Tekelec EAGLE® 5

ELAP Administration Manual - 9.0

910-5887-001 Revision A
September 2010

Copyright 2010 Tekelec. All Rights Reserved. Printed in USA.
Legal Information can be accessed from the Main Menu of the optical disc or on the
Tekelec Customer Support web site in the *Legal Information* folder of the *Product Support* tab.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Topics:

This chapter contains general information about the ELAP user interface documentation, the organization of this manual, and how to get technical assistance.

Overview

This manual describes how to administer the EAGLE LNP Application Processor (ELAP), and how to use the ELAP user interface menus to perform configuration, maintenance, debug, and platform operations.

The Local Number Portability (LNP) 384 Million Records feature supports 240 to 384 Million provisionable Telephone Numbers (TNs).

Note: Refer to the *LNP Feature Activation Guide* for the available configurations.

The MPS hardware platform supports high-speed provisioning of large databases for the Tekelec EAGLE 5 Integrated Signaling System (ISS). The MPS is composed of hardware and software components that interact to create a secure and reliable platform.

MPS running ELAP supports provisioning from the Local Service Management System (LSMS) to the EAGLE 5 ISS Services Module cards, using the LNP 384 Million Records feature for North American LNP.

Scope and Audience

This manual is intended for anyone responsible for ELAP administration and using the ELAP user interface in the EAGLE 5 ISS. Users of this manual and the others in the EAGLE 5 ISS family of documents must have a working knowledge of telecommunications and network installations.

Manual Organization

This document is organized into these chapters:

- *Introduction* contains general information about the ELAP user interface documentation, the organization of this manual, and how to get technical assistance.
- *Functional Description* provides a description of ELAP overall design and operation.
- *ELAP Graphical User Interface* describes how to log into the ELAP user interface and how to use the ELAP user interface menus.
- *Messages, Alarms, and Status Reporting* describes ELAP status reporting, alarms, and error messages.
- *ELAP Software Configuration* describes the text-based user interface that performs ELAP configuration and initialization.
- *Time Zone File Names*, lists the valid UNIX file names for setting the time zone in ELAP software configuration.
- *ELAP Local Provisioning Utility*, provides user guide information for 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

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

Customer Care Center

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

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

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

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

Tekelec - Global

Email (All Regions): support@tekelec.com

- **USA and Canada**

  Phone:

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

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

TAC Regional Support Office Hours:

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

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

  Phone:

  USA access code +1-800-658-5454, then 1-888-FOR-TKLC or 1-888-367-8552 (toll-free)

  TAC Regional Support Office Hours (except Brazil):

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

  - **Argentina**

    Phone:

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

  - **Brazil**

    Phone:

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

    TAC Regional Support Office Hours:

    8:30 a.m. through 6:30 p.m. (GMT minus 3 hours), Monday through Friday, excluding holidays

  - **Chile**

    Phone:

    1230-020-555-5468

  - **Colombia**

    Phone:

    01-800-912-0537

  - **Dominican Republic**

    Phone:

    1-888-367-8552

  - **Mexico**

    Phone:

    001-888-367-8552

  - **Peru**

    Phone:

    0800-53-087

  - **Puerto Rico**

    Phone:

    1-888-367-8552 (1-888-FOR-TKLC)

  - **Venezuela**

    Phone:

0800-176-6497

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

  Regional Office Hours:

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

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

- **Asia**

  - **India**

    Phone:

    +91 124 436 8552 or +91 124 436 8553

    TAC Regional Support Office Hours:

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

  - **Singapore**

    Phone:

    +65 6796 2288

    TAC Regional Support Office Hours:

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

Emergency Response

In the event of a critical service situation, emergency response is offered by the Tekelec Customer Care Center 24 hours a day, 7 days a week. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with an EAGLE 5 ISS that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical problems affect service and/or system operation resulting in:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system

- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

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

Related Publications

For information about additional publications that are related to this document, refer to the *Related Publications* document. The *Related Publications* document is published as a part of the *Release Documentation* and is also published as a separate document on the Tekelec Customer Support Site.

Documentation Availability, Packaging, and Updates

Tekelec provides documentation with each system and in accordance with contractual agreements. For General Availability (GA) releases, Tekelec publishes a complete EAGLE 5 ISS documentation set. For Limited Availability (LA) releases, Tekelec may publish a documentation subset tailored to specific feature content or hardware requirements. Documentation Bulletins announce a new or updated release.

The Tekelec EAGLE 5 ISS documentation set is released on an optical disc. This format allows for easy searches through all parts of the documentation set.

The electronic file of each manual is also available from the *Tekelec Customer Support* site. This site allows for 24-hour access to the most up-to-date documentation, including the latest versions of Feature Notices.

Printed documentation is available for GA releases on request only and with a lead time of six weeks. The printed documentation set includes pocket guides for commands and alarms. Pocket guides may also be ordered separately. Exceptions to printed documentation are:

- Hardware or Installation manuals are printed without the linked attachments found in the electronic version of the manuals.
- The Release Notice is available only on the Customer Support site.

Note: Customers may print a reasonable number of each manual for their own use.

Documentation is updated when significant changes are made that affect system operation. Updates resulting from Severity 1 and 2 Problem Reports (PRs) are made to existing manuals. Other changes are included in the documentation for the next scheduled release. Updates are made by re-issuing an electronic file to the customer support site. Customers with printed documentation should contact their Sales Representative for an addendum. Occasionally, changes are communicated first with a Documentation Bulletin to provide customers with an advanced notice of the issue until officially released in the documentation. Documentation Bulletins are posted on the Customer Support site and can be viewed per product and release.

Locate Product Documentation on the Customer Support Site

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

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

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

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

Chapter 2

Functional Description

Topics:

This chapter provides a description of ELAP overall design and operation.

General Description

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 5 ISS E5-SM4G cards

The Multi-Purpose Server (MPS) hardware platform supports high-speed provisioning of large databases for the EAGLE 5 ISS. 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.

The Local Number Portability (LNP) feature supports from 24 to 384 million provisionable Telephone Numbers (TNs).

The LNP feature utilizes the "master" or "golden" Real Time database (RTDB) that is loaded from the (MPS) to E5-SM4G cards on the EAGLE 5 ISS.

See the *LNP Feature Activation Guide* for more information.

Definition of Terms

These terms are used throughout this manual.

MPS

One Tekelec 1100 Application Server (T1100 AS) is referred to as an MPS server.

The two MPS servers installed at one EAGLE 5 ISS location are installed in one frame. The two MPS servers that are located at one EAGLE 5 ISS location are "mate servers"—from one MPS server, the other MPS server in the frame can be referred to as its mate. The two servers are also referred to as "server A" and "server B."

MPS System

An MPS system consists of two MPS servers and associated hardware that are located at one EAGLE 5 ISS location.

Usually, a minimum of two MPS systems are deployed in the customer network (one at each mated EAGLE 5 ISS). These two MPS systems are considered "mate MPS systems" on mated EAGLE 5 ISSs.

ELAP

The EAGLE LNP Application Processor (ELAP) software that is supported by MPS includes support for the LNP 384 Million Records feature.

An MPS server that is hosting ELAP is referred to as an MPS running ELAP. One MPS server running ELAP is also referred to as ELAP A, while the mate MPS server running ELAP is referred to as ELAP B.

The two MPS servers running ELAP at each EAGLE 5 ISS site have exactly the same software installed.

SP (or SPID) refers to the Service Provider ID. These are 4 alphanumeric characters assigned to each carrier. The ELAP can store up to 32,700 SP entries in the RTDB.

MR (Message Relay) is another name for service (CNAM, CLASS, LIDB, ISVM, WSMSC). Each Message Relay entry contains ri (routing indicator) and ngt (new gtt translation) data. The ELAP is capable of storing up to 65,500 MR entries in the RTDB.

An MR Group (Message Relay Group) is a group of one or more MR entries that are assigned to a particular TN. The ELAP supports up to 2 million MR groups.

Overall Design

The Multi Purpose Server (MPS) hardware platform supports high-speed provisioning of large databases for the EAGLE 5 ISS running ELAP 9.0.

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 5 ISS E5-SM4G cards

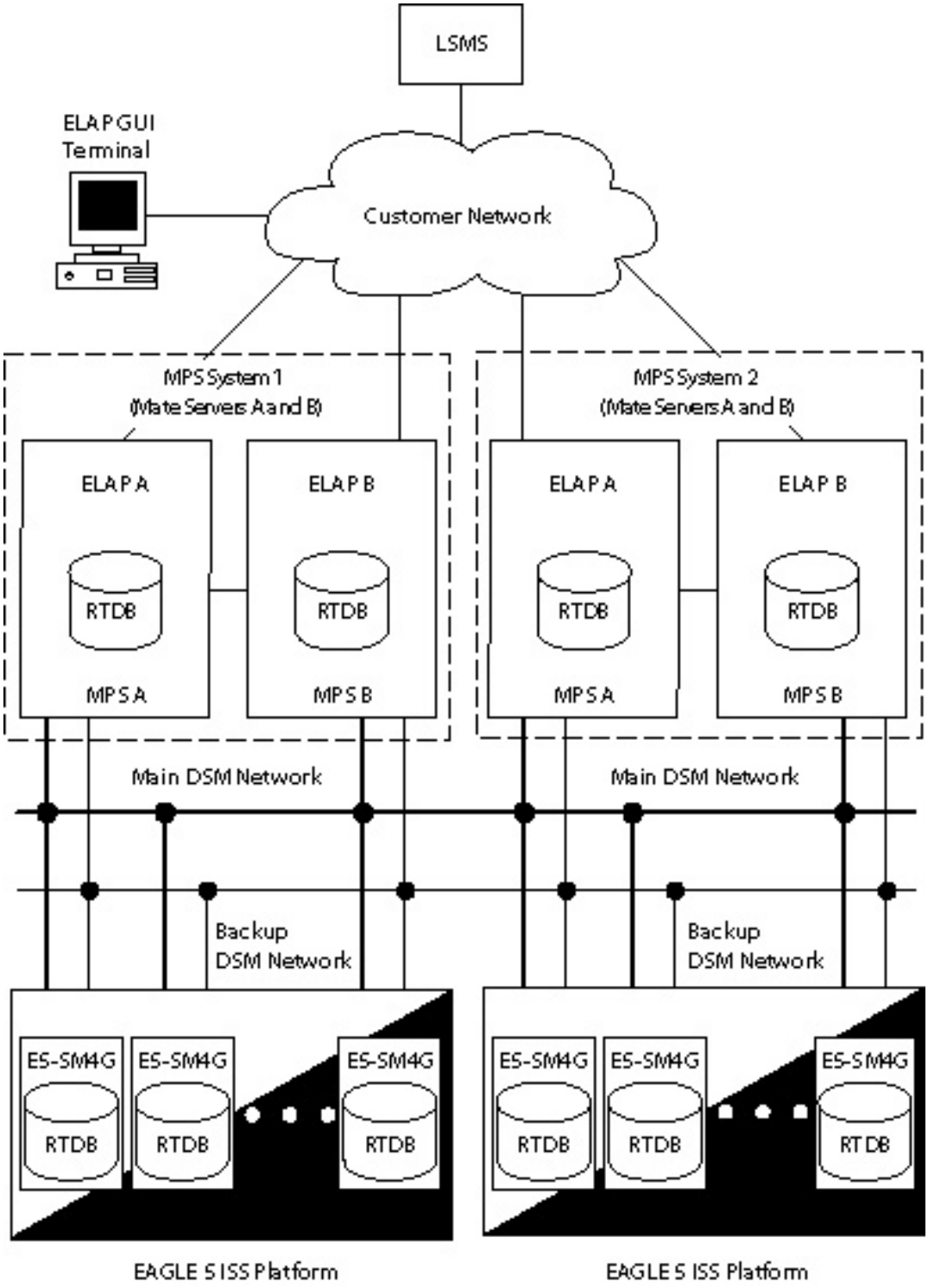
During normal operation, information flows through the ELAP with no intervention.

ELAP provides a direct user interface for performing configuration, maintenance, debugging, and platform operations. *Overview of the ELAP User Interfaces* describes the ELAP user interface menus and operations.

Figure 1: ELAP Installation illustrates a typical ELAP installation.

The LNP feature requires the use of up to 18 E5-SM4G cards.

Figure 1: ELAP Installation



An MPS system consists of two mated Tekelec 1100 AS processors (MPS Server A and MPS Server B) installed as part of an EAGLE 5 ISS. 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 E5-SM4G cards and the ELAPs. Another Ethernet network connects the two ELAPs; it is referred to as the ELAP Sync network. (See *Network Connections*.)

