

Oracle® Communications
EAGLE LNP Application Processor
Administration and LNP Feature Activation Guide
E58656 Revision 1

December 2014

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

Chapter 1: Introduction.....	16
Overview	17
Scope and Audience.....	17
Manual Organization.....	18
Documentation Admonishments.....	19
My Oracle Support (MOS).....	20
Emergency Response.....	20
Related Publications.....	21
Customer Training.....	21
Locate Product Documentation on the Oracle Technology Network Site.....	21
 Chapter 2: ELAP Administration.....	 22
EAGLE LNP Application Processor (ELAP).....	23
ELAP Initialization and First Configuration.....	23
 Chapter 3: ELAP Functional Description.....	 24
Definition of Terms.....	25
Overall Design.....	26
Overview of the ELAP User Interfaces.....	28
ELAP Switchover.....	29
Network Connections.....	30
LSMS-to-ELAP Connection.....	32
Network Time Protocol (NTP).....	32
Support ELAP Reload Via Database Image Function.....	34
Network Address Translation on MPS.....	35
ELAP Security Functions.....	36
LSMS/ELAP PING Enhancement.....	37
Service Module Card Provisioning.....	37
Incremental Loading.....	38
Service Module Card Reload.....	38
Service Module Card Warm Restart.....	38
MPS/Service Module Card RTDB Audit Overview.....	38
General Description.....	38

Functional Description.....	39
Chapter 4: ELAP Graphical User Interface.....	41
Overview of ELAP Graphical User Interface.....	42
ELAP Support for HTTPS on GUI	43
Login Screen.....	51
ELAP GUI Main Screen.....	52
ELAP GUI Menus.....	57
Select Mate.....	58
Process Control Menu.....	59
Maintenance Menu.....	59
RTDB Menu.....	67
Debug Menu.....	74
Platform Menu.....	78
User Administration Menu.....	80
Change Password.....	90
Logout.....	91
ELAP Messages.....	92
ELAP Error Messages.....	92
Chapter 5: LNP Feature Activation.....	97
The LNP Solution.....	98
The LNP Feature.....	98
LNP-Related Features and Functions.....	98
Chapter 6: LNP Feature Description.....	101
LNP Message Relay.....	102
LNP Query Service (LNPQS).....	110
The LNP Local Subsystem.....	120
Hardware, System, and Feature Requirements.....	122
Chapter 7: LNP Feature Configuration.....	123
Introduction.....	124
System Prerequisites.....	124
LNP Feature Prerequisites.....	125
LNP Feature Activation Procedure.....	126
LNP Feature Configuration on the EAGLE.....	133
Adding an LNP Service.....	136

Removing an LNP Service.....	141
Changing an LNP Service.....	142
Changing LNP Options.....	144
Changing the LNP Telephone Number Alarm Thresholds.....	149
Adding a Subsystem Application.....	150
Removing a Subsystem Application.....	152
Increasing the LRN and NPANXX Quantities on the EAGLE.....	153
Activating the LNP Local Subsystem.....	154
Changing the State of a Subsystem Application.....	156
Increasing LNP Telephone Number Quantity on EAGLE.....	158
LNP Short Message Service Feature Configuration.....	159
LNP SMS Feature Prerequisites.....	159
LNP Short Message Service (LNP SMS) Feature Configuration Procedure.....	160
Turning Off the LNP Short Message Service Feature.....	161
Clearing a Temporary FAK Alarm.....	162
ITU TCAP LRN Query (LRNQT) Feature Configuration.....	163
LRNQT Feature Prerequisites.....	163
ITU TCAP LRN Query (LRNQT) Feature Configuration Procedure.....	164
Triggerless LNP Feature Configuration.....	165
Configuring the Service Module Card Ethernet Link to the MPS.....	171
Removing DSM Cards.....	175

Chapter 8: LNP Measurements.....177

LNP Measurements.....	178
-----------------------	-----

Chapter 9: EMS, RTDB, and LSMS-Related Functions.....182

EMS Routing.....	183
EMS Configuration Component.....	183
Creating an EMS Configuration Component.....	183
Modifying an EMS Configuration Component.....	187
Viewing an EMS Configuration Component.....	189
Deleting an EMS Configuration Component.....	190
Managing Bulk Load from the LSMS.....	192
Bulk Load Procedure.....	192
Support ELAP Reload Via Database Image Function.....	198
Bulk Load Log File.....	204
Bulk Load Error Messages.....	206
Copying One RTDB from Another RTDB.....	206
Verifying RTDB Status.....	207
Verifying RTDB Status at the EAGLE Terminal.....	207

Verifying RTDB Status at the ELAP User Interface.....	208
Restore RTDB on ELAP.....	209
Copy RTDB from Remote.....	211
Distributing the LNP Database after LSMS-Based Operation or RTDB Copy.....	212
Distributing an RTDB to Service Module Cards.....	213
Disabling Bulk Load.....	215
Manually Verifying and Restarting the Eagle Agents on the LSMS.....	215

Chapter 10: EAGLE 5 Status Reporting and Alarms for ELAP and

LNP.....	217
EAGLE 5 Status and Alarm Reporting.....	218
Maintenance Blocks.....	218
Alarm Priorities.....	219
Multiple Alarm Conditions.....	219
Service Module Card Status Requests and Status Messages.....	220
EAGLE 5 Maintenance Commands.....	221
Unsolicited Alarm Messages and Unsolicited Information Messages.....	222
ELAP-to-Service Module Card Connection Status.....	223
Feature Quantity Capacity UAMs.....	225
Physical Memory Usage UAMs.....	226
EAGLE Service Module Card Audit UIMs.....	227
Measurement Capacity UIMs.....	227

Chapter 11: Automatic Call Gapping (ACG) Configuration.....229

Overview.....	230
Determining the ACG Node Overload Control Level Query Rates.....	233
Adding an ACG Node Overload Control Level.....	236
Removing an ACG Node Overload Control Level.....	237
Changing an ACG Node Overload Control Level.....	238
Adding ACG Manual Initiated Controls.....	238
Removing ACG Manual Initiated Controls.....	240
Changing ACG Manual Initiated Controls.....	240

Appendix A: ELAP Software Configuration.....242

Setting Up an ELAP Workstation.....	243
Screen Resolution.....	243
Compatible Browsers.....	243
Java.....	243

ELAP Configuration and Initialization.....	248
Required Network Address Information	249
ELAP Firewall Port Assignments.....	250
Configuration Menu Conventions.....	251
Overview of ELAP Configuration.....	253
ELAP Configuration Procedure.....	261
MPS Health Check Procedure.....	279
 Appendix B: Time Zone File Names.....	 281
Time Zone File Names.....	282
 Appendix C: ELAP Local Provisioning Utility.....	 284
Introduction.....	285
LPU Commands.....	285
Update Commands.....	285
Delete Commands.....	297
Retrieve Command.....	300
Miscellaneous Commands.....	301
Common Information.....	302
Perl Statements and Functions.....	304
Glossary.....	307

List of Figures

Figure 1: Typical ELAP Installation	27
Figure 2: ELAP Restore the RTDB GUI with servdiDownload Option.....	35
Figure 3: NAT on MPS.....	36
Figure 4: Process Architecture View of the ELAP UI.....	43
Figure 5: ELAP Login.....	45
Figure 6: Security Certificate.....	45
Figure 7: HTTPS Login Page.....	45
Figure 8: Certificate Error.....	46
Figure 9: Certificate.....	46
Figure 10: Certificate Import Wizard.....	47
Figure 11: Certificate Store.....	48
Figure 12: Select Certificate Store.....	48
Figure 13: Certificate Store.....	49
Figure 14: Completing the Certificate Import Wizard.....	50
Figure 15: Security Warning.....	50
Figure 16: Import Successful.....	51
Figure 17: ELAP Banner Applet.....	52
Figure 18: ELAP Alarm Information Area.....	53
Figure 19: LSMS Connection Status Area.....	54
Figure 20: Service Module Card Status.....	54
Figure 21: Status of an Individual Card.....	55
Figure 22: Service Module Card Status Information.....	56

Figure 23: ELAP Menu.....	58
Figure 24: Maintenance Menu.....	60
Figure 25: View High Availability Status Screen.....	61
Figure 26: Automatic RTDB Backup screen.....	62
Figure 27: Maintenance / ELAP Transaction Logging / View Configuration.....	66
Figure 28: Maintenance / ELAP Transaction Logging / Change Configuration.....	66
Figure 29: RTDB Menu.....	68
Figure 30: Local Provisioning Menu.....	71
Figure 31: Debug Menu.....	74
Figure 32: View Maintenance Log Password Screen.....	75
Figure 33: View Maintenance Log Screen.....	76
Figure 34: Connect to MMI Port Screen.....	77
Figure 35: Platform Menu.....	78
Figure 36: List All Running Processes Screen.....	79
Figure 37: User Administration Menu.....	80
Figure 38: Specify the UI User's Permissions Screen.....	83
Figure 39: User Administration / Groups Menu.....	85
Figure 40: List All Authorized UI IP Addresses Screen.....	87
Figure 41: Terminate Active Sessions Screen.....	88
Figure 42: Modify System Defaults Screen.....	89
Figure 43: Change Password Screen.....	91
Figure 44: Message Flow For Global Title Translation and Message Relay.....	107
Figure 45: LNP Query Processing.....	114
Figure 46: LNP Service Determination Process.....	116
Figure 47: Inter-Network Support for LNP Queries.....	119

Figure 48: View LSMS Connection Allowed Dialog.....	128
Figure 49: Change LSMS Connection Allowed Dialog.....	128
Figure 50: Change LSMS Connection Allowed - Disable Success Dialog.....	129
Figure 51: View LSMS Connection Allowed - Connection Enabled Dialog.....	130
Figure 52: Change LSMS Connection Allowed - Connection Disabled Dialog.....	130
Figure 53: Change LSMS Connection Allowed - Enable Success Dialog.....	131
Figure 54: View LSMS Connection Allowed - Connection Enabled Dialog.....	131
Figure 55: Change LSMS Connection Allowed - Connection Enabled Dialog.....	132
Figure 56: Change LSMS Connection Allowed - Disable Success Dialog.....	132
Figure 57: View LSMS Connection Allowed - Connection Enabled Dialog.....	132
Figure 58: Change LSMS Connection Allowed - Connection Disabled Dialog.....	133
Figure 59: Change LSMS Connection Allowed - Enabled Success Dialog.....	133
Figure 60: LNP System Menu – Create EMS.....	183
Figure 61: Create LNP System EMS Address Info Tab.....	184
Figure 62: Create LNP System EMS Component Info.....	185
Figure 63: Create LNP System EMS Contact Info.....	186
Figure 64: Update Successful Dialog.....	187
Figure 65: Field Required Dialog.....	187
Figure 66: LNP System Menu – Modify EMS.....	188
Figure 67: Modify LNP System EMS Window.....	188
Figure 68: EMS Routing Dialog.....	189
Figure 69: Update Successful Dialog.....	189
Figure 70: More Fields Needed Dialog.....	189
Figure 71: View LNP System EMS Dialog.....	190
Figure 72: Delete LNP System EMS Dialog.....	191

Figure 73: Update Successful Dialog.....	191
Figure 74: ELAP Main Menu.....	193
Figure 75: Enabling Change HS Bulk Download	193
Figure 76: Bulk Load Window.....	194
Figure 77: Abort Bulk Load Operation Dialog.....	196
Figure 78: Bulk Load Complete Information Dialog.....	196
Figure 79: Bulk Load Complete.....	197
Figure 80: ELAP Reload Via DB Image Function.....	198
Figure 81: ELAP Reload Via DB Image.....	199
Figure 82: Generate Image.....	200
Figure 83: Database Image Completed.....	200
Figure 84: Abort Bulk Download.....	201
Figure 85: Abort Confirmation.....	202
Figure 86: Transfer Database Image to ELAP.....	203
Figure 87: Image Transfer Complete.....	203
Figure 88: Open Log Files Window.....	204
Figure 89: Example Bulk Load Log File.....	205
Figure 90: ELAP Main Screen.....	208
Figure 91: ELAP RTDB Status.....	209
Figure 92: Stopping Software on the ELAP GUI.....	210
Figure 93: Stop ELAP Software - Success.....	210
Figure 94: Restore the RTDB.....	210
Figure 95: Confirm RTDB Restore.....	211
Figure 96: Successful RTDB Restoration.....	211
Figure 97: Copy RTDB from Remote Screen.....	211

Figure 98: Copy RTDB from Remote Selection.....	212
Figure 99: Change LSMS HS Bulk Download Enabled Dialog.....	215
Figure 100: Security Warning Window.....	244
Figure 101: License Agreement.....	244
Figure 102: Java Installation Progress Window.....	245
Figure 103: Java Installation Complete Window.....	246
Figure 104: Java Control Panel, Java Tab.....	247
Figure 105: Java Runtime Settings Dialog Box.....	247
Figure 106: Configuration Menu Header Format.....	252
Figure 107: Initial Configuration Text Screen	253
Figure 108: Initial Configuration Continues	253
Figure 109: Entering the elapdev Password.....	254
Figure 110: ELAP Configuration Menu	254
Figure 111: Example of Display Configuration Output.....	255
Figure 112: Configure Network Interfaces Menu.....	256
Figure 113: Configure Provisioning Network Output.....	256
Figure 114: Configure DSM Network.....	257
Figure 115: Configuring NAT Addresses Prompt.....	257
Figure 116: Select Time Zone Menu.....	258
Figure 117: Exchange Secure Shell Keys Output.....	258
Figure 118: Change Password	258
Figure 119: Platform Menu Output.....	259
Figure 120: Main Menu View.....	279
Figure 121: Platform Folder Open View.....	279
Figure 122: Run Health Check View.....	280

List of Tables

Table 1: Admonishments.....	19
Table 2: ELAP Switchover Matrix.....	29
Table 3: Sample Network IP Addresses Configured from UI.....	30
Table 4: IP Addresses on the DSM Network.....	31
Table 5: Inconsistent Service Module Card Alarm.....	39
Table 6: Corrupted RTDB Database Alarm.....	40
Table 7: Effect of Corrupted record received from MPS.....	40
Table 8: Options for ELAP Transaction Logging.....	67
Table 9: Navigation Commands.....	76
Table 10: ELAP UI Logins.....	81
Table 11: ELAP Error Messages.....	92
Table 12: LNP Message Relay.....	103
Table 13: LNP Message Relay - Ported Subscribers.....	104
Table 14: LNP Message Relay - Nonported Subscribers.....	105
Table 15: LNP Query OPCODE Values.....	115
Table 16: System Prerequisites.....	124
Table 17: LNP Feature Prerequisites.....	125
Table 18: Example LNP Service Configuration.....	138
Table 19: Changing the LNP Service.....	143
Table 20: LNPOPTS Configuration Options.....	145
Table 21: Subsystem Allow /Inhibit.....	155
Table 22: LNP SMS Feature Prerequisites.....	159

Table 23: LRNQT Feature Prerequisites.....	163
Table 24: Commands to Display the Last Screen in a GWS Screen Set.....	169
Table 25: Procedures for Changing GWS Screens to include the TLNP Stop Action.....	169
Table 26: Procedures to Create a GWS Screen Set with a TLNP Stop Action.....	170
Table 27: Procedures to Assign a Screen Set to a Linkset for TLNP.....	170
Table 28: Procedures to Create a Linkset and Assign a Screen Set to the Linkset for TLNP.....	171
Table 29: Valid Subnet Mask Parameter Values.....	172
Table 30: Pegs for Daily Maintenance (MTCD) and Hourly Maintenance (MTCH) Per System LNP Measurements.....	178
Table 31: Pegs for Daily Maintenance (MTCD) and Hourly Maintenance (MTCH) Per SSP LNP Measurements.....	179
Table 32: Pegs for Daily Maintenance (MTCD) and Hourly Maintenance (MTCH) LNP LRN Measurements.....	181
Table 33: Pegs for Daily Maintenance (MTCD) and Hourly Maintenance (MTCH) LNP NPA Measurements.....	181
Table 34: Fields in Bulk Load Window	195
Table 35: EAGLE 5 MPS Application and Platforms UAM Alarms.....	218
Table 36: MPS Platform and ELAP Alarm Category UAMs.....	223
Table 37: MPS Available UAM.....	223
Table 38: RTDB Audit Alarms.....	224
Table 39: Feature Quantity Capacity Alarms.....	225
Table 40: Physical Memory Usage Alarms.....	227
Table 41: Measurement Capacity UIMs.....	227
Table 42: Duration and Gap Interval Index Values.....	230
Table 43: ACG NOC Configuration Examples.....	235
Table 44: Commands to Set ACG NOC Levels in Example 1 and Example 2.....	236

Table 45: Information for MPS at EAGLE 5 ISS A.....	249
Table 46: Information for MPS at EAGLE 5 ISS B.....	250
Table 47: Firewall Requirements.....	251
Table 48: Sample IP Addresses Used in Configuration.....	255
Table 49: MPS Configuration Symbols.....	262
Table 50: Time zone File Names.....	282
Table 51: Mapping EAGLE 5 ISS to upd_lnp_npanxx LPU Command.....	291
Table 52: Mapping EAGLE 5 ISS to upd_lnp_lrn LPU Command.....	296

Chapter 1

Introduction

Topics:

- *Overview17*
- *Scope and Audience.....17*
- *Manual Organization.....18*
- *Documentation Admonishments.....19*
- *My Oracle Support (MOS).....20*
- *Emergency Response.....20*
- *Related Publications.....21*
- *Customer Training.....21*
- *Locate Product Documentation on the Oracle Technology Network Site.....21*

This chapter provides a brief overview of the Oracle Communications EAGLE LNP Application Processor (ELAP). The chapter also includes the scope, audience, and organization of the manual; how to contact Oracle for assistance and locate product documentation.

Overview

This manual is organized into two main parts.

ELAP Administration

The ELAP Administration part describes how to administer the Oracle Communications EAGLE LNP Application Processor (ELAP), and how to use the ELAP user interface menus to perform configuration, maintenance, debug, and platform operations.

ELAP and the EAGLE LNP feature support from 24 to 384 million LNP ported Telephone Numbers (TNs) that are provisioned in the Real Time Database (RTDB), which is the implementation of a Number Portability Database (NPDB) on the EAGLE. The LNP Feature Activation part describes the available configurations.

The MPS hardware platform supports high-speed provisioning of large databases for the EAGLE. The MPS is composed of hardware and software components that interact to create a secure and reliable platform.

MPS running ELAP supports subscriber provisioning from the Local Service Management System (LSMS) to the EAGLE Services Module cards.

LNP Feature Activation

The LNP Feature Activation part describes the LNP Query and LNP Message Relay functions of the Local Number Portability (LNP) feature, the LNP local subsystem, and related features and functions.

The LNP Feature Configuration chapter contains procedures that can be used by database administration personnel or translations personnel to make the LNP feature and the following the LNP-related functions and features fully operational on the EAGLE:

- LNP services
- LNP options
- LNP local subsystem application
- Triggerless LNP feature
- Mapping of LNP translation types
- Increased LRN and NPANXX feature quantities on the EAGLE
- LNP Short Message Service (LNP SMS) feature
- ITU TCAP LRN Query (LRNQQT) feature
- Automatic Call Gapping

Scope and Audience

This manual is intended for anyone responsible for the following activities:

- Configuration and administration of ELAP

- Use of the ELAP text-based and Graphical User Interfaces
- Configuration the Local Number Portability (LNP) feature, LNP services, configuration options, LNP local subsystem application, and other LNP-related features and functions on the EAGLE.

Users of this manual and the other manuals in the EAGLE family of documents must have a working knowledge of telecommunications and network installations.

Manual Organization

This manual is organized as follows:

- [Introduction](#) contains general information about ELAP, LNP, and the organization of this manual.

ELAP Administration

- [ELAP Administration](#) describes the chapters and appendices which relate to the administration and configuration of ELAP.
- [ELAP Functional Description](#) describes ELAP functions and overall design, RTDB auditing, and ELAP status reporting and alarms.
- [Overview of ELAP Graphical User Interface](#) describes the ELAP GUI menus and screens and the use of the GUI.

LNP Feature Activation

- [LNP Feature Activation](#) describes the LNP Solution, LNP and LNP-related features, and chapters associated with these features.
- [LNP Feature Description](#) provides detailed descriptions of the LNP feature and LNP-related functions and features.
- [LNP Feature Configuration](#) describes the procedures used to configure these functions and features of the EAGLE for LNP:
 - The LNP feature
 - LNP services
 - LNP Local Subsystem Application
 - LNP configuration options
 - Mapping LNP translation types
 - Increased LRN and NPANXX quantities
 - The LNP Short Message Service (LNP SMS) feature
 - The Triggerless LNP (TLNP) feature
 - The ITU TCAP LRN Query (LRNQ) feature
- [LNP Measurements](#) describes LNP measurements, measurements reports, and methods of collection.
- [Automatic Call Gapping \(ACG\) Configuration](#) describes the procedures used to configure automatic Call Gapping for the LNP feature.

LSMS, ELAP, and LNP Functions and EAGLE Status Reporting

- [EMS, RTDB, and LSMS-Related Functions](#) describes and contains procedures for EMS configuration, bulk load management, and RTDB management.
- [EAGLE 5 Status Reporting and Alarms for ELAP and LNP](#) describes ELAP and LNP alarms, LNP UIMs, and EAGLE maintenance commands.





Appendices

- [ELAP Software Configuration](#) describes the ELAP workstation and the ELAP text-based interface, and contains the procedure for ELAP initialization and first configuration.
- [Time Zone File Names](#) lists the time zone file names used for setting the time zone in ELAP software configuration.
- [ELAP Local Provisioning Utility](#) describes the ELAP Local Provisioning Utility (LPU) batch command language.

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 <i>personal injury</i> .)
 WARNING	Warning: (This icon and text indicate the possibility of <i>equipment damage</i> .)
 CAUTION	Caution: (This icon and text indicate the possibility of <i>service interruption</i> .)
 TOPPLE	Topple: (This icon and text indicate the possibility of <i>personal injury and equipment damage</i> .)

My Oracle Support (MOS)

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

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

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

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

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

Emergency Response

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

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

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

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

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications Reference* document, which is published as a separate document on the Oracle Technology Network (OTN) site. See [Locate Product Documentation on the Oracle Technology Network Site](#) for more information.

Customer Training

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

<http://education.oracle.com/communication>

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

www.oracle.com/education/contacts

Locate Product Documentation on the Oracle Technology Network Site

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

1. Log into the Oracle Technology Network site at <http://docs.oracle.com>.
2. Select the **Applications** tile.
The **Applications Documentation** page appears.
3. Select **Apps A-Z**.
4. After the page refreshes, select the **Communications** link to advance to the **Oracle Communications Documentation** page.
5. Navigate to your Product and then the Release Number, and click the **View** link (note that the Download link will retrieve the entire documentation set).
6. To download a file to your location, right-click the **PDF** link and select **Save Target As**.

Chapter 2

ELAP Administration

Topics:

- [*EAGLE LNP Application Processor \(ELAP\).....23*](#)
- [*ELAP Initialization and First Configuration.....23*](#)

The first part of this manual describes ELAP functions, the ELAP Graphical User Interface, and ELAP status reporting.

EAGLE LNP Application Processor (ELAP)

This ELAP Administration part describes how to administer the EAGLE LNP Application Processor (ELAP) after the initialization and first configuration are complete.

[ELAP Functional Description](#) describes ELAP platform, maintenance, and debug functions.

[ELAP Graphical User Interface](#) describes the ELAP Graphical User Interface (GUI) menus and how to use them to perform configuration, maintenance, debug, and platform operations.

ELAP Initialization and First Configuration

Before the ELAP GUI can be used, the activities described in [ELAP Software Configuration](#) must be performed:

- Workstation setup - connection of a local terminal to the MPS.
- Initialization and first configuration of the ELAP software for a new installation or an upgrade - log in as the "elapconfig" user, allow the automatic initialization to complete on both mated ELAPs, and perform the ELAP software configuration procedure using the text-based interface.

Note: All network connections and the mate ELAP must be present and verified to allow the initial configuration to complete successfully.

When the initialization and first configuration are complete, the ELAP Graphical User Interface (GUI) will be available for use.

Chapter 3

ELAP Functional Description

Topics:

- *Definition of Terms.....25*
- *Overall Design.....26*
- *Service Module Card Provisioning.....37*
- *MPS/Service Module Card RTDB Audit Overview.....38*

This chapter describes the overall design and main functions of ELAP, and Service Module card RTDB audit functions .

Definition of Terms

The following terms are used in this manual.

Database	Database refers to all data that can be administered by the user, including shelves, cards, links, routes, global title translation tables, and gateway screening tables.
ELAP	<p>The EAGLE LNP Application Processor (ELAP) is application software that runs on each MPS.</p> <p>One MPS server running ELAP is referred to as ELAP A, while the mate MPS server running ELAP is referred to as ELAP B.</p> <p>The two MPS servers running ELAP at each EAGLE location have exactly the same software installed.</p>
MPS	<p>One EAGLE Application B Card (E5-APP-B Card) is referred to as an MPS server.</p> <p>The two MPS servers that are located at one EAGLE location are <i>mate servers</i> —from one MPS server, the other MPS server can be referred to as its mate. The two servers are also referred to as <i>Server A</i> and <i>Server B</i>.</p>
MPS System	<p>An MPS system consists of two MPS servers and associated hardware that are located at one EAGLE location.</p> <p>Usually, a minimum of two MPS systems are deployed in the customer network (one at each mated EAGLE). These two MPS systems are considered <i>mate MPS systems</i> on mated EAGLE.</p>
RTDB	<p>The implementation of the Number Portability Database on the EAGLE is the Real Time Database or RTDB. The <i>master</i> or <i>golden</i> copy of the RTDB resides on the primary ELAP, and is loaded to and updated on each Service Module card in the EAGLE.</p> <p>The RTDB is provisioned from customer data that is sent from LSMS to ELAP. The RTDB can contain up to 384 million LNP ported TN entries.</p>
Service Module card	Service Module card refers to the E5-SM4G card or the E5-SM8G-B card that contains the Real Time Database (RTDB) downloaded from an ELAP system. If a specific type of Service Module card is required, that Service Module card type is stated explicitly.
System Software	System software refers to data that cannot be administered by the user, including generic program loads (GPLs).
"the LNP feature"	The LNP quantity feature that is enabled in the EAGLE. The LNP feature quantities range from 24 through 384 million telephone numbers, in increments of 12 million. The enabled quantity is shown in the output of the <code>rtrv-ctrl-feat</code> command, in the <code>LNP ported TNs</code> entry.

Overall Design

The main functions of ELAP are:

- Accept and store data provisioned by the customer from LSMS over the provisioning network
- Update and reload provisioning data to the EAGLE Service Module cards.

The Multi-Purpose Server (MPS) hardware platform supports high-speed provisioning of large databases for the EAGLE. The MPS system is composed of hardware and software components that interact to create a secure and reliable platform.

During normal operation, information flows through the ELAP with no intervention.

ELAP provides two direct user interfaces for performing configuration, maintenance, debugging, and platform operations. See [Overview of the ELAP User Interfaces](#).

[Figure 1: Typical ELAP Installation](#) illustrates a typical ELAP installation.

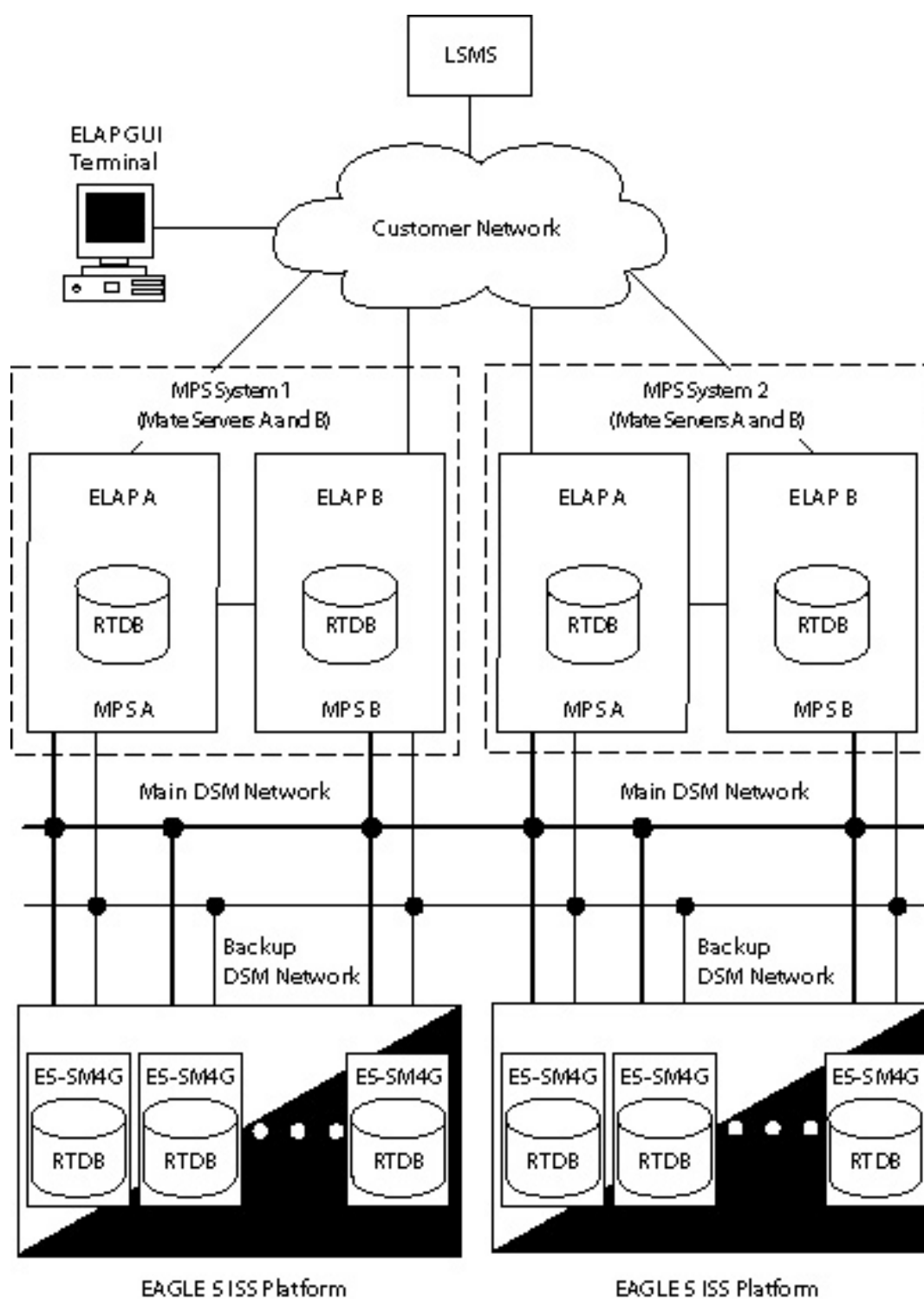


Figure 1: Typical ELAP Installation

An MPS system consists of two mated EAGLE Application B Cards (E5-APP-B cards), which are MPS Server A and MPS Server B, installed as part of an EAGLE. Each server runs ELAP: ELAP A on MPS Server A and ELAP B on MPS Server B.

Two Ethernet networks, referred to as the A and B DSM networks, connect the Service Module cards and the ELAPs. Another Ethernet network connects the two ELAPs, and is referred to as the ELAP Sync network. (See [Network Connections](#).)

Figure 1: Typical ELAP Installation shows the network layout. *Table 4: IP Addresses on the DSM Network* shows examples of typical IP addresses of the network elements.

The ELAPs connect to the LSMS at ELAP initialization and receive provisioning data from the LSMS. The ELAPs store the provisioning data in redundant copies of the Real-Time Database (RTDB) and use the data to provision the EAGLE. Each Service Module card holds a copy of the RTDB.

The A and B DSM networks are redundant, load-balanced, 1GigE full duplex networks that carry provisioning data from the RTDBs on the ELAP to the RTDBs on the Service Module cards. If one DSM network fails, the Active ELAP uses the other DSM network to continue provisioning the RTDBs on the Service Module cards.

One ELAP runs as the Active ELAP and the other as the Standby ELAP. In normal operation, the RTDB on each Service Module card is provisioned through the DSM network by the Active ELAP. In case of failure of the Active ELAP, the Standby ELAP takes over the role of Active ELAP and continues to provision the RTDBs on the Service Module cards.

The LNP feature uses the “master” or “golden” Real-Time Database (RTDB) that is loaded from the ELAP to Service Module cards on the EAGLE. Up to 18 Service Module cards can be used to contain the RTDB on the EAGLE.

ELAP and the LNP feature support a maximum of 24 million to 384 million Telephone Numbers (TNs) in the RTDB. LNP quantity feature part numbers with feature access keys are used to enforce quantity limits. The LNP ELAP Configuration feature indicates that ELAP is used for LNP in the system. The LNP ELAP Configuration feature must be enabled before LNP can be enabled and must be turned on before LNP becomes operational in the system.

Two additional features, LNP NPANXX QTY, and LNP LRN QTY, regulate the maximum capacity allowed in the system and contain a finite increment of the quantity field.

Overview of the ELAP User Interfaces

ELAP provides two user interfaces:

- The text-based User Interface provides the Configuration menu and other menus to perform the ELAP initialization and first configuration. Use of the interface is described in [ELAP Software Configuration](#).
- The Graphical User Interface provides GUI menus and screens that are used to maintain, debug, and operate the platform. The GUI and its associated error messages are described in this chapter.

Communication with the ELAP using either interface requires a PC connected to the MPS. The ELAP GUI Interface requires a network connection and a network browser. To set up a PC workstation, see [Setting Up an ELAP Workstation](#).

ELAP Switchover

ELAPs assume an Active or a Standby role through negotiation and algorithm. This role impacts the way the ELAP handles its various external interfaces. External provisioning is allowed only through the Active ELAP. Only the Active ELAP can provide maintenance information to the EAGLE.

An ELAP can switch from an Active to a Standby role under the following circumstances:

1. The ELAP maintenance component becomes isolated from the maintenance component on the mate ELAP and from the EAGLE.

This implies that the maintenance subsystem has attempted and failed to establish communication with each of these:

- The mate ELAP maintenance task across the Sync network
- The mate ELAP maintenance task across the main DSM network
- Any Service Module card on any DSM network

2. The RTDB becomes corrupt.
3. All of the UDT channels have failed.
4. A fatal software error occurred.

If the Active ELAP has one or more of the four switchover conditions and the Standby ELAP does not, a switchover occurs. [Table 2: ELAP Switchover Matrix](#) lists the possibilities.

Table 2: ELAP Switchover Matrix

Active state	Standby state	Event	Switchover?
No switchover conditions	No switchover conditions	Condition occurs on Active	Yes
Switchover conditions exist	Switchover conditions exist	Conditions clear on Standby; switches to Active	Yes
No switchover conditions	Switchover conditions exist	Condition occurs on Active	No
Switchover conditions exist	Switchover conditions exist	Condition occurs on Active	No
Switchover conditions exist	Switchover conditions exist	Condition occurs on Standby	No
Switchover conditions exist	Switchover conditions exist	Conditions clear on Active	No

The exceptions to the switchover matrix is:

If the mate maintenance component cannot be contacted and the mate ELAP is not visible on the DSM networks, the ELAP assumes an Active role if any Service Module cards are visible on the DSM networks.

If none of the Standby conditions exist for either ELAP, the MPS servers negotiate an Active and a Standby. The mate is considered unreachable after two seconds of attempted negotiation.

Network Connections

Each MPS system is equipped with three network connections.

- [DSM Networks](#)
- [ELAP Sync Network](#)
- [Provisioning Network](#)

This section describes the three networks and the IP address assignment for the networks that require them.

Table 3: Sample Network IP Addresses Configured from UI

Network Connection	Sample MPS A Value	Sample MPS B Value
Hostname	MPSA-000000	MPSB-000001
Provisioning Network IP Address	10.25.50.45	10.25.50.46
Provisioning Network Netmask	255.255.255.0	255.255.255.0
Provisioning Network Default Router	10.25.50.250	10.25.50.250
Sync Network IP Address	169.254.1.100	169.254.1.200
DSM Network A IP Address	192.168.120.100	192.168.120.200
DSM Network B IP Address	192.168.121.100	192.168.121.200

Note: These values are examples only. The values entered to configure the ELAPs are unique to each network configuration. The method to determine the actual network values is described in *Hardware Reference*.

DSM Networks

The A and B DSM networks are redundant, load-balanced, 1GigE full duplex networks that carry provisioning data from the RTDBs on the ELAP to the RTDBs on the Service Module cards. These networks also carry reload and maintenance traffic to the Service Module cards. If one network fails, the other network carries all of the traffic normally carried by the both networks. Each network connects ELAP A and ELAP B to each Service Module card on a single EAGLE.

The first two octets of the ELAP network addresses for this network are 192.168. These are the first two octets for private class C networks as defined in RFC 1597.

The third octet for each DSM network is configured, usually to the default value .120 for the network A and the default value .121 for the network B. These are not visible to any external networks, and should not need to be changed.

The fourth octet of the address is selected as if:

- ELAP is configured as ELAP A, the fourth octet has a value of 100.
- ELAP is configured as ELAP B, the fourth octet has a value of 200.

Table 4: IP Addresses on the DSM Network summarizes the derivation of each octet.

The configuration menu of the ELAP user interface contains menu items for configuring the ELAP network addresses. See *ELAP Software Configuration*.

Table 4: IP Addresses on the DSM Network

Octet	Derivation
1	192
2	168
3	Usually already configured as: 120 for DSM network A 121 for DSM network B
4	100 for ELAP A 200 for ELAP B 1 - 25 for Service Module cards on the networks

ELAP Sync Network

The Sync network is a redundant, 1GigE, bonded network that connects ELAP A and ELAP B on a single Multi-Purpose Server (MPS) system. This network provides a high-bandwidth dedicated communication channel for MPS data synchronization. The two ELAPs are connected using Telco switches over two Ethernet ports bonded together to provide redundant paths between the two MPSs.

The first two octets of the ELAP IP addresses for the Sync network are 169.254.

The third octet for each ELAP Sync network address is set to .1.

The fourth octet of the Sync network IP address is .100 for ELAP A, and .200 for ELAP B.

Note: The Sync network IP address (169.254.1) is a link local IP address which can never be routed and cannot be changed.

Redundancy in Synchronization Network

Redundancy in Synchronization Network enables the mate server to be reachable from the local server if the synchronization interface from the ELAP servers to any of the switches is not functioning due to problems with cable connectivity, the switch, or other synchronization network operations.

When the connectivity of the ELAP servers with Switch B is intact, the synchronization network operates through Switch B using the connection from Ethernet Port eth03 of ELAP A server to Port 3 of Switch B and from Ethernet Port eth03 of ELAP B server to Port 4 of Switch B.

If a connectivity problem develops from the ELAP servers to Switch B, the synchronization network continues to function using Switch A because of the synchronization interface on Switch A. The

connectivity is from Ethernet Port eth04 of ELAP A server to Port 5 of Switch A and from Ethernet Port eth04 of ELAP B server to Port 6 of Switch A.

Provisioning Network

The provisioning network is the only network connected directly to the customer network. All provisioning information from the customer provisioning system travels over this network. In addition, all traffic required to keep remote MPS systems synchronized also travels across this network.

The provisioning (customer) network carries ELAP user interface traffic and traffic between ELAP and the LSMS.

The port is a 1GigE, auto-sensing device; it automatically runs as fast as the customer equipment allows. A dedicated network is recommended, but it is possible that unrelated customer traffic could also use this network.

LSMS-to-ELAP Connection

All normal LNP provisioning is conducted through the LSMS. Localized retrieval of data can be accomplished through the ELAP user interface.

The LSMS communicates only with the HA-Active ELAP in the MPS system using a Virtual IP (VIP) address interface. The LSMS connects to the HA-Active ELAP at initialization.

Although there are three ELAP states (HA-Active, HA-Standby, and Down) only the HA-Active member of the ELAP HA pair is connected to the VIP and listens for provisioning, audit and bulk download connections from the LSMS.

The LSMS provisions LNP data to the HA-Active ELAP across a TCP/IP connection in the customer network.

The LSMS collects subscription data from the Number Portability Administration Center (NPAC). It also collects local provisioning data (for default NPANXX, split NPANXX and other types of LNP records). This data is sent to the HA-Active ELAP, which performs minimal parsing and validation before updating its Real Time database (RTDB) and replicating the data to the mate ELAP RTDB. The ELAP with the LSMS primary connection ensures that the RTDBs on both ELAPs receive the provisioning data.

Network Time Protocol (NTP)

The Network Time Protocol (NTP) is a Internet protocol that synchronizes clocks of computers to Universal Time Coordinated (UTC) as a time reference. NTP reads a time server's clock and transmits the reading to one or more clients; each client adjusts its clock as required. NTP assures accurate local timekeeping with regard to radio, atomic, or other clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over extended time periods.

If left unchecked, the system time of Internet servers will drift out of synchronization with each other.

The MPS A server of each mated MPS pair is configured, by default, as a “free-running” NTP server that communicates with the mate MPS servers on the provisioning network. (“Free-running” refers to a system that is not synchronized to UTC; it runs off of its own clocking source.) This allows mated MPS servers to synchronize their time.

All MPS servers running the ELAP application have the option to be configured to communicate and synchronize time with an LSMS server or with a customer-defined NTP time server. The *prefer* keyword prevents “clock-hopping” when additional MPS or NTP servers, LSMS servers for example, are defined.

If this optional feature uses an LSMS, the LSMS must be configured as an NTP server. Refer to *LSMS Configuration Guide* for configuration instructions. After the LSMS has been configured, configure the MPS servers to synchronize with the LSMS. See [Procedure for Configuring ELAPs](#) for instructions on configuring the MPS servers through the application user interface.

Understanding Universal Time Coordinated (UTC)

Universal Time Coordinated (UTC) is an official standard for determining current time. The UTC is based on the quantum resonance of the cesium atom. UTC is more accurate than Greenwich Mean Time (GMT), which is based on solar time.

The term *universal* in UTC means that this time can be used anywhere in the world; it is independent of time zones. To convert UTC to your local time, add or subtract the same number of hours as is done to convert GMT to local time. The term *coordinated* in UTC means that several institutions contribute their estimate of the current time, and the UTC is calculated by combining these estimates.

UTC is disseminated by various means, including radio and satellite navigation systems, telephone modems, and portable clocks. Special-purpose receivers are available for many time-dissemination services, including the Global Position System (GPS) and other services operated by various national governments.

Generally, it is too costly and inconvenient to equip every computer with a UTC receiver. However, it is possible to equip a subset of computers with receivers; these computers relay the time to a number of clients connected by a common network. Some of those clients can disseminate the time, in which case they become lower stratum servers. The industry-standard NTP is one time dissemination implementation.

Understanding NTP

NTP is an Internet protocol used to synchronize clocks of computers using UTC as a time reference. NTP primary servers provide their clients time that is accurate within a millisecond on a LAN and within a few tens of milliseconds on a WAN. This first level of accuracy is called stratum-1. At each stratum, the client can also operate as a server for the next stratum.

A hierarchy of NTP servers is defined with several strata to indicate how many servers exist between the current server and the original time source external to the NTP network, as follows:

- A stratum-1 server has access to an external time source that directly provides a standard time service, such as a UTC receiver.
- A stratum-2 server receives its time from a stratum-1 server.
- A stratum-3 server receives its time from a stratum-2 server.
- This NTP network hierarchy supports up to stratum-15.

Normally, client workstations do not operate as NTP servers. NTP servers with a relatively small number of clients do not receive their time from a stratum-1 server. At each stratum, it is usually necessary to use redundant NTP servers and diverse network paths to protect against broken software, hardware, or network links. NTP works in one or more of these association modes:

- Client/server mode, in which a client receives synchronization from one or more servers, but does not provide synchronization to the servers

- Symmetric mode, in which either of two peer servers can synchronize to the other, in order to provide mutual backup
- Broadcast mode, in which many clients synchronize to one or a few servers, reducing traffic in networks that contain a large number of clients. IP multicast can be used when the NTP subnet spans multiple networks.

The MPS servers are configured to use the symmetric mode to share their time with their mate MPS servers. For an ELAP system, customers using the application user interface have the option to configure the MPS system to receive NTP from LSMS or a customer-provided NTP server.

Support ELAP Reload Via Database Image Function

The Support ELAP Reload via Database Image (SERVDI) function performs bulk data downloads (BDD) that significantly reduce the time needed to reload an ELAP database. SERVDI is included with optional LNP feature.

The SERVDI function is executed on the LSMS system and creates an LNPRTDB image file directly from the LSMS LNP databases. The `servdiDownload` file must be transferred to the ELAP system backup directory. Once transferred, the file can be activated by using the restore from backup process in the ELAP GUI. For more information on the restore from backup process, refer to the "Restore RTDB on ELAP 9.0" section in *LNP Database Synchronization Manual*.

Note: Although the exchange of ELAP Secure Shell (SSH) Keys is performed automatically by the configuration software at the start of the ELAP configuration, exchange of SSH keys with the LSMS must be performed manually for the ELAP to receive bulk downloads from the LSMS. See [Step 17](#) in *Procedure for Configuring ELAPs*.

The key exchange must also be performed from the LSMS. Login as `lsmsadm` on the LSMS Active server CLI and execute the command `keyexchange elapdev@<ELAP VIP>` to exchange the key with the `elapdev` user.

See also [Restore RTDB](#).

A

Restore the RTDB

 **CAUTION:** This action will restore the RTDB from the specified file on the selected ELAP. The ELAP software must be stopped on the selected ELAP in order for the restore to be allowed.

Select	Type	Originating Host	File Name	File Size	Creation Time
<input type="radio"/>	servdiDownload	BONAIRE	servdiDownload BONAIRE...	19M bytes	Fri May 30 2008 14:00:55 EDT
<input type="radio"/>	rtdbBackup	bonaire-a	rtdbBackup bonaire-a...	837M bytes	Tue June 03 2008 12:56:50 EDT
<input type="radio"/>	bulkDownload	bonaire-a	bulkDownload bonaire-a...	2.0G bytes	Wed June 04 2008 16:41:21 EDT
<input type="radio"/>	bulkDownload	bonaire-a	bulkDownload bonaire-a...	2.0G bytes	Mon June 02 2008 14:25:53 EDT

Restore RTDB from the Selected File.

Figure 2: ELAP Restore the RTDB GUI with servdiDownload Option

Network Address Translation on MPS

The MPS supports 2 types of network address translation (NAT), Port Forwarding and Static Address Mapping. In both cases, the MPS will have private IP addresses that are not available outside of the firewall protected internal network. The firewall will translate particular addresses and port numbers to the internal addresses for the MPS.

The addresses in [Figure 3: NAT on MPS](#) are examples. Addresses are not restricted to particular classes/ranges.

Port Forwarding

Port Forwarding allows a single external address to be used for multiple internal systems. The Port Forwarding firewall maintains a list of services (basically port numbers) and corresponding internal addresses.

Although the MPS has two individual internal IP addresses, external clients are allowed to reach the internal network using only one external address. The MPS servers must use different port numbers for each externally available service in order to distinguish MPS A from MPS B to external clients.

The MPS uses 3 ports for the Web UI and another 2 ports for the LSMS connections. At a minimum, one MPS side must be configured with 3 Web UI ports different from the default values. The firewall must be configured to forward 3 Web UI ports to MPS A and 3 different Web UI ports to MPS B.

The LSMS does not currently allow configuration of alternate LSMS ports. Until this changes, the LSMS is required to be on the internal network of a Port Forwarding firewall. Do not change the default values for these ports.

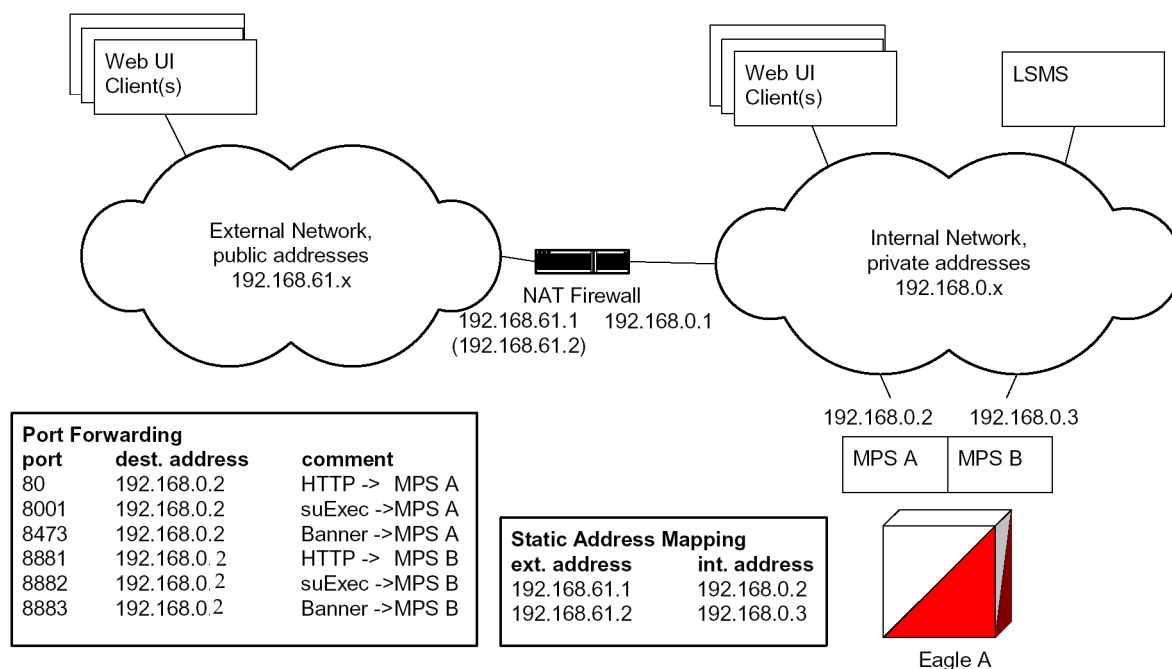


Figure 3: NAT on MPS

Static Address Mapping

Static Address Mapping makes systems that are behind the firewall appear to have public addresses on the external network. A one-to-one mapping exists between internal and external addresses.

An external address must be assigned to the NAT firewall for each MPS side. The external addresses must be entered into the MPS database in order for the Web UI to be fully functional.

ELAP Security Functions

ELAP Security functions control access to an ELAP GUI to specific IP addresses. The specified allowed IP addresses are kept in an ELAP list and can be added to, deleted from, and retrieved only by an authorized user. These functions also allow an authorized user to toggle IP authorization checking on and off through the GUI.

The administrator or user with IP action privileges can add, delete, and retrieve IP addresses. Deleting an IP would result in that IP address no longer residing in the IP table, hence preventing that IP address from being able to connect to an ELAP.

Note: While each of the IP action privileges can be assigned to any individual user, the IP action privileges of add and delete should be granted only to users who are knowledgeable about the customer network.

The ability to add, delete, and retrieve client IP addresses and to toggle IP authorization checking is assignable by function. This is accessible through the ELAP GUI (see [User Administration Menu](#)). The IP mechanism implemented in this feature provides the user a means of further enhancing ELAP privilege control.

The ELAP Security functions are available through the ELAP GUI and are available initially to only the administrator. The ability to view IP addresses on the customer's network is a security consideration and should be restricted to users with administration group privileges. In addition, privileged users can prepare a custom message to replace the standard 403 Forbidden site error message.

Note: IP access and range constraints provided by the web server and the ELAP Security functions cannot protect against IP spoofing. (The term 'spoofing' refers to the creation of TCP/IP packets using another's IP address; it is IP impersonation or misrepresentation). The customer must rely on the security of the customer's intranet network to protect against spoofing.

ELAP maintains a list of the IP addresses that are authorized to access the graphical user interface. Only requests from IP addresses on the authorized list can connect to the ELAP GUI. Attempts from any unauthorized address are rejected.

Note: No IP addresses are restricted from accessing the ELAP GUI until the administrator toggles IP authorization to 'enabled'. When IP authorization checking is enabled, any IP address not present in the IP authorization list will be refused access to the ELAP GUI.

ELAP Security functions also provide the means to enable or disable the IP address list once it is provisioned. If the list is disabled, the provisioned addresses are retained in the database, but access is not blocked from IP addresses not on the list. The ELAP GUI restricts permission to enable/disable the IP address list to specific user names and passwords.

The IP actions for adding, deleting, retrieving authorized IP Addresses and for toggling authorized IP checking are available only from the ELAP GUI (described in [Overview of ELAP Graphical User Interface](#)), but not from the ELAP text-based UI described in [ELAP Software Configuration](#).

LSMS/ELAP PING Enhancement

Depending on customer network architecture, the LSMS and ELAP may be on different internal networks. To increase security, as few ports as necessary should be required to be open inbound to the ELAP network. The original LSMS/ELAP interface supports a UDP PING function to monitor the connectivity between the two systems. The LSMS/ELAP PING enhancement feature moves the monitoring function within the HSOP interface, such that the UDP PING port is no longer required.

The LSMS continues to support the original UDP PING method to address operation with ELAPs that have not been upgraded, as well as continued UDP PING operation in conjunction with the HSOP keep alive.

The procedures to set up the LSMS/ELAP PING function are done on the LSMS.

Service Module Card Provisioning

One of the core functions of the ELAP is to provision the Service Module cards with database updates. The ELAP provides Real Time database (RTDB) loading and provisioning functions for the EAGLE Service Module cards using the main DSM network between the MPS system and the EAGLE Service Module cards; the backup DSM network is used, if necessary. Real-time updates are sent to the EAGLE Service Module cards in parallel using UDT technology.

The VSCCP application, running on the Service Module cards, conducts all database communications between the Active ELAP and each Service Module card.

The LNP feature auto-inhibits any Service Module card that does not meet the minimum hardware requirements based upon feature quantity capacities and the LNP ELAP Configuration feature status. See [Hardware, System, and Feature Requirements](#) for more information on minimum requirements.

Incremental Loading

Incremental loading occurs when a Service Module card has missed some updates, but does not need a complete reload.

The ELAP can broadcast a stream of current updates to all Service Module cards at a rate of 100 updates per second. When the ELAP detects that a Service Module card is back-level from the current provisioning stream, the ELAP attempts to start a new stream at that level.

Note: Incremental loading and normal provisioning are done in parallel. The Service Module card provisioning task supports up to five incremental loading streams in addition to the normal provisioning stream.

Incremental reload streams are terminated when the database level contained in that stream matches that of another stream. This is expected to happen most often when the incremental stream “catches up to” the current provisioning stream. Service Module cards accept any stream with the “next” sequential database level for that card.

Service Module Card Reload

Service Module cards might require a complete database reload in the event of reboot or loss of connectivity for a significant amount of time. The ELAP provides a mechanism to quickly load a number of Service Module cards with the current database. The database on the ELAP is large and may be updated constantly. The database sent to the Service Module card or cards is likely to be missing some updates, making it corrupt as well as back level. The upload process is divided in to two stages, one to sequentially send the raw database records and another to send all of the updates missed since the beginning of the first stage. The Service Module card reload stream uses a separate UDT channel from the provisioning and incremental update streams.

Service Module Card Warm Restart

When a Service Module card is rebooted with a warm restart and there were no database updates transmitted during the reboot, the existing database is retained. If updates were transmitted from the ELAP RTDB during the reboot, the Service Module card database is reloaded when the reboot is complete.

MPS/Service Module Card RTDB Audit Overview

General Description

The fact that the ELAP advanced services use several databases creates the need for an audit that validates the contents of the different databases against each other. The audit runs on both MPS

platforms to validate the contents of the Real Time databases (RTDBs). The active ELAP machine validates the database levels for each of the Service Module cards.

Functional Description

MPS RTDB Audit

This audit maintains the integrity of the RTDB Database on the MPS. This audit cycles through the entire RTDB within a 24-hour period and reports any anomalies in the form of an alarm. Once the RTDB is determined to be corrupt, provisioning is stopped and a data reload is required.

The audit is controlled through the **RTDB Audit** item on the **MPS GUI Maintenance Menu**. The state of the audit can be viewed and Enabled or Disabled through the [Maintenance Menu](#).

When the RTDB Audit is enabled, an audit is automatically performed daily at 6:00 a.m. This audit file is stored in the ELAP system backup directory. Only the five most recent audits are stored and the older ones are automatically deleted. The stored audits can be viewed through the View Logs item in the [Debug Menu](#).

When the RTDB Audit is enabled, the RTDB validates the CRC32 values per record entry within all tables. If corruption is encountered, an alarm is set on the MPS scrolling banner. All provisioning from the LSMS is halted until the condition is corrected via RTDB Reload.

ELAP-to-Service Module Card DB Level

Each Service Module card validates its own database level against the received ELAP database level. An inconsistent alarm is generated at the EAGLE for every inconsistent Service Module card. The EAGLE command `rept-stat-db` displays the LNP database on the Service Module card as *Diff* level. See [Table 5: Inconsistent Service Module Card Alarm](#).

Table 5: Inconsistent Service Module Card Alarm

UAM#	Severity	Message Text	Output Group (UI Output Direction)
444	Major	RTDB database is inconsistent	card

EAGLE Service Module Card Audit of MPS Databases

This audit is responsible for maintaining the integrity of the RTDB on the Service Module card. It cycles through the entire RTDB within a 24-hour period, reporting any anomalies in the form of alarms and possibly attempts to repair any found corrupted records with those from a mate Service Module card.

The EAGLE STP Options (`chg-stpopts`) command is used to set this audit. The DSMAUD parameter has two states, OFF and ON. When the DSMAUD parameter is set to OFF the auditing capabilities on each of the Service Module cards is disabled from auditing the RTDBs. Setting the DSMAUD parameter to ON enables the auditing capabilities, producing corruption alarms when corruption is detected.

When corruption is encountered, several events occur:

- The RTDB is set to Corrupt Status

- A UAM (Corrupted RTDB Database Alarm) is sent to the OAM
- The Corruption is logged and stored in a memory array and contains:
 - Table ID
 - Record Number
 - Table High-water-mark
 - Old CRC32 value
 - New CRC32 value
 - Record Address in memory
 - Record entry Contents

Table 6: Corrupted RTDB Database Alarm

UAM#	Severity	Message Text	Output Group (UI Output Direction)
443	Minor	RTDB database corrupted	card

A maximum of 250 Log entries are permitted within an audit cycle. When this maximum is exceeded, the first 25 corrected records are output to the DB output group, and the card initiates a Full Re-Load.

Service Module cards in the corrupted state continue to receive updates from the MPS and continue to service MSU traffic.

All records received from the MPS are validated through the CRC32 routines prior to being written to memory. If a corrupted record is encountered, data is collected and depending upon the loading phase state, events will differ:

Table 7: Effect of Corrupted record received from MPS

MPS Loading Phase	Effect of Corrupted Record Received
Phase I - Loading	Booting of Card and Full Reload Requested
Phase II - Resynchronization	Booting of Card and Full Reload Requested
Load Complete	Alarm Incoherent and Reload Required

Chapter 4

ELAP Graphical User Interface

Topics:

- [Overview of ELAP Graphical User Interface.....42](#)
- [ELAP GUI Menus.....57](#)
- [ELAP Messages.....92](#)

This chapter describes how to log into the ELAP Graphical User Interface (GUI) and how to use the ELAP GUI menus. See [ELAP Software Configuration](#) for instructions for using the ELAP text-based interface.

Overview of ELAP Graphical User Interface

This section describes the various screens, screen structure and layouts, and input prompts of the ELAP Graphical User Interface (GUI). It describes the login screen, the contents of the main screen, and explains the three frames displayed in the browser window of the ELAP GUI.

ELAP employs a Web-based user interface. It uses the typical client-server paradigm. The front end appears on an Internet browser. The back end operates on the MPS platform. The front end is officially supported on Microsoft Internet Explorer, version 8.0 or later. The ELAP user interface may not function properly with Mozilla Firefox.

The ELAP GUI pages have three different sections:

- Banner header section for displaying the real-time status of the MPS servers
- Menu section for selecting desired actions
- Work area section for entering requested information and displaying results

The banner header sections are a Java applet that communicates directly with the GUI Server process on the MPS. The menu and work area sections primarily consist of HTML and JavaScript generated by CGI (Common Gateway Interface) scripts on the back end.

An http web server starts the process of handling requests from browsers. It receives the requests and loads the requested document. If the document is a simple HTML file, the http web server just returns the document to the browser. The ELAP software may also connect with the GUI Server to request that actions be performed. HTML output from the script is returned to the browser and displayed. The user can open only one ELAP GUI per system.

Figure 4: Process Architecture View of the ELAP UI shows the process architecture view of the ELAP user interface.

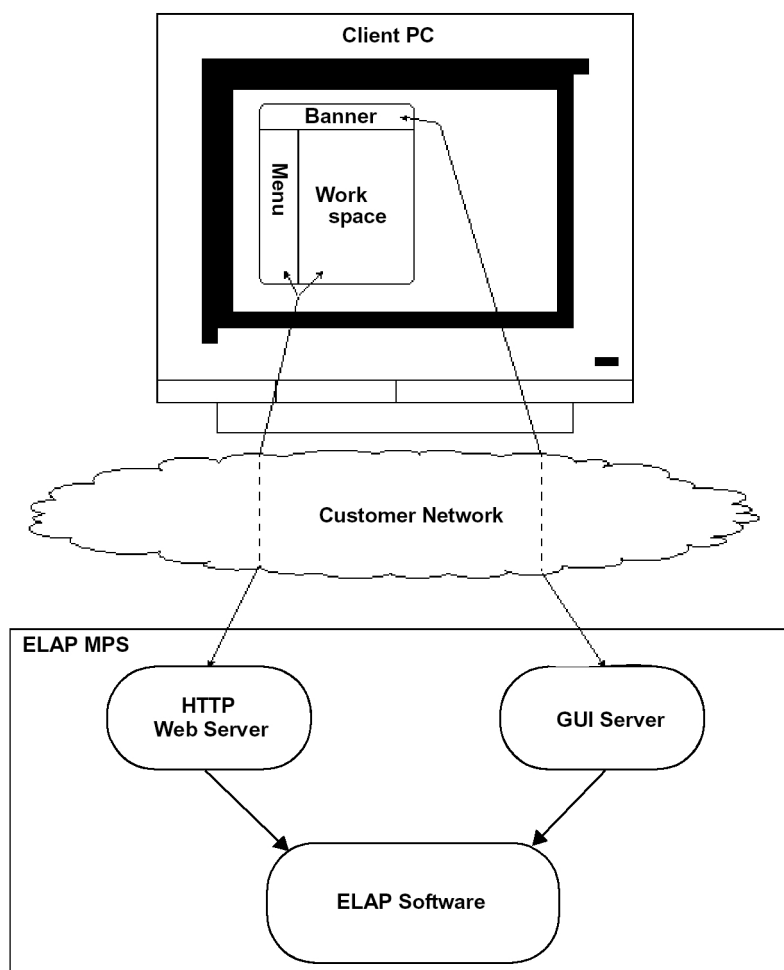


Figure 4: Process Architecture View of the ELAP UI

ELAP Support for HTTPS on GUI

The ELAP Support for HTTPS on GUI feature allows users to configure how the GUI can be accessed: by standard HTTP (Hypertext Transfer Protocol), by HTTPS (Secure Hypertext Transfer Protocol), or by both. For a more secure system, Oracle recommends enabling HTTPS and disabling HTTP.

In standard HTTP protocol, the data transfer between the Web server and the GUI is not encrypted; therefore, it can be captured by any network analyzer and viewed.

Secure HTTP (HTTPS) supports encryption of data exchanged between the Web server and the browser.

ELAP allows admin user group members to configure the ELAP GUI. The admin group user can disable HTTP. The ability to configure HTTP and HTTPS and the ability to disable HTTP can be limited to a specific user class or group.

Starting the Non-secure Web-based GUI

To start the non-secure Web-based GUI, open a Web browser (examples: Firefox, Internet Explorer). In the Address field, enter one of the following URLs and press **Go**:

- `http://<ELAP_server_IP_address>/`
- `< ELAP_server_IP_address>`
- `< ELAP_server_hostname>`

If the HTTP interface is disabled, the Web browser displays an error message.

Starting the Secure Web-based GUI

To start the secure Web-based GUI, open a Web browser (examples: Firefox, Internet Explorer). In the Address field, enter one of the following URLs and press **Go**:

- `https://<ELAP_server_IP_address>/`
- `https://<ELAP_server_hostname>/`

If the HTTPS interface is disabled, the browser displays an error message.

Enabling HTTPS

Perform the following procedure to enable HTTPS on ELAP.

1. Log in to the Active ELAP as either the `root` or `elapdev` user.
2. Enter the following to enable HTTPS:

```
# /usr/TKLC/elap/bin/httpConfig.pl https
```

The changed status is displayed.

```
HTTPS Enabled
HTTP Disabled
```

3. To confirm the status, enter the following:

```
# /usr/TKLC/elap/bin/httpConfig.pl status
```

```
Http Enable    NO
Https Enable   YES
```

Installing the Security Certificate

Perform the following procedure to install the Security Certificate. For the Select Mate tab to function properly, this procedure must be completed for three ELAP IP addresses: Server A IP, Server B IP, and VIP. The actual dialog boxes, displayed outputs, and required steps for installing the Security Certificate may vary for different versions of Web browsers, Java, and operating systems.

1. Access the ELAP GUI by opening a Web browser and entering the IP address of ELAP, using HTTPS.

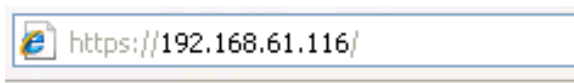


Figure 5: ELAP Login

2. Click on **Continue to this website (not recommended)**.

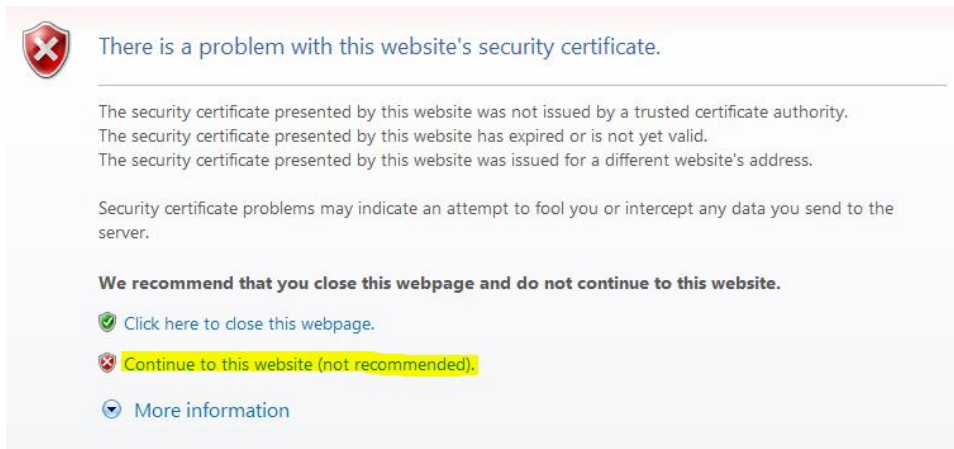


Figure 6: Security Certificate

The HTTPS Login Page is displayed.

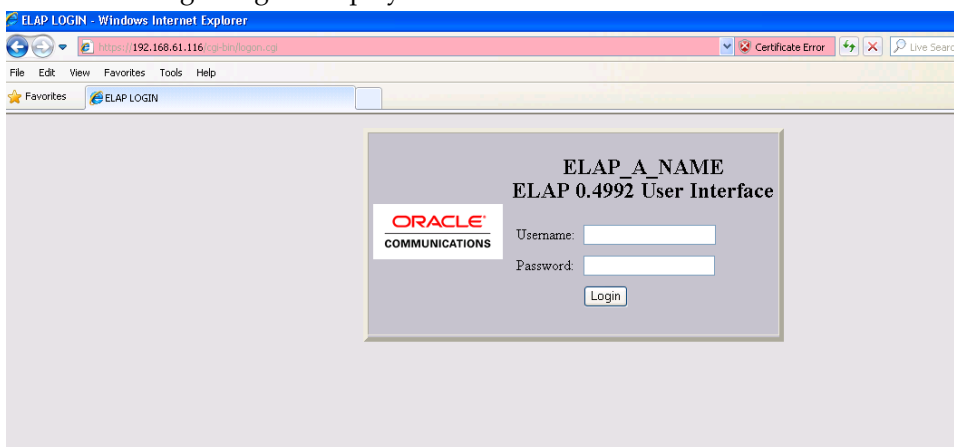


Figure 7: HTTPS Login Page

3. Click on **Certificate Error**.

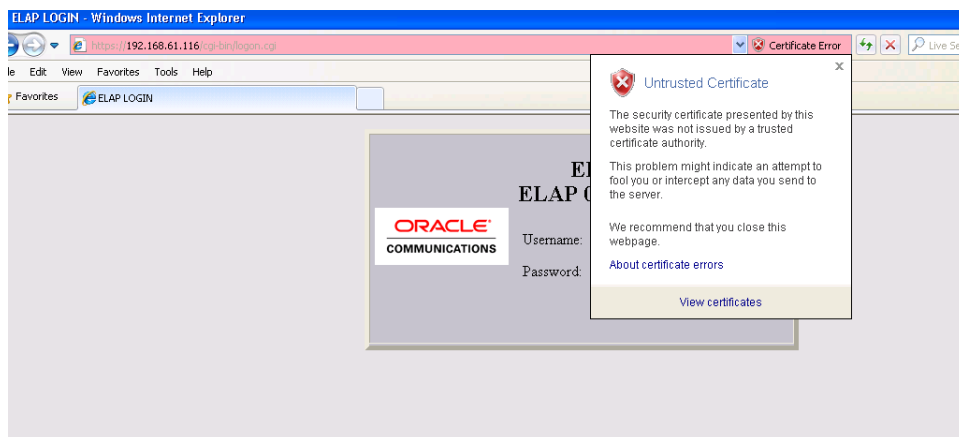


Figure 8: Certificate Error

4. In the popup window titled **Certificate Invalid**, click on the **View certificates** link to display the **Certificate** dialog box.

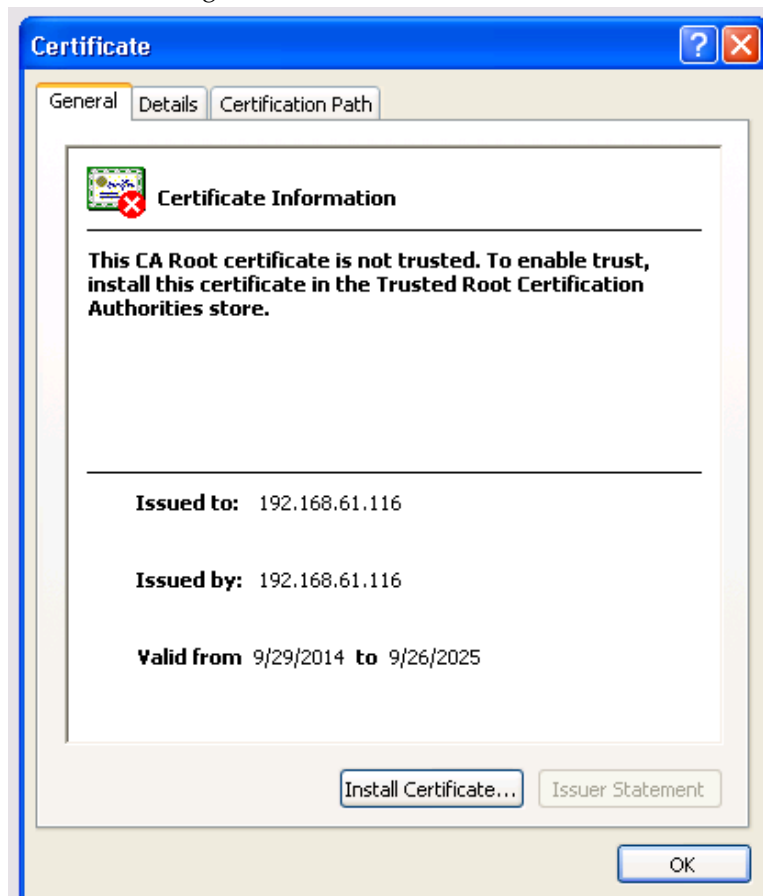


Figure 9: Certificate

5. Click **Install Certificate** to begin the Certificate Import Wizard. The **Certificate Import Wizard Welcome** page is displayed.



