv	Either • Measurements data collected on active NOAMP from downstream SOAM and MPs • Measurements data collected on active SOAM from downstream MPs
	KPI_<timestamp>.csv	Either • KPI data collected on active NOAMP from downstream SOAM and MPs • KPI data collected on the active SOAM from downstream MPs
	PdbiLog_<timestamp>.csv	PDBI command logs collected on active NOAMP
	SecuLog_<timestamp>.csv	A-source security logs collected on active NOAMP from downstream SOAMP and MPs
	PdbiStatus_<timestamp>.csv	PDBI Status data collected on the active NO server
	Association_SS7_<timestamp>.csv	Site based Association SS7 configuration data collected on the active SO servers
	Route_SS7_<timestamp>.csv	Site based Route SS7 configuration data collected on the active SO servers
	RMU_SS7_<timestamp>.csv	Site based RMU SS7 configuration data collected on the active SO servers

File Type	File Name	Description
	Link_SS7_<timestamp>.csv	Site based Link SS7 configuration data collected on the active SO servers
	Linkset_SS7_<timestamp>.csv	Site based Linkset SS7 configuration data collected on the active SO servers
	MatedHLR_SS7_<timestamp>.csv	Site based Mated HLR configuration data collected on the active SO servers
	ExceptionRouting_SS7_<timestamp>.csv	Site based Exception Routing configuration data collected on the active SOAM servers
	AdjacentServerAndGroup_SS7_<timestamp>.csv	Site based Adjacent Server and Group configuration data collected on the active SOAM servers
	LocalSignalingPoint_SS7_<timestamp>.csv	Site based Local Signaling Point configuration data collected on the active SOAM servers
	RemoteSignalingPoint_SS7_<timestamp>.csv	Site based Remote Signaling Point configuration data collected on the active SOAM servers
	AssocConfigSet_SS7_<timestamp>.csv	Site based Association Configuration Set data collected on the active SOAM servers
	SccpOptions_SS7_<timestamp>.csv	Site based SCCP Options configuration data collected on the active SOAM servers
	Mtp3Options_SS7_<timestamp>.csv	Site based MTP3 Options configuration data collected on the active SOAM servers

File Type	File Name	Description
	M3uaOptions_SS7_<timestamp>.csv	Site based M3UA Options configuration data collected on the active SOAM servers
	LocalCongestionOptions_ SS7_<timestamp>.csv	Site based Local Congestion Options configuration data collected on the active SOAM servers

Note: It is recommended that policies be developed to prevent overuse of the storage area. These might include a procedure to delete export files after transferring them to an alternate location, or removing backup files after a week, for example.

Signaling reports

You can export signaling reports that provide details about various aspects of your signaling network.

For information about running each signaling report see the section of the HLR Router online help relevant to the report you want to run.

Associations report elements

This table describes the fields contained within an Associations report. For information about running this report see the task Generating a report on Associations in the HLR Router online help.

Table 33: Associations Report Elements

Field	Description
Report Summary	Includes: • Report Generated: Date and time report was run • From: Server the user was logged into when running the report • Report Version: Application version • User: Login ID of the user who ran the report
Associations Summary	Information provided is organized by the Association and includes: • MP Server Hostname: Hostname of the MP server that hosts the local end of the SCTP Association

Field	Description
	• MP Server IP Address: IP Address hosted by the MP Server that is bound to this SCTP Association • Adjacent Server: Adjacent server for the association • Local SCTP Port: Local SCTP port number for this SCTP Association • Remote SCTP Port: Remote SCTP port number for this SCTP Association • Configuration Set Name: SCTP configuration parameter set used for this SCTP Association
Associations Configuration Sets Report	Information provided is organized by the Association and includes: • Configuration Set Name: Name of the configuration set the association is related to • M3UA Connection Mode: Type of M3UA signaling process that hosts the Associations using this configuration set • SCTP Connection Mode: This is current disabled in the application and should not contain a value
Adjacent Servers Report	Information provided is organized by the Association and includes: • Adjacent Server Name: Remote server identifier • Primary IP Address: Primary IP address of the adjacent server

Links report elements

This table describes the fields contained within a Links report. For information about running this report see the task Generating a report on Links in the HLR Router online help.