Figure 1: 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 5 ISS E5-SM4G cards. The set of E5-SM4G cards, each of which holds a copy of the RTDB, is part of the EAGLE 5 ISS.

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 E5-SM4G cards.

One ELAP runs as the Active ELAP and the other as the Standby ELAP. In normal operation, the RTDB on the E5-SM4G 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 E5-SM4Gcards.

MPS running ELAP 8.0 or later supports the LNP feature.

The LNP feature supports a maximum of 24 million to 384 million Telephone Numbers (TNs) in the RTDB. 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 you can enable LNP.

Three additional feature keys, LNP TN QTY, LNP NPANXX QTY and LNP LRN QTY,regulate the maximum capacity allowed within the LNP DB System and contain a finite increment of the quantity field. The LNP, LNP NPAXXX, and LNP LRN feature quantities indicate the maximum number of TN, NPAXXX, and LRNs allowed in the RTDB.

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 EAGLE 5 ISS.

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 EAGLE 5 ISS.

   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 RMTP channels have failed.
4. A fatal software error occurred.

5. The ELAP is forced to Standby by the user interface Force to Become Standby operation.

If the Active ELAP has one or more of the five 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 are:

1. 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.
2. If the ELAP user interface menu item is used to force an ELAP to Standby role, no condition causes it to become Active until the user removes the interface restriction with another menu item.

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 four network connections.

- *DSM Networks*
- *ELAP Sync Network*
- *Dialup PPP Network*
- *Provisioning Network*

This section describes the four 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	192.168.1.100	192.168.1.200
DSM Network B IP Address	192.168.2.100	192.168.2.200

Note: These values are not the correct values for your network! The values that you enter while configuring the ELAPs will be unique to your network configuration. The *Signaling Products Hardware Manual* describes how to determine the actual values for your network.

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. They 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 5 ISS.

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 Configuration and Initialization*).

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 2 ELAPs are connected using Telco switches over 2 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.

Dialup PPP Network

Dialup Point-To-Point Protocol (PPP) Network allows multiple user interface sessions to be established to the ELAP from a remote workstation over a dialup connection with the user's own client.

The MPS servers are configured for the use of a modem located on the Out of Band Message (OOBM) card on server A. The modem connection supports PPP (TCP/IP). With this capability, multiple networked applications can be run across the PPP link at the same time.

The remote dial-in serial port is configured as:

- Hardware flow control (RTS/CTS)
- 38400 bps port speed
- 8-bit data
- No parity

Contact the *Customer Care Center* for assistance in configuring the Dialup PPP Network.

If the remote dial-in serial port is not functional at one EAGLE 5 ISS site, dialing into the remote EAGLE 5 ISS site and connecting back to the functional MPS at the failed EAGLE 5 ISS site allows remote recovery.

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 (for example, LSMS servers) are defined.

If this optional feature uses an LSMS, the LSMS must be configured as an NTP server. Refer to the *LSMS Configuration Manual* for configuration instructions. When the LSMS has been configured, you can configure the MPS servers to synchronize with the LSMS. Refer to *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 Tekelec 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

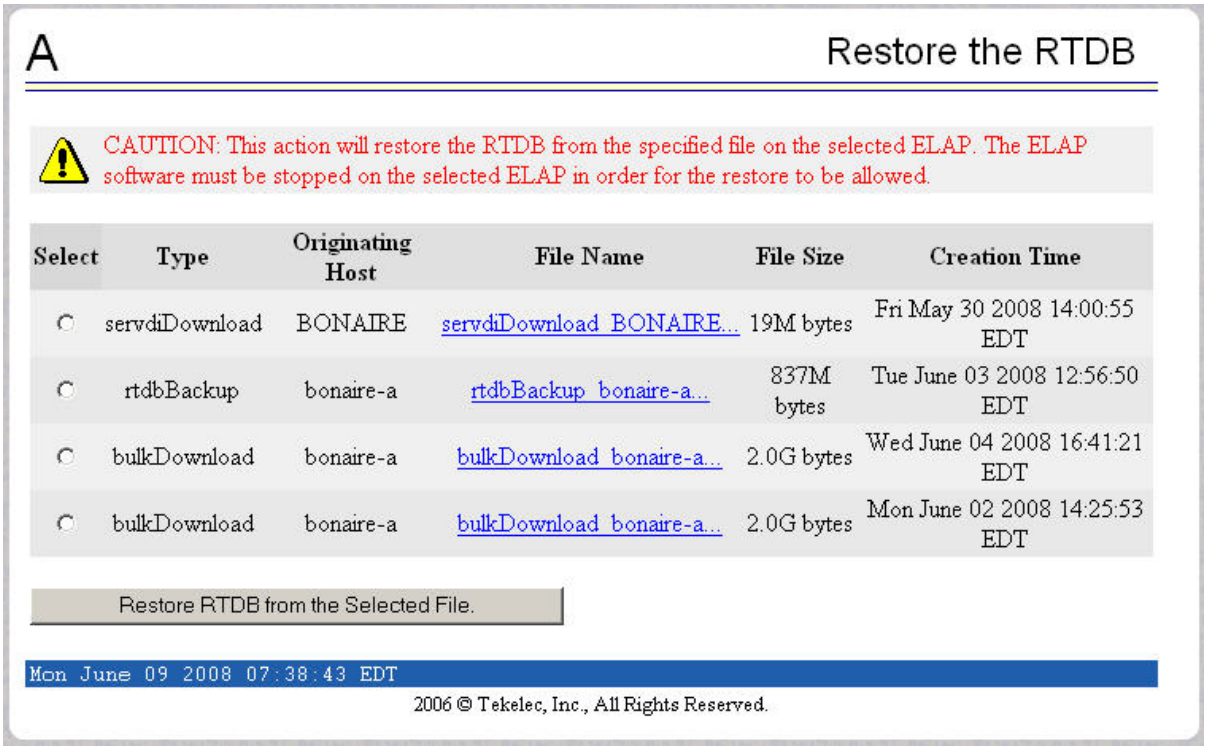
The Support ELAP Reload via Database Image (SERVDI) function performs bulk data downloads (BDD) that significantly reduce the time needed to reload an ELAP database. SERVDI is included with optional LNP feature.

The SERVDI function is executed on the LSMS system and creates an LNP RTDB 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 the *LNP Database Synchronization Manual*.

Note: Although the exchange of ELAPSecure 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 in order for the ELAP to receive bulk downloads from the LSMS (see *Step 17* in *Procedure for Configuring ELAPs*.

See also *Restore RTDB*.

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

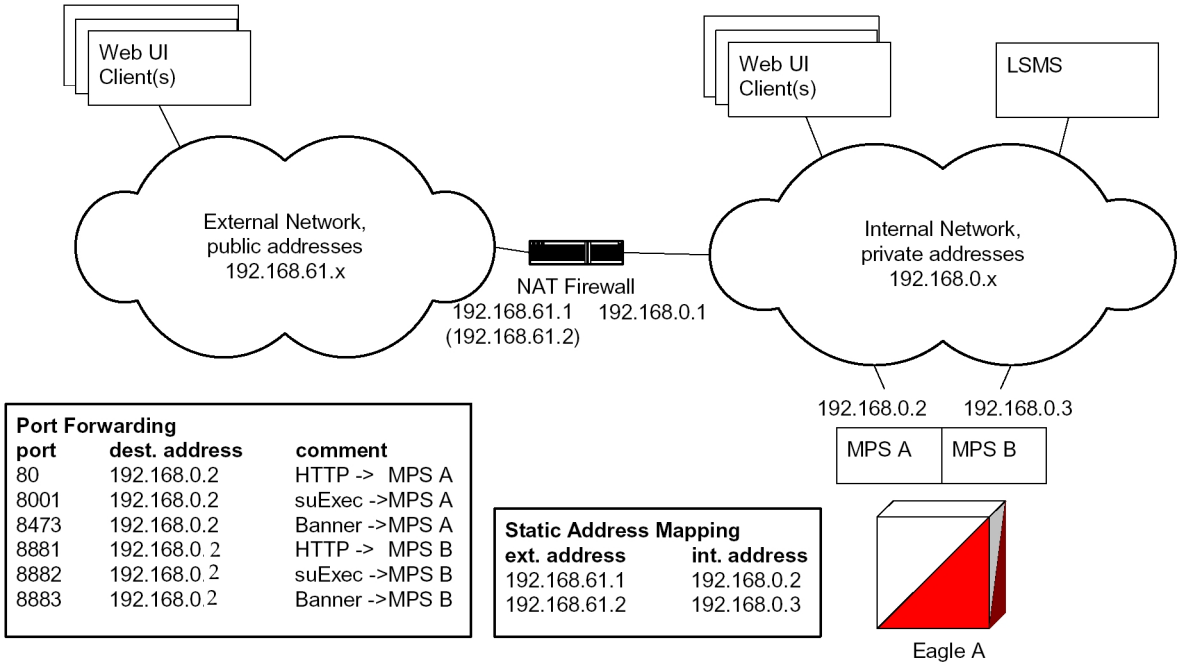
Port Forwarding allows a single external address to be used for multiple internal systems. The Port Forwarding firewall maintains a list of services (basically port numbers) and corresponding internal addresses.

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 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 Enhancements

The ELAP Security Enhancements feature controls 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. This feature also allows 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 Enhancements feature is available through the ELAP GUI and is 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 Enhancement feature 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 Enhancement also provides the means to enable/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 *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 5 ISS Service Module cards using the main (and backup if necessary) DSM network between the MPS system and the EAGLE 5 ISS Service Module cards. Real-time updates are sent to the EAGLE 5 ISS Service Module cards in parallel using RMTP multicast technology.

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

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. Refer to the *LNP Feature Activation Guide* for more information on minimum requirements.

Note: The LNP feature does not support measurement collection performed by theOAM.LNP measurement collection is disabled on the OAM when any Service Module card is loaded from anELAP with the LNP feature.

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.

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 25 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 RMTP channel from the provisioning and incremental update streams. This allows Service Module card multicast hardware to filter out the high volume of reload traffic from Service Module cards that do not require it.

Continuous Reload

The ELAP handles reloading of multiple Service Module cards from different starting points. Reload begins when the first Service Module card requires it. Records are read sequentially from the Real Time database (RTDB) from an arbitrary starting point, wrapping back to the beginning. If another Service Module card requires reloading at this time, it uses the existing record stream and notifies the Service Module card provisioning task of the first record it read. This continues until all Service Module cards are satisfied.

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.

ELAP User Interface Menus

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

ELAP Graphical User Interface describes how to log into the interface 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

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 5 ISS for every inconsistent Service Module card. The EAGLE 5 ISS 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	Minor	RTDB database is inconsistent	`card`

EAGLE 5 ISS 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 though 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 5 ISS 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

Status Reporting and Alarms

The MPS systems and ELAPs have no direct means of displaying output messages on EAGLE 5 ISS 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. Static information is exchanged across this interface at initialization, and dynamic information is exchanged on occurrence.

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 ISS `rept-stat-mps` command (see *Commands*).

The alarm reporting mechanism and various alarm messages are described in *Messages, Alarms, and Status Reporting*.

Chapter 3

ELAP Graphical User Interface

Topics:

This chapter describes how to log into the ELAP user interface and how to use the ELAP user interface menus. See also *ELAP Software Configuration*.

Overview of the ELAP User Interfaces

The EAGLE LNP Application Processor (ELAP) User Interface, consists of two user interfaces:

- The Graphical User Interface provides GUI menus that maintain, debug, and operate the platform; it and its associated error messages are described in this chapter.
- The text-based User Interface has a Configuration menu that performs the ELAP configuration and initialization; it is described in *ELAP Software Configuration*.

The GUI provides the user with menus and screens to perform routine operations. The text-based user interface provides the ELAP Configuration menu to perform the initial configuration.

To communicate with the ELAP graphical user interface, you use a PC with a network connection and a network browser. For information about using the ELAP GUI, see *ELAP Graphical User Interface*

To configure ELAP, you use the ELAP text-based user interface. For information about configuring the ELAP and how to set up its PC workstation, refer to *ELAP Software Configuration*.

ELAP Graphical User Interface

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 5.0 or later, and on Mozilla Firefox, version 1.0.2 or later.

When using Firefox, you might encounter this message upon 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.