Figure 10: Certificate Import Wizard

6. Click on **Next** to display the *Certificate Store* page of the Certificate Import Wizard.

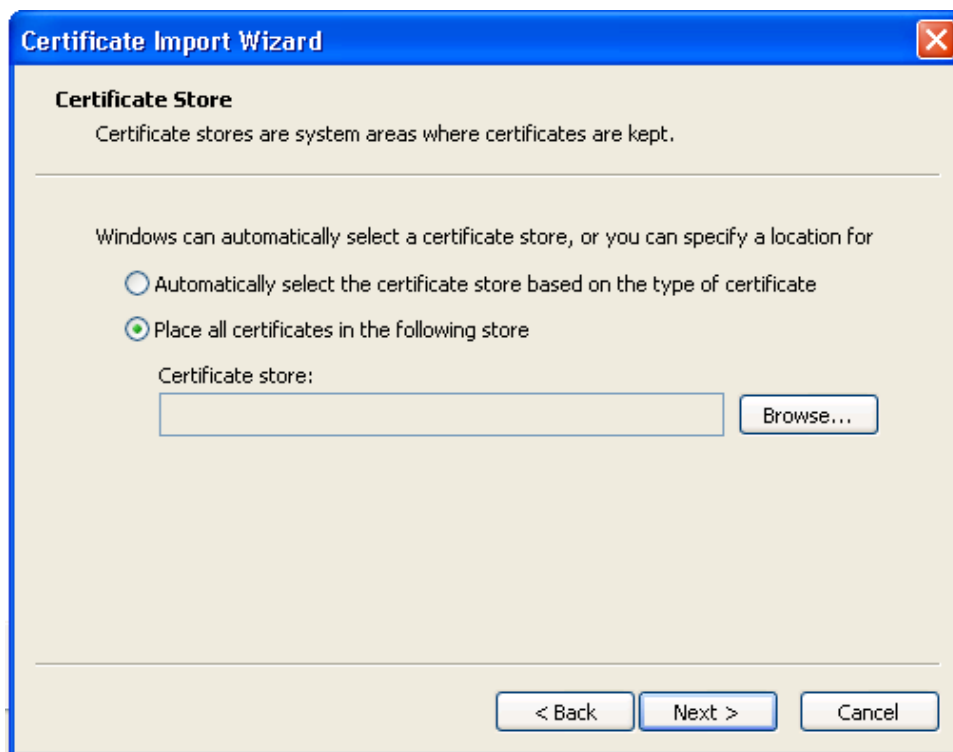


Figure 11: Certificate Store

7. Select the **Place all certificates in the following store** radio button, then click **Browse** to display the **Select Certificate Store** window.



Figure 12: Select Certificate Store

8. Select the **Trusted Root Certification Authorities** option and click **OK** to display the Certificate dialog box.

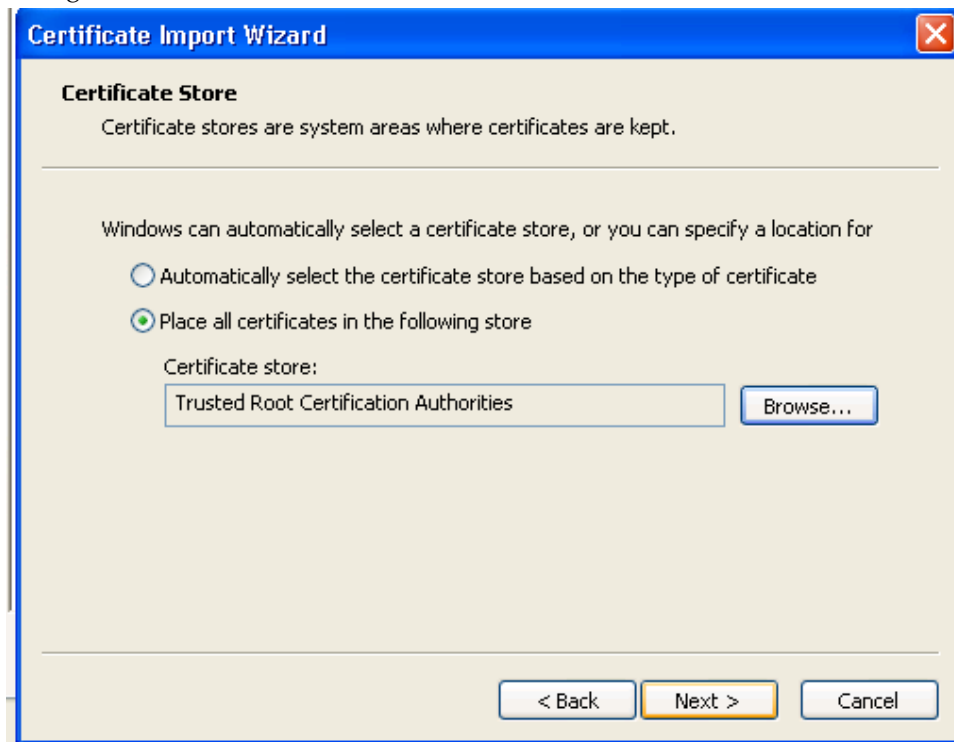


Figure 13: Certificate Store

9. Click **Next**. The Certificate Import Wizard *Completing the Certificate Import Wizard* page is displayed:

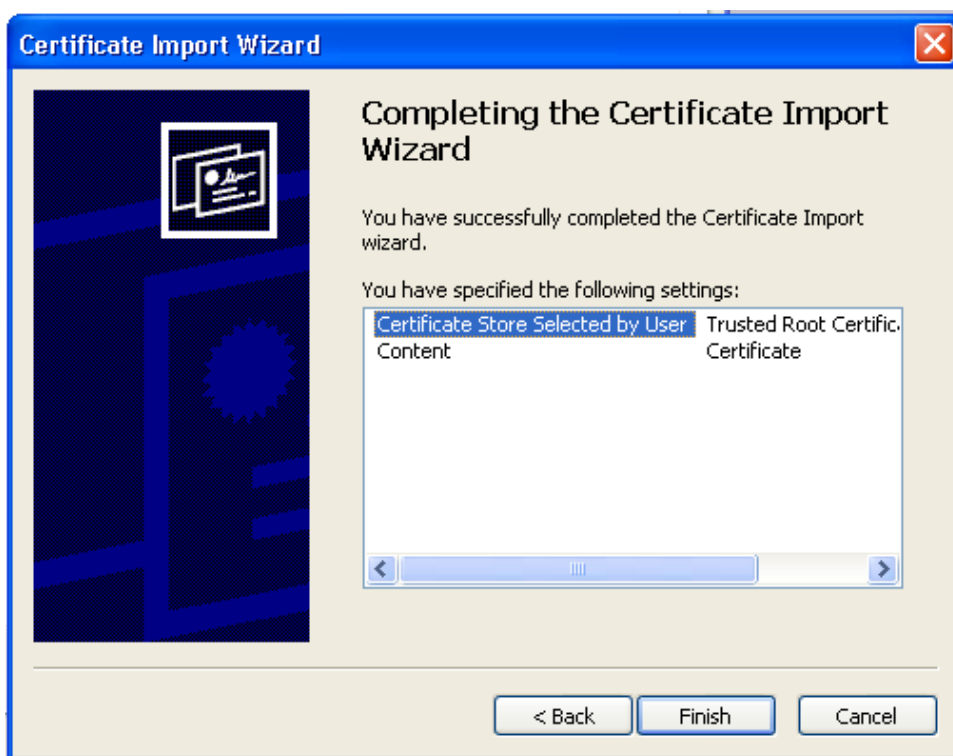


Figure 14: Completing the Certificate Import Wizard

10. Click **Finish**. If a Security Warning dialog box is displayed, click **Yes**.



Figure 15: Security Warning



Figure 16: Import Successful

11. After the message box *The import was successful* is displayed, click **OK** to close the **Certificate Import Wizard**.
12. Log in to the ELAP GUI as `uiadmin` or any other user to verify that all GUI pages are opening successfully.

Enabling HTTPS and HTTP

Perform the following steps to enable HTTPS and HTTP .

1. Log in to the Active ELAP as `root` or `elapdev` user.
2. Enter the following:

```
# /usr/TKLC/elap/bin/httpConfig.pl both
```

HTTPS and HTTP are both enabled.

3. To confirm the status, enter the following:

```
# /usr/TKLC/elap/bin/httpConfig.pl status
```

```
Http Enable      YES
Https Enable     YES
```

Login Screen

The first screen in the ELAP GUI is the login screen. Two fields appear on this screen: **Username** and **Password**. To log in, enter a valid user name and password, and click the **Login** button. These fields provide the user identification and verification.

When you log in successfully, the screen workspace indicates that the user is logged in.

After logging into the ELAP GUI, you do not need to log in again as long as the Web browser session remains active, with the exception of the following menu choices:

- **View Logs** (see [View Logs Menu](#))
- **Connect to MMI Port** (see [Connect to EAGLE MMI Port](#))
- **SSH to MPS** (see [SSH to MPS](#))

These menu choices display a password window.

Subsequent user authentication is handled with “cookies,” which are stored in the user's browser and remain there throughout the duration of the browser's operation.

Use the **Logout** menu option to terminate the session and invalidate the cookie. Alternatively, the user can be logged out by session inactivity (defined by [User Permissions](#)), terminated by the administrator, and by selecting another window on another independent browser.

ELAP GUI Main Screen

The ELAP GUI main screen contains three sections:

- [ELAP GUI Banner Section](#)
- [ELAP GUI Menu Section](#)
- [ELAP GUI Workspace Section](#)

The banner is the topmost section. It extends the entire width of the browser window. The remainder of the screen is divided vertically into two sections. The smaller left section is the menu section. The larger right section is the workspace section.

ELAP GUI Banner Section

The banner section of the ELAP GUI main screen has a Java applet that remains in constant communication with the ELAP program. This allows the banner section to display real-time ELAP information.



- Yellow with red triangle - ELAP is inhibited
- A - Active ELAP
- S - Standby ELAP

Clicking on an ELAP IP address toggles between the ELAP IP address and the ELAP host names.

ELAP Alarm Information Area

The ELAP alarm information area of the ELAP banner applet provides alarm-related information.

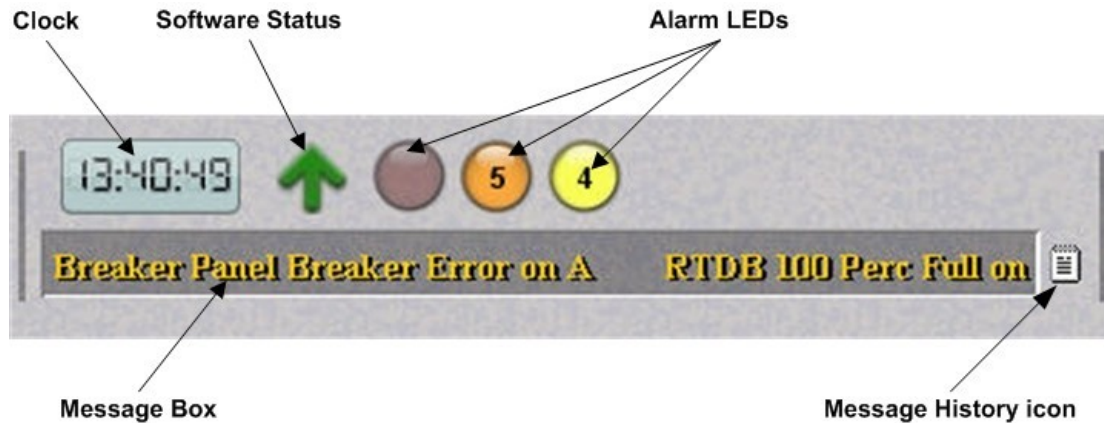


Figure 18: ELAP Alarm Information Area

The ELAP alarm information area provides these features:

- Clock - Displays the time on the selected ELAP. Clicking on the clock changes the display mode.
- ELAP software status - Displays the status of the ELAP software.

When the ELAP software is running, a green up arrow is displayed (see [Figure 18: ELAP Alarm Information Area](#)). When ELAP software is down, a red (down) arrow is displayed. When there is a GUI time-out, TERMINATED is displayed in red.

- Alarm LEDs - The alarm LEDs displays the existence and severity of alarms on the selected ELAP. The LEDs are:

Critical alarms (left LED) - turns red when a Critical alarm occurs

Major alarms (middle LED) - turns orange when a Major alarm occurs

Minor alarms (right LED) - turns yellow when a Minor alarm occurs

When a number is displayed on the LEDs, this indicates the number of alarms of that type that are currently active.

- Alarm message history - Clicking the **Message History** icon displays a history of the alarms and information messages for the selected server. Entries are color-coded to match alarm severity:

Red - critical messages

Orange - major messages

Yellow - minor messages

White - informational messages

To remove cleared messages from the message history, click the **Clear** button.

To refresh the messages displayed, click the **Refresh** button.

To prevent the message from displaying in the banner message box, click the **Hide** checkbox associated with a message.

- Banner message box - The banner message box is a horizontal scroll box that displays text messages for the user. Banner messages indicate the status of the ELAP machine.

LSMS Connection Status

The LSMS connection status area provides 5 types of LSMS information (from left to right):

- LSMS provisioning indicator (enabled/disabled)
- LSMS provisioning connection status indicator (connected/unconnected/listening/unknown)
- LSMS audit connection status indicator (connected/unconnected/listening/unknown)
- LSMS bulk download connection status indicator (connected/unconnected/listening/unknown)
- LSMS bulk download indicator (enabled/disabled)

The color of the LSMS connection status indicators signifies the state:

- Gray - disabled
- Orange - unknown (displays only during state transitions)
- Yellow - listening
- Green - connected or enabled

Note: LSMS audit and LSMS bulk download cannot be enabled at the same time. Enabling one toggles the other to a disabled state.



Figure 19: LSMS Connection Status Area

Moving the cursor over any of the five sections in the application displays a pop-up that provides LSMS information.

Service Module Card Status

The Service Module card status area of the ELAP Banner Applet provides information for up to 18 Service Module card slots on the EAGLE.

Figure 20: Service Module Card Status



The color of the card slots indicates:

- Grey - unknown card state
 - Booting
 - Inhibited card
 - Previously provisioned slot with undetectable card
- Light green (with ascending loading bar) - card loading (loading status is shown)
- Green striped - inconsistent card state
- Dark green - loaded consistent state
- P - indicates Primary Service Module card

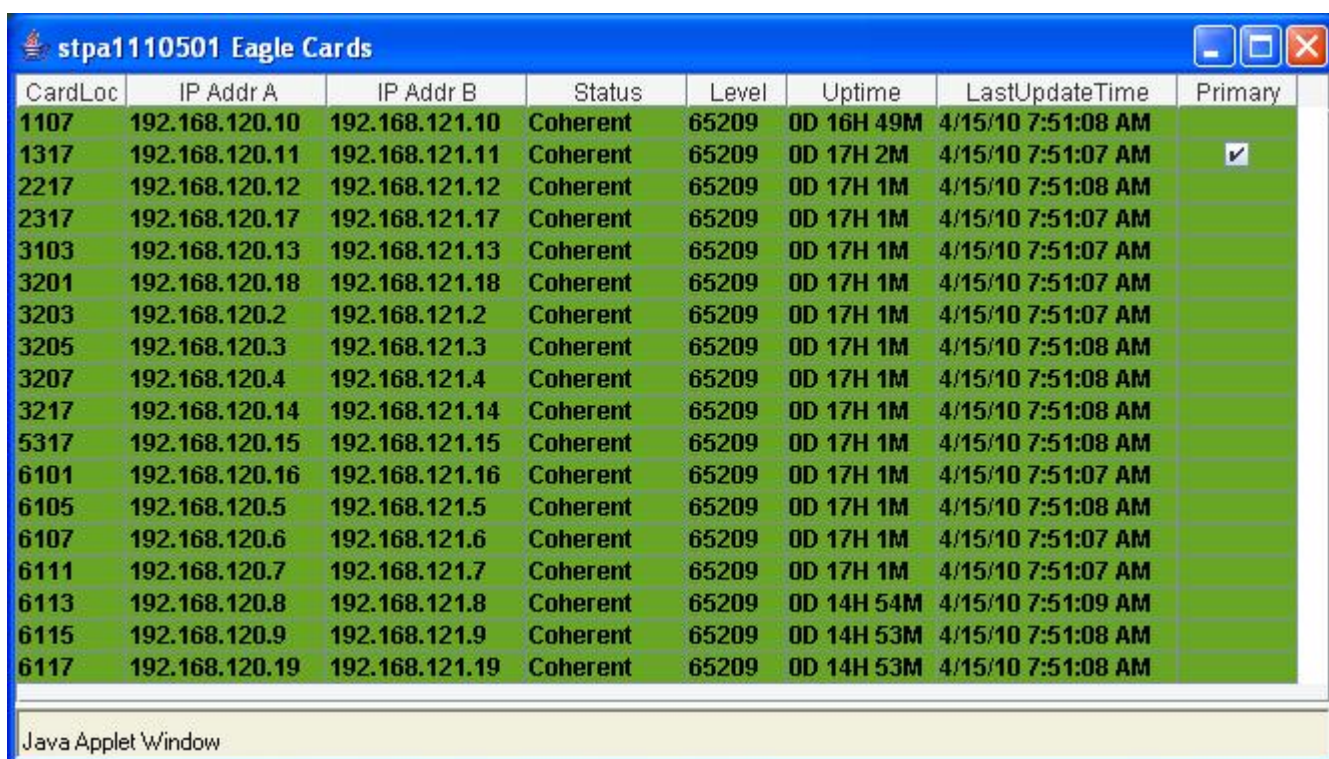
Moving the cursor over an occupied slot icon displays the card information in a pop-up window.

Clicking on the a card slot icon provides information on that Service Module card:



Figure 21: Status of an Individual Card

Clicking on the **Service Module Card Status Information** icon displays all 18 Service Module Card slots on the EAGLE and information about installed cards:



CardLoc	IP Addr A	IP Addr B	Status	Level	Uptime	LastUpdateTime	Primary
1107	192.168.120.10	192.168.121.10	Coherent	65209	0D 16H 49M	4/15/10 7:51:08 AM	
1317	192.168.120.11	192.168.121.11	Coherent	65209	0D 17H 2M	4/15/10 7:51:07 AM	<input checked="" type="checkbox"/>
2217	192.168.120.12	192.168.121.12	Coherent	65209	0D 17H 1M	4/15/10 7:51:08 AM	
2317	192.168.120.17	192.168.121.17	Coherent	65209	0D 17H 1M	4/15/10 7:51:07 AM	
3103	192.168.120.13	192.168.121.13	Coherent	65209	0D 17H 1M	4/15/10 7:51:07 AM	
3201	192.168.120.18	192.168.121.18	Coherent	65209	0D 17H 1M	4/15/10 7:51:07 AM	
3203	192.168.120.2	192.168.121.2	Coherent	65209	0D 17H 1M	4/15/10 7:51:07 AM	
3205	192.168.120.3	192.168.121.3	Coherent	65209	0D 17H 1M	4/15/10 7:51:08 AM	
3207	192.168.120.4	192.168.121.4	Coherent	65209	0D 17H 1M	4/15/10 7:51:08 AM	
3217	192.168.120.14	192.168.121.14	Coherent	65209	0D 17H 1M	4/15/10 7:51:08 AM	
5317	192.168.120.15	192.168.121.15	Coherent	65209	0D 17H 1M	4/15/10 7:51:08 AM	
6101	192.168.120.16	192.168.121.16	Coherent	65209	0D 17H 1M	4/15/10 7:51:07 AM	
6105	192.168.120.5	192.168.121.5	Coherent	65209	0D 17H 1M	4/15/10 7:51:08 AM	
6107	192.168.120.6	192.168.121.6	Coherent	65209	0D 17H 1M	4/15/10 7:51:07 AM	
6111	192.168.120.7	192.168.121.7	Coherent	65209	0D 17H 1M	4/15/10 7:51:07 AM	
6113	192.168.120.8	192.168.121.8	Coherent	65209	0D 14H 54M	4/15/10 7:51:09 AM	
6115	192.168.120.9	192.168.121.9	Coherent	65209	0D 14H 53M	4/15/10 7:51:08 AM	
6117	192.168.120.19	192.168.121.19	Coherent	65209	0D 14H 53M	4/15/10 7:51:08 AM	

Java Applet Window

Figure 22: Service Module Card Status Information

ELAP GUI Menu Section

The ELAP graphical user interface menu section is located in the left side of ELAP browser. The top of the frame is the software system title (ELAP) and a letter that designates the selected ELAP, either A or B. One or more submenus appear below the title. The content of the menu corresponds to the access privileges of the user.

By clicking on the name or folder icon of a directory, the user may expand and contract the listing of submenu content (typical “tree-menu” view). Directory contents may be either menu actions or more submenus. When you click the menu actions, the output is displayed in the workspace section (the right frame of ELAP browser interface).

ELAP GUI Workspace Section

The ELAP graphical user interface workspace section displays the results of menu actions taken by the user. The content of the workspace section can be various things such as prompts or status reports. Every menu action that writes to the workspace uses a standard format.

The format for the workspace is a page header and footer, and page margins on either side. In the header two data fields are displayed. The left-justified letter A or B designates the ELAP server that is currently select for menu action. The other data field has the right-justified menu action title. The footer consists of a bar and text with the time when the page was generated. At the bottom of the footer, a copyright notice is shown.

Workspace Section Syntax Checking

The web browser user interface uses layers of syntax checking to validate user input for text-entry fields.

- Mouse-over syntax check: For many of the **entry fields**, you can move the mouse over the field, causing a list of syntax hints for that field to appear.
- Pop-up syntax checking: When you click the **Submit** button, syntax is verified on the client side by code running on the user's browser. Incorrect syntax appears in a pop-up window, which contains a description of the syntax error. When the window is dismissed, you can correct the error and submit the input again.
- Back-end syntax checking: When you have clicked **Submit** button and the client side syntax checking has found no errors, back-end syntax checking is performed. If back-end syntax checking detects an error, it is displayed in the work space with an associated error code.

ELAP GUI Menus

The ELAP GUI consists of menus of items that provide functions for maintenance, debugging, and platform operations. When a menu item is chosen, the ELAP performs the requested action.

This chapter describes the ELAP GUI menus and how to use the menu items. The descriptions include:

- Login user names that can access the user interface menus
- The menu presented to each user for each login name
- Basic function provided by each menu item
- Response syntax expected by any prompts presented to the user by each menu item
- Output that can be displayed for each menu item operation
- Error responses that can be expected

ELAP Menu

The ELAP menu is the main menu of the ELAP application. It provides the functions of the ELAP User Interface. [Figure 23: ELAP Menu](#) shows the ELAP main menu.



Figure 23: ELAP Menu

The ELAP menu provides three actions common to all users: **Select Mate**, **Change Password**, and **Logout**. All of the remaining actions are options assignable by the system administrator to groups and individual users.

- [*Select Mate*](#)
- [*Process Control Menu*](#)
- [*Maintenance Menu*](#)
- [*RTDB Menu*](#)
- [*Debug Menu*](#)
- [*Platform Menu*](#)
- [*User Administration Menu*](#)
- [*Change Password*](#)
- [*Logout*](#)

Select Mate

The Select Mate menu selection changes the menus and workspace areas to point to the ELAP mate. This selection exchanges the status of the active and standby ELAPs. This basic action is available to all users and is accessible from the main menu.

If using ELAP A at the main menu, click the **Select Mate** button on the main menu to switch to ELAP B. The initial sign-on screen for the alternate server will appear.

When performing the Select Mate action, the contents of the banner do not change. However, the side (server) changes in the workspace and at the top of the menu area to indicate the active ELAP.

When a standby ELAP is selected, a subsection of the menu appears that corresponds to the menu actions associated with the standby ELAP.

Process Control Menu

The Process Control menu provides the start and stop software actions.

- [Start ELAP Software](#)
- [Stop ELAP Software](#)

Start ELAP Software

The Start ELAP Software menu option allows the user to start the ELAP software processes. The screen contains a button to confirm that you do want to start the software processes.

Stop ELAP Software

The Stop ELAP Software screen allows the user stop the ELAP software processes. The screen contains a button to confirm that the user wants to stop the software processes. It also provides a choice to automatically start the software when the server reboots.

Maintenance Menu

The Maintenance Menu allows the user to perform various ELAP platform tasks:

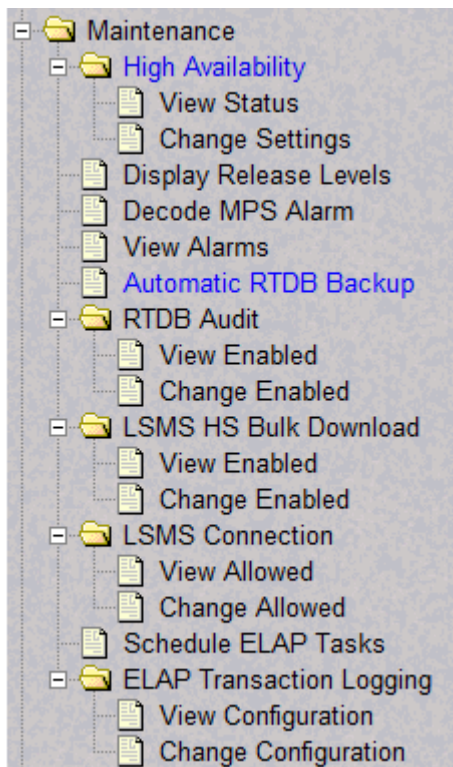


Figure 24: Maintenance Menu

- [High Availability Menu](#)
- [Display Release Levels Screen](#)
- [Decode EAGLE MPS Alarm](#)
- [View Alarms Menu](#)
- [Automatic RTDB Backup](#)
- [RTDB Audit Menu](#)
- [LSMS High Speed Bulk Download Menu](#)
- [LSMS Connection Menu](#)
- [Schedule ELAP Tasks Menu](#)
- [ELAP Transaction Logging](#)

High Availability Menu

The Maintenance / High Availability menu allows the user to view and change High Availability state settings for the Local and Remote ELAP.

The High Availability menu provides these actions:

- [View Status](#)

- [Change Settings](#)

View Status

The Maintenance / High Availability / View Status screen provides High Availability state information for the Local and remote ELAP:

- High Availability State
 - Active
 - Standby
 - Inhibited
- DRDB Resource
- Connection State
 - Connected
 - WFConnection
 - StandAlone
 - SyncSource
 - SyncTarget
- Node State
 - Primary
 - Secondary
 - Unknown
- Disk State
 - Up to Date
 - Diskless
 - DUknown

A View High Availability Status

	HA State	DRDB Resource	Connection State	Node State	Disk State
Local	ACTIVE	drbd0	Connected	Primary	UpToDate
Remote	STANDBY			Secondary	UpToDate

Figure 25: View High Availability Status Screen

Change Settings

The Maintenance / High Availability / Change Settings screen allows the user to change High Availability state settings for the Local and Mate ELAP.

Display Release Levels Screen

The Maintenance / Display Release Levels screen displays release information.

Decode EAGLE MPS Alarm

The Maintenance / Decode EAGLE MPS Alarm menu selection lets the user decode the EAGLE output of MPS alarms. The user enters the 16-character hexadecimal string from the EAGLE `rept-stat-mps` command. The strings are encoded from one of six categories, which are reported by UAM alarm data strings:

- Critical Platform Alarm (UAM #0370, alarm data h'1000 . . .')
- Critical Application Alarm (UAM #0371, alarm data h'2000 . . .')
- Major Platform Alarm (UAM #0372, alarm data h'3000 . . .')
- Major Application Alarm (UAM #0373, alarm data h'4000 . . .')
- Minor Platform Alarm (UAM #0374, alarm data h'5000 . . .')
- Minor Application Alarm (UAM #0375, alarm data h'6000 . . .')

The string included in the alarm messages is decoded into a category and a list of each MPS alarm that the hexadecimal string represents. The user should compare the decoded category with the source of the hex string as a sanity check. More details about the messages are in *Alarms and Maintenance* for ELAP.

The text for the alarms indicated by the alarm hex string is described in [MPS Platform and ELAP Application Alarms](#).

View Alarms Menu

The Maintenance / View Alarms menu allows the user to view alarms for the Local and Mate ELAP.

Automatic RTDB Backup

The Maintenance / Automatic RTDB Backup menu allows the user to schedule customized automatic RTDB backups from the active ELAP server. After selecting the Automatic RTDB Backup menu option, the screen shown in [Figure 26: Automatic RTDB Backup screen](#) is displayed to configure the Automatic RTDB Backup schedule. The filename created by the automatic RTDB backup is `autortdbBackup_<hostname>_<CurrentTime>.gz`, where `CurrentTime` = `YYYYMMDDHHMMSS` (year, month, day, hours, minutes, seconds); this filename cannot be changed by the user.

ELAP_A_NAME		Automatic RTDB Backup	
Backup Type (Select None to Cancel Backups)	<input type="button" value="Local and Mate"/>		
Time of the day to start the Backup	<input type="text" value="6:00"/>		
Frequency	<input type="button" value="1 Day"/>		
File Path (Directory only)	<input type="text"/>		
Remote Machine IP Address (xxx.xxx.xxx.xxx)	<input type="text"/>		
Login Name	<input type="text"/>		
Password	<input type="text"/>		
Save the local copies in the default path	<input type="radio"/> Yes <input type="radio"/> No		
Option to delete old backups Note: If you select Yes, by default 5 backup files will be maintained	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Specify the number of files to maintain	<input type="text" value="5"/>		
<input type="button" value="Submit Schedule"/>			

Figure 26: Automatic RTDB Backup screen

Options for Scheduling Automatic RTDB Backups

Backup Type	<p>The Backup Type selection determines which other fields are enabled. Local and Mate is the default Backup Type. If Automatic RTDB Backup is not configured, the None option is not available in the Backup Type field.</p> <ul style="list-style-type: none"> • Local - creates the automatic RTDB backup file on the local ELAP server • Mate - creates the automatic RTDB backup file on the local ELAP server and moves the backup file to the mate ELAP server • Local and Mate - creates the automatic RTDB backup file on the local ELAP server and copies the backup file to the mate ELAP server • Remote - creates the automatic RTDB backup on the local ELAP server and copies the automatic RTDB backup to the remote server • None - cancels all currently scheduled backups, disables all options except the Submit button.
Time of the day to start the Backup	Time of the day to start the Backup must be in 24-hour format (hh:mm). The default value is 06:00. The automatic RTDB backup cannot be cancelled after the backup begins at the scheduled time.
Frequency	Frequency is defined in the following increments with one automatic RTDB backup operation performed per increment: 12 hours, 1 day (default), 2 days, 3 days, 5 days, 7 days. The default value is 1 day.
File Path (Directory only)	<p>File Path allows the user to create subdirectories within the directory: /var/TKLC/elap/free/backup/. If the user does not specify any subdirectories, the automatic RTDB backup file is saved to the default file path /var/TKLC/elap/free/backup/.</p> <p>If Backup Type = Remote, the specified File Path is the absolute path for storing the backup file. If the user specifies a directory that does not exist on the remote server, the directory is not created and the backup file cannot be transferred to the remote server.</p>
Remote Machine IP Address	Remote Machine IP Address must be in the <i>xxx.yyy.zzz.aaa</i> format (example: 192.168.210.111). The remote machine, or remote server, can be any server on the network and is not required to be running ELAP software. Only one remote server can be configured. This field is enabled when Backup Type = Remote .
Login Name	Login Name is a valid user login name for the remote server specified by Remote Machine IP Address. This field is enabled when Backup Type = Remote .
Password	Password is the valid password for the specified user login name for the remote server. The password is displayed as asterisks (*) when the user enters the password. This field is enabled when Backup Type = Remote .
Save the local copies in the default path	Selecting yes allows the backup file to be retained on the local ELAP server at the default file path /var/TKLC/elap/free/backup/. This field is enabled when Backup Type = Remote .
Option to delete old backups	Selecting yes results in deletion of all old backup files, except the number of backup files specified by the <i>Specify the number of files to maintain</i> option.
Specify the number of files to maintain	If the <i>Option to delete old backups</i> is yes , a minimum of one and maximum of seven backup files can be maintained. By default, five backup files are maintained.

RTDB Audit Menu

The Maintenance / RTDB Audit menu lets the user view and change the state of the RTDB audit on the selected ELAP.

The RTDB Audit menu provides these RTDB Audit tasks:

- [View Enabled](#)
- [Change Enabled](#)

View Enabled

The Maintenance / RTDB Audit / View Enabled menu screen displays the status of the RTDB audit on the selected ELAP.

Change Enabled

The Maintenance / RTDB Audit / Change Enabled screen turns auditing on and off for the RTDB that is on the selected ELAP. The user interface detects whether RTDB audit is enabled or disabled, and provides the associated screen to toggle the state.

To disable the RTDB audit, click the **Disable RTDB Audit** button. A screen displays, confirming that the RTDB audit was successfully disabled.

To restore the RTDB audit to enabled status, click the **Change Enabled** option on the Maintenance / RTDB Audit menu and then click the **Enable RTDB Audit** button. A screen displays, confirming that the RTDB audit was successfully enabled.

Note: When the RTDB Audit is enabled, an audit is automatically performed daily at 6:00 a.m. This audit file is stored in the ELAP system backup directory. Only the five most recent audits are stored and the older ones are automatically deleted. For this reason, it is advised that you do not disable the RTDB Audit.

Note: RTDB audit and LSMS bulk download cannot be enabled at the same time. Enabling one toggles the other to a disabled state.

LSMS High Speed Bulk Download Menu

The Maintenance / LSMS HS Bulk Download menu lets the user view and change the state of high speed bulk downloading of the selected ELAP.

The LSMS High Speed Bulk Download menu provides these actions:

- [View Enabled](#)
- [Change Enabled](#)

View Enabled

The Maintenance / LSMS HS Bulk Download / View Enabled menu selection displays the state of the LSMS High Speed Bulk Download / LSMS High Speed Resync.

Change Enabled

The Maintenance / LSMS HS Bulk Download / Change Enabled menu selection lets the user enable and disable the LSMS Bulk Download/LSMS HS Resync state. The user interface detects whether LSMS Bulk Download/LSMS HS Resync is enabled or disabled, and provides the associated screen to toggle the state.

To disable the LSMS High Speed Bulk Download, click the **Disable LSMS Bulk Download for this ELAP** button.

To restore the LSMS HS Bulk Download to Enabled status, click the **Change Enabled** option on the Maintenance / LSMS HS Bulk Download menu and then click the **Enable LSMS Bulk Download for this ELAP** button. A message displays, confirming that the LSMS High Speed Bulk Download, was successfully enabled.

LSMS Connection Menu

The Maintenance / LSMS Connection menu lets the user view and change the state of the LSMS connection.

The LSMS Connection menu provides these actions:

- [View Allowed](#)
- [Change Allowed](#)

View Allowed

The Maintenance / LSMS Connection / View Allowed menu selection displays the state of the LSMS connection.

Change Allowed

The Maintenance / LSMS Connection / Change Allowed menu selection lets the user enable and disable the LSMS connection. The user interface detects whether the LSMS Connection is enabled or disabled, and provides the associated screen to toggle the state.

To disable the LSMS connection, click the **Disable LSMS Connection** button. A message displays, confirming that the LSMS connection was successfully disabled.

To restore the LSMS HS Bulk Download to Allowed status, click the **Change Allowed** option on the Maintenance / LSMS Connection menu and then click the **Enable LSMS Connection** button. A message displays, confirming that the LSMS Connection was successfully enabled.

Schedule ELAP Tasks Menu

The Maintenance / Schedule ELAP Tasks menu allows the user to schedule tasks for the active ELAP.

ELAP Transaction Logging

The Maintenance / ELAP Transaction Logging menu lets the user turn on or off logging history of LNP provisioning records, and configure the logging on the ELAP server when the ELAP Logging Enhancement Feature is on. The ELAP Transaction Logging menu option appears on the ELAP GUI for the Active ELAP server only.

The logfile named `lnptrans_debug.log` is stored at `/var/TKLC/elap/logs/transLogs` in ASCII format.

The LNP provisioning records format is:

```
YYYYMMDDHHMMSS|TIME_ZONE_IDENTIFIER|COMMAND_TYPE|TN|SYSTEM_IDENTIFIER
For example: 0121016072627|UTC|UPD|9999999996|CHRLNCCA03W
```

The logging history is retained on the ELAP server for seven days. If the ELAP software is not restarted, then only one logfile per day is stored. By default, each logfile contains the records of all successful provisioning transactions for a 24-hour period, beginning after midnight. If the **Log files export to remote machine option** is set to *Enabled* and the remote server is configured, then the logfiles from the previous day are moved to the folder `/var/TKLC/appl/free/logsExport` in compressed format with filename `lnptrans.MM-DD-YYYY.<system_identifier>.log.tar.gz`, where MM-DD-YYYY is the date of the logfile.

- [View Configuration](#)
- [Change Configuration](#)

View Configuration

The Maintenance / ELAP Transaction Logging / View Configuration menu screen displays the status of the ELAP transaction logging. An example screen displayed after selecting View Configuration is shown in [Figure 27: Maintenance / ELAP Transaction Logging / View Configuration](#) (ELAP Logging Enhancement Feature = On; Log files export to remote machine = Enabled).

ELAP_A_NAME	View ELAP Transaction Logging Configuration
ELAP Logging Enhancements Feature:	On
Time Format:	System Defined
Log files export to remote machine:	Enabled
Remote system IP address:	10.248.15.12
Remote system user name:	root
Remote system sftp location:	/var/tmp

Figure 27: Maintenance / ELAP Transaction Logging / View Configuration

Change Configuration

The Maintenance / ELAP Transaction Logging / Change Configuration menu option allows the user to configure the ELAP Logging Enhancement Feature from the Active ELAP server only.

An example screen displayed after selecting Change Configuration is shown in [Figure 28: Maintenance / ELAP Transaction Logging / Change Configuration](#) (ELAP Logging Enhancement Feature = On; Log files export to remote machine = Enabled).

ELAP_A_NAME	Change ELAP Transaction Logging Configuration
ELAP Logging Enhancements Feature:	<input checked="" type="radio"/> On <input type="radio"/> Off
Time Format:	<input type="radio"/> UTC <input checked="" type="radio"/> System Defined
Log files export to remote machine:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Remote system IP address:	<input type="text" value="10.248.15.12"/>
Remote system user name:	<input type="text" value="root"/>
Remote system password:	<input type="password" value="*****"/>
Remote system sftp location:	<input type="text" value="/var/tmp"/>
<input type="button" value="Submit Data"/>	

Figure 28: Maintenance / ELAP Transaction Logging / Change Configuration

Table 8: Options for ELAP Transaction Logging

Option	Description
ELAP Logging Enhancement Feature	On, Off (default) When this option is set to <i>Off</i> , the other GUI fields are disabled. When this option is set to <i>On</i> , successful LNP provisioning transactions are logged on the ELAP server.
Time Format	UTC (default) = Coordinated Universal Time System Defined = System Local Time, appears as <i>SD</i> in the logging records
Log files export to remote machine	Enabled, Disabled (default) The Remote system fields can be accessed only when Log files export to remote machine is set to <i>Enabled</i> .
Remote system IP address	User-defined Remote system IP address can be any valid IP address, including the IP address of the Local/Mate server.
Remote system user name	User-defined
Remote system password	User-defined The password is stored in encrypted format.
Remote system sftp location	User-defined

To validate the authenticity of the remote server during configuration, the system attempts to execute a temporary SFTP operation on the remote server in the specified directory. If the temporary SFTP operation fails, the **Log files export to remote machine** option is reset to *Disabled* and an error message is displayed.

RTDB Menu

The RTDB (Real Time Database) Menu allows the user to interact with the RTDB for status, reloading, and updating.

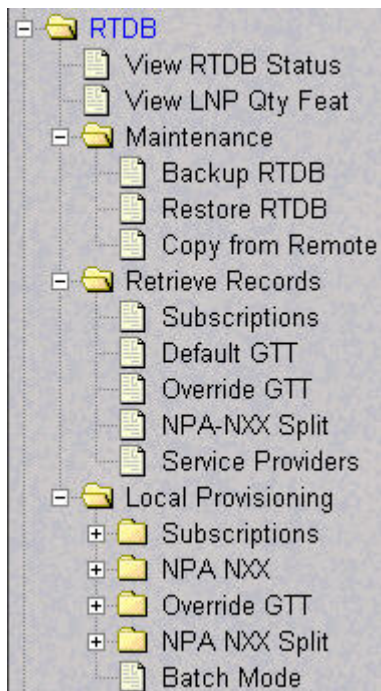


Figure 29: RTDB Menu

The RTDB menu supports various ELAP tasks, including:

- [View RTDB Status](#)
- [View LNP Quantity Features](#)
- [Maintenance Menu](#)
- [Retrieve Records Menu](#)
- [Local Provisioning Menu](#)

View RTDB Status

The RTDB / View RTDB Status screen displays the current DB level and DB birthday (date and time of the creation of the database) of the RTDB on the Local ELAP. The View RTDB Status screen displays the counts for:

- TNs
- NPBs
- DGTTs
- OGTTs
- Splits
- LRNMRs
- LRNs
- MRs
- NPANXXs
- TN-NPANXXs

The NPBs, DGTs, and Splits counts are updated once every minute. The other counts are constantly updated

View LNP Quantity Features

The RTDB / View LNP QTY screen displays the enabled LNP quantity features and quantity enabled as provisioned on the EAGLE 5 ISS (requires View LNP Qty Features action privilege to view this menu selection).

Maintenance Menu

The RTDB / Maintenance menu allows the user to:

- [Backup RTDB](#)
- [Restore RTDB](#)
- [Copy from Remote](#)

Backup RTDB

The RTDB / Maintenance / Backup RTDB screen lets the user backup the RTDB to a file on the selected ELAP.

Note: When the backup is complete, it is automatically copied to the standby ELAP.

To backup the RTDB, click the **Backup RTDB** button. A screen displays to confirm your backup choice. Click the **Confirm RTDB Backup** button. A message appears, confirming successful startup of the RTDB backup.

Restore RTDB

The RTDB / Maintenance / Restore the RTDB screen lets the user restore the RTDB from an RTDB image file. The software must be down for the restore to be allowed to ensure that no updates are occurring.

Note: For information on restoring the RTDB from a backup file, see *Alarms and Maintenance* for ELAP.

Copy from Remote

The RTDB / Maintenance / Copy RTDB from Remote screen lets the user copy RTDB files from a mate or remote ELAP to the local ELAP.

To copy the remote RTDB, the remote box's IP address and a password for the *elapdev* user ID must be entered on the screen and the file to be transferred is selected. See the [Copy RTDB from Remote](#) procedure.

Retrieve Records Menu

The RTDB / Retrieve Records menu lets the user retrieve a single subscription record, a single default GTT record, a single override GTT record, a single NPANXX record, and a service provider record or list all service providers.

The RTDB / Retrieve Records menu provides these actions:

- [Subscriptions](#)
- [Default GTT](#)
- [Override GTT](#)
- [NPA-NXX Split](#)
- [Service Providers](#)

Subscriptions

The RTDB / Retrieve Records / Subscriptions menu option lets the user retrieve a single subscription record using a 10-digit subscription as the key.

Enter the single ten-digit subscription number in the **Start TN** field, and click the **Retrieve** button.

Default GTT

The RTDB / Retrieve Records / Default GTT Records from RTDB screen lets you retrieve a single default GTT record using a six-digit NPA NXX number as the key.

Enter the single NPA NXX number in the **Default GTT NPANXX** field, and click the **Retrieve** button.

Override GTT

The RTDB / Retrieve Records / Override GTT screen lets the user retrieve a single override GTT record using a 10-digit LRN number as the key.

Enter the single Location Routing Number in the **LRN** field, and click the **Retrieve** button.

NPA-NXX Split

The RTDB / Retrieve Records / NPA NXX Split screen lets the user retrieve a single split NPA NXX record using a 6-digit NPA NXX number as the key.

Enter the single NPA NXX split record number in the **NPANXX** field, and click the **Retrieve** button.

Service Providers

The RTDB / Retrieve Records / Service Providers from RTDB screen lets you retrieve a single service provider record or list all the service providers in the database.

Enter the number in the **Service Provider ID** field, and click the **Retrieve** button.

Note: To retrieve a list of all of the service providers, leave the **Service Provider ID** field blank and click the **Retrieve** button.

Local Provisioning Menu

The RTDB / Local Provisioning menu allows the user provision LNP data directly to the RTDB.

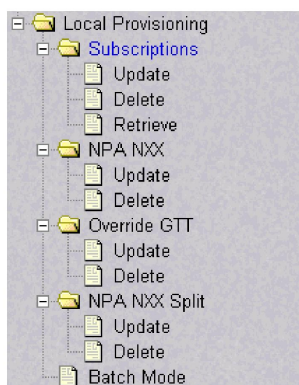


Figure 30: Local Provisioning Menu

Local Provisioning Utility

The Local Provisioning Utility (LPU) handles customer data received locally and processes Local Provisioning commands.

The LPU provides the ability to update the HA-Active ELAP RTDB or execute provisioning commands during an emergency situation. Otherwise, the LPU should not be used to update the ELAP database (this is the function of the LSMS).

In the event of a loss of the TCP/IP connection between the LSMS and the HA-Active ELAP, the LPU allows the customer to send manual updates to the RTDB of the HA-Active ELAP. The LPU also allows the user to process commands.



Caution: Manually applying updates to the ELAP RTDB using the LPU can result in LSMS and ELAP databases that are not synchronized (contain different data).

CAUTION

The RTDB / Local Provisioning menu provides these actions:

- [Subscriptions](#)
- [NPA NXX Menu](#)
- [Override GTT Menu](#)
- [NPA NXX Split Menu](#)
- [Batch Mode](#)

Subscriptions

The RTDB / Local Provisioning / Subscriptions menu options lets the user update, delete, and retrieve LNP data directly to the RTDB.

The RTDB / Local Provisioning / Subscriptions menu provides these actions:

- [Subscriptions / Update](#)
- [Subscriptions / Delete](#)
- [Subscriptions / Retrieve](#)

Subscriptions / Update

The RTDB / Local Provisioning / Subscriptions / Update LNP Subscription Records screen lets the user update values for a specific subscription using a 10-digit subscription number as a key.

Enter the required information and click the **Update** button.

Subscriptions / Delete

The RTDB / Local Provisioning / Subscriptions / Delete LNP Subscription Records screen lets the user delete a specific subscription record using a 10-digit subscription number as a key.

Enter the single ten-digit subscription number in the **TN** field, and click the **Retrieve** button.

Subscriptions / Retrieve

The RTDB / Local Provisioning / Subscriptions / Retrieve LNP Subscription Records screen lets the user retrieve a specific subscription record using a 10-digit subscription number as a key.

Enter the single ten-digit subscription number in the **TN** field, and click the **Retrieve** button.

NPA NXX Menu

The RTDB / Local Provisioning / NPA NXX menu lets the user update and delete a single NPA NXX record directly to the RTDB.

The RTDB / Local Provisioning / NPA NXX menu provides these actions:

- [NPA NXX / Update](#)
- [NPA NXX / Delete](#)

NPA NXX / Update

The RTDB / Local Provisioning / NPA NXX / Update NPA NXX Records screen allows you to update values for a specific NPA NXX record using a 6-digit subscription number as a key.

Enter the required information and click the **Update** button.

NPA NXX / Delete

The RTDB / Local Provisioning / NPA NXX / Delete NPA NXX Records screen allows you to delete values for a specific NPA NXX record using a 6-digit subscription number as a key.

Enter the single NPA NXX number in the **Default GTT NPANXX** field, and click the **Delete** button.

NPA NXX / Retrieve

The RTDB / Local Provisioning / NPA NXX / Retrieve NPA NXX Records screen allows you to retrieve values for a specific NPA NXX record using a 6-digit subscription number as a key.

Enter the single NPA NXX number in the **Default GTT NPANXX** field, and click the **Retrieve** button.

Note: The RTDB / Local Provisioning / NPA NXX / Retrieve NPA NXX Records screen displays NPANXX records if DGTT is not explicitly provisioned on the LSMS for the NPANXX.

Override GTT Menu

The RTDB / Local Provisioning / Override GTT menu lets the user update and delete a single LRN (Location Routing Number) record directly on the RTDB.

The RTDB / Local Provisioning / Override GTT menu provides these actions:

- [*Override GTT / Update*](#)
- [*Override GTT / Delete*](#)
- [*Override GTT / Retrieve*](#)

Override GTT / Update

The RTDB / Local Provisioning / Override GTT / Update Override GTT Records screen lets the user update values for a specific LRN record using a 10-digit LRN number as a key.

Enter the required information and click the **Update** button.

Override GTT / Delete

The RTDB / Local Provisioning / Override GTT / Delete Override GTT Records screen lets the user delete a specific LRN record using a 10-digit LRN number as a key.

Enter the specific Location Routing Number in the **LRN** field, and click the **Delete** button.

Override GTT / Retrieve

The RTDB / Local Provisioning / Override GTT / Retrieve Override GTT Records screen lets the user retrieve a specific LRN record using a 10-digit LRN number as a key.

Enter the specific Location Routing Number in the **LRN** field, and click the **Retrieve** button.

NPA NXX Split Menu

The RTDB / Local Provisioning / NPA NXX Split menu lets the user update and delete a single Split NPA NXX record directly on the RTDB.

The RTDB / Local Provisioning / NPA NXX Split menu provides these actions:

- [*NPA NXX Split / Update*](#)
- [*NPA NXX Split / Delete*](#)
- [*NPA NXX Split / Retrieve*](#)

NPA NXX Split / Update

The RTDB / Local Provisioning / NPA NXX Split / Update NPA NXX Split Records screen lets the user update values for a single Split NPA NXX record using a 6-digit NPA NXX number as a key.

Enter the required information and click the **Update** button.

NPA NXX Split / Delete

The RTDB / Local Provisioning / NPA NXX Split / Delete screen lets the user delete a single Split NPA NXX record using a 6-digit NPA NXX number as a key.

Enter the single Split NPA NXX record using a 6-digit NPA NXX number in the **Old or New NPANXX:** field, and click the **Update** button.

NPA NXX Split / Retrieve

The RTDB / Local Provisioning / NPA NXX Split / Retrieve screen lets the user retrieve a single Split NPA NXX record using a 6-digit NPA NXX number as a key.

Enter the single Split NPA NXX record using a 6-digit NPA NXX number in the **NPANXX:** field, and click the **Retrieve** button.

Batch Mode

The RTDB / Local Provisioning / Batch Mode screen lets the user upload an LPU batch file for local provisioning.

Debug Menu

The Debug Menu allows the user to view logs, list running processes, and access the EAGLE 5 ISSMMI port.

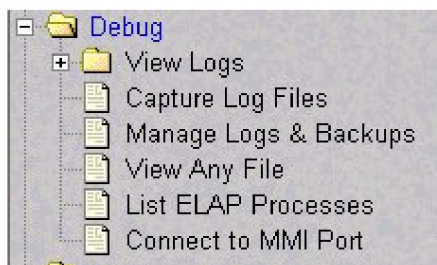


Figure 31: Debug Menu

The Debug menu provides these actions:

- [View Logs Menu](#)
- [Capture Log Files](#)
- [Manage Logs and Backups](#)
- [View Any File](#)
- [List ELAP Software Processes](#)
- [Connect to EAGLE MMI Port](#)

View Logs Menu

The Debug / View Logs menu allows the user to view such logs as the Maintenance, RTDB, Provisioning, RTDB audit, and UI logs. When the user selects the View Logs menu, a password window is displayed as shown in [Figure 32: View Maintenance Log Password Screen](#).

ELAP A

View Maintenance Log

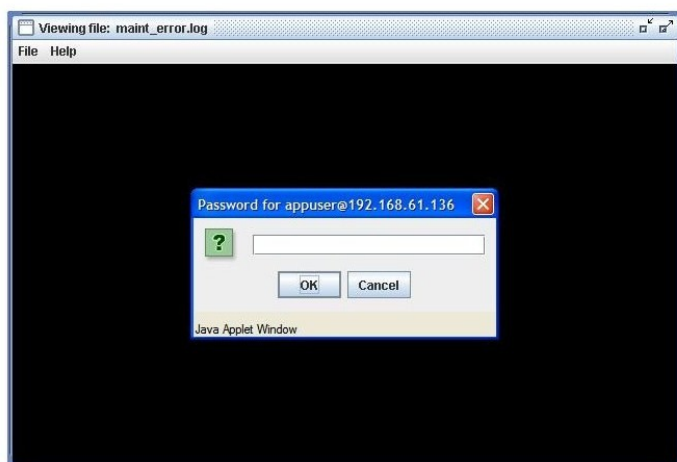


Figure 32: View Maintenance Log Password Screen

To view logs, the "appuser" must enter a password. The initial password setting for "appuser" is eagle2.

Note: The "appuser" is the only user authorized to view logs.

After logging in, the following View Logs menu options are available:

- LNPTRANS
- Maintenance
- RTDB
- Provisioning
- RTDB Audit
- LSMS Audit
- CGI
- GS
- TRPD

When any of the Debug / View Logs menu options are chosen, the process is the same. The chosen selection causes the Log Viewer window, similar to [Figure 33: View Maintenance Log Screen](#), to appear.

A

View Maintenance Log

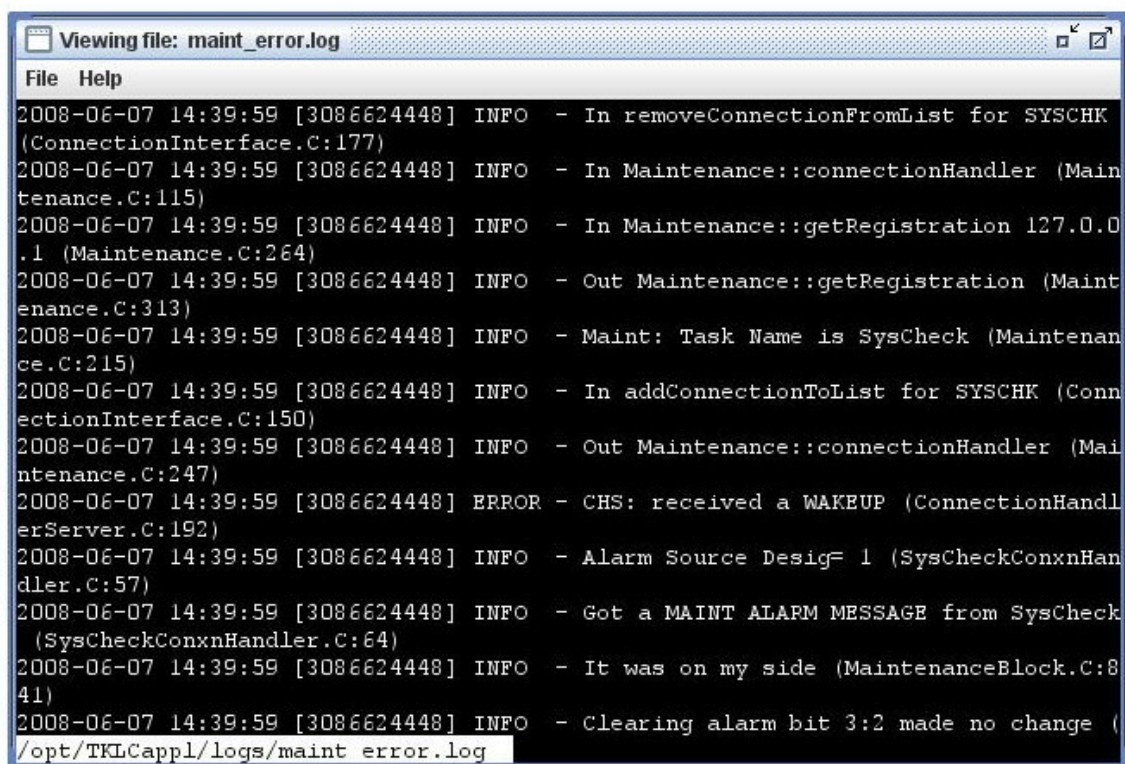


Figure 33: View Maintenance Log Screen

Use the navigation commands in [Table 9: Navigation Commands](#) to navigate through the displayed file.

Table 9: Navigation Commands

Command	Action
<return>	Scroll down 1 line
<space>	Scroll down 1 page
b	Scroll up 1 page
G	Go to bottom of file
/ {pattern}	Search for {pattern} from current position in file
n	Repeat search

Capture Log Files

The **Debug / Capture Log Files** screen allows for copying of the logs for the current MPS. Optionally, you can capture files with the logs.

To capture the log files, click the **Capture Logs** button. A successful completion message appears.

Manage Logs and Backups

The Debug / Manage Logs and Backups screen displays the captured log files and allows the user to view and manage (delete) captured log and backup files. It also allows the user to copy the selected files to a Mate ELAP.

In the initial Manage Logs and Backups screen, enter a subdirectory name in the **File Path** text box and click the **OK** button to display the desired logs and backups.

To delete a log or backup file, click the **Checkbox** associated with a log or backup and click the **Delete Selected File(s)** button. A screen displays, confirming successful file removal.

To copy a log or backup file to a Mate ELAP, click the **Checkbox** associated with a log or backup and click the **Copy to Mate Selected File(s)** button. A screen displays, confirming successful copy.

View Any File

The Debug / View Any File screen allows the user to view any file on the system.

List ELAP Software Processes

The Debug / List ELAP Software Processes screen shows the ELAP processes started when the ELAP boots or when the “Start ELAP software” prompt is used. The `/bin/ps -auxw` command generates this list. (The operating system's manual page for the `ps` command thoroughly defines the output for this command.).

When you have finished viewing the List ELAP Software Processes screen, you can click the **Back** button on the browser or select another menu item to perform.

Connect to EAGLE MMI Port

The Debug / Connect to EAGLE MMI Port screen lets the user connect to the EAGLE using an MMI port. This connection can only be made from ELAP B. See *Commands Manual* for a detailed listing of EAGLE commands and the input and output from the EAGLE MMI port.

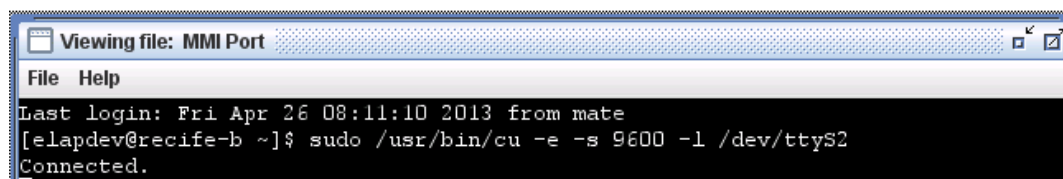


Figure 34: Connect to MMI Port Screen

This menu option opens a window and starts a SSH session allowing where EAGLE commands can be issued. Select **File > Quit** to close connection. Select another menu item to close the window.

The MMI port is on only ELAP B; connection to the port is only allowed when on ELAP B. Attempting to connect to the MMI from ELAP A results in an error dialog.

Platform Menu

The Platform Menu allows the user to perform various platform-related functions, including running health checks, listing processes, viewing logs, rebooting the MPS, and initiate an SSH connection as shown in [Figure 35: Platform Menu](#).

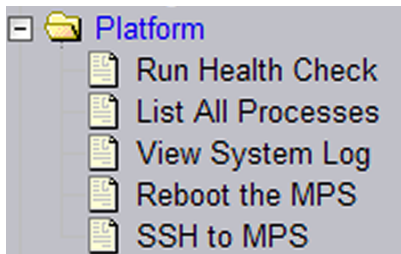


Figure 35: Platform Menu

The Platform menu provides these actions:

- [Run Health Check](#)
- [List All Running Processes](#)
- [View System Log](#)
- [Reboot the MPS](#)
- [SSH to MPS](#)

Run Health Check

The Platform / Run Health Check screen allows the user to execute the health check routine on the selected ELAP. *Alarms and Maintenance* for ELAP describes the health check, which is also called system health check and syscheck, in detail.

The first screen presented in the workspace frame lets the user select the normal or verbose mode of output detail.

The ELAP system health check utility performs multiple tests of the server. For each test, checks and balances verify the health of the MPS server and platform software. Refer to *Alarms and Maintenance* for ELAP for the functions performed and how to interpret the results of the normal outputs.

List All Running Processes

The Platform / List All Running Processes screen lists all processes running on the selected ELAP. The `/bin/ps auxw` command generates this list. The operating system's manual page for the `ps` command thoroughly defines the output for this command. [Figure 36: List All Running Processes Screen](#) shows an example of the process list.

USER	PID	%CPU	%MEM	SZ	RSS	TT	S	START	TIME	COMMAND
nobody	8574	4.5	5.2	6736	6336	?	S	10:00:54	0:00	/opt/TKLCplat/bin.
root	1	0.2	0.2	752	144	?	S	Nov 08	6:57	/etc/init -
root	8587	0.2	1.1	1528	1272	?	O	10:00:55	0:00	/usr/ucb/ps -auxw
nobody	1432	0.1	1.3	2704	1560	?	S	Nov 08	0:00	/opt/TKLCplat/apa
elapdev	2916	0.1	2.0	4904	2392	?	S	Nov 08	3:24	/opt/TKLCappl/bin.
root	3	0.1	0.0	0	0	?	S	Nov 08	4:32	fsflush
elapdev	4904	0.0	2.2	4432	2632	?	S	09:51:48	0:00	/opt/TKLCelap/bin.
root	0	0.0	0.0	0	0	?	T	Nov 08	0:01	sched
root	2	0.0	0.0	0	0	?	S	Nov 08	0:03	pageout
root	75	0.0	0.2	1264	144	?	S	Nov 08	0:00	/usr/lib/devfsadm.
root	77	0.0	0.0	2264	?	?	S	Nov 08	0:00	/usr/lib/devfsadm.
root	141	0.0	0.0	1800	?	?	S	Nov 08	0:00	/etc/opt/SUNWconn.
root	156	0.0	0.0	1744	?	?	S	Nov 08	0:00	/usr/sbin/aspppd
root	176	0.0	0.4	2152	504	?	S	Nov 08	0:00	/usr/sbin/rpcbind
root	178	0.0	0.8	2352	896	?	S	Nov 08	0:00	/usr/sbin/keyserv
root	208	0.0	0.0	1992	?	?	S	Nov 08	0:00	/usr/sbin/inetd -.
daemon	210	0.0	0.9	2416	1072	?	S	Nov 08	0:00	/usr/lib/nfs/stat.
root	211	0.0	0.0	1808	?	?	S	Nov 08	0:00	/usr/lib/nfs/lock
root	222	0.0	1.2	2480	1400	?	S	Nov 08	0:00	/usr/lib/autofs/a
root	234	0.0	1.2	2976	1464	?	S	Nov 08	0:00	/usr/sbin/syslogd
root	240	0.0	0.0	1784	?	?	S	Nov 08	0:00	/usr/sbin/cron

Note: The exact processes shown here will not be the same on your ELAP servers. The output from this command is unique for each ELAP, depending on the ELAP software processes, the number of active ELAP user interface processes, and other operational conditions.

Figure 36: List All Running Processes Screen

View System Log

The Platform / View System Log screen allows the user to display the System Log. Each time a system maintenance activity occurs, an entry is made in the System Log. When the user chooses this menu selection, the View the System Log screen appears.

Reboot the MPS

The Platform / Reboot the MPS screen allows the user to reboot the selected ELAP. All ELAP software processes running on the selected ELAP are shut down normally.

When you click the **Reboot MPS** button, a cautionary message appears, informing the user that this action causes ELAP to stop all activity and to prevent the RTDB from being updated with new subscriber data.

When you are certain that you want to reboot, click the **Continue** button. Another screen informs you that MPS is being rebooted and that the User Interface will be reconnected when the reboot is completed.

SSH to MPS

The Platform / SSH to MPS menu option allows the user to initiate an SSH connection to the user interface. Selecting this option opens a Java applet prompting the user for authentication.

The user must supply a username and the hostname (VIP address) of the ELAP (separated by an ampersand) and click **OK**:

Note: The hostname is the VIP address of the ELAP as displayed in the **Address Bar** of the browser.

A **Password** applet displays, prompting the user to enter a password and click **OK**.

A **Warning** dialog displays allowing the user to confirm the SSH connection to the specified MPS.

Upon clicking **yes**, the SSH connection is established to the MPS and the **SSH to MPS** window displays.

User Administration Menu

The User Administration menu allows the user to perform various platform tasks, including administering users and groups, terminating active sessions, and modifying system defaults. The user interface allows for many users with multiple and varied configurations of permissions. It is designed for convenience and ease of use while supporting complex user set-ups where required.

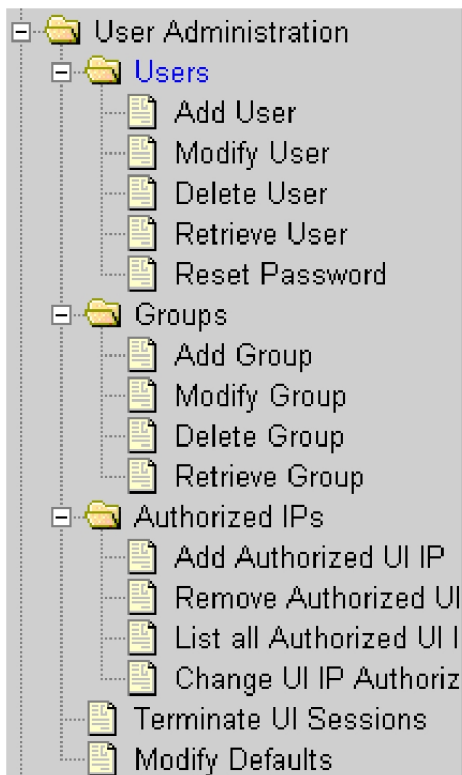


Figure 37: User Administration Menu

When a user successfully logs into the UI, he is considered to have a session open. These rules apply to session management and security.

- **Idle Port Logout:** If no messages are exchanged with the UI client session for a configurable amount of time, the session is automatically closed on the server side. The default length of the timeout is a system-wide value, configurable by the administrator. The administrator can also set a different timeout length for an individual user, if desired.

- Multiple Sessions per User: The administrator can turn off multiple sessions allowed per user on a global system-wide basis.
- Revoke/Restore User: The administrator can revoke a userid. A revoked userid remains in the database but can no longer log in. Likewise, the administrator can restore a userid that was previously revoked.
- Manage Unused UserIDs: The ELAP UI automatically revokes userids that are not accessed within a specified number of days. The number of days is a system-wide value that is definable by the administrator.
- Login Tracking: When a user successfully logs in, the UI displays the time of the last successful login and the number of failed login attempts for that userid.
- Intrusion Alert: When the number of successive failed login attempts from a specific IP address reaches 5 (five), the ELAP automatically writes a message to the UI security log and displays a message on the banner applet to inform any administrator logged in at that time.
- Revoke Failed User: The UI automatically revokes any user who has N successive login failures within 24 hours. N is a system-wide configurable number, with a default of 3 (three). This restriction is turned off if N is set to 0 by the administrator.

The User Administration menu performs administration functions for users and groups, and handles terminating active sessions and modifying system defaults. See these topics discussed:

- [Users Menu](#)
- [Groups Menu](#)
- [Authorized IP Address Menu](#)
- [Terminate Active UI Sessions](#)
- [Modify System Defaults](#)

Users Menu

The User Administration / Users menu allows the system administrator to administer users functions such as add, modify, delete, retrieve, and reset user password.

A user is someone who has been given permission with system administrator authority to log in to the user interface. The administrator creates these user accounts and associates them with the groups to which they belong. A user automatically has access to all actions allowed to the groups he is a member. In addition to the user's groups, the administrator can set other user-specific permissions or restrictions to any user's set of individual permissions.

The ELAP user interface comes pre-defined with user interface users in order to provide a seamless transition to the user interface. This is done by duplicating the Unix user logins and permissions that exist on the text-based UI. In addition, The default password for a new uiadmin is uiadmin. See [Table 10: ELAP UI Logins](#) for login names.

Table 10: ELAP UI Logins

Login Name	Access Granted
elapmaint	Maintenance menu and all submenus
elapdatabase	Database menu and all submenus

Login Name	Access Granted
elapdebug	Debug menu and all submenus
elapplatform	Platform menu and all submenus
uiadmin	User Administration menu
elapall	All of the above menus
elapconfig	Configuration menu and all submenus (text-based UI)

The Users menu provides these actions:

- [Add User](#)
- [Modify User](#)
- [Delete User](#)
- [Retrieve User](#)
- [Change System User Password](#)
- [Reset User Password](#)

Add User

The User Administration / Users / Add User screen lets the administrator add a new user interface user name and a default password.

Modify User

The User Administration / Users / Modify User screen lets the administrator change these aspects of a user permission profile.

- [User Permissions](#)
- [User Group Memberships](#)
- [User Action Privileges](#)

The administrator must first select a user name from the list of current users.

User Permissions

After selecting a user name, the user permissions screen appears, as shown in [Figure 38: Specify the UI User's Permissions Screen](#). In this screen, the administrator can view and specify the permissions allowed to the user, such as directly specifying the number of concurrent log-ins, an inactivity time limit, and a password age limit.

A
Modify UI User

User Name:	ric-test	User ID:	7
Administrator:	<input type="checkbox"/>	Debug User:	<input type="checkbox"/>
Reset Password:	<input checked="" type="checkbox"/>	User Revoked:	<input type="checkbox"/>
Maximum Concurrent Logins:	<input checked="" type="radio"/> System Default (1) <input type="radio"/> Infinite <input type="radio"/> User Specific <input style="width: 50px;" type="text"/>		
Session Inactivity Limit:	<input checked="" type="radio"/> System Default (10) <input type="radio"/> Infinite <input type="radio"/> User Specific <input style="width: 50px;" type="text"/> in minutes		
Maximum Password Age:	<input checked="" type="radio"/> System Default (Infinite) <input type="radio"/> Infinite <input type="radio"/> User Specific <input style="width: 50px;" type="text"/> in days		

Submit Profile Changes

Modify Group Membership

Modify Specific Actions

Figure 38: Specify the UI User's Permissions Screen

After modifying any of the direct entries, such as concurrent logins or inactivity, click the **Submit Profile Changes** button. A screen confirming the changes displays.

User Group Memberships

To customize the individual's access to groups, click the **Modify Group Membership** button in [Figure 38: Specify the UI User's Permissions Screen](#). The Modify UI User's Group Membership Screen displays the group membership choices available for the user.

After making any changes to the user's group memberships, click the **Submit Group Membership Changes** button to submit the changes.

User Action Privileges

To specify the action privileges for the user, click the **Modify Specific Actions** button in [Figure 38: Specify the UI User's Permissions Screen](#). The Modify UI User's Specific Actions Screen displays action privileges that can be specified for the user that is being modifying.

This screen contains many selections from which to choose. After customizing the settings, click the **Submit Specific Action Changes** button at the bottom of the screen.

The bottom of the Modify UI User's Special Actions screen contains these explanatory notes:

- ^A - Permission for this action has been explicitly added for this user.
- ^R - Permission for this action has been explicitly removed for this user.

These notes indicate the privileges specifically added or removed for an individual user from the groups to which he/she is a member. This allows discrete refinement of user privileges even though he/she may be a member of groups.

Delete User

The User Administration / Users / Delete User screen lets an administrator remove a user name from the list of user interface names. First select the user name to be deleted and click the **Delete User** button. A confirmation screen appears, requesting approval of the change.

In the confirmation screen, click the **Confirm Delete User** button. After confirmation, a success screen is generated.

Retrieve User

The User Administration / Users / Retrieve User screen allows the administrator to display the user name permission profiles from the user interface information. First select a user name to be retrieved, and click the **Select User** button. The Retrieve UI User screen displays the permissions allowed to the selected user, including the maximum allowed number of concurrent log-ins and the inactivity time limit.

Group membership information for the user can be viewed by clicking the **View Group Membership** button.