Table 34: Links Report Elements

Field	Description
Report Summary	Includes: • Report Generated: Date and time report was run • From: Server the user was logged into when running the report • Report Version: Application version • User: Login ID of the user who ran the report

Field	Description
Links Summary	Information provided is organized by the Link and includes: • Link Set: Link Set the link belongs to • Association: Association for the link
Link Sets Report	Information provided is organized by the Link and includes: • Link Set Name: Name of the Link Set • Mode: Relationship between the local and remote peer for this Link Set • Local Signaling Point: Local Signaling Point served by this Link Set • LSP Point Code: Point code of the selected Local Signaling Point • Adjacent Remote Signaling Point: Adjacent Remote Signaling Point representing the Adjacent Signaling Gateway • Routing Context: Message parameter used to uniquely identify the application context
Associations Report	Information provided is organized by the Link and includes: • Association Name: Association identifier • Hostname: Hostname of the MP server that hosts the local end of the SCTP Association • MP Server IP Address: IP Address hosted by the MP Server that is bound to this SCTP Association • Adjacent Server: Adjacent Server that hosts the remote end of the SCTP Association • Local SCTP Port: Local SCTP port number for this SCTP Association • Remote SCTP Port: Remote SCTP port number for this SCTP Association • Configuration Set Name: SCTP configuration parameter set used for this SCTP Association

Link Sets report elements

This table describes the fields contained within a Link Sets report. For information about running this report see the task Generating a report on Link Sets in the HLR Router online help.

Table 35: Link Sets Report Elements

Field	Description
Report Summary	Includes: • Report Generated: Date and time report was run • From: Server the user was logged into when running the report • Report Version: Application version • User: Login ID of the user who ran the report
Link Sets Summary	Information provided is organized by the Link Set and includes: • Mode: Relationship between the local and remote peer for this Link Set • Local Signaling Point: Local Signaling Point served by this Link Set • LSP Point Code: Point code of the selected Local Signaling Point • Adjacent Remote Signaling Point: Adjacent Remote Signaling Point representing the Adjacent Signaling Gateway • Routing Context: Message parameter used to uniquely identify the application context
Remote Signaling Points Report	Information provided is organized by the Link Set and includes: • Remote Signaling Point Name: Remote signaling point identifier • SS7 Domain: SS7 Domain in which the node resides • MTP Point Code: MTP point code that identifies this Local Signaling Point • Adjacent Server Group: Name of the adjacent server group
Local Signaling Points Report	Information provided is organized by the Link Set and includes: • Local Signaling Point Name: Local signaling point identifier • SS7 Domain: SS7 Domain in which the node resides • MTP True Point Code: MTP point code that identifies this Local Signaling Point • MTP Capability Point Code: MTP point code that this Local Signaling Point share with another

Field	Description
Associations Report	Information provided is organized by the Remote Signaling Point Name and includes: • Association Name: Association identifier • Hostname: Hostname of the MP server that hosts the local end of the SCTP Association • MP Server IP Address: IP Address hosted by the MP Server that is bound to this SCTP Association • Local SCTP Port: Local SCTP port number for this SCTP Association • Remote SCTP Port: Remote SCTP port number for this SCTP Association • Configuration Set Name: SCTP configuration parameter set used for this SCTP Association

Local Signaling Points report elements

This table describes the fields contained within a Local Signaling Points report. For information about running this report see the task Generating a report on Local Signaling Points in the HLR Router online help.

Table 36: Local Signaling Points Report Elements

Field	Description
Report Summary	Includes: • Report Generated: Date and time report was run • From: Server the user was logged into when running the report • Report Version: Application version • User: Login ID of the user who ran the report
Local Signaling Points Summary	Information provided is organized by the Local Signaling Point Name. Includes: • SS7 Domain: SS7 Domain in which the node resides • MTP True Point Code: MTP point code that identifies this Local Signaling Point • MTP Capability Point Code: MTP point code that this Local Signaling Point share with another • ServerGroupName: Server Groups that serve this Local Signaling Point

Field	Description

Server Groups Report	Information provided is organized by the Local Signaling Point Name and includes:
	
	• Server Group Identifier: Server Group the server for this local signaling point belongs to
	• Network Element Name: Name of the Network Element the Server Group is assigned to
	• Redundancy Model:
	
	  • Active/Standby with VIP - two servers in an active/standby relationship that share a VIP
	  • Active/Standby without VIP - two servers in an active/standby relationship that do not share a VIP
	  • Stateless Cluster - servers in this model do not participate in a high availability (active/standby) relationship
	
	• Heartbeat Interval (ms): Interval at which messages are sent; measured in milliseconds
	• UDP Port: UDP port number

Remote Signaling Points report elements

This table describes the fields contained within a Remote Signaling Points report. For information about running this report see the task Generating a report on Remote Signaling Points in the HLR Router online help.