The graphical user interface pages have three different sections:

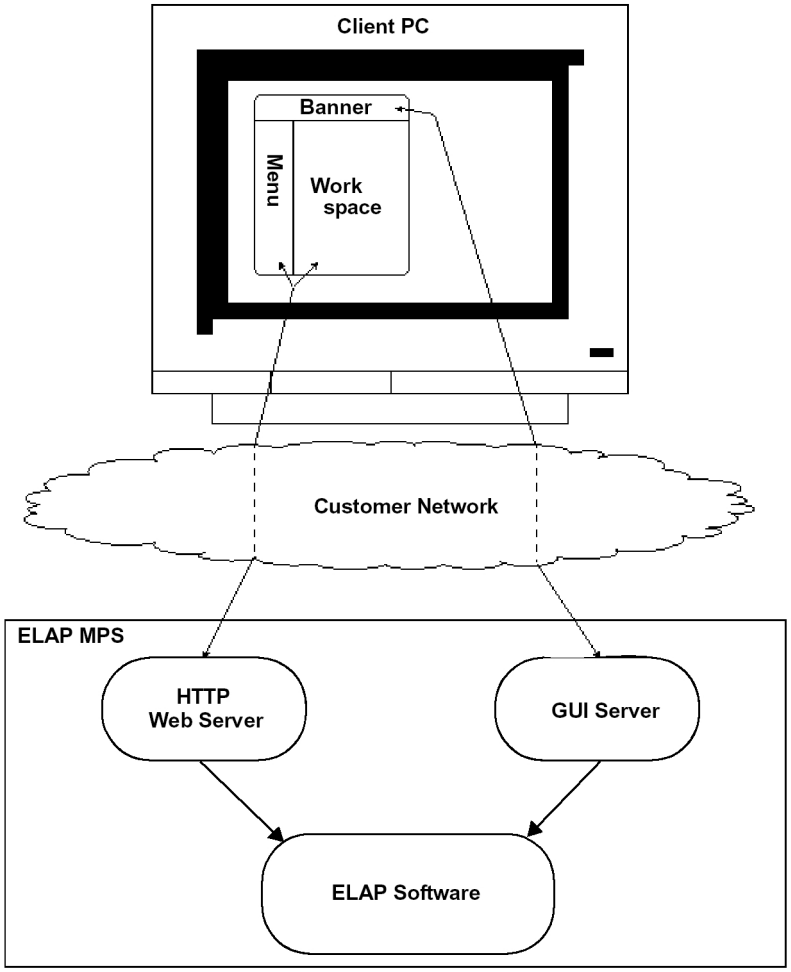
- A banner header section for displaying the real-time status of the MPS servers
- A menu section for selecting desired actions
- A work area section for entering requested information and displaying results.

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.

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



This section describes the various screens, screen structure and layouts, and input prompts of the ELAP 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 user interface.

Login Screen

The first screen in the ELAP Internet interface 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 UI, 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 5 ISS 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 Administration), terminated by the administrator, and by selecting another window on another independent browser.

ELAP GUI Main Screen

The ELAP graphical user interface 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 graphical user interface 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.

Figure 5: ELAP Banner Applet

The banner applet contains five information areas:

- *Busy Icon*
- *ELAP Host Addresses*
- *ELAP Alarm Information Area*
- *LSMS Connection Status*
- *Service Module Card Status*

Busy Icon

The Tekelec company logo is located at the top left of the banner applet and performs as the busy icon. Its serves as an indicator of activity in progress. When a menu action is being executed, the Tekelec icon rotates; when the action ends, the icon is at rest.

ELAP Host Addresses

The ELAP host addresses area of the ELAP banner applet provides address connection information for:

- HA ELAP Pair VIP address
- ELAP A server provisioning IP address connection

- ELAP B server provisioning IP address connection

The LEDs provide the following information:

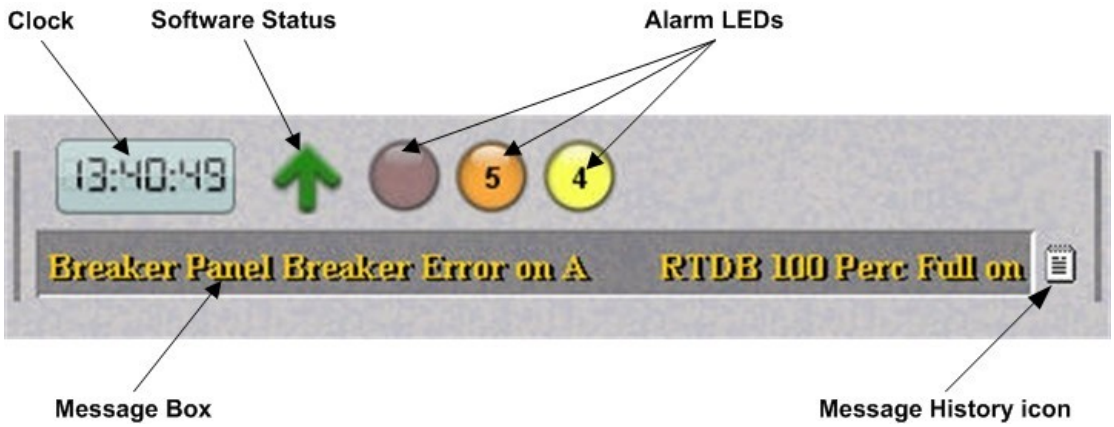
- Green - ELAP is connected
- Yellow with red triangle - ELAP is inhibited
- A - Active ELAP
- S - Standby ELAP

Clicking on an ELAP IP address toggles between the ELAP IP address and the ELAP host name(s).

ELAP Alarm Information Area

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

Figure 6: 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 6: 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):

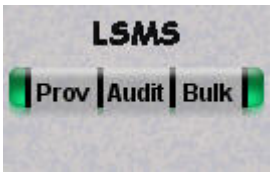
- LSMS provisioning indicator (enabled/disabled)
- LSMS provisioning connection status indicator (connected/unconnected/listening/unknown)
- LSMS audit connection status indicator (connected/unconnected/listening/unknown)
- LSMS bulk download connection status indicator (connected/unconnected/listening/unknown)
- 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 7: 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 5 ISS.

Figure 8: Service Module Card Status

The color of the card slots indicates:

- Grey - unknown card state

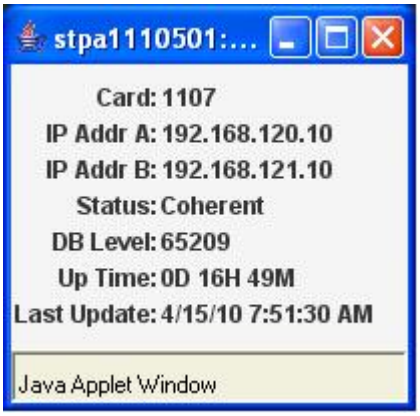
  Booting
  Inhibited card
  Previously provisioned slot with undetectable card

- 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.

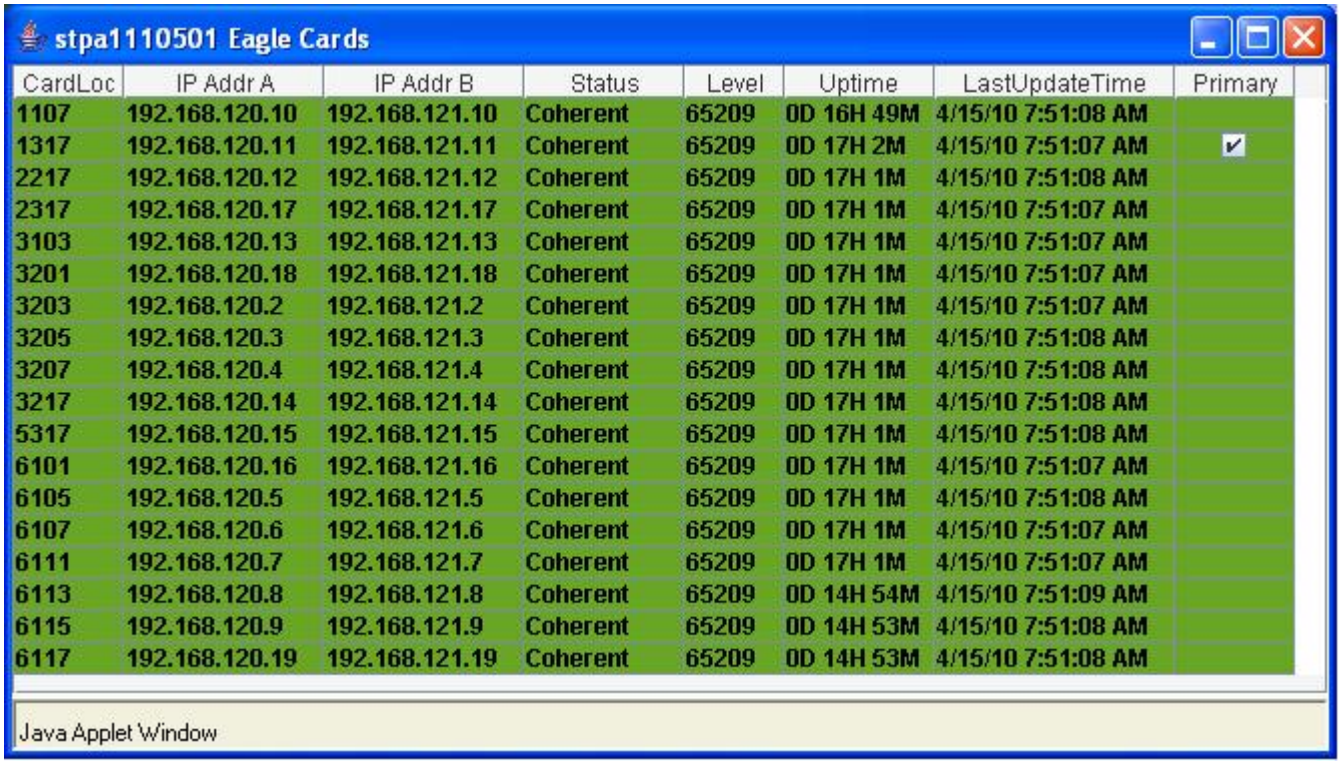
Clicking on the a card slot icon provides information on that Service Module card:

Figure 9: Status of an Individual Card



Clicking on the **Service Module Card Status Information** icon displays all 18 Service Module Card slots on the EAGLE 5 ISS and information about installed cards:

Figure 10: 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 Tekelec copyright notice appears.

Workspace Section Syntax Checking

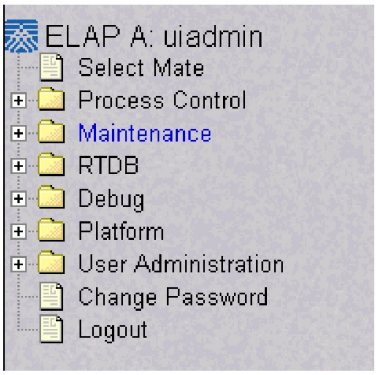
The web browser user interface uses layers of syntax checking to validate user input for text-entry fields.

- 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 menu is the main menu of the ELAP application. It provides the functions of the ELAP User Interface. *Figure 11: ELAP Menu* shows the ELAP main menu.

Figure 11: ELAP Menu



The ELAP menu provides three actions common to all users, Select Mate, Change Password, and Logout. All 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.

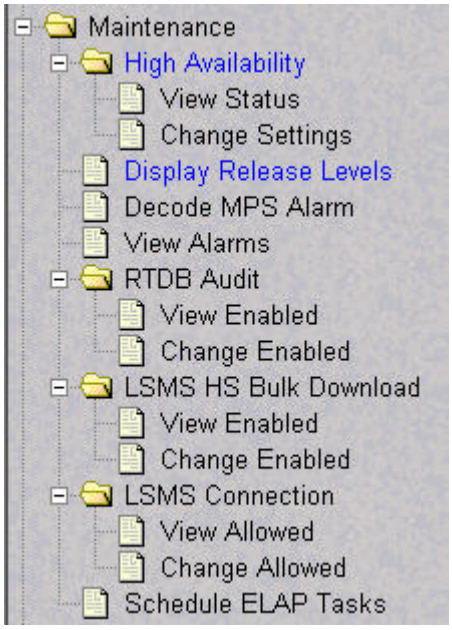
Stop ELAP Software

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 12: Maintenance Menu



- *High Availability Menu*
- *Display Release Levels Screen*
- *Decode EAGLE 5 ISS MPS Alarm Screen*
- *View Alarms Menu*
- *RTDB Audit Menu*
- *LSMS High Speed Bulk Download Menu*
- *LSMS Connection Menu*
- *Schedule ELAP Tasks Menu*

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

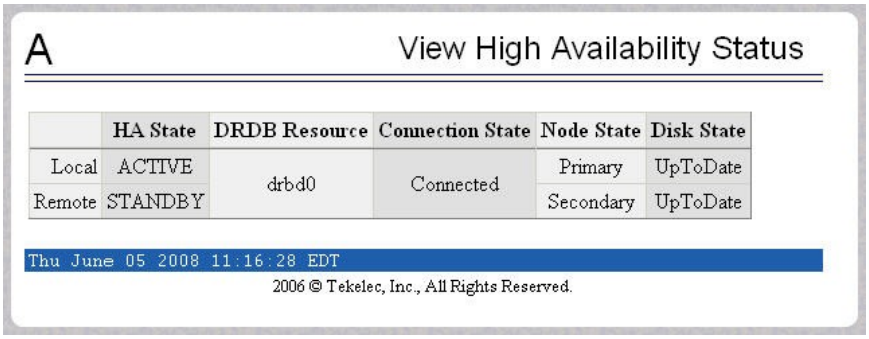
- Node State

  Primary
  Secondary
  Unknown

- Disk State

  Up to Date
  Diskless
  DUknown

Figure 13: 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 5 ISS MPS Alarm Screen

The Maintenance / Decode EAGLE 5 ISS MPS Alarm menu selection lets the user decode the EAGLE 5 ISS output of MPS alarms. The user enters the 16-character hexadecimal string from the EAGLE 5 ISS `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 is in the *MPS Platform Software and Maintenance Manual - T1100*.