User privileges can be accessed from the Retrieve UI User screen by clicking on the **View Specific Actions** button. The bottom of Retrieve UI User screen contains these explanatory notes:

- ^A - Permission for this action has been explicitly added for this user.
- ^R - Permission for this action has been explicitly removed for this user.

These notes indicate the privileges specifically added or removed for an individual user from the group to which he/she is a member. These permissions allow individual variations to user privileges even though the user is a member of a group.

Change System User Password

All system users can change their own passwords. The **elapdev** and **appuser** users use the `passwd` command provided by the Operating System. If changing a password using the `passwd` command, then the Linux PAM credit rules are used.

The system user **elapconfig** uses the option provided in the [Figure 110: ELAP Configuration Menu](#) . Linux PAM rules are not applicable while changing the password for **elapconfig** user. Only the configured minimum password length applies.

Reset User Password

The User Administration / Users / Reset User Password screen lets the administrator select a user name and change the password. When the user's password is correctly updated, a confirmation screen appears.

Groups Menu

The User Administration / Groups menu allows the user to administer group functions.

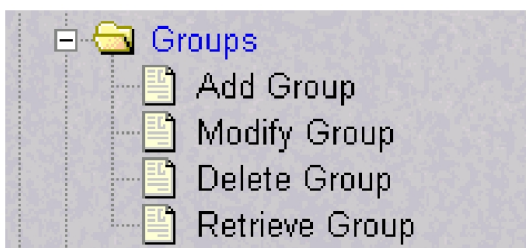


Figure 39: User Administration / Groups Menu

For convenience, actions can be grouped together. These groups can be used when assigning permissions to users. The groups can consist of whatever combinations of actions that system administrators deem reasonable. Group permissions allow any given action to be employed by more than one group.

Groups can be added, modified, deleted, and viewed through the menu items in the User Administration / Groups menu.

The ELAP user interface comes with pre-defined groups with the same names and action permissions used in the text-based (ELAP version 1.0) user interface:

- maint
- database
- platform
- debug
- admin

One additional pre-defined group used is new to ELAP version 3.0. This group is called `readonly`. The `readonly` group contains only actions that view status and information. The `readonly` group is the default group for new users.

Note: The ELAP User Interface concept of groups should not be confused with the Unix concept of groups. The two are not related.

The Groups menu performs these actions:

- [Add Group](#)
- [Modify Group](#)
- [Delete Group](#)
- [Retrieve Group](#)

Add Group

The User Administration / Groups / Add Group screen allows the administrator to enter a new user interface group and assign action privileges with the new group.

After successfully adding a new group, designate the Action Privileges for the new group. See [Modify Group](#).

Modify Group

The User Administration / Group / Modify Group screen allows the administrator to modify user interface group permission profiles. Select the Group Name, and click the **Select Group** button. The Modify Group Permission Profiles screen displays the current action privileges assigned to the user interface group.

Specify the Action Privileges to assign to this user interface group and click the **Submit Specific Action Changes**. A screen confirming the changes appears.

Delete Group

The User Administration / Group / Delete Group screen allows the administrator to remove a user interface group from the user interface information.

First select the user interface group name and click the **Select Group** button. A confirmation banner and button appear. Finally, select the **Confirm Delete Group** button to delete the user interface group name and its permissions.

If a group is part of the New User Default Groups field as shown in [Figure 42: Modify System Defaults Screen](#), it cannot be deleted unless it is removed from the New User Default Groups list.

Retrieve Group

The User Administration / Users / Retrieve Group screen allows the administrator to display the permission profiles for user interface groups.

First select a user interface group name to be retrieved and click the **Select Group** button. The Retrieval of UI User Information Screen displays the permissions allowed to the this user interface group. Only the actions supported for the group appear.

Authorized IP Address Menu

The User Administration / Authorized IP menu allows the administrator to add, remove, and list all authorized UI IP addresses and also change the UI IP address authorization status.

The User Administration / Authorized IP menu provides these actions:

- [Add Authorized UI IP Address Screen](#)
- [Remove Authorized UI IP Address Screen](#)
- [List All Authorized UI IP Addresses](#)
- [Change UI IP Authorization Status](#)

Add Authorized UI IP Address Screen

The User Administration / Authorized IP / Add Authorized UI IP screen lets the user add a new IP address to the list of authorized IP addresses.

Enter the IP address to be authorized and press the **Allow IP** button. When an authorized IP address is accepted, the message indicating a successful acceptance of the address appears.

An error notification screen appears when:

- A duplicate IP address is entered (the address already exists)
- An attempt to add more than the maximum allowable number of addresses (i.e., more than 1,000)

- Any internal failure is detected

Remove Authorized UI IP Address Screen

The User Administration / Authorized IP / Remove Authorized UI IP screen lets the user remove an IP address from the list of authorized IP addresses. Enter the individual IP address or Classless Interdomain Routing Format (CIDR) IP format in the **IP to Remove** field.

When the authorized IP address is deleted, a message confirming the removal of the specified address appears.

List All Authorized UI IP Addresses

The User Administration / Authorized IP / List All Authorized UI IPs screen retrieves and displays all authorized IP addresses. The screen also shows whether the authorization list is Enabled or Disabled. See [Figure 40: List All Authorized UI IP Addresses Screen](#) for an example of the List All Authorized UI IP address screen.

A List All Authorized UI IPs

The authorization list is currently **Disabled**.

Allowed Addresses				
10.25.60.137	192.168.10.2/24	192.168.57.2/24	192.168.57.73	192.168.57.77
192.168.61.123				

Figure 40: List All Authorized UI IP Addresses Screen

For information about enabling and disabling the authorization list, see [Change UI IP Authorization Status](#).

Change UI IP Authorization Status

The User Administration / Authorized IP / Change UI IP Authorization Status screen permits toggling (that is, alternating) the state of authorization list between 'enabled' and 'not enabled.'

When this menu option is chosen, the current authorization state is displayed in the **INFO** field.

If the authorization state is 'NOT Enabled', click the **Enable IP Checking** button to toggle the state to 'Enabled'.

The enforcement of the checking for authorization status is immediate. The IP address of every message of every IP device using the GUI is checked as soon as the authorization status is enabled. The checking for authorized IPs does not occur only when devices log in.

Terminate Active UI Sessions

The User Administration / Terminate Active Sessions screen allows the administrator to selectively terminate individual active user interface sessions. See the Terminate Active Sessions screen in [Figure 41: Terminate Active Sessions Screen](#).

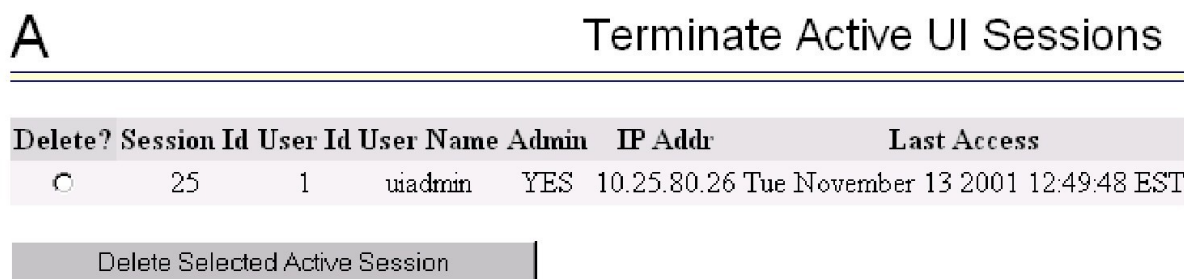


Figure 41: Terminate Active Sessions Screen

Select a user interface session for termination, by clicking in the **Delete?** column. A message confirming a successful termination is displayed.

Modify System Defaults

The User Administration / Modify System Defaults screen allows the administrator to manage the systems defaults. See [Figure 42: Modify System Defaults Screen](#).

abaco-a Modify System Defaults

Maximum Failed User Logins:
This field represents the number of consecutive failed logins for a specific user before that user's account is revoked.

Password Reuse Limit:
This field represents the number of passwords for user that must be used before a previous password is allowed to be reused.

Maximum Account Inactivity:
This field represents the number of days that a specific user account can be idle before the account is automatically revoked.

Session Idle Timeout:
This field represents the number of minutes that an open session can remain idle before it is closed automatically by the server.

Maximum Password Age:
This field represents the number of days that a user can have the same password before he is forced to change it by the user interface.

Maximum Concurrent User Logins:
This field represents the number of concurrent login sessions that each user can have. This limitation does not apply to users with Administrative privileges.

Maximum Concurrent Logins:
This field represents the total number of concurrent login sessions that can exist on the ELAP pair. Users with Administrative privileges are not included in the total session count.

Login Message Text:

Figure 42: Modify System Defaults Screen

The system defaults that you can modify are:

- **Maximum Failed User Logins:** This field specifies the number of consecutive failed logins allowed for a specific user before that user's account is revoked.
- **Password Reuse Limit:** This field requires a specified number of unique passwords that a user must use before accepting a previous password.
- **Maximum Account Inactivity:** This field specifies the number of days that a user account can be idle before the account is automatically revoked. If a user account is revoked, the user must contact the system administrator before being able to use the system again.

The account inactivity value is calculated by date. An expiration value of 1 day does not mean that the user will be revoked after 24 hours. Hours and minutes are not considered. For example, an expiration value of 1 day set at any time on January 1 will cause the user to be revoked after the expiration of the new date, which is the current date plus the timeout value. In this example, the new date is January 2 (January 1 + 1 day). The user would be revoked at the start of January 3.

- **Session Idle Timeout:** This field limits the number of minutes that an open session can remain idle before the server automatically closes the session.
- **Maximum Password Age:** This field limits the number of days that a user can have the same password before requiring him/her to change it.
- **Maximum Concurrent User Logins:** This field limits the number of concurrent login sessions that each user can have. This limitation does not apply to users with Administrative privileges.
- **Maximum Concurrent Logins:** This field limits the number of concurrent login sessions that can exist on the ELAP pair. Users with Administrative privileges are excluded from this total session count.
- **Login Message Text:** This field contains the text message displayed in the initial work area at login. The field is limited to 255 characters. The default text is:

NOTICE: This is a private computer system. Unauthorized access or use may lead to prosecution.

- **New User Default Groups:** This field contains a list of group names (comma-delimited) with which newly created users are automatically assigned. The default group name is readonly.
- **Unauthorized IP Access Message:** This field contains the text message displayed when a connection is attempted from an IP address that does not have permission to use the UI. The default text is:
NOTICE: This workstation is not authorized to access the GUI.
- **Status Refresh Time:** This field contains the system default for the refresh time used for the **View RTDB Status**. The time must be set to either 5-600 seconds or 0 (no refreshing). The refresh time shown in **View RTDB Status** screen will be set to 5 if a value of 1 to 4 is entered.
- **ELAP A Pretty Name:** This field defines the name that is displayed on the top left of menu screens on the ELAP A GUI. The default text is ELAP_A_NAME.
- **ELAP B Pretty Name:** This field defines the name that is displayed on the top left of menu screens on the ELAP B GUI. The default text is ELAP_B_NAME.
- **Configurable Quantity Threshold Alarm:** This field shows the configurable percentage for the Quantity Threshold Alarm.
- **Non-Configurable Quantity Threshold:**

This field is non-configurable and read-only, and it shows the non-configurable percentage for the Quantity Threshold alarm. It raises a major alarm upon reaching the 100% RTDB level.

When the changes to the system defaults are complete, click the **Submit Defaults** button. A message confirming a successful change appears.

Change Password

The Change Password menu selection provides a screen from which an ELAP user can change her/his password. This basic action is available to all users and is accessible from the [ELAP GUI Menus](#).

To change the password, enter the current password, enter the new password, and retype the new password. Click the **Set Password** button, as shown in [Figure 43: Change Password Screen](#).

abaco-a Change Password

Password complexity is being enforced. You must adhere to the following rules when setting your password.

1. Your new password must not contain your logon name or its mirror.
2. Your new password must be at least 8 characters in length.
3. Your new password must contain at least one number and at least one letter character.
4. Your new password must contain at least one of the following special punctuation characters: ?
., !, ., ,
5. Your new password must not contain three or more repeated alpha-numeric characters in a row.
6. Your new password must not contain three or more consecutive, ascending or descending alpha-numeric characters in a row.

Current password:

New password:

Retype new password:

Figure 43: Change Password Screen

With the ability to support many users comes the need for tighter security. The user interface addresses security concerns with various restrictions and controls. In many cases, the frequency or severity of these checks is configurable by the administrator at both a user specific and system-wide level.

Users are required to use a password to log in to the UI. The following rules govern passwords.

- *Complexity.* Passwords:
 - Must be at least eight characters in length
 - Must include at least one alpha character
 - Must include at least one numeric character
 - Must not contain three or more of the same alphanumeric character in a row
 - Must not contain three or more consecutive ascending or descending alphanumeric characters in a row
 - Must not contain the user account name or its reverse
 - Must contain at least one of the following special punctuation character: question mark (?), period (.), exclamation point (!), comma (,), or semi-colon(;
 - Must not use blank, null, or default passwords
- *Aging.* Users can be forced to change their passwords after a certain number of days. The administrator can set a maximum password age of up to 60 days as a default for the system. The administrator can also specify a different maximum password age for any individual user, if that is desired.
- *Force Change on Initial Login.* Users can be forced to change their password the first time that they log in. The administrator can assign a password to a user, either when the user is first created or when the password of an existing user is reset, and the user must change the password the first time that he/she logs in.
- *Password Reuse.* Users cannot reuse their last *N* passwords. *N* is a system-wide configurable number from 3 to 99, with the default of 5 (five).

Logout

The Logout menu selection allows the user to confirm logging out of the current session. This basic action is available to all users and is accessible from the main menu.

At logout, a message notifying that the current session will be terminated is displayed. Click the **Logout** button to complete the logout.

When logout is complete, the ELAP UI Login screen is displayed.

ELAP Messages

This section includes [Table 11: ELAP Error Messages](#). For alarm-related banner messages that appear on the UI browser screen in the Message Box described in [ELAP GUI Main Screen](#), refer to *Alarms and Maintenance* for ELAP for alarm recovery procedures.

ELAP Error Messages

[Table 11: ELAP Error Messages](#) lists all of the possible error codes and associated text that the ELAP user interface can generate. The <> fields indicate values that are different for each error; they are filled in at run time.

Table 11: ELAP Error Messages

E1000	Unknown error <error number>. No error text is available.
E1001	Invalid menu selection: <menu selection>
E1002	Invalid syntax: <input>
E1003	Mate ELAPs may not have the same designation.
E1004	ELAP software is running. You must stop the ELAP software before performing this operation.
E1005	ELAP software is not running. You must start the ELAP software before performing this operation.
E1006	Mate ELAP not available
E1007	Could not eject media: <device>
E1008	Could not read file: <file name>
E1009	Active PDBA is not available.
E1010	This host is not an ELAP.
E1011	Cannot find ELAP <A B> (host name <host name>)
E1012	Subscription (SP= <subscription number>) does not exist.
E1013	Subscription (SP= <subscription number>) already exists.
E1014	SP <identifier> does not exist.
E1015	IMSI <identifier> does not exist.

E1016	DN <identifier> does not exist.
E1017	PDBI error: <error text>
E1018	DN <identifier> already associated with IMSI <identifier>.
E1019	Device <device> unavailable.
E1020	Remote PDB unavailable.
E1021	IP address <address> is not authorized for PDB access.
E1022	RN <identifier> does not exist.
E1023	Invalid value for <prompt >: <value>. Valid values are <range>. Hit the Escape key to abort the command.
E1024	MTSU error: <error text>
E1025	File lock failed: <file name>
E1026	Environment variable <variable name> not defined.
E1027	ssh error: <error text>
E1028	IP address <IP address> is already authorized for PDBI access.
E1029	IP address <IP address> is not authorized for PDBI access.
E1030	Operation timed out waiting for a response from the PDBA.
E1031	Operation timed out waiting for a response from the RTDB.
E1032	Operation aborted by user.
E1033	Unexpected response received from the PDBA: id=<txid>, return code=<return code>
E1034	Unexpected response received from the RTDB: id=<txid>, return code=<return code>
E1035	Script <script name> failed: status=<status>
E1036	ELAP configuration failed. Please use the configuration menu to manually configure the ELAP sync and DSM networks.
E1037	One or more ELAP software processes did not start
E1038	One or more ELAP software processes did not stop
E1039	Transaction log query failed: <error text>
E1040	Transaction log response file was not created.
E1041	Transaction log response file could not be parsed.
E1042	Transaction log export failed: <error text>

E1043	The specified ELAP was not available.
E1044	Remote ELAP software is running. You must stop the remote ELAP software before performing this operation.
E1045	RTDB copy operation failed.
E1046	Improperly encoded alarm string. Re-check source.
E1047	RTDB did not respond to query.
E1048	Invalid response received from RTDB.
E1049	Could not connect to <i><device or process></i> : <i><error text></i>
E1050	Secure shell daemon is not running on mate ELAP. Config files could not be synchronized !!!
E1051	No feature(s) specified.
E1052	Both ELAP and EPAP features specified.
E1053	This action may only be performed on the local ELAP.
E1054	Another user is currently performing this same action.
E1055	Missing mandatory parameter: <i><parameter></i>
E1056	Unexpected parameter was provided: <i><parameter></i>
E1057	The ELAP must be in Forced Standby mode for this operation.
E1058	An internal error in the <i><parameter></i> occurred: <i><error text></i>
E1059	The passwords did not match.
E1060	The provisioning addresses for MPS A and B must be different.
E1061	The provisioning addresses for MPS A and B must be on the same network.
E1062	The default router must be on the same network as MPS A and MPS B.
E1063	The local and remote PDB addresses must be different.
E1064	This action may only be performed on ELAP A.
E1065	<i><device or process></i> must be configured.
E1066	The requested user <i><user></i> was not found.
E1067	The requested group <i><group></i> was not found.
E1068	The password entered was not correct.
E1069	The new password has been used too recently.

E1070	The provided password does not meet the security requirements. Reason: <i><reason text></i>
E1071	The specified group already exists.
E1072	This action may only be performed on ELAP B.
E1073	The file you have attempted to upload is larger than the <i><number></i> bytes of allocated storage space.
E1074	LPU batch failure: <i><error text></i>
E1075	This action must be done on the Active PDBA.
E1076	This action may only be performed while the LSMS connection is disabled.
E1077	File system violation: <i><error text></i>
E1078	File ' <i><file name></i> ' was empty
E1079	There are no PDBI connections available. Try again later.
E1080	The provisioning addresses for the main and backup networks must be different.
E1081	The specified IP already exists.
E1082	The specified IP does not exist.
E1083	The maximum number of authorized UI IPs has been reached.
E1084	This action may only performed on a provisionable MPS.
E1085	The specified address is local to this MPS.
E1086	PDBA has had a replication error.
E1087	The port number is already configured for another service.
E1088	Attempt to access the PDBA was not successful.
E1089	Duplicate entry the system <i><entry></i> already exists.
E1090	The <i><input></i> must be the same length.
E1091	The beginning <i><input></i> is past the ending.
E1092	The range would overlap the existing range <i><start range></i> to <i><end range></i> .
E1093	The <i><value></i> does not exist.
E1094	Must enable or disable both VIPs simultaneously.
E1095	Unable to perform requested operation because PDBA Proxy enabled.
E1096	<i><value></i> must not be configured for this action.

E1097	The maximum capacity for this provisioning has been reached.
E1098	Unable to establish SSH tunnel to <machine identifier> machine.
E1099	Invalid IP Address/Username/Password combination.
E1100	Task Scheduler error: <error text>.
E1101	Both the entered DSM IPs are same.
E1102	Loopback IP is same as Main/Backup DSM IP.
E1103	IP address <IP address> is not authorized to perform this action: <error text>
E1104	The localhost can not be removed from the access list.

Chapter 5

LNP Feature Activation

Topics:

- [*The LNP Solution.....98*](#)
- [*The LNP Feature.....98*](#)
- [*LNP-Related Features and Functions.....98*](#)

The second part of this manual describes the LNP feature, LNP-related features and functions, and LNP feature activation in the system.

The LNP Solution

With the LNP Solution, the EAGLE LNP subsystem can support from 24 million up to 384 million TNs on a single Service Module card. For ELAP 9.0 or higher, up to 18 Service Module cards can be installed in the EAGLE 5. The E5-SM4G cards and E5-SM8G-B cards provide increased processor capacity and improved performance that enables faster reload times and rates for download. DSM cards are not supported as Service Module cards with the EAGLE LNP subsystem.

At a high level, the LNP provisioning instructions are received and stored at the LSMS and distributed to the ELAP pair associated with an EAGLE 5. The ELAP provides persistent storage for the data and provides database update and data loading services for the EAGLE 5 LNP feature. The system is designed such that each Service Module card contains an exact image of the ELAP Real Time Database (RTDB). This enables the EAGLE 5 to support fast transaction rates for database lookup requests from the LIMs.

The LNP Feature

In the EAGLE 5 ISS, "the LNP feature" refers to any one of a collection of FAK-controlled LNP quantity features. Each feature represents a maximum number of Telephone Numbers (LNP ported TNs) that can be contained in the RTDB on the ELAP and the Service Module cards. Only one of the LNP quantity features can be "enabled" (operating) in the system at one time. When one of the LNP quantity features is enabled, the phrases "the LNP feature is enabled" or "the LNP feature is on" are used; quantity features are automatically turned on when they are enabled in the system.

The LNP feature will work only for ANSI messages. The LNP feature is not defined for ITU.

LNP-Related Features and Functions

The LNP feature is described in [LNP Feature Description](#).

The following LNP-related features and functions can be used with the LNP feature to provide the indicated processing:

- **LNP Short Message Service (LNP SMS) Feature**

LNP SMS is an additional service offered in the Message Relay function. The DPC/SSN for the Wireless Short Message Service Center (WSMSC) is provisioned in the subscription versions received from the NPAC through the LSMS.

Configuration of the WSMSC service, provisioning of default GTT for WSMSC, and provisioning of LRN Override GTT for WSMSC are not supported until the LNP SMS feature is on in the EAGLE 5 ISS. See [LNP Short Message Service \(LNP SMS\) Feature Configuration Procedure](#).

- **ITU TCAP LRM Query (LRNQT) Feature**

LRNQT provides support for an ITU TCAP LRN query/response using the LRN method in order to support Number Portability.

The LRNQT MSU Handler receives an incoming MSU, decodes the required data, and generates a response MSU based on decoded information and RTDB lookup. LRNQT handles ITU TCAP LRN query messages coming over ANSI links. The handler supports ANSI Class 0 SCCP UDT messages only. TCAP must be TC-BEGIN with Invoke component and the Local OpCode must be Provide Instructions – Start

- **TT Independence for LNP Queries Function**

With the TT Independence for LNP Queries function, the LNP subsystem is able to determine the protocol of the query based on other fields in the SS7 message, rather than relying on the TT value. This allows the same translation type to be used for multiple protocols, and allows a query between two networks to be handled properly.

The LNP service LNPQS defines the translation type used for LNP queries between networks. This service is defined with the `serv=lnpqs` parameter in the `chg-lnpopts` command. While the EAGLE 5 ISS allows any translation type to be assigned to the LNPQS service, it is recommended that translation type 11 is assigned to the LNPQS service.

- **Service Portability**

The Service Portability option allows splitting services between TN records and LRN override records. This allows the LNP craftsman to update LRN overrides for Message Relay services in the network, and the EAGLE 5 ISS will fall back to the NPCA subscription data (that is, TN gateway point code) for Message Relay services the CLEC wants to provide. When the option is turned off, if no LRN override services are provisioned, then the TN gateway point codes are used to route queries out of the network. If one or more LRN override services are provisioned, then the TN is considered to be ported into the network. In this case, if an LRN override service is requested and the LRN has other services administered, but the requested service is not provisioned, then a UDTs response for the service is provided. See [Changing LNP Options](#).

- **Triggerless Local Number Portability (TLNP) Feature**

The Triggerless LNP (TLNP) feature provides service providers a method to route calls to ported numbers without having to upgrade their signaling switch (End Office or Mobile Switching Center) software. In a trigger-based LNP solution, the service providers have to modify the End Office (EO) or Mobile Switching Center (MSC) to contain the LNP triggers. These triggers cause the EO or MSC to launch the query to the LNP database and route the call based on the returned location routing number (LRN).

The TLNP feature does not require any updates to the EO or MSC. Instead, the Initial Address Message (IAM) sent from the end office is intercepted by the Triggerless LNP feature on the EAGLE 5 ISS and converted to include the LRN if the call is to a ported number.

The Gateway Screening feature is used to capture the IAM messages that are converted for the TLNP feature. The database must contain a gateway screening screen set that contains the following items:

- An allowed SIO screen that allows ISUP messages into the EAGLE 5 ISS. ISUP messages are MSUs that contain the value 5 in the Service Indicator field (SI=5) of the Service Information Octet (SIO) of the MSU.
- The gateway screening stop action `tlnp`. The gateway screening stop actions can be verified with the `rtrv-gws-actset` command.

Note: When Gateway Screening is in the screen test mode, as defined by the linkset parameters `gwsa=off` and `gwsn=on`, the gateway screening action in the gateway screening stop action set

specified by the actname parameter of the gateway screening screen set at the end of the gateway screening process will be performed.

- **Wireless Local Number Portability (WNP) Feature**

WNP allows completion of a call to a ported wire-line number. The WNP feature or the PLNP feature must be on before some of the LNP configuration options can be provisioned. See [Changing LNP Options](#).

- **PCS (Personal Communication Service) 1900 Number Portability (PLNP) Feature**

PLNP provides for LNP query/response in a PCS wireless environment using the LRN method to support Service Provider Number Portability. The WNP feature or the PLNP feature must be on before some of the LNP configuration options can be provisioned. See [Changing LNP Options](#).

- **Automatic Call Gapping (ACG)**

When a node overload condition is detected and an ACG control is configured for that overload level, the EAGLE 5 ISS sends an ACG component within each LRN query response it processes. The ACG control is invoked for the first 6 or 10 digits of the called party address in all queries sent to the EAGLE 5 ISS to control the rate that queries are processed.

If no overload control is in place, LRNQT sends an ACG for a manually initiated control to block queries. Manually initiated control procedures are similar to overload control procedures, but can vary the number of digits that are to be placed under control (3 or 6-10 digits).

[Automatic Call Gapping \(ACG\) Configuration](#) describes the use of ACG.

Chapter 6

LNP Feature Description

Topics:

- [*LNP Message Relay.....102*](#)
- [*LNP Query Service \(LNPQS\).....110*](#)
- [*The LNP Local Subsystem.....120*](#)
- [*Hardware, System, and Feature Requirements.122*](#)

This chapter describes the Local Number Portability (LNP) feature and the LNP services used for Query and Message Relay.

LNP Message Relay

LNP MR performs Enhanced GTT routing to perform 10-digit LNP GTT. It includes the ability to decode the TCAP portion of the message to determine the 10-digit Called Party Number for the supported services.

LNP Message Relay (LNP MR) performs the following functions:

- Extraction of the 10-digit dialed number from the TCAP portion of the message – If the MSU contains a 6-digit Called Party Address, Message Relay gets the 10-digit Dialed Number (DN) from the TCAP portion of the MSU.
- Increased number of translations – For each 10-digit Dialed Number, up to 6 translations are available. The previous limit was 270,000 total translations. The number of Dialed Numbers that can be entered depends on the hardware. The minimum hardware configuration supports 500,000 Dialed Numbers; 3 million translations can be entered on the minimum hardware configuration. The maximum hardware configuration supports 2 million Dialed Numbers; 12 million Message Relay translations can be entered on the maximum hardware configuration.
- Replacement of the Global Title Address – Message Relay provides the option of replacing the Global Title Address in the Called Party Address with the Location Routing Number (LRN) associated with the ported Dialed Number.

Message Relay is performed in the following stages:

1. The message arrives at the EAGLE 5 ISS as Route-on-GT. The EAGLE 5 ISS performs 6-digit (NPANXX) translation. The result of this translation indicates if Message Relay is required. If it is required, the result of this translation also gives the default data that may be used in stage 3.
2. If stage 1 indicates that Message Relay is required, the EAGLE 5 ISS performs 10-digit message relay. If the 10-digit number is found, the translation data for the 10-digit number is used to route the message.
3. If the 10-digit number is found and the number has an LRN assigned to it, the EAGLE 5 ISS checks for Message Relay override data. If there is override data for the LRN, the EAGLE 5 ISS uses this override data to route the message.
4. If no location routing number is assigned, or the location routing number does not have override data, the EAGLE 5 ISS uses the data assigned to the 10-digit number.
5. If the LRN has override data but not for the requested translation type or service, and the Service Portability option is on (shown in the SERVPORT parameter value in the LNPOPTS table), then the EAGLE 5 ISS uses the data assigned to the 10-digit number. If the Service Portability option is not on, then the message is discarded and UIM and UDTs messages are generated.
6. If no data is assigned to the 10-digit number, and the Service Portability option is on, then the EAGLE 5 ISS uses the default data from stage 1 to route the message. If the Service Portability option is not on, then the message is discarded and UIM and UDTs messages are generated.
7. If the 10-digit number is not found, the Dialed Number is not ported and the default data from stage 1 is used to route the message.

It's possible that Message Relay is required, but no default data exists for the NPANXX. This is because EAGLE 5 ISS creates an NPANXX entry when the NPAC sends down a ported subscriber record for a nonported NPANXX. Normally, data is provisioned in the following order:

1. The NPANXX default data is entered.
2. The NPANXX is marked as portable (the value of the mr parameter is yes).
3. The NPAC sends down information for ported subscribers in the portable NPANXX.

However, it is possible that step 3 can occur before step 1. In this case, if a message arrives for the ported subscriber, the EAGLE 5 ISS routes the message according to the subscriber data entered by the NPAC.

- The 10-digit number is found in the subscription record. The LRN has a matching entry in the override table. If override data exists for the requested service, the LRN override Global Title Translation is used. If LRN override data exists, but not for the requested translation type, and the Service Portability option is not on, then the result is no translation, the message is discarded, and UIM and UDS messages are generated. If the Service Portability option is on, then the NPAC Global Title Translation data is used.
- The 10-digit number is found in the subscription record. The LRN does not have a matching entry in the override table. If NPAC Global Title Translation data exists, the NPAC Global Title Translation is used. If NPAC Global Title Translation data does not exist for the 10-digit number, and the Service Portability option is not on, then the result is no translation, the message is discarded, and UIM and UDS messages are generated. If the Service Portability option is on, then the NPANXX Global Title Translation data is used.

If a message arrives for a nonported subscriber in that NPANXX, and normal Global Title Translation information is defined for the message, the message is routed using the normal Global Title Translation data. But if a message arrives for a nonported subscriber in that NPANXX, and no normal Global Title Translation information is defined for the message, the message is discarded, and UIM and UDS messages are generated.

[Table 12: LNP Message Relay](#) shows the result of the 10-digit Message Relay processing, and the processing required to route a message.

Table 12: LNP Message Relay

Ported MR NPANXX	Ported TN	LNP Message Relay Processing	NPAC GTT Data for any Service
No	No	Nonported subscriber. See Table 14: LNP Message Relay - Nonported Subscribers .	N/A
No (See Note).	Yes	Ported subscriber.	Yes - See Table 13: LNP Message Relay - Ported Subscribers .
			No - See Table 14: LNP Message Relay - Nonported Subscribers .
Yes	No	Nonported subscriber. See Table 14: LNP Message Relay - Nonported Subscribers .	N/A

Ported MR NPANXX	Ported TN	LNP Message Relay Processing	NPAC GTT Data for any Service
Yes	Yes	Ported subscriber.	Yes - See Table 13: LNP Message Relay - Ported Subscribers .
			No - See Table 14: LNP Message Relay - Nonported Subscribers .
Ported MR NPANXX - An MR NPANXX that is marked portable			
Ported TN - A subscription record that is found for a 10-digit number, the location routing number is assigned or NPAC global title translation data is defined for service (translation type).			
Note: The EAGLE 5 ISS creates an NPANXX entry, if none exists, when it receives a ported subscriber record.			

[Table 13: LNP Message Relay - Ported Subscribers](#) lists possible combinations for NPAC and override Global Title Translation data provisioning, and the resulting action of Message Relay for ported subscribers. Message Relay data exists for the 10-digit number and service.

Table 13: LNP Message Relay - Ported Subscribers

TN GTT DATA defined for 10-Digit Number and Service (TT)	LRN Override GTT DATA defined for 10-Digit Number and Service (TT)	LRN Override GTT DATA defined for 10-Digit Number	Service Portability	LNP Message Relay Action
No	No	No See Note 1.	No	The message is discarded. The “No Translation Available” UIM and UDTS messages are generated if return on error is set.
No	No	No See Note 1.	Yes	The message is routed using NPANXX or normal Global Title Translation data. See Table 14: LNP Message Relay - Nonported Subscribers .
No	Yes	N/A	N/A	The message is routed using the LRN override Global Title Translation data.
No	N/A	Yes See Note 2.	No	The message is discarded. The “No Translation Available” UIM and UDTS messages are generated if return on error set.

TN GTT DATA defined for 10-Digit Number and Service (TT)	LRN Override GTT DATA defined for 10-Digit Number and Service (TT)	LRN Override GTT DATA defined for 10-Digit Number	Service Portability	LNP Message Relay Action
No	N/A	Yes See Note 2.	Yes	The message is routed using NPANXX or normal Global Title Translation data. See Table 14: LNP Message Relay - Nonported Subscribers .
Yes	No	No See Note 1.	N/A	The message is routed using the NPAC Global Title Translation data.
Yes	Yes	N/A	N/A	The message is routed using the LRN override Global Title Translation data.
Yes	N/A	Yes See Note 2.	Yes	The message is routed using the NPAC Global Title Translation data.
Yes	N/A	Yes See Note 2.	No	The message is discarded, The “No Translation Available” UIM and UDTS messages are generated if return on error set.
Notes: 1. The 10-digit number has an LRN assigned, but the LRN has no matching entry in the override table. 2. The 10-digit number has an LRN override Global Title Translation data assigned, but not for the requested service (translation type).				

[Table 14: LNP Message Relay - Nonported Subscribers](#) lists possible combinations for traditional and LNP default Global Title Translation data provisioning and the resulting action of Message Relay for nonported subscribers. The Message Relay data does not exist for the 10-digit number and service.

Table 14: LNP Message Relay - Nonported Subscribers

Traditional (Non-LNP) GTT DATA defined for Service (TT)	LNP 6-digit Default GTT DATA defined for Service (TT)	LNP Message Relay Action
No	No See Note.	The message is discarded. The “No Translation Available” UIM and UDTS messages are generated if return on error is set.

Traditional (Non-LNP) GTT DATA defined for Service (TT)	LNP 6-digit Default GTT DATA defined for Service (TT)	LNP Message Relay Action
No	Yes	The message is routed using the LNP 6-digit default Global Title Translation data.
Yes	No See Note.	The message is routed using the traditional (non-LNP) Global Title Translation data.
Yes	Yes	The message is routed using the LNP 6-digit default global title translation data.
Note: Either the 6-digit default Global Title Translation data is not present (the NPANXX entry is created when the NPAC sends down a ported subscriber record for a nonported NPANXX), the NPANXX is not ported, or the LNP 6-digit default Global Title Translation data present but not for requested LNP service (translation type).		

Figure 44: Message Flow For Global Title Translation and Message Relay shows how normal Global Title Translation and Message Relay are performed on EAGLE 5 ISS.

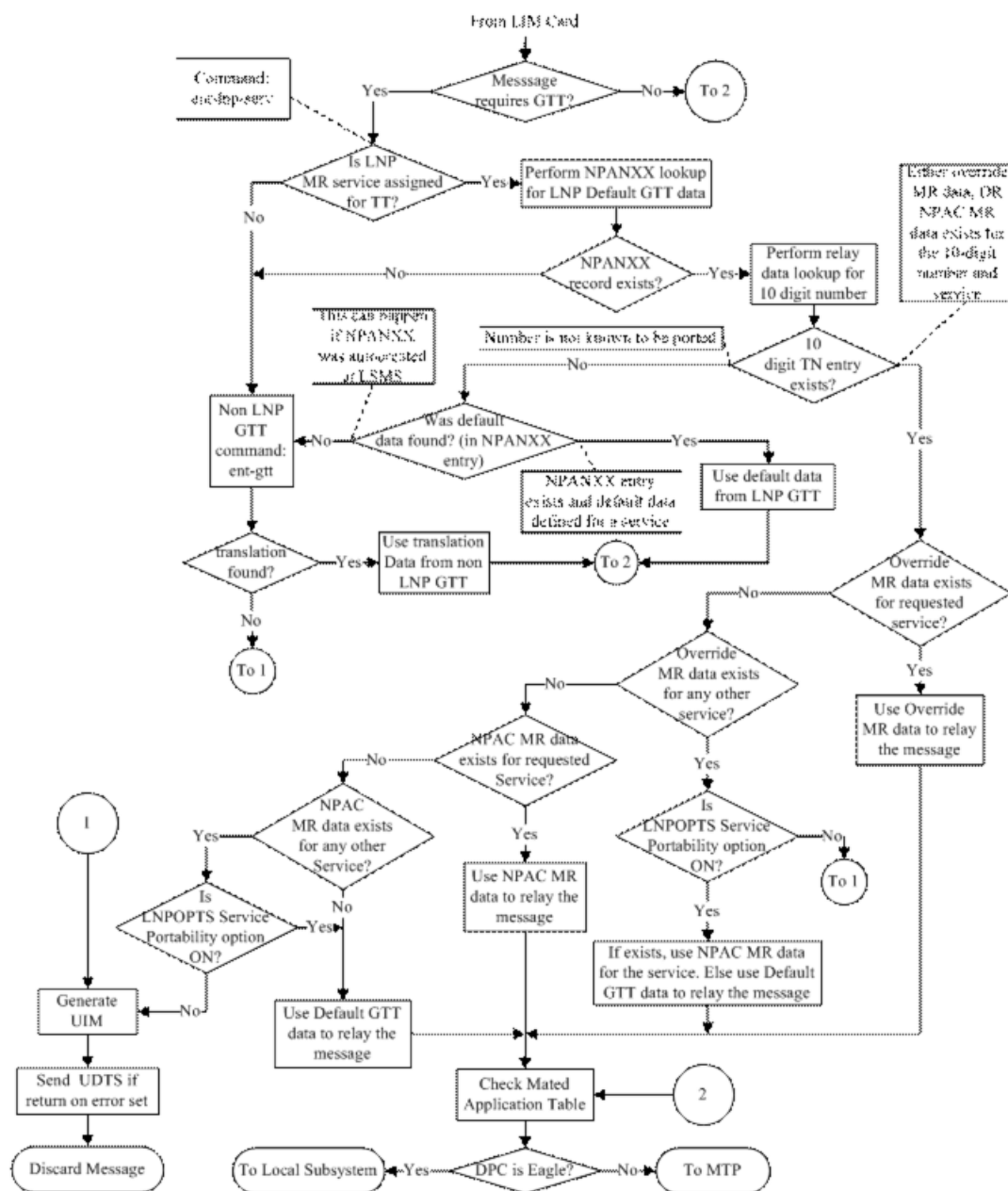


Figure 44: Message Flow For Global Title Translation and Message Relay

Fall-back to GTT Processing after LNP MR Service

The Fall-back to GTT after LNP MR Service function provides a generic mechanism to perform GTT on an LNP Message Relayed MSU in order to determine the alternative database node for optimal routing, after the message is updated with relay data (NPANXX, TN or LRN MR data) from an LNP MR service RTDB lookup. The function is available for the LIDB, CLASS, CNAM, ISVM and WSMSC LNP Message Relay services.

Configuration options in the LNP Service Table control the operation of the Fall-back to GTT after LNP MR processing. The options can be provisioned for both True TT and Alias TT for any of the LNP MR services. The configuration options are not used in standard Fall through to GTT message processing for LNP MSUs that are not relayed. The EGTT feature must be turned on to provision the following options:

- GTT Required
 - Examined after the successful execution of LNP MR service RTDB lookup, to determine whether GTT needs to be performed on the LNP Message Relayed MSU.
 - If the LNP MR service processing requires the message to be relayed and the GTT Required option is OFF, then standard routing is performed for the LNP Message Relayed MSU.
 - If the LNP MR service processing requires the message to be relayed and the GTT Required option is ON, then the GTT Selector ID from the selected LNP Service table entry is used to perform GTT on the LNP Relayed MSU. The GTT Hierarchy provisioned for the incoming linkset is used to perform GTT on the LNP Relayed MSU.
- GTT Selector ID
 - Used as the Selector ID for a GTT Selector search, to perform GTT when the Fall-back to GTT after LNP MR Service function is invoked for the LNP Message Relayed message.
 - Used to find a matching translation.
- Default Action

Action taken when a GTT selector search (using the GTT Selector ID from the LNP Service table entry) fails while performing Fall-back to GTT after LNP MR Service processing.

 - Fall through GTT
 - Discard GTT Action ID
 - UDTs GTT Action ID
 - TCAP Error GTT Action ID
 - Fall-back (Route MSU based on MR data from RTDB)

Successful LNP MR service processing means that any of the following data is found in the RTDB:

- Default GTT data from an NPANXX entry
- Subscription MR data from a TN entry
- Override data from an LRN entry

When LNP MR service processing is successful, the GTT Required configuration option value in the selected LNP Service table entry is examined to determine whether GTT needs to be performed on the LNP Message Relayed MSU.

- If the LNP MR service processing requires the message to be relayed and the GTT Required option is OFF, then standard routing is performed for the LNP Message Relayed MSU.
- If the LNP MR service processing requires the message to be relayed and the GTT Required option is ON, then the GTT Selector ID from the selected LNP Service table entry is used to perform GTT

on the LNP Message Relayed MSU. The GTT Hierarchy provisioned for the incoming linkset is used to perform GTT on the LNP Message Relayed MSU.

If the GTT selector search finds a matching GTT translation, and

- If the matching GTT translation contains routing data (XLAT is not NONE), then the GTT data is applied to the MSU in addition to the relay data from the RTDB.
- If the matching GTT translation does not contain routing data (XLAT=NONE), then the MSU continues to use the relay data from the RTDB.
- If the matching GTT translation contains Cancel GT data, then Cancel GT data is applied according to standard GT Modification processing.
- If the Final GTT Loadsharing (FGTTLS) feature is ON, the GTT translation entry for the LNP Message Relayed message has XLAT=NONE, the message CdPA RI is RT-on-GT, and an MRNSET is provisioned for the GTT translation, loadsharing is performed using the provisioned MRNSET.
- If the FGTTLS feature is OFF, the GTT translation has XLAT=NONE, the message CdPA RI is RT-on-SSN, and a MAPSET is provisioned for the GTT translation, loadsharing can be performed using the provisioned MAPSET.
- If the GTT translation has XLAT=NONE, only the IGTTLS feature is ON, and the message CdPA RI is RT-on-GT, loadsharing can be performed using the default MRNSET.
- If the message CdPA RI is RT-on-SSN and the EPAP translated PC/SSN combination is not present in the provisioned MAPSET, then UIM 1195 is generated and the message is discarded.
- If the message CdPA RI is RT-on-GT and the EPAP translated PC is not present in the provisioned non-default MRNSET, then UIM 1444 is generated with the EPAP translated date and the message is routed without loadsharing.
- If a GTT Action Set is associated with the matched translation, then appropriate GTT Actions functions and data are applied to the MSU (refer to the GTT Actions descriptions in the *Database Administration Manual - GTT*). A GTT Action ID (of type Discard, UDTs or TCAP Error) can be configured as the Default Action option value only if the GTT Action – Discard feature is turned ON.
- If applicable, SCCP Conversion is applied.
- Standard GTT message routing is performed on routed messages.

If the GTT selector search to find the matching translation fails while performing GTT on the LNP Message Relayed MSU, then one of the following actions is taken based on the value of the Default Action option in the corresponding LNP Service table entry:

- For Discard GTT Action ID, the message is discarded, and a UIM is generated if a request is provisioned in the database.
- For UDTs GTT Action ID, the message is discarded, a UDTs/XUDTs message is returned with a provisioned or default (Unqualified) error code, and a UIM is generated if a request is provisioned in the database.
- For TCAP Error GTT Action ID, the message is discarded, a reject message is generated to the originator with a provisioned or default (0) ANSI/ITU error code, and a UIM is generated if a request is provisioned in the database.

- For FALL BACK, the message is relayed on the basis of the relay data from the RTDB.
- For FALL THROUGH GTT, the GTT Selector ID value in the corresponding LNP Service table entry is examined:
 - If the GTT Selector ID value is not NONE, then GTT is attempted again with GTT selector ID=NONE.

If GTT is successful, the MSU is routed based on translation data.

If a subsequent error occurs, existing GTT error handling is performed.
 - If the GTT Selector ID is NONE, then subsequent GTT lookup is not needed because a GTT selector search with GTT Selector ID=NONE has already been attempted. The message is discarded, and UIM 1042 “SCCP rcvd inv Cld Party - bad Selectors” or UIM 1191 “SCCP rcvd inv Clg Party - bad Selectors” is generated depending on the GTT Hierarchy provisioned for the incoming linkset.

If Fall-back to GTT after LNP MR Service processing for the LNP Message Relayed MSU fails due to any reason other than GTT selector search failure, then standard GTT error handling is performed.

LNP Query Service (LNPQS)

All the LNP query messages for call connection to ported DN received by the EAGLE 5 ISS are processed by LNPQS. LNPQS receives queries from the subsystem management task.

LNPQS performs the following functions:

1. Query verification

All Queries are verified to conform to encoding rules. If query does not conform to encoding standard, it is considered an invalid query and either it is discarded or a TCAP error response is generated.

2. Query decoding

The Dialed Number (DN) is decoded from the query. The DN is used to search for a provisioned LRN.

3. Response generation

A response message encoded with a DN, an LRN, or both, to be sent back to the generator of the query.

LNP Query is performed in the following stages:

1. The message arrives at the EAGLE 5 ISS, which performs 6 digit (NPANXX) translation on the 10-digit DN. The result of this translation indicates if local AIN/IN data is to be used.
 - If so, the data is inherited from the local LNP subsystem and Site ID True Point Code (SID and SS_APPL tables).
 - Otherwise, continue to stage 2.

2. If stage 1 does not indicate local AIN or IN data is to be used, the EAGLE 5 ISS looks for default AIN/IN data in the NPANXX record.
 - If the data is found (point code and subsystem), it is used.
 - Otherwise, continue to stage 3.
3. If stage 2 does not result in default AIN/IN data, the EAGLE 5 ISS performs a non-LNP Global Title Translation to obtain the requested AIN/IN data.

If the EAGLE 5 ISS fails Global Title Translation in stage 3, or SID and local subsystem data has not been administered in stage 1, a UIM is generated and the message is discarded.

Pre-LNP Query Service GTT Processing

The Pre-LNP Query Service GTT Processing function provides a generic mechanism to perform GTT on the messages destined for LNP Query services, before the message could be processed by the LNP local subsystem. Performing GTT before local subsystem processing is done in order to determine whether the originator of the query has an agreement with the LNP service provider to perform RTDB lookup. If there is an agreement with the LNP service provider, the LNP Query service processing is performed and an appropriate response is sent to the originator. Otherwise, the query is routed as indicated by the GTT translation result. The Pre-LNP Query Service GTT Processing function is available for the AIN, IN, LRNQT, LNPQS, PCS and WNP LNP Query services.

Configuration options in the LNP Service Table control the operation of the Pre-LNP Query Service GTT processing. The options can be provisioned for both True TT and Alias TT for any of the LNP Query services. The EGTT feature must be turned on to provision the following options:

- GTT Required
 - Indicates whether GTT needs to be performed on an LNP Query Service message before performing an RTDB lookup in LNP service processing.
 - If GTT Required is ON, then the GTT Selector ID that is provisioned in the LNP Service table entry is used as the Selector ID to perform GTT on the LNP Query Service message, based on the GTT Hierarchy provisioned for the incoming linkset of the message.
 - If GTT Required is OFF, the LNP Query Service message is routed with standard processing for the service.
- .GTT Selector ID
 - Used to perform GTT before the LNP Query service processing occurs.
 - The GTT Selector ID from the LNP Service table entry is used as the Selector ID in the GTT selector search to find only the first GTT set. If a further GTT selector search is required (when the matching GTT translation entry is provisioned with CdSelID or CgSelID), then the GTT selector ID found from the previously matched GTT translation entry is used.
 - The GTT selector ID from the LNP Service table entry is not used while performing GTT as a part of Fall through to GTT message processing.
- Default Action

- Action taken when the GTT selector search (using the GTT Selector ID from the LNP Service table entry) fails to find the matching translation while performing Pre-LNP Query Service GTT processing.
 - Fall-back (Send MSU to LNP local subsystem)
 - Fall through GTT
 - Discard GTT Action ID
 - UDTS GTT Action ID
 - TCAP Error GTT Action ID

When the GTT Required option in the selected LNP Service table entry is ON, then the GTT Selector ID provisioned in corresponding LNP Service Table entry shall be used to perform GTT on an LNP Query Service message, based on the GTT Hierarchy configured for the incoming linkset of the message.

- AIN and LRNQT services

NPANXX lookup is performed. If the AIN flag in the NPANXX entry is ON, then the GTT Required option value of the selected LNP Service table entry is examined.

If the GTT Required option is ON, then, before LNP Query service processing is performed, the provisioned GTT Selector ID is used to perform GTT on the LNP Query message.

If the GTT Required option is OFF, then standard LNP Query service processing is performed for the message.

- IN service

NPANXX lookup is performed. If the local IN flag in the NPANXX entry is ON, then the GTT Required option value of the selected LNP Service table entry is examined. If the GTT Required option is OFF, then existing LNP Query service processing is performed for the message.

If the GTT Required option is ON, then the provisioned GTT Selector ID is used to perform GTT on the LNP Query message.

If the GTT Required option is OFF, then existing LNP Query service processing is performed for the message.

- WNP and PCS services

If the LNP WQREDRCT configuration option in the LNPOPTS table is OFF, the GTT Required option in the selected LNP Service table entry is examined.

If the GTT Required option is ON, then then GTT is performed on the message using the GTT Selector ID provisioned in the corresponding LNP Service table entry.

If the GTT Required option is OFF, then the message is forwarded to the EAGLE 5 ISS LNP local subsystem.

If the LNP WQREDRCT option in the LNPOPTS table is ON, then the message falls through to GTT, irrespective of the GTT Required option value in the selected LNP Service table entry.

- LNPQS service

If the selected LNP Service table entry refers to the LNPQS service, then the TT Independence for LNP Queries function analyzes the TCAP portion of the LNP Query message to determine the service type to be applied (which can be AIN, IN, or WNP).

If the type of service is successfully determined, then Pre-LNP Query Service GTT processing is performed for the message for the service type.

If the type of service cannot be determined, then standard LNP Query message processing is performed.

If a valid translation is found in Pre-LNP Query Service GTT processing, then translation data, GTMOD data, SCCP Conversion, and GTT Actions, if any are applicable, are applied and message routing is performed according to standard GTT processing.

Note: If the GTT translation found as result of the Pre-LNP Query Service GTT processing has XLAT=NONE configured, then XLAT=NONE processing for GTT is used to process the MSU.

If the GTT selector search fails to find the matching translation while performing Pre-LNP Query Service GTT processing, then one of the following actions is taken based on the value of the Default Action option in the corresponding LNP Service table entry:

- For Discard GTT Action ID, the message is discarded and a UIM will be generated if a request is provisioned in the database.

For UDTs GTT Action ID, the message is discarded, a UDTs/XUDTs message is returned with a provisioned or default (Unqualified) error code, and a UIM is generated if a request is provisioned in the database.

For TCAP Error GTT Action ID, the message is discarded, a reject message is generated to the originator with a provisioned or default (0) ANSI/ITU error code, and a UIM is generated if a request is provisioned in the database.

For FALL BACK, the message is forwarded to the LNP local subsystem for LNP Query service processing.

For FALL THROUGH GTT, the GTT Selector ID value in the corresponding LNP Service table entry is examined:

- If the GTT Selector ID value is not NONE, then GTT is attempted again with GTT Selector ID=NONE.

If GTT is successful, the message is routed based on GTT translation data.

If a subsequent error occurs, standard GTT error handling is performed.

- If 'GTT Selector ID' is NONE, then subsequent GTT lookup is not needed because GTT selector search with GTT Selector ID=NONE has already been attempted.

The message is discarded, and UIM 1042 "SCCP rcvd inv Cld Party - bad Selectors" or UIM 1191 "SCCP rcvd inv Clg Party - bad Selectors" is generated depending on the GTT Hierarchy provisioned for the incoming linkset.

If Pre-LNP Query Service GTT processing on the LNP Relayed MSU fails due to any reason other than GTT selector search failure, then standard GTT error handling is performed.

LNP Query Processing

LNP queries are processed as described in [Figure 45: LNP Query Processing](#).

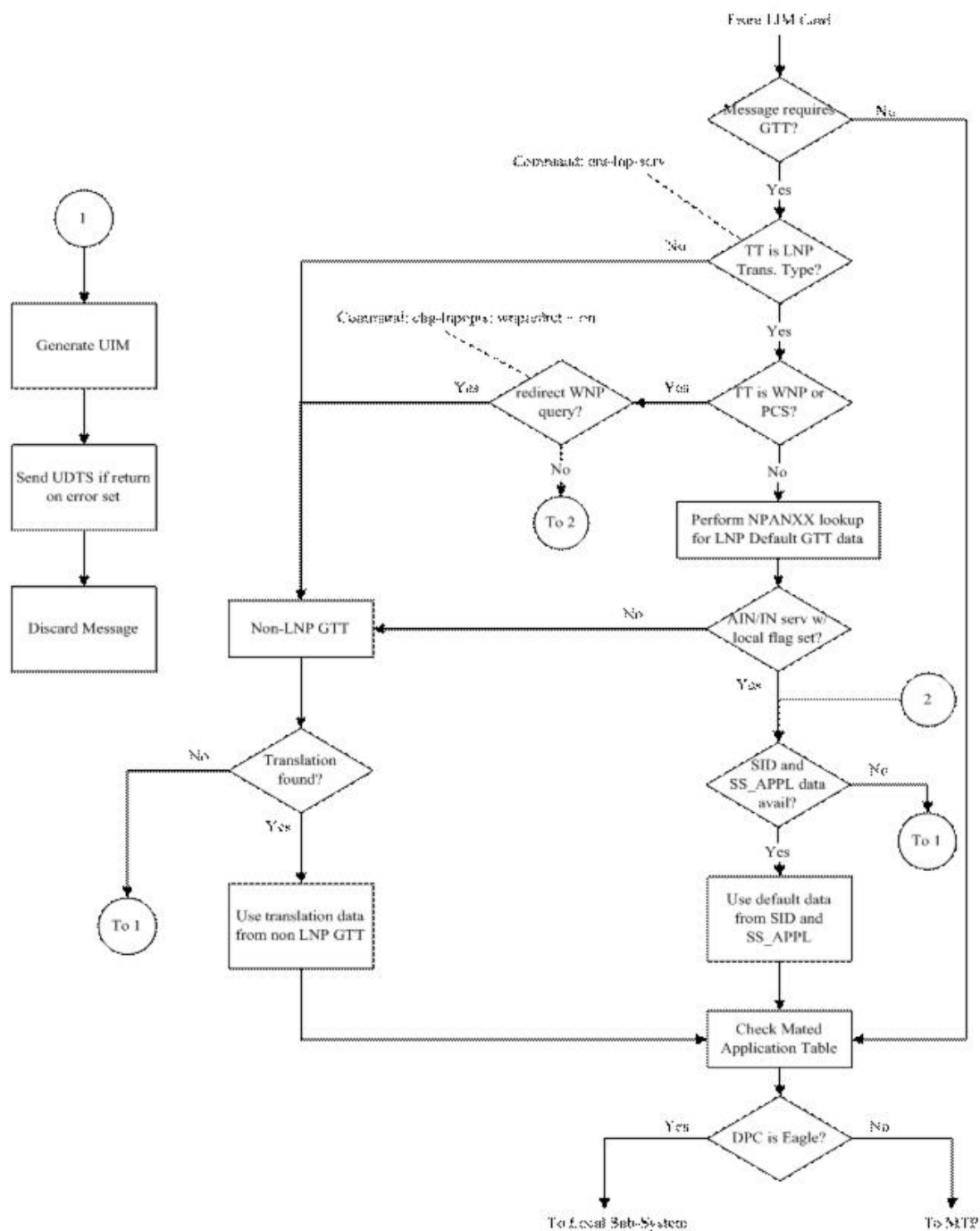


Figure 45: LNP Query Processing

When an LNP query arrives at the EAGLE 5 ISS with the LNPQS service translation type, the EAGLE 5 ISS partially decodes the TCAP portion of the query. After the TCAP portion of the query is decoded down to the OPCODE, and the Package type, TCAP Transaction ID, and Component parameters are verified, the OPCODE TAG, OPCODE FAMILY, and OPCODE SPEC parameters are examined to determine the LNP service required to process the query. There are four basic types of queries: AIN,

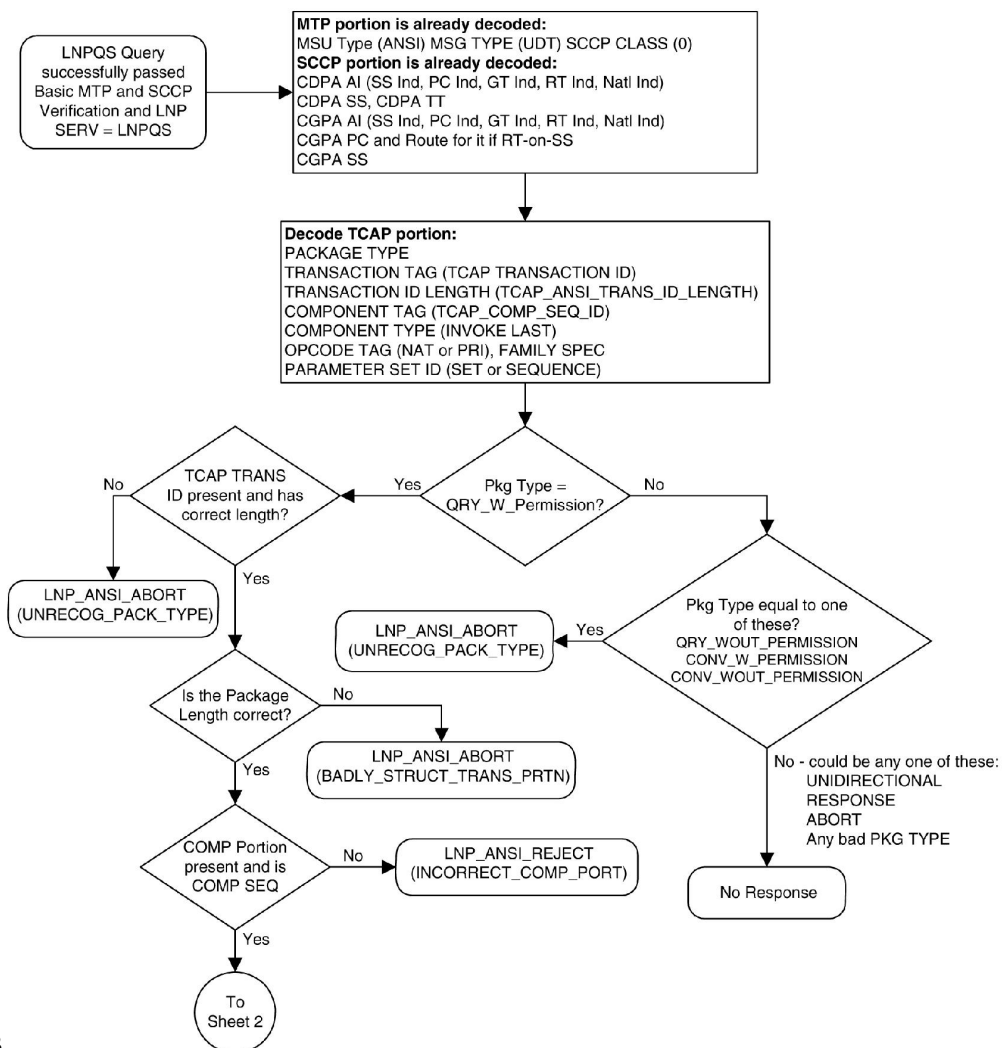
IN, PCS, and WNP. [Table 15: LNP Query OPCODE Values](#) shows the OPCODE values for the query types.

Table 15: LNP Query OPCODE Values

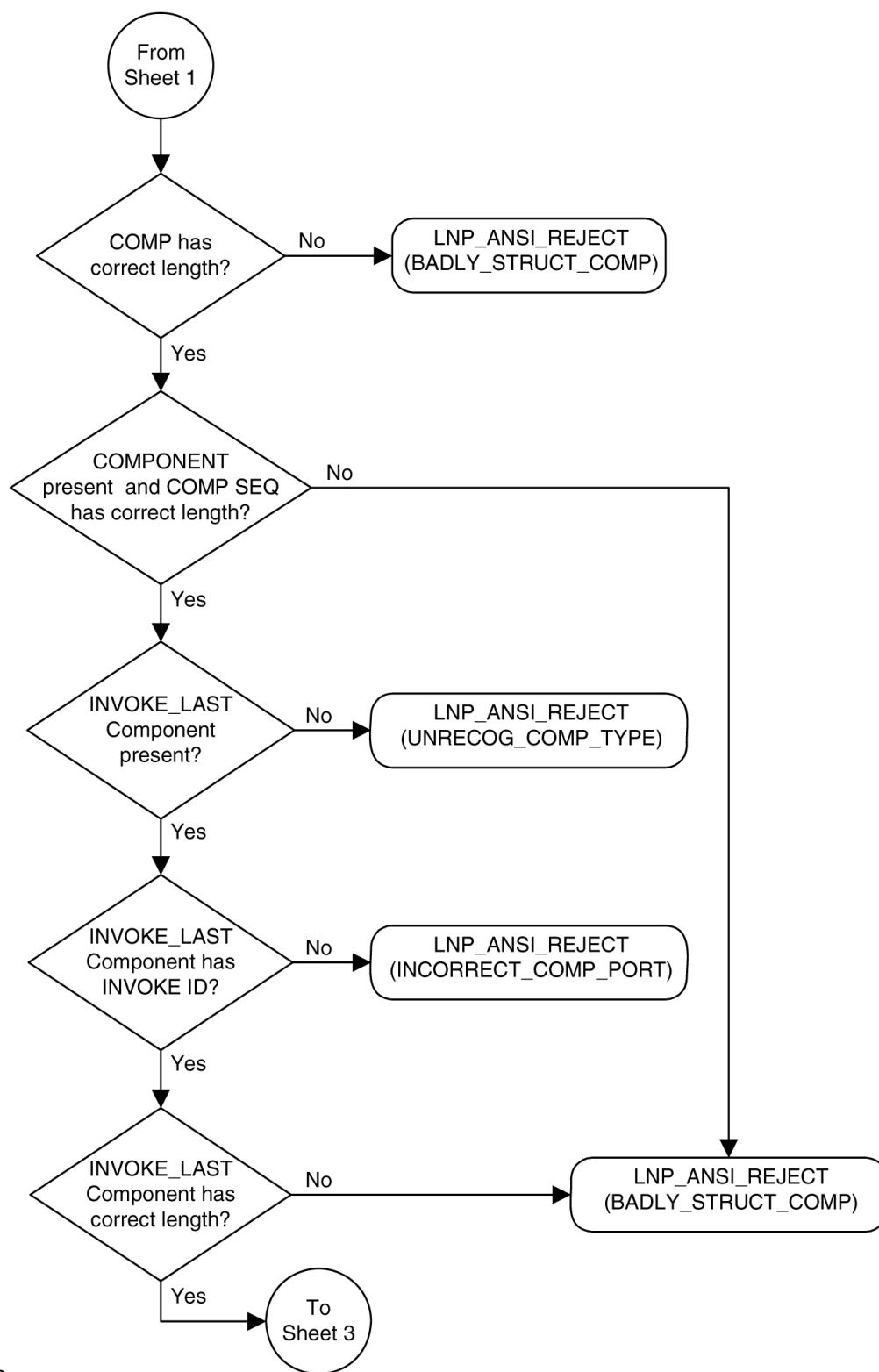
Query Type	OPCODE TAG Value	OPCODE FAMILY Value	OPCODE SPEC Value
AIN	PRI	REQUEST INSTRUCT	INFO ANALYZED
IN	NAT	PROVIDE INSTRUCTION	IN START
PCS	NAT	PROVIDE INSTRUCTION	IN START
WNP	PRI	IS41 OP FAMILY	IN IS41 NUM PORT REQ

After the OPCODE values are determined, the query is treated by the EAGLE 5 ISS as either an AIN, IN, or WNP query. Since IN and PCS queries use the same OPCODE values, PCS queries are treated as IN queries. If a query is received at the EAGLE 5 ISS containing the specific PCS translation type, the query is treated as a PCS query.

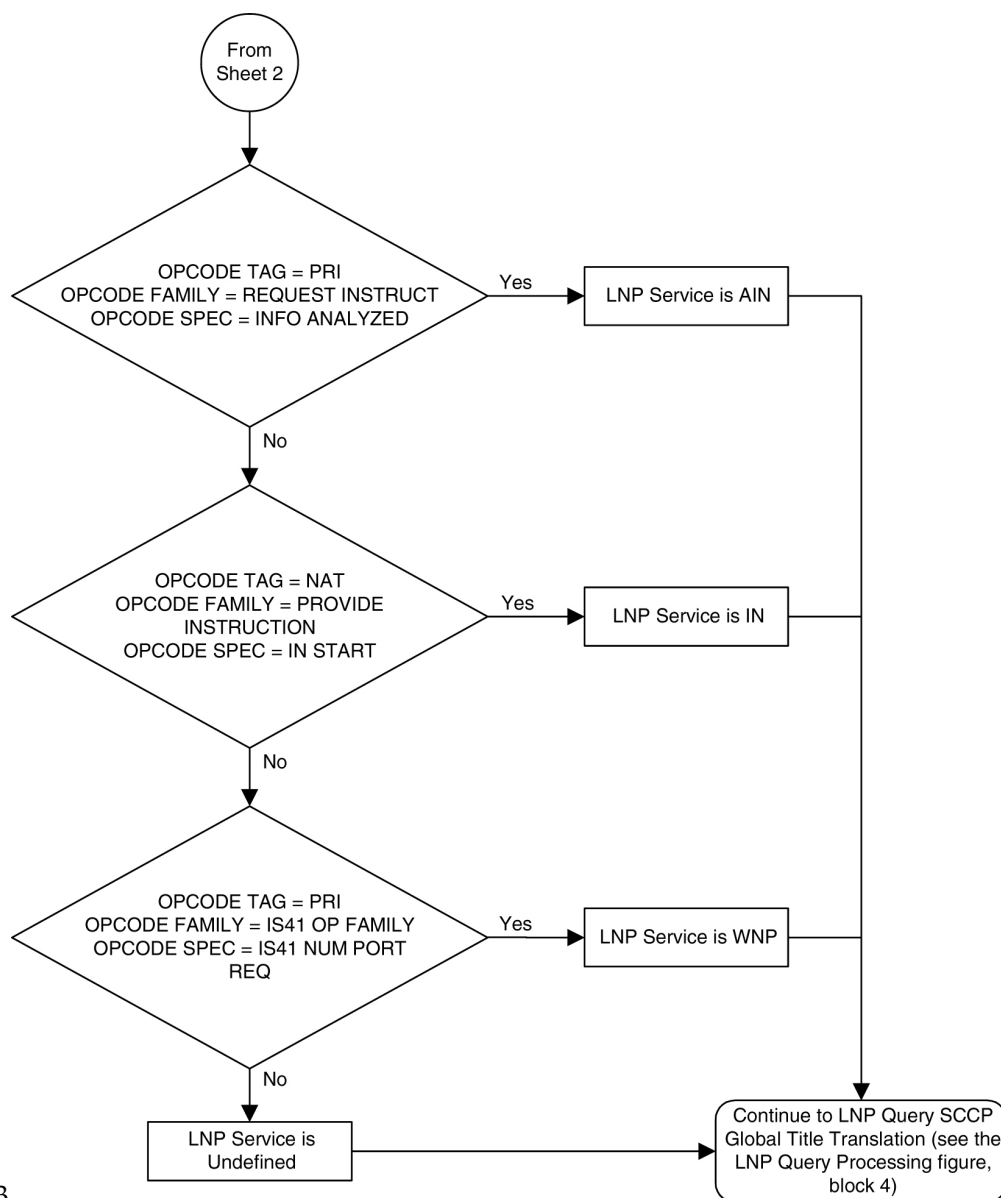
[Figure 46: LNP Service Determination Process](#) shows the LNP service determination process for queries containing the LNPQS translation type.



Sheet 1 of 3



Sheet 2 of 3



Sheet 3 of 3

Figure 46: LNP Service Determination Process

The translation type in the query message is used to determine the type of LNP query (AIN, IN, WNP, or PCS) for correct decoding and response formulation.

LNP queries between networks are defined to use translation type 11, regardless of the protocol used. Also, there are other cases where the TT alone may not be enough to determine the type of protocol being used, thus making it impossible to correctly decode all queries. See [Figure 47: Inter-Network Support for LNP Queries](#).

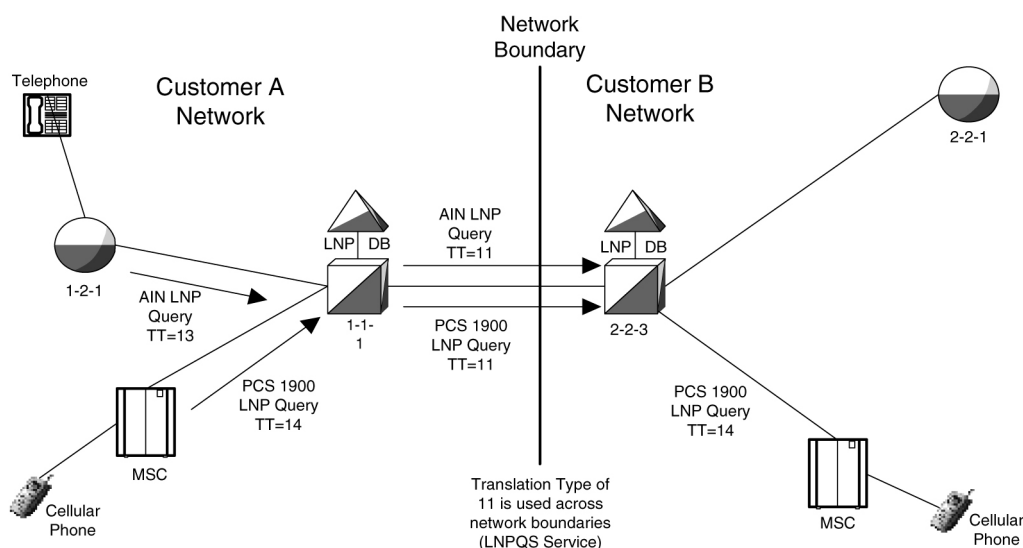


Figure 47: Inter-Network Support for LNP Queries

In this example, Network B would not be able to differentiate between the two types of LNP queries received from Network A.

The TT Independence for LNP Queries function addresses this issue by providing a method of protocol determination of an incoming query.

With the TT Independence for LNP Queries function, the LNP subsystem is able to determine the protocol of the query based on other fields in the SS7 message, rather than relying on the TT value. This allows the same translation type to be used for multiple protocols, and allows a query between two networks to be handled properly.

Note: TT independence for LNP Queries is not supported for ITU TCAP LRN (LRNQT) queries.

The LNP service LNPQS defines the translation type used for LNP queries between networks. This service is defined with the `serv=lnpqs` parameter in the `chg-lnpopts` command. While the EAGLE 5 ISS allows any translation type to be assigned to the LNPQS service, it is recommended that translation type 11 is assigned to the LNPQS service.

Limitations

PCS queries containing the LNPQS translation type are processed as IN queries. Thus, erroneous PCS queries containing the LNPQS translation type are shown in the `rept-stat-lnp` output in the LNPQS field, not the PLNPQS field.