Table 37: Remote Signaling Points Report Elements

Field	Description
Report Summary	Includes: • Report Generated: Date and time report was run • From: Server the user was logged into when running the report • Report Version: Application version • User: Login ID of the user who ran the report
Remote Signaling Points Summary	Information provided is organized by the Remote Signaling Point Name. Includes: • SS7 Domain: SS7 Domain in which the node resides • MTP Point Code: MTP point code that identifies this Local Signaling Point

Field	Description
	• Adjacent Server Group: Name of adjacent server group • Remote MTP3 Users: Remote MTP3 user identifier • Assocaition Name: Association identifier
Adjacent Server Groups Report	Information provided is organized by the Remote Signaling Point Name and includes: • Adjacent Server Name: remote server identifier • Primary IP Address: Primary IP address of the adjacent server
Remote MTP3 Users Report	Information provided is organized by the Remote Signaling Point Name and includes: • Remote MTP3 User Name: Remote MTP3 user identifier • Remote Point Code: Remote point code configured in the selected Remote Signaling point. • Remote SSN: Specific subsystem number to track the status of the Remote MTP3 User
Associations Report	Information provided is organized by the Remote Signaling Point Name and includes: • Association Name: Association identifier • Hostname: Hostname of the MP server that hosts the local end of the SCTP Association • MP Server IP Address: IP Address hosted by the MP Server that is bound to this SCTP Association • Local SCTP Port: Local SCTP port number for this SCTP Association • Remote SCTP Port: Remote SCTP port number for this SCTP Association • Configuration Set Name: SCTP configuration parameter set used for this SCTP Association

Routes report elements

This table describes the fields contained within a Routes report. For information about running this report see the task Generating a report on Routes in the HLR Router online help.

Table 38: Routes Report Elements

Field	Description
Report Summary	Includes: • Report Generated: Date and time report was run • From: Server the user was logged into when running the report • Report Version: Application version • User: Login ID of the user who ran the report
Routes Summary	Information provided is organized by the Link Set and includes: • Remote Signaling Point: Identifies the destination of Route • Remote Signaling Point Code: Point code of the remote signaling point • Link Set: Link Set used by this route • Adjacent Point Code: Point code configured in the Adjacent Remote Signaling Point being used by the Link Set • Relative Cost: Relative Cost of route
Remote Signaling Points Report	Information provided is organized by the Link Set and includes: • Remote Signaling Point Name: Remote signaling point identifier • SS7 Domain: SS7 Domain in which the node resides • MTP Point Code: MTP point code that identifies this Local Signaling Point
Linkset Report	Information provided is organized by the Remote Signaling Point Name and includes: • Link Set Name: Name of the linkset • Mode: Relationship between the local and remote peer for this Link Set • Local Signaling Point: Local Signaling Point served by this Link Set • LSP Point Code: Point code of the selected Local Signaling Point

PDE CSV File Formats

PDE feature will generate collected reports in a CSV (Comma-Separated-Value) format. This section provides information about the content of these CSV files. For information about file name formats for the PDE CSV files see *File name formats*.

PDE Active Alarms CSV File Format

This table describes the fields contained within a PDE Active Alarms CSV file.

Table 39: PDE Active Alarms CSV File

Field	Description
Seq#	OAM server wide unique sequence number assigned to each alarm
AlarmNum	Unique number assigned to each alarm in the system
TimeStamp	Date and time the alarm occurred
Severity	Alarm severity – Critical, Major, Minor, Info
Product	Name of the product or application that generated the alarm
Process	Name of the process that generated the alarm
NE	Name of the Network Element where the alarm occurred
Server	Name of the Server where the alarm occurred
Type	Alarm Type e.g. Link, Disk, SW, CPU, LOG, HA
Instance	Instance of the alarm, e.g. Link01 or GUI
AlarmText	Description of the alarm
AddlInfo	Additional information about alarm that might help fix the root cause of alarm

PDE KPI CSV File Format for centralized configuration data

This table describes the fields contained within a PDE KPI CSV file generated on the active NOAMP server.