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.

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.

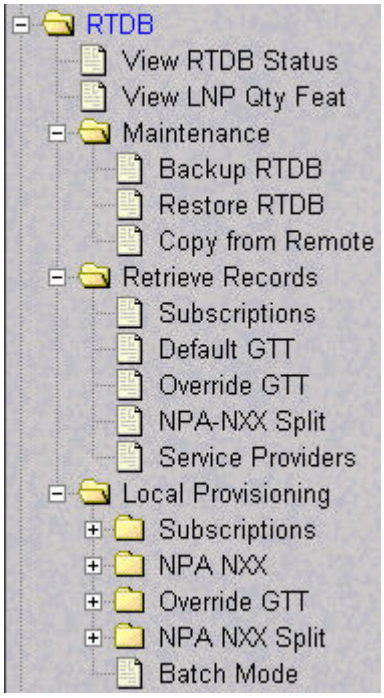
Schedule ELAP Tasks Menu

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

RTDB Menu

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

Figure 14: 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, DGTTs, 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.

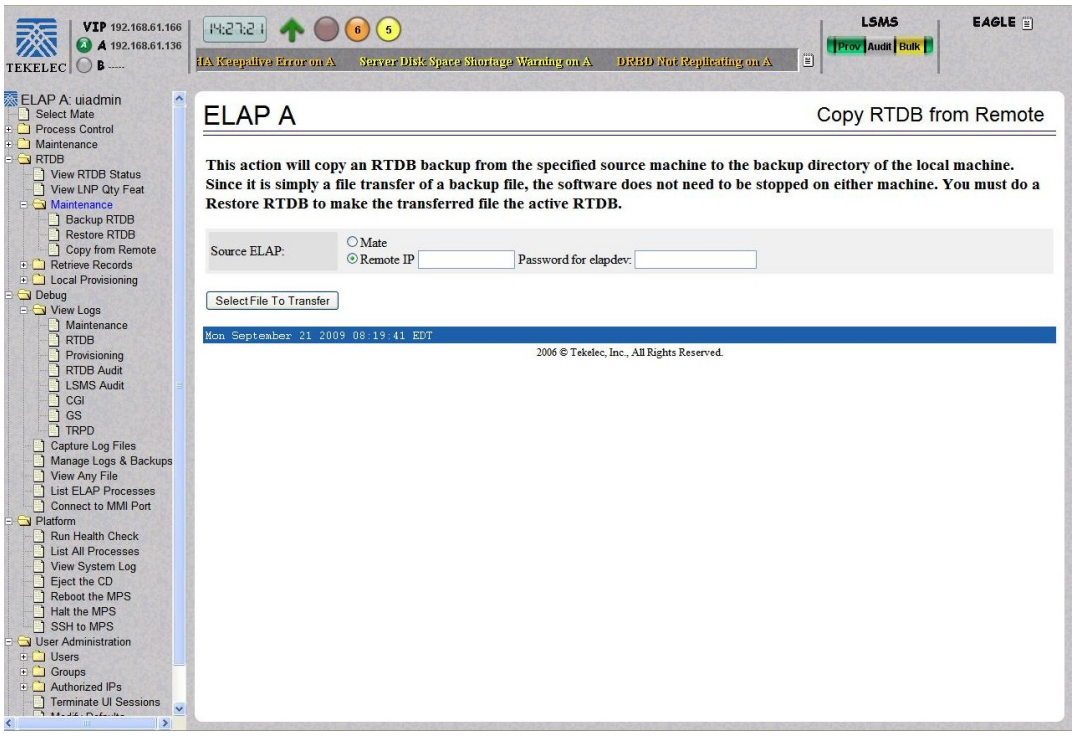
Note: For information on restoring the RTDB from a backup file, see the *Tekelec 1100 AS MPS Platform Software and Maintenance Manual* .

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, enter the remote box's IP address and a password for the "elapdev" user ID in the fields shown in *Figure 15: Copy RTDB from Remote Screen*.

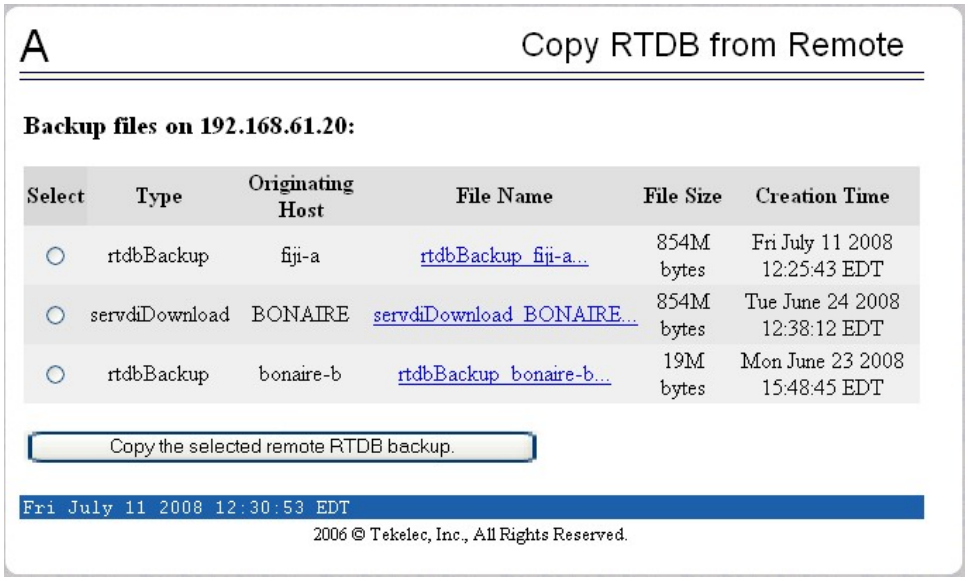
Figure 15: Copy RTDB from Remote Screen



Then, click the **Select File To Transfer** button.

Select the appropriate file from the screen that is displayed, as shown in *Figure 16: Copy RTDB from Remote Selection*. Then, click the **Copy the selected remote RTDB backup** button.

Figure 16: Copy RTDB from Remote Selection



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 NPA NXX 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.

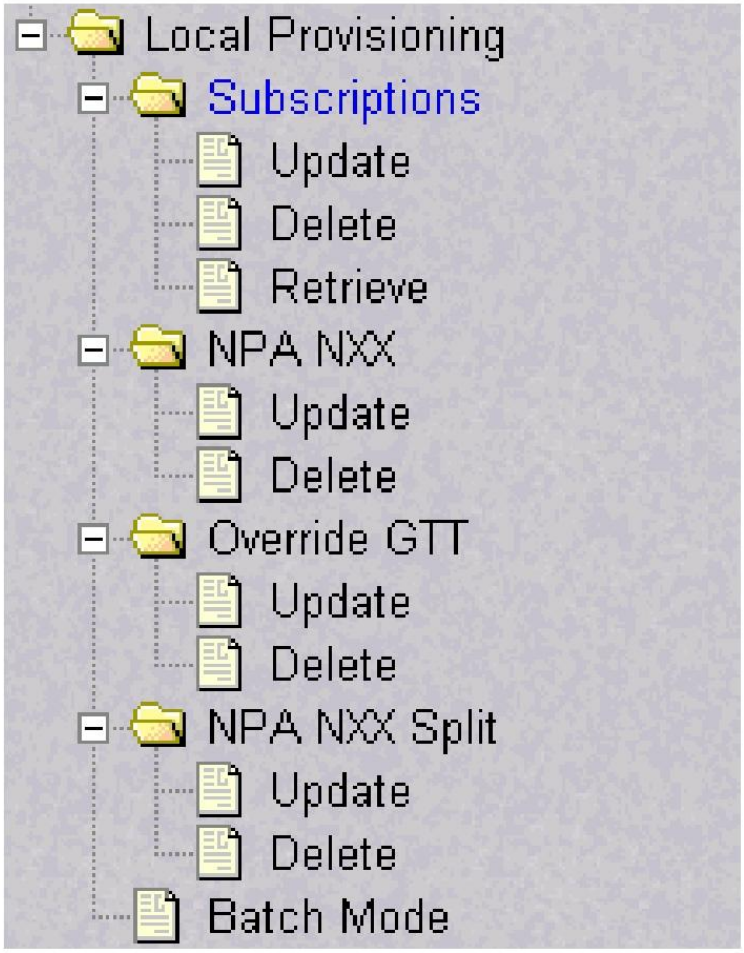
Enter the number in the **Service Provider ID** field, and click the **Retrieve** button.

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 17: 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).

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.

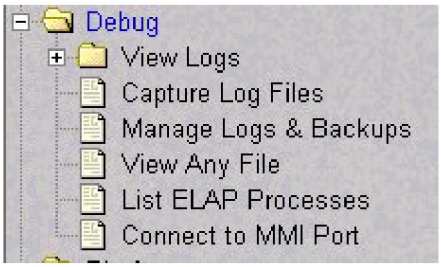
Batch Mode

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 18: Debug Menu



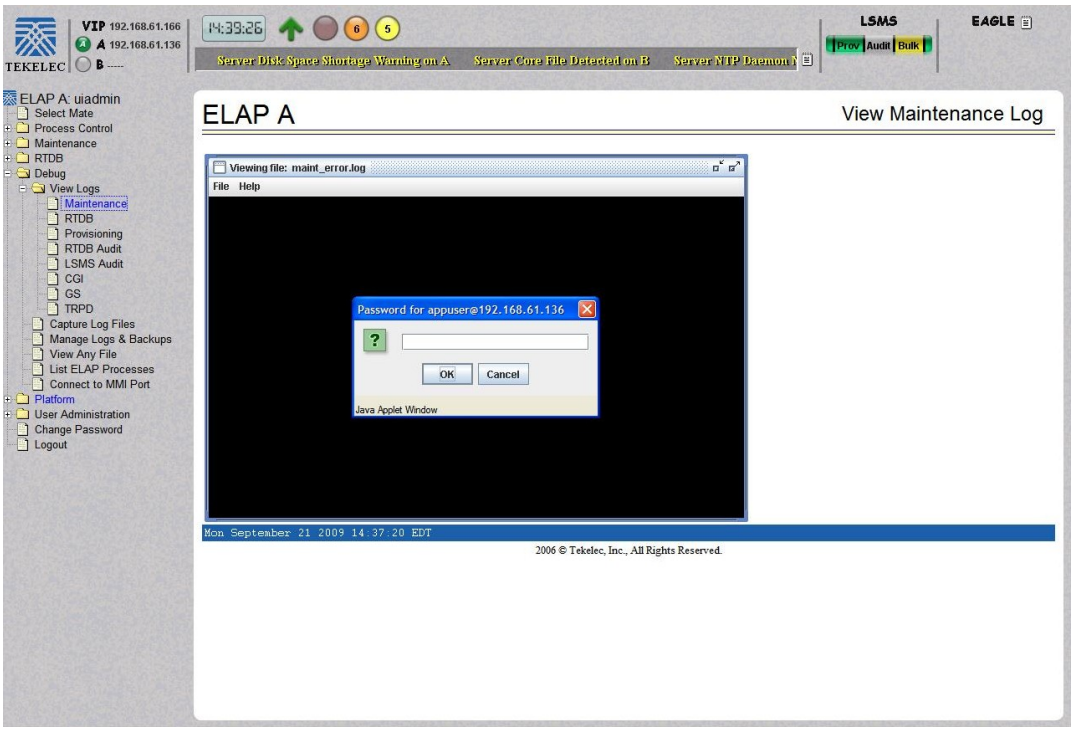
The Debug menu provides these actions:

- *View Logs Menu*
- *Capture Log Files*
- *Manage Logs and Backups*
- *View Any File*
- *List ELAP Software Processes*
- *Connect to EAGLE 5 ISS 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 19: View Maintenance Log Password Screen*.