If the OPCODE fields in a LNPQS query do not match any of the combination for IN, AIN or WNP queries is not an invalid service, but an undefined service. An undefined service may be used to transmit some non-LNP messages between networks. A query for an undefined service is sent to GTT for further processing.

However, the OPCODE TAG values in LNPQS queries are verified to determine if the values are either NAT or PRI. These OPCODE values are the only values supported by the EAGLE 5 ISS. If the OPCODE TAG value is not NAT or PRI, the generic TCAP ANSI Reject (UNRECOG_OP_CODE) response is sent back.

The specific LNP services know what LNP service the query is coming to based on the CdPA TT value, so each service verifies all three OPCODE fields for itself. The IN, AIN, WNP and PCS services react on the OPCODE errors as follows:

- An IN query not containing any of the following OPCODE values produces the IN REJECT (IN_UNRECOG_OPER_CODE) error response:
 - The OPCODE TAG value NAT
 - The OPCODE FAMILY value PROVIDE_INSTRUCTION
 - The OPCODE SPEC value IN_START
- An AIN query not containing any of the following OPCODE values produces the AIN RETURN ERROR (ERRONEOUS DATAVAL) error response:
 - The OPCODE TAG value PRI
 - The OPCODE FAMILY value REQUEST_INSTRUCT
 - The OPCODE SPEC value INFO_ANALYZED
- The error responses for a WNP query depends on the OPCODE values that are not provided:
 - The WNPS_REJECT (INCORRECT_COMP_PORT) error response is produced when the OPCODE TAG value is not PRI and not NAT.
 - The WNPS_REJECT (UNRECOG_OP_CODE) error response results is produced when the OPCODE TAG value is not PRI or the OPCODE FAMILY value is not IS41_OP_FAMILY.
 - The WNPS_RET_ERROR (IS41_OP_NOT_SUP) error response is produced when the OPCODE SPEC value is not IS41_NUM_PORT_REQ.
- A PCS query not containing any of the following OPCODE values, produces the PLNPS_REJECT (IN_UNRECOG_OPER_CODE) error response:
 - The OPCODE TAG value NAT
 - The OPCODE FAMILY value PROVIDE_INSTRUCTION
 - The OPCODE SPEC value IN_START

TCAP errors detected before the OPCODE values are verified and the service is determined, causes different responses between LNPQS and specific LNP services (IN, AIN, WNP, PLNP). The EAGLE 5 ISS cannot generate service specific responses before the service is determined.

The LNP Local Subsystem

Local Subsystems in the EAGLE 5 ISS are maintainable entities for query and response. Specific point codes can be defined for routing to Local Subsystems independently of the STP in the network.

A Local Subsystem can be taken online and offline as needed in the system, using the procedures in [LNP Feature Configuration](#). A coordinated state change between the Local Subsystem and its mate can

be manually initiated. When the Local Subsystem changes state, the EAGLE 5 ISS broadcasts SSP/SSA to the CSPC group.

The LNP Query Local Subsystem must be entered into the MAP table, and may have a mate Subsystem and a concerned point code group assigned to it. The LNP Query Local Subsystem cannot be set to Load Shared mode, but can be set only to Dominant or Solitary mode.

For LNP, EAGLE 5 ISS supports ANSI capability point code types. ITU point codes are not supported. Capability point codes for the LNP Query Local Subsystem can be configured only after the LNP feature is enabled.

In performing translation for a message, the LNP NPANXX table is checked first for a match. If a match is found, the LNP data will be used for translation. If no match is found, the non-LNP database is checked for a match.

Messages for the LNP Local Subsystem

Messages for the LNP local subsystem can arrive Rt-on-SSN or Rt-on-GT.

Rt-on-SSN Handling

If a message arrives Rt-on-SSN with the EAGLE 5 ISS LNP Query Subsystem Number (SSN) in the Called Party Subsystem field of the message, the message is forwarded to the LNP Query Local Subsystem.

If a message is destined for the LNP Query Local Subsystem, the status of the LNP Query Local Subsystem is checked before the message is forwarded to the Local Subsystem.

If a message arrives Rt-on-SSN for the EAGLE 5 ISS LNP Query Subsystem and the Subsystem is not available, a Response Method SSP is sent to the OPC of the message. The SSP is sent even if the message can be routed to the mate Subsystem.

If the Local Subsystem is not available and the mated Subsystem is either not defined or not available, the message is discarded and a UDTs is generated if the Return on Error option is set.

Rt-on-GT Handling

If a message arrives Rt-on-GT with the result of translation being the EAGLE 5 ISS true point code and EAGLE 5 ISS LNP Query Subsystem Number (SSN), GTT is performed for the message and the message is forwarded to the LNP Query Local Subsystem.

If a message arrives Rt-on-GT with the result of translation indicating that Message Relay is required, GTT is performed for the message and Message Relay is invoked for the message.

If a message arrives Rt-on-GT for one of EAGLE 5 ISS Capability Point Codes, and the result of translation is the EAGLE 5 ISS LNP Query Local Subsystem, and the Subsystem is not available, MTP sends a TFP to the adjacent point code.

If a message is destined for the LNP Query Local Subsystem, the status of the LNP Query Local Subsystem is checked before the message is forwarded to the Local Subsystem.

If the Local Subsystem is not available and the mated Subsystem is available, EAGLE 5 ISS will route the message to the mated Subsystem.

If the Local Subsystem is not available and the mated Subsystem is either not defined or not available, the message is discarded and a UDTs is generated if the Return on Error option is set.

Hardware, System, and Feature Requirements

The following hardware is required for the LNP feature:

- Up to 18 Service Module cards (E5-SM4G cards or E5-SM8G-B cards) must be configured and installed in the EAGLE.

Note: DSM cards are not supported for ELAP 9.0 or higher.

- The LSMS must be running release 12.0 or higher.
- The ELAP (EAGLE LNP Application Processor) must be running release 10.0 on the MPS platform.

If any of these systems are not running the required release, contact [My Oracle Support \(MOS\)](#).

The maximum LNP telephone number quantity for the EAGLE is set with a feature part number corresponding to the quantity, from 24 million through 384 million numbers in increments of 12 million. To configure a particular LNP telephone number quantity in the EAGLE, the EAGLE must contain Service Module cards. Refer to the `enable-ctrl-feat` command description in *Commands User's Guide* for information on the LNP telephone number quantities, the part numbers that correspond to these quantities, and the Service Module card requirements for that LNP telephone number quantity. The [LNP Feature Configuration on the EAGLE](#) procedure explains how to configure the LNP feature for a specific quantity.

The LNP data is collected at the LSMS from the NPAC for subscription data, and from local provisioning on the LSMS for default NPANXX, split NPANXX and other types of LNP records. This data is sent to the active ELAP on the MPS platform at an EAGLE across a TCP/IP connection in the customer's network. The ELAP stores the data and replicates it to the mate ELAP. The LNP data is sent to the Service Module cards of the EAGLE from the ELAP using two dedicated Ethernet networks between the MPS platform and the Service Module cards of the EAGLE.

When the LNP feature is enabled for the first time, the LRN (location routing number) and NPANXX quantities are set at 100,000 (for LRN) and 150,000 (for NPANXXs). These quantities can be increased to 200,000 LRNs and 350,000 NPANXXs. See the [Increasing the LRN and NPANXX Quantities on the EAGLE](#) procedure.

Telco Switches

Two redundant 1GigE full duplex networks for the A and B ports are connected with Telco Ethernet switches. This requires the installation of the Telco switches and network cabling.

Note:

An upgrade from DSM cards or mixed DSM/E5-SM4G/E5-SM8G-B cards to only E5-SM4G cards and E5-SM8G-B cards is required for the LNP feature with ELAP 9.0 or higher.

The E5-SM4G Throughput Capacity feature must be turned on to achieve higher TPSs on E5-SM4G cards and E5-SM8G-B cards. Refer to the procedure "Activating the E5-SM4G/E5-SM8G-B Throughput Capacity Feature" in *Database Administration - GTT User's Guide*.

Chapter 7

LNP Feature Configuration

Topics:

- *Introduction.....124*
- *LNP Feature Prerequisites.....125*
- *LNP Feature Activation Procedure.....126*
- *LNP Short Message Service Feature Configuration.....159*
- *ITU TCAP LRN Query (LRNQT) Feature Configuration.....163*
- *Triggerless LNP Feature Configuration.....165*
- *Configuring the Service Module Card Ethernet Link to the MPS.....171*
- *Removing DSM Cards.....175*

This chapter contains the procedures used to configure the Local Number Portability (LNP) feature and the following LNP-related features.

- Triggerless LNP (TLNP)
- LRN and NPANXX Quantities on the EAGLE 5 ISS
- LNP Short Message Service (LNP SMS)
- ITU TCAP LRN Query (LRNQT)

Introduction

This chapter contains the procedures for configuring the LNP feature and the following LNP-related functions and features.

- LNP services
- LNP subsystem applications
- LNP configuration options
- Mapping LNP translation types
- The Triggerless LNP feature
- Increasing the LRN and NPANXX Quantities on the EAGLE 5 ISS
- LNP Short Message Service (LNP SMS) feature
- ITU TCAP LRN Query (LRNQT) feature

Note: EAGLE 5 ISS database administration privileges are password restricted. Only those persons with access to the command class Database Administration can execute the LNP administrative functions.

It is possible for two or more users to make changes to the same database element at any time during their database administration sessions. It is strongly recommended that only one user at a time make any changes to the database.

System Prerequisites

Before any feature that is described in this manual can be enabled, the prerequisites listed in [Table 16: System Prerequisites](#) are required in the system.

Table 16: System Prerequisites

Prerequisite	Verification and Provisioning
<p>The system serial number must be correct and locked.</p> <p>For new installations, the system is shipped with an unlocked serial number. The serial number can be changed if necessary and must be locked after the system is on-site.</p> <p>For systems that are being upgraded, the serial number is usually already verified and locked.</p>	<p>Note: The serial number cannot be changed after it is entered and locked in the system.</p> <p>Locate the serial number for the system on a label affixed to the control shelf (1100).</p> <p>Enter the <code>rtrv-serial-num</code> command to display the serial number and its locked status.</p> <p>Verify that the displayed serial number is correct for the system.</p> <p>If no serial number is displayed, enter the <code>ent-serial-num</code> command (without the lock parameter) to provision the serial number that appears on the control shelf label. Enter the</p>

Prerequisite	Verification and Provisioning
	<p><code>rtrv-serial-num</code> command and verify that the serial number was entered correctly.</p> <p>Enter the <code>ent-serial-num</code> command with the <code>lock=yes</code> parameter to lock the serial number in the system.</p>
A sufficient number of Service Module cards must be equipped.	<p>Enter the <code>rtrv-stp:type=dsm</code> command to list the Service Module cards in the system.</p> <p>If additional Service Module cards or cards of a different type are needed, refer to the procedures in <i>Database Administration Manual - GTT</i> to add Service Module cards (E5-SM4G, E5-SM8G-B) or to remove DSM cards.</p>
<p>The GTT feature must be on in the system.</p> <p>Some features require an additional GTT-related feature such as EGTT. See the specific feature prerequisites in this chapter.</p>	<p>Enter the <code>rtrv-feat</code> command to display the GTT feature status.</p> <p>If the GTT feature is on, the <code>gtt=on</code> entry appears in the output.</p> <p>If the <code>gtt=off</code> entry appears in the output, use the procedures in <i>Database Administration Manual - GTT</i> to turn on and provision the GTT feature and any other GTT-related features and functions that will be used in the system.</p>

LNP Feature Prerequisites

Before an LNP quantity feature can be enabled, the following prerequisites are required in the system:

Table 17: LNP Feature Prerequisites

Prerequisite	Verification and Provisioning
ELAP 10.0 and LSMS 12.0 or higher must be used with the EAGLE.	<p>Enter the <code>rept-stat-mps</code> command to display the ELAP version.</p> <p>Verify the LSMS and ELAP versions with your system administrator or account representative.</p>
All Service Module cards for LNP must be E5-SM4G cards or E5-SM8G-B cards. DSM cards are not supported.	<p>Enter the <code>rept-stat-card:type=dsm</code> command.</p> <p>If any cards of TYPE DSM are listed as running the VSCCP GPL, use the Removing DSM Cards procedure to remove these DSM cards.</p> <p>If E5-SM4G or E5-SM8G-B Service Module cards need to be added, use the procedure <i>Adding a</i></p>

Prerequisite	Verification and Provisioning
	<i>Service Module</i> in <i>Database Administration - GTT User's Guide</i> to add the cards.
Oracle recommends that the ELAP is connected to the EAGLE before LNP telephone number data is loaded onto the ELAP and before the LNP telephone number quantity feature is enabled on the EAGLE.	<p>When the LNP telephone number quantity feature is enabled on the EAGLE, the feature access key and quantity information is sent to the ELAP, resulting in the ELAP database quantity being the same as the LNP quantity on the EAGLE. If the ELAP database quantity is larger than the LNP quantity on the EAGLE, the ELAP RTDB is not loaded onto the entire set of Service Module cards on the EAGLE. Some of the Service Module cards load the ELAP RTDB to provide a restricted level of GTT/LNP service. The remainder of the Service Module cards are put into a restricted state. UIM 1323 is generated at the EAGLE. To avoid this situation, ensure that the LNP quantity to be configured on the EAGLE in this procedure is greater than the ELAP RTDB quantity.</p> <p>Verify the ELAP RTDB quantity by performing the Verifying RTDB Status at the EAGLE Terminal.</p> <p>Verify that the LNP feature quantity to be enabled on the system is greater than the ELAP RTDB quantity.</p>

LNP Feature Activation Procedure

This procedure contains the basic steps necessary to activate the LNP feature which makes the feature fully operational in the system. Some of the steps refer to other detailed procedures contained in this manual.

Refer to *Commands User's Guide* for complete descriptions of the EAGLE commands used in this procedure, including parameter names, valid parameter values, rules for using the commands, and output examples.

To make the LNP feature fully operational in the system, actions need to be taken at the LSMS, each ELAP, and the EAGLE.

1. At the EAGLE, perform [Step 2](#) through [Step 7](#).
2. Display the FAK-controlled features that are enabled in the system. Enter the `rtrv-ctrl-feat` command.

Note: For an LNP ported TNs quantity (the "LNP feature") to be enabled or for the LNP ELAP Configuration feature to be enabled, the following features cannot be enabled:

- All EPAP-related features
- MTP Routed Messages for SCCP Applications feature

If any EPAP-related features or the MTP Routed Messages for SCCP Applications feature are enabled, the LNP feature cannot be enabled; this procedure cannot be performed. If you want to enable the LNP feature, contact [My Oracle Support \(MOS\)](#) for assistance.

Note: The E5-SM4G Throughput Capacity feature and the LNP feature can be enabled at the same time.

- If both an LNP ported TNS quantity and the EAGLE LNP ELAP Configuration feature are not enabled, perform the [LNP Feature Configuration on the EAGLE](#) procedure. Then continue with [Step 3](#).
 - If the LNP ELAP Configuration feature is enabled but the LNP ported TNS entry does not appear in the output, continue with [Step 3](#).
 - If both an LNP ported TNS quantity and the LNP ELAP Configuration feature appear in the command output, continue with [Step 3](#).
3. Verify the state and location of the Service Module cards running the VSCCP application. Enter the `rept-stat-card:appl-vsccp` command.

Note: DSM cards are not supported. Only E5-SM4G cards and E5-SM8G-B cards running the VSCCP application and the SCCPHC GPL can be used as Service Module cards.

 - If a sufficient number of E5-SM4G and E5-SM8G-B Service Module cards running the SCCPHC GPL and no DSM cards running the VSCCP GPL are in the system, continue with [Step 4](#).
 - If no cards running the VSCCP GPL or the SCCPHC GPL (Service Module cards) are shown in the output, perform the procedure *Adding a Service Module* in *Database Administration - GTT User's Guide* to configure and install a sufficient number of E5-SM4G or E5-SM8G-B Service Module cards in the system. Then continue with [Step 4](#).
 - If DSM cards running the VSCCP GPL appear in the output, perform the [Removing DSM Cards](#) procedure to remove all DSM cards from the system. Then continue with [Step 4](#).
 4. Verify the Service Module card Ethernet configuration to the ELAPs. Enter the `rtrv-ip-lnk` command.
 - If all Service Module cards have IP links to the ELAPs, continue with [Step 5](#).
 - If the output does not show IP links from some or any Service Module cards to the ELAPs, perform the [Configuring the Service Module Card Ethernet Link to the MPS](#) procedure to configure the IP link to ELAP A or ELAP B from each Service Module card that does not have an IP link configured. Then continue with [Step 5](#).
 5. Verify that the state of all Service Module cards is IS-NR (In-Service-Normal). Enter the `rept-stat-sccp` command.

The state of the Service Module cards is shown in the `PST` column of the output.

 - If all Service Module cards are in the IS-NR state, continue with [Step 6](#).
 - If the state of any Service Module card is not IS-NR, place each of these cards back into service. Enter the `rst-card` command for each card, with the `loc` parameter to specify the location for the card that is shown in the `rept-stat-sccp` command output. Then continue with [Step 6](#).
 6. Test port A of each Service Module card using the `ping pass` command with the card location of the Service Module card and the IP address for port A of that Service Module card shown in the command output in [Step 5](#).

```
pass:cmd="ping 192.168.120.1":loc=1301
```

7. Test port B of each Service Module card using the ping pass command with the card location of the Service Module card and the IP address for port B shown in the command output in [Step 5](#).

```
pass:cmd="ping 192.168.121.1":loc=1301
```

8. At the MPS (ELAP A or B), perform [Step 9](#) through [Step 13](#).
9. Log into ELAP A or B.
10. From **ELAP Menu**, select **Maintenance > Display Release Levels** to verify that the ELAP version is correct .
If the ELAP version is not correct, contact [My Oracle Support \(MOS\)](#) for assistance before continuing with this procedure.
11. Perform a health check of the MPS.
Perform the [MPS Health Check Procedure](#). Then continue with [Step 12](#).
12. Disable the LSMS Connection.
 - a) Select **Maintenance > LSMS Connection > View Allowed**.

The **View LSMS Connection Allowed** dialog box is displayed. See [Figure 48: View LSMS Connection Allowed Dialog](#).

A View LSMS Connection Allowed

i INFO: The LSMS Connection is currently Enabled.

Figure 48: View LSMS Connection Allowed Dialog

- If the connection is disabled, no action is necessary. Go to [Step 13](#).
 - If the connection is enabled, continue with [Substep b](#).
- b) Select **Maintenance > LSMS Connection > Change Allowed**.

The **Change LSMS Connection Allowed** dialog box is displayed showing the **Disable LSMS Connection** button. See [Figure 49: Change LSMS Connection Allowed Dialog](#).

A Change LSMS Connection Allowed

i INFO: The LSMS Connection is currently Enabled.

! CAUTION: This action will Disable the LSMS Connection.

Disable LSMS Connection

Figure 49: Change LSMS Connection Allowed Dialog

- c) Click the **Disable LSMS Connection** button.

The **Change LSMS Connection Allowed** dialog box is displayed. See [Figure 50: Change LSMS Connection Allowed - Disable Success Dialog](#).



Figure 50: Change LSMS Connection Allowed - Disable Success Dialog

13. Repeat [Step 9](#) through [Step 12](#) for the other ELAP.

Then continue with [Step 14](#).

14. Verify the telephone number quantity on the ELAP.

Perform the [Verifying RTDB Status at the ELAP User Interface](#) procedure.

Record the TNs quantity shown in the Counts : line in the RTDB Status, for use in [Step 15](#).

Continue with [Step 15](#).

15. **At the EAGLE**, verify the LNP feature quantity if the LNP feature is enabled.

Enter the `rtrv-ctrl-feat` command.

If the LNP ported TNs entry appears in the output, record the quantity shown in the command output.

If the LNP ported TNs entry does not appear in the output (the LNP feature is not enabled yet), determine the quantity for the LNP feature that will be enabled in [Step 16](#).

Note: The number of telephone numbers on the ELAP (recorded in [Step 14](#)) must be less than the configured LNP feature quantity on the EAGLE. If the telephone number quantity on the ELAP is greater than the LNP feature quantity enabled on the EAGLE, the ELAP RTDB is not loaded onto the entire set of Service Module cards on the EAGLE. Some of the Service Module cards load the ELAP RTDB to provide a restricted level of GTT and LNP service. The remainder of the Service Module cards are put into a restricted state. UIM 1323 is generated at the EAGLE. To avoid this situation, make sure when performing [Step 16](#) that the LNP feature quantity configured on the EAGLE is greater than the ELAP telephone number quantity.

If the telephone number quantity that you recorded from the ELAP in [Step 14](#) is less than the quantity shown in the LNP ported TNs entry in the `rtrv-ctrl-feat` output or is less than the LNP feature quantity that will be enabled in [Step 16](#), continue with [Step 16](#).

16. **At the EAGLE**, enable the LNP feature for the desired LNP telephone number quantity.

Perform the [LNP Feature Configuration on the EAGLE](#) procedure. Then continue with [Step 17](#).

17. **At the LSMS**, perform [Step 18x](#) through [Step 20](#).

18. Contact [My Oracle Support \(MOS\)](#) to enable the LNP telephone quantity on the LSMS.

19. Create a new EMS for the new MPSs.

Perform the [Creating an EMS Configuration Component](#) procedure.

Then continue with [Step 20](#).

20. Configure new MPSs in the EMS Routing window.
Perform the [EMS Routing](#) procedure. Then continue with [Step 21](#).

21. At the MPS (ELAP A or B), perform [Step 22](#) through [Step 23](#).

22. Enable the LSMS Connection.

- a) Select **Maintenance > LSMS Connection > View Allowed**.

The **View LSMS Connection Allowed** dialog box is displayed. See [Figure 51: View LSMS Connection Allowed - Connection Enabled Dialog](#).

A View LSMS Connection Allowed

i INFO: The LSMS Connection is currently Enabled.

Figure 51: View LSMS Connection Allowed - Connection Enabled Dialog

- If the connection is enabled, no action is necessary. Go to [Step 24](#).
 - If the connection is disabled, continue with [Substep b](#).
- b) Select **Maintenance > LSMS Connection > Change Allowed**.

The **Change LSMS Connection Allowed** dialog box is displayed showing the **Enable LSMS Connection** button. See [Figure 52: Change LSMS Connection Allowed - Connection Disabled Dialog](#).

A Change LSMS Connection Allowed

i INFO: The LSMS Connection is currently Disabled.

! CAUTION: This action will Enable the LSMS Connection.

Enable LSMS Connection

Figure 52: Change LSMS Connection Allowed - Connection Disabled Dialog

- c) Click the **Enable LSMS Connection** button.

The **Change LSMS Connection Allowed Dialog** dialog box is displayed. See [Figure 53: Change LSMS Connection Allowed - Enable Success Dialog](#).

A Change LSMS Connection Allowed


 SUCCESS: The LSMS Connection is now Enabled.

Figure 53: Change LSMS Connection Allowed - Enable Success Dialog

23. Repeat [Step 22](#) for the other ELAP.
Then continue with [Step 24](#).
24. **At the LSMS**, perform a bulk download or SERVDI (Support ELAP Reload Via Database Image) bulk download to one of the ELAPs.
Perform the procedures in [Bulk Load Procedure](#) or in [SERVDI Bulk Download](#). Then continue with [Step 25](#).
25. **At the MPS (the ELAP specified in [Step 9](#))**, perform [Step 26](#) through [Step 27](#).
26. Copy the bulk downloaded database to the other ELAP; or if the SERVDI procedure is used, restore the RTDB.
Perform the procedures in [Copying One RTDB from Another RTDB](#), or in [Restore RTDB on ELAP](#) for SERVDI. Then continue with [Step 27](#).
27. Perform a health check of the MPS.
Perform the procedure in [MPS Health Check Procedure](#). Then continue with [Step 28](#).
28. **At the EAGLE**, distribute the RTDB to each Service Module card in the EAGLE.
Perform the procedures in [Distributing the LNP Database after LSMS-Based Operation or RTDB Copy](#). Then continue with [Step 29](#).
29. **At the MPS (ELAP A or B)**, perform [Step 30](#) through [Step 33](#).
30. Disable the LSMS Connection.
 - a) Select **Maintenance > LSMS Connection > View Allowed**.
The **View LSMS Connection Allowed** dialog box is displayed. See [Figure 51: View LSMS Connection Allowed - Connection Enabled Dialog](#).

A View LSMS Connection Allowed

 INFO: The LSMS Connection is currently Enabled.

Figure 54: View LSMS Connection Allowed - Connection Enabled Dialog

If the connection is disabled, no action is necessary. Continue with [Step 32](#).

If the connection is enabled, continue with [Substep b](#).

- b) Select **Maintenance > LSMS Connection > Change Allowed**.

The **Change LSMS Connection Allowed** dialog box is displayed showing the **Disable LSMS Connection** button. See [Figure 55: Change LSMS Connection Allowed - Connection Enabled Dialog](#).

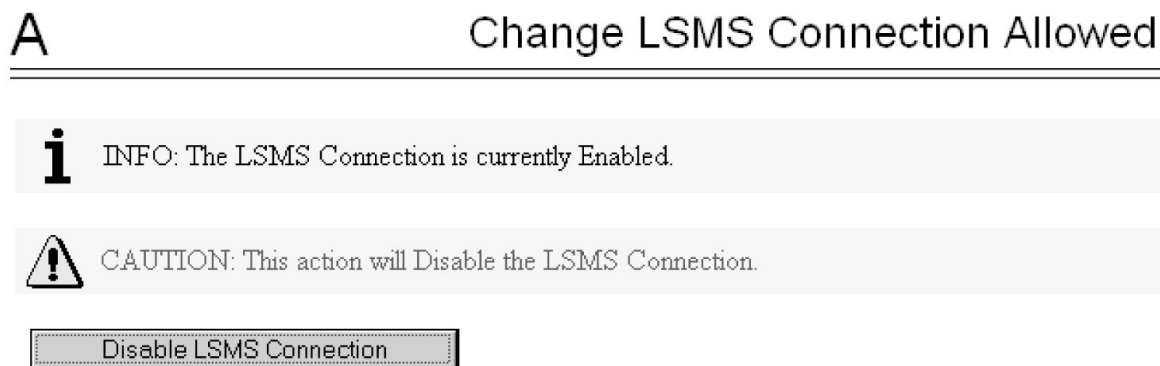


Figure 55: Change LSMS Connection Allowed - Connection Enabled Dialog

- c) Click the **Disable LSMS Connection** button.

The **Change LSMS Connection Allowed Dialog** is displayed. See [Figure 56: Change LSMS Connection Allowed - Disable Success Dialog](#).



Figure 56: Change LSMS Connection Allowed - Disable Success Dialog

31. Repeat [Step 30](#) for the other ELAP.
Then continue with [Step 32](#).

32. Enable LSMS Connection.

- a) Select **Maintenance > LSMS Connection > View Allowed**.

The **View LSMS Connection Allowed** dialog box is displayed. See [Figure 57: View LSMS Connection Allowed - Connection Enabled Dialog](#).

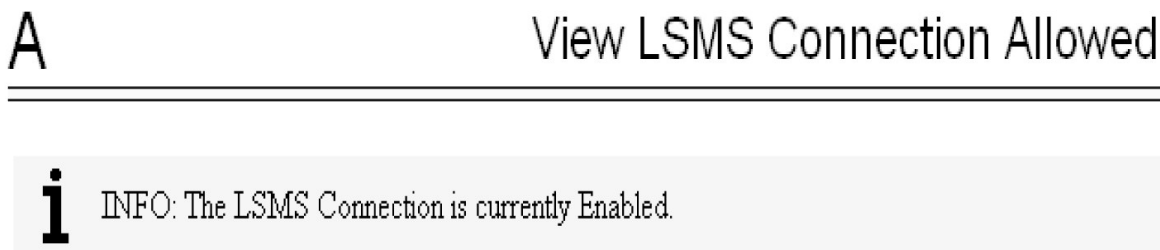


Figure 57: View LSMS Connection Allowed - Connection Enabled Dialog

If the connection is enabled, no action is necessary. Continue with [Step 34](#).

If the connection is disabled, continue with [Substep b](#).

- b) Select **Maintenance > LSMS Connection > Change Allowed**.

The **Change LSMS Connection Allowed** dialog box is displayed showing the **Enable LSMS Connection** button. See [Figure 58: Change LSMS Connection Allowed - Connection Disabled Dialog](#).

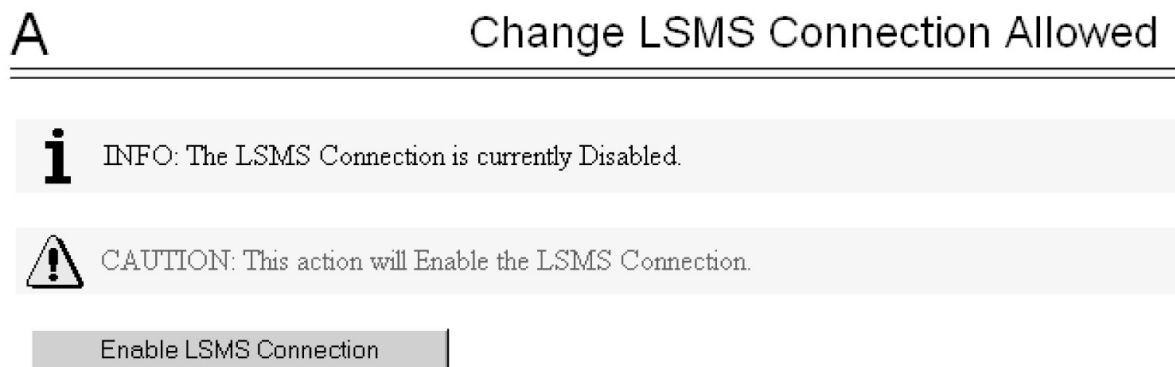


Figure 58: Change LSMS Connection Allowed - Connection Disabled Dialog

- c) Click the **Enable LSMS Connection** button.

The **Change LSMS Connection Allowed** dialog box is displayed. See [Figure 59: Change LSMS Connection Allowed - Enabled Success Dialog](#).



Figure 59: Change LSMS Connection Allowed - Enabled Success Dialog

33. Repeat [Step 32](#) for the other ELAP.

Then continue with [Step 34](#).

34. **At the LSMS**, verify that both EMSs are associated with the LSMS.

The EMS Status area in the LSMS Console window should show that the EMSs connected to the LSMS are green.

LNP Feature Configuration on the EAGLE

This procedure is performed on the EAGLE to configure the LNP feature.

Refer to *Commands User's Guide* for complete descriptions of the commands used in this procedure, including parameter names and valid values, rules for using the commands correctly, and output examples.

The LNP feature is a quantity feature that specifies the maximum number of LNP ported TNs that can be defined in the ELAP RTDB. The quantity that can be enabled per EAGLE node ranges from 24 million LNP numbers and number blocks to 384 million LNP numbers and number pool blocks. LNP-related features can provide up to 200,000 LRNs and 350,000 NPANXX numbers on a single node.

The LNP feature prerequisites are ELAP 10.0 and LSMS 12.0 or higher.

The LNP ELAP Configuration feature must be enabled and turned on before the LNP quantity feature can be enabled. The LNP feature is automatically turned on when it is enabled.

The LNP quantity feature and the LNP ELAP Configuration feature must be purchased before they can be enabled on the EAGLE. If you are not sure if you have purchased the desired LNP quantity feature and the LNP ELAP Configuration feature, or do not have the Feature Access Key (FAK) for the LNP quantity being enabled or for the LNP ELAP Configuration feature, contact your system administrator or [My Oracle Support \(MOS\)](#).

Refer to the description of the `enable-ctrl-feat` command in *Commands User's Guide* for a list of the part numbers for the available LNP telephone number quantities. The Feature Access Key (FAK), which is provided when the feature is purchased, is based on the feature part number and the serial number of the EAGLE, which means that the Feature Access Key (FAK) is site-specific.

After the LNP feature is enabled for a specific quantity, that quantity cannot be reduced. The LNP ELAP Configuration and LNP features cannot be disabled or turned off, and cannot be enabled with a temporary Feature Access Key.

1. Display the status of the EAGLE database by entering the `rept-stat-db` command.

The EAGLE database is backed up to the fixed disk and a removable cartridge or medium before the LNP feature is enabled. The removable cartridge or medium that contains the database must be inserted in the removable cartridge drive or USB port.

- If the `RD BKUP` field of the `rept-stat-db` output contains dashes, the removable cartridge drive or USB port does not contain a removable cartridge or medium. If dashes are shown in the `RD BKUP` field, insert the removable cartridge or medium that contains the database into the removable cartridge drive or USB port.
- If the removable cartridge or medium is not the one that contains the database, replace the removable cartridge or medium with the one that contains the database.

2. Back up the database using the `chg-db:action=backup:dest=fixed` command.

The following messages appear. The active Maintenance and Administration Subsystem Processor (MASP) message appears first.

```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.  
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.  
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.  
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

3. Back up the database to the removable cartridge or medium using the `chg-db:action=backup:dest=remove` command.

The following messages appear:

```
BACKUP (REMOVABLE) : MASP B - Backup starts on active MASP.  
BACKUP (REMOVABLE) : MASP B - Backup to removable cartridge complete.
```

4. Display the status of the databases by entering the `rept-stat-db` command.
 - If the databases are not coherent after [Step 2](#) and [Step 3](#) are performed, stop performing this procedure and contact [My Oracle Support \(MOS\)](#).

- If the databases are coherent after [Step 2](#) and [Step 3](#) are performed, remove the removable cartridge or medium from the removable cartridge drive or USB port and store the removable cartridge or medium in a secure place.
5. Display a summary report of all of the device trouble notifications in the EAGLE by entering the `rept-stat-trbl` command.
If any alarms are shown in the `rept-stat-trbl` output, stop performing this procedure and contact [My Oracle Support \(MOS\)](#).
 6. Display the status of the cards in the EAGLE by entering the `rept-stat-card` command.
If the PST status of any of the cards shown in the `rept-stat-card` output is not IS-NR, stop performing this procedure and contact [My Oracle Support \(MOS\)](#).
 7. Display the status of the Service Module Cards running the VSCCP application by entering the `rept-stat-sccp` command.
Note: The `rept-stat-sccp` command output contains fields that are not used by this procedure. To see the fields displayed by the `rept-stat-sccp` command, refer to the `rept-stat-sccp` command description in *Commands User's Guide*.
 8. Display the controlled features that are enabled in the system, by entering the `rtrv-ctrl-feat` command..
 - If the LNP ELAP Configuration feature entry does not appear in the `rtrv-ctrl-feat` command output, continue with [Step 9](#)
 - If the `rtrv-ctrl-feat` output shows the LNP ELAP Configuration feature with Status of off, go to [Step 10](#),
 9. Enable the LNP ELAP Configuration feature by entering the following command.
`enable-ctrl-feat:partnum=893010901:fak=<LNP ELAP Configuration Feature Access Key>`
 10. Turn the LNP ELAP Configuration feature on by entering the following command.
`chg-ctrl-feat:partnum=893010901:status=on`
 11. Verify the changes by entering the `rtrv-ctrl-feat` command.
`rtrv-ctrl-feat:partnum=893010901`
 12. Enable the LNP quantity feature using the `enable-ctrl-feat` command with the part number of the desired quantity and the Feature Access Key for that quantity.
Note: The Feature Access Key (FAK) is provided when the feature is purchased. If you do not have the Feature Access Key for the desired LNP quantity, contact [My Oracle Support \(MOS\)](#).
`enable-ctrl-feat:partnum=893011012:fak=<Feature Access Key>`
 13. Verify the changes by entering the `rtrv-ctrl-feat` command with the LNP feature part number that was enabled in [Step 12](#).
 14. Verify the changes to the Service Module cards running the VSCCP application by entering the `rept-stat-sccp` command.
In the `rept-stat-sccp` output, the primary state (PST) of each card should be IS-NR, and dashes should be shown in the AST column.
Note: The `rept-stat-sccp` command output contains fields that are not used by this procedure. To see the fields displayed by the `rept-stat-sccp` command, see the `rept-stat-sccp` command description in *Commands User's Guide*.

15. Display a summary report of all of the device trouble notifications in the EAGLE by entering the `rept-stat-trbl` command.
If any alarms are shown in the `rept-stat-trbl` output, stop performing this procedure and contact [My Oracle Support \(MOS\)](#).
16. Display the overall status of the ELAP subsystem running on the MPS (Multi-Purpose Server) by entering the `rept-stat-mps` command.
If any alarms are shown in the `rept-stat-mps` output, stop performing this procedure and contact [My Oracle Support \(MOS\)](#).
17. Back up the changes using the `chg-db:action=backup:dest=fixed` command.
The following messages appear. The active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

18. Display the status of the databases with the `rept-stat-db` command.
If the databases are not coherent, or if ELAP A and ELAP B do not have the same birthdate, contact [My Oracle Support \(MOS\)](#).
If the databases are coherent, and if ELAP A and ELAP B have the same birthdate, this procedure is finished.

Adding an LNP Service

This procedure is used to assign an LNP translation type to a unique LNP service using the `ent-lnp-serv` command. The `ent-lnp-serv` command uses these parameters.

Note: LNP Translation type name referenced in the ENT-LNP-SERV command is different from the Translation type name referenced in ENT-TT command.

:serv – the LNP service assigned to the LNP translation type

:tt – the LNP translation type

:ttn – the LNP translation type name

:dv – the type of digits used by LNP (SCCP, TCAP)

:alias – the alias LNP translation type

:on/:off=gttrqd - GTT Required; indicates whether GTT needs to be performed on an LNP MSU before NP Query Service processing or after LNP MR processing.

:gttselid - GTT Selector ID used to perform GTT on an MSU before LNP Query processing or after LNP Message Relay processing

:dfiltact - Action taken when a GTT selector search (using the GTT Selector ID from the LNP Service table entry) fails while performing Pre-LNP Query Service GTT processing or Fall-back to GTT after LNP MR Service processing

The LNP feature must be enabled. Verify this by entering the `rtrv-ctrl-feat` command. If the LNP feature is enabled, the entry `LNP ported TNS` is shown in the `rtrv-ctrl-feat` output with a quantity greater than zero.

A maximum of 10 LNP services can be assigned to LNP translation types.

The following LNP MR services can be assigned to LNP translation types:

- CLASS
- CNAM
- LIDB
- ISVM
- LNP Short Message Service (Wireless Short Message Service Center `serv=wsmc`)
- Four user-defined services (UDF1, UDF2, UDF3, UDF4).

The following LNP Query services can be assigned to LNP translation types:

- AIN
- IN
- Wireless Number Portability (`serv=wnp`)
- PCS 1900 Number Portability (`serv=pcs`)
- LNP Query Service (`serv=lnpqs`)
- ITU TCAP LRN Query `serv=lrnqt`
- Four user-defined services (UDF1, UDF2, UDF3, UDF4).

The alias LNP translation type provides an alternate value for the LNP translation type, so that different networks can use different translation type values for the specified LNP service. If the alias translation type in the SCCP Called Party Address is defined in the database as an alias LNP translation type, the alias translation type value is mapped to the associated true LNP translation type value, defined by the `tt` parameter, in the database to determine the LNP service that is used on the message. All translation type values (0 - 255) can be used as values for the alias parameter, as long as that value is not already in the database as a value for the `tt` parameter.

The `tt` and `serv` parameter combination can be specified only once.

The `tt` and alias parameters cannot be specified at the same time. To add a new LNP service and an alias translation type for that service, the `ent-lnp-serv` command must be entered at least twice, depending on how many aliases you wish to enter. The first time the `ent-lnp-serv` command is entered, the LNP service (`serv`) and true translation type (`tt`) is defined in the database. When the `ent-lnp-serv` command is entered again with the specified LNP service and the `alias` parameter, the alias translation types (`alias`) are assigned to the LNP service.

The value of the alias parameter cannot be in the database as an LNP translation type (`tt`).

The value of the `tt` parameter cannot be in the database as an alias LNP translation type (`alias`).

If the `serv` and `tt` parameters are specified, the service type specified by the `serv` parameter cannot be in the database.

Translation type names can be assigned to the LNP service and translation type with the `ttn` parameter. If the parameter is not specified, the translation type name is set to the LNP service name. The translation type name must be unique in the database. The word `none` is used as a value for the `ttn` parameter of the `chg-lnp-serv` command and cannot be used as a translation type name with the `ent-lnp-serv` command.

A translation type name can be the service type name only if the service type name matches the value of the `serv` parameter.

If the value of the `serv` parameter is a user defined service type, the value of the `dv` parameter must be `sccp`.

If the value of the `serv` parameter is either `ain`, `in`, `wnp`, `pcs`, or `lnpqs`, the value of the `dv` parameter must be `tcap`.

The translation type and LNP service specified with the `ent-lnp-serv` command cannot be in the database.

To specify the `serv=wnp` parameter with the `ent-lnp-serv` command, the Wireless Number Portability feature must be turned on. This can be verified with the `WNP = on` entry in the `rtrv-feat` command output.

To specify the `serv=pcs` parameter with the `ent-lnp-serv` command, the PCS 1900 Number Portability feature must be turned on. This can be verified with the `PLNP = on` entry in the `rtrv-feat` command output.

To specify the `serv=wsmc` parameter with the `ent-lnp-serv` command, the LNP Short Message Service (LNP SMS) feature must be enabled and on. This can be verified in the `rtrv-ctrl-feat` command output. If the LNP SMS feature is not enabled and on, perform the [LNP Short Message Service \(LNP SMS\) Feature Configuration Procedure](#) procedure to enable and turn the LNP SMS feature on.

The LNP service LNPQS defines the translation type used for LNP queries between networks. This service is defined with the `serv=lnpqs` parameter. While the EAGLE allows any translation type to be assigned to the LNPQS service, it is recommended that translation type 11 is assigned to the LNPQS service. If any LNP service is assigned translation type 11, and you wish to provision the LNPQS service, the existing service using translation type 11 must be changed to use another translation type. Perform the [Changing an LNP Service](#) procedure to change the translation type of the existing service. See [LNP Query Service \(LNPQS\)](#) for more information on LNPQS queries.

The examples in this procedure are used to add the LNP services and alias translation types shown in [Table 18: Example LNP Service Configuration](#).

Table 18: Example LNP Service Configuration

SERV	TT	TTN	DV	ALIAS
IN	30	INGTE	TCAP	---
IN	---	---	----	150
IN	---	---	----	175
UDF3	100	UDF3	SCCP	---
UDF3	---	---	----	40
UDF3	---	---	----	45

SERV	TT	TTN	DV	ALIAS
AIN	---	---	----	240
LIDB	---	---	----	80
WNP	50	WNP50	TCAP	---
PCS	19	PCS19	TCAP	---
WSMSC	139	WSMSC1	TCAP	---
LNPQS	11	LNPQS	TCAP	---

1. Verify that the LNP feature is enabled by entering the `rtrv-ctrl-feat` command.
 If the LNP feature is enabled, the entry `LNP ported TNS` should appear in the `rtrv-ctrl-feat` output with a quantity greater than 0.
 If the LNP feature is not enabled, perform the procedures in [LNP Feature Activation Procedure](#) to enable the LNP feature.
 If the LNP feature is enabled, continue with [Step 2](#).
2. Display the LNP services and translation type assignments in the database with the `rtrv-lnp-serv` command.
 - If the `rtrv-ctrl-feat` output in step 1 showed that the LNP feature was not enabled, go to [Step 4](#)
 - If the `serv=wnp` or `serv=pcs` parameters will not be specified with the `ent-lnp-serv` command, go to [Step 6](#).
3. Verify that the Wireless Number Portability feature (if the `serv=wnp` parameter will be specified in the `ent-lnp-serv` command) or the PCS 1900 Number Portability feature (if the `serv=pcs` parameter will be specified in the `ent-lnp-serv` command), by entering the `rtrv-feat` command.
Note: The `rtrv-feat` command output contains other fields that are not used by this procedure. If you wish to see all the fields displayed by the `rtrv-feat` command, see the `rtrv-feat` command description in *Commands User's Guide*.
 If the Wireless Number Portability Feature is on, the entry `WNP = on` appears in the `rtrv-feat` output.
 If the PCS 1900 Number Portability Feature is on, the entry `PLNP = on` appears in the `rtrv-feat` output.
 Perform [Step 4](#) only if the wireless number portability feature is off and the `serv=wnp` parameter will be specified with the `ent-lnp-serv` command.
 Perform [Step 5](#) only if the PCS 1900 number portability feature is off and the `serv=pcs` parameter will be specified with the `ent-lnp-serv` command.
4. Turn the Wireless Number Portability Feature on with the `chg-feat` command.
 Enter this command: `chg-feat:wnp=on`
Note: Once the Wireless Number Portability feature is turned on with the `chg-feat` command, it cannot be turned off. The Wireless Number Portability feature must be purchased before you

turn the feature on with the `chg-feat` command. If you are not sure if you have purchased the feature, contact [My Oracle Support \(MOS\)](#).

5. Turn the PCS 1900 Number Portability Feature on with the `chg-feat` command.

Enter this command: `chg-feat:plnp=on`

Note: After the PCS 1900 Number Portability Feature is turned on with the `chg-feat` command, it cannot be turned off. The PCS 1900 Number Portability feature must be purchased before you turn the feature on with the `chg-feat` command. If you are not sure if you have purchased the PCS 1900 number portability feature, contact [My Oracle Support \(MOS\)](#).

Note: If you are not assigning a translation type to the WSMSC service, go to [Step 7](#).

6. If the `rtrv-ctrl-feat` output in [Step 1](#) shows that the LNP SMS feature is enabled and on, go to [Step 7](#).

If the `rtrv-ctrl-feat` output in [Step 1](#) shows that the LNP SMS feature is not enabled or on, perform the [LNP Short Message Service \(LNP SMS\) Feature Configuration Procedure](#) procedure to enable and turn the LNP SMS feature on. Continue with [Step 7](#).

Note:

If you are not assigning a translation type to the LNPQS service, go to [Step 8](#).

7. Any translation type can be assigned to the LNPQS service, but because translation type 11 is used for LNP queries between networks, it is recommended that translation type 11 is assigned to the LNPQS service.

Examine the `rtrv-lnp-serv` output in [Step 2](#) to verify whether or not translation type 11 is assigned to any existing LNP services. If translation type 11 is assigned to any existing LNP services, perform the [Changing an LNP Service](#) procedure and change the translation type of the service using translation type 11.

8. Add the LNP services or alias translation types to the database using the `ent-lnp-serv` command.

For this example, enter these commands:

- `ent-lnp-serv:serv=in:tt=30:ttn=ingte:dv=tcap`
- `ent-lnp-serv:serv=udf3:tt=100:dv=sccp`
- `ent-lnp-serv:serv=ain:alias=240`
- `ent-lnp-serv:serv=in:alias=150`
- `ent-lnp-serv:serv=in:alias=175`
- `ent-lnp-serv:serv=lidb:alias=80`
- `ent-lnp-serv:serv=udf3:alias=40`
- `ent-lnp-serv:serv=udf3:alias=45`
- `ent-lnp-serv:serv=wnp:tt=50:ttn=wnp50:dv=tcap`
- `ent-lnp-serv:serv=pcs:tt=19:ttn=pcs19:dv=tcap`
- `ent-lnp-serv:serv=wsmsc:tt=139:ttn=wsmsc1:dv=tcap`
- `ent-lnp-serv:serv=lnpqs:tt=11:ttn=lnpqs:dv=tcap`

9. Verify the changes with the `rtrv-lnp-serv` command.

10. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.  
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.  
BACKUP (FIXED): MASP A - Backup starts on standby MASP.  
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Removing an LNP Service

This procedure is used to remove an LNP service from the database using the `dlt-lnp-serv` command. The `dlt-lnp-serv` command uses two parameters.

`:serv` – the LNP service

`:alias` – the alias LNP translation type assigned to the LNP service

If the alias parameter is specified, the alias translation type value must be assigned to the specified LNP service. The alias translation types are shown in the `ALIAS` field of the `rtrv-lnp-serv` command output.

The value of the alias parameter cannot be in the database as a true translation type value. The true translation types are shown in the `TT` field of the `rtrv-lnp-serv` command output.

Before an LNP service can be removed from the database, all alias translation types assigned to that service must be removed from the database.

The example in this procedure removes LNP service UDF3 from the database.

1. Display the LNP services and translation type assignments in the database with the `rtrv-lnp-serv` command.
2. Remove the LNP service from the database using the `dlt-lnp-serv` command.

For this example, enter these commands:

```
dlt-lnp-serv:serv=udf3:alias=40
```

```
dlt-lnp-serv:serv=udf3:alias=45
```

```
dlt-lnp-serv:serv=udf3
```

3. Verify the changes with the `rtrv-lnp-serv` command.
4. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.  
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.  
BACKUP (FIXED): MASP A - Backup starts on standby MASP.  
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Changing an LNP Service

This procedure is used to change the attributes of an existing LNP service using the `chg-lnp-serv` command. The `chg-lnp-serv` command uses these parameters.

`:serv` – the LNP service

`:nserv` – the new LNP service

`:tt` – the current LNP translation type assigned to the LNP service

`:ntt` – the new LNP translation type assigned to the LNP service

`:nttn` – the new LNP translation type name assigned to the LNP service

`:ndv` – the new digits valid indication for the LNP service

`:on/:off=gtrqd` - GTT Required; indicates whether GTT needs to be performed on an LNP MSU before NP Query Service processing or after LNP MR processing.

`:gtrselid` - GTT Selector ID used to perform GTT on an MSU before LNP Query processing or after LNP Message Relay processing

`:dfact` - Action taken when a GTT selector search (using the GTT Selector ID from the LNP Service table entry) fails while performing Pre-LNP Query Service GTT processing or Fall-back to GTT after LNP MR Service processing

The values of the `serv` and `tt` parameters must be in the database.

To change the attributes of an LNP service, either the `serv` or `tt` parameters must be specified, but not both parameters. If you are changing the translation type assigned to the LNP service, the `serv` and `ntt` parameters must be specified. If you are changing the LNP service assigned to a translation type, the `tt` and `nserv` parameters must be specified. The `nserv` and `ntt` parameters cannot be specified together in the `chg-lnp-serv` command.

The new translation type name must be unique in the database.

The new translation type (`ntt`) cannot be in the database as a true translation type or an alias translation type. The true translation types and alias translation types are shown in the `rtv-lnp-serv` command output. The true translation types are shown in the `TT` field and the alias translation types are shown in the `ALIAS` field.

The word `none` sets the translation type name value to the service type name. A translation type name can be the service type name only if the service type name matches the value of the `serv` parameter.

If the value of the `serv` parameter is a user defined service type or `wsmc`, the value of the `ndv` parameter must be `scpc`.

If the value of the `serv` parameter is either `ain`, `in`, `wnp`, `pcs`, or `lnpqs`, the value of the `ndv` parameter must be `tcap`.

If the `ndv` parameter is specified, the value must be different from the current value of the `DV` field. The `DV` value can be changed only for these services: `cnam`, `lids`, `isvm`, or `class`.

An LNP service cannot be changed if an alias translation type is assigned to the service. The aliases must be removed from the database using the `dlt-lnp-serv` command. If you wish to continue using the alias translation types with the LNP service after the LNP service has been changed, they must be re-assigned to the LNP service using the `ent-lnp-serv` command.

Any translation type can be assigned to the LNPQS service, but it is recommended that translation type 11 is assigned to the LNPQS service. If you are changing the translation type of another service, and the LNPQS service is provisioned in the database, select a translation type other than 11.

The examples in this procedure are used to change the AIN and CLASS services to the values shown in [Table 19: Changing the LNP Service](#).

Table 19: Changing the LNP Service

SERV	TT	NTT	DV	NDV	TTN	NTTN
AIN	15	55	TCAP	----	AINGTE	AINLIDB
CLASS	25	140	SCCP	TCAP	CLASSGTE	CLASS
WNP	50	75	TCAP	---	WNP50	WNP75

1. Display the LNP services and translation type assignments in the database with the `rtrv-lnp-serv` command.
2. If the LNP service being changed has any alias translation types assigned to it, shown in the ALIAS field in the output of [Step 1](#), remove the alias translation types from the LNP service using the `dlt-lnp-serv` command.

If the LNP service does not have any alias translation types assigned to it, go to [Step 3](#). For this example, the AIN service has alias translation types assigned to it. Remove the alias translation types with these commands:

```
dlt-lnp-serv:serv=ain:alias=235
```

```
dlt-lnp-serv:serv=ain:alias=236
```

```
dlt-lnp-serv:serv=ain:alias=240
```

3. Verify that the Wireless Number Portability feature (if the `nserv=wnp` parameter will be specified in the `chg-lnp-serv` command) or the PCS 1900 Number Portability (PLNP) feature (if the `nserv=pcs` parameter will be specified in the `chg-lnp-serv` command), by entering the `rtrv-feat` command.

Note: The `rtrv-feat` command output contains other fields that are not used by this procedure. If you wish to see all the fields displayed by the `rtrv-feat` command, see the `rtrv-feat` command description in the *Commands User's Guide*.

If the Wireless Number Portability feature is on, the entry `WNP = on` appears in the `rtrv-feat` output. If the PCS 1900 Number Portability feature is on, the entry `PLNP = on` appears in the `rtrv-feat` output. Perform [Step 4](#) only if the Wireless Number Portability feature is off and the `nserv=wnp` parameter will be specified with the `chg-lnp-serv` command. Perform [Step 5](#) only if the PCS 1900 Number Portability feature is off and the `nserv=pcs` parameter will be specified with the `chg-lnp-serv` command.

4. Turn the Wireless Number Portability feature on with the `chg-feat` command.

For this example, enter this command `chg-feat:wnp=on`

Note: After the Wireless Number Portability feature is turned on with the `chg-feat` command, it cannot be turned off. The wireless number portability feature must be purchased before you turn the feature on with the `chg-feat` command. If you are not sure if you have purchased the Wireless Number Portability feature, contact [My Oracle Support \(MOS\)](#).

5. Turn the PCS 1900 Number Portability feature on with the `chg-feat` command.

For this example, enter this command: `chg-feat:plnp=on`

Note: Once the PCS 1900 Number Portability feature is turned on with the `chg-feat` command, it cannot be turned off. The PCS 1900 Number Portability feature must be purchased before you turn the feature on with the `chg-feat` command. If you are not sure if you have purchased the PCS 1900 Number Portability feature, contact [My Oracle Support \(MOS\)](#).

Note: If the LNP service name (serv parameter value) is being changed to a service name other than WSMSC, go to [Step 7](#).

6. Verify that the LNP Short Message Service is enabled and on by entering the `rtrv-ctrl-feat` command.

If the `rtrv-ctrl-feat` output shows that the LNP SMS feature is enabled, and on, go to [Step 7](#). If the `rtrv-ctrl-feat` output shows that the LNP SMS feature is not enabled or on, perform [LNP Short Message Service \(LNP SMS\) Feature Configuration Procedure](#) to enable and turn the LNP SMS feature on.

Note: If only the alias translation type values for the LNP service are being changed, go to [Step 9](#) to add the new alias translation type values.

7. Change the LNP service using the `chg-lnp-serv` command.
8. Verify the changes with the `rtrv-lnp-serv` command.
9. To continue using the alias translation types removed in [Step 2](#) with the changed LNP service, or add new alias translation types to the LNP service, add them with the `ent-lnp-serv` command. For this example, the alias translation types removed in [Step 2](#) are added back to the AIN service. Enter these commands:

```
ent-lnp-serv:serv=ain:alias=235
ent-lnp-serv:serv=ain:alias=236
ent-lnp-serv:serv=ain:alias=240
```

10. Verify the changes with the `rtrv-lnp-serv` command.
11. Back up the changes using the `chg-db:action=backup:dest=fixed` command. The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED): MASP A - Backup starts on standby MASP.
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Changing LNP Options

This procedure is used to change the LNP configuration options (shown in [Table 20: LNPOPTS Configuration Options](#)), using the `chg-lnpopts` command.

Note: If LNPOPTS options for the following features need to be changed, do not use this procedure; use the procedures in the indicated section of this manual:

- Triggerless LNP (TLNP) - use the procedures in [Triggerless LNP Feature Configuration](#).

- LNP Short Message Service (LNP SMS) - use the procedures in [LNP Short Message Service \(LNP SMS\) Feature Configuration Procedure](#).

Table 20: LNPOPTS Configuration Options

Parameter	Value	Description	Notes
ADMINHIPRI - LNP Database Administration Highest Administrative Priority	Yes	LNP database administration can starve out normal STP updates during LNP administration of 2 TNs per second.	
	No	STP and LNP updates receive the same priority. Depending on the system activity level, the performance of LNP updates may be reduced.	
AMATYPE - AMA Call Type	3 digits		
AMAFEATID - AMA Feature ID	3 digits		
AMASLPID - AMA Slip ID	9 digits		
CCP - Copy Charge Parameters	Yes	The EAGLE copies the Charge Number and Charge Party Station type from an LNP AIN query (if present) to the LNP AIN Response message.	
	No	The Charge Number and Charge Party Station type are not copied from the AIN query to the AIN Response message.	
CIC - Carrier Identification Code	3-4 digits		
DRA - Destination Routing Address content	LRNTN	LRN and TN	
	LRN	LRN only	
FRCSMPLX - Allow Simplex Database Updates	Yes	LNP updates are accepted when the EAGLE is in the simplex	

Parameter	Value	Description	Notes
		mode (when the standby MASP is incoherent, at a different level compared to the active MASP, or unstable).	
	No	LNP updates are not accepted when the EAGLE is in the simplex mode (when the standby MASP is incoherent, at a different level compared to the active MASP, or unstable).	
GTWYSTP - LNP System is also a Gateway STP	Yes	The system is configured as a Gateway STP running the LNP feature.	The NPAC sends LNP subscriptions that contain capability point codes that do not have routes assigned to them in the EAGLE database.
	No	The EAGLE is not configured as a Gateway STP.	
INCSLP - AMA Service Logic ID included in the response	Yes	AMA Service Logic ID is included in the response.	
	No	AMA Service Logic ID is not included in the response.	
JIPDIGITS - Jurisdiction Information Parameter value	6 digits		The Triggerless LNP (TLNP) feature must be on. See Triggerless LNP Feature Configuration .
JIPPRV - Add Jurisdiction Information Parameter value to IAM	Yes	A Jurisdiction Information Parameter value is added to the IAM.	The Triggerless LNP (TLNP) feature must be on. See Triggerless LNP Feature Configuration .
	No	A Jurisdiction Information Parameter value is not added to the IAM.	
LRNDGTS - LRN digits	1-10 digits		

Parameter	Value	Description	Notes
NAIV - Name of Address Indicator Value	0-127 digits		
SERVPORT - Service Portability	Yes	A protocol setting that allows splitting services between TN and LRN override records.	This setting lets the EAGLE LNP craftsman update LRN overrides for Message Relay services that are to be supported in the network. The EAGLE then uses the TN gateway point code (NPAC subscription data) for Message Relay services the CLEC wants to provide.
	No	If no LRN override services are provisioned, then the TN gateway point codes (NPAC subscription data) are used to route queries out of the network.	If one or more LRN override services are provisioned, the TN is considered to be ported into the network. In this case, if an LRN override service is requested and the LRN has other services administered, but the requested service is not provisioned, then a UDTs response for the service is provided.
SP - Service Provider ID	4 alphanumeric characters		
TNDGTS - TN Digits	1-10 digits		
WQREDRCT - Wireless Queries Directed to default GTT	Yes	Allows GTT to treat any wireless LNP (WNP and PLNP) queries that require GT as a normal GTT.	The Wireless Number Portability (WNP) feature or the PCS 1900 Number Portability (PLNP) feature must be on.
	No	Routes all wireless LNP queries (WNP and PCS) that require GTT directly to the local subsystem.	
WSMSC10DIG - SCCP GTA Digit Length	Yes	The system verifies that either 10 or 11 digits are present in the CdPA	The LNP SMS feature must be on. See LNP

Parameter	Value	Description	Notes
Indicator for 10 or 11 digits		GTA. If 11 digits are present, the first digit is stripped to derive 10 digits for LNP SMS translation. If 10 digits are present, all 10 digits are used for LNP WSMSC translation.	Short Message Service (LNP SMS) Feature Configuration Procedure.
	No	The system verifies that 11 digits (plus a padded 0 digit) are present in the CdPA GTA. If 11 digits are present, the system strips the first digit and considers only 10 digits for LNP WSMSC translation.	

The LNP feature must be enabled before the LNPOPTS options can be configured.

The value is not changed for any option that is not specified in the `chg-lnpopts` command.

1. Verify that the LNP feature is enabled by entering the `rtrv-ctrl-feat` command.
If the LNP feature is enabled, the `LNP ported TNs` entry appears in the `rtrv-ctrl-feat` output with a quantity greater than 0.
 - If the LNP feature is enabled, continue with [Step 2](#)
 - If the LNP feature is not enabled, perform the procedures in [LNP Feature Activation Procedure](#) to enable the LNP feature. Then continue with [Step 2](#).
2. Display the LNP option values in the database. Enter the `rtrv-lnpopts` command.
3. If the `wqredrct` option will be changed in this procedure, verify that the Wireless Number Portability (WNP) feature or the PCS 1900 Number Portability (PLNP) feature is on. Enter the `rtrv-feat` command.
 - If the `wqredrct` option will not be specified in this procedure, go to [Step 5](#).
 - If the `wqredrct` option will be specified in this procedure, continue with this step.

If the WNP feature is on, the entry `WNP = on` appears in the `rtrv-feat` output.

If the PLNP feature is on, the entry `PLNP = on` appears in the `rtrv-feat` output.

 - If the WNP feature or the PLNP feature or both features are on, go to [Step 5](#).
 - If the WNP feature or the PLNP feature or both features are not on, continue with [Step 4](#).
4. Turn on the WNP feature or the PLNP feature or both features.

The Wireless Number Portability and PCS 1900 Number Portability features must be purchased before you turn these features on with the `chg-feat` command. If you are not sure if you have purchased these features, contact [My Oracle Support \(MOS\)](#).

Note: After the Triggerless LNP, Wireless Number Portability or PCS 1900 Number Portability features are turned on with the `chg-feat` command, they cannot be turned off.

To turn on the Wireless Number Portability feature, enter the `chg-feat:wnp=on` command.

To turn on the PCS 1900 Number Portability feature, enter the `chg-feat:plnp=on` command.

To turn on both features in the same command, enter the `chg-feat:wnp=on:plnp=on` command.

5. Change the LNP option values that need to be changed, using the `chg-lnpopts` command.
6. Verify the changes with the `rtrv-lnpopts` command.
7. Back up the new changes using the `chg-db:action=backup:dest=fixed` command.

The following messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED): MASP A - Backup starts on standby MASP.
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Changing the LNP Telephone Number Alarm Thresholds

This procedure is used to change the alarm thresholds for generating alarms when the LNP Telephone number quantity has exceeded the defined percentage of the maximum number of LNP telephone numbers the EAGLE 5 ISS can contain. The alarm thresholds are changed using the `chg-th-alm` command and these parameters:

`:lnptndblv1` – The percentage, from 0 to 100, of the maximum number of LNP telephone numbers the EAGLE 5 ISS can contain that generates major alarm UAM 0288. The system default value for the `lnptndblv1` parameter is 90. The current value of this parameter is shown in the LNP TN DB Alarm Level 1: field of the `rtrv-th-alm` command output.

`:lnptndblv2` – The percentage, from 0 to 100, of the maximum number of LNP telephone numbers the EAGLE 5 ISS can contain that generates critical alarm UAM 0287. The system default value for the `lnptndblv2` parameter is 95. The current value of this parameter is shown in the LNP TN DB Alarm Level 2: field of the `rtrv-th-alm` command output.

The `chg-th-alm` command contains other optional parameters. These parameters are not shown here because they are not necessary to provision the LNP telephone number alarm thresholds. These parameters are explained in more detail in the *Commands Manual*.

The maximum number of LNP telephone numbers the EAGLE 5 ISS can contain is shown in the `rtrv-ctrl-feat` command output or in the TN: row in the PROVISIONED TABLE QTY: section of the `rept-stat-lnp` command output.

1. Display the current LNP telephone number alarm thresholds by entering the `rtrv-th-alm` command.

This is an example of the possible output.

```
rlghncxa03w 06-08-28 09:12:36 GMT EAGLE5 35.1.0
LNP TN DB Alarm Level 1:          80%
LNP TN DB Alarm Level 2:          90%
Command Executed
```

Note:

The `rtrv-th-alm` command output contains other fields that are not used in this procedure. If you wish to see all the fields displayed by the `rtrv-th-alm` command, see the `rtrv-th-alm` command description in the *Commands Manual*.

2. Change the LNP telephone number alarm thresholds by entering the `chg-th-alm` command with at least one of the LNP telephone number alarm thresholds.

One or both LNP telephone number alarm threshold parameters can be specified with the `chg-th-alm` command. If a parameter is not specified with the `chg-th-alm` command, that parameter value will not be changed. However, after the `chg-th-alm` command is performed, the `lnptndblv2` parameter value must be greater than the `lnptndblv1` parameter value. For this example, enter this command:

```
chg-th-alm:lnptndblv1=70:lnptndblv2=80
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 06-08-28 09:12:36 GMT EAGLE5 35.1.0
CHG-TH-ALM: MASP A - COMPLTD
```

3. Verify the changes using the `rtrv-th-alm` command.

This is an example of the possible output.

```
rlghncxa03w 06-08-28 09:12:36 GMT EAGLE5 35.1.0
LNP TN  DB Alarm Level 1:          70%
LNP TN  DB Alarm Level 2:          80%
Command Executed
```

Note:

The `rtrv-th-alm` command output contains other fields that are not used in this procedure. If you wish to see all the fields displayed by the `rtrv-th-alm` command, see the `rtrv-th-alm` command description in the *Commands Manual*.

4. Backup the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

Adding a Subsystem Application

This procedure is used to reserve a subsystem number for the LNP application and place the LNP application either online or offline using the `ent-ss-appl` command. The `ent-ss-appl` command uses the following parameters:

:appl – the application type, LNP

:ssn – the LNP subsystem number

:stat – the state of the LNP application

The LNP feature must be enabled. Verify this by entering the `rtrv-ctrl-feat` command. If the LNP feature is enabled, the entry `LNP ported TNs` should appear in the `rtrv-ctrl-feat` output with a telephone quantity greater than 0. If the LNP feature is not enabled, perform the procedures in [LNP Feature Activation Procedure](#) to enable the LNP feature.

Only one subsystem number for each application can be defined.

If the `stat` parameter is not specified, the application will be offline.

The LNP application applies to both global title translation services and LNP queries.

The application specified by the `appl` parameter cannot already be in the database.

Before the subsystem application can be added to the database, the EAGLE 5 ISS true point code and the subsystem number must be in the mated application table. The EAGLE 5 ISS true point code is verified with the `rtrv-sid` command and shown in the `PCA` field. The mated application table is displayed with the `rtrv-map` command. The EAGLE 5 ISS true point code is shown in the `PCA` field of the `rtrv-map` command output and the subsystem number is shown in the `SSN` field of the `rtrv-map` command output. If the EAGLE 5 ISS's true point code and the subsystem number are not shown in the `rtrv-map` command output, perform one of the "Mated Application" procedure in the *Database Administration Manual – Global Title Translation* and add the EAGLE 5 ISS true point code and the subsystem to the database.

The example in this procedure reserves the subsystem number 254 for the LNP application and sets the LNP application online.

1. Verify that the LNP feature is enabled by entering the `rtrv-ctrl-feat` command.
 - If the LNP feature is enabled, the entry `LNP ported TNs` appears in the `rtrv-ctrl-feat` output with a quantity greater than 0. If the LNP feature is enabled, continue with [Step 2](#).
 - If the LNP feature is not enabled, perform the procedures in [LNP Feature Activation Procedure](#) to enable the LNP feature. Then continue with [Step 2](#).
2. Display the subsystem number for the LNP application in the database with the `rtrv-ss-appl` command.
3. Display the EAGLE 5 ISS true point code using the `rtrv-sid` command.

The EAGLE 5 ISS true point code is shown in the `PCA` field of the `rtrv-sid` output.
4. Display the mated applications using the `rtrv-map` command specifying the EAGLE 5 ISS true point code (shown in [Step 3](#)) and the LNP subsystem number.

For this example, enter the following command:

```
rtrv-map:pca=100-100-100:ssn=254
```
5. Add the subsystem number for the LNP application using the `ent-ss-appl` command.

For this example, enter the following command:

```
ent-ss-appl:appl=lnp:ssn=254:stat=online
```
6. Verify the changes with the `rtrv-ss-appl` command.
7. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

The following messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED): MASP A - Backup starts on standby MASP.
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Removing a Subsystem Application

This procedure is used to remove a subsystem application from the database using the `dlt-ss-appl` command. The `dlt-ss-appl` command uses only one parameter:

`:appl` – the subsystem application, LNP .

The subsystem application must be in the database, and the subsystem must be out of service.

1. Display the status of the LNP subsystem with the `rept-stat-lnp` command.
2. Display the subsystem application number for the LNP application in the database with the `rtrv-ss-appl` command.
3. Place the LNP subsystem application out of service with the `inh-map-ss` command specifying the LNP subsystem number displayed in [Step 2](#).

For this example, enter this command.`inh-map-ss:ssn=254`

4. Verify that the LNP subsystem is out of service with the `rept-stat-lnp` command.
5. Remove the LNP subsystem application from the database using the `dlt-ss-appl` command.

For this example, enter this command.`dlt-ss-appl:appl=lnp`

When the command has successfully completed, the following message appears.

```
rlghncxa03w 09-04-05 17:34:20 EST EAGLE 41.0.0
DLT-SS-APPL: MASP A - CAUTION: DELETED APPL SSN MAY BE REFERENCED BY GTT ENTRY
DLT-SS-APPL: MASP A - COMPLTD
;
```

6. Verify the changes with the `rtrv-ss-appl` command.
7. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

The following messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED): MASP A - Backup starts on standby MASP.
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Increasing the LRN and NPANXX Quantities on the EAGLE

When the LNP feature is enabled for the first time for a quantity less than 240 million numbers, the LRN (Location Routing Number) and NPANXX quantities are set at 100,000 LRNs and 150,000 NPANXXs.

When the LNP quantity is 60-228 million numbers, the LRN and NPANXX quantities can be increased to 150,000 LRNs and 300,000 NPANXXs. The procedure in this section explains how to increase the quantities. (To increase the current LNP quantity, see the [Increasing LNP Telephone Number Quantity on EAGLE](#) procedure.)

When the LNP telephone number quantity is 240-384 million numbers, the LRN and NPANXX quantities are automatically increased to 200,000 LRNs and 350,000 NPANXXs. No action is necessary for the increase.

The current assigned quantities can be verified by entering the `rtrv-ctrl-feat` command.

The LRN and NPANXX quantities are increased using the `enable-ctrl-feat` command to specify the Feature Access Key (FAK) and part number of the desired LRN quantity feature (part number 893010501) and the NPANXX quantity feature (part number 893009402). The Feature Access Key (FAK), which is provided when the feature is purchased, is based on the feature part number and the serial number of the EAGLE, which means that the Feature Access Key (FAK) is site-specific.

To fully use the increased LRN and NPANXX quantities for 60-384 million LNP numbers, the Measurements Platform must be configured on the EAGLE. If the Measurements Platform is not configured, the measurements for LRNs are capped at 100,000 LRNs, and the measurements for NPANXXs are capped at 150,000 NPANXXs. Measurements for LRN and NPANXX quantities beyond 100,000 LRNs and 150,000 NPANXXs will be truncated. To configure the Measurements Platform, refer to the procedures in *Database Administration - System Management User's Guide*.

1. Display the status of the LNP-related features. Enter the `rtrv-ctrl-feat` command and verify the entries for LRN and NPANXX quantities:
 - If the `rtrv-ctrl-feat` output shows that the LRN quantity is 150,000, and the NPANXX quantity is 300,000, no further action is necessary. This procedure cannot be performed.
 - If the `rtrv-ctrl-feat` output shows that the LRN quantity is 200,000, and the NPANXX quantity is 350,000, no further action is necessary. This procedure cannot be performed.
 - If the LNP ported TNs quantity shown in the `rtrv-ctrl-feat` output is 48000000 or less, see [Increasing LNP Telephone Number Quantity on EAGLE](#) to increase the LNP telephone number quantity to 60000000 or greater. Then continue with [Step 2](#).
2. Verify the NPANXX and LRN quantities on the ELAP.

Perform the [Verifying RTDB Status at the ELAP User Interface](#) procedure.

The number of NPANXXs and LRNs on the ELAP must be less than the configured quantity on the EAGLE. If either the NPANXX and LRN quantity on the ELAP is greater than the quantity shown in the `rtrv-ctrl-feat` output, the ELAP RTDB is not loaded onto the entire set of Service Module cards on the EAGLE. Some of the Service Module cards load the ELAP RTDB to provide a restricted level of GTT/LNP service. The remainder of the Service Module cards are put into a restricted state.

UIM 1324 is generated at the EAGLE if the NPANXX quantity on the ELAP is greater than the NPANXX quantity configured on the EAGLE.

UIM 1325 is generated at the EAGLE if the LRN quantity on the ELAP is greater than the LRN quantity configured on the EAGLE.

To avoid this situation, make sure when performing this procedure that the NPANXX and LRN quantities configured on the EAGLE are greater than the NPANXX and LRN quantities on the ELAP. If the NPANXX and LRN quantity on the ELAP is less than the quantity shown in the `rtrv-ctrl-feat` output in [Step 1](#), or is less than the quantity that will be configured in this procedure, continue with [Step 3](#).

3. Verify whether or not the Measurements Platform is functioning on the EAGLE.

Enter the `rtrv-feat` command. If the Measurements Platform feature is on, the `measplat=on` entry appears in the command output.

Enter the `rtrv-measopts` command. If Measurements Platform collection is enabled, the `PLATFORMENABLE = on` entry appears in the output.

Note: The `rtrv-measopts` command output contains other fields that are not used by this procedure. To see all the of the fields that are displayed by the `rtrv-measopts` command, refer to the `rtrv-measopts` command description in *Commands User's Guide*.

If Measurements Platform collection is not enabled, perform the procedure in *Database Administration - System Management User's Guide* to configure the Measurements Platform.

4. Increase the LRN and NPANXX quantities by entering these commands.