Table 40: PDE KPI CSV File (Centralized Configuration Data)

Field	Description
Network Element	Name of the Network Element where the KPI is collected
Server Hostname	Name of the Server where the KPI is collected
Connections	PDBI client connections currently established
Received Msgs/Sec	PDBI messages received per second
Successful Msgs/Sec	PDBI messages successful per second
Failed Msgs/Sec	PDBI messages failed per second
Sent Msgs/Sec	PDBI messages sent per second
Discarded Msgs/Sec	PDBI messages discarded per second
Imported Msgs/Sec	PDBI messages imported per second
Committed Txns/Sec	PDBI transactions committed per second to the database (memory and on disk) on the active server of the primary NOAMP cluster
Failed Txns/Sec	PDBI transactions failed per second
Aborted Txns/Sec	PDBI transactions aborted per second
Txns Active	PDBI transactions currently active (Normal transaction mode only)
Txns Non-Durable	PDBI transactions committed, but not yet durable
CPU	Percentage utilization of all processors on the server by all software as measured by the operating system
RAM	Percentage utilization of physical memory on the server by all software
Swap	Percentage utilization of swap space on the server by all software
Uptime	Total amount of time the server has been running. Format: Days HH:MM:SS

PDE KPI CSV File Format for decentralized configuration data

This table describes the fields contained within a PDE KPI CSV file generated on the active SOAM server.

Table 41: PDE KPI CSV File (Deentralized Configuration Data)

Field	Description
Network Element	Name of the Network Element where the KPI is collected
Server Hostname	Name of the Server where the KPI is collected
GttPerformed	Total number of global title translations performed
ExhrGttExceptionRouting	Number of times exception routing was used
SCCP Xmit Msgs/Sec	Number of SCCP messages transmitted per second
SCCP Recv Msgs/Sec	Number of CCP messages received per second
SS7 Process CPU Utilization	Average percentage of SS7 Process CPU utilization (0-100%) on a MP server
Ingress Message Rate	Average Ingress Message Rate (messages per second) utilization on a MP server
M3RL Xmit Msgs/Sec	M3RL DATA MSUs/Sec sent
M3RL Recv Msgs/Sec	M3RL DATA MSUs/Sec received
CPU	Percentage utilization of all processors on the server by all software as measured by the operating system
RAM	Percentage utilization of physical memory on the server by all software
Swap	Percentage utilization of swap space on the server by all software
Uptime	Total amount of time the server has been running. Format: Days HH:MM:SS

PDE Measurements CSV File Format

This table describes the fields contained within a PDE Measurements CSV file.

Table 42: PDE Measurements CSV File

Field	Description
Node	Name of the Server where measurement is collected
MeasName	Name of the measurement
Type	Type of the measurement
Total	Totsl count of the measurement

PDE PDBI Command Logs CSV File Format

This table describes the fields contained within a PDE PDBI Command Logs CSV file.

Table 43: PDE PDBI Command Logs CSV File

Field	Description
SrcNode	Name of the node/server on which the info was obtained
TimeStamp	Date and time the PDBI command occurred
SystemId	PDBI system identifier
ConnectId	PDBI connection identifier
Msg	PDBI request or response message

PDE Security Logs CSV File Format

This table describes the fields contained within a PDE Security Logs CSV file.

Table 44: PDE Security Logs CSV File

Field	Description
Seq#	OAM server wide unique sequence number assigned to each GUI user interaction
Server	Name of the Server where the GUI user interaction occurred
NE	Name of the Network Element where the GUI user interaction occurred
TimeStamp	Date and time the GUI user interaction occurred
Status	Status of the interaction: SUCCESS, ERROR, UNKNOWN
Status Message	A short string explaining the interaction and its status
Data	A free text containing extra data about the GUI user interaction

PDE PDBI Status CSV file format

This table describes the fields contained within a PDE PDBI Status CSV file.