Figure 19: 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.

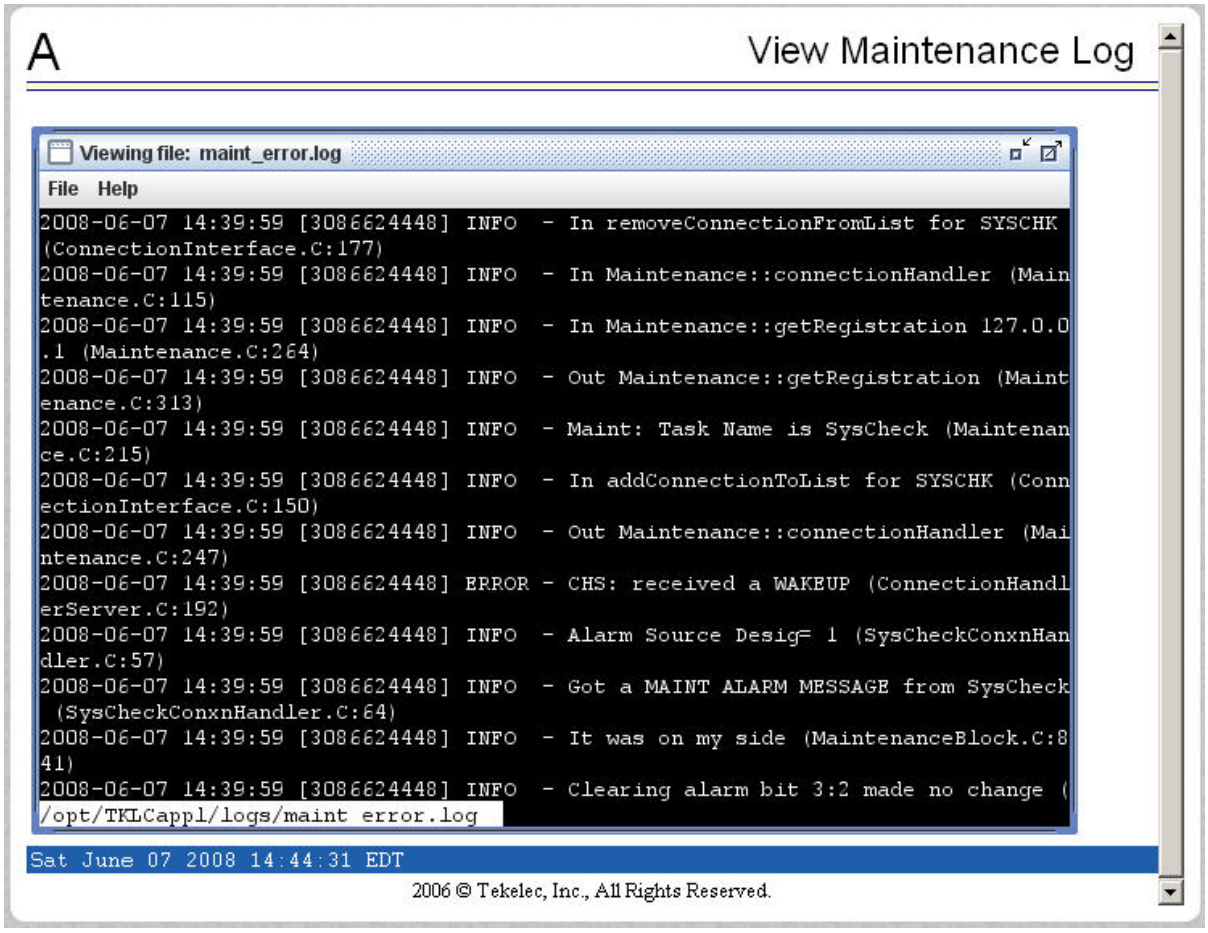
After logging in, the following View Logs menu options are available:

- Maintenance Log
- RTDB Log
- Provisioning Log
- RTDB Audit Log
- LSMS Audit Log

- CGI Log
- GS Log
- TRPD Log

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 20: View Maintenance Log Screen*, to appear.

Figure 20: View Maintenance Log Screen



Use the navigation commands in *Table 8: Navigation Commands* to navigate through the displayed file.

Table 8: Navigation Commands

Command	Action
<return>	Scroll down 1 line
<space>	Scroll down 1 page
b	Scroll up 1 page

Command	Action
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

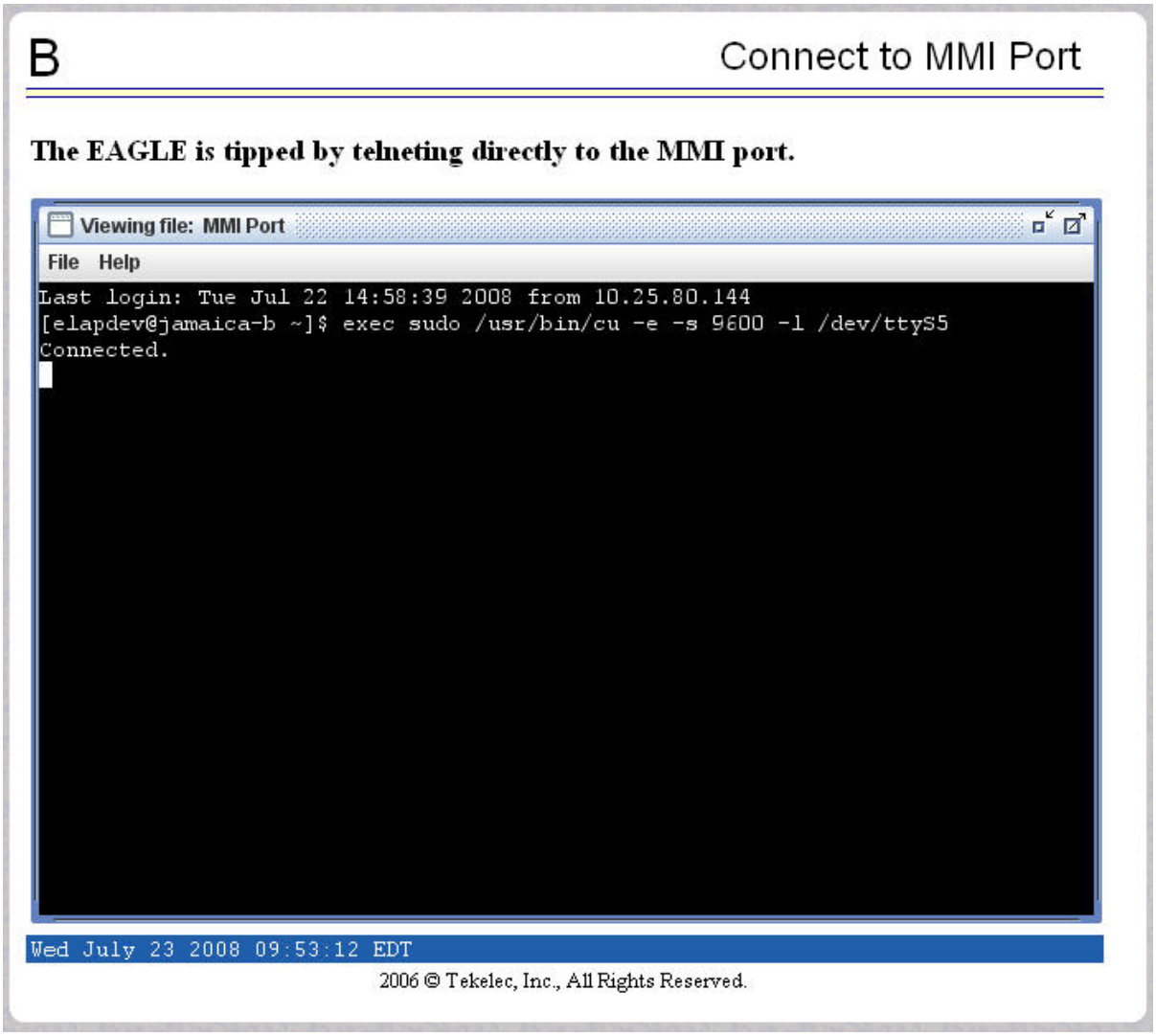
The Debug / List ELAP Software Processes screen shows the ELAP processes started when the ELAP boots or when the "Start ELAP software" prompt is used. The `/usr/ucb/ps -auxw` command generates this list. (The operating system's manual page for the ps command thoroughly defines the output for this command.).

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 5 ISS MMI Port

The Debug / Connect to EAGLE 5 ISS MMI Port screen lets the user connect to the EAGLE 5 ISS using an MMI port. This connection can only be made from ELAP B. See the *Commands Manual* for a detailed listing of EAGLE 5 ISS commands and the input and output from the EAGLE 5 ISS MMI port.

Figure 21: Connect to MMI Port Screen



This menu option opens a window and starts a SSH session allowing where EAGLE 5 ISS 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, back ups, upgrades, shut downs, etc., shown in Platform Menu.

Figure 22: Platform Menu

The Platform menu provides these actions:

- *Run Health Check Screen*
- *List All Running Processes*
- *View System Log*
- *Eject the CD*
- *Reboot the MPS*
- *Halt the MPS*
- *SSH to MPS*

Run Health Check Screen

The Platform / Run Health Check screen allows the user to execute the health check routine on the selected ELAP. The *Tekelec 1100* AS MPS *Platform Software and Maintenance Manual* describes the health check (also called system health check and syscheck) in detail.

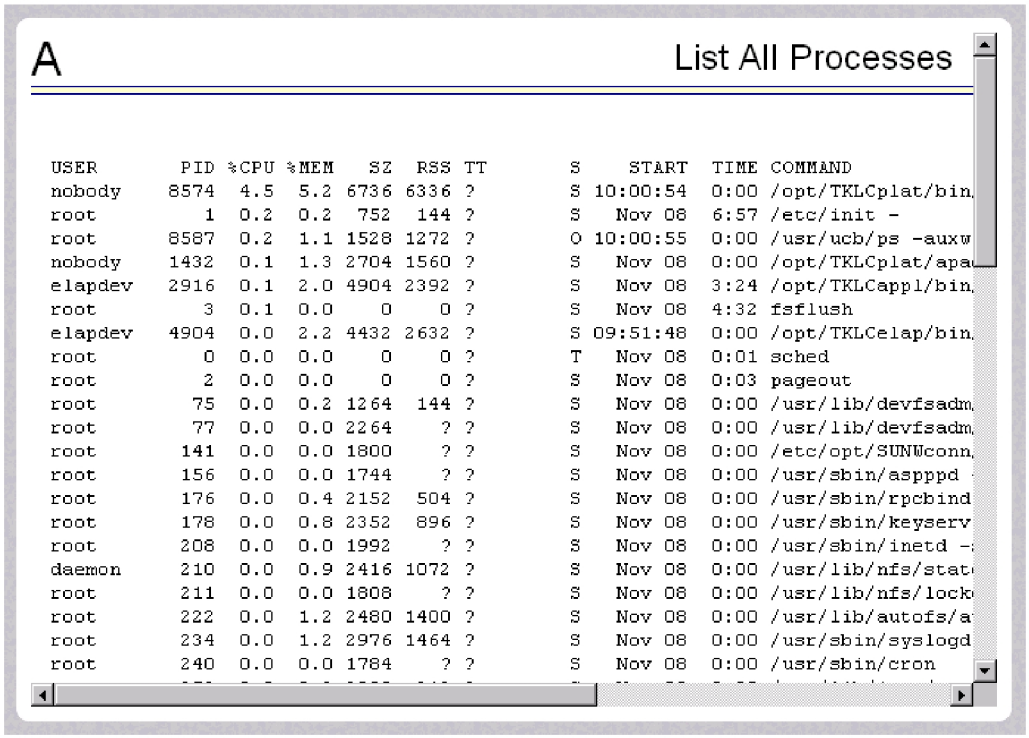
The first screen presented in the workspace frame lets the user select the “normal” or “verbose” mode of output detail.

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 the *Tekelec 1100* AS MPS *Platform Software and Maintenance Manual* 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 23: List All Running Processes Screen* shows an example of the process list.

Figure 23: List All Running Processes Screen



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.

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.

Eject the CD

The Platform / Eject the CD screen allows the to user to eject the CD on the selected CD device on the selected ELAP server.