```
enable-ctrl-feat:partnum=893010501:fak=<LRN Quantity Feature Access Key>
```

```
enable-ctrl-feat:partnum=893009402:fak=<NPANXX Quantity Feature Access Key>
```

The Feature Access Key (FAK) is provided when the feature is purchased. If you do not have the Feature Access Key for the desired quantity, contact [My Oracle Support \(MOS\)](#).

5. Verify the changes by entering these commands.

```
rtrv-ctrl-feat:partnum=893010501. The following is an example of the possible output.
```

```
rtrv-ctrl-feat:partnum=893009402. The following is an example of the possible output.
```

6. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

Activating the LNP Local Subsystem

The procedure in this section explains how to activate the LNP local subsystem.

When all configuration is complete for the feature or features, the LNP subsystem application must taken online and the local subsystem must be activated to allow it to begin operation.

When the local subsystem operating state is Inhibited, the `chg-ss-appl:appl=lnp` command can be used to specify the value online or the value offline to control the persistent setting for the local subsystem. The `rtrv-ss-appl` command always displays the online or offline provisioned value. When the first Service Module card is loaded, this state tells whether the subsystem should be considered allowed (online) or inhibited (offline). This is a database state. If the command is accepted, then the change is made to the tables and can be read after an `init-sys` command is entered to initialize the system.

When the Service Module cards are in-service and the subsystem application is online, the `alw/inh-map-ss` commands can be used to change the dynamic operating state of the local subsystem. The `inh-map-ss` command does not necessarily force a state change, because it can fail if the mate does not send SOG. The `force=yes` parameter must be specified to bypass the SOR/SOG exchange and inhibit immediately. (There is no `rtrv-map-ss` command.)

The procedures in [Changing the State of a Subsystem Application](#) explain how to take a local subsystem online and offline.

Table 21: Subsystem Allow/Inhibit

Command\ Subsystem State	Offline	Online
<code>alw-map-ss</code>	Command is rejected.	Attempts to make the local subsystem active.
<code>inh-map-ss</code>	Command accepted, but no action because offline implies inhibited.	Attempts to inhibit the local subsystem. Use of the <code>force=yes</code> parameter bypasses the SOR/SOG exchange and inhibits immediately.
<code>chg-ss-appl :appl=lnp :nstat=online</code>	Command is rejected, because the subsystem must be online to be in the allowed state.	Changes local subsystem database status to online.
<code>chg-ss-appl :appl=inp :nstat=offline</code>	Command is rejected because the subsystem must be inhibited to go offline.	Changes local subsystem database status to offline.

1. Display the status of the LNP subsystem application, by entering the `rtrv-ss-appl` command.

```
tekelecstp 07-07-25 08:02:22 EST EAGLE 37.6.0
APPL  SSN  STAT
LNP    11   offline

SS-APPL TABLE IS 25% FULL (1 OF 4)
;
```

2. Change the LNP subsystem to status to online.
`chg-ss-appl:appl=lnp:nstat=online`
3. Enter the command to allow the INP subsystem to begin operation.
`alw-map-ss:ssn=<LNP ssn>`

```
integrat40 00-05-24 10:37:22 EST EAGLE5 37.6.0
Allow map subsystem command sent to all SCCP cards.
```

```
Command Completed.
;
```

4. Display the operating status of the LNP subsystem, by entering the `rept-stat-sccp` command.

Changing the State of a Subsystem Application

The procedures in this section are used to set the state of an existing subsystem application to either online or offline using the `chg-ss-appl` command. The `chg-ss-appl` command uses the following parameters..

`:appl` – the application type, LNP

`:nstat` - the new state of the subsystem application.

The online or offline status of the subsystem application is shown in the STAT field of the `rtrv-ss-appl` command output.

The `rept-stat-lnp` command displays the operating state (in or out of service) of the subsystem.

If the subsystem application is to be taken online, the subsystem application must be offline.

If the subsystem application is to be taken offline, the subsystem application must be online. The subsystem must be taken out of service (OOS-MT-DSBLD) with the `inh-map-ss` command before it can be taken offline.

Taking the Subsystem Application Online

Use the procedure in this section to take the subsystem application online.

1. Verify the state of the subsystem application - online or offline, by entering the `rtrv-ss-appl` command.

```
tekelecstp 08-07-25 08:02:22 EST EAGLE 39.2.0
APPL  SSN  STAT
LNP    11  offline

SS-APPL TABLE IS 25% FULL (1 OF 4)
;
```

If the LNP subsystem is online, this procedure does not need to be performed.

2. Display the operating status of the subsystem by entering the `rept-stat-lnp` command.
3. Take the subsystem application online. Enter the `chg-ss-appl` command with the `nstat=online` parameter.
`chg-ss-appl:appl=lnp:nstat=online`
4. Verify the changes by entering the `rtrv-ss-appl` command.

```
tekelecstp 08-07-25 08:02:22 EST EAGLE 39.2.0
APPL  SSN  STAT
LNP    11  online

SS-APPL TABLE IS 25% FULL (1 OF 4)
;
```

5. Back up the new changes using the `chg-db:action=backup:dest=fixed` command.

The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED): MASP A - Backup starts on standby MASP.
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Taking the Subsystem Application Offline

Use the procedure in this section to take a subsystem application offline.

1. Verify the online or offline state of the subsystem application, by entering the `rtrv-ss-appl` command.

```
tekelecstp 08-07-25 08:02:22 EST EAGLE 39.2.0
APPL  SSN  STAT
LNP    11  online

SS-APPL TABLE IS 25% FULL (1 OF 4)
;
```

If the LNP subsystem application is offline, this procedure does not need to be performed.

2. Verify the operating status of the subsystem by entering the `rept-stat-sccp` command.
3. Place the subsystem out of service. Specify the subsystem number displayed in the output in [Step 1](#).

```
inh-map-ss:ssn=11
```

```
rlghncxa03w 08-06-28 14:42:38 GMT EAGLE 39.2.0
LNP Subsystem has been inhibited.
Command Completed.
;
```

4. Verify that the subsystem is out of service, by entering the `rept-stat-lnp` command.
5. Take the subsystem offline. Enter the `chg-ss-appl` command with the `nstat=offline` parameter.
`chg-ss-appl:appl=inp:nstat=offline`
6. Verify the changes by entering the `rtrv-ss-appl` command.

```
tekelecstp 08-07-25 08:02:22 EST EAGLE 39.2.0
APPL  SSN  STAT
LNP    11  offline

SS-APPL TABLE IS 25% FULL (1 OF 4)
;
```

7. Back up the new changes using the `chg-db:action=backup:dest=fixed` command.

The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED): MASP A - Backup starts on standby MASP.
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Increasing LNP Telephone Number Quantity on EAGLE

Note: Use this procedure only if the LNP ELAP Configuration feature is enabled and turned on and an LNP quantity feature is enabled. Enter the `rtrv-ctrl-feat` command, and verify that an LNP ported TNS entry appears in the output. If the LNP ported TNS entry is not in the output, do not perform this procedure but go to [LNP Feature Activation Procedure](#) to enable and turn on the LNP ELAP Configuration feature and enable the LNP feature.

This procedure is used to increase the current quantity of LNP telephone numbers in the EAGLE using the `enable-ctrl-feat` command specifying the Feature Access Key (FAK) and part number of the desired LNP telephone number quantity. The current LNP telephone number quantity is shown in the LNP ported TNS entry in the `rtrv-ctrl-feat` command output.

If the current LNP ported TNS quantity is 384 million numbers, this procedure cannot be performed. 384 million numbers is the maximum available quantity.

The Feature Access Key (FAK) is based on the LNP telephone number quantity part number and the serial number of the EAGLE, which means that the Feature Access Key is site-specific.

Note: After a specific LNP telephone number quantity is enabled with the `enable-ctrl-feat` command, that quantity cannot be reduced. The LNP feature cannot be turned off using the `chg-ctrl-feat` command, and cannot be enabled with a temporary Feature Access Key.

The LNP telephone number quantity must be purchased before you can enable that quantity with the `enable-ctrl-feat` command. If you are not sure if you have purchased the desired LNP telephone number quantity or do not have the Feature Access Key for the LNP telephone number quantity being enabled, contact [My Oracle Support \(MOS\)](#).



Caution: Make sure that the LNP telephone number quantity configured in this procedure is greater than the ELAP telephone number quantity. The ELAP telephone number quantity can be verified by performing the [Verifying RTDB Status at the ELAP User Interface](#) procedure. If the telephone number quantity on the ELAP is greater than the LNP telephone number quantity configured in this procedure, the ELAP RTDB is not loaded onto the entire set of Service Module cards on the EAGLE. Some of the Service Module cards load the ELAP RTDB to provide a restricted level of GTT/LNP service. The remainder of the Service Module cards are put into a restricted state. UIM 1323 is generated at the EAGLE.

1. Display the status of the controlled features in the system, by entering the `rtrv-ctrl-feat` command.

If the `rtrv-ctrl-feat` output shows that the LNP ELAP Configuration feature is not enabled or turned on, do not perform this procedure but go to [LNP Feature Activation Procedure](#) to enable and turn on the LNP ELAP Configuration feature and enable the LNP feature.

2. Display the status of the Service Module cards by entering the `rept-stat-sccp` command.
3. Enable the new LNP telephone number quantity using the `enable-ctrl-feat` command with the part number of the desired quantity and the Feature Access Key (FAK) for that quantity.
`enable-ctrl-feat:partnum=893011036:fak=<LNP Telephone Number Quantity Feature Access Key>`

Refer to the description of the `enable-ctrl-feat` command in *Commands User's Guide* for a list of the LNP quantity feature part numbers.

Note: The Feature Access Key (FAK) is provided when the feature is purchased. If you do not have the Feature Access Key for the desired LNP telephone number quantity, contact [My Oracle Support \(MOS\)](#).

- Verify the changes by entering the `rtrv-ctrl-feat` command with the part number specified in [Step 3](#).

```
rtrv-ctrl-feat:partnum=893011012
```

```
rlghncxa03w 10-05-01 21:16:37 GMT EAGLE5 42.0.0
The following features have been permanently enabled:
Feature Name          Partnum    Status    Quantity
LNP ELAP Configuration 893010901  on       ----
LNP ported TNs        893011036  on       384000000
```

- Back up the changes using the `chg-db:action=backup:dest=fixed` command. The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED): MASP A - Backup starts on standby MASP.
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

LNP Short Message Service Feature Configuration

This section describes the prerequisites and procedures for the configuration of the LNP Short Message Service (LNP SMS) feature.

[LNP Short Message Service \(LNP SMS\) Feature Configuration Procedure](#) lists the steps for enabling and turning on the LNP SMS feature, and for the provisioning required for the feature. Each step contains a link or reference to information and procedures to use to complete the step. Feature provisioning can be performed after the feature is enabled and before the feature is turned on.

Controlled features are optional and must be purchased from Oracle before they can be used in your system. If you are not sure whether you have purchased a specific feature, contact [My Oracle Support \(MOS\)](#).

LNP SMS Feature Prerequisites

Before the LNP SMS feature can be enabled, the following prerequisites are required in the system:

Table 22: LNP SMS Feature Prerequisites

Prerequisite	Verification and Provisioning
The LNP feature must be enabled in the system.	Enter the <code>rtrv-ctrl-feat</code> command. If the LNP feature is enabled, the LNP ported TNs entry appears in the command output, with a quantity greater than zero.

Prerequisite	Verification and Provisioning
	If the LNP feature is not enabled, perform the procedures in LNP Feature Activation Procedure to enable the LNP feature and make it fully operational in the system.
The Wireless Number Portability (WNP) feature must be on in the system, and the WNP service must be provisioned for the feature.	<p>Enter the <code>rtrv-feat</code> command.</p> <p>If the WNP feature is on, the <code>wnp = on</code> entry appears in the output.</p> <p>If the WNP feature is off (<code>wnp = off</code> appears in the output), perform the <code>x</code> to turn the WNP feature on and provision the WNP service.</p>

LNP Short Message Service (LNP SMS) Feature Configuration Procedure

The EAGLE 5 ISS configuration of the LNP SMS feature consists of the following steps. The steps contain links and references to detailed procedures and information needed to complete each step.

1. Verify, and provision if needed, the feature prerequisites. See [LNP SMS Feature Prerequisites](#).
2. Display the status of the LNP Short Message Service feature by entering the `rtrv-ctrl-feat` command.

```
rlghncxa03w 07-08-01 21:15:37 GMT EAGLE5 37.0.0
The following features have been permanently enabled:
Feature Name      Partnum    Status    Quantity
LNP Short Message Service 893006601  on        ----
```

The LNP SMS feature can be temporarily enabled for a trial period, using part number 893006699 and a feature access key for that part number. If the feature will continue to be used after evaluating the trial results or after the trial period expires, the feature must then be permanently enabled.

The LNP SMS feature can be permanently enabled using part number 893006601 and a feature access key for that part number.

- If the `rtrv-ctrl-feat` output shows that the LNP Short Message Service feature is permanently enabled and the Status is on, no further action is necessary. This procedure does not need to be performed.
- If the LNP Short Message Service feature is permanently enabled and the Status is off, go to [Step 4](#) to turn on the feature and continue with the configuration process.
- If the LNP SMS feature is temporarily enabled, the Status is on, and the trial period has not expired and needs to continue, no further action is necessary.

The `rtrv-ctrl-feat` command output shows the remaining time in the trial period if the period has not expired. If the trial period has expired, the feature is shown in the list of features with an expired temporary key, and an alarm is generated. The alarm can be cleared either by using the `chg-ctrl-feat` command or by permanently enabling the feature.

- If the LNP Short Message Service feature is temporarily enabled but has not been turned on (Status is off), go to [Step 4](#).

- If the LNP Short Message Service feature is temporarily enabled and you want to permanently enable the feature (the temporary trial period for the feature has expired or the trial evaluation is complete), continue with [Step 3](#) to permanently enable the feature..
3. Enable the LNP Short Message Service feature.
 - To permanently enable the feature, enter the `enable-ctrl-feat` command with part number 893006601 and the feature access key for that the permanent part number.
 - To temporarily enable the feature, enter the `enable-ctrl-feat` command with part number 893006699 and the feature access key for the temporary part number.
 4. Turn on the LNP Short Message Service feature. enabled in step 3 must be activated using the `chg-ctrl-feat` command, specifying the controlled feature part number used in step 3 and the `status=on` parameter.
 - To turn on the permanently enabled feature, enter the `chg-ctrl-feat` command with part number 893006601 and the `status=on` parameter.
 - To turn on the temporarily enabled feature, enter the `chg-ctrl-feat` command with part number 893006699 and the `status=on` parameter.
 5. Verify the changes by entering the `rtrv-ctrl-feat` command with the LNP Short Message Service feature permanent or temporary feature part number.
 6. Add the Wireless Short Message Service Center (`serv=wsmc`) to the LNP Service table. Perform the [Adding an LNP Service](#) procedure for the wsmc service. Then continue with .
 7. Provision the WSMSC10DIC and WQREDRCT LNP configuration options for the WNP feature. Perform the [Changing LNP Options](#) procedure for the two options. Then continue with x.
 8. Back up the changes using the `chg-db:action=backup:dest=fixed` command. These messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

Turning Off the LNP Short Message Service Feature

This procedure is used to turn off the LNP Short Message Service feature, using the `chg-ctrl-feat` command.

Note:

If the LNP Short Message Service feature is deactivated, the WSMSC LNP service cannot be used for local number portability.

1. Display the controlled features whose status is on by entering the `rtrv-ctrl-feat:status=on` command.

```
rlghncxa03w 07-08-01 21:15:37 GMT EAGLE5 37.0.0
The following features have been permanently enabled:
```

Feature Name	Partnum	Status	Quantity
LNP Short Message Service	893006601	on	----

2. Turn off the LNP Short Message Service feature.

To turn off the feature that is temporarily enabled, enter the `chg-ctrl-feat` command with the `partnum=893006699` and `status=off` parameters.

To turn off the feature that is permanently enabled, enter the `chg-ctrl-feat` command with `partnum=893006601` and `status=off` parameters.

3. Verify that the LNP Short Message Service feature has been turned off by entering the `rtrv-ctrl-feat:` command, with part number 894006699 if the feature is temporarily enabled or part number 893006601 if the feature is permanently enabled.

```
rlghncxa03w 07-08-01 21:16:37 GMT EAGLE5 37.0.0
The following features have been permanently enabled:
Feature Name      Partnum      Status      Quantity
LNP Short Message Service 893006601  off        ----
```

4. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

These messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

Clearing a Temporary FAK Alarm

This procedure is used to clear the critical alarm that is generated when the trial period is about to expire (UAM 0367) or expires (UAM 0368) for a temporarily enabled controlled feature has expired.

The controlled feature must have been temporarily enabled and is now in danger of expiration or in an *expired* state.

1. Display the enabled controlled features by entering the `rtrv-ctrl-feat` command.

The command output lists the features for which the trial period will soon expire and the features for which the trial period has expired.

```
rlghncxa03w 07-08-01 21:17:37 GMT EAGLE5 37.0.0
The following features have expired temporary keys:
Feature Name      Part Num
LNP Short Message Service 893006601
```

2. Clear the EAGLE 5 ISS alarm in the database by entering the `chg-ctrl-feat` command with the feature part number parameter and the `alarm=clear` parameter.

The following alarm is generated to indicate that the original alarm is cleared.

```
rlghncxa03w 07-08-01 21:16:37 GMT EAGLE5 37.0.0
0366.0181 * SYSTEM Temp Key(s) expiration alarm cleared.
```

3. Verify that the alarm has cleared in the database by entering the `rtrv-ctrl-feat:` command.
4. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

ITU TCAP LRN Query (LRNQT) Feature Configuration

This section describes the prerequisites and procedures for the configuration of the ITU TCAP LRN Query (LRNQT) feature.

[ITU TCAP LRN Query \(LRNQT\) Feature Configuration Procedure](#) lists the steps for enabling and turning on the LRNQT feature, and for the provisioning required for the feature. Each step contains a link or reference to information and procedures to use to complete the step. Feature provisioning can be performed after the feature is enabled and before the feature is turned on.

Controlled features are optional and must be purchased from Oracle before they can be used in your system. If you are not sure whether you have purchased a specific feature, contact [My Oracle Support \(MOS\)](#).

LRNQT Feature Prerequisites

Before the LRNQT feature can be enabled, the following prerequisites are required in the system:

Table 23: LRNQT Feature Prerequisites

Prerequisite	Verification and Provisioning
The LNP feature must be enabled in the system.	<p>Enter the <code>rtrv-ctrl-feat</code> command.</p> <p>If the LNP feature is enabled, the LNP ported TNs entry appears in the command output, with a quantity greater than zero.</p> <p>If the LNP feature is not enabled, perform the procedures in LNP Feature Activation Procedure to enable the LNP feature and make it fully operational in the system.</p>

Prerequisite	Verification and Provisioning
TT Independence cannot be used in the system.	Enter the <code>rtrv-lnp-serv</code> command. If the <code>lnpqs</code> service is provisioned,

ITU TCAP LRN Query (LRNQT) Feature Configuration Procedure

This procedure is used to configure the LRNQT feature to allow the LNP platform to handle queries with the TCAP portion encoded as per ITU standards. This feature uses existing LNP subsystems.

The feature is enabled using the `enable-ctrl-feat` command with feature part number 893026301 and the Feature Access Key (FAK). The Feature Access Key, which is provided when the feature is purchased, is based on the feature part number and the serial number of the EAGLE, which means that the Feature Access Key (FAK) is site-specific.

The feature cannot be enabled with a temporary Feature Access Key. After the LRNQT feature is enabled, it must be turned on using the `chg-ctrl-feat` command with the feature part number and the `status=on` parameter. The LRNQT feature cannot be turned off.

This procedure contains the basic steps necessary to configure the LRNQT feature. Some of these basic steps refer to detailed procedures contained elsewhere in this guide.

1. Verify, and provision if necessary, the LRNQT feature prerequisites. See [LRNQT Feature Prerequisites](#).
2. Configure the system's True Point Code (ANSI point code) (`pca`) and Capability Point Code (`cpc`) using the `chg-sid` command.



CAUTION

Caution: Changing a system's point code requires a system reboot using the `init-sys` command to fully implement the changes. The `init-sys` command causes a complete system reload and should be used only in an environment that is not in service. Using this command ensures the updated self identification information is loaded onto all cards but does interrupt service.

- a) Change the true point code using `chg-sid:pca=<ANSI point code>`
 - b) Add a new LNP-type Capability Point Code (`cpc`) using `chg-sid:cpctype=lnp:cpc=<lnp capability point code>`
- When any of the `pca` or `cpc` parameters change, the following caution message indicates that the system needs to be reinitialized.

CAUTION: SYSTEM SITE ID HAS BEEN CHANGED, MANUAL RE-INITIALIZATION IS NEEDED



CAUTION

Caution: The `init-sys` command causes a complete system reload and should be used only in an environment that is not in service. Using this command ensures the updated self identification information is loaded on to all cards, but does interrupt service. When the `init-sys` command executes, the system does not retain the manually initiated state (for example, OOS-MT-DSBLD) for the signaling link card, or terminal. After the command executes, the system attempts to bring all provisioned links, cards, and terminals on line, including those that were previously out of service. You will need to manually put each device back into its previous state after the system is back on line. Print or electronically capture the output of the `rept-stat-slk`, `rept-stat-card`, and `rept-stat-trm` commands for reference prior to issuing

the `init-sys` command. To restore a device to its previous state, issue the appropriate inhibit/deactivate command listed in *Commands User's Guide* in the Related Commands section for each of the above `rept-stat` commands.

3. Add a MATED application using True Point Codes using the `ent-map` command.

```
ent-map:pc=<ANSI point code>:ssn=<lnp subsystem number>:rc=<relative
cost>:mpc=<mate ANSI point code>:mssn=<lnp subsystem number>:materc=<mate
relative cost>
```

4. Place the LNP subsystem offline using the `ent-ss-appl` command.

```
ent-ss-appl:appl=lnp:ssn=<lnp subsystem number>:stat=offline
```

5. Enable the LRNQT feature. Enter the `enable-ctrl-feat` command with part number 893026301 and the Feature Access Key.

Note: The Feature Access Key is provided when the feature is purchased. If you do not have the Feature Access Key for the LRNQT feature, contact [My Oracle Support \(MOS\)](#).

6. Turn on the LRNQT feature. Enter the `chg-ctrl-feat` command with part number 893026301 and the `status=on` parameter.

7. Route the final global title translation (GTT) to the EAGLE point code and LNP local subsystem.

Refer to the procedures in *Database Administration - GTT User's Guide*.

Note: Directing the DPC/SSN routing to the EAGLE PC and LNP local subsystem number is handled on the network card. No provisioning is required.

8. Activate the LNP subsystem.

- a) Place the LNP subsystem online

```
chg-ss-appl:appl=lnp:nstat=online
```

- b) Allow the LNP subsystem to be active in the system.

```
alw-map-ss:ssn=<lnp subsystem number>
```

9. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

Triggerless LNP Feature Configuration

This procedure is used to configure the Triggerless LNP (TLNP) feature.

Prerequisites and Requirements

Steps in this procedure explain how to verify that the following prerequisites and requirements are present or how to provide them in the system:

- Before the TLNP feature can be turned on, the LNP feature must be enabled in the system.
- The Gateway Screening feature is used to capture the IAM messages that are converted for the TLNP feature. The Gateway Screening (GWS) feature must be turned on and the database must contain a gateway screening screen set that contains the following items:
 - An allowed SIO screen that allows ISUP messages into the EAGLE. ISUP messages are MSUs that contain the value 5 in the Service Indicator field (SI=5) of the Service Information Octet (SIO) of the MSU.
 - The gateway screening stop action `tlnp`. The gateway screening stop actions can be verified with the `rtrv-gws-actset` command.

Steps in the procedure in this section refer to procedures in *Database Administration - GWS User's Guide* to turn on the GWS feature, and to configure Gateway Screening with the required screen set in the database.

Note: It is recommended that the screening for ISUP messages allowed into the EAGLE stop at either the Allowed SIO, Allowed DPC, Blocked DPC, or Allowed ISUP screens. Screening on these messages can continue to the Allowed DESTFLD, Allowed CGPA, Allowed TT, Allowed CDPA, or Allowed AFTPC screens, but these screens do not contain any screenable criteria contained in an ISUP message. After these messages are passed on to the Allowed DESTFLD or Allowed CGPA screens, they will continue to be passed during the gateway screening process until the gateway screening process stops.

When the IAMs are converted, a Jurisdiction Indicator Parameter (JIP) is added to the IAM message after RTDB lookup if the Jurisdiction Information Parameter does not exist in original IAM message and either:

- The `jipprv` configuration option value in the LNPOPTS table is set to yes.
- A valid Calling Party Number exists in the original IAM message.

The following JIP configuration options can be provisioned in the LNPOPTS table after the TLNP feature has been turned on:

- `jipprv` – Indicates whether or not a Jurisdiction Information Parameter value is to be added to the IAM.
- `jipdigits` – The value of the Jurisdiction Information Parameter as a 6-digit number.

Canceling the RTRV-LS Command

Because the `rtrv-ls` command used in this procedure can display information for a long period of time, the `rtrv-ls` command can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-ls` command can be canceled.

- Press the F9 function key on the keyboard at the terminal where the `rtrv-ls` command was entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-ls` command was entered.
- From another terminal other than the terminal where the `rtrv-ls` command was entered, enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-ls` command was entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration

commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

Refer to *Commands User's Guide* for a complete description of the `canc-cmd` command, including parameters and valid parameter values, rules for using the command correctly, and output examples.

1. Display the FAK-controlled features that are enabled in the system. Enter the `rtrv-ctrl-feat` command.

The LNP feature must be enabled and the ISUP NP with EPAP cannot be enabled before the TLNP feature can be turned on.

- If the ISUP NP with EPAP feature is enabled, this procedure cannot be performed. Contact your [My Oracle Support \(MOS\)](#) for assistance.
- If the LNP feature is enabled (an `LNP ported TNS` entry appears in the output), continue with [Step 2](#).
- If the LNP feature is not enabled, perform the procedures in [LNP Feature Activation Procedure](#) to enable the LNP feature and make it fully operational in the system. Then continue with [Step 2](#).

2. Display the status of the TLNP feature. Enter the `rtrv-feat` command.

- If the TLNP feature is off (`tlnp = off` appears in the output), continue with [Step 3](#).
- If the TLNP feature is on (`tlnp = on` appears in the output), go to [Step 5](#).

3. Turn on the TLNP feature. Enter the `chg-feat:tlnp=on` command.

After the TLNP feature is turned on with the `chg-feat` command, it cannot be turned off.

The TLNP feature must be purchased before you turn on the feature with the `chg-feat` command. If you are not sure if you have purchased the TLNP feature, contact [My Oracle Support \(MOS\)](#).

4. Verify the status of the TLNP feature. Enter the `rtrv-feat` command.

The `tlnp=on` entry appears in the output when the feature is on.

5. Display the Jurisdiction Information Parameter configuration option values in the LNPOPTS table. Enter the `rtrv-lnpopts` command.

- If the Jurisdiction Information Parameter option values do not need to change, go to [Step 7](#).
- To change the Jurisdiction Information Parameter option values, enter the `chg-lnpopts` command with the desired values for the `jipprv` and `jipdigits` parameters. Then continue with [Step 6](#).

6. Verify the LNPOPTS changes. Enter the `rtrv-lnpopts` command.

7. Display the status of the Gateway Screening (GWS) feature. Enter the `rtrv-feat` command.

After the Gateway Screening feature is turned on with the `chg-feat` command, it cannot be turned off.

The Gateway Screening feature must be purchased before you turn the feature on with the `chg-feat` command. If you are not sure if you have purchased the Gateway Screening feature, contact [My Oracle Support \(MOS\)](#).

- If the Gateway Screening feature is on (`gws = on` appears in the output), continue with [Step 8](#).

- If the Gateway Screening feature is off (gws = off appears in the output), refer to the procedures in *Database Administration - GWS User's Guide* to verify that the required cards for GWS are equipped and to turn on the GWS feature. Then continue with [Step 8](#).
8. Display the GWS stop actions that are provisioned in the database. Enter the `rtrv-gws-actset` command.

The TLNP feature requires a gateway screening stop action set with the `tlnp` gateway screening stop action. The `tlnp` gateway screening stop action is shown by the entry `tlnp` in the `rtrv-gws-actset` command output.

```
rlghncxa03w 07-08-07 00:57:31 GMT EAGLE5 37.0.0
ACT  ACT      ACT  ACT  ACT  ACT  ACT  ACT  ACT  ACT  ACT  ACT
ID   NAME      1    2    3    4    5    6    7    8    9    10
--   --
1    copy      copy
2    rdct      rdct
3    cr        copy rdct
4    crcncf    copy cncf rdct
5    cncf      cncf
6    cfrd      cncf rdct
7    tlnp      tlnp
8    cptlnp    copy tlnp
GWS action set table is (8 of 16) 38% full
```

There can be only 2 TLNP GWS stop action sets, one with ACT1=TLNP and another with ACT1=COPY and ACT2=TLNP.

- If 2 TLNP GWS stop actions appear in the output, continue with [Step 9](#).
 - If 1 TLNP GWS stop action appears in the output and a second one is needed, use the "Configuring TLNP Gateway Screening Stop Action Sets" procedure in the *Database Administration - GWS User's Guide* to configure the second stop action set. Then continue with [Step 9](#).
 - If the `chg-feat` command was used to turn on the Gateway Screening feature in 4 (no TLNP stop actions appear in the output), go to [Step 13](#).
9. Display Allowed SIO screens with SI=5. Enter the `rtrv-scr-sio:si=5` command.
 - If no entries are shown, go to [Step 13](#) to create a new screen set.
 - If entries are shown, continue with [Step 10](#).
 10. Display the screen sets that contain the desired Allowed SIO screen. Enter the `rtrv-scrset:nsr=<SR value of the Allowed SIO screen>` command.
 11. Display all of the screens in one of the screen sets shown in [Step 10](#). Enter the `rtrv-scrset:scrn=<SCRN value>` command, with the SCR value shown in [Step 10](#).
 - To use the displayed screen set with all of the screens that are shown, continue with [Step 12](#).
 - If you do not want to use the displayed screen set, display another screen set. until you find the screen set that you want to use. Then continue with [Step 12](#).
 12. Display the last screen in the screen set.

Enter one of the commands shown in [Table 24: Commands to Display the Last Screen in a GWS Screen Set](#), based on the NSFI value of the last screen, with the name of the screen that is shown in the NSR/ACT column.

Table 24: Commands to Display the Last Screen in a GWS Screen Set

NSFI Value	Command
OPC	rtrv-scr-opc:sr-<screen name>
BLKOPC	rtrv-scr-blkopc:sr-<screen name>
SIO	rtrv-scr-sio:sr-<screen name>
DPC	rtrv-scr-dpc:sr-<screen name>
BLKDPC	rtrv-scr-blkdpc:sr-<screen name>
DESTFLD	rtrv-scr-destfld:sr-<screen name>
ISUP	rtrv-scr-isup:sr-<screen name>
CGPA	rtrv-scr-cgpa:sr-<screen name>
TT	rtrv-scr-tt:sr-<screen name>
CDPA	rtrv-scr-cdpa:sr-<screen name>
AFTPC	rtrv-scr-aftpc:sr-<screen name>

- If the screen contains the TLNP GWS stop action, go to [Step 14](#).
- If the screen does not contain the TLNP GWS stop action, go to the in *Database Administration - GWS User's Guide* and perform the appropriate procedure listed in [Table 25: Procedures for Changing GWS Screens to include the TLNP Stop Action](#), to assign the TLNP GWS stop action to the screen. Then go to [Step 14](#).

Table 25: Procedures for Changing GWS Screens to include the TLNP Stop Action

NSFI Value	Procedure
OPC	Changing an Allowed OPC Screen
BLKOPC	Changing an Allowed BLKOPC Screen
SIO	Changing an Allowed SIO Screen
DPC	Changing an Allowed DPC Screen
BLKDPC	Changing an Allowed BLKDPC Screen
DESTFLD	Changing an Allowed DESTFLD Screen
ISUP	Changing an Allowed ISUP Screen
CGPA	Changing an Allowed CGPA Screen
TT	Changing an Allowed TT Screen
CDPA	Changing an Allowed CDPA Screen
AFTPC	Changing an Allowed AFTPC Screen

13. Create a new screen set.

Go to *Database Administration - GWS User's Guide* and perform the procedures listed in [Table 26: Procedures to Create a GWS Screen Set with a TLNP Stop Action](#) as needed, to create a screen set the contains an Allowed SIO screen with the Service Indicator value 5 (SI=5).

Then continue with [Step 14](#).

Table 26: Procedures to Create a GWS Screen Set with a TLNP Stop Action

GWS Entity	Procedure
A screen set	Adding a Screen Set
An Allowed OPC screen	Adding an Allowed OPC screen
A Blocked OPC screen	Adding a Blocked OPC screen
An Allowed SIO screen	Adding an Allowed SIO screen
An Allowed DPC screen	Adding an Allowed DPC screen
A Blocked DPC screen	Adding a Blocked DPC screen
An Allowed ISUP screen	Adding an Allowed ISUP screen
Adding a TLNP GWS Stop Action	Configuring TLNP Gateway Screening Stop Action Sets

14. Display the linksets that are provisioned in the database. Enter the `rtv-ls` command.

- If the linkset that will screen messages for the TLNP feature is shown in the output and the screen set specified in [Step 10](#) is assigned to the linkset, go to last.
- If the linkset that will screen messages for the TLNP feature is shown in the output and the screen set specified in [Step 10](#) is not assigned to the linkset, go to the indicated manuals and perform the procedures listed in [Table 27: Procedures to Assign a Screen Set to a Linkset for TLNP](#) as required, to assign the screen set to the linkset.

Then continue with [Step 15](#).

Table 27: Procedures to Assign a Screen Set to a Linkset for TLNP

Procedure	In Manual
Changing an SS7 Linkset	<i>Database Administration - SS7 User's Guide</i>
Changing an IPGWx Linkset	<i>Database Administration - IP7 User's Guide</i>
Changing an IPSG M3UA Linkset	<i>Database Administration - IP7 User's Guide</i>
Changing an IPSG M2PA Linkset	<i>Database Administration - IP7 User's Guide</i>

- If the linkset that will screen messages for the TLNP Feature is not shown in the output, go to the indicated manuals and perform the required procedures that are listed in [Table 28: Procedures to Create a Linkset and Assign a Screen Set to the Linkset for TLNP](#), to configure the required linkset and assign the screen set to the linkset.

Then continue with [Step 15](#).

Table 28: Procedures to Create a Linkset and Assign a Screen Set to the Linkset for TLNP

Procedure	In Manual
Adding an SS7 Linkset	<i>Database Administration - SS7 User's Guide</i>
Adding an IPSG M2PA Linkset	<i>Database Administration - IP7 User's Guide</i>
Adding an IPSG M3UA Linkset	<i>Database Administration - IP7 User's Guide</i>
Configuring an IPGWx Linkset	<i>Database Administration - IP7 User's Guide</i>

Note: When Gateway Screening is in the screen test mode, as defined by the linkset parameters `gwsa=off` and `gwsn=on`, the gateway screening action in the gateway screening stop action set specified by the `actname` parameter of the gateway screening screen set at the end of the gateway screening process will be performed.

15. Back up the changes using the `chg-db:action=backup:deist=fixed` command.

The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED): MASP A - Backup starts on standby MASP.
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Configuring the Service Module Card Ethernet Link to the MPS

This procedure is used to configure the Ethernet link parameters for the Service Module cards using the `chg-ip-lnk` command. The `chg-ip-card` command is used to connect to the Virtual IP networks.

The `chg-ip-link` command uses the following parameters.

`:loc` – Card location. The location of the Service Module card.

`:port` – The Ethernet interface on the Service Module card, A or B.

`:ipaddr` – IP address assigned to the Ethernet interface on the Service Module card. This is an IP address expressed in standard “dot notation.” IP addresses consist of the system’s network number and the machine’s unique host number.

`:submask` – The subnet mask of the IP interface. A subnet mask is an IP address with a restricted range of values. The bits in the mask must be a string of one’s followed by a string of zeros. There must be at least two one’s in the mask, and the mask cannot be all one’s. See [Table 29: Valid Subnet Mask Parameter Values](#) to assign the correct parameter values.

`:auto` – Tells hardware whether to automatically detect the duplex and speed.

`:mactype` – This is the Media Access Control Type of the interface.

When a Service Module card is entered into the database, these values are automatically configured in the IP Link table for both Ethernet interfaces on the Service Module. If the values are not configured as listed below, you may need to change them.

- MACTYPE = DIX
- AUTO = YES
- MCAST = NO

The IPADDR and SUBMASK columns in the `rttrv-ip-lnk` output are shown as dashes. Each Ethernet link assigned to the Service Module card requires the IP address and submask of the MPS. The MCAST value for both Ethernet links must be `no` (`mcast=no`). No other values need to be changed.

A zero `ipaddr` parameter value (0.0.0.0) indicates the Service Module card Ethernet interface to the MPS is disabled.

The Service Module card must be placed out of service.

If either the `ipaddr` or `submask` parameters are specified, then both parameters must be specified. If the `ipaddr` parameter value is zero (0.0.0.0), the `submask` parameter is not required.

The A or B interface can be used with the Service Module card.

The value of the IP address specified for the `ipaddr` parameter is defined as follows:

- The first two octets of the IP address are 192.168. These are the first two octets for private class C networks as defined in RFC 1597.
- The third octet is configured, usually to the default value .120 for the main network (port A of the Service Module card) and the default value .121 for the backup network (port B of the Service Module card). These are not visible to any external networks, and should not need to be changed.
- The fourth octet of the address is selected as follows:
 - If the ELAP is configured as ELAP A, the fourth octet has a value of 100.
 - If the ELAP is configured as ELAP B, the fourth octet has a value of 200.

The `submask` parameter value is based upon the `ipaddr` setting. See [Table 29: Valid Subnet Mask Parameter Values](#) for the valid input values for the `submask` and `ipaddr` parameter combinations.

Table 29: Valid Subnet Mask Parameter Values

Network Class	IP Network Address Range	Valid Subnet Mask Values
A	1.0.0.0 to 127.0.0.0	255.0.0.0 (the default value for a class A IP address) 255.192.0.0 255.224.0.0 255.240.0.0 255.248.0.0 255.252.0.0 255.254.0.0

		255.255.128.1
A+B	128.1.0.0 to 191.255.0.0	255.255.0.0 (the default value for a class B IP address) 255.255.192.0 255.255.224.0 255.255.240.0 255.255.248.0 255.255.252.0 255.255.254.0 255.255.255.128
A+B+C	192.0.0.0 to 223.255.255.0	255.255.255.0 (the default value for a class C IP address) 255.255.255.192 255.255.255.224 255.255.255.240 255.255.255.248 255.255.255.252

The `chg-ip-card` command is used to provision IP networking parameters for the Service Module cards. The `chg-ip-card` command supports two parameters, `:bpipaddr` and `:bpsubmask`, that are allowed only if the Service Module card is in the inhibited state. The `:bpipaddr` and `:bpsubmask` parameters are used to implement bonded ports on the Service Module cards, which allow the A and B networks to be used as a single redundant network.

`:bpipaddr` – Bonded Port IP address. This parameter specifies an IP address for the Service Module card.

`:bpsubmask` – Bonded Port IP submask. The subnet values are the same as for the `chg-ip-link` values, shown in [Table 29: Valid Subnet Mask Parameter Values](#).

The `:bpsubmask` parameter must be specified if `:bpipaddr` is specified for `chg-ip-card`, and `:bpipaddr` must be specified or already have a valid value if a valid `:bpsubmask` is specified.

The `:bpipaddr` IP value must be unique among all IP cards and IP links.

When specifying `:bpipaddr` with a NULL network address, the `chg-ip-card` command will reset both `:bpipaddr` and `:bpsubmask`.

1. Display the current Ethernet link parameters associated with the Service Module card in the database by entering the `rtrv-ip-lnk` command.
2. Verify the status of the Service Module card being configured in this procedure using the `rept-stat-card` command.

For example, enter the command `rept-stat-card:loc=1301`.

- If the state of the Service Module card being configured in this procedure is in service-normal (IS-NR), continue with [Step 3](#) to inhibit the card.

- If the state of the Service Module card is out-of-service-maintenance disabled (OOS-MT-DSBLD), go to [Step 5](#) to change the Ethernet link parameters.
3. Place the Service Module card out of service using the `inh-card` command.
For example, enter this command: `inh-card:loc=1301`. This message should appear.

```
rlghncxa03w 06-08-01 21:18:37 GMT EAGLE5 35.1.0
Card has been inhibited.
```

4. Display the status of the Service Module card to verify that it is out-of-service maintenance-disabled (OOS-MT-DSBLD).
Enter the command `rept-stat-card:loc=1301`.
5. Configure the Ethernet link parameters associated with the Service Module card in the database using the `chg-ip-lnk` command.
For this example, enter the following commands:
`chg-ip-lnk:loc=1301:port=a:ipaddr=192.168.120.1:submask=255.255.255.0:auto=yes:mcast=no`
`chg-ip-lnk:loc=1301:port=b:ipaddr=192.168.121.1:submask=255.255.255.0:auto=yes:mcast=no`
6. Verify the new Ethernet link parameters associated with the Service Module card that was changed in [Step 5](#) by entering the `rtrv-ip-lnk` command with the card location specified in [Step 5](#).
For example, enter the command `rtrv-ip-lnk:loc=1301`.
Note: If [Step 3](#) was not performed, go to [Step 11](#).
7. Configure the Ethernet card parameters associated with the Service Module card in the database using the `chg-ip-card` command.
For example, enter the following command:
`chg-ip-card:bpipaddr=128.1.120.1:bpsubmask=255.255.192.0`
8. Verify the parameters associated with the Service Module card that was changed in [Step 7](#) by entering the `rtrv-ip-card` command with the card location specified in [Step 7](#).
9. Put the Service Module card that was inhibited in [Step 3](#) back into service by using the `alw-card` command.
For example, enter the command `alw-card:loc=1301`.
10. Verify the in-service normal (IS-NR) status of the Service Module card using the `rept-stat-card` command.
For example, enter the command `rept-stat-card:loc=1301`.
11. Repeat this procedure for all other Service Module cards in the EAGLE 5 ISS.
12. Back up the new changes using the `chg-db:action=backup:dest=fixed` command.
These messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

You have now completed this procedure.

Removing DSM Cards

This procedure is used to remove DSM cards from the database, using the `dlt-card` command. LNP with ELAP 9.0 or higher does not support DSM cards. Any DSM cards must be removed from the system and replaced with E5-SM4G or E5-SM8G-B cards.

Note: When any Service Module card is removed, the hourly measurements data that has not been collected will be lost. It is important to remove these cards right after hourly collection to minimize measurements data loss.



CAUTION

Caution: If the DSM Service Module card is the last service module card in service, removing this card from the database will cause a Global Title Translation and Local Number Portability traffic to be lost.

The examples in this procedure are used to remove the DSM card in card location 1204. Refer to the *Commands Manual* for descriptions of the commands used in this procedure, including parameter names, valid parameter values, and output examples.

1. Display the Service Module cards (card type DSM) in the system and the status of each card by entering the `rept-stat-card:appl=vsccp` command.
The cards that are running the VSCCP GPL are DSM cards (E5-SM4G cards and E5 SM4G-B cards run the SCCPHC GPL).

2. Remove a DSM card from service using the `rmv-card` command and specifying the card location that was recorded in [Step 1](#).

If the card to be removed from service (inhibited) is the only Service Module card in service, the `force=yes` parameter must also be specified. The cards that are in service are shown by the entry **IS-NR** in the **PST** field in the output in [Step 1](#). For this example, enter the following command:

```
rmv-card:loc=1204
```

```
rlghncxa03w 07-08-01 09:12:36 GMT EAGLE5 37.0.0  
Card has been inhibited.
```

3. Remove the card from the database using the `dlt-card` command with the `loc` parameter to specify the card location.

For this example, enter this command.

```
dlt-card:loc=1204
```

4. Verify the changes using the `rtrv-card` command and specifying the location of the card that was removed in [Step 3](#). For this example, enter the following command:

```
rtrv-card:loc=1204
```

```
E2144 Cmd Rej: Location invalid for hardware configuration
```

5. Remove the card specified in [Step 3](#) from the shelf.
6. Repeat this procedure for all other DSM cards in the EAGLE 5 ISS that need to be removed.
7. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

These messages appear. The active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.  
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.  
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.  
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

Chapter 8

LNP Measurements

Topics:

- [LNP Measurements.....178](#)

This chapter describes the measurements that can be collected and generated for the LNP feature.

LNP Measurements

The EAGLE 5 ISS Measurements system supports the collection and retrieval of measurements for the LNP feature. The LNP measurements can be collected and reported with the following collection methods:

- OAM-based (UI) measurements collection - LNP measurements are available using the File Transfer Area (FTA) and not directly to EAGLE 5 ISS UI terminals.

Note: .OAM-based LNP measurement collection is disabled when the E5-OAM Integrated Measurements feature is on.

- The Measurements Platform feature enabled and the Measurements Platform collection option on

Note: When the Measurements Platform is installed, the Measurements subsystem collects measurements data for all provisioned LRNs and NPANXXs, up to 200,000 LRNs and 350,000 NPANXXs. Full LNP reports are available using FTP or by enabling the schedule option. LNP measurement reports are still available using FTA, but are limited to 100,000 LRNs and 150,000 NPANXXs.

- The E5-OAM Integrated Measurements feature enabled and on and the E5-OAM Integrated Measurements collection option on.

Refer to the *Measurements* manual for detailed descriptions of measurements and measurements reports.

Refer to the *Commands Manual* for descriptions of the commands used to enable and turn on features, turn on measurements collection options, and schedule and generate measurements reports.

Refer to the procedures in the *Database Administration Manual - System Management* to configure the Measurements Platform feature or E5-OAM Integrated Measurements feature for use with the LNP feature.

Per System, Per SSP, Per LRN, and Per NPA LNP measurements are available in the Daily (MTCD) and Hourly (MTCH) reports for Entity Type LNP.

[Table 30: Pegs for Daily Maintenance \(MTCD\) and Hourly Maintenance \(MTCH\) Per System LNP Measurements](#) describes the Per System measurement peg counts of LNP MSUs (Message Signalling Units) that are supported for the LNP feature.

Table 30: Pegs for Daily Maintenance (MTCD) and Hourly Maintenance (MTCH) Per System LNP Measurements

Event Name	Description	Type	Unit
LNPQRCV	<i>Trigger Based</i> Total number of queries received by LNPQS	System	Peg count
	<i>Triggerless</i> Number of encapsulated IAM messages received by LNPQS	System	Peg count
LNPQDSC	<i>Trigger Based</i>	System	Peg count

Event Name	Description	Type	Unit
	Number of invalid queries that are discarded because no reply can be generated		
	<i>Triggerless</i> All invalid IAM message are routed without LNP; LNPQTCPE is pegged.	System	N/A
LNPQTCPE	<i>Trigger Based</i> Number of error replies with TCAP error codes	System	Peg count
	<i>Triggerless</i> Number of invalid encapsulated IAMm messages received by LNPQS. These messages are routed to their destinations with no LNP lookup.	System	Peg count
LNPSREP	<i>Trigger Based</i> Number of successful replies	System	Peg count
	<i>Triggerless</i> Number of successful IAM messages	System	Peg count
LNPQUNPA	<i>Trigger Based</i> Number of correct queries received for a non-ported DN when the NPAXXX is not provisioned	System	Peg count
	<i>Triggerless</i> Number of correct encapsulated IAM messages received for a non-ported DN when the NPAXXX is not provisioned	System	Peg count
STATUS	Indication of Data Validity: <ul style="list-style-type: none"> • K indicates good data • I indicated incomplete interval • N indicates data not current 	System	Status

Table 31: Pegs for Daily Maintenance (MTCD) and Hourly Maintenance (MTCH) Per SSP LNP Measurements describes the Per SSP measurement peg counts of LNP MSUs that are supported for the LNP feature.

Table 31: Pegs for Daily Maintenance (MTCD) and Hourly Maintenance (MTCH) Per SSP LNP Measurements

Event Name	Description	Type	Unit
SSPQRCV	<i>Trigger Based</i> Number of correct queries received per originating SSP	Point Code	Peg count

Event Name	Description	Type	Unit
	<i>Triggerless</i> Number of correct encapsulated IAM messages received by LNPQS per OPC	System	Peg count
CLASSGTRQ	Number of valid CLASS Global Title Translation received per originating SSP	Point Code	Peg count
LIDBGTRQ	Number of valid LIDB Global Title Translation received per originating SSP	Point Code	Peg count
SSPQRCVP	Number of correct queries received for ported TNs per originating SSP	Point Code	Peg count
SSPQRCVNP	Number of correct queries received for non-porting TNs per originating SSP	Point Code	Peg count
CLASSGTRQP	Number of CLASS Global Title Translation received for ported TNs per originating SSP	Point Code	Peg Count
CLASSGTRQNP	Number of CLASS Global Title Translation received for non-porting TNs per originating SSP	Point Code	Peg count
LIDBGTRQP	Number of LIDB Global Title Translation received for ported TNs per originating SSP	Point Code	Peg count
LIDBGTRQNP	Number of LIDB Global Title Translation received for non-porting TNs per originating SSP	Point Code	Peg count
CNAMGTRQP	Number of CNAM Global Title Translation received for ported TNs per originating SSP	Point Code	Peg count
CNAMGTRQNP	Number of CNAM Global Title Translation received for non-porting TNs per originating SSP	Point Code	Peg count
ISVMGTRQP	Number of ISVM Global Title Translation received for ported TNs per originating SSP	Point Code	Peg count
ISVMGTRQNP	Number of ISVM Global Title Translation received for non-porting TNs per originating SSP	Point Code	Peg count
WSMSCGTRQP	Number of WSMSC Global Title Translation received for ported TNs per originating SSP	Point Code	Peg count
WSMSCGTRQNP	Number of WSMSC Global Title Translation received for non-porting TNs per originating SSP	Point Code	Peg count
STATUS	Indication of Data Validity: <ul style="list-style-type: none"> • K indicates good data • I indicated incomplete interval • N indicates data not current 	Point Code	Status
The following equations apply: $SSQRCV = SSPQRCVP + SSPQRCVNP$			

Event Name	Description	Type	Unit
CLASSGTRQ = CLASSGTRQP + CLASSGTRQNP			
LIBDGTRQ = LIBDGTRQP + LIBDGTRQNP			

The measurement events described in [Table 32: Pegs for Daily Maintenance \(MTCD\) and Hourly Maintenance \(MTCH\) LNP LRN Measurements](#) are included on the STP Daily Maintenance (MTCD) and the STP Hourly (MTCH) measurement reports.

Table 32: Pegs for Daily Maintenance (MTCD) and Hourly Maintenance (MTCH) LNP LRN Measurements

LRNQRCV	<i>Trigger Based</i> Number of correct queries received per LRN
	<i>Triggerless</i> Number of correct encapsulated IAM messages received per LRN
STATUS	Indication of Data Validity: <ul style="list-style-type: none"> • K indicates good data • I indicated incomplete interval • N indicates data not current

The measurement events described in [Table 33: Pegs for Daily Maintenance \(MTCD\) and Hourly Maintenance \(MTCH\) LNP NPA Measurements](#) are included on the STP Daily Maintenance (MTCD) and the STP Hourly (MTCH) measurement reports.

Table 33: Pegs for Daily Maintenance (MTCD) and Hourly Maintenance (MTCH) LNP NPA Measurements

NPAQRCV	Number of correct queries received per NPAXXX for non-ported DN
STATUS	Indication of Data Validity: <ul style="list-style-type: none"> • K indicates good data • I indicated incomplete interval • N indicates data not current

Chapter 9

EMS, RTDB, and LSMS-Related Functions

Topics:

- *EMS Routing.....183*
- *EMS Configuration Component.....183*
- *Managing Bulk Load from the LSMS.....192*
- *Copying One RTDB from Another RTDB.....206*
- *Verifying RTDB Status.....207*
- *Restore RTDB on ELAP.....209*
- *Copy RTDB from Remote.....211*
- *Distributing the LNP Database after LSMS-Based Operation or RTDB Copy.....212*
- *Manually Verifying and Restarting the Eagle Agents on the LSMS.....215*

This chapter describes and provides procedures for the following functions:

- ELAP EMS Routing and Configuration
- Copying, Bulk Loading, Restoring, Verifying, and Distributing the Real Time Database (RTDB)
- Manually Verifying and Restarting the EAGLE Agents on the LSMS

EMS Routing

EMS routing information enables the LSMS to send subscription information to the proper network elements. The EMS routing function allows you to modify or view the routing info that you defined using the TN Filters and GTT Groups (see Chapter 4 of *Database Administrator's Guide* for LSMS).

EMS Configuration Component

Use the following procedures to manage TekPath or ELAP EMS configuration components:

- [Creating an EMS Configuration Component](#)
- [Modifying an EMS Configuration Component](#)
- [Viewing an EMS Configuration Component](#)
- [Deleting an EMS Configuration Component](#)

Creating an EMS Configuration Component

For each network element to be supported by the LSMS, create an EMS configuration component using the following procedure.

Note: For each EMS configuration created, you must perform a bulk download to the associated EMS/network element. Refer to the *LNP Database Synchronization User's Guide* for bulk loading procedures.

1. Log into the LSMS as a user in the `lsmsadm` or `lsmsall` group.
2. From the LNP System menu, shown in [Figure 60: LNP System Menu – Create EMS](#), select **Configure > LNP System > EMS > Create**.

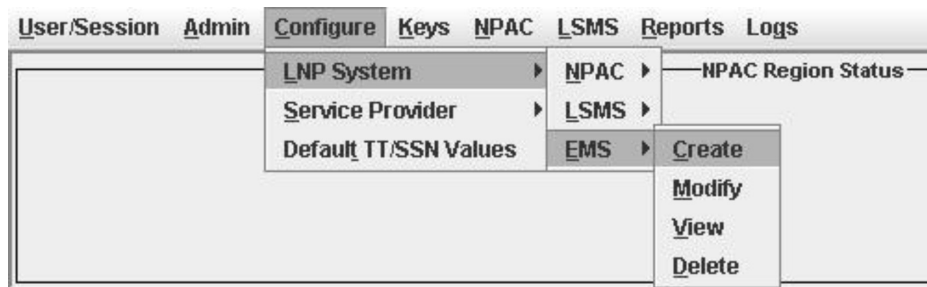


Figure 60: LNP System Menu – Create EMS

The EMS Configuration Component window, [Figure 61: Create LNP System EMS Address Info Tab](#) displays. The window usually opens with the **Address Info** tab displayed; if the **Address Info** tab is not displayed, click its tab to display it.

The screenshot shows a dialog box titled "Create LNP System EMS <TKLC>". It has three tabs: "Address Info", "Component Info", and "Contact Info". The "Address Info" tab is selected. Inside the tab, there are three radio button options: "TekPath Based System", "ELAP Based System" (which is selected), and "ELAP (Version 7 or older)". Below each radio button is a section for IP addresses. For "TekPath Based System", there is a "Virtual IP Address" section with a label "MPS" and four input boxes. For "ELAP Based System", there is a "Virtual IP Address" section with a label "MPS" and four input boxes. For "ELAP (Version 7 or older)", there is an "ELAP IP Addresses" section with labels "MPS A" and "MPS B", each followed by four input boxes. At the bottom of the dialog, there is a button with a question mark icon and the text "Create EMS Component?", and two buttons labeled "OK" and "Cancel".

Figure 61: Create LNP System EMS Address Info Tab

3. Ensure that the radio button for an ELAPMPS or a TekPath MPS is selected. For an ELAPMPS (ELAP version 7 or older), enter the IP addresses for MPS A and MPS B (enter a value from 0 to 255 in each of the first three octets and a value from 0 to 254 in the forth octet). For a TekPath MPS, enter the IP address for MPS A only.
4. Click the **Component Info** tab, shown in [Figure 63: Create LNP System EMS Contact Info](#).

The screenshot shows a dialog box titled "Create LNP System EMS <TKLC>". It has three tabs: "Address Info", "Component Info" (which is selected), and "Contact Info". The "Component Info" tab contains the following fields:

- System Type:** A dropdown menu with "EMS" selected.
- Owner ID:** A text input field.
- Platform Type:** A text input field.
- Platform Supplier:** A text input field.
- Platform SW Release:** A text input field.
- Platform Model:** A text input field.
- CLLI:** A text input field.
- Mate CLLI:** A text input field.
- PC:** Three separate numeric input boxes.
- Mate PC:** Three separate numeric input boxes.
- LNP Capability PC:** Three separate numeric input boxes.

At the bottom of the dialog, there is a question mark icon, the text "Create EMS Component?", and "OK" and "Cancel" buttons.

Figure 62: Create LNP System EMS Component Info

5. Enter the **Component Info** data as follows (all fields in this tab must contain data):

- *Owner ID* – ID of the network element owner (maximum 20 alphanumeric characters)
- *Platform Type* – hardware platform of the network element (maximum 20 alphanumeric characters)
- *Platform Supplier* – name of the supplier of the network element hardware platform (maximum 20 alphanumeric characters)
- *Platform SW Release* – release level of the software running on the network element platform (maximum 20 alphanumeric characters)
- *Platform Model* – model number of the network element platform (maximum 20 alphanumeric characters)
- *CLLI* – CLLI code of the network element (maximum 11 numeric and uppercase alphabetic characters)
- *Mate CLLI* – CLLI of the mate EMS component (maximum 11 numeric and uppercase alphabetic characters)
- *PC* – point code of the EMS component (must contain three 3-digit octets; first octet must have a value from 1 to 255; last two octets must have a value from 0 to 255; second octet must not be 001 if the first octet has a value from 1 to 5)
- *Mate PC* – point code of the mate EMS component (must contain three 3-digit octets; first octet must have a value from 1 to 255; last two octets must have a value from 0 to 255; second octet must not be 001 if the first octet has a value from 1 to 5)
- *LNP Capability PC* – LNP capability point code of the network element (must contain three 3-digit octets; first octet must have a value from 1 to 255; last two octets must have a value from 0 to 255; second octet must not be 001 if the first octet has a value from 1 to 5)

6. Click the **Contact Info** tab, shown in [Figure 62: Create LNP System EMS Component Info](#).

The screenshot shows a dialog box titled "Create LNP System EMS <TKLC>". It has three tabs: "Address Info", "Component Info", and "Contact Info", with "Contact Info" being the active tab. The form contains the following fields:

- Name**: A text input field.
- Email**: A text input field.
- Street**: A text input field.
- City**: A text input field.
- State**: A dropdown menu.
- ZIP Code**: A text input field.
- Province**: A dropdown menu.
- Country**: A text input field.
- Phone Number**: A text input field.
- Fax Number**: A text input field.
- Pager Number**: A text input field.
- Pager PIN**: A text input field.

At the bottom of the dialog, there is a question mark icon next to the text "Create EMS Component?". Below this are two buttons: "OK" and "Cancel".

Figure 63: Create LNP System EMS Contact Info

7. All fields in this tab are optional. If you wish to enter the **Contact Info** data, do so as follows:
- *Name* – name of the person to contact for network element information (maximum 40 alphanumeric characters)
 - *Email* – email address of the network element contact person (maximum 60 alphanumeric characters)
 - *Street* – street address of the network element contact person (maximum 40 alphanumeric characters)
 - *City* – city address of the network element contact person (maximum 20 alphanumeric characters)
 - *State* – state address of the network element contact person (two-letter uppercase abbreviation). If you use the *Province* field, enter -- (the default).
 - *ZIP Code* – the postal zip code of the network element contact person (five numeric characters)
 - *Province* – the province of the network element contact person (two-letter uppercase abbreviation). If you use the *State* field, enter -- (the default).
 - *Country* – country of the network element contact person (maximum 20 alphanumeric characters).
 - *Phone Number* – phone number of the network element contact person (ten numeric characters required).
 - *FAX Number* – FAX number of the network element contact person (ten numeric characters required).
 - *Pager Number* – pager number of the network element contact person (ten numeric characters required)

- *Pager PIN*– pager PIN number of the network element contact person (ten numeric characters maximum)
8. When finished, click **OK** to apply the changes.
- If the **Update Successful** dialog, [Figure 64: Update Successful Dialog](#) appears, click **OK**. The GUI returns to the main console window.

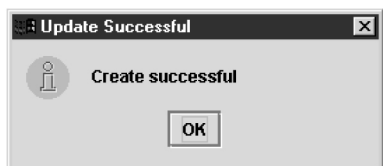


Figure 64: Update Successful Dialog

- When a mandatory field is empty or a field is not properly configured, the **Field Required** [Figure 65: Field Required Dialog](#) dialog displays.



Figure 65: Field Required Dialog

Click **OK** and correct the appropriate field.

Repeat this step until you receive an **Update Successful** notification.

Modifying an EMS Configuration Component

To modify an existing EMS configuration component, use the following procedure.

Note: For each EMS configuration created, you must perform a bulk download to the associated EMS/network element. Refer to the *LNP Database Synchronization User's Guide* for bulk loading procedures.

1. Log into the LSMS as a user in the `lsmsadm` or `lsmsall` group.
2. Click the **EMS status** icon for the EMS you wish to modify so that the icon is highlighted.
3. From the **Main Menu**, select **Configure > LNP System > EMS > Modify**, as shown in [Figure 66: LNP System Menu – Modify EMS](#).

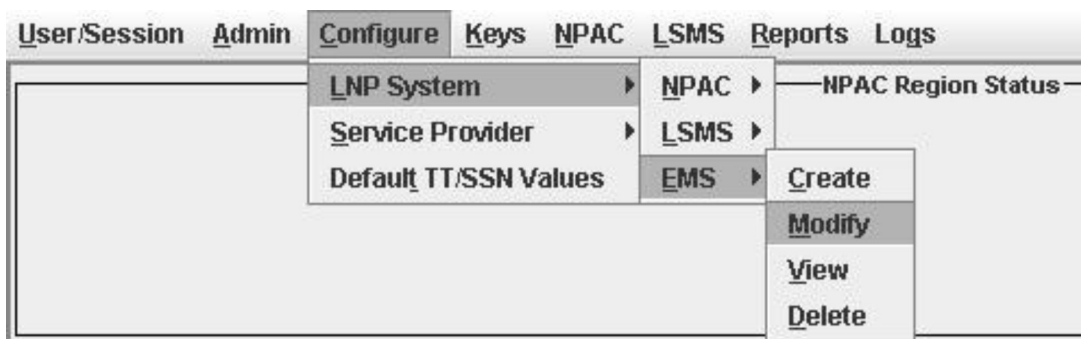


Figure 66: LNP System Menu – Modify EMS

The **Modify LNP System EMS** window, [Figure 67: Modify LNP System EMS Window](#), appears.

 A screenshot of a 'Modify LNP System EMS' window. The title bar reads 'Modify LNP System EMS <TKLC, REGION1>'. There are three tabs: 'Address Info', 'Component Info', and 'Contact Info'. The 'Address Info' tab is active. It contains three radio button options: 'TekPath Based System', 'ELAP Based System' (which is selected), and 'ELAP (Version 7 or older)'. Below each option is a 'Virtual IP Address' field. For 'ELAP Based System', the field shows 'MPS 192 168 17 5'. For 'ELAP (Version 7 or older)', the field shows 'MPS A' and 'MPS B' with empty input boxes. At the bottom, there is a question mark icon and the text 'Modify EMS Component?'. Below this are 'OK' and 'Cancel' buttons.

Figure 67: Modify LNP System EMS Window

The window usually opens with the **Address Info** tab displayed; if the **Address Info** tab is not displayed, click its tab to display it.

4. Modify the EMS data as required.
See [Creating an EMS Configuration Component](#) for detailed field information.
5. Click OK.
The **EMS Routing** dialog appears, [Figure 68: EMS Routing Dialog](#).

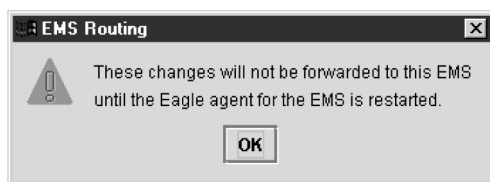


Figure 68: EMS Routing Dialog

Click **OK**.

The **Update Successful** dialog displays, [Figure 69: Update Successful Dialog](#).

Figure 69: Update Successful Dialog



You have completed this procedure.

If a mandatory field is empty or a field is not properly configured, the **More Fields Needed** message is displayed, [Figure 70: More Fields Needed Dialog](#).



Figure 70: More Fields Needed Dialog

Click **OK** and correct the appropriate field.

Repeat this step until you receive an **Update Successful** notification.

Note: Changes do not take effect until the eagleagent is restarted (refer to "Manually Verifying and Restarting the Eagle Agents" in the *Alarms and Maintenance Guide*).

Viewing an EMS Configuration Component

To view EMS configuration component information, use the following procedure.

1. Log into the LSMS as a user in the `lsmsview`, `lsmsuser`, `lsmsuext`, or `lsmsadm` group.
2. Click the **EMS status** icon for the EMS you wish to view (highlight the icon).
3. From the **Main Menu**, select **Configure > LNP System > EMS > View**.

The **View LNP System EMS** dialog displays, [Figure 71: View LNP System EMS Dialog](#).

Figure 71: View LNP System EMS Dialog

4. Click on any of the tabs to view additional information.
For more information about the meaning of the fields on any of the tabs, see [Creating an EMS Configuration Component](#).
- Note:** You cannot modify information in any of the tabs.
5. When finished viewing, click **OK**.

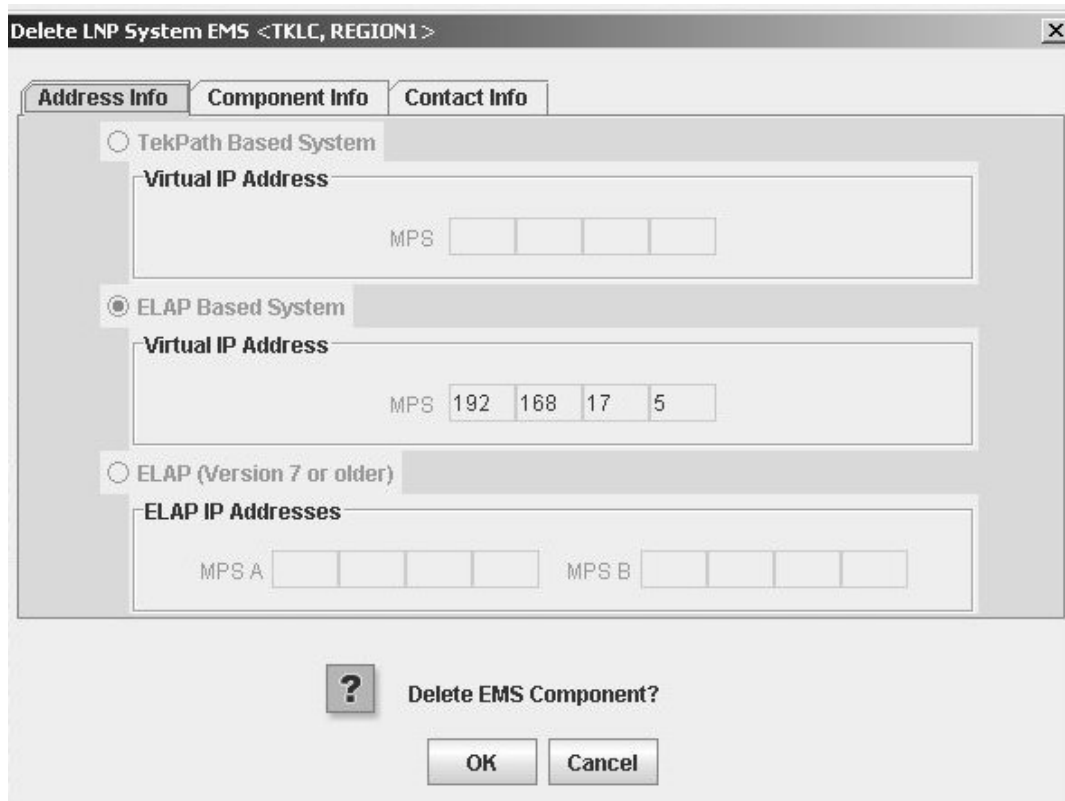
Deleting an EMS Configuration Component

To delete an EMS configuration component, use the following procedure.

Note: The deletion of the EMS configuration component does not take effect until the LSMS is idled and restarted (refer to “Idling an Active Server” and “Starting or Restarting an Idle Server” in the *Alarms and Maintenance Guide*).

1. Log into the LSMS as a user in the `lsmsadm` or `lsmsall` group.
2. Click the **EMS Status** icon for the EMS you wish to delete (highlight the icon).
3. From the **Main Menu**, select **Configure > LNP System > EMS > Delete**.

The **Delete LNP EMS** dialog displays, [Figure 72: Delete LNP System EMS Dialog](#).



The dialog box is titled "Delete LNP System EMS <TKLC, REGION1>". It has three tabs: "Address Info", "Component Info", and "Contact Info". The "Address Info" tab is selected. It contains three radio button options: "TekPath Based System", "ELAP Based System" (which is selected), and "ELAP (Version 7 or older)". Below each option is a field for "Virtual IP Address" or "ELAP IP Addresses". The "ELAP Based System" option shows a "MPS" field with the value "192.168.17.5". The "ELAP (Version 7 or older)" option shows two "MPS" fields, "MPS A" and "MPS B", both empty. At the bottom, there is a question mark icon and the text "Delete EMS Component?". Below this are "OK" and "Cancel" buttons.

Figure 72: Delete LNP System EMS Dialog

4. View the information in this window to verify that this is the EMS you wish to delete. Click on any of the tabs to view additional information. For more information about the meaning of the fields on any of the tabs, see [Creating an EMS Configuration Component](#). You cannot modify information in any of the tabs.
5. Click **OK** or **Cancel**.
 - If you click **Cancel**, you are returned to the LSMS console window.
 - If you click **OK**, the **Update Successful** dialog displays, [Figure 73: Update Successful Dialog](#).



Figure 73: Update Successful Dialog

6. Click **OK**.

Managing Bulk Load from the LSMS

This section describes how to perform a bulk load, view bulk load log files, and understand bulk load error messages.

Bulk Load Procedure

Use the following procedure to manage a bulk load from the LSMS user interface.

Note: Before starting this procedure, contact [My Oracle Support \(MOS\)](#) to be available for assistance if any problems are encountered while performing this procedure.

1. Perform the following substeps to ensure that no NPA Splits will activate during the bulk download procedure:

- a) As `lsmsadm`, enter the following `lsmsdb` commands to output the counts for both Subscription Version and Number Pool Block objects:

```
% cd $LSMS_DIR/./tools
% lsmsdb -c counts | grep SubscriptionVersion
1,012,345 ... CanadaDB.SubscriptionVersion
5,434,123 ... MidAtlanticDB.SubscriptionVersion
7,111,222 ... MidwestDB.SubscriptionVersion
6,333,999 ... NortheastDB.SubscriptionVersion
8,044,000 ... SoutheaststDB.SubscriptionVersion
4,999,800 ... SouthwestDB.SubscriptionVersion
6,500,000 ... WestCoastDB.SubscriptionVersion
5,250,500 ... WesternDB.SubscriptionVersion
% lsmsdb -c counts | grep NumberPoolBlock
1,205 ..... CanadaDB.NumberPoolBlock
10,400 ..... MidAtlanticDB.NumberPoolBlock
8,005 ..... MidwestDB.NumberPoolBlock
4,000 ..... NortheastDB.NumberPoolBlock
7,500 ..... SoutheaststDB.NumberPoolBlock
1,225 ..... SouthwestDB.NumberPoolBlock
7,700 ..... WestCoastDB.NumberPoolBlock
5,500 ..... WesternDB.NumberPoolBlock
```

- b) Total the counts listed in the first column of the output from both commands in substep a. Divide this total by 2 million, to determine the estimated number of hours for the bulk load.
- c) Generate an NPA Split Report.
Select **Pending** for Status and **All NPAC Regions** for NPAC Region. For information about creating and viewing NPA Split Data Reports, refer to *LSMS Database Administrator's Guide*.
- d) Determine if NPA Splits are scheduled to be activated during the time the Bulk Load is to be performed:
 - If no Pending NPA Splits were listed in the report in substep c, or if none of the Pending NPA Splits has a PDP Start Date that occurs within the time period required to complete the Bulk Load, go to step 2.
 - If any Pending NPA Split has a PDP Start Date that occurs within the time period required to complete the Bulk Load, continue with next substep.

- e) Determine the date on which you want the NPA Splits to be activated.
This should be the next day after the expected completion of the Bulk Load Procedure (based on the start date/time anticipated and the estimated length of the Bulk Load procedure, from substep b). For example, if the Bulk Load is estimated to require 24 hours to complete and the Bulk Load planned to be performed starting at 12 noon on April 1st, the NPA Split should be postponed until April 3rd.
 - f) Postpone the NPA Split. (Refer to *LSMS Database Administrator's Guide*.)
2. Ensure that the network element is prepared to receive a bulk load by doing the following:
 - a) Connect your web browser to the ELAP user interface. See [Setting Up an ELAP Workstation](#).
 - b) Log in with the user name and password for a user who is authorized to access the menu items shown in this procedure.

The ELAP GUI is displayed, as shown in [Figure 74: ELAP Main Menu](#).

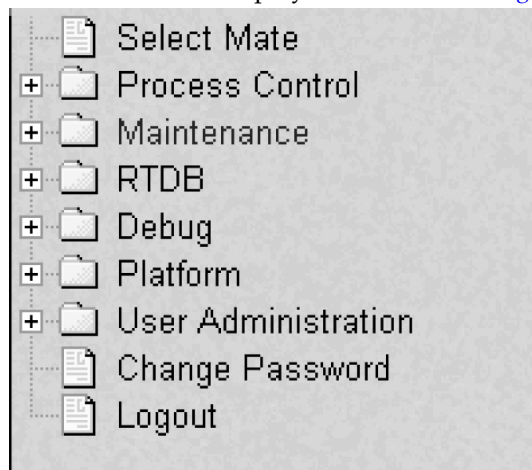


Figure 74: ELAP Main Menu

- c) Select **Maintenance > LSMS HS Bulk Download > Change Enabled**.
The window shown in [Figure 75: Enabling Change HS Bulk Download](#) is displayed.

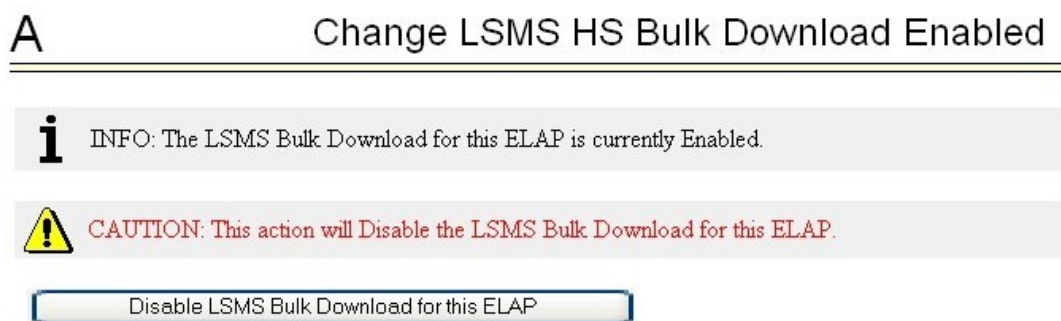


Figure 75: Enabling Change HS Bulk Download

- d) If the information field indicates that the Bulkload for the ELAP is currently enabled, click the Disable Bulkload for this ELAP button and this will allow the audit.
3. At the LSMS, log in as a member of the `lsmsuser`, `lsmsuext`, or `lsmsall` user group.
 4. Start the Bulk Load window using either of the following:

- a) From the **Main Menu** on the **LSMS Console** window, select **LSMS > LNP Database Synchronization > Bulk Load > <CLLI>**, where **<CLLI>** is the Common Language Location Identifier for the network element that requires the bulk load.
- b) Right-click the **LSMS Console** window's EMS status icon that corresponds to the network element requiring the bulk load, and select **LNP Database Synchronization > Bulk Load**.
The **Bulk Load** window displays. An example of this window is shown in [Figure 76: Bulk Load Window](#).

Bulk Load <STPA, lsmsuser>

LNP Data Type	Bulk Loaded	Resynced	Download Total	Errors
LNP Services	0	0	0	0
NPA Splits	0	0	0	0
Number Pool Blocks	0	0	0	0
Subscription Versions	0	0	0	0
Default GTTs	0	0	0	0
Override GTTs	0	0	0	0
Totals	0	0	0	0

Phase	Start Date/Time	End Date/Time	Elapsed Time
Bulk Load			
Re-sync			

Start Bulk Load to Network Element - STPA?

Ready

Figure 76: Bulk Load Window

5. To initiate the bulk load, click the **Start** button.

The **Start** button is replaced by the **Abort** button, and the **View Log** button becomes selectable. Progress is indicated by start time, elapsed time, numbers of successful and failed update commands, and status reported in the status field at the bottom of the window. When the bulk load phase completes (as indicated in the status field and by a value appearing in the End Date/Time field for the Bulk Load phase), the Re-sync phase begins and progress continues to be indicated in the same ways. All other buttons become non-selectable. [Table 34: Fields in Bulk Load Window](#) shows the meaning of each of the fields that appears in this window.

Table 34: Fields in Bulk Load Window

Field	Description	Possible Values
Bulk Loaded	Total number of LNP commands that were successfully transmitted and applied to the NE's LNP database during the initial download phase of the bulk load operation.	0 — 99,999,999
Resynced	Total number of LNP commands that were successfully transmitted and applied to the NE's LNP database during the resynchronization phase of the bulk load operation.	0 — 99,999,999
Download Total	Total number of LNP commands that were successfully transmitted and applied to the NE's LNP database during initial download and the resynchronization phases of the bulk load operation.	0 — 99,999,999
Errors	Total number of commands that were successfully transmitted but rejected by the NE during the initial download and the resynchronization phases of the bulk load operation.	0 — 99,999,999
Bulk Load Start Date/Time	Time at which the initial download phase of the bulk load operation was started by the user.	MM/DD ¹ hh:mm:ss ¹
Bulk Load End Date/Time	Time at which the initial download phase of the bulk load operation completed successfully or terminated abnormally.	MM/DD ¹ hh:mm:ss ¹
Bulk Load Elapsed Date/Time	Amount of time the initial download phase of the bulk load operation took to complete or the amount of time it ran before the user aborted it.	MM/DD ¹ hh:mm:ss ¹ [A F] ²
Re-sync Start Date/Time	Time at which the resynchronization phase of the bulk load operation was started by the user.	MM/DD ¹ hh:mm:ss ¹
Re-sync End Date/Time	Time at which the resynchronization phase of the bulk load operation completed successfully (with or without command rejections at the NE) or terminated abnormally.	MM/DD ¹ hh:mm:ss ¹
Re-sync Elapsed Date/Time	Amount of time the resynchronization phase of the bulk load operation took to complete or the amount of time it ran before the user aborted it.	hh:mm:ss ¹ [A F] ²
Status	Appears as text at the bottom left of the window to indicate the current status of the resynchronization operation.	Varies
1 MM indicates month, range 01—12 DD indicates day, range 01—31		

Field	Description	Possible Values
hh	indicates hour, range 00—23	
mm	indicates minute, range 00—59	
ss	indicates second, range 00—59	
2	A is appended at the end of the time if the operation is aborted.	
F	is appended at the end of the time if the operation fails.	

The time required to download a database from the LSMS to the network element varies depending on the number of records provisioned in the database and the quality of the transmission and connections. To view the bulk load log file, see [Bulk Load Log File](#). To abort during either the bulk load phase or the resynchronization phase of an electronic bulk load is in progress, click the **Abort** button. A confirmation dialog displays, as shown in [Figure 77: Abort Bulk Load Operation Dialog](#).

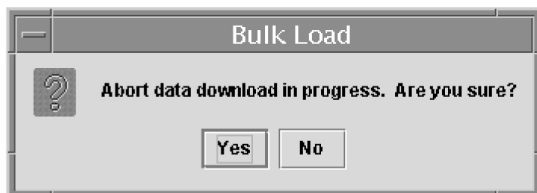


Figure 77: Abort Bulk Load Operation Dialog

- a) Click the **Yes** button to immediately terminate the operation in progress.
Go to [Step 7](#) as if the bulk load had completed.
 - b) Click the **No** button to close the **Abort** confirmation dialog and return back to the main **Bulk Load** window with no other effect.
6. When the bulk load operation completes, the information dialog shown in [Figure 78: Bulk Load Complete Information Dialog](#) appears.



Figure 78: Bulk Load Complete Information Dialog

Click **OK**.

7. When the bulk load operation completes or is aborted, the **Abort** and **Close** buttons are replaced by **Commit** and **Discard** buttons, as shown in [Figure 79: Bulk Load Complete](#).

Bulk Load <STPA, Ismsall>

LNP Data Type	Bulk Loaded	Resynced	Download Total	Errors
LNP Services	6	0	6	0
NPA Splits	1	0	1	0
Number Pool Blocks	1	0	1	0
Subscription Versions	1	0	1	0
Default GTTs	1	0	1	0
Override GTTs	1	0	1	0
Totals	11	0	11	0

Phase	Start Date/Time	End Date/Time	Elapsed Time
Bulk Load	10/23 14:18:46	10/23 14:20:07	00:01:21
Re-sync	10/23 14:20:08	10/23 14:20:08	00:00:00

View Log

?

Commit or Discard data downloaded to the NE?

Commit

Discard

Please wait...

Figure 79: Bulk Load Complete

Commit before you click the **Discard** button, you can view the bulk load log file by clicking the **View Log** button (for more information about the file, including how to view it at other times, see [Bulk Load Log File](#)). To conclude the bulk load operation, you must click one of the following buttons:

Click the **Discard** button to end the bulk load application (closing the **Bulk Load** window) and to send the NE a discard command that results in changes to the ELAP RTDB that cannot be undone. (For whatever reason you are performing this procedure, the ELAP RTDB is now in a state of requiring database maintenance, but the bulk load application is no longer running.)

Note: On the active MPS, verify that the DB Status is Coherent and the RTDB Level is greater than zero before copying the newly downloaded database to the mated ELAP.

8. The NE operator must continue with the following steps to cause the RTDB to be distributed and return the NE to normal operation as follows:
 1. Copy the newly restored RTDB to its mate ELAP RTDB, as described in [Copy RTDB from Remote](#).
 2. Distribute the data to the Service Module cards, as described in [Distributing an RTDB to Service Module Cards](#).

Support ELAP Reload Via Database Image Function

The Support ELAP Reload via Database Image (SERVDI) function performs bulk data downloads (BDD) that significantly reduces the time needed to reload an ELAP database.

The SERVDI function is executed on the LSMS system and creates an ELAP RTDB image file directly from the LSMS LNP databases. See [Figure 80: ELAP Reload Via DB Image Function](#). The SERVDI download file must be transferred to the ELAP system backup directory. Once transferred, the file is activated by using the [Restore RTDB on ELAP](#) process in the ELAP GUI.

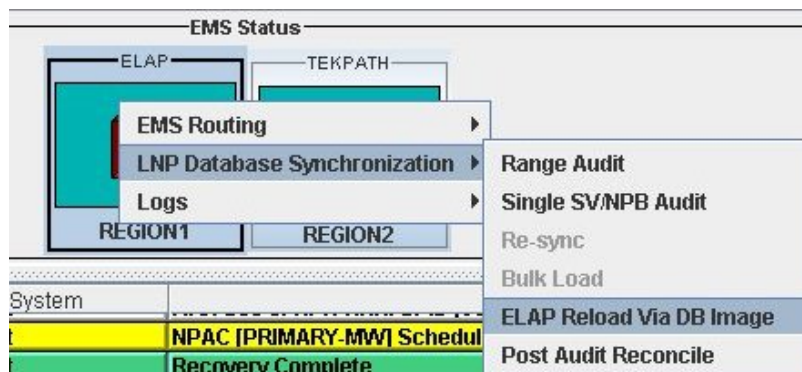


Figure 80: ELAP Reload Via DB Image Function

SERVDI Bulk Download

Use the following procedure to perform an ELAP bulk download from the LSMS.

Note: SERVDI is part of the optional LNP feature. Contact [My Oracle Support \(MOS\)](#) for more information.

Note: The LSMS bulk download SERVDI creates the bulkload file, but cannot send it to the active ELAP unless the Secure Shell Keys (SSKs) have been exchanged. The procedure for exchanging the keys is part of the ELAP configuration procedure, and is illustrated in [Copy RTDB from Remote](#). After the key exchange procedure is complete, the SERVDI bulk download can be sent from the LSMS to the active ELAP.

1. Log in to the LSMS GUI as a member of the permission group that is authorized to perform this operation.
2. From the LSMS Console window, select **LSMS > LNP Database Synchronization > ELAP Reload Via DB Image > <CLLI>** where <CLLI> is the ELAP network element that requires the bulk download.

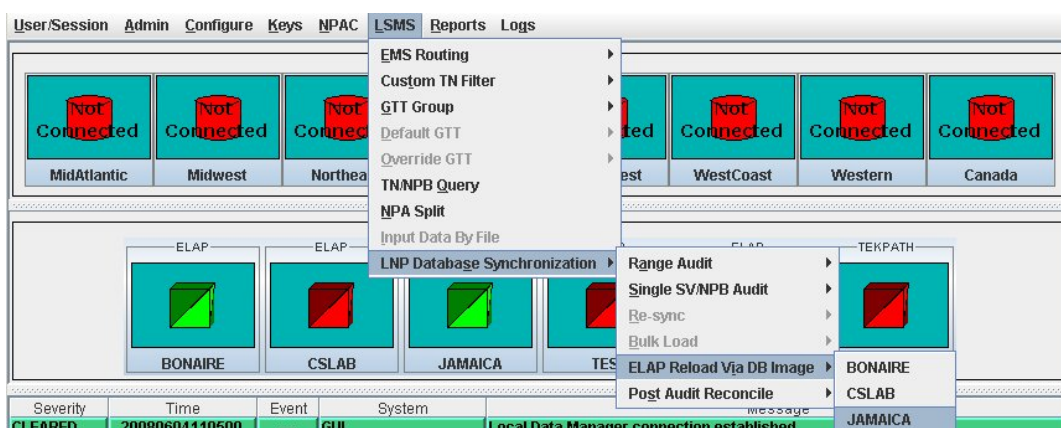


Figure 81: ELAP Reload Via DB Image

3. Click Generate Image.

ELAP Reload Via Database Image <JAMAICA, lsmsadm>

Supported DB	Total Count	Read	Parse Errors	Written	Update Errors
NPA Splits	0	0	0	0	0
Default GTTs	0	0	0	0	0
Override GTTs	0	0	0	0	0
Totals	0	0	0	0	0

Regional DB SV's	Total Count	Read	Parse Errors	Written	Update Errors
MidAtlantic	0	0	0	0	0
Midwest	0	0	0	0	0
Northeast	0	0	0	0	0
Southeast	0	0	0	0	0
Southwest	0	0	0	0	0
WestCoast	0	0	0	0	0
Western	0	0	0	0	0
Canada	0	0	0	0	0
Totals	0	0	0	0	0

Regional DB NPB's	Total Count	Read	Parse Errors	Written	Update Errors
MidAtlantic	0	0	0	0	0
Midwest	0	0	0	0	0
Northeast	0	0	0	0	0
Southeast	0	0	0	0	0
Southwest	0	0	0	0	0
WestCoast	0	0	0	0	0
Western	0	0	0	0	0
Canada	0	0	0	0	0
Totals	0	0	0	0	0

Phase	Start Date/Time	End Date/Time	Elapsed Time
Creation			
Transfer			

[View Log](#)

? Start Database Image Generation for Network Element - JAMAICA?

[Generate Image](#) [Close](#)

Ready

Figure 82: Generate Image

- The LSMS creates a database file of the ELAP database image. When the process completes, a confirmation dialog appears.

ELAP Reload Via Database Image

i Generation of network element's (JAMAICA) LNP database image completed.

The database image can now be transferred to the network element.

[OK](#)

Figure 83: Database Image Completed

Click **OK** to continue.

Note: If necessary, you can stop the bulk download process before the database image is complete. To stop the bulk download process, click **Abort**. A confirmation dialog appears. Click **Yes** to terminate the bulk download in progress. Click **No** to continue with the bulk download.

ELAP Reload Via Database Image <JAMAICA, lsmsadm>


Supported DB	Total Count	Read	Parse Errors	Written	Update Errors
NPA Splits	0	0	0	0	0
Default GTTs	0	0	0	0	0
Override GTTs	0	0	0	0	0
Totals	0	0	0	0	0

Regional DB SV's	Total Count	Read	Parse Errors	Written	Update Errors
MidAtlantic	94990709	200000	0	60000	0
Midwest	14500000	240000	0	100000	0
Northeast	11165590	260000	0	80000	0
Southeast	13020000	160000	0	40000	0
Southwest	59000000	140000	0	20000	0
WestCoast	95000000	280000	0	100000	0
Western	95200000	240000	0	100000	0
Canada	0	0	0	0	0
Totals	382876299	1520000	0	500000	0

Regional DB NPB's	Total Count	Read	Parse Errors	Written	Update Errors
MidAtlantic	0	0	0	0	0
Midwest	0	0	0	0	0
Northeast	0	0	0	0	0
Southeast	0	0	0	0	0
Southwest	0	0	0	0	0
WestCoast	0	0	0	0	0
Western	0	0	0	0	0
Canada	0	0	0	0	0
Totals	0	0	0	0	0

Phase	Start Date/Time	End Date/Time	Elapsed Time
Creation	06/04 12:03:23		00:00:27
Transfer			

[View Log](#)

 Click 'Abort' to Stop Operation.

[Abort](#) [Close](#)

Generating database image, please wait...

Figure 84: Abort Bulk Download

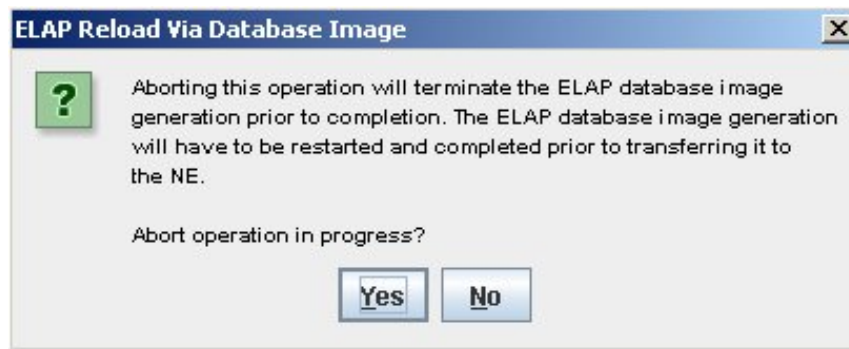


Figure 85: Abort Confirmation

5. Click **Transfer Image** to transfer the bulk download to the ELAP.

ELAP Reload Via Database Image <JAMAICA, lsmsadm>

Supported DB	Total Count	Read	Parse Errors	Written	Update Errors
NPA Splits	6	6	0	3	0
Default GTTs	0	0	0	0	0
Override GTTs	0	0	0	0	0
Totals	6	6	0	3	0

Regional DB SV's	Total Count	Read	Parse Errors	Written	Update Errors
MidAtlantic	0	0	0	0	0
Midwest	0	0	0	0	0
Northeast	0	0	0	0	0
Southeast	0	0	0	0	0
Southwest	0	0	0	0	0
WestCoast	0	0	0	0	0
Western	0	0	0	0	0
Canada	3999998	3999998	0	3999998	0
Totals	3999998	3999998	0	3999998	0

Regional DB NPB's	Total Count	Read	Parse Errors	Written	Update Errors
MidAtlantic	0	0	0	0	0
Midwest	0	0	0	0	0
Northeast	0	0	0	0	0
Southeast	0	0	0	0	0
Southwest	0	0	0	0	0
WestCoast	0	0	0	0	0
Western	0	0	0	0	0
Canada	0	0	0	0	0
Totals	0	0	0	0	0

Phase	Start Date/Time	End Date/Time	Elapsed Time
Creation	06/04 08:23:42	06/04 08:26:39	00:02:57
Transfer			

[View Log](#)

? Transfer Database Image to Network Element - JAMAICA?

[Transfer Image](#) [Close](#)

Operation complete.

Figure 86: Transfer Database Image to ELAP

When the transfer completes, a confirmation dialog appears. Click **OK** to continue.

ELAP Reload Via Database Image

i Database image generation and transfer for network element (JAMAICA) complete.

[OK](#)

Figure 87: Image Transfer Complete

- Click **Close** to return to the main LSMS Console window.

In order to complete this process, you must reload the ELAP database using the file generated in [Step 4](#). For more information about how to reload an ELAP database, refer to the procedure, [Restore RTDB on ELAP](#).

Bulk Load Log File

This section describes the following topics:

- [Viewing the Bulk Load Log File](#)
- [Bulk Load Log File Contents](#)

Viewing the Bulk Load Log File

After a resynchronization has begun, you can view the electronic bulk load log file by clicking the **View Log** button. The browser window displays the log file `LsmsBulkload.log.<MMDD>`. The file is located in the directory `/usr/local/LSMS/logs/<CLLI>`. `<CLLI>` is the Common Language Location Identifier of the network element receiving the bulk load. `<MMDD>` is the timestamp that contains month and day that the file was created.

You can also use one of the following methods to open the window shown in [Figure 88: Open Log Files Window](#) to browse for this log:

- Select **Logs > Other...** from the main menu of the **LSMS Console** window.
- Click on the **LSMS Console** window's **EMS Status** icon that corresponds to the network element receiving the bulk load so that the icon is highlighted. Right-click and select **Logs > LNP Database Synchronization > Bulk Load**.

The Open Log Files window displays.



Figure 88: Open Log Files Window

Scroll down to find the folder that has the `<CLLI>` name for the NE that was bulk loaded. Double-click the folder name, and then double-click the file name `LsmsBulkload.log.<MMDD>` that corresponds to the month and day you desire.

Note: Log files are maintained for seven days and then automatically removed from the LSMS.

Bulk Load Log File Contents

When a bulk load is started, the bulk load log file for that day is appended (if this is the first bulk load of the day, the file is created). For each bulk load performed on that day, the bulk load log file contains information similar to the information displayed on the Bulk Load main window, such as start and end times for the bulk load, and numbers of successes and failures in various LNP categories.

The bulk load log file contains the following sections:

- Header Section
- Bulk Load Section
- Resynchronization Section
- Summary Section
- Download Commit/Discard Section

Refer to Appendix C of *LNP Database Synchronization User's Guide* for more information on these sections.

Figure 89: Example Bulk Load Log File shows an example of a bulk load log file.

Wed Oct 31 14:02:03 GMT 2001

Username: lsmsall
NE CLI: STPB

Wed Oct 31 14:02:02 GMT 2001

Connection established with network element (192.168.61.202:1030)

Bulk download started on Wed Oct 31 14:02:13 GMT 2001

Bulk download completed on Wed Oct 31 14:02:27 GMT 2001

LNP Services	6 Downloaded	0 errors
NPA Splits	1 Downloaded	0 errors
Number Pool Blocks	2 Downloaded	0 errors
Subscription Versions	1004 Downloaded	0 errors
Default GTTs	1 Downloaded	0 errors
Override GTTs	1 Downloaded	0 errors
Total	1015 Downloaded	0 errors

Re-sync started on Wed Oct 31 14:02:29 GMT 2001

New NE LNP Database Time Stamp: Wed Oct 31 14:02:30 GMT 2001

```

Re-sync completed on Wed Oct 31 14:02:30 GMT 2001

      NPA Splits           0 Downloaded          0 errors
    Number Pool Blocks     0 Downloaded          0 errors
  Subscription Versions     0 Downloaded          0 errors
      Default GTTs         0 Downloaded          0 errors
      Override GTTs        0 Downloaded          0 errors
          Total           0 Downloaded          0 errors

Commit completed on Wed Oct 31 14:02:48 GMT 2001.

Username: lsmsall
NE CLI:  STPB

```

```

Bulk download started on Wed Oct 31 15:04:54 GMT 2001

```

```

Bulk download completed on Wed Oct 31 15:05:09 GMT 2001

```

```

      LNP Services         6 Downloaded          0 errors
      NPA Splits           1 Downloaded          0 errors
    Number Pool Blocks     2 Downloaded          0 errors
  Subscription Versions    1004 Downloaded        0 errors
      Default GTTs         1 Downloaded          0 errors
      Override GTTs        1 Downloaded          0 errors
          Total           1015 Downloaded        0 errors

```

```

Re-sync started on Wed Oct 31 15:05:19 GMT 2001

```

```

New NE LNP Database Time Stamp: Wed Oct 31 15:05:20 GMT 2001

```

```

Re-sync completed on Wed Oct 31 15:05:20 GMT 2001

```

```

      NPA Splits           0 Downloaded          0 errors
    Number Pool Blocks     0 Downloaded          0 errors
  Subscription Versions     0 Downloaded          0 errors
      Default GTTs         0 Downloaded          0 errors
      Override GTTs        0 Downloaded          0 errors
          Total           0 Downloaded          0 errors

```

```

Discard completed on Wed Oct 31 15:10:55 GMT 2001.

```

Figure 89: Example Bulk Load Log File

Bulk Load Error Messages

For a listing of error messages that can appear on the GUI, along with explanation of possible cause and suggested recovery, refer to Appendix A in *LNP Database Synchronization User's Guide*.

Copying One RTDB from Another RTDB

This section describes the two methods for copying an EAGLE LNP Application Processor (ELAP) Real Time Database (RTDB) from another ELAP RTDB to reload a corrupted or backlevel RTDB:

- [Restore RTDB on ELAP](#)
- [Copy RTDB from Remote](#)

For more information about when to perform each method, refer to the "Choosing a Database Maintenance Procedure" section in the *LNP Database Synchronization Manual*.

Restore the RTDB from the Mated ELAP

ELAP uses a Distributed Replicated Block Device (DRBD) to replicate the database. The DRBD replicates the database by using a snapshot image of the database. The Support ELAP Reload Via Database Image function, or SERVDI, is executed on the LSMS for the bulk download, and the process is completed with the procedure to restore the RTDB. See [Restore RTDB on ELAP](#) for the detailed procedure.

For more information on the SERVDI function, see [SERVDI Bulk Download](#).

Copy RTDB from Remote ELAP

ELAP uses a snapshot image of the database to replicate the database. The [Copy RTDB from Remote](#) procedure is used to copy the RTDB from the remote ELAP.

After completing the copy procedure, the database must be restored to make the transferred file the active RTDB. See [Restore RTDB on ELAP](#) for the procedure to restore the RTDB.

Verifying RTDB Status

Before or after executing the Copy One RTDB to Another RTDB procedure, verify the status of the RTDBs using either or both of the following methods:

- [Verifying RTDB Status at the EAGLE Terminal](#)
- [Verifying RTDB Status at the ELAP User Interface](#)

Verifying RTDB Status at the EAGLE Terminal

To verify the status of the ELAP RTDBs at the EAGLE terminal, enter the `rept-stat-db:db=mps` command.

The command output displays the database timestamp (DBTS) of both ELAP RTDBs in the RTDB-EAGLE field, as shown in bold in the following example. The DBTS indicates the last time an update was received by this RTDB from the LSMS. If the two DBTS values are not the same, the RTDB with the lower DBTS may need database maintenance.

```
tekelecstp 02-10-29 08:55:54 NZST EAGLE 39.0.0

          ELAP A  ( ACTV )
          C  BIRTHDATE                LEVEL      EXCEPTION
          -  -
RTDB      Y  02-10-29 08:20:04         12345        -
RTDB-EAGLE 02-10-29 08:20:04 12345 -
-

```

	ELAP B (STDBY)				
	C	BIRTHDATE		LEVEL	EXCEPTION
	-	-	-	-	-
RTDB	Y	02-10-29 08:20:04		12345	-
RTDB-EAGLE	02-10-29 08:20:04	12345	-		
;					

Verifying RTDB Status at the ELAP User Interface

To verify the status of ELAP RTDBs at the ELAP Graphic User Interface (view the status of the databases), perform the following procedure.

1. Open a browser window and connect your web browser to the ELAP GUI.
2. Log into the ELAP GUI with the user name and password for a user who is authorized to access the menu items shown in this procedure.

The ELAP GUI is displayed, as shown in [Figure 90: ELAP Main Screen](#).

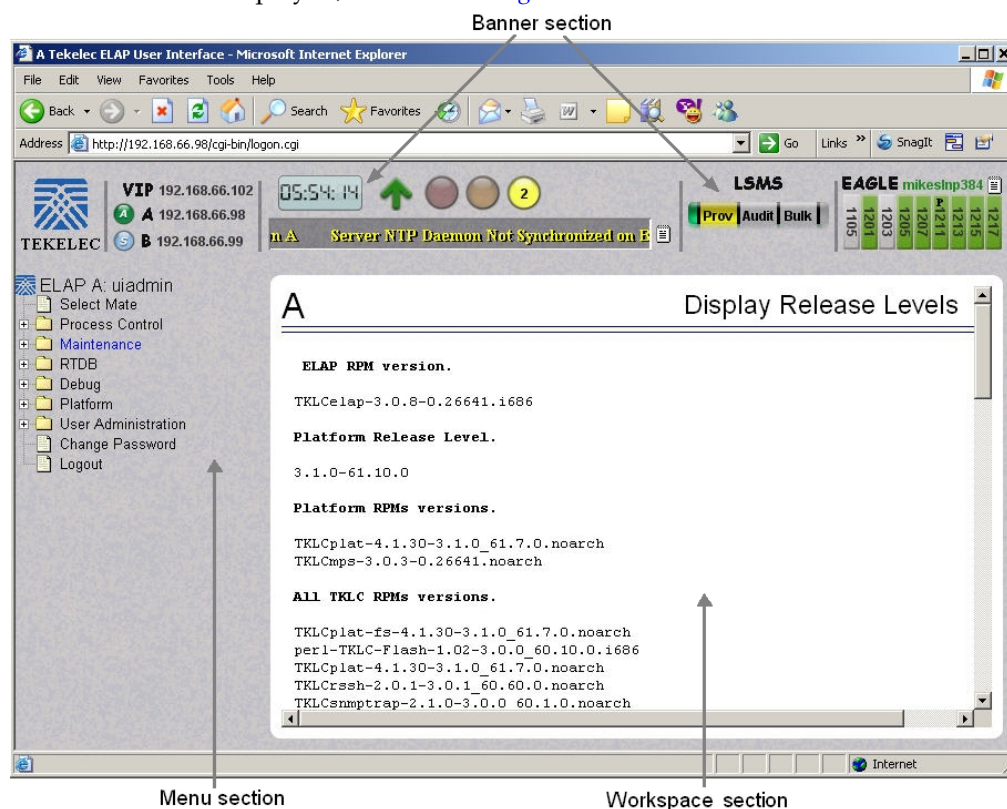


Figure 90: ELAP Main Screen

3. From the Main Menu, select **RTDB > View RTDB Status**.

The ELAP GUI workspace displays the RTDB status, as shown in [Figure 91: ELAP RTDB Status](#).

Local RTDB Status			
DB Status:	Coherent	Audit Enabled:	Yes
RTDB Level:	8708	RTDB Birthday:	09/26/2005 20:44:35 GMT
Counts:	TNs=8708, NPANXXs=778, LRNs=2, SPs=2, MRs=8, MRGroups=2		
Reload:	None		

Mate RTDB Status			
DB Status:	Coherent	Audit Enabled:	Yes
RTDB Level:	8708	RTDB Birthday:	09/26/2005 20:44:44 GMT
Counts:	TNs=8708, NPANXXs=778, LRNs=2, SPs=2, MRs=8, MRGroups=2		
Reload:	None		

Figure 91: ELAP RTDB Status

Note the values displayed for DB Level and DB Birthday for both the local RTDB and the mate RTDB.

4. To verify that both RTDBs are ready for normal service, ensure that:
 - a) The status for both RTDBs displays
 - b) Both RTDBs are coherent
 - c) Both RTDBs have the same birthday
 - d) Both RTDBs have the same level (if provisioning is occurring, the levels might be different by a small number)

If you are not sure how to interpret the status of the RTDBs, contact [My Oracle Support \(MOS\)](#).

You have now completed this procedure.

Restore RTDB on ELAP

Follow these steps to restore the RTDB from a backup file after performing a bulk download.

1. Open a browser window and connect your Web browser to the ELAP GUI.
2. Log into the ELAP GUI with the user name and password for an authorized user.
3. From the ELAP GUI menu, select **Process Control > Stop Software** to ensure that no other updates are occurring. The screen shown in [Figure 92: Stopping Software on the ELAP GUI](#) displays. Click the **Stop ELAP Software** button.

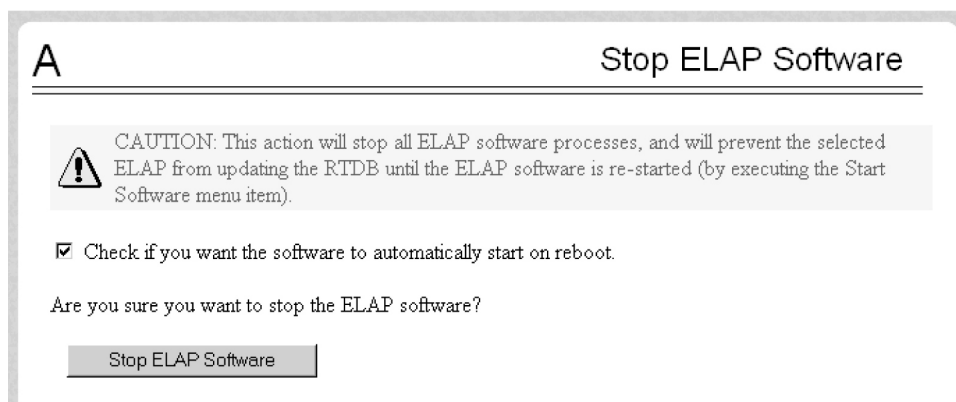


Figure 92: Stopping Software on the ELAP GUI

After the software on the selected ELAP has stopped, the screen shown in [Figure 93: Stop ELAP Software - Success](#) is displayed.

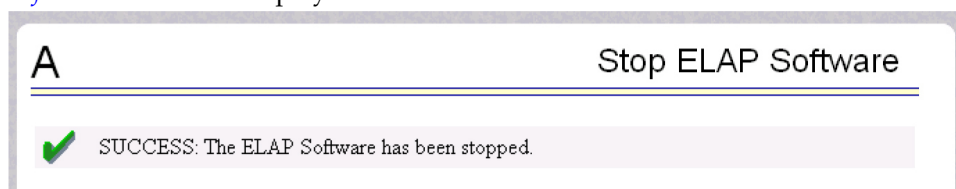


Figure 93: Stop ELAP Software - Success

4. Select **RTDB > Maintenance > Restore RTDB**.

The Restore the RTDB screen displays, [Figure 94: Restore the RTDB](#).

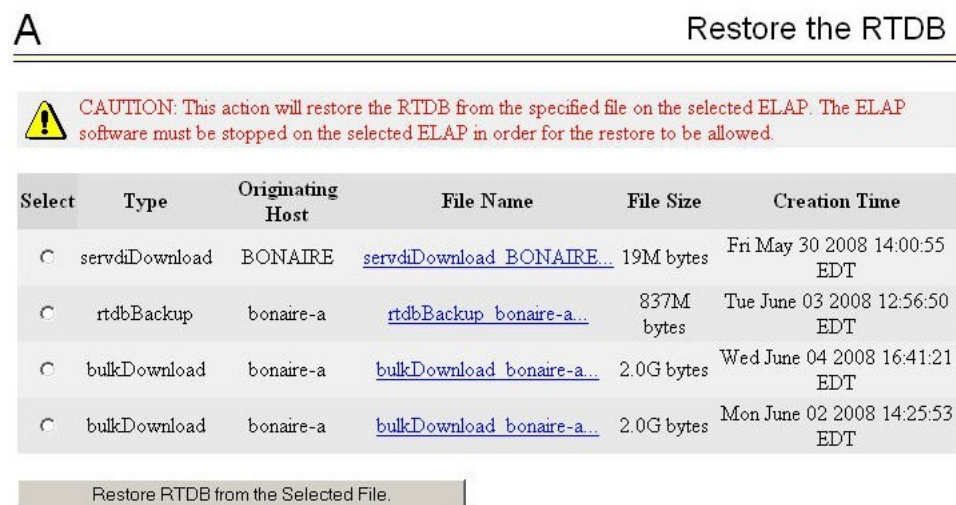


Figure 94: Restore the RTDB

5. Select the appropriate file to restore and click the **Restore RTDB from the Selected File** button.
6. To confirm restoring the file, click the **Confirm RTDB Restore** button on the confirmation dialog, [Figure 95: Confirm RTDB Restore](#).



Figure 95: Confirm RTDB Restore

- After the file is successfully restored, the screen shown in [Figure 96: Successful RTDB Restoration](#) displays.

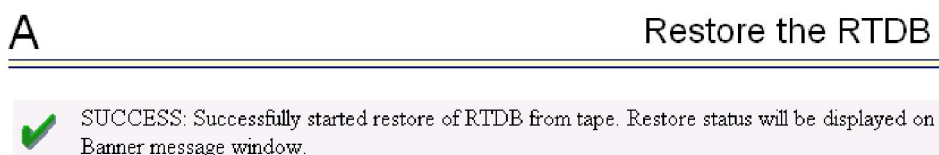


Figure 96: Successful RTDB Restoration

Copy RTDB from Remote

Note: The software does not have to be stopped before performing this procedure.

Restore the RTDB to make the transferred file the active RTDB.

Follow these steps to copy the RTDB from a remote ELAP to the local ELAP.

- Open a browser window and connect your Web browser to the ELAP GUI.
- Log into the ELAP GUI with the user name and password for a user who is authorized to access the menu items shown in this procedure.
- From the ELAP GUI menu, select **RTDB > Maintenance > Copy from Remote**.

The [Figure 97: Copy RTDB from Remote Screen](#) screen is displayed.

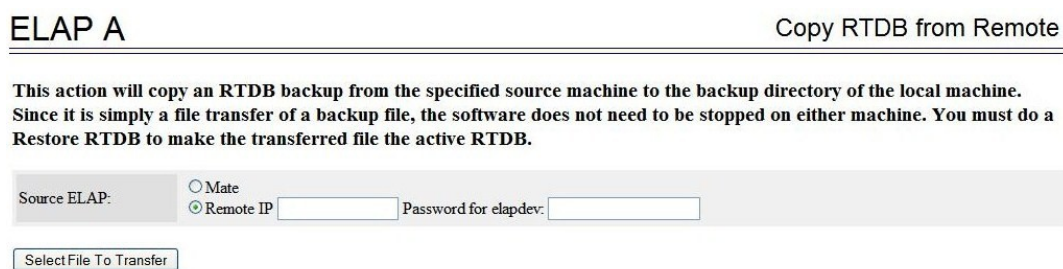


Figure 97: Copy RTDB from Remote Screen

- To copy the remote RTDB, enter the remote box's IP address and a password for the "elapdev" user ID in the fields shown in [Figure 97: Copy RTDB from Remote Screen](#). Then, click the **Select File To Transfer** button.

5. Select the appropriate source from the screen that is displayed, as shown in [Figure 98: Copy RTDB from Remote Selection](#). Then, click the **Copy the selected remote RTDB backup** button.

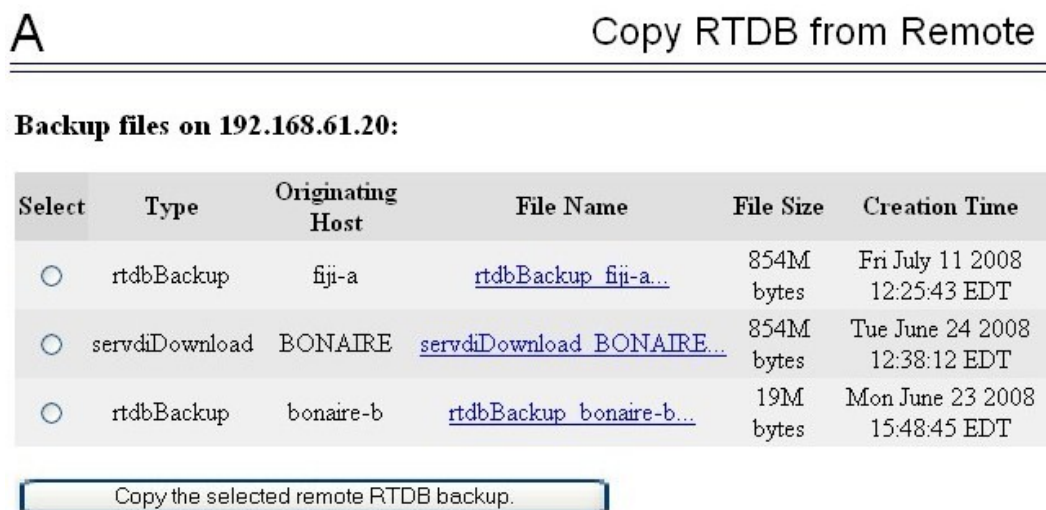


Figure 98: Copy RTDB from Remote Selection

After the copy is complete, a confirmation message is displayed.

To reload the RTDB, follow the procedure as shown in [Restore RTDB on ELAP](#).

Distributing the LNP Database after LSMS-Based Operation or RTDB Copy

The network element has multiple copies of the LNP database. Synchronization operations are performed on one database. After an RTDB copy or a synchronization operation initiated from the LSMS GUI, the remaining NE LNP databases must be synchronized with the newly synchronized NE database in one of the following ways:

- Automatic Data Distribution

After the following LNP database synchronization operations, data is distributed automatically from the network element's newly synchronized LNP database to all other LNP databases at the network element:

- Automatic resynchronization (see "Automatic Resynchronization Process" in *LNP Database Synchronization User's Guide*)
- Reconcile (see "Audit and Reconcile Overview" in *LNP Database Synchronization User's Guide*)

- Network Element Database is not Required after Copying an RTDB from its Mate ELAP

If network element's database synchronization is accomplished only by copying an RTDB from its mate ELAP's RTDB, but not when copying from the mate RTDB is performed after copying an RTDB from the remote mated network element or after a bulk load from the LSMS, it is not necessary to distribute the data to the Service Module cards because they are already synchronized with the

RTDB that was used to restore from. Therefore, after the copy, the Service Module cards are now synchronized with both RTDBs.

- Other Network Element Database Distribution

After other LNP database synchronization operations, the network element main LNP database must be distributed by operator intervention to other LNP databases within the network element (both the mate RTDB and the Service Module cards). See [Distributing an RTDB to Service Module Cards](#).

Distributing an RTDB to Service Module Cards

This section describes how to distribute the data from the ELAP RTDB to the Service Module cards after the RTDB has been updated by one of the following actions:

- Copied from an RTDB on the mated network element (see [Copying One RTDB from Another RTDB](#))
- Updated by one of the following operations sent from the LSMS:
 - Bulk loaded from the LSMS (see [Managing Bulk Load from the LSMS](#))
 - Support ELAP Reload Via Database Image (SERVDI) bulk download from the LSMS (see [SERVDI Bulk Download](#).)

1. Distribute the imported RTDB onto each Service Module card, which will also silence the LNP database alarms.

Use one of the following methods:

- Method A loads the imported LNP database onto one Service Module card at a time by reloading each Service Module card.

This method allows the global title translation and LNP functions to continue running while the new RTDB is being loaded. When the Service Module card is reinitializing, its database goes temporarily out of service for the period of time that it takes to reload the database on the Service Module card. The time required to reload the database depends upon the size of the database and can take as long as 23 minutes for an RTDB containing 384 million LNP subscriptions.

- Method B loads the imported RTDB onto all Service Module cards in the EAGLE by reinitializing all the Service Module cards at once.



CAUTION

Caution: This method not only loads the imported LNP database onto the Service Module cards at the same time, but takes all the Service Module cards out of service and the LNP subsystem will be offline. This method should be used only in emergency situations.

Method A: Perform steps 1 and 2 in this method for each Service Module card, one Service Module card at a time.

1. Take the Service Module card out of service with the `rmv-card` command specifying the location of the Service Module card. If there is only one Service Module card in the EAGLE, the `force=yes` parameter must be specified with the `rmv-card` command. For this example, enter this command:

```
rmv-card:loc=1301
```

After successful completion of this command, the EAGLE returns the following output:

```
rlghncxa03w 06-08-01 11:11:28 GMT EAGLE5 39.0
Card has been inhibited.
```

2. Return the Service Module card to service with the `alw-card` command with the location of the Service Module card and the option `data=persist` to allow a warm restart if possible. This command validates that the RTDB on the specified Service Module card is correct. If the RTDB is correct, no further loading is required. If the LNP database is not correct, it is automatically reloaded from the ELAP RTDB; loading may require up to an hour. For this example, enter this command:

```
alw-card:loc=1301:data=persist
```

After successful completion of this command, the EAGLE returns the following output:

```
rlghncxa03w 06-06-01 11:11:28 GMT Eagle5 39.0.0
Card has been allowed.
```

When the Service Module card is returned to service, the major alarm is silenced and UAM 0431, LNP database has been corrected, is generated.

3. Repeat 1 and 2 of Method A for each of the other Service Module cards in the EAGLE.

If any of the Service Module cards continue to boot, contact [My Oracle Support \(MOS\)](#).

Method B: Load the imported RTDB onto all Service Module cards in the EAGLE by reinitializing all the Service Module cards at once by entering the following command:

```
init-card:appl=vsccp
```



CAUTION

Caution: This command initializes all the Service Module cards at once and not only loads the imported RTDB onto the Service Module cards at the same time, but takes all the Service Module cards out of service and the LNP subsystem will be offline. This method should only be used in emergency situations.

Note: A more graceful way of initializing the Service Module cards is to reroute all global title translation traffic, including LNP traffic, to the mate network element using the `inh-map-ss` command. The `inh-map-ss` command takes the mated application subsystem out of service. When the mated application subsystem is out of service, all global title translation traffic, including LNP traffic, is rerouted to the mate network element.

The mated application subsystem must be inhibited with the `inh-map-ss` command before the Service Module cards are reinitialized with the `init-card:appl=vsccp` command. After the `init-card:appl=vsccp` command has finished executing and all the Service Module cards have reinitialized, return the mated application subsystem to service with the `alw-map-ss` command.

When the imported database has been loaded onto each Service Module card, UAM 0431 is displayed for each Service Module card showing that the UAM 0429 has been cleared and the database on the Service Module card matches the database on the MASPs.

If any of the Service Module cards continue to boot, contact [My Oracle Support \(MOS\)](#).

2. Verify that the Service Module cards are in-service by entering the `rept-stat-sccp` command.

The state of the Service Module cards, shown in the `PST` field of the `rept-stat-sccp` command output, should be `IS-NR` (in-service normal). If the state of any Service Module card is not `IS-NR`, contact [My Oracle Support \(MOS\)](#).

Note: The `rept-stat-sccp` command output contains fields that are not used by this procedure. If you want to see the fields displayed by the `rept-stat-sccp` command, see the `rept-stat-sccp` command description in the *Commands User's Guide* for EAGLE.

Disabling Bulk Load

If you have distributed a restored the RTDB LNP data to the Service Module cards (as described in [Distributing an RTDB to Service Module Cards](#)) after an LSMS-initiated procedure, perform the following procedure.

1. If you do not already have a browser window connected to the ELAP, open a browser window and connect your web browser to the ELAP graphical user interface. See [Setting Up an ELAP Workstation](#).

Log in with the user name and password of a user who is authorized to access the menu items shown in this procedure.

2. Select **Maintenance > LSMSHS Bulk Download > Change Enabled**.

The Change LSMS HS Bulk Download Enabled dialog opens, [Figure 99: Change LSMS HS Bulk Download Enabled Dialog](#).

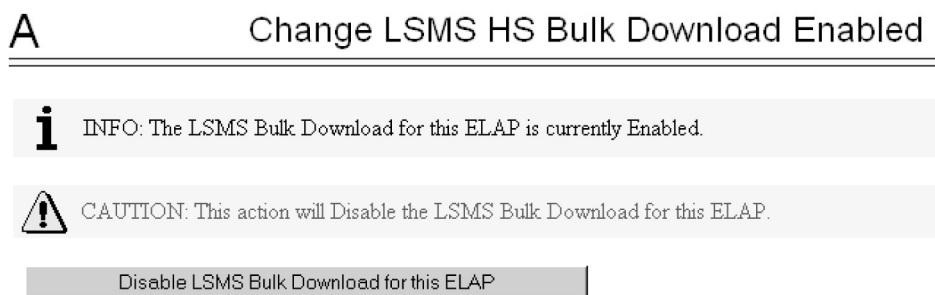


Figure 99: Change LSMS HS Bulk Download Enabled Dialog

The information field should show that the LSMS Bulk Download for this ELAP is currently enabled.

3. Click the **Disable LSMSHS Bulk Download for this ELAP** button.

You have completed this procedure.

Manually Verifying and Restarting the Eagle Agents on the LSMS

This procedure explains how to verify that an Eagle agent has started on the LSMS. It also explains how to stop and start the agent, using the `eagle` command.

The Eagle Agent application (`eagleagent`) is responsible for:

- Subscribing to the broadcast channels to receive all NPAC and local data updates

- Connecting with a single EAGLE node using the HSOP (High Speed Operations Protocol) protocol and forwarding LNP updates to the EAGLE
- Filtering LNP data based on the provisioned filter information before forwarding it to the EAGLE (for more information, refer to [EMS Routing](#))
- Performing automatic resynchronization with an EAGLE node upon connection establishment (for more information, refer to *LNP Database Synchronization User's Guide*)

One instance of the *eagleagent* process exists for each supported EAGLE node.

1. Log in to the LSMS as `lsmsadm` on the active server.
2. Enter the following command to display the status of all EAGLE processes:

```
$ eagle status
```

```
CLLI Pid    State      Resync Conn A Conn B EBDA Debug Queue Memory CPU Timestamp
STPB 27111  NONE_ACTIVE NO_CONNECTION DOWN --- IDLE OFF 0 % 70 M 0.0 % 13:32:53
STPA --- not running
STPC 14616 A_ACTIVE COMPLETE ACTIVE --- IDLE OFF 0 % 70 M 1.0 % 13:32:53
```

If a line similar to the one shown in bold above appears for each supported EAGLE node, you have completed the procedure. If, instead, a line similar to the following line appears, one of these processes has failed; perform the remaining steps of this procedure to restart the processes.

```
STPA --- not running
```

3. Start the Eagle agent by entering this command at the active server, where **<CLLI>** is the Common Language Location Identifier (such as STPA in the example above) for the EAGLE node:

```
$LSMS_DIR/eagle start <CLLI>
```

4. Verify that the Eagle agent has started by repeating [Step 2](#).
If the Eagle agent fails to start, contact [My Oracle Support \(MOS\)](#).

You have now completed this procedure.

Chapter 10

EAGLE 5 Status Reporting and Alarms for ELAP and LNP

Topics:

- *EAGLE 5 Status and Alarm Reporting.....218*
- *EAGLE 5 Maintenance Commands.....221*
- *Unsolicited Alarm Messages and Unsolicited Information Messages.....222*

This chapter describes the ELAP alarm reporting process, EAGLE 5 commands for maintenance functions and status reporting, and EAGLE 5 Unsolicited Alarms and Information Messages.

EAGLE 5 Status and Alarm Reporting

The MPS systems and ELAPs have no direct means of displaying output messages on EAGLE 5 terminals. Maintenance, measurements, status, and alarm information must be routed from the Active ELAP to an arbitrarily selected Service Module card, known as the primary Service Module card.

All the alarms are reported in a common message format. The Active ELAP generates and sends Maintenance Blocks to the primary Service Module card. One Maintenance Block is sent when the IP link is established between the Active ELAP and the primary Service Module card. Additional Maintenance Blocks are sent whenever the ELAP needs to report any change in status or error conditions. The information returned in Maintenance Blocks is included in the status reports produced by the EAGLE 5 `rept-stat-mps` command (see [EAGLE 5 Maintenance Commands](#)).

The ELAP sends Maintenance Blocks that contain (at a minimum) the following information:

- MPS major, minor, and dot software versions
- MPS Status (down/up)
- MPS Status (Active/Standby)

If the ELAP needs to report one or more alarm conditions, it inserts the appropriate alarm data string for the indicated alarm category into the Maintenance Block.

[Table 35: EAGLE 5 MPS Application and Platforms UAM Alarms](#) defines the application and platform alarms that are forwarded to the EAGLE 5. The EAGLE 5 receives the alarm number, alarm text, and alarm data string recovered from the MPS/ELAP.

Table 35: EAGLE 5 MPS Application and Platforms UAM Alarms

Alarm Number	Level	Device	Error Description
370	Critical	MPS A or B	Critical Platform Failure
371	Critical	MPS A or B	Critical Application Failure
372	Major	MPS A or B	Major Platform Failure
373	Major	MPS A or B	Major Application Failure
374	Minor	MPS A or B	Minor Platform Failure
375	Minor	MPS A or B	Minor Application Failure
250	Clearing	MPS A or B	MPS Available

Maintenance Blocks

MPS and ELAP have no direct means of accepting user input from or displaying output messages on EAGLE terminals. Maintenance, measurements, error, and status information are routed to the EAGLE through the primary Service Module card.

The Active ELAP generates and sends Maintenance Blocks to an arbitrarily selected Service Module card known as the primary Service Module card. One Maintenance Block is sent as soon as the IP link is established between the Active ELAP and the primary Service Module card. Additional Maintenance Blocks are sent whenever the ELAP needs to report any change in status or error conditions. The information returned in Maintenance Blocks is also included in the output of the EAGLE `rept-stat-mps` command.

It is possible for the ELAP to be at a provisioning congestion threshold, and to be entering and exiting congested mode at a very high rate of speed. To minimize this *thrashing* effect, the ELAP is restricted to sending no more than one ELAP Maintenance Block per second.

ELAP Maintenance Block Contents

The ELAP sends Maintenance Blocks that contain (at a minimum) the following information. The actual states are defined in the description of the `rept-stat-mps` command in *Commands Manual*.

- MPS major, minor, and dot software versions
- MPS Status (down/up)
- MPS Status (Active/Standby)

If the ELAP needs to report one or more alarm conditions, it inserts the appropriate alarm data string for the indicated alarm category into the Maintenance Block.

EAGLE Alarm Reporting of ELAP Alarms

A 16-character hexadecimal alarm data string reports any errors found during the last System Health Check and the level of severity for each error. The first character (four bits) uniquely identifies the alarm severity for the alarm data. The remaining 15 characters (60 bits) uniquely identify up to 60 individual failure cases for the alarm category.

The System Health Check (syscheck) is responsible for forwarding platform errors to the application. The application combines the platform alarms with the application alarms and forwards all of this information to EAGLE. The information that is transferred is described in *Alarms and Maintenance for ELAP*. [MPS Platform and ELAP Application Alarms](#) describes the application and platform alarms that are forwarded to the EAGLE. The EAGLE receives the alarm number, alarm text, and alarm data string recovered from the MPS/ELAP.

Alarm Priorities

The ELAP sends the maintenance information, including the alarm data strings, to the EAGLE 5 ISS for interpretation. Alarm priorities determine which alarm category is displayed at the EAGLE 5 ISS terminal when multiple alarm levels exist simultaneously. EAGLE 5 ISS prioritizes the data and displays only the alarm category with the highest severity level and priority for each MPS.

If an alarm category of lower priority is sent from the MPS, the lower priority alarm category is not displayed on the EAGLE 5 ISS terminal until any higher priority alarms are cleared.

Multiple Alarm Conditions

Critical, major and minor alarms appear repeatedly in each alarm delivery to the EAGLE 5 ISS until the alarm condition clears.

If multiple alarms exist, the highest priority alarm category is the Active Alarm. The Active Alarm is shown in the output from the `rept-stat-trbl` command and the `rept-stat-mps` command, and the alarm count associated with this alarm is included in the `rept-stat-alm` command output.

Though only the highest priority alarm is displayed at the EAGLE 5 ISS terminal when multiple alarms are reported, you can use the EAGLE 5 ISS `rept-stat-mps` command to list the alarm data strings for all of the alarm categories with existing alarms. Then you can use the ELAP user interface Maintenance menu item Decode EAGLE 5 ISS Output of MPS Alarms to convert the hexadecimal alarm data string to text. The output text shows the alarm category represented by the string and the alarm text for each alarm encoded in the string.

Service Module Card Status Requests and Status Messages

When the ELAP needs to know the status of a Service Module card, it can send a Service Module Card Status Request to all Service Module cards. Because status messages are sent over UDP, the ELAP broadcasts the Service Module Card Status Request and each Service Module card returns its status to the ELAP.

Service Module cards send a Service Module Card Status Message to the ELAP when any of the following events occur in the Service Module card:

- The Service Module card is booted.
- The Service Module card receives a Service Module Card Status Request message from the ELAP
- The Service Module card determines that it needs to download the entire RTDB; for example, the Service Module card determines that the RTDB needs to be downloaded because it is totally corrupted, or a craftsperson requests that the RTDB be reloaded.
- The Service Module card starts receiving RTDB downloads or updates. When a Service Module card starts downloading the RTDB, or if the Service Module card starts accepting database updates, it sends a Service Module Card Status Message informing the ELAP of the first record received. This helps the ELAP keep track of downloads in progress.

The Service Module Card Status Message provides the following information to the ELAP:

- Service Module card Memory Size - When the Service Module card is initialized, it determines the amount of applique memory present. The ELAP uses this value to determine if the Service Module card has enough memory to hold the RTDB.
- Database Level Number - The ELAP maintains a level number for the RTDB. Each time the database is updated, the level number will be incremented. When the database is sent to the Service Module card, the Service Module card keeps track of the database level number. The database level number is included in all Status messages sent from the Service Module card. A level number of 0 signifies that no database has been loaded into the Service Module card (this can be done any time the Service Module card wants to request a full database download).
- Database Download Starting Record Number - When the Service Module card starts downloading either the entire RTDB or updates to the database, it will identify the starting record number. This allows the ELAP to know when to wrap around the end of the file, and when the Service Module card has finished receiving the file or updates.

EAGLE 5 Maintenance Commands

The EAGLE 5 commands described in this section can be used for maintenance functions for LNP, including reporting status and alarm information.

Refer to *Commands Manual* for complete command descriptions, parameters and valid values, rules for using the commands correctly, and output examples.

rept-stat-lnp

The `rept-stat-lnp` command reports LNP status information.

When the `rept-stat-lnp` command is entered with no parameters, a summary of the LNP status of all equipped Service Module cards is provided. The summary includes Global Title Translation (GTT) and LNP function status for every Service Module card, as well as LNP Query Service system information.

When the `loc` parameter is specified, a detailed status of LNP information for the specified Service Module card is provided. The detailed reports include information for each of the following functions: Global Title Translation (GTT), LNP Message Relay (LNPMR), LNP Query Service (LNPQS), Personal Communication Service LNP Query Service (PLNPQS) (if the PLNP feature is turned on), Wireless LNP Query Service (WNPQS) (if the WNP feature is turned on), Triggerless LNP (TLNP) (if the TLNP feature is turned on), LRNQT (if the ITU TCAP LRN Query feature is turned on), and Automatic Call Gap (ACG).

When the `card=sccp` all parameter is specified, a detailed status of LNP information for all Service Module cards is provided.

rept-stat-db

The `rept-stat-db` command report includes the RTDB birthdate, level, and status. This information is used to help determine the need for and method to use for an RTDB resynchronization, audit and reconcile, reload from another RTDB, or bulk load from LSMS.

rept-stat-mps

The `rept-stat-mps` command reports the status of the provisioning system, including MPS platform status and ELAP status.

The `rept-stat-mps` command produces a summary report showing the overall status of the provisioning system and a moderate level of information for each Service Module card.

The `rept-stat-mps:loc=xxxx` command produces a more detailed report showing the status of a specific Service Module card.

When the ELAP sends database updates to the Service Module cards, the update messages include a field that contains the new database memory requirements. This version of the `rept-stat-mps` command displays the amount of memory used by the RTDB as a percent of available Service Module card memory.

Each Service Module card monitors the database size requirements and issues a minor alarm if the size of the database exceeds the configured percentage allowed. See [Modify System Defaults](#) for more information on configured percentages. If a database increases to the point that it occupies 100% of the Service Module card memory, it issues a major alarm.

rept-stat-trbl

The `rept-stat-trbl` command output includes the Service Module card and ELAP IP link alarms.

rept-stat-alm

The `rept-stat-alm` command output includes the alarm totals for the Service Module card and ELAP IP links.

Unsolicited Alarm Messages and Unsolicited Information Messages

The following sections describe MPS and ELAP Unsolicited Alarm Messages (UAMs) and Unsolicited Information Messages (UIMs).

The EAGLE outputs two types of unsolicited messages:

- **Unsolicited Alarm Messages (UAMs)** - Denotes persistent problems with a device or object that needs the attention of a craftsman.
- **Unsolicited Informational Messages (UIMs)** - Indicates transient events that have occurred.

Unsolicited Alarm Messages are generated by the maintenance system as trouble notification for the OS. The maintenance system is able to determine the status of the system through polling and periodic audits. Troubles are detected through analysis of system status and notifications from various subsystems in the EAGLE. The EAGLE controls and generates the alarm number, associated text, and formatting for alarms sent to EAGLE through the Maintenance Block mechanism for the ELAP.

Unsolicited Alarm and Information Messages describes all EAGLE UAMs and the appropriate recovery actions.

MPS Platform and ELAP Application Alarms

MPS platform and ELAP application alarms are reported in the following six categories of alarms:

- **Critical Platform Alarm**—This is a 16-character hexadecimal string in which each bit represents a unique critical platform failure and alarm. An alarm in this category results in the associated MPS state being set to OOS-MT / / Fault.
- **Major Platform Alarm**—This is a 16-character hexadecimal string in which each bit represents a unique major platform failure and alarm. An alarm in this category results in the associated MPS state being set to OOS-MT / / Fault.
- **Minor Platform Alarm**—This is a 16-character hexadecimal string in which each bit represents a unique minor platform failure and alarm. An alarm in this category results in the associated MPS state being set to IS-ANR / / Restricted.
- **Critical Application Alarm**—This is a 16-character hexadecimal string in which each bit represents a unique critical application failure/ alarm. An alarm in this category results in the associated MPS state being set to OOS-MT / / Fault.
- **Major Application Alarm**—This is a 16-character hexadecimal string in which each bit represents a unique major application failure/ alarm. An alarm in this category results in the associated MPS state being set to OOS-MT / / Fault.

- **Minor Application Alarm**—This is a 16-character hexadecimal string in which each bit represents a unique minor application failure and alarm. An alarm in this category results in the associated MPS state being set to IS-ANR/Restricted.

The alarm categories, shown in [Table 36: MPS Platform and ELAP Alarm Category UAMs](#), are forwarded to the EAGLE when MPS and ELAP failures or errors are detected. Each alarm category is sent with a hexadecimal alarm data string that encodes all alarms detected in that category (see [EAGLE 5 Status and Alarm Reporting](#)). The clearing alarm for all of the MPS Platform and Application alarms is UAM 0250, MPS Available.

Note: The recovery actions for the platform and application alarms are defined in *Alarms and Maintenance* for ELAP.

Table 36: MPS Platform and ELAP Alarm Category UAMs

UAM #	Severity	Message Text
370	Critical	Critical Platform Failure(s)
371	Critical	Critical Application Failure(s)
372	Major	Major Platform Failure(s)
373	Major	Major Application Failure(s)
374	Minor	Minor Platform Failure(s)
375	Minor	Minor Application Failure(s)

Table 37: MPS Available UAM

UAM #	Severity	Message Text
250	None	MPS available

The clearing alarm is generated after existing alarms have been cleared. The clearing alarm sets the MPS primary status to IS-NR.

ELAP-to-Service Module Card Connection Status

The ELAP and the Service Module card are connected over one 100BASE-T Ethernet network that runs at 100 Mbps and one 10BASE-T Ethernet network that runs at 10 Mbps, and use TCP/IP. In the event connection is inoperative, the Service Module card is responsible for generating an appropriate UAM. Loss of connectivity or inability of the ELAP to communicate (from hardware or software failure, for example) is detected and reported within 30 seconds.

ELAP-Service Module Card UAMs

Maintenance Blocks sent from the ELAP have a field to identify error message requests. (See [Maintenance Blocks](#)). The Service Module card processes incoming Maintenance Blocks and generates the requested UAM. The Service Module card acts only as a delivery agent. The recovery actions for the ELAP-Service

Module card UAMs are defined in "UAM/UIM Troubleshooting" chapter in *Unsolicited Alarm and Information Messages Manual*.

Service Module Card-ELAP Link Status Alarms

Two alarms indicate the Service Module card-to-MPS link status:

- 0084 "IP Connection Unavailable" (Major)
- 0085 "IP Connection Available" (Normal/Clearing)

Example:

```

      1      2      3      4      5      6      7
8
123456789012345678901234567890123456789012345678901234567890
      station1234 00-09-30 16:28:08 EST EAGLE 35.0.0-35.10.0
** 3582.0084 ** DSM B 1217 IP Connection Unavailable

```

RTDB Audit Alarms

During an audit of the Service Module cards and the ELAPs, the status of each Real-Time Database (RTDB) is examined and the following alarms can be raised. The recovery actions for the RTDB Audit Alarms are defined in the "UAM/UIM Troubleshooting" chapter in *Unsolicited Alarm and Information Messages Manual*.

Table 38: RTDB Audit Alarms

UAM #	Alarm Level	Trigger	Message Text
443	Major	An RTDB has become corrupted.	RTDB database corrupted
444	Minor	A card's RTDB is inconsistent (its contents are not identical to the current RTDB on the Active ELAP fixed disks	RTDB database is inconsistent
445	N/A	An inconsistent, incoherent, or corrupted RTDB has been fixed and the card or ELAP is an IS-NR condition.	RTDB database has been corrected
448	Minor	The RTDB is being downloaded or an update has failed. Therefore, the RTDB is in an incoherent state.	RTDB database incoherent

UAM #	Alarm Level	Trigger	Message Text
449	Major	A Service Module card detects that its RTDB needs to be resynchronized and has started the resyn operation.	RTDB resynchronization in progress
450	Informational	A Service Module card completes its RTDB resync operation.	RTDB resynchronization complete
451	Major	A Service Module card detects that its RTDB needs to be reloaded because the resync log does not contain all of the required updates.	RTDB reload required

Feature Quantity Capacity UAMs

The following alarms are issued when the Service Module card detects the capacity has been exceeded. The recovery actions for the Feature Quantity Capacity Alarms are defined in the "UAM/UEM Troubleshooting" chapter in *Unsolicited Alarm and Information Messages Manual*.

Table 39: Feature Quantity Capacity Alarms

UAM #	Alarm Level	Trigger	Message Text
283	Major	The NPANXXX totals on the Service Module cards have reached 90% of the total NPANXX capacity that is currently configured for the EAGLE 5 ISS.	LNP Ported LRNs approaching Feat. Capacity
284	N/A	A previous fault with the number of LNP ported NPAs is greater than the capacity this feature supports has been corrected.	LNP Ported NPAs exceeds feat. Capacity
285	Major	The LRN totals on the Service Module cards has reached 90% of the total LRN capacity that is currently configured for the EAGLE 5 ISS.	LNP Ported NPAs approaching Feat. Capacity

UAM #	Alarm Level	Trigger	Message Text
286	N/A	A previous fault with the number of LNP ported LRNs is greater than the capacity this feature supports has been corrected.	LNP Ported NPAs Capacity Normal
287	Critical	The total TNs in the LNP database has reached the configurable percentage (default value is 95%) of the allowed Feature Access Key (FAK) capacity currently configured for the EAGLE 5 ISS.	RTDB Table Level 2 FAK Cap Exceeded
288	Major	The total TNs in the LNP database has reached the configurable percentage (default value is 80%) of the allowed Feature Key capacity currently configured for the EAGLE 5 ISS. The configured threshold value for UAM 0288 must be less than the configured threshold value for UAM 0287.	RTDB Table Level 2 FAK Cap Exceeded
289	N/A	A previous LNP FAK alarm condition no longer exists.	RTDB Table FAK Capacity Normal

Physical Memory Usage UAMs

The following alarms are issued when the Service Module card detects the RTDB memory capacity is not adequate for the ELAP feature. The recovery actions for the Physical Memory Usage Alarms are defined in "UAM/UIM Troubleshooting" chapter in the *Unsolicited Alarm and Information Messages Manual*.

Table 40: Physical Memory Usage Alarms

UAM #	Alarm Level	Trigger	Message Text
442	Critical	The RTDB physical memory usage threshold exceeds 95% for the specified number of TNs, LRNs, or NPAs.	RTDB database capacity is 90% full
446	Minor	The RTDB physical memory usage threshold exceeds 80% for the specified number of TNs, LRNs, or NPAs.	RTDB database capacity is 80% full
447	N/A	A previous RTDB physical memory usage alarm condition no longer exists.	RTDB database capacity alarm cleared

EAGLE Service Module Card Audit UIMs

The Service Module card performs data validation checks prior to applying updates and changes to the RTDB. This consist of comparing the checksum in the data about to be overwritten with the old checksum (new data element) in the update about to be applied.

A UIM is created when validation failure occurs because the target-cell checksums do not match the source-cell checksums. The updates are not applied and the database is marked incoherent.

Measurement Capacity UIMs

When the Measurements Platform is not installed, the OAM-based Measurements Subsystem will collect up to 100,000 LRNs and 150,000 NPANXXs from the SCCP cards. If the number of provisioned LRNs exceeds 100,000 or the number of provisioned NPANXXs exceeds 150,000, the Measurements Subsystem will generate a UIM at each hourly collection interval. The UIM is a warning that measurements data have been discarded. The UIM output may be suppressed by setting the UIM threshold limit to zero. More information on the Measurement Capacity UIMs are defined in "UAM/UIM Troubleshooting" chapter in the *Unsolicited Alarm and Information Messages Manual*.

Table 41: Measurement Capacity UIMs

UIM #	Alarm Level	Trigger	Message Text
1310	N/A	The Measurements Platform is not enabled and the number of provisioned LRNs exceeds 100,000. This UIM is notification that the LNPLRN	System Meas. Limit exceeded for LRN

UIM #	Alarm Level	Trigger	Message Text
		measurements report will be truncated, and additional LRN measurements will not be collected or reported.	
1311	N/A	The Measurements Platform is not enabled and the number of provisioned NPANXXs exceeds 150,000. This UIM is notification that the LNPNPANXXs measurements report will be truncated, and additional NPANXX measurements will not be collected or reported.	System Meas. Limit exceeded for NPANXX

Chapter 11

Automatic Call Gapping (ACG) Configuration

Topics:

- [*Overview.....230*](#)
- [*Determining the ACG Node Overload Control Level Query Rates.....233*](#)
- [*Adding an ACG Node Overload Control Level.....236*](#)
- [*Removing an ACG Node Overload Control Level.....237*](#)
- [*Changing an ACG Node Overload Control Level.....238*](#)
- [*Adding ACG Manual Initiated Controls.....238*](#)
- [*Removing ACG Manual Initiated Controls.....240*](#)
- [*Changing ACG Manual Initiated Controls.....240*](#)

This chapter describes how to determine traffic capacity and node overload control levels, and how to add and remove ACG node overload control levels and ACG manual initiated controls.

Overview

Location routing number (LRN) queries for a particular telephone number or a portion of a telephone number are received by the EAGLE 5 ISS when a particular threshold is reached. ACG controls are used under two conditions:

1. When a node overload condition is detected and an ACG control is configured for that overload level, the EAGLE 5 ISS sends an ACG component within each LRN query response it processes. The ACG control is invoked for the first 6 or 10 digits of the called party address in all queries sent to the EAGLE 5 ISS to control the rate that queries are processed.
2. If no overload control is in place, LRNQT sends an ACG for a manually initiated control to block queries. Manually initiated control procedures are similar to overload control procedures, but shall be able to vary the number of digits that are to be placed under control (3 or 6-10 digits). Since LRNQT may have to process queries for ported (LRN routing) and non-ported numbers (default routing), the user shall be able to initiate control on any number. A list of all numbers for which the user has initiated controls shall be maintained. This list shall be the same across AIN and LRNQT services.

In addition to the digits applied to the ACG control, the ACG control contains a duration index and a gap interval index. The duration index is a timer defining the amount of time the ACG control is in effect. The gap interval index is a timer that defines the rate that queries are processed in the EAGLE 5 ISS. For example, the ACG control may be in effect for 128 seconds, the duration index, and a query is processed every 2 seconds, the gap interval index. When the ACG control is detected, the duration timer and gap interval timer are started. Until the gap timer expires, all calls containing the specified number of digits or the specified digits are routed to reorder tone or to an announcement indicating that the call cannot be completed. Once the gap timer has expired, the next call containing the matching dialed digits is processed normally and the gap timer is restarted. This cycle continues until the ACG control is cancelled by the EAGLE 5 ISS or the duration timer expires. [Table 42: Duration and Gap Interval Index Values](#) shows the values for the duration index and the gap index used in the automatic call gapping commands.

Table 42: Duration and Gap Interval Index Values

Index	Duration Index Value (DRTN) in seconds	Node Overload Control Interval or IN Manual Initiated Control Interval Index Value (INTVL) in seconds	AIN Manual Initiated Control Interval Index Value (AINTVL) in seconds
0	N/A	0	N/A
1	1	3	0
2	2	4	0.1
3	4	6	0.25
4	8	8	0.5
5	16	11	1

Index	Duration Index Value (<i>DRTN</i>) in seconds	Node Overload Control Interval or IN Manual Initiated Control Interval Index Value (<i>INTVL</i>) in seconds	AIN Manual Initiated Control Interval Index Value (<i>AINTVL</i>) in seconds
6	32	16	2
7	64	22	5
8	128	30	10
9	256	42	15
10	512	58	30
11	1024	81	60
12	2048	112	120
13	infinite	156	300
14	N/A	217	600
15	N/A	300	infinite

Node Overload Control

The EAGLE 5 ISS does not maintain overload levels for individual subsystems, but maintains an overload level for the entire EAGLE 5 ISS, the node. There are 10 overload levels that are defined for the EAGLE 5 ISS. Each overload level contains the following information.

- The number of queries in a 30-second period that defines each overload level. When the defined number of queries is reached, the ACG control for the overload level goes into effect.
- The number of digits to control from AIN queries
- The number of digits to control from IN queries
- The duration index of the ACG control
- The gap interval index of the ACG control

Only overload levels 1 through 9 can be added or removed from the database; level 10 cannot be removed but can be changed. Overload level 10 is predefined with the following values:

- The number of queries = 2,147,483,647
- The number of digits from AIN queries to control = 6
- The number of digits from IN queries to control = 6
- The gap interval index = 7 - 22 seconds
- The duration index = 1 - 1 second

Any overload levels that are not configured are not used. If no overload levels are configured or if any LIMs are denied SCCP service, then overload level 10 is used for the ACG node overload control.

Manually Initiated Control

Manually initiated controls are applied to a specific 10-digit telephone number or to a part of a specific telephone number in either AIN queries or IN queries. The manually initiated control can contain the first 3, 6, 7, 8, or 9 digits, or all 10 digits, of the telephone number.

The duration index of a manually initiated control uses the same values as the duration index of a node overload control.

A manually initiated control contains a gap interval index for IN queries, using the same values as the gap interval index for the node overload control levels, and a gap interval index for AIN queries using different values.

For IN queries, the digits sent for manually initiated controls are the original 10 digits of the Called Party Number. For example, if a query for Called Party Number 919-460-2132 triggers a manually initiated control for the digits 919, the digits parameter of the ACG is 919-460-2132 instead of 919.

A manually initiated control can be applied to all queries sent to the EAGLE 5 ISS. This type of manually initiated control specifies the number of digits from the dialed digits of the query. For manually initiated controls that apply to particular query services and Called Party digits, the number of digits to use in the ACG component is the number of digits in the specified digit string.

The database can contain a manually initiated control that applies to all queries and manually initiated controls that apply to specific combinations of query service and Called Party digits. When more than one control applies to a specific query, the one selected is the one containing the higher number of digits. If a manually initiated control cannot be selected with the number of digits, then the control with the higher gap interval index value is selected. If the controls contain the same gap interval index value, then the control with the higher duration index value is selected. The following example illustrates how the controls are selected.

1. A control for AIN LNP queries for Called Party digits of 919-460-2 is entered into the database. (ent-acg-mic:serv=ain:aintvl=1:dgts=9194602:drtn=3).
2. A control with an interval index of 10 for AIN LNP queries for Called Party digits of 919-460 is entered into the database. (ent-acg-mic:aintvl=10:serv=ain:dgts=919460:drtn=12:).
3. A control with an interval index of 7 for all queries, and the number of digits used for the control is 6, is entered into the database. (ent-acg-mic:intvl=7:type=all:nd=6:drtn=12:aintvl=7)
4. The EAGLE 5 ISS receives an AIN query for the Called Party Address 919-461-1017.
5. The EAGLE 5 ISS sends an ACG for 919-461. The control entered in item 3 is the only one that applies.
6. The EAGLE 5 ISS receives an AIN query for Called Party Address 919-460-2132.
7. The EAGLE 5 ISS sends ACG for 919-460-2. The control entered in item 1 is more specific than the controls entered in items 2 and 3.
8. The EAGLE 5 ISS receives an AIN query for Called Party Address 919-460-5500.
9. The EAGLE 5 ISS sends ACG with a interval index of 10 for 919-460. The control entered in item 2 is more specific than the control entered in item 3. The control entered in item 1 does not apply.

Determining the ACG Node Overload Control Level Query Rates

The query rates for the ACG node overload control levels are the number of LNP queries (messages or transactions) received by the EAGLE 5 ISS in a 30-second period. When the defined number of queries is reached, the ACG control for that node overload control level goes into effect.

The following values are used to calculate the query rates for the node overload control levels.

N = the number of Service Module cards running the VSCCP application installed in the EAGLE 5 ISS.

S = the total EAGLE 5 ISS SCCP traffic capacity in messages per second

P = The LNP query portion of the SCCP traffic, from 0% to 100%, determined from the traffic studies.

Q = The LNP query portion of the total EAGLE 5 ISS SCCP traffic capacity in messages per second

F = The query rate of the first ACG node overload control level at 80% of the total LNP query portion of the SCCP traffic, in messages per 30 seconds

L = The query rate of the last ACG node overload control level at 100% of the total SCCP traffic, in messages per 30 seconds

NL = The number of ACG node overload control levels being used.

I = The increment of the query rate between the node overload control levels.

The query rates are configured with the `qr` parameter of `ent-acg-noc` and `chg-acg-noc` commands.

Any node overload control levels that are not configured are not used. If no node overload control levels are configured or if any LIMs are denied SCCP service, then node overload control level 10 is used for the ACG node overload control. Node overload control level 10 cannot be added with the `ent-acg-noc` command or removed with the `dlt-acg-noc` command, but can be changed with the `chg-acg-noc` command. It is recommended that the query rate for node overload control level 10 is not changed. The default query rate for node overload control level 10 is 2,147,483,647 messages per 30 seconds.



Caution: If the query rate for node overload control level 10 is changed, then node overload control level 10 is used as any other node overload control level, in addition to the default conditions that node overload control level 10 is used for (no node overload control levels are configured or for any LIMs denied SCCP service). If the query rate for node overload control level 10 is changed, make sure that the duration and interval timer values assigned to node overload control level 10 are appropriate for all three conditions or traffic may be lost.

When the query rate of node overload control level 10 is not changed, node overload control level 10 is used only for its default conditions and is not treated as another node overload control level.

Determining the Total EAGLE 5 ISS SCCP Traffic Capacity (S)

The total EAGLE 5 ISS traffic capacity is determined from the number of Service Module cards running the VSCCP application installed in the EAGLE 5 ISS (N). LNP requires E5-SM4G cards and E5-SM8G-B cards as Service Module cards. E5-SM4G cards can operate at either 5000 transactions (or messages) per second (TPS) or 6800 TPS, depending on the enabled quantity of the E5-SM4G Throughput Capacity feature in the EAGLE 5 ISS. E5-SM8G-B cards can operate at 5000, 6800, or 10,000 TPS, depending on the enabled quantity of the E5-SM4G Throughput Capacity feature in the EAGLE 5 ISS. The number

of Service Module cards used in this calculation is one less than the total number of Service Module cards in the EAGLE 5 ISS. One Service Module card is used as a standby card.

To determine the total EAGLE 5 ISS SCCP traffic capacity (S), subtract 1 from the total number of Service Module cards running the VSCCP application and multiply the result by the enabled E5-SM4G/E5-SM8G-B card TPS value.

$$(N-1) \times \text{E5-SM4G/E5-SM8G-B TPS} = \text{Total SCCP traffic capacity (S)}$$

Determining the LNP Query Portion of the Total SCCP EAGLE 5 ISS Traffic Capacity (Q)

The LNP query portion of the SCCP traffic (Q) is a percentage of the total EAGLE 5 ISS SCCP traffic (P) as determined from the traffic studies.

After the LNP query percentage is determined, multiply the total EAGLE 5 ISS SCCP traffic capacity (S) by the LNP query percentage.

$$S \times P = Q$$

Determining the Query Rate of the First ACG Node Overload Control Level (F)

The ACG node overload controls should start when the LNP query portion of the SCCP traffic reaches 80% of the total LNP query portion of the SCCP traffic (Q). The ACG node overload control level is determined by the number of messages received over a 30 second period of time.

To determine the query rate of the first ACG node overload control level (F), in messages per 30 seconds, multiply the total LNP query portion of the SCCP traffic (Q) by 0.8, then multiply that result by 30.

$$Q \times 0.8 \times 30 = F$$

Determining the Query Rate of the Last ACG Node Overload Control Level (L)

The ACG node overload controls should continue until the LNP query portion of the SCCP traffic reaches 100% of the total SCCP traffic (S).

To determine the query rate of the last ACG node overload control level (L), in messages per 30 seconds, multiply the total LNP query portion of the SCCP traffic by 30.

$$S \times 30 = L$$

Determining the Increment of Query Rates between ACG Node Overload Control Levels (I)

If the number of ACG node overload control levels being used is 3 or more, the query rates of each node overload control level between the first and the last node overload control level can be evenly divided.

Subtract the query rate of the first level from the query rate of the last level and divide the result by the number of node overload control levels (NL) being used minus 1.

$$(L - F) / (NL - 1) = I$$

Setting the Query Rate for ACG Node Overload Control Levels

To determine the query rate for each ACG NOC level after the first level and before the last level, add the increment value (I) to each successive level. For example,

If three node overload control levels are being used:

- The query rate for the first node control level = F
- The query rate for the second node control level = F + I
- The query rate for the third node control level = L

If four node overload control levels are being used:

- The query rate for the first node control level = F
- The query rate for the second node control level = F + I
- The query rate for the third node control level = F + 2I
- The query rate for the fourth node control level = L

If nine node overload control levels are being used:

- The query rate for the first node control level = F
- The query rate for the second node control level = F + I
- The query rate for the third node control level = F + 2I
- The query rate for the fourth node control level = F + 3I
- The query rate for the fifth node control level = F + 4I
- The query rate for the sixth node control level = F + 5I
- The query rate for the seventh node control level = F + 6I
- The query rate for the eighth node control level = F + 7I
- The query rate for the ninth node control level = L

ACG NOC Configuration Examples

[Table 43: ACG NOC Configuration Examples](#) illustrates ACG NOC configuration for different numbers of ACG NOC levels, Service Module cards, and E5-SM4G/E5-SM8G-B TPS rates.

Table 43: ACG NOC Configuration Examples

Example	1	2
Configuration: P=% LNP Query traffic N=Service Module cards NL=Number of ACG NOC levels Card TPS rate	P=0.7 (70%) N=21 NL=7 (3-9) 5000 TPS	P=0.6 (60%) N=17 NL=4 (2, 4, 6, 8) 6800 TPS
1. Total SCCP traffic capacity	$(N-1) \times 5000 = S$ $20 \times 5000 = 100000$	$(N-1) \times 6800 = S$ $16 \times 6800 = 108800$
2. LNP Query portion of SCCP traffic	$S \times P = Q$ $100000 \times 0.7 = 70000 \text{ TPS}$	$S \times P = Q$ $108800 \times 0.6 = 652800 \text{ TPS}$
3. Query rate of first ACG NOC level	$Q \times 0.8 \times 30 = F$ $70000 \times 0.8 \times 30 = 1680000$	$Q \times 0.8 \times 30 = F$ $652800 \times 0.8 \times 30 = 1566720$
4. Query rate of last ACG NOC level	$S \times 30 = L$	$S \times 30 = L$

Example	1	2
	$100000 \times 30 = 3000000$	$108800 \times 30 = 3264000$
5. Increment between levels	$(L-F)/(NL-1) = I$ $(3000000-1680000)/6 = 220000$	$(L-F)/(NL-1) = I$ $(3264000-1566720)/3 = 565760$
6. Commands to set levels - see Table 44: Commands to Set ACG NOC Levels in Example 1 and Example 2 .		

The commands in [Table 44: Commands to Set ACG NOC Levels in Example 1 and Example 2](#) could be used to set the ACG NOC levels for Example 1 and Example 2 in [Table 43: ACG NOC Configuration Examples](#).

Table 44: Commands to Set ACG NOC Levels in Example 1 and Example 2

Example 1	Example 2
ent-acg-noc:lvl=3:qr=1680000:drtn=3:intvl=3	ent-acg-noc:lvl=2:qr=1566720:drtn=3:intvl=3
ent-acg-noc:lvl=4:qr=1900000:drtn=4:intvl=4	ent-acg-noc:lvl=4:qr=2132480:drtn=4:intvl=4
ent-acg-noc:lvl=5:qr=2120000:drtn=5:intvl=5	ent-acg-noc:lvl=6:qr=2698240:drtn=6:intvl=6
ent-acg-noc:lvl=6:qr=2340000:drtn=6:intvl=6	ent-acg-noc:lvl=8:qr=3264000:drtn=8:intvl=8
ent-acg-noc:lvl=7:qr=2560000:drtn=7:intvl=7	
ent-acg-noc:lvl=8:qr=2780000:drtn=8:intvl=8	
ent-acg-noc:lvl=9:qr=3000000:drtn=9:intvl=9	

Adding an ACG Node Overload Control Level

This procedure is used to add an ACG node overload control level to the database using the `ent-acg-noc` command.

Refer to the *Commands Manual* for a complete description of the `ent/chg/rtrv-acg-noc` commands, including parameter names, valid values, rules for using the command correctly, and output examples.

The interval index is the amount of time between ACGs. This is a number that is mapped to a time value at the LNP node. See [Table 42: Duration and Gap Interval Index Values](#).

The duration index is the amount of time that the ACG is in effect. This is a number that is mapped to a time value at the LNP node. See [Table 42: Duration and Gap Interval Index Values](#).

Overload level 10 is predefined in the database and cannot be added to or removed from the database. Its values can be changed, though it is recommended that they not be changed. See [Node Overload Control](#).

Prerequisite for Adding an ACG NOC Level

Before an ACG node overload control can be added, the LNP feature must be enabled.

- Enter the `rtrv-ctrl-feat` command to display the controlled features that are enabled in the system.
- If the LNP feature is enabled, the entry `LNP ported TNs` is shown in the `rtrv-ctrl-feat` output with a quantity greater than 0. Continue with the procedure in this section.
- If the LNP feature is not enabled, perform the procedures in the [LNP Feature Configuration](#) to enable the LNP feature. Then continue with the procedure in this section.

1. Display the ACG node overload levels in the database by entering the `rtrv-acg-noc` command.
Verify that the ACG NOC level that is to be added is not already in the database.
2. Add the ACG node overload control level to the database using the `ent-acg-noc` command.
See [Determining the ACG Node Overload Control Level Query Rates](#) for an explanation of how to determine the Query Rate for the level.
3. Verify the changes using the `rtrv-acg-noc` command.
4. Back up the changes using the `chg-db:action=backup:dest=fixed` command.
The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.  
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.  
BACKUP (FIXED): MASP A - Backup starts on standby MASP.  
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Removing an ACG Node Overload Control Level

This procedure is used to remove an ACG Node Overload Control Level from the database using the `dlt-acg-noc` command.

The `dlt-acg-noc` command uses only one parameter, `lvl` – the overload levels 1 through 9. The database contains 10 ACG node overload levels, but only nine can be added or removed.

Overload level 10 cannot be removed from the database, but its values can be changed using the [Changing an ACG Node Overload Control Level](#) procedure.

The overload level to be removed must be in the database.

Refer to the *Commands Manual* for complete descriptions of the commands that are used in the following procedure, including parameter names, valid values, rules for using the command correctly, and output examples.

1. Display the ACG node overload levels in the database by entering the `rtrv-acg-noc` command.
2. Remove the ACG node overload control level from the database using the `dlt-acg-noc` command.
3. Verify the changes using the `rtrv-acg-noc` command.
4. Back up the changes using the `chg-db:action=backup:dest=fixed` command.
The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.  
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.  
BACKUP (FIXED): MASP A - Backup starts on standby MASP.  
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Changing an ACG Node Overload Control Level

This procedure is used to change the values of an existing ACG Node Overload Control Level in the database using the `chg-acg-noc` command.

Refer to the Commands Manual for complete descriptions of the commands used in the procedure in this section, including parameter names, valid values, rules for using the command correctly, and output examples.

he interval index is the amount of time between ACGs. This is a number that is mapped to a time value at the LNP node. See [Table 42: Duration and Gap Interval Index Values](#).

he duration index is the amount of time that the ACG is in effect. This is a number that is mapped to a time value at the LNP node. See [Table 42: Duration and Gap Interval Index Values](#).

1. Display the ACG node overload levels in the database by entering the `rtrv-acg-noc` command.
Verify that the ACG NOC level to be changed is in the database.
2. Change the ACG node overload control level values in the database using the `chg-acg-noc` command.
3. Verify the changes using the `rtrv-acg-noc` command.
4. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.  
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.  
BACKUP (FIXED): MASP A - Backup starts on standby MASP.  
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Adding ACG Manual Initiated Controls

This procedure is used to assign ACG controls to all LNP queries or to specific LNP query services and Called Party digits using the `ent-acg-mic` command. If the EAGLE 5 ISS query service receives a query to which a control applies, then the EAGLE 5 ISS sends an ACG, encoded as configured, with the response.

Refer to the Commands Manual for complete descriptions of the commands used in the procedure in this section, including parameter names, valid values, rules for using the command correctly, and output examples..

The duration index is the amount of time that the ACG is in effect. This is a number that is mapped to a time value at the LNP node. See [Table 42: Duration and Gap Interval Index Values](#).

The INinterval index is the amount of time between ACGs for IN queries. This is a number that is mapped to a time value at the LNP node. See [Table 42: Duration and Gap Interval Index Values](#).

The interval index is the amount of time between for queries. This is a number that is mapped to a time value at the node. See [Table 42: Duration and Gap Interval Index Values](#).

Prerequisite for Adding an ACG MIC Control

Before an ACG manual initiated control can be added, the LNP feature must be enabled.

- Enter the `rtrv-ctrl-feat` command.
- If the LNP feature is enabled, the entry `LNP ported TNS` is shown in the `rtrv-ctrl-feat` output with a quantity greater than 0.
- If the LNP feature is not enabled, perform the procedures in the [LNP Feature Configuration](#) to enable the LNP feature. Then continue with the procedure in this section.

If the `type=all` parameter is specified, the `nd`, `intvl`, and `aintvl` parameters must be specified and the `serv` and `dgts` parameters cannot be specified. To specify the `type=all` parameter, no existing ACG manually initiated control specifying all LNP query services can be in the database.

ACG Manually Initiated Control #1

Type of Control = All

Number of Digits = 6

IN Interval Index = 4 - 8 seconds

AIN Interval Index = 7 - 5 seconds

Duration Index = 8 - 128 seconds

ACG Manually Initiated Control #2

Type of Control = SD

Query Service = AIN

AIN Interval Index = 8 - 10 seconds

Digits = 910584

Duration Index = 7 - 64 seconds

ACG Manually Initiated Control #3

Type of Control = SD

Query Service = IN

IN Interval Index = 6 - 16 seconds

Digits = 4237431234

Duration Index = 5 - 16 seconds

1. Display the manually initiated controls in the database using the `rtrv-acg-mic` command.
Verify that the ACG MIC to be added is not already in the database.
2. Add the ACG manually initiated controls to the database using the `ent-acg-mic` command.
3. Verify the changes using the `rtrv-acg-mic` command with either the `type=all` parameter, or the parameters and values specified with the `type=sd` parameter in [Step 2](#).
4. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.  
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.  
BACKUP (FIXED): MASP A - Backup starts on standby MASP.  
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Removing ACG Manual Initiated Controls

This procedure is used to remove an ACG manually initiated control using the `dlt-acg-mic` command.

Refer to the Commands Manual for complete descriptions of the commands used in the procedure in this section, including parameter names, valid values, rules for using the command correctly, and output examples.

1. Display the ACG manually initiated controls in the database using the `rtrv-acg-mic` command.
Verify that the ACG MIC to be removed is in the database.
2. Remove the ACG manually initiated controls from the database using the `dlt-acg-mic` command.
3. Verify the changes using the `rtrv-acg-mic` command with either the `type=all` parameter, or the parameters and values specified with the `type=sd` parameter in [Step 2](#).
4. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.  
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.  
BACKUP (FIXED): MASP A - Backup starts on standby MASP.  
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Changing ACG Manual Initiated Controls

This procedure is used to change an existing ACG manually initiated controls using the `chg-acg-mic` command.

Refer to the Commands Manual for complete descriptions of the commands used in the procedure in this section, including parameter names, valid values, rules for using the command correctly, and output examples.

The duration index is the amount of time that the ACG is in effect. This is a number that is mapped to a time value at the LNP node. See [Table 42: Duration and Gap Interval Index Values](#).

The IN interval index is the amount of time between ACGs for IN queries. This is a number that is mapped to a time value at the LNP node. See [Table 42: Duration and Gap Interval Index Values](#).

The AIN interval index – the amount of time between ACGs for AIN queries. This is a number that is mapped to a time value at the LNP node. See [Table 42: Duration and Gap Interval Index Values](#).

1. Display the ACG manually initiated controls in the database using the `rtrv-acg-mic` command.
Verify that the ACG MIC that is to be changed is in the database.
2. Add the ACG manually initiated controls to the database using the `chg-acg-mic` command.
3. Verify the changes using the `rtrv-acg-mic` command with either the `type=all` parameter, or the `serv` and `dgts` parameters and values specified with the `type=sd` parameter in [Step 2](#).
4. Back up the changes using the `chg-db:action=backup:dest=fixed` command.

The following messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
BACKUP (FIXED): MASP A - Backup starts on active MASP.  
BACKUP (FIXED): MASP A - Backup on active MASP to fixed disk complete.  
BACKUP (FIXED): MASP A - Backup starts on standby MASP.  
BACKUP (FIXED): MASP A - Backup on standby MASP to fixed disk complete.
```

Appendix

A

ELAP Software Configuration

Topics:

- [*Setting Up an ELAP Workstation.....243*](#)
- [*ELAP Configuration and Initialization.....248*](#)
- [*MPS Health Check Procedure.....279*](#)

This appendix describes the text-based user interface that performs ELAP configuration and initialization.

Setting Up an ELAP Workstation

The customer workstation serving as a client PC must meet certain criteria, which are described next.

Screen Resolution

For optimum usability, the workstation must have a minimum resolution of 800x600 pixels and a minimum color depth of 16 thousand colors per pixel.

Compatible Browsers

The ELAP user interface was designed and written to perform with Microsoft Internet Explorer 8.0 or later. The ELAP user interface may not function properly with Mozilla Firefox.

Java

The ELAP GUI uses a Java banner applet to display real-time updates and status for both A and B sides of the MPS.

The Java installation must be performed in the sequence shown:

1. [Install Java Plug-In](#)
2. [Install Java Policy File](#)
3. [Add Security Parameters to an Existing Java Policy File](#) or [Create a New Java Policy File](#)

Install Java Plug-In

Because the Java applet is required for the ELAP GUI to operate, perform the following procedure to install the Java plug-in after you complete the ELAP configuration. Java 1.7 clients are supported. Java 1.6 or earlier clients are not supported.

Note: The selected browser must be the only browser open on your PC when you modify or create the Java policy file or the change will not take effect.

1. Using the selected browser (Internet Explorer 8.0 or later or Mozilla Firefox 3.0.0 or later), enter the IP address for your ELAP A machine. You will see the login screen.
2. Attempt to log in to the ELAP User Interface screen. If using Firefox, you will encounter the following message when logging into the ELAP GUI:

The User Interface may not function correctly with the browser you are using. Microsoft Internet Explorer, version 5 and later, has been certified for this application

When you have successfully entered the Username and Password, the login process checks for the required Java plug-in. When it finds the Java plug-in not present (but you had a previous version of Java installed), the system displays a **Security Warning** window as shown in [Figure 100: Security Warning Window](#).



Figure 100: Security Warning Window

3. Click the **Install** button to begin the process of loading the Java plug-in.
4. Next, the Java installation presents a **License Agreement** screen as shown in [Figure 101: License Agreement](#).

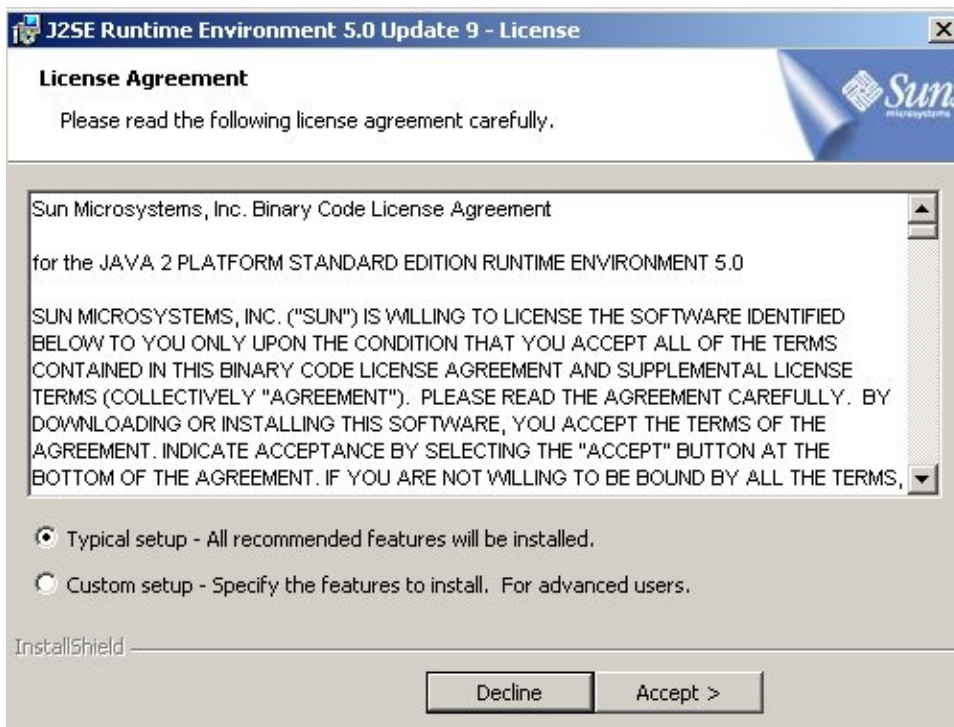


Figure 101: License Agreement

5. Ensure that the **Typical Setup** radio button is selected, and click the **Accept** button to accept the Sun Microsystems agreement.
6. The installation process starts, and a progress window appears as shown in [Figure 102: Java Installation Progress Window](#).

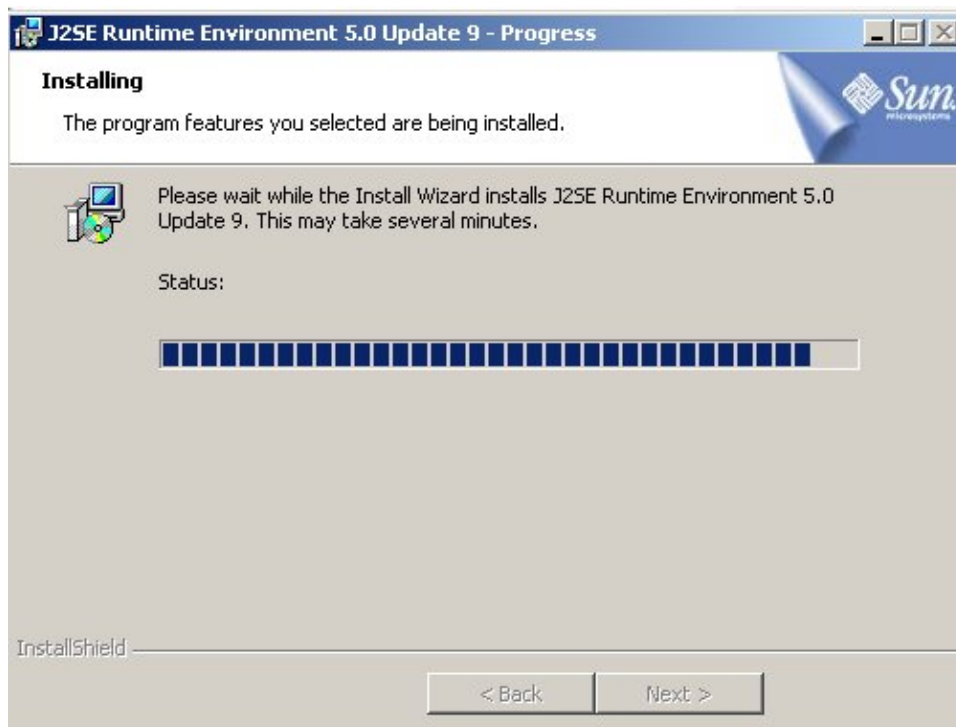


Figure 102: Java Installation Progress Window

7. When the installation is complete, the Installation Complete window appears as shown in [Figure 103: Java Installation Complete Window](#).

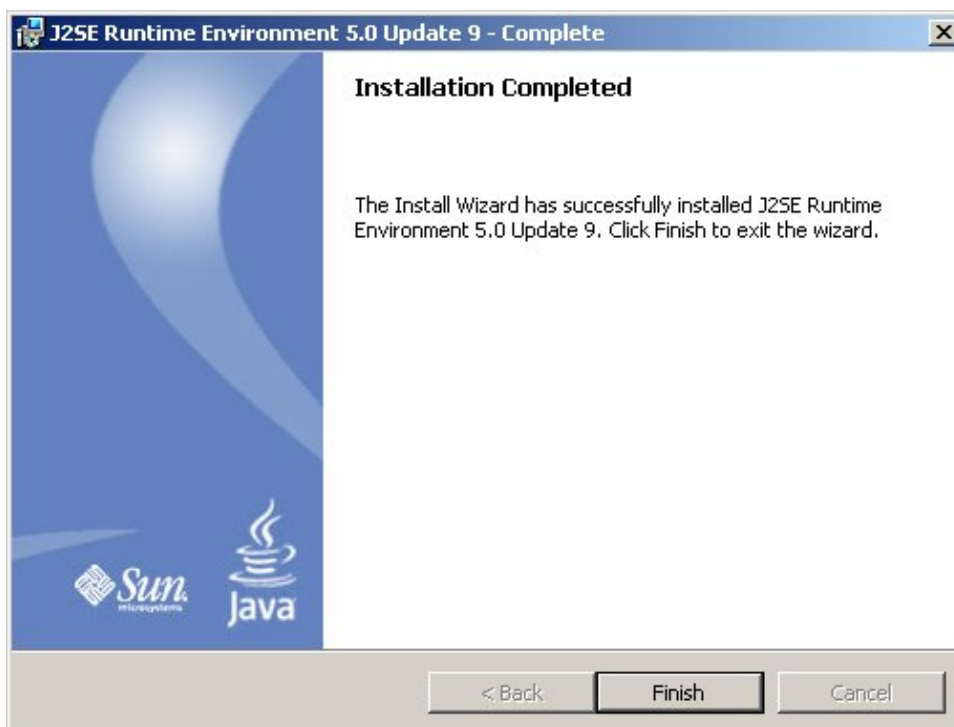


Figure 103: Java Installation Complete Window

8. The installation is complete. Click the **Finish** button. You return to the browser screen containing the ELAP login screen.

Install Java Policy File

The banner applet makes a network connection to each MPS side. A Java policy file must exist for the banner applet to connect properly. If the Java policy file is not present, you will receive a Violation status (VIOL) for the machine.

Note: The selected browser must be the only browser open on your PC when you modify or create the Java policy file, or else the change does not take effect.

Add Security Parameters to an Existing Java Policy File

To check to see if a Java policy file is already in place, perform the following actions:

1. From the Windows **Start** menu, select **Control Panel**.
2. Select the **Java Control Panel**. When the **Java Control Panel** appears, click the **Java** tab as shown in [Figure 104: Java Control Panel, Java Tab](#).

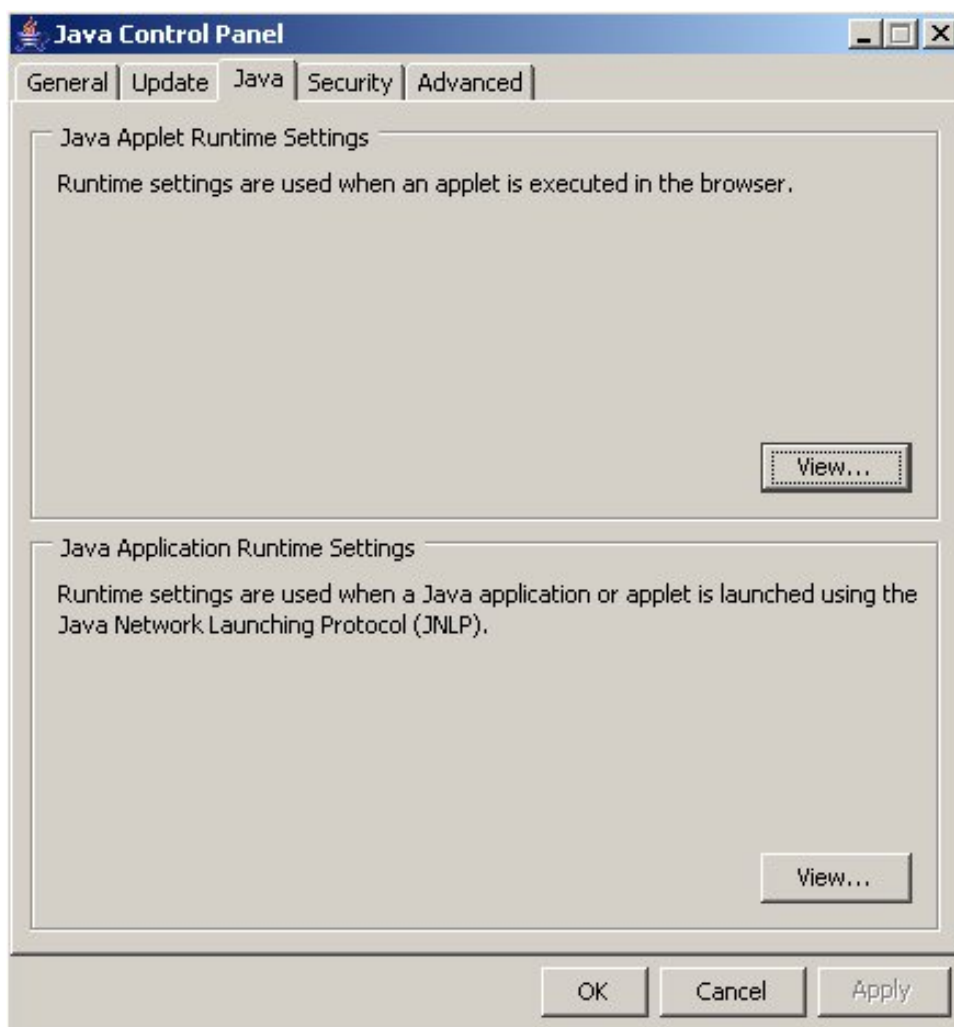


Figure 104: Java Control Panel, Java Tab

3. Click **View** in the **Java Applet Runtime Settings** pane. The Java Runtime Settings dialog box appears as shown in [Figure 105: Java Runtime Settings Dialog Box](#).

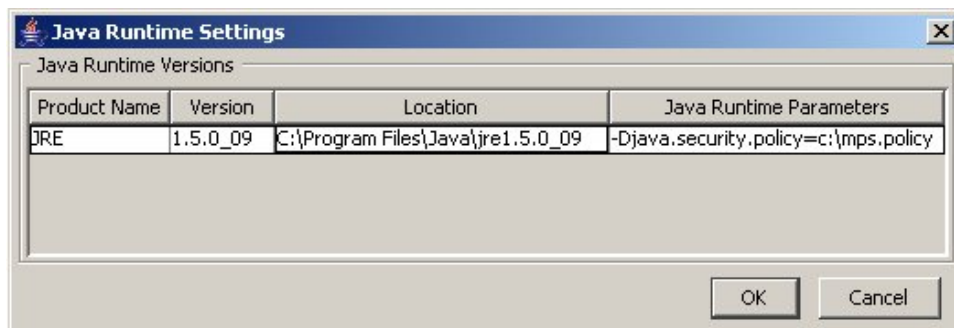


Figure 105: Java Runtime Settings Dialog Box

4. Adjust the width of the columns until you can read the contents of the Java Runtime Parameters column (at the far right).
5. Open the policy file indicated in the Java Runtime Parameters column, and insert the following text.

```
grant {  
  {permission java.net.SocketPermission "*:8473", "connect";  
};
```

Create a New Java Policy File

To create a Java policy file:

1. Insert the following text into a file accessible by the workstation:

```
grant {  
  permission java.net.SocketPermission "*:8473", "connect";  
};
```

2. Follow steps 2 through 4 in the procedure described in [Add Security Parameters to an Existing Java Policy File](#).
3. In the Java Runtime Parameters column of the Java Runtime Settings Dialog Box, type the path to the file you created in step 1 of this procedure. An example is shown below.

```
-Djava.security.policy={full_path_to_file}
```

Note: Java 1.6 clients are supported, and backwards compatibility is maintained for Java 1.5 clients.

Note: If the path name on your system contains spaces, enclose the path name in double quotes (""). An example path is shown below.

```
-Djava.security.policy="C:\Documents and Settings\doe\mps.ploicy"
```

ELAP Configuration and Initialization

Before you can use the ELAP GUI, you must initialize and configure the ELAP software. The ELAP configuration and initialization is performed through the ELAP text-based user interface.

You will connect a local (optional) terminal connected to port 0 of the 8 -port connector box on the MPS frame at each EAGLE 5 ISS. (Refer to the *Installation Manual - EAGLE 5 ISS*.) To begin the initialization, you will log into ELAP A the first time as the “*elapconfig*” user. An automatic configuration is performed on both mated ELAPs.

Note: All network connections and the mate ELAP must be present and verified to allow the initial configuration to complete successfully.

No other user is able to log in to an ELAP until the configuration step is completed for that system.

Errors and Other Messages

The following rules are applicable to configuring the ELAP:

- Mate MPS servers (MPS A and MPS B) must be powered on.
- “Initial Platform Manufacture” for the mate MPS servers must be complete.
- The Sync Network between the mate MPS servers must be operational.
- You must have the correct password for the elapdev user on the mate MPS server.

Required Network Address Information

The following information is needed to configure the MPSs at EAGLE 5 ISS A ([Table 45: Information for MPS at EAGLE 5 ISS A](#)) and EAGLE 5 ISS B ([Table 46: Information for MPS at EAGLE 5 ISS B](#)). Fill in the following tables for reference during the installation procedure.

Table 45: Information for MPS at EAGLE 5 ISS A

Common Information	
MPS A Provisioning Network Address	. . .
MPS B Provisioning Network Address	. . .
Netmask	. . .
Default Router	. . .
Provisioning VIP Address	
Port Forwarding and Static NAT Information (optional)	
MPS A Forwarded HTTP Port	
MPS B Forwarded HTTP Port	
MPS A Forwarded SuExec Port	
MPS B Forwarded SuExec Port	
MPS A Forwarded LSMS Port	7483*
MPS A Forwarded LSMS Port	7483*
MPS A Forwarded Banner Port	
MPS B Forwarded Banner Port	
MPS A Provisioning Static NAT Addr.	. . .
MPS B Provisioning Static NAT Addr.	. . .
* Do not change the default values for these ports	

..

Table 46: Information for MPS at EAGLE 5 ISS B

Common Information	
MPS A Provisioning Network Address	. . .
MPS B Provisioning Network Address	. . .
Netmask	. . .
Default Router	. . .
Port Forwarding and Static NAT Information (optional)	
MPS A Forwarded HTTP Port	
MPS B Forwarded HTTP Port	
MPS A Forwarded SuExec Port	
MPS B Forwarded SuExec Port	
MPS A Forwarded LSMS Port	7483*
MPS A Forwarded LSMS Port	7483*
MPS A Forwarded Banner Port	
MPS B Forwarded Banner Port	
MPS A Provisioning Static NAT Addr.	. . .
MPS B Provisioning Static NAT Addr.	. . .
* Do not change the default values for these ports	

ELAP Firewall Port Assignments

If a firewall is installed in the provisioning network between the MPS systems or between the MPS systems and the provisioning system, the firewall must be configured to allow selected traffic to pass. Firewall protocol filtering for the various interfaces from the perspective of each MPS is defined in [Table 47: Firewall Requirements](#).

Note: The information in [Table 47: Firewall Requirements](#) is used for both internal customer network configuration and VPN access for support.

Table 47: Firewall Requirements

Server Interface	IP Address	TCP/IP Port	Inbound	Outbound	Use/Comments
ELAP Application Firewall Requirements:					
Port 1	Provisioning IP or VIP configured on ELAP	22	Yes	Yes	SSH/SCP/SFTP
Port 1	Provisioning IP or VIP configured on ELAP	80	Yes	No	APACHE - needed for ELAP Web-based GUI
Port 1	NTP server IP(s) configured on ELAP	123	Yes	Yes	NTP - needed for time-sync
Port 1	Provisioning IP or VIP configured on ELAP	443	Yes	No	SSL (HTTPS) - needed for ELAP Web-based GUI
Port 1	Provisioning IP or VIP configured on ELAP	1030	Yes	Yes	used for bulkdownload between LSMS and ELAP
Port 1	Provisioning IP or VIP configured on ELAP	7483	Yes	No	used for download the normal provisioning data from LSMS to ELAP
Port 1	Provisioning IP or VIP configured on ELAP	8473	Yes	Yes	GUI server (process) - needed by ELAP Web-based GUI
Port 1	Provisioning IP or VIP configured on ELAP	9691	Yes	Yes	used for HSOPD watcher

Configuration Menu Conventions

After you have logged into the ELAP user interface with the **elapconfig** user name, the menu that corresponds to that user login name appears. Below are descriptions of the Menu Format, Prompts and Default Values, and Error Message Format.

Menu Format

The configuration menu has a header format that displays specific information. The first line indicates the MPS Side A or B with which you are active. On the same line, you are shown the hostname and hostid. The second and third lines show the Platform Version, followed by the Software Version. The last line displays the date and time. See a sample configuration header format in [Figure 106: Configuration Menu Header Format](#).

```
MPS Side A:  hostname: mps-a  hostid: fd0a4666
              Platform Version: 5.5.0-75.11.0
              Software Version: ELAP 10.0.0_100.13.0
              Wed Apr 10 09:34:14 EDT 2013
```

Figure 106: Configuration Menu Header Format

When you see a menu, choose a an item by entering the number of the item (or *e* for Exit) in response to the Enter Choice prompt that follows the menu, and press Return.

When you choose a menu item, the user interface performs the requested operation. The operation and any associated output for each menu item are described in detail later in this section.

If you enter an invalid choice (such as a letter or a number that is not available for that menu), an error appears. Perform the corrective action described for that error.

Prompts and Default Values

Depending on the menu item that you choose, you might be prompted for data (such as IP addresses) that is required to complete the selected operation. Optional fields are indicated by the text “(optional)” at the end of the prompt. To bypass an optional field without entering a value, press Return.

Default values are enclosed in square brackets at the end of the prompt text: *[default value]*. Example default values are shown in this chapter; they might not be the same as the default values that appear for your system. To accept the default value for a prompt instead of entering a response, press Return.

You can press the Escape key to exit any operation without entering a value for the prompt. The operation is aborted, and you are returned to the menu.

Error Message Format

Invalid menu selections, invalid user input, and failed user interface operations generate error messages on the screen. The error message remains on the screen until you press Return.

All error messages have a unique four-digit error number and associated text. The numbers and text for all error messages generated by the ELAP user interface are listed in [ELAP Error Messages](#). The possible error messages that can occur for each ELAP user interface menu item are listed in the description of the menu item in this chapter.

Error messages have the following format, where *xxxx* is the unique four-digit error number for the error and *Error text* is the corresponding error text:

```
Exxxx
: Error text
Press return to continue
```

You are prompted whenever the software must be stopped to perform an operation:

```
ELAP software is running.  Stop it? [N]: Y
```

However, you must remember that while the ELAP software is stopped, the ELAP cannot process any provisioning updates.

Overview of ELAP Configuration

When you log into an ELAP with user name “elapconfig” after the first initialization of the ELAP, the configuration process begins. (See the details in [Procedure for Configuring ELAPs](#).) The configuration process lets you change IP addresses, time zone, and the password for “elapconfig”. You can display the host ID and exchange secure shell keys. This section describes each of these items in configuration menu.

Initial “elapconfig” User Login

The first time the elapconfig user logs in to the system, the text screen is displayed as shown in [Figure 107: Initial Configuration Text Screen](#).

```
Caution: This is the first login of the text user interface.  Please
          review the following checklist before continuing.  Failure
          to enter complete and accurate information at this time will
          have unpredictable results.

          1. The mate MPS servers (MPS A and MPS B) must be powered on.
          2. "Initial Platform Manufacture" for the mate MPS servers
             must be complete.
          3. The sync network between the mate MPS servers must be
             operational.
          4. You must have the correct password for the ELAPdev user on
             the mate MPS server.

          Press return to continue...
```

Figure 107: Initial Configuration Text Screen

If all four items in the displayed checklist above are not met, the configuration cannot proceed. Ensuring that the MPS servers are powered on requires a visual check. If the “Initial Platform Manufacture” is not complete, the configuration cannot proceed; furthermore, if the sync network is not operational, the user is notified.

When the four items in the checklist are met, press Return and the process resumes. [Figure 108: Initial Configuration Continues](#) shows the continuation of the screen information. The installer enters y if the installation is to continue.

```
Are you sure you wish to continue? [N]: y
```

Figure 108: Initial Configuration Continues

Note: The information required for the following section should be recorded in “[Required Network Address Information](#)”. Make certain all required information is obtained and recorded in the tables provided.

Next, the installer is prompted for the elapdev user password on the mate MPS server. [Figure 109: Entering the elapdev Password](#) shows sample output that is generated after the correct password is entered.

```

Password for ELAPdev@mate:

Keys exchanged.
Verifying that ssh works correctly.
ssh is working correctly.
Building the initial database on slave.
Building the initial database on master.
There was no elap.cfg file. Using default configuration.
Allowing access from slave.
Stopping mysql on master.
Stopping mysql on slave.
Setting up master config file.
Setting up slave config file.
Copying database to slave.
Starting MySQL on master.
Starting MySQL on slave.

```

Figure 109: Entering the elapdev Password

At this point, the first appearance of the Configuration Menu occurs.

Text-based Configuration Menu

After the report as shown in [Figure 109: Entering the elapdev Password](#), the ELAP Configuration Menu is displayed as shown in [Figure 110: ELAP Configuration Menu](#). The elapconfig user can now begin configuring the MPS local and remote servers.

```

MPS Side A:  hostname: mps-a  hostid: 0
              Platform Version: 5.5.0-75.11.0
              Software Version: ELAP 10.0.0_100.13.0
              Wed Apr 10 09:34:14 EDT 2013

```

```

/-----ELAP Configuration Menu-----\
/-----\
| 1 | Display Configuration |
|---|-----|
| 2 | Configure Network Interfaces Menu |
|---|-----|
| 3 | Set Time Zone |
|---|-----|
| 4 | Exchange Secure Shell Keys |
|---|-----|
| 5 | Change Password |
|---|-----|
| 6 | Platform Menu |
|---|-----|
| 7 | Configure NTP Server |
|---|-----|
| 8 | Mate Disaster Recovery |
|---|-----|
| e | Exit |
\-----/

```

```
Enter Choice: 2
```

Figure 110: ELAP Configuration Menu

To choose a menu item, enter the number or letter of the menu item in response to the **Enter Choice** prompt that follows the menu item list, and press Return.

Display Configuration

The Display Configuration menu option 1 displays network address information and the time zone. See an example in [Figure 111: Example of Display Configuration Output](#).

```
MPS Side A:  hostname: mps-a  hostid: 0
              Platform Version: 5.5.0-75.11.0
              Software Version: ELAP 10.0.0_100.13.0
              Wed Apr 10 09:34:14 EDT 2013

ELAP A Provisioning Network IP Address = 10.250.51.130
ELAP B Provisioning Network IP Address = 10.250.51.131
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 10.250.51.1
Provisioning VIP                        = 10.250.51.21
ELAP A Sync Network Address            = 169.254.1.100
ELAP B Sync Network Address            = 169.254.1.200
ELAP A Main DSM Network Address         = 192.168.120.100
ELAP B Main DSM Network Address         = 192.168.120.200
ELAP A Backup DSM Network Address       = 192.168.121.100
ELAP B Backup DSM Network Address       = 192.168.121.200
ELAP A HTTP Port                       = 80
ELAP B HTTP Port                       = 80
ELAP A HTTP SuExec Port                 = 8001
ELAP B HTTP SuExec Port                 = 8001
ELAP A Banner Connection Port           = 8473
ELAP B Banner Connection Port           = 8473
ELAP A Static NAT Address               = Not configured
ELAP B Static NAT Address               = Not configured
ELAP A LSMS Connection Port             = Not configured
ELAP B LSMS Connection Port             = Not configured
ELAP A EBDA Connection Port             = Not configured
ELAP B EBDA Connection Port             = Not configured
Time Zone                              = America/New_York

Press return to continue...
```

Figure 111: Example of Display Configuration Output

Addresses should not conflict with the internal network addresses. The class C networks chosen should not conflict with the class C network used in the network scheme. [Table 48: Sample IP Addresses Used in Configuration](#) shows an example of IP addresses used in the configuration process.

Table 48: Sample IP Addresses Used in Configuration

Provisioning Network Information	MPS A (Local) IP Addresses	MPS B (Local) IP Addresses
ELAP A Provisioning Network IP Address (MPS A)	192.168.61.90	192.168.61.119

Provisioning Network Information	MPS A (Local) IP Addresses	MPS B (Local) IP Addresses
ELAP B Provisioning Network IP Address (MPS B)	192.168.61.91	192.168.61.120
Network Net Mask	255.255.255.0	255.255.255.0
Default Router	192.168.61.250	192.168.61.250
Provisioning VIP Address	192.168.61.166	192.168.61.166

Configure Provisioning Network

The Configure Network Interfaces Menu option 2 of the Configuration Menu displays the submenu shown in [Figure 112: Configure Network Interfaces Menu](#). It supports the configuration of all the network interfaces for the ELAP

```

/-----Configure Network Interfaces Menu-\  

|-----|  

| 1 | Configure Provisioning Network |  

|-----|  

| 2 | Configure DSM Network |  

|-----|  

| 3 | Configure Forwarded Ports |  

|-----|  

| 4 | Configure Static NAT Addresses |  

|-----|  

| e | Exit |  

|-----|  

\-----/

```

Enter Choice:

Figure 112: Configure Network Interfaces Menu

Configure Provisioning Network

The Configure Provisioning Network option 1 of the Configure Network Interfaces Menu configures the ELAP provisioning network. These include the provisioning network's IP address, netmask, and IP address. This information allows the ELAP to communicate with an existing customer network.

In response to each prompt, you can enter a dotted decimal IP address or press Return to leave the current value unchanged (the current value is shown in brackets after the prompt text). See [Figure 113: Configure Provisioning Network Output](#) for the option 1 output.

```

Verifying connectivity with mate...
ELAP A provisioning network IP Address [192.168.61.104]: 192.168.61.208
ELAP B provisioning network IP Address [192.168.61.105]: 192.168.61.209
ELAP provisioning network netmask [255.255.255.0]:
ELAP provisioning network default router [192.168.61.250]:
ELAP local provisioning Virtual IP Address [192.168.61.100]: 192.168.61.215

Please Wait, this may take a while...

```

Figure 113: Configure Provisioning Network Output

Configure DSM Network

The Configure DSM Network option 2 of the Configure Network Interfaces Menu prompts you for the ELAP DSM network IP addresses. This information allows the ELAP to communicate with the main and backup DSM networks.

In response to each prompt, you can enter a dotted decimal IP address or press Return to leave the current value unchanged (the current value is shown in brackets after the prompt text).

See [Figure 114: Configure DSM Network](#) for the option 2 output.

```
First 3 octets for the ELAP main DSM network [192.168.120]:  
First 3 octets for the ELAP backup DSM network [192.168.121]:  
First 3 octets for the ELAP loopback DSM network [192.168.123]:
```

Figure 114: Configure DSM Network

Configure Forwarded Ports

The Configure Forwarded Ports option 3 of the Configure Network Interfaces Menu provides the functionality to configure ELAP ports for the Web UI.

Each numbered item of the Configure Forwarded Ports menu allows the user to specify a port number used for remote access to the MPS.

This information should be received from the customer for the MPS and recorded in [Table 46: Information for MPS at EAGLE 5 ISS B](#) and [Table 45: Information for MPS at EAGLE 5 ISS A](#).

Configure Static NAT Addresses

The Configure Static NAT Addresses option 4 from the Configure Network Interfaces Menu provides the functionality to configure the static NAT addresses of the ELAP.

Each numbered item of the Configure Static NAT Addresses menu allows the user to specify an IP Address used outside of the firewall for remote access to the MPS. [Figure 115: Configuring NAT Addresses Prompt](#) shows an example of a resulting prompt.

```
ELAP A Static NAT Address:
```

Figure 115: Configuring NAT Addresses Prompt

Select Time Zone

Note: Do not perform the Select the Time Zone function on a running system. Contact [My Oracle Support \(MOS\)](#) for assistance.

The Select Time Zone option 3 prompts you for the time zone to be used by the ELAP. The time zone can be the zone where the ELAP is located, Greenwich Mean Time, or another zone that is selected by the customer to meet the needs of the system.

Note: The value for the time zone should be obtained from the customer's Information Services department. The default value for the time zone is *US/Eastern*.

To select a file in one of the subdirectories, enter a relative path name, such as *US/Eastern*, in response to the prompt. See [Figure 116: Select Time Zone Menu](#) for the option 3 output.

```
Press return to continue...
Verifying connectivity with mate...
Are you sure you wish to change the timezone for MPS A and B? [N]: y
Enter a time zone:
```

Figure 116: Select Time Zone Menu

You must enter a valid UNIX time zone file name. Alternatively, to display a complete list of the valid time zones, simply press Return in response to the prompt, and all valid time zone names are displayed. See [Time Zone File Names](#) for the list that appears when you press the Return key or enter an invalid time zone file name.

The time zone change does not take effect until the next time the MPS is rebooted. The **Reboot MPS** screen is described in [Reboot the MPS](#).

Exchange Secure Shell Keys

The Exchange Secure Shell Keys option 4 from the ELAP Configuration Menu, enables connections between local and remote ELAPs. The ELAPs exchange encryption keys, which are required to run the secure shell.

The exchange normally occurs automatically during ELAP initialization. Use this menu item only if the exchange must be performed manually.

The elapconfig user must know the password for the ELAPdev@mate.

See [Figure 117: Exchange Secure Shell Keys Output](#) for the option 4 output.

```
Are you sure you wish to exchange keys? [N]: y
```

Figure 117: Exchange Secure Shell Keys Output

Change Password

The Change Password option 5 from the ELAP Configuration Menu changes the text-based user interface password for the elapconfig login name for both MPS A and MPS B.

See [Figure 118: Change Password](#) for the option 5 output.

```
Verifying connectivity with mate...
Are you sure you wish to change the text UI password on MPS A and B? [N]: y
Enter new password for text UI user:
Re-enter new password:

Press return to continue...
```

Figure 118: Change Password

Platform Menu and Options

The ELAP Platform Menu option 6, from the ELAP Configuration Menu, accesses the Platform menu so that the `elapconfig` user can access and manage platform functions. See [Figure 119: Platform Menu Output](#) for the option 6 output.

```

MPS Side A:  hostname: mps-a  hostid: 0
              Platform Version: 5.5.0-75.11.0
              Software Version: ELAP 10.0.0_100.13.0
              Wed Apr 10 09:34:14 EDT 2013

/-----ELAP Platform Menu-----\
/-----\
| 1 | Initiate Upgrade |
|---|
| 2 | Reboot MPS      |
|---|
| 3 | MySQL Backup    |
|---|
| 4 | RTDB Backup     |
|---|
| e | Exit            |
\-----/

Enter Choice: 2

```

Figure 119: Platform Menu Output

Initiate Upgrade

The Initiate Upgrade menu option **1** initiates an upgrade on the selected ELAP. For upgrade procedures, contact [My Oracle Support \(MOS\)](#).

Reboot MPS

The Reboot MPS menu option **2** initiates a reboot of either MPS or both. The default is BOTH.

Note: The `elapconfig` user can abort rebooting the MPS by pressing the **Escape** key at the displayed prompt.

```
Reboot MPS A, MPS B or [BOTH]:
```



CAUTION

Caution: Rebooting the MPS stops all ELAP processes. Databases cannot be updated until MPS is fully booted.

MySQL Backup

The MySQL Backup menu option **3** backs up the MySQL database.

Note: ELAP software must be stopped or MySQL backup will abort and return to the **ELAP Platform Menu**.

```
Are you sure you want to back up the MySQL database on MPS A? [N]: y
```

```
Connecting to local MySQL server...
Getting read lock...
Tarring the NPDB...
Disconnecting from local MySQL server...
```

RTDB Backup

The RTDB Backup menu option **4** backs up the RTDB.

Note: ELAP software must be stopped or RTDB backup will abort and return to the **ELAP Platform Menu**.

```
Are you sure you want to back up the RTDB database on MPS A to
"/var/TKLC/appl/free/rtdbBackup_mps-a_20050926110224.tar"? [N]: y
```

ELAP Platform Menu Exit

The Exit menu option **e** exits from the ELAP Platform Menu and returns to the ELAP Configuration Menu.

Configure NTP Server and Options

The Configure NTP Server option **7** allows for the display, addition, and removal of an external NTP server.

Display External NTP Server

The Display External NTP Server menu option **1** displays External NTP Server information. If a server is present, the server name and IP address are displayed. If an NTP Server is not present, the following message is displayed.

```
There are no External NTP Servers. Press return to continue...
```

Add External NTP Server

The Add External NTP Server menu option **2** adds an External NTP Server.

Note: The IP address must be a valid address for an External NTP Server.

Remove External NTP Server

The Remove External NTP Server menu option **3** removes an External NTP Server. If a server is present, selecting the Remove External NTP Server removes the server. If an NTP Server is not present, the following message appears:

```
There are no External NTP Servers. Press return to continue...
```

ELAP Configure NTP Server Menu Exit

The ELAP Configure NTP Server Menu Exit menu option **e** exits the ELAP Configure NTP Server Menu, and returns to the ELAP Configuration Menu.

Exit

The Exit menu option `e` exits the ELAP Configuration menu.

ELAP Configuration Procedure

Initialization and configuration are provided through a text-based user interface (UI) described in this chapter.

The first time user `elapconfig` logs into MPS A, the system performs an auto-configuration on both MPS ELAP pairs. The sync network and main and backup DSM networks are initialized to their default values, described in [Network Connections](#) and defined in the *Installation Manual - EAGLE 5 ISS*. Various internal configuration parameters are also set to their default values. The installer must perform initial configuration on MPS A on EAGLE 5 ISS A and MPS A on EAGLE 5 ISS B.

Configuration Terms and Assumptions

- The initial configuration steps assume that each MPS has previously undergone successful Initial Product Manufacture (IPM).
- The network paths must be present and verified before the MPS servers are ready for configuration.
- Initial configuration can be implemented on only the MPS A side of EAGLE A and MPS A side of EAGLE B. Attempting to perform initial configuration on MPS B of EAGLE A is not allowed, and the `elapconfig` user will be notified. The attempted configuration will be aborted with no impact on either MPS A or B.

After the initial configuration of MPS A on EAGLE A and MPS A on EAGLE B, both ELAPs should be operational unless the system failed to successfully initialize during reboot or the configured values for the Sync and/or DSM networks conflict with other equipment in the network. Changing the default network values is not recommended.

- The provisioning values displayed for the following initialization and configuration steps are example values only.
- Default values can be accepted just by pressing the **Return** key at the prompt; default values are shown enclosed in brackets [].
- The customer is responsible for determining the timing and frequency of performing database backups. Databases should be backed up when they are initially populated with data; however, the priority that the customer assigns to data and time lost in restoring the data dictates the frequency of database backups.
- Adding an NTP server is optional. Additionally, only one NTP server is needed to provide time synchronization for all the MPS servers on both EAGLE pairs.
- The ELAP terms *local* and *remote* are relative with respect to the ELAP configuration software. In other words, if the user is running the configuration software on the physical MPS (that is, the MPS that the user is physically on-site and has a terminal connected to), the configuration software refers to that MPS as *local*. However if the user connects through the network into the MPS A on EAGLE B, the configuration software executing at EAGLE B sees itself as *local*, and identifies the MPS to which the user is physically connected as the *remote*.

The *local* MPS is whichever MPS A that the configuration software is being executed on, regardless of where the user is physically located.



The MPS of EAGLE A is the first MPS to which the user physically connects and on which initial configuration of the ELAPs is always begun.

To avoid confusion of these relative terms, the MPS A on EAGLE A is considered to be the on-site MPS to which the user has the physical connection. This document refers to the MPS to which the user does not have the physical connection as MPS A on EAGLE B.

Configuration Symbols

During the Configuration Procedure, the installer will initialize and configure the MPSs to perform various functions. Special instructions are required occasionally for an MPS on EAGLE 5 ISS A, an MPS on EAGLE 5 ISS B. To assist the installer, this manual uses these symbols to indicate individual instructions to be performed for those specific MPSs.

Table 49: MPS Configuration Symbols

MPS Symbol	Symbol Description
	This symbol indicates installation instructions to be performed specifically for the MPSs (MPS A and MPS B) on EAGLE 5 ISS A.
	This symbol indicates installation instructions to be performed specifically for the MPSs (MPS A and MPS B) on EAGLE 5 ISS B.

Initial Setup and Connecting to MPSs

Installation personnel may choose to employ various methods for connecting to an MPS. The ELAP software requires that an MPS be configured from side A. This procedure describes a likely method for connecting to EAGLE 5 ISS A and then EAGLE 5 ISS B. Installers require that all console output be captured.

Connecting to EAGLE 5 ISS A

To prepare for the configuration of the MPS on EAGLE 5 ISS A, the installer connects directly to the MPS at EAGLE 5 ISS A. Use the following method to connect to MPS B of EAGLE 5 ISS A.

1. Use a PPP utility to connect the modem located in the OOBM card in server A.
For information about setting up a PPP utility, refer to "Network Connections" the .
2. When the prompt appears, enter the following command to start a secure shell session with an ELAP server:

```
ssh elapconfig@<server_IP_address>
```

where **<server_IP_address>** is the IP address of the MPS B at EAGLE 5 ISS A.

3. This will access the ELAP text interface.

The **elapconfig** username and a password provided by your system administrator are required to continue.

Connecting to EAGLE 5 ISS B

To prepare for the configuration of the MPS on EAGLE 5 ISS B, the installer must first complete the connection to and configuration of the MPS on EAGLE 5 ISS A. The installer is then able to use a secure shell session to MPS at EAGLE 5 ISS B to configure it.

The installer can now use a secure shell session from the system prompt to the MPS A on EAGLE 5 ISS B, using the IP address shown in [Table 46: Information for MPS at EAGLE 5 ISS B](#).

```
ssh 192.168.61.119 Trying 192.168.61.119... Connected to 192.168.61.119. Escape
character is '^]'. SunOS 5.7
```

Procedure for Configuring ELAPs

Perform the configuration procedure by following these steps in the text-based user interface. After you have connected to an MPS (as described in [Initial Setup and Connecting to MPSs](#)), you can perform this procedure to configure the ELAPs in your network.

Note: Initial configuration cannot be performed through the GUI. The IP addresses required for browser connectivity are not defined until the initial configuration, using the text-based UI, is completed.

Using the set up and connection described previously, the installer connects to an MPS to perform configuration. In a typical installation, the installer connects directly to the MPS at EAGLE 5 A to configure it, then uses ssh to connect to the MPS at EAGLE 5 B and configure it.

1. Upon connecting to the MPS on EAGLE 5 A, login to the ELAP.

- a) Log in as elapconfig.

A caution appears.

```
mposa-f0c7c3 console login: elapconfig
Password:
Caution: This is the first login of the text user interface. Please
          review the following checklist before continuing. Failure
          to enter complete and accurate information at this time will
          have unpredictable results.

          1. The mate MPS servers (MPS A and MPS B) must be powered on.
          2. "Initial Platform Manufacture" for the mate MPS servers
             must be complete.
          3. The sync network between the mate MPS servers must be
             operational.
          4. You must have the correct password for the ELAPdev user on
             the mate MPS server.

Press return to continue...
```

- b) Evaluate the conditions of the Caution notice. When the conditions are satisfied, press Return to continue.

Upon pressing **Return** to continue, you can end or continue with the initial configuration.

```
Are you sure you wish to continue? [N]: y
```

Note: Pressing Return accepts the default value **n**. To continue with the configuration, enter **y**.

c) Press **y**.

Upon pressing **y**, the configuration software executes on the MPSs on EAGLE 5 B. While the MPSs on EAGLE 5 B were formerly referred to as 'remote', remember that the configuration software now considers the same MPS pair now to be 'local' (for more information, see [Configuration Terms and Assumptions](#)).

d) Enter the **elapdev** user password on the mate MPS server to confirm the secure shell keys are successfully exchanged.

The example shows the output generated when the correct password is entered, the secure shell keys are successfully exchanged, and the UI database is set up on MPS A and MPS B at this site.

```
Password for ELAPdev@mate:
Keys exchanged.
Verifying that ssh works correctly.
ssh is working correctly.
Building the initial database on slave.
Building the initial database on master.
There was no elap.cfg file. Using default configuration.
Allowing access from slave.
Stopping mysql on master.
Stopping mysql on slave.
Setting up master config file.
Setting up slave config file.
Copying database to slave.
Starting MySQL on master.
Starting MySQL on slave.
```

A successful configuration file setup results in the initial display of the **ELAP Configuration Menu** and its associated header information.

The server designation of MPS A at this site is displayed as well as hostname, hostid, Platform Version, Software Version, and the date.

```
MPS Side A:  hostname: mps-a  hostid: 0
              Platform Version: 5.5.0-75.11.0
              Software Version: ELAP 10.0.0_100.13.0
              Wed Apr 10 09:34:14 EDT 2013
```

```
/-----ELAP Configuration Menu-----\
/-----\
| 1 | Display Configuration |
|---|-----|
| 2 | Configure Network Interfaces Menu |
|---|-----|
| 3 | Set Time Zone |
|---|-----|
| 4 | Exchange Secure Shell Keys |
|---|-----|
| 5 | Change Password |
|---|-----|
| 6 | Platform Menu |
|---|-----|
```

```

 7 | Configure NTP Server
---|-----
 8 | Mate Disaster Recovery
---|-----
 e | Exit
\-----/

```

Enter Choice: 1

2. Choose option 1, Display Configuration, to view ELAP A and ELAP B Provisioning Network IP addresses, the Time Zone, and other values for the MPS on EAGLE 5 A.

```

MPS Side A:  hostname: mps-a  hostid: 0
               Platform Version: 5.5.0-75.11.0
               Software Version: ELAP 10.0.0_100.13.0
               Wed Apr 10 09:34:14 EDT 2013
ELAP A Provisioning Network IP Address = 192.168.61.136
ELAP B Provisioning Network IP Address = 192.168.61.137
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 192.168.61.250
Provisioning VIP                       = 192.168.61.166
ELAP A Sync Network Address            = 169.254.1.100
ELAP B Sync Network Address            = 169.254.1.200
ELAP A Main DSM Network Address        = 192.168.120.100
ELAP B Main DSM Network Address        = 192.168.120.200
ELAP A Backup DSM Network Address      = 192.168.121.100
ELAP B Backup DSM Network Address      = 192.168.121.200
ELAP A HTTP Port                      = 80
ELAP B HTTP Port                      = 80
ELAP A HTTP SuExec Port                = 8001
ELAP B HTTP SuExec Port                = 8001
ELAP A Banner Connection Port          = 8473
ELAP B Banner Connection Port          = 8473
ELAP A Static NAT Address              = Not configured
ELAP B Static NAT Address              = Not configured
ELAP A LSMS Connection Port            = Not configured
ELAP B LSMS Connection Port            = Not configured
Time Zone                             = America/New_York

Press return to continue...

```

3. Press Return to return to the ELAP Configuration Menu.
4. Choose option 2, Configure Network Interfaces Menu, from the ELAP Configuration Menu.

```

/-----ELAP Configuration Menu-----\
/-----\
 1 | Display Configuration
---|-----
 2 | Configure Network Interfaces Menu
---|-----
 3 | Set Time Zone
---|-----
 4 | Exchange Secure Shell Keys
---|-----
 5 | Change Password
---|-----

```

6	Platform Menu
7	Configure NTP Server
8	Mate Disaster Recovery
e	Exit

Enter Choice: 2

5. Choose option 1, Configure Provisioning Network form the Configure Network Interfaces Menu.

The **Configure Provisioning Network Menu** allows you to accept the default IP address values presented by the configuration software for ELAP A and ELAP B provisioning network and network netmask, or to enter specific IP values previously received from the customer for the MPS.