Table 45: PDE PDBI Status CSV File

Field	Description
dblevel	Database Level
Birthdate	Database Birth Date
imsi count	The total number of IMSI's
dn count	The total number of DN's
ne count	The total number of NE's

SS7 Association Configuration CSV File Format

This table describes the fields contained within a SS7 Association Configuration CSV file.

Table 46: SS7 Association Configuration CSV File

Field	Description
Association Name	Name that uniquely identifies this Association
MP Server Hostname	Hostname of the MP server that will host the local end of the SCTP Association
MP Server IP Address	IP Address hosted by the MP Server that will be bound to this SCTP Association
Adjacent Server	Adjacent Server that will host the remote end of the SCTP Association
Adjacent Server IP Address	IP Address configured for the Adjacent Server to host the remote end of the SCTP Association
Local SCTP Port	Local SCTP port number for this SCTP Association
Remote SCTP Port	Remote SCTP port number for this SCTP Association
Configuration Set Name	SCTP configuration parameter set to be used for this SCTP Association

SS7 Route Configuration CSV file format

This table describes the fields contained within a PDE SS7 Route Configurations CSV file.

Table 47: PDE SS7 Route Configuration CSV File

Field	Description
Route Name	Name that uniquely identifies the Route

Field	Description
Remote Signaling Point	RSP that identifies the destination of this Route
Remote Point Code	Point code configured in the selected RSP
Link Set	Link Set to be used by this route
Adjacent Point Code	Point code configured in the Adjacent RSP being used by the selected Link Set
Relative Cost	Relative cost assigned to this route

SS7 RMU Configuration CSV file format

This table describes the fields contained within a PDE SS7 RMU Configuration CSV file.

Table 48: PDE SS7 RMU Configuration CSV File

Field	Description
Remote MTP3 User Name	Name that uniquely identifies the Remote MTP3 User
Remote Signaling Point	RSP associated with this Remote MTP3 User
Remote Point Code	Remote point code configured in the selected Remote Signaling point
Remote SSN	Specific subsystem number to track the status of the Remote MTP3 User

SS7 Link Configuration CSV file format

This table describes the fields contained within a PDE SS7 Link Configuration CSV file.

Table 49: PDE SS7 Link Configuration CSV File

Field	Description
Link Name	Name that uniquely identifies the link
Link Set	Link Set to which the link is being added
Association	SCTP Association that will host the link

SS7 Linkset Configuration CSV file format

This table describes the fields contained within a PDE SS7 Linkset Configuration CSV file.

Table 50: PDE SS7 Linkset Configuration CSV File

Field	Description
Link Set Name	Name that uniquely identifies this Link Set
Mode	Desired relationship between the local and remote peer for this Link Set
Local Signaling Point	LSP served by this Link Set
LSP Point Code	Point code of the selected Local Signaling Point to be served by this Link Set
Adjacent Remote Signaling	Name of the Adjacent RSP representing the Adjacent Signaling Gateway to be served by this Link Set
Routing Context	Message parameter used to uniquely identify the application context

SS7 Mated HLR CSV file format

This table describes the fields contained within a SS7 Mated HLR CSV file.

Table 51: SS7 Mated HLR CSV File

Field	Description
HLR	A string that uniquely identifies the primary Home Location Register
HLRpc	The point code associated with this primary Home Location Register
HLRssn	The subsystem number associated with this primary Home Location Register
MateHLR	A string that uniquely identifies the backup Home Location Register
MateHLRpc	The point code associated with this backup Home Location Register
MateHLRssn	The subsystem number associated with this backup Home Location Register

SS7 Exception Routing CSV file format

This table describes the fields contained within a SS7 Exception Routing CSV file.

Table 52: SS7 Exception Routing CSV File

Field	Description
TT	The Called Party Address Translation Type of the incoming message
NP	The Called Party Address Numbering Plan of the incoming message
MPpc	The True Point Code (or the Capability Point Code) of the MP processing the incoming message
ExceptionHLR	A string that uniquely identifies the exception Home Location Register
ExceptionHLRpc	The point code associated with this exception Home Location Register
ExceptionHLRssn	The subsystem number associated with this exception Home Location Register

SS7 Adjacent Servers and Groups CSV file format

This table describes the fields contained within a SS7 Adjacent Servers and Groups CSV file.