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.

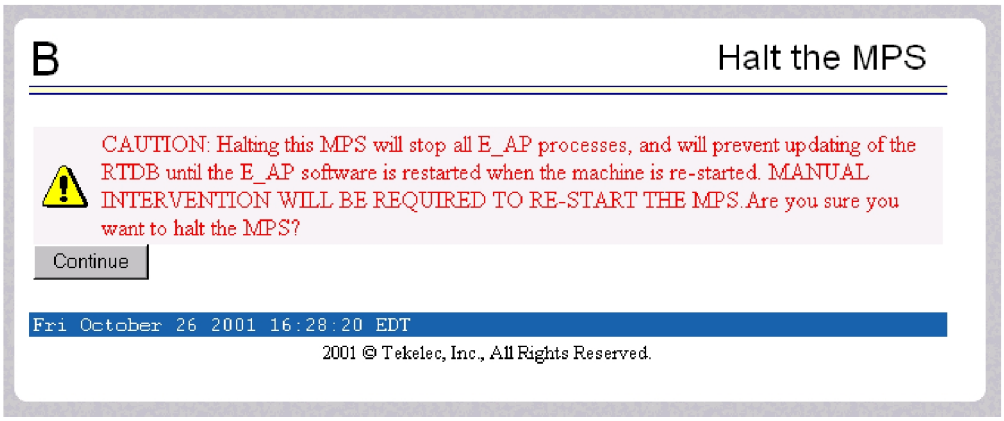
When you are certain that you want to reboot, click the **Continue** button. Another screen informs you that MPS is being rebooted and that the User Interface will be reconnected when the reboot is completed.

Halt the MPS

The Platform / Halt the MPS screen allows the user to halt the selected ELAP. All ELAP software processes running on the selected ELAP are shut down normally. Initially, a Caution screen will display. Confirmation is required to halt the MPS.

To perform this action, click the **halt_MPS** button. Next 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. See *Figure 24: Caution about Halting the MPS*.

Figure 24: Caution about Halting the MPS



To halt the MPS, click the **Continue** button. Another screen informs you that MPS is being halted and that the process may require up to 50 seconds.

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**.

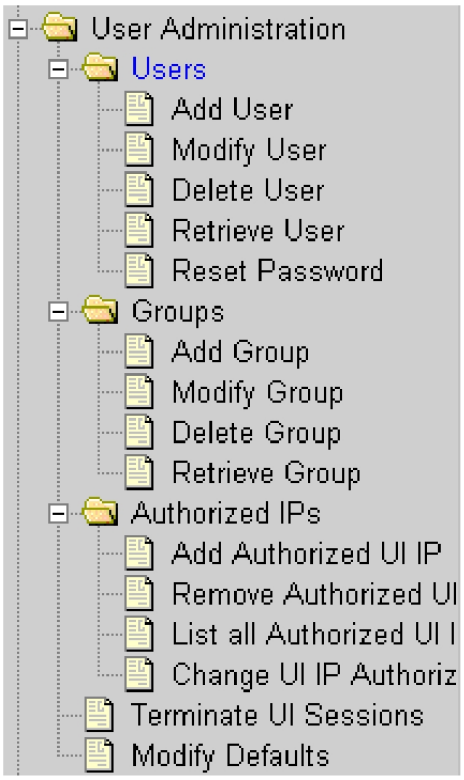
A **Warning** dialog displays allowing the user to confirm the SSH connection to the specified MPS.

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 25: 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 configurablnumber, 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 existe on the text-based UI. In addition, The default password for a new `uiadmin` is `uiadmin`. See *Table 9: ELAP UI Logins* for login names.

Table 9: ELAP UI Logins

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

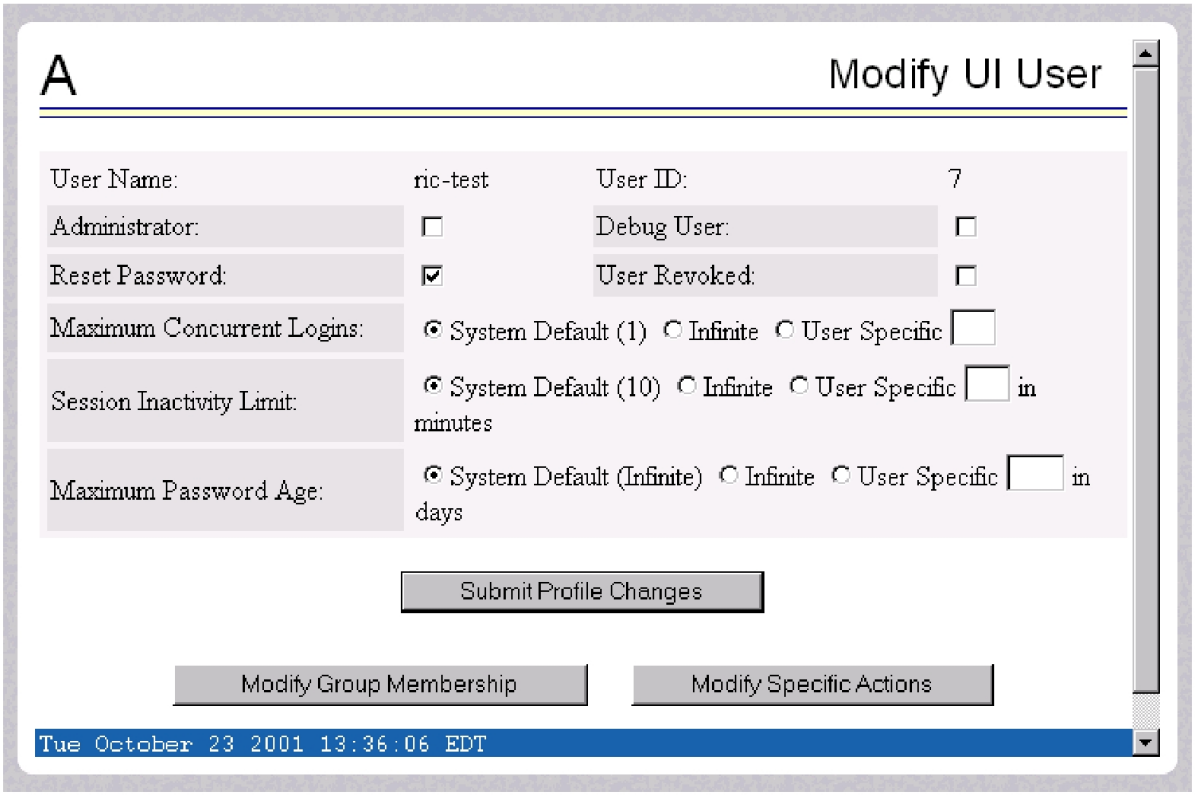
- *User Permissions*
- *User Group Memberships*
- *User Action Privileges*

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 26: 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.

Figure 26: 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 26: 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 26: 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.

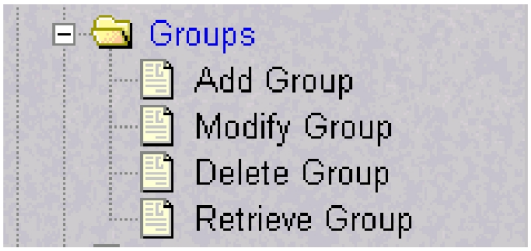
Reset User Password

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 27: 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 30: 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

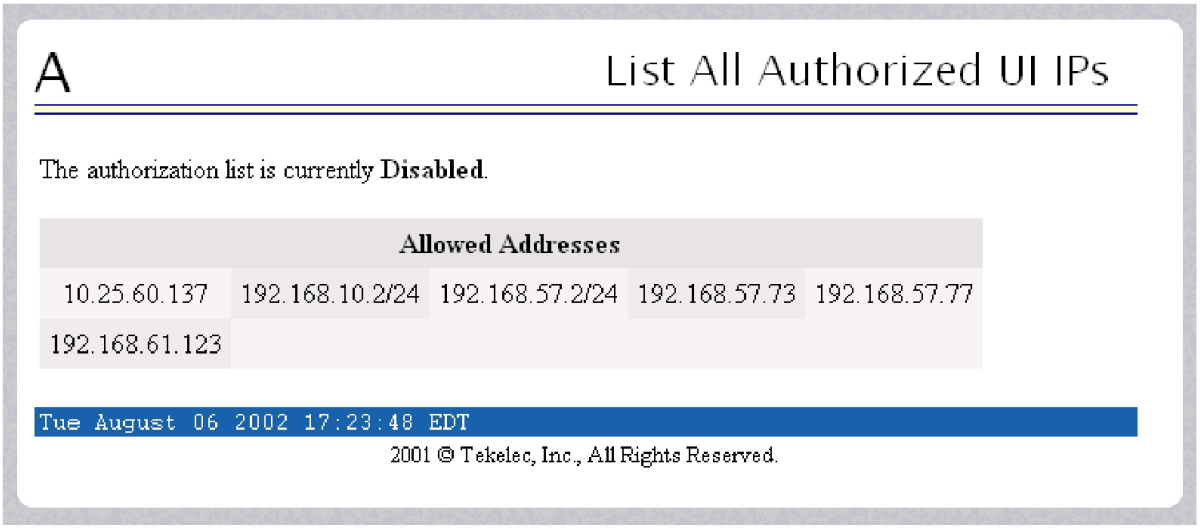
The User Administration / Authorized IP / Remove Authorized UI IP screen lets the user remove an IP address from the list of authorized IP addresses. Enter the individual IP address or Classless Interdomain Routing Format (CIDR) IP format in the **IP to Remove** field.

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 28: List All Authorized UI IP Addresses Screen* for an example of the List All Authorized UI IP address screen.

Figure 28: 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.

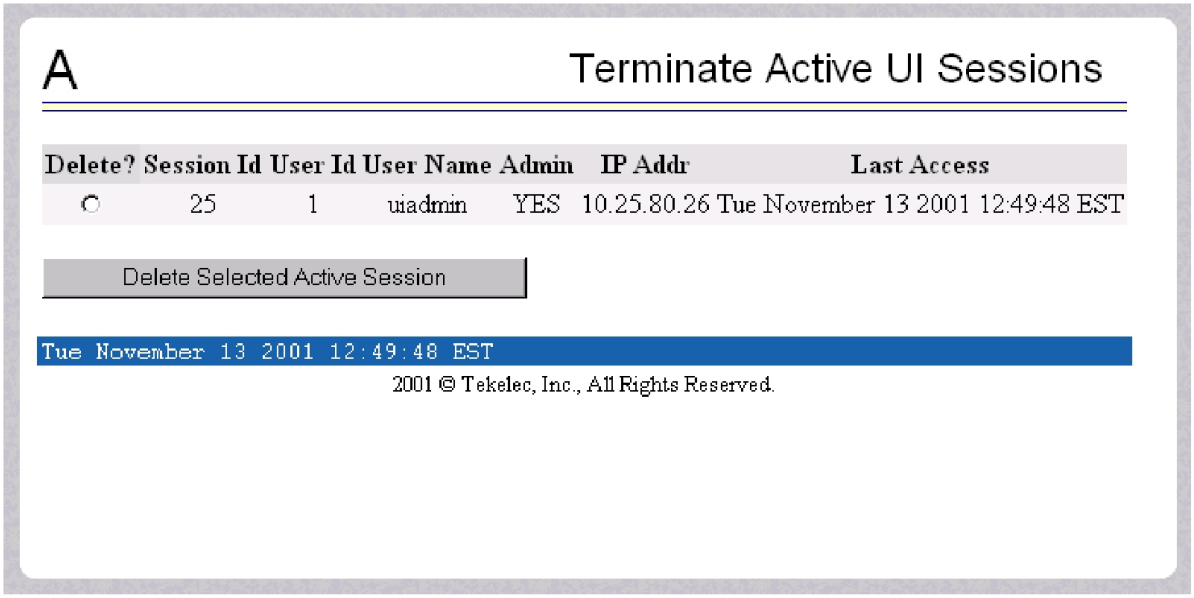
If the authorization state is 'NOT Enabled’, click the **Enable IP Checking** button to toggle the state to 'Enabled'.

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 29: Terminate Active Sessions Screen*.