/-----Configure Network Interfaces Menu-----\	
1	Configure Provisioning Network
2	Configure DSM Network
3	Configure Forwarded Ports
4	Configure Static NAT Addresses
e	Exit

Enter Choice: 1

See the information recorded in [Table 45: Information for MPS at EAGLE 5 ISS A](#) and [Table 46: Information for MPS at EAGLE 5 ISS B](#) for the correct addresses.

Note: No default value is provided for the ELAP provisioning network default router. This value must be received from the customer.

Information for the submenu for configuring communications networks is displayed.

```
Verifying connectivity with mate...
Enter the ELAP A provisioning network IP Address [192.168.61.90]:
Enter the ELAP B provisioning network IP Address [192.168.61.91]:
Enter the ELAP provisioning network netmask [255.255.255.0]:
Enter the ELAP provisioning network default router IP Address: 192.168.54.250
ELAP local provisioning Virtual IP Address [192.168.61.100]:
Please Wait, this may take a while...
```

6. Press Return to return to the **Configure Network Interfaces Menu**.
 - If there is a known network address conflict, continue with [Step 7](#).
 - If there is not a known network address conflict, go to [Step 9](#)

7. Choose option 2, Configure DSM Network, from the **Configure Network Interfaces Menu**.

```

/-----Configure Network Interfaces Menu-----\
| 1 | Configure Provisioning Network |
| 2 | Configure DSM Network         |
| 3 | Configure Forwarded Ports     |
| 4 | Configure Static NAT Addresses|
| e | Exit                           |
\-----\

Enter Choice: 2

```

The Configure DSM Network choice automatically adds the DSM network IP address to the list of known hosts.

8. Accept default IP address octets for the ELAP main DSM network and the ELAP backup DSM network presented by the configuration software unless a known network conflict exists.

```

First 3 octets for the ELAP main DSM network [192.168.120]:
First 3 octets for the ELAP backup DSM network [192.168.121]:
First 3 octets for the ELAP loopback DSM network [192.168.123]:

```

Upon accepting the default value or entering a specific ELAP backup DSM network octet IP address value, you are returned to the **Configure Network Interfaces Menu**.

- If the MPS is separated from GUI workstations and provisioning systems by a port forwarding firewall, continue with [Step 9](#).
- If the MPS is separated from GUI workstations and provisioning systems by a port forwarding firewall, go to [Step 10](#).

9. Choose option 3, Configure Forwarded Ports, from the **Configure Network Interfaces Menu**.

```

/-----Configure Forwarded Ports Menu-----\
| 1 | Change ELAP A HTTP Port       |
| 2 | Change ELAP B HTTP Port       |
| 3 | Change ELAP A HTTP SuExec Port|
| 4 | Change ELAP B HTTP SuExec Port|
| 5 | Change ELAP A Banner Connection Port|
| 6 | Change ELAP B Banner Connection Port|
| 7 | Change ELAP A LSMS Connection Port|
| 8 | Change ELAP B LSMS Connection Port|
| e | Exit                           |
\-----\

Enter choice: 1

```

- a) Enter the correct option number for the port information to be entered.

See the information recorded in [Table 45: Information for MPS at EAGLE 5 ISS A](#) and [Table 46: Information for MPS at EAGLE 5 ISS B](#) for the correct information.

Note: The LSMS is not capable of changing the LSMSports it can connect to on the MPS. Therefore, the default values for options 7 through 8 on the Configure Forwarded Ports Menu should not be changed.

```
ELAP A HTTP Port [80]:
```

- b) Enter the appropriate information and press return once to return to the **Configure Forwarded Ports Menu**.
- c) Enter the option number or enter **e** to return to the **Configure Network Interfaces Menu**.

10. Choose option 4, Configure Static NAT Addresses from the **Configure Network Interfaces Menu**.

```

/-----Configure Network Interfaces Menu--\
|-----|
| 1 | Configure Provisioning Network |
|-----|
| 2 | Configure DSM Network |
|-----|
| 3 | Configure Forwarded Ports |
|-----|
| 4 | Configure Static NAT Addresses |
|-----|
| e | Exit |
|-----|
\-----/

Enter Choice: 4

```

11. Enter Configure Static NAT Addresses Menu option 1 or 2.

Each numbered item of the **Configure Static NAT Addresses Menu** allows you to specify an IP Address used outside of the firewall for remote access to the MPS.

```

/-----Configure Static NAT Addresses Menu--\
|-----|
| 1 | Change ELAP A Static NAT Address |
|-----|
| 2 | Change ELAP B Static NAT Address |
|-----|
| e | Exit |
|-----|
\-----/

```

- a) Enter a valid NAT IP address from [Table 45: Information for MPS at EAGLE 5 ISS A](#) and [Table 46: Information for MPS at EAGLE 5 ISS B](#).

```
ELAP A Static NAT Address:
```

- b) Choose option **e** on the **Configure Static NAT Addresses Menu** to return to the **Configure Network Interfaces Menu**.
- c) Choose option **e** (Exit), from the **Configure Network Interfaces Menu**, to return to the **ELAP Configuration Menu**.

- If the time zone is not correct for this installation, as shown in the output of the Display Configuration [Step 2](#), continue with [Step 12](#).
- If the time zone is correct for this installation, as shown in the output of the Display Configuration [Step 2](#), go to [Step 14](#).

12. Choose option 3, Set Time Zone, on the ELAP Configuration Menu.

Note: Obtain the value for the time zone from the customer's Information Services department. The default value for the time zone is **US/Eastern**.

```

/-----ELAP Configuration Menu-----\
/-----\
| 1 | Display Configuration |
|---|-----|
| 2 | Configure Network Interfaces Menu |
|---|-----|
| 3 | Set Time Zone |
|---|-----|
| 4 | Exchange Secure Shell Keys |
|---|-----|
| 5 | Change Password |
|---|-----|
| 6 | Platform Menu |
|---|-----|
| 7 | Configure NTP Server |
|---|-----|
| 8 | Mate Disaster Recovery |
|---|-----|
| e | Exit |
\-----/

```

Enter Choice: 3

An important Caution statement is displayed.

```

Caution: This action requires a reboot of the affected MPS servers to
          activate the change. Operation of the ELAP software before
          the MPS servers are rebooted may have unpredictable
          consequences.
Press return to continue...

```

- Press **Return** to continue.
You are prompted for confirmation on setting the time zone for MPS A and MPS B at his site.
- Enter **y** to confirm the change.
Pressing **Return** accepts the default of **n** (no) and the action is aborted.

```

Are you sure you wish to change the timezone for MPS A and B? [N]: y

```

When the affirmative response **y** is given to change the time zone, the following prompt is displayed. The time zone can be the zone where the ELAP is located, Greenwich Mean Time, or another zone that is selected by the customer to meet the needs of the system.

If the time zone is known, it can be entered at the prompt.

If the exact time zone value is not known, press **Return**, and a list of the valid names is displayed. The installer can select a value from the list. The list is also displayed if an invalid time zone is entered and **Return** is pressed. This list of valid time zones is also in [Time Zone File Names](#).

```
Enter a time zone file (relative to /usr/share/lib/zoneinfo):
```

The time zone change does not take effect until the next time the MPS is rebooted.

After setting the time zone successfully, you are returned to the **ELAP Configuration Menu**.

- If you want to exchange secure shell keys, continue with [Step 13](#).

Note: Although the exchange of ELAP Secure Shell (SSH) Keys is performed automatically by the configuration software at the start of the ELAP configuration ([Substep d](#)), exchange of SSH keys with the LSMS ([Step 17](#)) must be performed manually in order for the ELAP to receive bulk downloads from the LSMS.

- If you do not want to exchange SSH keys, go to [Step 18](#).

13. Enter option 4, Exchange Secure Shell Keys, from the ELAP Configuration Menu.

```
/-----ELAP Configuration Menu-----\
/-----\
| 1 | Display Configuration |
|---|-----|
| 2 | Configure Network Interfaces Menu |
|---|-----|
| 3 | Set Time Zone |
|---|-----|
| 4 | Exchange Secure Shell Keys |
|---|-----|
| 5 | Change Password |
|---|-----|
| 6 | Platform Menu |
|---|-----|
| 7 | Configure NTP Server |
|---|-----|
| 8 | Mate Disaster Recovery |
|---|-----|
| e | Exit |
\-----/
```

```
Enter Choice: 4
```

The **Exchange Secure Shell Keys Menu** is displayed.

14. Enter 1, Exchange Keys with Mate.

```
Verifying connectivity with mate...

MPS Side A:  hostname: mps-a  hostid: 0
              Platform Version: 5.5.0-75.11.0
              Software Version: ELAP 10.0.0_100.13.0
              Wed Apr 10 09:34:14 EDT 2013

/-----Exchange Secure Shell Keys Menu-----\
/-----\
```

```

| 1 | Exchange Keys with Mate |
|---|-----|
| 2 | Exchange Keys with Remote |
|---|-----|
| 3 | Exchange Keys with Mate as Root User |
|---|-----|
| 4 | Exchange Keys with LSMS |
|---|-----|
| e | Exit |
|---|-----|
\-----/

```

Enter Choice: 1

Upon entering **1**, you are asked to confirm the SSH key exchange.

```
Are you sure you wish to exchange keys? [N]: Y
```

- a) Enter **Y** to continue.
You are prompted for the elapdev password.
- b) Enter the elapdev password to continue.

A message provides notification that SSH is working. You are returned to the **Exchange Secure Shell Keys Menu**.

15. Enter **2**, Exchange Keys with a Remote ELAP.

```
ssh is working correctly.
```

```
MPS Side A:  hostname: mps-a  hostid: 0
              Platform Version: 5.5.0-75.11.0
              Software Version: ELAP 10.0.0_100.13.0
              Wed Apr 10 09:34:14 EDT 2013
```

```

/-----Exchange Secure Shell Keys Menu-----\
/-----|
| 1 | Exchange Keys with Mate |
|---|-----|
| 2 | Exchange Keys with Remote |
|---|-----|
| 3 | Exchange Keys with Mate as Root User |
|---|-----|
| 4 | Exchange Keys with LSMS |
|---|-----|
| e | Exit |
|---|-----|
\-----/

```

Enter Choice: 2

You are prompted to confirm the exchange.

```
Are you sure you wish to exchange keys with remote? [N]:
```

- a) Enter **Y** to continue.

You are prompted for the IP address.

```
Remote IP Address:
```

b) Enter the IP address of the remote ELAP.

You are prompted for the elapdev password.

```
The server does not know of 192.168.66.98.
Will just exchange host keys for the name given!
Password of elapdev:
```

c) Enter the elapdev password.

A message provides notification that host keys were exchanged and SSH is working. You are returned to the **Exchange Secure Shell Keys Menu**.

16. Enter 3, Exchange Keys with a mate ELAP as a root user.

```
The server does not know of 192.168.66.98.
Will just exchange host keys for the name given!
ssh is working correctly.
```

```
MPS Side A:  hostname: mps-a  hostid: 0
               Platform Version: 5.5.0-75.11.0
               Software Version: ELAP 10.0.0_100.13.0
               Wed Apr 10 09:34:14 EDT 2013
```

```
/-----Exchange Secure Shell Keys Menu-----\
/-----\
| 1 | Exchange Keys with Mate |
|---|-----|
| 2 | Exchange Keys with Remote |
|---|-----|
| 3 | Exchange Keys with Mate as Root User |
|---|-----|
| 4 | Exchange Keys with LSMS |
|---|-----|
| e | Exit |
\-----/
```

```
Enter Choice: 3
```

You are prompted to confirm the exchange.

```
Are you sure you wish to exchange keys as root? [N]:
```

a) Enter **Y** to continue.

You are prompted to enter the root password.

```
Password of root:
```

b) Enter the root password.

A message provides notification that host keys were exchanged and SSH is working. You are returned to the **Exchange Secure Shell Keys Menu**.

17. Enter 4, Exchange Keys with LSMS.

Note: This procedure exchanges SSH keys between the two ELAP servers and ONE OF THE LSMS SERVERS. Consequently, **THIS PROCEDURE MUST BE PERFORMED FOR THE LSMS SERVER A (lsmspri) and REPEATED FOR THE LSMS SERVER B (lsmssec)**. Failure to perform this procedure for both LSMS servers can result in failure of the ELAP servers to receive SERVDI bulkloads from the LSMS servers.

Note: You will need the IP addresses for both LSMS server host names (lsmspri and lsmssec) as well as the lsmsadm password to complete this procedure.

```
ssh is working correctly.

MPS Side A:  hostname: mps-a  hostid: 0
              Platform Version: 5.5.0-75.11.0
              Software Version: ELAP 10.0.0_100.13.0
              Wed Apr 10 09:34:14 EDT 2013

/-----Exchange Secure Shell Keys Menu-----\
/-----\
| 1 | Exchange Keys with Mate |
|---|-----\
| 2 | Exchange Keys with Remote |
|---|-----\
| 3 | Exchange Keys with Mate as Root User |
|---|-----\
| 4 | Exchange Keys with LSMS |
|---|-----\
| e | Exit |
\-----/

Enter Choice: 4
```

You are prompted to confirm the exchange.

```
Are you sure you wish to exchange keys with LSMS? [N]:
```

- a) Enter **Y** to continue.
You are prompted to enter the LSMS IP address.

```
LSMS IP Address:
```

- b) Enter the IP address for the desired LSMS server.
You are prompted to enter the lsmsadm password.

```
The server does not know of 192.168.60.4.
Will just exchange host keys for the name given!
Password of lsmsadm:
```

- c) Enter the lsmsadm password.

A message provides notification that keys were exchanged (between ELAP A and the selected LSMS server) and SSH is working.

You are prompted to enter the lsmsadm password again for exchange of keys between ELAP B and the selected LSMS server.

```
The server does not know of 192.168.60.4.
Will just exchange host keys for the name given!
ssh is working correctly.
The server does not know of 192.168.60.4.
Will just exchange host keys for the name given!
Password of lsmsadm:
```

d) Enter the lsmsadm password.

A message provides notification that keys were exchanged (between ELAP B and the selected LSMS server) and SSH is working. You are returned to the **Exchange Secure Shell Keys Menu**.

```
The server does not know of 192.168.60.4.
Will just exchange host keys for the name given!
ssh is working correctly.

MPS Side A:  hostname: mps-a  hostid: 0
              Platform Version: 5.5.0-75.11.0
              Software Version: ELAP 10.0.0_100.13.0
              Wed Apr 10 09:34:14 EDT 2013
```

```
/-----Exchange Secure Shell Keys Menu-----\
/-----\
| 1 | Exchange Keys with Mate |
|---|-----\
| 2 | Exchange Keys with Remote |
|---|-----\
| 3 | Exchange Keys with Mate as Root User |
|---|-----\
| 4 | Exchange Keys with LSMS |
|---|-----\
| e | Exit |
\-----/
```

```
Enter Choice: 4
```

Note: The SSH keys must be exchanged between the ELAP servers and both LSMS servers (LSMS server A and LSMS server B).

- If you have exchanged SSH keys with only one LSMS server, repeat [Step 17](#) to exchange keys with the second LSMS server. .
 - If you have exchanged SSH keys with both LSMS server A and B (lsmspri and lsmssec), continue with [Substep e](#).
- e) Choose option **e** on the **Exchange Secure Shell Keys Menu** to return to the **ELAP Configuration Menu**.
- If you need to change the text-based UI password for the MPSs at this site, continue with [Step 18](#).
 - If you do not need to change the text-based UI password for the MPSs at this site, go to [Step 19](#).

18. Enter option 5, Change Password, from the **ELAP Configuration Menu** to change the text-based user interface password for the elapconfig login name for both MPS A and B at this site.

```

/-----ELAP Configuration Menu-----\
/-----\
| 1 | Display Configuration |
|---|-----|
| 2 | Configure Network Interfaces Menu |
|---|-----|
| 3 | Set Time Zone |
|---|-----|
| 4 | Exchange Secure Shell Keys |
|---|-----|
| 5 | Change Password |
|---|-----|
| 6 | Platform Menu |
|---|-----|
| 7 | Configure NTP Server |
|---|-----|
| 8 | Mate Disaster Recovery |
|---|-----|
| e | Exit |
\-----/

```

Enter Choice: 5

- a) Confirm the action of changing the password for both the MPS A and MPS B servers at this site. Pressing **Return** accepts the default of **n** (no) and aborts the action to change the password. Entering **y** invokes a prompt for the new password, followed by the re-entry of the password to confirm the entry.

```

Verifying connectivity with mate...
Are you sure you wish to change the text UI password on MPS A and B? [N]: y
Enter new password for text UI user:
Re-enter new password:
Press return to continue ...

```

- b) Enter the new password, confirm entry, and press **Return**. Successful entry of the new password returns the installer to the ELAP Configuration Menu.
- If you need to add an NTP server, continue with [Step 19](#).
 - If you do not need to add an NTP server, go to [Step 22](#)

19. Enter option 7, Configure NTP Server Menu, from the ELAP Configuration Menu to add an NTP Server.

```

/-----ELAP Configuration Menu-----\
/-----\
| 1 | Display Configuration |
|---|-----|
| 2 | Configure Network Interfaces Menu |
|---|-----|
| 3 | Set Time Zone |
|---|-----|
| 4 | Exchange Secure Shell Keys |
|---|-----|
| 5 | Change Password |
|---|-----|

```

6	Platform Menu
7	Configure NTP Server
8	Mate Disaster Recovery
e	Exit

Enter Choice: 7

- a) Enter option 2, Add External NTP Server, from the **ELAP Configure NTP Server Menu**.

/-----ELAP Configure NTP Server Menu-----\	
1	Display External NTP Server
2	Add External NTP Server
3	Remove External NTP Server
e	Exit

Enter Choice: 2

- b) Confirm the action of adding a new NTP Server.

Pressing **Return** accepts the default of **n** (no) and aborts the action to add an external NTP server.

- c) Enter **y** to add the IP address of the NTP server.

Note: The installer should now enter the same IP address for the NTP server that was previously added to the MPS A and B servers on EAGLE 5 A. This action allows the one NTP server to keep all MPS servers in synchronization.

```
Are you sure you wish to add new NTP Server? [N]: y
Enter the ELAP NTP Server IP Address: 192.168.61.69
Verifying NTP Server. It might take up to 1 minute.
External NTP Server [server 192.168.61.69 prefer]
has been added.
Press return to continue...
Verifying NTP Server. It might take up to 1 minute.
External NTP Server [server 192.102.61.91 prefer] has been added.
Press return to continue...
```

Note: All NTP Server IP addresses shown are only examples.

The display shows the server verification occurring. The installer receives a confirmation of a successful addition of the NTP server.

- To confirm successful addition of the NTP server, continue with [Step 20](#).
- Press **Return** to return to the **ELAP Configure NTP Server Menu**.

20. Enter option **1**, Display External NTP Server from the ELAP Configure NTP Server Menu, to confirm successful addition of the NTP server.

```

/-----ELAP Configure NTP Server Menu-----\
| 1 | Display External NTP Server |
| 2 | Add External NTP Server   |
| 3 | Remove External NTP Server|
| e | Exit                     |
\-----\
Enter Choice: 1

```

The output allows you to verify that the External NTP Server IP address is correct.

```

External NTP Server [server 192.168.61.69 prefer ]
Press return to continue...

```

- Press **Return** to return to the ELAP Configure NTP Server Menu.
- Enter option **e** to exit the ELAP Configure NTP Server Menu and return to the ELAP Configuration Menu.

```

/-----ELAP Configure NTP Server Menu-----\
| 1 | Display External NTP Server |
| 2 | Add External NTP Server   |
| 3 | Remove External NTP Server|
| e | Exit                     |
\-----\
Enter Choice: e

```

You are returned to the ELAP Configuration Menu.

Note: During configuration of MPSs on EAGLE 5 B, if the time zone was changed ([Step 12](#)) and if the Backup Provisioning Network ([Step 9](#)) was configured on either MPS, both MPS pairs on EAGLE 5 A and on EAGLE 5 B must be rebooted.

- If you do not need to reboot the MPS pairs on EAGLE 5 A and on EAGLE 5 B, continue with [Step 21](#).
- If you must reboot the MPS pairs on EAGLE 5 A and on EAGLE 5 B, go to [Step 22](#).

21. Enter option **e** to exit the **ELAP Configuration Menu**.
Configuration is complete. DO NOT continue with [Step 22](#).
22. Enter option **6**, Platform Menu, from the **ELAP Configuration Menu**.

```

/-----ELAP Configuration Menu-----\
| 1 | Display Configuration |
\-----\

```

```

 2 | Configure Network Interfaces Menu |
---|-----|
 3 | Set Time Zone                    |
---|-----|
 4 | Exchange Secure Shell Keys       |
---|-----|
 5 | Change Password                   |
---|-----|
 6 | Platform Menu                     |
---|-----|
 7 | Configure NTP Server              |
---|-----|
 8 | Mate Disaster Recovery            |
---|-----|
 e | Exit                             |
\-----/

Enter Choice: 6

```

23. Enter option 2, Reboot MPS, from the ELAP Platform Menu.

```

/-----ELAP Platform Menu--\
/-----\
 1 | Initiate Upgrade                |
---|-----|
 2 | Reboot MPS                      |
---|-----|
 3 | MySQL Backup                    |
---|-----|
 4 | RTDB Backup                     |
---|-----|
 e | Exit                           |
\-----/

Enter Choice: 3

```

```
Reboot MPS A, MPS B or [BOTH]:
```

24. At the prompt, press **Return** (default value of **BOTH**) to reboot MPS A and MPS B.

When the rebooting of the present MPS server pair on EAGLE 5 B ends, the Platform Menu may re-appear; however, the connection to the MPS server will be closed, and you are returned to the system prompt.

The console logon appears at the system prompt signifying the ELAP initial configuration is complete.

Note: The console logon is preceded by many lines of reboot output.

The initial configuration of MPSs on EAGLE 5 B is now complete. Both MPSs on EAGLE 5 A and MPSs on B are now configured and rebooted.

MPS Health Check Procedure

Run the `syscheck` utility to obtain the operational status of the MPS platform with the following procedure.

Refer to [Login Screen](#) and [User Administration Menu](#) for more details and information about logins and permissions.

For more information about the `syscheck` utility, see *Alarms and Maintenance* for ELAP.

1. Log into the **User Interface** screen of the ELAP GUI as `elapplatform`.

The main menu displays, [Figure 120: Main Menu View](#).

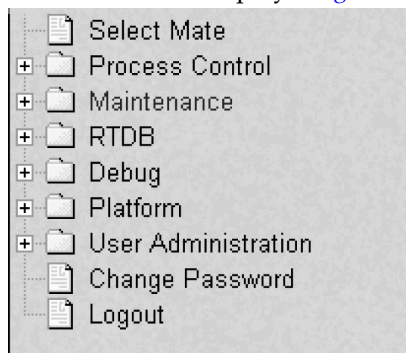


Figure 120: Main Menu View

Check the banner information above the menu to verify that you are logged into the correct ELAP.

2. If it is necessary to switch to another ELAP, select **Select Mate** from the main menu.

The Platform folder opens, [Figure 121: Platform Folder Open View](#).

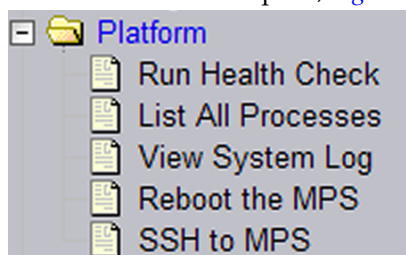


Figure 121: Platform Folder Open View

3. When the GUI shows you are logged into the desired ELAP, select **Platform** > **Run Health Check**.

The Run Health Check dialog opens, [Figure 122: Run Health Check View](#).

A Run Health Check

Output detail level: Normal ▼

Perform Check

Figure 122: Run Health Check View

4. On the **Run Health Check** screen, use the pull-down menu to select **Normal** or **Verbose** output detail level.
5. Click the **Perform Check** button to run the system health check on the selected MPS.
The system health check output data displays.

You have now completed this procedure.

Appendix B

Time Zone File Names

Topics:

- [Time Zone File Names.....282](#)

This appendix lists the valid UNIX file names for setting the time zone in ELAP software configuration.

Time Zone File Names

This appendix lists the valid UNIX file names, from the /usr/share/lib/zoneinfo /directory, for setting the time zone in ELAP software configuration. The initial default value for the time zone is "US/Eastern".

Table 50: Time zone File Names

africa	EET	Etc/GMT-9
asia	Egypt	etcetera
australasia	Eire	europe
Australia/ACT	EST	factory
Australia/Broken_Hill	EST5EDT	Factory
Australia/LHI	Etc/GMT	GB
Australia/North	Etc/GMT+0	GB-Eire
Australia/NSW	Etc/GMT+1	GMT
Australia/Queensland	Etc/GMT+10	GMT+0
Australia/South	Etc/GMT+11	GMT+1
Australia/Tasmania	Etc/GMT+12	GMT+10
Australia/Victoria	Etc/GMT+2	GMT+11
Australia/West	Etc/GMT+3	GMT+12
Australia/Yancowinna	Etc/GMT+4	GMT+13
backward	Etc/GMT+5	GMT+2
Brazil/Acre	Etc/GMT+6	GMT+3
Brazil/DeNoronha	Etc/GMT+7	GMT+4
Brazil/East	Etc/GMT+8	GMT+5
Brazil/West	Etc/GMT+9	GMT+6
Canada/Atlantic	Etc/GMT-0	GMT+7
Canada/Central	Etc/GMT-1	GMT+8
Canada/Eastern	Etc/GMT-10	GMT+9
Canada/East-Saskatchewan	Etc/GMT-11	GMT-0

Canada/Mountain	Etc/GMT-12	GMT-1
Canada/Newfoundland	Etc/GMT-13	GMT-10
Canada/Pacific	Etc/GMT-2	GMT-11
Canada/Yukon	Etc/GMT-3	GMT-12
CET	Etc/GMT-4	GMT-2
Chile/Continental	Etc/GMT-5	GMT-3
Chile/EasterIsland	Etc/GMT-6	GMT-4
CST6CDT	Etc/GMT-7	GMT-5
Cuba	Etc/GMT-8	GMT-6
GMT-7	Mideast/Riyadh89	Turkey
GMT-8	MST	UCT
GMT-9	MST7MDT	Universal
Greenwich	Navajo	US/Alaska
Hongkong	northamerica	US/Aleutian
HST	NZ	US/Arizona
Iceland	NZ-CHAT	US/Central
Iran	pacificnew	US/Eastern
Israel	Poland	US/East-Indiana
Jamaica	Portugal	US/Hawaii
Japan	PRC	US/Michigan
Kwajalein	PST8PDT	US/Mountain
Libya	ROC	US/Pacific
MET	ROK	US/Pacific-New
Mexico/BajaNorte	Singapore	US/Samoa
Mexico/BajaSur	solar87	UTC
Mexico/General	solar88	WET
Mideast/Riyadh87	solar89	W-SU
Mideast/Riyadh88	southamerica	Zulu

Appendix C

ELAP Local Provisioning Utility

Topics:

- [Introduction.....285](#)
- [LPU Commands.....285](#)
- [Common Information.....302](#)
- [Perl Statements and Functions.....304](#)

This appendix provides user guide information for the ELAP Local Provisioning Utility (LPU) batch command language.

Introduction

This chapter provides user guide information for the ELAP Local Provisioning Utility (LPU) batch command language.

LPU Commands

For each command listed in this section, the following information is given:

- A description of the command
- The command syntax
- A description of the command parameters
- An example of the command usage
- Rules, dependencies, and notes relevant to the command
- A list of related commands

Update Commands

ELAP supports the following update commands:

- *upd_lnp_sub*
- *upd_lnp_npanxx*
- *upd_lnp_lrn*
- *upd_split_npa*

upd_lnp_sub

Update LNP 10-Digit Subscription

Use this command to enter or change LNP 10-digit telephone number (TN) subscription or pooled TN's along with related services in the database.

Related services refer to message relay global title information. If the TN already exists, then the newly input data replaces the existing data. This command automatically creates the NPANXX for a TN-LRN record if the NPANXX does not already exist. It also creates an SP for a specified SP that does not already exist. The command updates data normally administered from the NPAC. Pooled TN's are allocated on an even 1000-block boundary. Specific ported TN's may overlap a pooled block and contain different routing.

Keyword

upd_lnp_sub

Parameters**TN => (mandatory)**

The telephone number.

Range = To specify a single TN subscription: 10 decimal digits

To pool a block of 1000 TNs: 7 digits with 3 asterisks (***) appended

SP=> (mandatory)

Service provider ID.

Range = 1-4 alphanumeric characters

LRN=> (mandatory)

The new location routing number.

Range = 10 decimal digits

CLASS_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for CLASS MR GTT.

Range = *ni* 001-255

nc 001-255 (if *ni* = 001-005)

000-255 (if *ni* = 006-255)

ncm 000-255

Default = Null

CLASS_SSN=> (optional)

Subsystem number for CLASS MR GTT

Range = 0, 2-255

Default = Null

LIDB_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for LIDB MR GTT.

Range = *ni*001-255

nc 001-255 (if *ni* = 001-005)

000-255 (if *ni* = 006-255)

ncm 000-255

Default = Null

LIDB_SSN=> (optional)

Subsystem number for LIDB MR GTT

Range = 0, 2-255

Default = Null

ISVM_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for ISVM MR GTT.

Range = ni 001-255

nc 001-255 (if *ni = 001-005*)

000-255 (if *ni = 006-255*)

ncm 000-255

Default = Null

ISVM_SSN=> (optional)

Subsystem number for ISVM MR GTT

Range = 0, 2-255

Default = Null

CNAM_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for CNAM MR GTT.

Range = ni 001-255

nc 001-255 (if *ni = 001-005*)

000-255 (if *ni = 006-255*)

ncm 000-255

Default = Null

CNAM_SSN=> (optional)

Subsystem number for CNAM MR GTT

Range = 0, 2-255

Default = Null

Examples

Individual TN:

```
upd_lnp_sub (TN => '1234567890', SP => 'A123', LRN => '1234567890', CLASS_DPC => '233-233-233',
CLASS_SSN => '0');
```

TN Pool

```
upd_lnp_sub (TN => '1234567***', SP => 'A123', LRN => '1234567890', CLASS_DPC => '233-233-233',
CLASS_SSN => '2');
```

Command Rules

The **TN** parameter must be 10 decimal digits or 7 decimal digits followed by 3 *s.

SP parameter must be 1-4 numbers/letters.

LRN parameter must be 10 decimal digits.

xxxxx_DPC parameter must be a valid ANSI DPC.

A service's DPC and SSN parameters must be specified together or not at all.

If the LRN parameter already exists, the SP parameter must be the same as the existing one for the LRN parameter.

Related Commands

dlt_lnp_sub, rtrv_lnp_sub

upd_lnp_npanxx

Update LNP NPANXX

Use this command to enter or change an existing LNP NPANXX record, including an LNP query or message relay default global title translation in the database.

The upd_lnp_npanxx command allows the user to enter or to change an LNP NPANXX and its associated LNP default global title translations in(to) the database. If the NPANXX already exists, then the newly input data replaces the existing data.

Keyword

upd_lnp_npanxx

Parameters

NPANXX=> (mandatory)

Block of 10,000 numbers.

Range = 6 digits

AIN=> (mandatory)

Local Advanced Intelligent Network (AIN) indicator.

Range = Y, N

IN=> (mandatory)

Local Intelligent Network (IN) indicator.

Range = Y, N

CLASS_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member (ni-nc-ncm)* for CLASS Default GTT.

Range = ni001-255

nc 001-255 (if ni = 001-005)

000-255 (if ni = 006-255)

ncm 000-255

Default = Null

CLASS_SSN=> (optional)

Subsystem number for CLASS Default GTT.

Range = 0, 2-255

Default = Null

CLASS_RI=> (optional)

Routing Indicator for CLASS Default GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) **D** (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

CLASS_NEWTT=> (optional)

New Translation Type for CLASS Default GTT.

Range = 0-255

Default = Null

LIDB_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member (ni-nc-ncm)* for LIDB Default GTT.

Range = ni001-255

nc 001-255 (if *ni = 001-005*)

000-255 (if *ni = 006-255*)

ncm 000-255

Default = Null

LIDB_SSN=> (optional)

Subsystem number for LIDB Default GTT

Range = 0, 2-255

Default = Null

LIDB_RI=> (optional)

Routing Indicator for LIDB Default GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) **D** (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

LIDB_NEWTT=> (optional)

New Translation Type for LIDB Default GTT.

Range = 0-255

Default = Null

ISVM_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for ISVM Default GTT.

Range = ni001-255

nc 001-255 (if *ni* = 001-005)

000-255 (if *ni* = 006-255)

ncm 000-255

Default = Null

ISVM_SSN=> (optional)

Subsystem number for ISVM Default GTT

Range = 0, 2-255

Default = Null

ISVM_RI=> (optional)

Routing Indicator for ISVM Default GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) **D** (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

ISVM_NEWTT=> (optional)

New Translation Type for ISVM Default GTT.

Range = 0-255

Default = Null

CNAM_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for CNAM Default GTT.

Range = ni001-255

nc 001-255 (if *ni* = 001-005)

000-255 (if *ni* = 006-255)

ncm 000-255

Default = Null

CNAM_SSN=> (optional)

Subsystem number for CNAM Default GTT

Range = 0, 2-255

Default = Null

CNAM_RI=> (optional)

Routing Indicator for CNAM Default GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) **D** (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

CNAM_NEWTT=> (optional)

New Translation Type for CNAM Default GTT.

Range = 0-255

Default = Null

Example

```
upd_lnp_npanxx (NPANXX => '123456', AIN => 'Y', IN => 'Y', CLASS_DPC => '233-233-233',  
CLASS_SSN => '0', CLASS_RI => 'G', CLASS_NEWTT => '71');
```

```
upd_lnp_npanxx (NPANXX => '234567', AIN => 'N', IN => 'N', CLASS_DPC => '33-23-33', CLASS_SSN  
=> '72', CLASS_RI => 'D', CLASS_NEWTT => '0');
```

Command Rules

NPANXX parameter must be 6 decimal digits.

AIN parameter must be **Y** (for Yes) or **N** (for No).

IN parameter must be **Y** (for Yes) or **N** (for No).

xxxxx_DPC parameter must be a valid ANSI DPC.

A service's **DPC** , **SSN** , **RI** , and **NEWTT** parameters must be specified together or not at all.

xxxxx_RI parameter must be **G** (for GT) or **D** (for DPC/SSN).

xxxxx_NEWTT parameter must be 0-255, inclusive.

A service's **NEWTT** parameter must be 0 unless its **RI** parameter is **G** and its **SSN** parameter is 0.

Notes

XXXX_RI => **G** is for an outgoing CDPA routing indicator of Route on Global Title.

XXXX_RI => **D** is for an outgoing CDPA routing indicator of Route on DPC/SSN.

Table 51: Mapping EAGLE 5 ISS to upd_lnp_npanxx LPU Command

EAGLE 5 ISS XLAT	EAGLE 5 ISS RI	EAGLE 5 ISS SSN	EAGLE 5 ISS NGT	LPU RI	LPU SSN	LPU NEWTT
DPC	GT	-	-	G	0	0
DPC	SSN	-	-	D	0	0
DPCSSN	GT	0-255	-	G	2-255	0
DPCSSN	SSN	0-255	-	D	2-255	0
DPCNGT	GT	-	0-255	G	0	1-255

Related Commands

dlt_lnp_npanxx

upd_lnp_lrn**Update LNP Location Routing Number**

Use this command to enter or change existing location routing number (LRN) specific information in the database.

This command allows the user to enter or to change an LNP Location Routing Number and its associated LNP message relay override global title translations in(to) the database. If the LRN already exists, then the newly input data replaces the existing data.

Keyword**upd_lnp_lrn****Parameters****LRN=> (mandatory)**

The location routing number.

Range = 10 decimal digits**SP=> (mandatory)**

Service provider ID.

Range = 1-4 alphanumeric characters**CLASS_DPC=> (optional)**

ANSI destination point code in the form of *network indicator-network cluster-network cluster member (ni-nc-ncm)* for CLASS MR Override GTT.

Range = *ni*001-255*nc* 001-255 (if *ni* = 001-005)**000-255** (if *ni* = 006-255)*ncm* 000-255**Default =** Null**CLASS_SSN=> (optional)**

Subsystem number for CLASS MR Override GTT.

Range = 0, 2-255**Default =** Null**CLASS_RI=> (optional)**

Routing Indicator for CLASS MR Override GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title)

D (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

CLASS_NEWTT=> (optional)

New Translation Type for CLASS MR Override GTT.

Range = 0-255

Default = Null

CLASS_RGTA=> (optional)

Replace Global Title Address (TN) with LRN for CLASS MR Override GTT.

Range = Y, N

Default = Null

LIDB_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for LIDB MR Override GTT.

Range = *ni*001-255

nc 001-255 (if *ni* = 001-005)

000-255 (if *ni* = 006-255)

ncm 000-255

Default = Null

LIDB_SSN=> (optional)

Subsystem number for LIDB MR Override GTT

Range = 0, 2-255

Default = Null

LIDB_RI=> (optional)

Routing Indicator for LIDB MR Override GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) D (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

LIDB_NEWTT=> (optional)

New Translation Type for LIDB MR Override GTT.

Range = 0-255

Default = Null

LIDB_RGTA=> (optional)

Replace Global Title Address (TN) with LRN for LIDB MR Override GTT.

Range = Y, N

Default = Null

ISVM_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for ISVM MR Override GTT.

Range = *ni*001-255

nc 001-255 (if *ni* = 001-005)

000-255 (if *ni* = 006-255)

ncm 000-255

Default = Null

ISVM_SSN=> (optional)

Subsystem number for ISVM MR Override GTT

Range = 0, 2-255

Default = Null

ISVM_RI=> (optional)

Routing Indicator for ISVM MR Override GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) D (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

ISVM_NEWTT=> (optional)

New Translation Type for ISVM MR Override GTT.

Range = 0-255

Default = Null

ISVM_RGTA=> (optional)

Replace Global Title Address (TN) with LRN for ISVM MR Override GTT.

Range = Y, N

Default = Null

CNAM_DPC=> (optional)

ANSI destination point code in the form of *network indicator-network cluster-network cluster member* (*ni-nc-ncm*) for CNAM MR Override GTT.

Range = *ni*001-255

nc 001-255 (if *ni* = 001-005)

000-255 (if *ni* = 006-255)

ncm 000-255

Default = Null

CNAM_SSN=> (optional)

Subsystem number for CNAM MR Override GTT

Range = 0, 2-255

Default = Null

CNAM_RI=> (optional)

Routing Indicator for CNAM MR Override GTT.

Range = G (the outgoing CDPA routing indicator of Route on Global Title) D (the outgoing CDPA routing indicator of Route on DPC/SSN)

Default = Null

CNAM_NEWTT=> (optional)

New Translation Type for CNAM MR Override GTT.

Range = 0-255

Default = Null

CNAM_RGTA=> (optional)

Replace Global Title Address (TN) with LRN for CNAM MR Override GTT.

Range = Y, N

Default = Null

Example

```
upd_lnp_lrn (LRN => '1234567890', SP => 'A123', CLASS_DPC => '233-233-233',
CLASS_SSN => '0', CLASS_RI => 'G', CLASS_NEWTT => '71', CLASS_RGTA => 'Y');

upd_lnp_lrn (LRN => '1234567890', SP => 'A123', CLASS_DPC => '33-23-33',
CLASS_SSN => '72', CLASS_RI => 'D', CLASS_NEWTT => '0', CLASS_RGTA => 'Y');
```

Command Rules

The **LRN** parameter must be 10 decimal digits.

The **SP** parameter must be 1-4 numbers/letters.

The **xxxxx_DPC** parameter must be a valid ANSI DPC.

The **xxxxx_RI** parameter must be **G** (for GT) or **D** (for DPC/SSN).

The **xxxxx_NEWTT** parameter must be 0-255, inclusive.

The **xxxx_RGTA** parameter must be **Y** (for Yes) or **N** (for No).

A service's **DPC**, **SSN**, **RI**, **NEWTT**, and **RGTA** parameters must be specified together or not at all.

A service's **NEWTT** parameter must be 0 unless its **RI** parameter is **G** and its **SSN** parameter is 0.

At least one service must be specified

If the **LRN** parameter already exists, the **SP** parameter must be the same as the existing one for the **LRN** parameter.

Notes

XXXX_RI => G is for an outgoing CDPA routing indicator of Route on Global Title.

XXXX_RI => D is for an outgoing CDPA routing indicator of Route on DPC/SSN.

Table 52: Mapping EAGLE 5 ISS to upd_lnp_lrn LPU Command

EAGLE 5 ISS XLAT	EAGLE 5 ISS RI	EAGLE 5 ISS SSN	EAGLE 5 ISS NGT	LPU RI	LPU SSN	LPU NEWTT
DPC	GT	-	-	G	0	0
DPC	SSN	-	-	D	0	0
DPCSSN	GT	0-255	-	G	2-255	0
DPCSSN	SSN	0-255	-	D	2-255	0
DPCNGT	GT	-	0-255	G	0	1-255

RGTA is not in the Table because it maps directly and is independent of the other parameters.

Related Commands

dlt_lnp_lrn

upd_split_npa

Update Split NPANXX

Use this command to force two different NPANXXs to reference the same last 4-digit telephone number (TN) in the database. During this time, updates to either NPANXX will update the same last 4-digit entry of a 10-digit ported TN. All existing NPANXX data is copied automatically to the new NPANXX for the split. It does not matter if the old block is specified as NNPANXX and the new is specified as NPANXX (i.e. the parameters are switched); they will still point to the same set of last 4 digits.

Keyword

upd_split_npa

Parameters

NPANXX=> (mandatory)

Block of 10,000 numbers.

Range = 6 digits

NNPANXX=> (mandatory)

New NPANXX.

Range = 6 digits

Example

```
upd_split_npa (NPANXX => '123456', NNPANXX => '234567');
```

Command Rules

NPANXX parameter must be 6 decimal digits.

NNPANXX parameter must be 6 decimal digits.

The NPANXX parameter must not already be split.

The new block cannot have any existing TNs.

The new block cannot be the same as the old.

The new block cannot have non-null service data that does not match the service data for the old block.

Related Commands

dlt_split_npa

Delete Commands

ELAP supports the following delete commands:

- *dlt_lnp_sub*
- *dlt_lnp_npanxx*
- *dlt_lnp_lrn*
- *dlt_split_npa*

dlt_lnp_sub**Delete LNP 10-Digit Telephone Number Subscription**

This command is used to remove an LNP 10-digit ported telephone number (TN) or a Pooled Block of 1000 TN's along with its related services from the database. Related services refer to message relay global title information. This command deletes data normally administered from the NPAC.

Keyword

dlt_lnp_sub

Parameters

TN => (mandatory)

The telephone number.

Range = To specify a single TN subscription: 10 decimal digits

To pool a block of 1000 TNs: 7 digits with 3 asterisks (***) appended

Examples

Individual TN:

dlt_lnp_sub (TN => '1234567890');

TN Pool

```
dlt_lnp_sub (TN => '1234567***');
```

Command Rules

The TN parameter must be 10 decimal digits or 7 decimal digits followed by 3 *s.

Notes

No error message when the TN parameter does not exist.

Related Commands

upd_lnp_sub, rtrv_lnp_sub

dlt_lnp_npanxx**Delete LNP Numbering Plan and Exchange**

This command is used to delete an LNP numbering plan area and exchange (NPANXX) and its associated LNP query or message relay default global title translations from the database.

Keyword

dlt_lnp_npanxx

Parameters

NPANXX=> (mandatory)

Block of 10,000 numbers.

Range = 6 digits

Example

```
dlt_lnp_npanxx (NPANXX => '123456');
```

Command Rules

The NPANXX parameter must be 6 decimal digits.

The NPANXX parameter cannot be part of a NPA split.

The NPANXX parameter cannot be part of a ported TN.

Notes

No error message when the NPANXX parameter does not exist.

Related Commands

upd_lnp_npanxx

dlt_lnp_lrn

Delete LNP Location Routing Number

Use this command to delete an existing location routing number (LRN) and its corresponding final overriding message relay global title translations from the database. The LRN can only be deleted if it is not referenced by a 10-digit telephone number.

Keyword

dlt_lnp_lrn

Parameters

LRN=> (mandatory)

The location routing number.

Range = 10 decimal digits

Example

```
dlt_lnp_lrn (LRN => '1234567890');
```

Command Rules

The LRN parameter must be 10 decimal digits.

Notes

No error message when LRN parameter does not exist.

Related Commands

upd_lnp_lrn

dlt_split_npa

Delete Split NPANXX

Use this command to remove the NPANXX from the database. This command allows the user to remove 1 of the 2 different NPANXXs referencing the same last 4 digits of TN in the database.

Keyword

dlt_split_npa

Parameters

NPANXX=> (mandatory)

Block of 10,000 numbers.

Range = 6 digits

Example

```
dlt_split_npa (NPANXX => '123456');
```

Command Rules

The NPANXX parameter must be 6 decimal digits.

The NPANXX parameter must be part of NPA split.

Notes

None

Related Commands

```
upd_split_npa
```

Retrieve Command

ELAP supports the [rtrv_lnp_sub](#) retrieve commands.

rtrv_lnp_sub**Retrieve LNP 10-digit Subscription**

Use this command to retrieve LNP 10 digit ported TN or a single Pooled Block of 1000 TN's along with related services from the database. Related services refer to message relay global title information. The command retrieves data normally administered from the NPAC.

Keyword

```
rtrv_lnp_sub
```

Parameters

TN=> (mandatory)

The telephone number.

Range = To specify a single TN subscription: 10 decimal digits

To pool a block of 1000 TNs: 7 digits with 3 asterisks (***) appended

Example

Individual TN:

```
rtrv_lnp_sub (TN => '1234567890');
```

TN Pool:

```
rtrv_lnp_sub (TN => '1234567***');
```

Command Rules

The TN parameter must be 10 decimal digits or 7 decimal digits followed by 3 *s.

Notes

None

Related Commands

upd_lnp_sub, dlt_lnp_sub

Output

Found:

```

TN = 2345678000
LRN = 0123456789
SP = ocl
Service TT   DPC           SSN RI  NEWTT
-----
CLASS      3 001-001-001    0 G    0
ISVM       6 001-002-003    4 D   ---
TN = 2345000***
LRN = 0123456789
SP = ocl
Service TT   DPC           SSN RI  NEWTT
-----
CLASS      3 001-001-001    0 G    0
ISVM       6 001-002-003    4 D   ---

```

Not Found:

```

TN 9195551234 not found.

```

Miscellaneous Commands

ELAP supports the following miscellaneous commands:

- [*set_echo*](#)
- [*set_cont_wo_remote*](#)

set_echo

This command is used to Turn on or off the output of calls to commands.

Example

```

set_echo(1);
dlt_lnp_sub(TN => '9195551234');
set_echo(0);

```

```
dlt_lnp_sub(TN => '9195554321');
```

Outputs

```
Processing dlt_lnp_sub (  
TN => '9195551234',  
)  
Done.
```

set_cont_wo_remote

This command is used to turn on or off the ability to continue to execute commands in the face of no connection to the remote LSMS port.

Example

```
set_cont_wo_remote(1);
```

Common Information

The information in these sub-sections highlights messages, formats, templates, and errors that are not specific to particular batch commands.

Success message

A success message is output when a batch file is successfully executed:

```
SUCCESS: The LPU batch file has been successfully executed.
```

Error message format

All command errors follow this format:

```
E1074: LPU batch failure: Batch Error: Message text at  
/export/home/elapall/LPU_batch line x
```

Message text will be replaced with the message text associated with the rule as provided in the command details.

The line number within the batch file where the error occurred replaces *x*.

Service parameters within error messages

When a service parameter is specified in the error message texts, one of the following templates is used to avoid repeating the message text for each possible service.

- *xxxx_DPC*
- *xxxx_SSN*

- `xxxx_RI`
- `xxxx_NEWTT`
- `xxxx_RGTA`

The appropriate service's mnemonic (e.g. CLASS, LIDB, ISVM, or CNAM) replaces `xxxx`.

Missing mandatory parameter

For all commands, the message text for a missing mandatory parameter is the following:

```
Missing mandatory argument x Need to insert the missing mandatory argument.
```

The parameter's mnemonic (for example, TN, SP, LRN, AIN, IN, or NPANXX) replaces `x`.

Communication errors

A number of connection errors may occur when processing batch commands. They are listed from most common to least common. The most likely corrective actions for each are included:

1. Could not connect to local LSMS port
 - Check the LSMS Connection Allowed state. If the LSMS Connection is Disabled, then Enable the LSMS Connection.
 - Check the LSMS HS Bulk Download Enabled state. If the LSMS Bulk Download for the ELAP is currently Enabled, then Disable the LSMS Bulk Download for the ELAP.
 - Check the state of the software on both ELAP sides. If the software is stopped (side is down), then start the software.
 - The LSMS may have been in the middle of connecting to the ELAPs. Try again.
2. No connection to remote LSMS port
 - The LSMS may have been in the middle of connecting to the ELAPs. Try again.
3. Could not connect to local LPU port
 - A user on the mate started a batch at the same time that grabbed the port before the local user's batch could. Try again.
4. Connection to LPU port closed by another instance
 - The local user's batch may have grabbed the port just before or just after it grabbed the mate user's batch. Try again.

Send and receive errors may occur when processing batch commands. They are listed in no particular order and should occur infrequently:

1. Could not send message
2. Receive header timed out
3. Could not receive header

4. Receive data timed out
5. Could not receive data

Perl errors

The following Perl-related error may occur:

```
Unable to create sub named "*Safe::Root0::x"
```

The most likely cause is a misspelled command or function name.

Perl Statements and Functions

The batch language is actually a subset of the Perl language with the addition of the functions/commands specified under [LPU Commands](#). For more information on Perl, see reference [1].

The following subsections highlight some of the more useful Perl statements and functions for batch processing.

#

If not quoted, comments out rest of line.

foreach

Iterates through a list, assigning the current element to a variable. For example, the following will retrieve TNs 919-555-0000 through 919-555-9999:

```
foreach $extension ('0000'..'9999')
{
    rtrv_lnp_sub(TN => "919555$extension");
}
```

print

Outputs string(s). For example, the following will output the TNs being deleted

```
foreach $tn ('9195550000'..'9195559999')
{
    print ("Deleting TN $tn \n");
    dlt_lnp_sub (TN => $tn);
}
```

scalar localtime

Returns the current time for the current locale in UNIX date command form. For example, the following:

```
print scalar localtime, "\n";
```

Output the following

```
Wed Apr 24 15:45:27 2002
```

eval

Allows user to catch an error without stopping execution of the batch. On error, the error message is put into the special variable \$@ and execution continues at the next line after the eval block.

For example without an eval, the following:

```
set_echo(1);
upd_lnp_sub (TN=>'9194601234', LRN=>'3456789012', SP=>'tklc',
CLASS_SSN=>2);
upd_lnp_sub (TN=>'9194602341', LRN=>'3456789012', SP=>'tklc');
rtrv_lnp_sub(TN=>'9194601234');
```

Produces:

```
Processing upd_lnp_sub (
  CLASS_SSN => '2',
  LRN => '3456789012',
  SP => 'tklc',
  TN => '9194601234',
)
ERROR: An error occurred while attempting the requested operation.
E1074: LPU batch failure: Batch Error: CLASS_DPC and CLASS_SSN must be specified
together at /export/home/elapall/LPU_batch line 3
```

However, if one puts the updates in an eval, the error can be caught and dealt with instead of exiting the batch execution. For example:

```
set_echo(1);
eval
{
  upd_lnp_sub (TN=>'9194601234', LRN=>'3456789012', SP=>'tklc',
CLASS_SSN=>2);
  upd_lnp_sub (TN=>'9194602341', LRN=>'3456789012', SP=>'tklc');
};
print $@ if $@;
rtrv_lnp_sub(TN=>'9194601234');
rtrv_lnp_sub(TN=>'9194602341');
```

Produces:

```
Processing upd_lnp_sub (
  CLASS_SSN => '2',
  LRN => '3456789012',
  SP => 'tklc',
  TN => '9194601234',
)
CLASS_DPC and CLASS_SSN must be specified together at
/export/home/elapall/LPU_batch line 5
Processing rtrv_lnp_sub (
```

```
    TN => '9194601234',  
  )  
TN 9194601234 not found.  
Processing rtrv_lnp_sub (  
  TN => '9194602341',  
)  
TN 9194602341 not found.  
Done.  
SUCCESS: The LPU batch file has been successfully executed.
```

A

ACG	<p>Automatic Call Gapping</p> <p>An element of the EAGLE LNP that controls the rate that location routing number (LRN) queries for a particular telephone number, or a portion of a telephone number, are received by the EAGLE LNP when a particular threshold is reached.</p>
ACT	<p>Activate</p>
AIN	<p>Advanced Intelligent Network</p> <p>A dynamic database used in Signaling System 7. It supports advanced features by dynamically processing the call based upon trigger points throughout the call handling process and feature components defined for the originating or terminating number.</p>
Allowed AFTPC	<p>The gateway screening entity that identifies the messages containing a specific affected point code. Messages containing the specified affected point code are allowed into the network.</p>
Allowed ISUP	<p>The gateway screening entity that identifies the ISUP or TUP message types that are allowed into the network.</p>

A**Allowed SIO**

The gateway screening entity that identifies the type of MSUs (ISUP, TUP, TCAP, and so forth) that are allowed into the network. The message type is determined by the network indicator code (NIC), priority (PRI), and service indicator (SI) fields of the signaling information octet (SIO) field in the MSU, and the H0 and H1 heading codes of the signaling information field of the MSU. Messages containing the specified message type go on to the next step in the gateway screening process, or are allowed into the network if the gateway screening process stops with this entity.

Allowed TT

The gateway screening entity that identifies the SCCP messages that have a specified translation type value in the called party address. SCCP messages containing specified translation type in the called party address go on to the next step in the gateway screening process, or are allowed into the network if the gateway screening process stops with this entity.

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

C

CdPA	<p>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 is located.</p>
CET	<p>Customer Environment Test</p>
CGI	<p>Cell Global Identity</p> <p>The standard identifier for geographically locating connected mobile phones.</p>
CLASS	<p>Custom Local Area Signaling Service</p> <p>Custom Local Area Subscriber Services</p>
CLEC	<p>Competitive Local Exchange Carrier</p>
CLLI	<p>Common Language Location Identifier</p> <p>The CLLI uniquely identifies the STP in terms of its physical location. It is usually comprised of a combination of identifiers for the STP's city (or locality), state (or province), building, and traffic unit identity. The format of the CLLI is:</p> <p>The first four characters identify the city, town, or locality.</p>

C

The first character of the CLLI must be an alphabetical character.

The fifth and sixth characters identify state or province.

The seventh and eighth characters identify the building.

The last three characters identify the traffic unit.

CNAM

Calling Name Delivery

An IN (Intelligent Network) service that displays the caller's name on the calling party's phone. This is similar to caller ID except that the calling party's name is displayed along with the calling number or instead of the calling number.

CSPC

Concerned Signaling Point Code

The point code that receives subsystem allowed and subsystem prohibited status messages about a particular global title translation node. These messages are broadcast from SCCP management.

D

daemon

A process that runs in the background (rather than under the direct control of a user) and performs a specified operation at predefined times or in response to certain events. Generally speaking, daemons are assigned names that end with the letter "d." For example, sentryd is the daemon that runs the Sentry utility.

Database

All data that can be administered by the user, including cards, destination point codes, gateway

D

screening tables, global title translation tables, links, LNP services, LNP service providers, location routing numbers, routes, shelves, subsystem applications, and 10 digit telephone numbers.

DB

Database
Data bus

DD

Detailed Design

DESTFLD

The point code in the affected destination field (the concerned signaling point code) of incoming MTP network management messages from another network that are allowed into the EAGLE.

DIX

Digital/Intel/Xerox
Digital/Intel/Xerox de facto standard for Ethernet Media Access Control Type.

DN

Directory number
A DN can refer to any mobile or wireline subscriber number, and can include MSISDN, MDN, MIN, or the wireline Dialed Number.

DPC

Destination Point Code - DPC refers to the scheme in SS7 signaling to identify the receiving signaling point. In the SS7 network, the point codes are numeric addresses which uniquely identify each signaling point. This point code can be adjacent to the EAGLE, but does not have to be.

D

DSM

Database Service Module.

The DSM provides large capacity SCCP/database functionality. The DSM is an application card that supports network specific functions such as EAGLE Provisioning Application Processor (EPAP), Global System for Mobile Communications (GSM), EAGLE Local Number Portability (ELAP), and interface to Local Service Management System (LSMS).

DV

Digits Valid

E

ELAP

EAGLE Local Number Portability Application Processor

The EAGLE LNP Application Processor (ELAP) platform provides capacity and performance required to support the ported number database.

EMS

Element Management System

The EMS feature consolidates real-time element management at a single point in the signaling network to reduce ongoing operational expenses and network downtime and provide a higher quality of customer service.

EO

End Office

EPAP-related features

Features that require EPAP connection and use the Real Time Database (RTDB) for lookup of subscriber information.

E

- ANSI Number Portability Query (AINPQ)
- ANSI-41 Analyzed Information Query – no EPAP/ELAP (ANSI41 AIQ)
- Anytime Interrogation Number Portability (ATI Number Portability, ATINP)
- AINPQ, INP, G-Port SRI Query for Prepaid, GSM MAP SRI Redirect, IGM, and ATINP Support for ROP
- A-Port Circular Route Prevention (A-Port CRP)
- Equipment Identity Register (EIR)
- G-Flex C7 Relay (G-Flex)
- G-Flex MAP Layer Routing (G-Flex MLR)
- G-Port SRI Query for Prepaid
- GSM MAP SRI Redirect to Serving HLR (GSM MAP SRI Redirect)
- GSM Number Portability (G-Port)
- IDP A-Party Blacklist
- IDP A-Party Routing
- IDP Relay Additional Subscriber Data (IDPR ASD)
- IDP Relay Generic Routing Number (IDPR GRN)
- IDP Service Key Routing (IDP SK Routing)
- IDP Screening for Prepaid
- INAP-based Number Portability (INP)
- Info Analyzed Relay Additional Subscriber Data (IAR ASD)
- Info Analyzed Relay Base (IAR Base)
- Info Analyzed Relay Generic Routing Number (IAR GRN)
- Info Analyzed Relay Number Portability (IAR NP)
- INP Circular Route Prevention (INP CRP)

E

- IS41 Mobile Number Portability (A-Port)
- IS41 GSM Migration (IGM)
- MNP Circular Route Prevention (MNPCRP)
- MO-based GSM SMS NP
- MO-based IS41 SMS NP
- MO SMS Generic Routing Number (MO SMS GRN)
- MO- SMS B-Party Routing
- MO SMS IS41-to-GSM Migration
- MT-based GSM SMS NP
- MT-based GSM MMS NP
- MT-based IS41 SMS NP
- MTP Routed Messages for SCCP Applications (MTP Msgs for SCCP Apps)
- MTP Routed Gateway Screening Stop Action (MTPRTD GWS Stop Action)
- Portability Check for MO SMS
- Prepaid IDP Query Relay (IDP Relay, IDPR)
- Prepaid SMS Intercept Phase 1 (PPSMS)
- Service Portability (S-Port)
- S-Port Subscriber Differentiation
- Triggerless ISUP Framework Additional Subscriber Data (TIF ASD)
- Triggerless ISUP Framework Generic Routing Number (TIF GRN)
- Triggerless ISUP Number Portability (TIF NP)
- Triggerless ISUP Framework Number Substitution (TIF NS)
- Triggerless ISUP Framework SCS Forwarding (TIF SCS Forwarding)
- Triggerless ISUP Framework Simple Number Substitution (TIF SNS)
- Voice Mail Router (V-Flex)

F

FTA	<p>File Transfer Area</p> <p>A special area that exists on each OAM hard disk, used as a staging area to copy files to and from the EAGLE using the Kermit file-transfer protocol.</p>
FTP	<p>File Transfer Protocol</p> <p>A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network.</p> <p>Feature Test Plan</p>

G

GB	<p>Gigabyte — 1,073,741,824 bytes</p>
GMT	<p>Greenwich Mean Time</p>
GT	<p>Global Title Routing Indicator</p>
GTT	<p>Global Title Translation</p> <p>A feature of the signaling connection control part (SCCP) of the SS7 protocol that the EAGLE uses to determine which service database to send the query message when an MSU enters the EAGLE and more information is needed to route the MSU. These service databases also verify calling card numbers and credit card numbers. The service databases are identified in the SS7 network by a point code and a subsystem number.</p>
GUI	<p>Graphical User Interface</p>

G

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

HS High Speed

HSOP High Speed Operation Protocol

HTTP Hypertext Transfer Protocol

I

IAM Initial Address Message
Ensures that the services offered are compatible with the reception devices, and can be used. For example, IAM prevents a phone being connected to a facsimile.

ID Identity, identifier

IMSI International Mobile Subscriber Identity
A unique internal network ID identifying a mobile subscriber.
International Mobile Station Identity

IN Intelligent Network
A network design that provides an open platform for developing, providing and managing services.

IP Intelligent Peripheral

I

Internet Protocol - IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides packet routing, fragmentation and re-assembly through the data link layer.

IP Address	The location of a device on a TCP/IP network. The IP Address is either a number in dotted decimal notation which looks something like (IPv4), or a 128-bit hexadecimal string such as (IPv6).
IPM	Initial Product Manufacture
IS-ANR	<p>In Service - Abnormal</p> <p>The entity is in service but only able to perform a limited subset of its normal service functions.</p>
IS-NR	In Service - Normal
ISS	Integrated Signaling System
ISUP	<p>ISDN User Part</p> <p>The ISDN-specific part of the transmission with additional information via a signaling channel between exchanges.</p>
ISVM	Inter-switch Voice Messaging

L

LAN	<p>Local Area Network</p> <p>A private data network in which serial transmission is used for direct data communication among data stations located in the same proximate location. LAN uses coax cable, twisted pair, or multimode fiber.</p> <p>See also STP LAN.</p>
LIDB	<p>Line Information Database</p>
LNP	<p>Local Number Portability</p> <p>The ability of subscribers to switch local or wireless carriers and still retain the same phone number.</p>
LNPQS	<p>LNP Query Service</p>
LNP SMS	<p>LNP Short Message Service</p>
LRN	<p>Location Routing Number</p> <p>A 10-digit number in a database called a Service Control Point (SCP) that identifies a switching port for a local telephone exchange. LRN is a technique for providing Local Number Portability.</p>
LRNQT	<p>ITU TCAP LRN Query Service</p> <p>A feature that provides support for an ITU TCAP LRN query/response using the LRN method in order to support Number Portability.</p>
LSMS	<p>Local Service Management System</p>

L

An interface between the Number Portability Administration Center (NPAC) and the LNP service databases. The LSMS receives LNP data from the NPAC and downloads that data to the service databases. LNP data can be entered into the LSMS database. The data can then be downloaded to the LNP service databases and to the NPAC.

M

MASP

Maintenance and Administration Subsystem Processor

The Maintenance and Administration Subsystem Processor (MASP) function is a logical pairing of the GPSM-II card and the TDM card. The GPSM-II card is connected to the TDM card by means of an Extended Bus Interface (EBI) local bus.

The MDAL card contains the removable cartridge drive and alarm logic. There is only one MDAL card in the Maintenance and Administration Subsystem (MAS) and it is shared between the two MASPs.

MMI

Man-Machine Interface

MPS

Multi-Purpose Server

The Multi-Purpose Server provides database/reload functionality and a variety of high capacity/high speed offboard database functions for applications. The MPS resides in the General Purpose Frame.

Messages Per Second

M

A measure of a message processor's performance capacity. A message is any Diameter message (Request or Answer) which is received and processed by a message processor.

MR

Message Relay

MSC

Mobile Switching Center

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

MSU

Message Signal Unit

The SS7 message that is sent between signaling points in the SS7 network with the necessary information to get the message to its destination and allow the signaling points in the network to set up either a voice or data connection between themselves. The message contains the following information:

- The forward and backward sequence numbers assigned to the message which indicate the position of the message in the traffic stream in relation to the other messages.
- The length indicator which indicates the number of bytes the message contains.
- The type of message and the priority of the message in the signaling information octet of the message.
- The routing information for the message, shown in the routing label of the message, with the

M

identification of the node that sent message (originating point code), the identification of the node receiving the message (destination point code), and the signaling link selector which the EAGLE uses to pick which link set and signaling link to use to route the message.

MTSU

Message Transfer System Utility

N

NAT

Network Address Translation

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

NGT

New Global Title

NPA

Number Plan Area

The North American "Area Codes." (3 digits: 2- to-9, 0-or 1, 0-to-9. Middle digit to expand soon).

N

NPAC	<p>Number Portability Administration Center</p> <p>This center administers the Service Management System (SMS) regional database, managed by an independent third party, to store all Local Number Portability data, including the status of a ported telephone number, the current service provider and the owner of the telephone number.</p>
NTP	Network Time Protocol
NXX	Central Office Exchange Code

O

OAM	<p>Operations, Administration, and Maintenance</p> <p>The application that operates the Maintenance and Administration Subsystem which controls the operation of many products.</p>
OOS-MT	<p>Out of Service - Maintenance</p> <p>The entity is out of service and is not available to perform its normal service function. The maintenance system is actively working to restore the entity to service.</p>
OOS-MT-DSBLD	<p>Out of Service - Maintenance Disabled</p> <p>The entity is out of service and the maintenance system is preventing the entity from performing its normal service function.</p>

P

P

PC

Point Code

The identifier of a signaling point or service control point in a network. The format of the point code can be one of the following types:

- ANSI point codes in the format network indicator-network cluster-network cluster member (**ni-nc-ncm**).
- Non-ANSI domestic point codes in the format network indicator-network cluster-network cluster member (**ni-nc-ncm**).
- Cluster point codes in the format network indicator-network cluster-* or network indicator-*.*.
- ITU international point codes in the format **zone-area-id**.
- ITU national point codes in the format of a 5-digit number (**nnnnn**), or 2, 3, or 4 numbers (members) separated by dashes (**m1-m2-m3-m4**) as defined by the Flexible Point Code system option. A group code is required (**m1-m2-m3-m4-gc**) when the ITUDUPPC feature is turned on.
- 24-bit ITU national point codes in the format main signaling area-subsignaling area-service point (**msa-ssa-sp**).

PCS

Personal Communications Service
(North American GSM)

PDBA

Provisioning Database Application

P

There are two Provisioning Database Applications (PDBAs), one in EPAP A on each EAGLE. They follow an Active/Standby model. These processes are responsible for updating and maintaining the Provisioning Database (PDB).

PDBI

Provisioning Database Interface

The interface consists of the definition of provisioning messages only. The customer must write a client application that uses the PDBI request/response messages to communicate with the PDBA.

PDP

Permissive Dialing Period
Packet Data Protocol

PIN

Personal Identification Number

PLNP

The Personal Communications Service (PCS) 1900 LNP Query (PLNP) feature provides for LNP query/response in a PCS wireless environment using the LRN method to support Service Provider Number Portability.

R

Restricted

The network management state of a route, link set, or signaling link that is not operating properly and cannot carry all of its traffic. This condition only allows the highest priority messages to sent to the database entity first, and if space allows, followed by the other traffic. Traffic that cannot be sent on the restricted database entity

R

must be rerouted or the traffic is discarded.

RFC

Request for Comment

RFCs are standards-track documents, which are official specifications of the Internet protocol suite defined by the Internet Engineering Task Force (IETF) and its steering group the IESG.

RI

Routing Indicator

RN

Routing Number

The number provided by the Freephone Service Provider (FSP) to the Access Service Provider (ASP) to enable a pre-determined routing of traffic to a specific network/carrier/customer.

Route

A signaling path from an LSP to an RSP using a specified Link Set

RTDB

Real Time Database

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.

S

Service Module card	DSM, E5-SM4G, or E5-SM8G-B card that contains the Real Time Database (RTDB) downloaded from an EPAP or ELAP system.
SIO	<p>Service Information Octet.</p> <p>The network indicator code (NIC), priority (PRI), and service indicator (SI) in the SIO field in the message signaling unit (MSU). This information identifies the type of MSU (ISUP, TCAP, and so forth) that is allowed in the network where the EAGLE is located.</p>
SP	<p>Service Provider</p> <p>Signaling Point</p> <p>A set of signaling equipment represented by a unique point code within an SS7 domain.</p>
Split NPA	<p>Split Number Planning Area</p> <p>A process that forces two different NPANXXs to reference the same last 4 digits of a 10 digit ported telephone number in the database. When either NPANXX is updated, the 10 digit ported telephone numbers in each NPANXX with the same last 4 digits are updated. When the NPANXX is split, all existing NPANXX data for the NPANXX being split is copied to the new NPANXX.</p>
SS7	<p>Signaling System #7</p> <p>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</p>

S

these signaling points. These messages are sent over its own network and not over the revenue producing voice and data paths. The EAGLE is an STP, which is a device that routes these messages through the network.

SSH

Secure Shell

A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.

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.

Subsystem Number

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.

SSP

Subsystem Prohibited network management message.

S

Subsystem Prohibited SCCP (SCMG) management message. (CER)

Service Switching Point (SS7 Network)

Signal Switching Point

Signal Switching Points are switches that originate, terminate, or tandem calls. An SSP sends signaling messages to other SSPs to setup, manage, and release voice circuits required to complete a call.

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

T

TCAP

Transaction Capabilities

Application Part - A protocol in the SS7 protocol suite that enables the deployment of advanced intelligent network services by supporting non-circuit related information exchange between signaling points using the Signaling Connection Control Part connectionless service. TCAP also supports remote control - ability to invoke features in another remote network switch.

TCP/IP

Transmission Control
Protocol/Internet Protocol

T

TFP	<p>TransFer Prohibited (Msg)</p> <p>A procedure included in the signaling route management (functionality) used to inform a signaling point of the unavailability of a signaling route.</p>
TN	<p>Telephone Number</p> <p>A 10 digit ported telephone number.</p>
Translation Type	<p>See TT.</p>
Triggerless LNP	<p>A feature that gives service providers a method to route calls to ported numbers without having to upgrade their signaling switch (end office or mobile switching center) software. This feature uses the gateway screening stop action TLNP to intercept through-switched ISUP messages on the LIM.</p>

U

UAM	<p>Unsolicited Alarm Message</p> <p>A message sent to a user interface whenever there is a fault that is service-affecting or when a previous problem is corrected. Each message has a trouble code and text associated with the trouble condition.</p>
UDP	<p>User Datagram Protocol</p>
UDT	<p>Unitdata Transfer</p>

U

UDTS	Unitdata Transfer Service An error response to a UDT message.
UI	User Interface
UIM	Unsolicited Information Message A message sent to a user interface whenever there is a fault that is not service-affecting or when a previous problem is corrected. Each message has a trouble code and text associated with the trouble condition.
UTC	Coordinated Universal Time

V

VIOL	A value displayed on an application GUI that indicates that the client browser's Java policy file is incorrect.
VIP	Virtual IP Address Virtual IP is a layer-3 concept employed to provide HA at a host level. A VIP enables two or more IP hosts to operate in an active/standby HA manner. From the perspective of the IP network, these IP hosts appear as a single host.
VSCCP	VxWorks Signaling Connection Control Part The application used by the Service Module card to support EPAP-related features and LNP

V

features. If an EPAP-related or LNP feature is not turned on, and a Service Module card is present, the VSCCP application processes normal GTT traffic.

W

WAN

Wide Area Network

A network which covers a larger geographical area than a LAN or a MAN.

WNP

Wireless Number Portability

The Wireless Number Portability feature enhances the Local Number Portability feature to allow wireless service providers to query the LNP database for ported telephone numbers. The query is used to find the location routing number associated with the ported telephone number so the telephone call can be routed to its proper destination. The Wireless Number Portability feature can only be used for ANSI messages not for ITU messages.

X

XLAT

Translate Indicator