Table 53: SS7 Adjacent Servers and Groups CSV File

Field	Description
Adjacent Server Name	A string that uniquely identifies the an Adjacent Server, which is a remote server, serving as the far end of an SCTP Association (for example, a signaling gateway).
Primary IP Address	Primary IP address of Adjacent Server
Adjacent Server Group Identifier	Unique identifier used to label an Adjacent Server Group.

SS7 Local Signaling Point CSV file format

This table describes the fields contained within a SS7 Local Signaling Point CSV file.

Table 54: SS7 Local Signaling Point CSV File

Field	Description
Local Signaling Point Name	Unique identifier used to label a logical element representing an SS7 Signaling Point assigned to an MP server group
SS7 Domain	The SS7 Domain in which the node resides.

Field	Description
MTP True Point Code	The MTP point code that identifies this LSP. Only one LSP can have this MTP True point code.
MTP Capability Point Code(s)	The MTP capability point code if this LSP shares a point code with one or more other LSPs.

SS7 Remote Signaling Point CSV file format

This table describes the fields contained within a SS7 Remote Signaling Point CSV file.

Table 55: SS7 Remote Signaling Point CSV File

Field	Description
Remote Signaling Point Name	Unique identifier used to label an RSP (Remote Signaling Point) represents an SS7 network node (point code) that signaling must be sent to from EAGLE XG HLR Router
SS7 Domain	The SS7 Domain in which the node resides.
MTP Point Code	The MTP point code that identifies this LSP. Only one LSP can have this MTP True point code.
Adjacent Server Group	Unique identifier used to label an Adjacent Server Group.

SS7 Association Configuration Set CSV file format

This table describes the fields contained within a SS7 Association Configuration Set CSV file.

Table 56: SS7 Association Configuration Set CSV File

Field	Description
AssociationCFGSet_Name	A name that uniquely identifies the SCTP Association Configuration Set.
M3UA_Connection_Mode	The type of M3UA signaling process that hosts the Associations using this configuration set.
SCTP_Connection_Mode	This field is currently disabled with Client selected.
Retrans_Initial_Timeout	The expected average network round-trip time in milliseconds.
Retrans_Min_Timeout	The minimum amount of time to wait for an acknowledgment for a message sent.
Retrans_Max_Timeout	The maximum amount of time to wait for an acknowledgment for a message sent.

Field	Description
Retrans_Assoc_Failure	The number of consecutive retransmits that will cause an SCTP Association to be marked as failed
Retrans_Init_Failure	The number of consecutive retransmits for INIT and COOKIE-ECHO chunks that will cause an SCTP Association to be marked as failed.
SACK_Delay	The number of milliseconds to delay after receiving a DATA chunk and prior to sending a SACK
Heartbeat_Interval	The interval in milliseconds between sending SCTP HEARTBEAT messages to a peer.
Connection_Retry_Interval	The interval in seconds between connection attempts when the connection is unsuccessful.
Sock_Send_Size	The socket send buffer size for outgoing SCTP messages.
Sock_Recv_Size	The socket receive buffer size for incoming SCTP messages

SS7 SCCP Options CSV file format

This table describes the fields contained within a PDE SS7 SCCP Options CSV file.

Table 57: PDE SS7 SCCP Options CSV File

Field	Description
Variable	A name of the SCCP option
Value	A value of the SCCP option

SS7 MTP3 Options CSV file format

This table describes the fields contained within a PDE SS7 MTP3 Options CSV file.

Table 58: PDE SS7 SCCP Options CSV File

Field	Description
Variable	A name of the MTP3 option
Value	A value of the MTP3 option

SS7 M3UA Options CSV file format

This table describes the fields contained within a PDE SS7 M3UA Options CSV file.

Table 59: PDE SS7 M3UA Options CSV File

Field	Description
Variable	A name of the M3UA option
Value	A value of the M3UA option

SS7 Local Congestion Options CSV file format

This table describes the fields contained within a PDE SS7 M3ULocal CongestionA Options CSV file.

Table 60: PDE SS7 Local Congestion Options CSV File

Field	Description
Variable	A name of the Local Congestion option
Value	A value of the Local Congestion option

Glossary

A

Adjacent Server Group

A collection of Adjacent Servers that implements a distributed IP signaling function.The group represents a set of Adjacent Servers that share a point code on the signaling gateway.An Adjacent Server Group has a name and a list of Adjacent Servers.