Figure 29: Terminate Active Sessions Screen

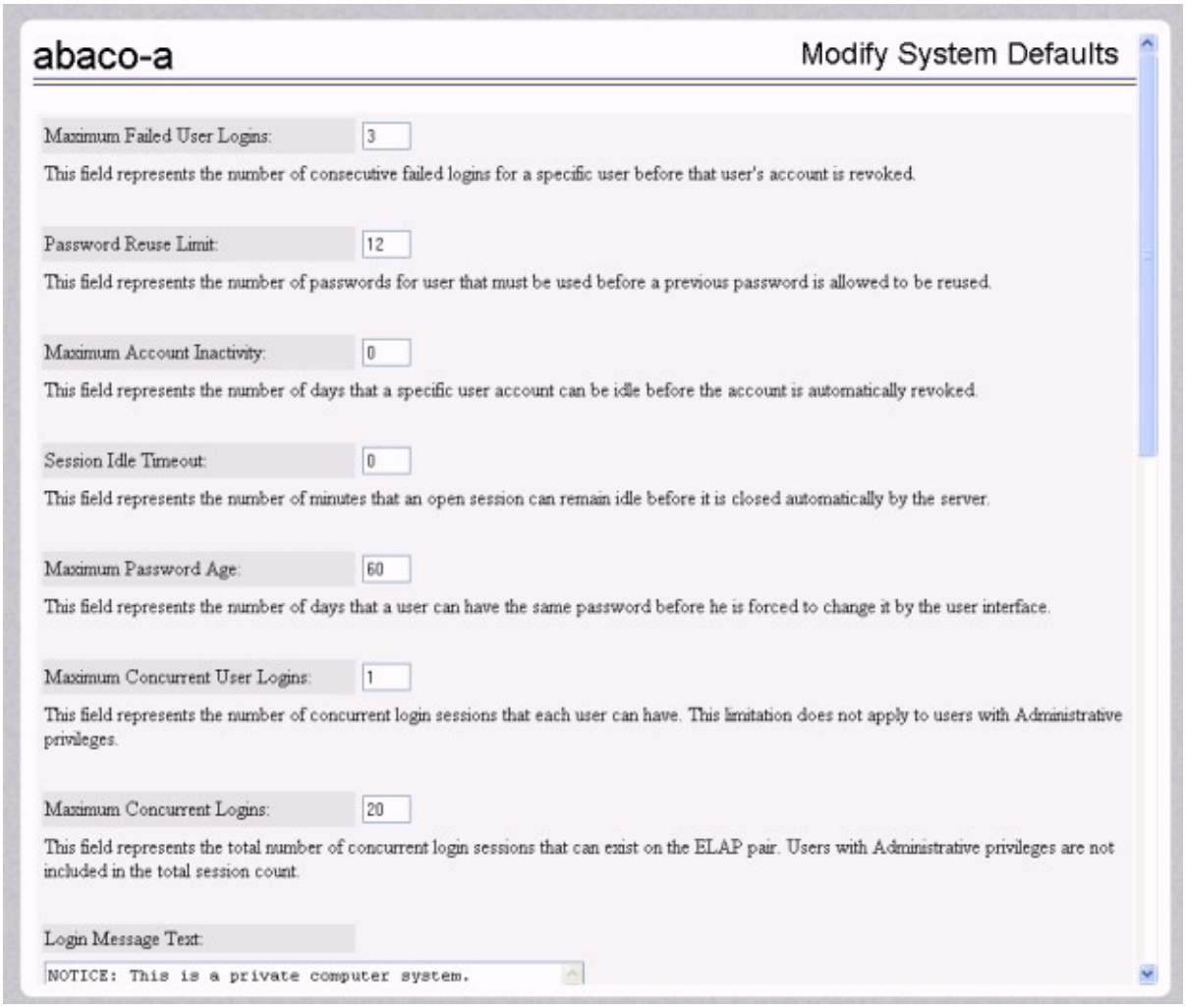


Select a user interface session for termination, by clicking in the **Delete?** column. A message confirming a successful termination appears.

Modify System Defaults

The User Administration / Modify System Defaults screen allows the administrator to manage the systems defaults. See *Figure 30: Modify System Defaults Screen*.

Figure 30: 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 maximum number of days that a user account can be idle before the account is automatically revoked.
- **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.

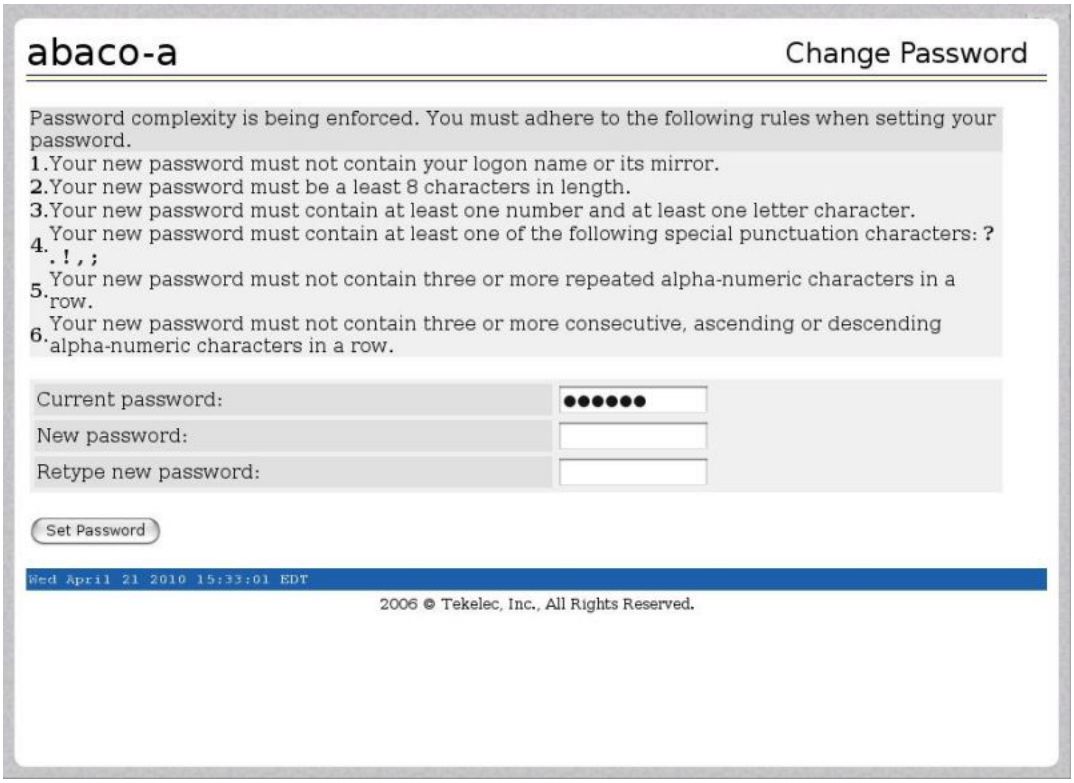
When the changes to the system defaults are complete, click the **Submit Defaults** button. A message confirming a successful change appears.

Change Password

The Change Password menu selection provides you, the ELAP user, with a screen to change your password. This basic action is available to all users and is accessible from the *ELAP GUI Menus*.

To change the password, you must enter the current password, enter the new password, and retype the new password. Click the **Set Password** button, as shown in *Figure 31: Change Password Screen*.

Figure 31: 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 appears. Click the **Logout** button to complete the logout.

When logout is complete, the Tekelec ELAP UI Login screen appears.

ELAP Messages

ELAP Error Messages

Table 10: 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 10: 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*>
E1023	Invalid value for <*prompt* >: <*value*>: Valid values are <*range*>. Hit the Escape key to abort the command.

E1025	File lock failed: <*file name*>
E1032	Operation aborted by user.
E1035	Script <*script name*> failed: status=<*status*>
E1037	One or more ELAP software processes did not start
E1038	One or more ELAP software processes did not stop
E1054	Another user is currently performing this same action.
E1055	Missing mandatory parameter: <*parameter*>
E1056	Unexpected parameter was provided:<*parameter*>
E1058	An internal error in the <*parameter*> occurred: <*error text*>
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.
E1065	<*device or process*> must be configured.
E1066	The requested user <*user*> was not found.
E1067	The requested group <*group*> 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: <*reason text*>
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 <number> bytes of allocated storage space.
E1074	LPU batch failure: <error text>
E1078	File '<file name>' was empty
E1081	The specified IP already exists.
E1082	The specified IP does not exist.
E1083	The maximum number of authorized UI IPs has been reached.

ELAP Banner Information Messages

Table 11: ELAP Informational Banner Messages lists the banner information messages that appear on the UI browser screen in the banner message box. These messages, sometimes referred to as ‘scroll by” messages, indicate the status of the ELAP machines.

Table 11: ELAP Informational Banner Messages

Attempt to correct MySQL replication failed
Backup Filesystem Failed
Backup filesystem in progress
Backup filesystem successful
Backup filesystem was aborted manually
Backup RTDB completed successfully
Backup RTDB failed
Backup RTDB in progress
Failure within filesystem backup utility. View backup_fs.fail log.
MPS Reboot in Progress
MPS Resynchronization in Progress

Reload RTDB from <source> completed successfully
Reload RTDB from <source> failed
Reload RTDB from <source> in progress
Restore RTDB completed successfully
Restore RTDB failed
Restore RTDB in progress
Transaction log export failed: <reason>
Transaction log export in progress
Transaction log successfully exported to file: <file>

Table 12: ELAP Alarm Related Banner Messages lists the alarm related banner information messages that appear on the UI browser screen in the Message Box described. If any of the following alarm related messages appear, refer to the *Tekelec 1100 AS MPS Platform Software and Maintenance Manual* for the related corrective procedure.

Table 12: ELAP Alarm Related Banner Messages

LVM Snapshot Detected that is Too Old
LVM Snapshot Detected that is Too Full
LVM Snapshot Detected with Invalid Attributes
DRBD Split Brain
Uncorrectable ECC Memory Error
LSMS DB Maintenance Required
Server Fan Failure
Server Internal Disk Error
Server RAID Disk Error
Server Platform Error
Server File System Error

Server Platform Process Error
Server Swap Space Shortage Failure
Server Provisioning Network Error
Server Eagle Network A Error
Server Eagle Network B Error
Server Sync Network Error
Server Disk Space Shortage Error
Server Default Route Network Error
Server Temperature Error
Server Mainboard Voltage Error
Server Power Feed Error
Server Disk Health Test Error
Server Disk Unavailable Error
Correctable ECC Memory Error
Server Power Supply 1 Error
Server Power Supply 2 Error
Breaker Panel Feed Error
Breaker Panel Breaker Error
Breaker Panel Monitoring Error
Mate ELAP Unavailable
Congestion
File System Full

Log Failure
Fatal Software Error
RTDB Corrupt
RTDB Inconsistent
RTDB Incoherent
Transaction Log Full
RTDB 100% Full
RTDB Resynchronization in Progress
RTDB Reload Is Required
RTDB DSM Over-Allocation
Server Disk Space Shortage Warning
Server Application Process Error
Server Hardware Configuration Error
Server RAM Shortage Warning
Server Swap Space Shortage Warning
Server Default Router Not Defined
Server Temperature Warning
Server Core File Detected
Server NTP Daemon Not Synchronized
Server CMOS Battery Voltage Low
Server Disk Self Test Warning
Server Reboot Watchdog Initiated

RTDB 80% Full

Chapter 4

Messages, Alarms, and Status Reporting

Topics:

This chapter describes ELAP status reporting, alarms, and error messages.

MPS and ELAP Status and Alarm Reporting

The System Health Check (syscheck) utility runs automatically at least every five minutes, and can be run manually, to test for error conditions in each MPS Server and in each ELAP. See *Run Health Check Screen* and refer to the *Tekelec 1100* AS MPS *Platform Software and Maintenance Manual* for more information about executing and viewing results from the System Health Check.

Alarms of minor, major, and critical levels of severity are reported for error conditions detected for the MPS hardware platform and for the ELAP application.

On the MPS, a critical alarm lights the Fault LED, a major alarm lights the Alarm 1 LED, and a minor alarm lights the Alarm 2 LED. If more than one alarm level is active, all applicable LED lights are illuminated (not just the most severe) until all alarms in that level are cleared.

Maintenance Blocks

MPS and ELAP have no direct means of accepting user input from or displaying output messages on EAGLE 5 ISS terminals. Maintenance, measurements, error, and status information are routed to the EAGLE 5 ISS through the primary Service Module card.

The Active ELAP generates and sends Maintenance Blocks to 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 5 ISS `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 the *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 5 ISS Alarm Reporting

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 5 ISS. The information that is transferred is described in the *Tekelec 1100 AS/MPS Platform Software and Maintenance Manual*.

Table 13: EAGLE 5 ISS MPS Application and Platforms UAM Alarms defines the application and platform alarms that are forwarded to the EAGLE 5 ISS. The EAGLE 5 ISS receives the alarm number, alarm text, and alarm data string recovered from the MPS/ELAP.