ANSI

American National Standards Institute

An organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system. ANSI develops and publishes standards. ANSI is a non-commercial, non-government organization which is funded by more than 1000 corporations, professional bodies, and enterprises.

C

CdPA

Called Party Address

The field in the SCCP portion of the MSU that contains the additional addressing information of the destination of the MSU. Gateway screening uses this additional information to determine if MSUs that contain the DPC in the routing label and the subsystem number in the called party address portion of the MSU are allowed in the network where the EAGLE 5 ISS is located.

CPU

Central Processing Unit

C

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.

G

GT

Global Title Routing Indicator

GUI

Graphical User Interface

The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

H

HA

High Availability

High Availability refers to a system or component that operates on a continuous basis by utilizing redundant connectivity, thereby circumventing unplanned outages.

HLR

Home Location Register

A component within the Switching Subsystem of a GSM network. The HLR database is the central database within the GSM

H

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

ID

Identity, identifier

IMSI

International Mobile Subscriber Identity

A unique internal network ID identifying a mobile subscriber.

International Mobile Station Identity

INTL

FNAI class International

ITU

International Telecommunications Union

An organization that operates worldwide to allow governments and the private telecommunications sector to coordinate the deployment and operating of telecommunications networks and services. The ITU is responsible for regulating, coordinating and developing international telecommunications, and for harmonizing national political interests.

L

LSP

Local Signaling Point

L

A logical element representing an SS7 Signaling Point. The Local Signaling Point assigns a unique primary/true point code within a particular SS7 Domain to an MP server.

M

M3UA

SS7 MTP3-User Adaptation Layer

M3UA enables an MTP3 User Part to be connected to a remote MTP3 via a reliable IP transport.

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&P 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.

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

Module Test Plan

MTP3

Message Transfer Part, Level 3

N

N

NATL

    FNAI class National

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.

    Network Entity

Network Element

    See NE

NOAMP

    Network Operations, Administration, Maintenance, and Provisioning

O

OAM

    Operations, Administration, and Maintenance

    The application that operates the Maintenance and Administration Subsystem which controls the operation of many products.

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.

S

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.

SCTP	Stream Control Transmission Protocol

An IETF transport layer protocol, similar to TCP that sends a message in one operation.

The transport layer for all standard IETF-SIGTRAN protocols.

SCTP is a reliable transport protocol that operates on top of a connectionless packet network such as IP and is functionally equivalent to TCP. It establishes a connection between two endpoints (called an association; in TCP, these are sockets) for transmission of user messages.

SG	Secure Gateway

Signaling Gateway

A network element that receives/sends SCN native signaling at the edge of the IP network. The SG function may relay, translate or terminate SS7 signaling in an SS7-Internet Gateway. The SG function may also be coresident with the MG function to process SCN signaling associated with line or trunk terminations controlled by the MG (e.g., signaling backhaul). A Signaling Gateway could be modeled as one or more Signaling Gateway

S

Processes, which are located at the border of the SS7 and IP networks. Where an SG contains more than one SGP, the SG is a logical entity and the contained SGPs are assumed to be coordinated into a single management view to the SS7 network and to the supported Application Servers.

Sigtran

Signaling Transport

SOAM

System Operations, Administration, and Maintenance

Site Operations, Administration, and Maintenance

SS7

Signaling System #7

A communications protocol that allows signaling points in a network to send messages to each other so that voice and data connections can be set up between these signaling points. These messages are sent over its own network and not over the revenue producing voice and data paths. The EAGLE 5 ISS is an STP, which is a device that routes these messages through the network.

SSN

SS7 Subsystem Number

The subsystem number of a given point code. The subsystem number identifies the SCP application that should receive the message, or the subsystem number of the destination point code to be assigned to the LNP subsystem of the EAGLE 5 ISS.

Subsystem Number

S

A value of the routing indicator portion of the global title translation data commands indicating that no further global title translation is required for the specified entry.

Subsystem Number

Used to update the CdPA.

STP

Signal Transfer Point

The STP is a special high-speed switch for signaling messages in SS7 networks. The STP routes core INAP communication between the Service Switching Point (SSP) and the Service Control Point (SCP) over the network.

Spanning Tree Protocol

SW

Software
Switch

U

UDP

User Datagram Protocol