Table 13: EAGLE 5 ISS 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

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

When the ELAP needs to know the status of a Service Module card, it can send a Service Module card Status Request to that Service Module card. Because status messages are sent over UDP, the ELAP broadcasts the Service Module card Status Request and all Service Module cards return their status.

Service Module Card Status Reporting to the ELAP

The ELAP needs to know the current status of various aspects of the Service Module cards. Accordingly, the Service Module card sends a Service Module card status message to the ELAP when the following events occur:

- When the Service Module card is booted
- When the Service Module card receives a Service Module card Status Request message from the ELAP
- When the Service Module card determines that it needs to download the entire database

  For example, the database could become totally corrupted, or a user could initialize the card.
- When the Service Module card starts receiving DB downloads or DB updates.

  When a Service Module card starts downloading the RTDB, or if the Service Module card starts accepting database updates, it needs to send a status message informing the ELAP of the first record received. This helps the ELAP keep track of downloads in progress.

Service Module Card Status Message Fields

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.
- Load Mode Status

  This flag indicates whether or not 80% of the IS-NR LIMs have access to SCCP services.
- 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.

System Hardware Verification

Service Module card loading verifies the validity of the hardware configuration for the Service Module cards. The verification of the hardware includes:

- Validity of the Service Module card motherboard
- Verification of daughterboard memory size

System hardware verification includes checks for the appropriate LNP capable hardware when an LNP quantity feature is on. If the hardware is not capable, the feature cannot be turned on and the provisioning mode is set to LNP Degraded. If capacity on the ELAP has exceeded the provisioned LNP feature quantity, the Major MPS alarm is set and the Service Module cards will not load.

DSM Motherboard Verification

An AMD-K6 (or better) motherboard is required to support the feature VSCCP application on the Service Module card. EAGLE 5 ISS maintenance stores the validity status of the Service Module card's motherboard configuration. The system does not allow the LNP ELAP configuration feature to be enabled if the hardware configuration is invalid.

When the VSCCP application is initializing, it determines the motherboard type. If the motherboard is determined to be invalid for the LNP ELAP configuration application, loading of the Service Module card is automatically inhibited and the card is booted through PMTC. Booting the card in this manner suppresses any obituary.

Service Module Card Daughterboard Memory Validation

The VSCCP application performs two types of memory validation to determine whether or not a Service Module card has sufficient memory to run the VSCCP application: Local Memory validation and Continual Memory validation.

The report from the EAGLE 5 ISS `rept-stat-sccp` command includes the daughterboard memory both allocated and physically present on each Service Module card. (See the *Commands Manual* for a description of the `rept-stat-sccp` command output.)

Local Memory Validation

Any time the LNP ELAP configuration feature is enabled and a Service Module card is initializing, VSCCP checks to see if the Service Module card has at least one 4G of memory. After this is successful, VSCCP application requests the RTDB size from the MPS and determine if the Service Module card contains sufficient memory to download the RTDB. These two checks occur before starting the data loading operation from the MPS.

Real-Time Memory Validation

After communications between the Service Module card and ELAP have been established, and the Service Module card has joined the RMTP Tree, the ELAP starts downloading the RTDB to the Service Module card. After the Service Module card has downloaded the RTDB, it continues to receive database updates as necessary. The ELAP includes the size of the current RTDB in all records sent to the Service Module card. The Service Module card compares the size required to the amount of memory installed, and issues a minor alarm whenever the database exceeds the configured percentage allowed of Service

Module card memory. If the database completely fills the Service Module card memory, a major alarm is issued and the Service Module card status changes to IS-ANR/Restricted.

Actions Taken for Invalid Hardware

When the hardware configuration for a Service Module card is determined to be invalid for the LNP ELAP Configuration feature, SCM automatically inhibits loading for that specific card. A major alarm is generated indicating that loading for that Service Module card has failed and that the card has been automatically inhibited (prevented from reloading again). When card loading is inhibited, the primary state of the card is set to OOS-MT-DSBLD, and the secondary state of the card is set to MEA (Mismatch of Equipment and Attributes).

The following actions apply to a Service Module card determined to be invalid:

- The Service Module card will not download the EAGLE 5 ISS databases.
- The Service Module card will not download the RTDB from the ELAP.
- The Service Module card will not accept RTDB updates (additions, changes, and deletes) from the ELAP.

Refer to the *Tekelec 1100 AS MPS Platform Software and Maintenance Manual* to determine the appropriate corrective actions.

Service Module Card Memory Capacity Status Reporting

The Service Module card sends a message to the ELAP containing the amount of memory on the Service Module card board. The ELAP determines whether the Service Module card has enough memory to store the RTDB and sends an ACK or NAK back to the Service Module card indicating whether or not the Service Module card has an adequate amount of memory.

When the ELAP sends database updates to the Service Module cards, the update messages includes a field that contains the new database memory requirements. Each Service Module card monitors the DB size requirements and issues a minor alarm if the size of the DB exceeds the allowed configurable percentage of the memory. See *Modify System Defaults* for more information on allowed configurable percentages. If a database increases to the point that it occupies 100% of the Service Module card memory, a major alarm is issued.

The EAGLE 5 ISS `rept-stat-mps:loc=xxxx` command shows the amount of memory used by the RTDB as a percent of available Service Module card memory (see *rept-stat-mps*).

Unstable Loading Mode

At some point, having a number of invalid Service Module cards will result in some of the LIMs being denied SCCP services. There is a threshold that needs to be monitored: if the number of valid Service Module cards is insufficient to provide service to at least 80% of the IS-NR LIMs, the system is said to be in an unstable Loading Mode.

The system interrupts and aborts card loading upon execution of an STP database change command. Loading Mode support denies the execution of STP database change commands when the system is in an unstable loading mode.

An unstable loading mode exists when any of the following conditions are true:

- The system's maintenance baseline has not been established.

- Less than 80% of the number of LIMs provisioned are IS-NR or OOS-MT-DSBLD.

  The conditions that an insufficient number of Service Module cards are IS-NR or OOS-MT-DSBLD relative to 80% of the number of provisioned LIMs is called a failure to provide adequate SCCP capacity.

- The number of IS-NR and OOS-MT-DSBLD SCCP cards is insufficient to service at least 80% of all provisioned LIMs.

  Loading Mode is based on the ability of the system to provide SCCP service to at least 80% of the LIMs. No more than 16 LIMs can be serviced by each SCCP Service Module card.

- There is insufficient SCCP service, which occurs if an insufficient number of IS-NR Service Module cards are available to service at least 80% of the number of IS-NR LIMs.

  It is possible for LIMs or Service Module cards to be inhibited or to have problems that prevent them from operating normally. If enough Service Module cards are out of service, it may not be possible for the remaining IS-NR Service Module cards to service at least 80% of the number of IS-NR LIMs. This is called "insufficient SCCP service." When this occurs, some of the LIMs will be denied SCCP service. It is possible to use the EAGLE 5 ISS `inh-card` command to inhibit LIMs to bring the ratio back to 16:1 or better (see *Actions Taken During System Unstable Loading Mode*).

- If LIM cards are being denied SCCP service and any Service Module cards are in an abnormal state (OOS-MT, IS-ANR)

Actions Taken During System Unstable Loading Mode

- Unstable loading mode has no impact on RTDB downloads or the stream of RTDB updates.
- When the loading mode is unstable, the `rept-stat-sys` command will report the existence of the unstable loading mode and the specific trigger that caused it.
- When in an unstable Loading Mode, the EAGLE 5 ISS will not accept STP database updates. When updates are rejected, the reason will be given as `E3112 Cmd Rej: Loading Mode unstable due to SCCP service is deficient.`

  The `inh-card` and `alw-card` commands can be used to alter SCCP service levels to achieve the 80% threshold. This can be repeated for each card until the system is able to supply SCCP services to at least 80% of the IS-NR LIMs. The remaining 20% LIM or supporting Service Module cards may remain out of service until the stream of STP database updates ceases. This stream of updates can be temporarily interrupted to allow the remaining 20% of the system to come in service.

  Once an STP database has been loaded, that database can be updated (as long as the system is not in an unstable Loading Mode). However, if an STP update comes in during STP database loading, the Service Module card will abort the current loading, issue a `class 01D7 obit` message, and reboot.

- If executing the `ent-card` or `inh-card` command would cause the system to enter an unstable Loading Mode, it will be necessary to use the force parameter on the command.

Commands

The EAGLE 5 ISS commands described in this section report status information for the provisioning system.

Refer to the *Commands Manual* for command descriptions, parameters, and output examples.

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.

Samples of the reports these commands produce are shown below.

```
rept-stat-mps
                                                          rlghncxa03w 04-01-07
 10:23:93 EST  EAGLE 31.3.0
                  VERSION       PST            SST        AST
ELAP A            027-015-000   OOS-MT         Fault     Standby
CRITICAL PLATFORM    ALARM DATA = No Alarms
MAJOR    PLATFORM    ALARM DATA = h'0123456789ABCDEF
MINOR    PLATFORM    ALARM DATA = h'0123456789ABCDEF
CRITICAL APPLICATION ALARM DATA = No Alarms
MAJOR    APPLICATION ALARM DATA = h'0123456789ABCDEF
MINOR    APPLICATION ALARM DATA = No Alarms
      ALARM STATUS = ** 0371  Major Platform Failure(s)

               VERSION       PST            SST        AST
ELAP B         027-015-000   OOS-MT         Fault     Active
CRITICAL PLATFORM    ALARM DATA = No Alarms
MAJOR    PLATFORM    ALARM DATA = No Alarms
MINOR    PLATFORM    ALARM DATA = No Alarms
CRITICAL APPLICATION ALARM DATA = h'0123456789ABCDEF
MAJOR    APPLICATION ALARM DATA = h'0123456789ABCDEF
MINOR    APPLICATION ALARM DATA = No Alarms
      ALARM STATUS = *C 0373  Critical Application Failure(s)

CARD   PST          SST       LNP STAT
1106 P IS-NR        Active    ACT
1201   IS-ANR       Active    SWDL
1205   OOS-MT-DSBLD Manual    -------
1302   OOS-MT       Isolated  -------
1310   IS-ANR       Standby   SWDL
```

```
CARD 1106 ALARM STATUS = No Alarms
  DSM PORT A:    ALARM STATUS       = No Alarms
  DSM PORT B:    ALARM STATUS       = No Alarms
CARD 1201 ALARM STATUS = No Alarms
  DSM PORT A:    ALARM STATUS       = **  0084 IP Connection Unavailable
  DSM PORT B:    ALARM STATUS       = **  0084 IP Connection Unavailable
CARD 1205 ALARM STATUS = No Alarms
  DSM PORT A:    ALARM STATUS       = **  0084 IP Connection Unavailable
  DSM PORT B:    ALARM STATUS       = **  0084 IP Connection Unavailable
CARD 1302 ALARM STATUS = ** 0013 Card is isolated from the system
  DSM PORT A:    ALARM STATUS       = **  0084 IP Connection Unavailable
  DSM PORT B:    ALARM STATUS       = **  0084 IP Connection Unavailable
CARD 1310 ALARM STATUS = No Alarms
  DSM PORT A:    ALARM STATUS       = **  0084 IP Connection Unavailable
  DSM PORT B:    ALARM STATUS       = **  0084 IP Connection Unavailable
Command Completed.
;
```

rept-stat-trbl

The `rept-stat_trbl` command includes the Service Module card and ELAP IP link alarms.

rept-stat-alm

The `rept-stat-alm` command 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 5 ISS outputs two types of unsolicited messages:

- Unsolicited Alarm Messages (UAMs) - Denotes persistent problems with a device or object that needs the attention of a craftsperson.
- 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 5 ISS. The EAGLE 5 ISS controls and generates the alarm number, associated text, and formatting for alarms sent to EAGLE 5 ISS through the Maintenance Block mechanism for the ELAP.

The *Unsolicited Alarm and Information Messages Manual* describes all EAGLE 5 ISS 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 14: MPS Platform and ELAP Alarm Category UAMs*, are forwarded to the EAGLE 5 ISS 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 *MPS and ELAP 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 *Tekelec 1100 AS/MPS Platform Software and Maintenance Manual*.

Table 14: 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 15: 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 the *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
12345678901234567890123456789012345678901234567890123456789012345678901234567890

    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 the *Unsolicited Alarm and Information Messages Manual* .

Table 16: RTDB Audit Alarms

UAM #	Alarm Level	Trigger	Message Text
443	Minor	An RTDB has become corrupted.	RTDB database corrupted

UAM #	Alarm Level	Trigger	Message Text
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
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 resynchroniation 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/UIM Troubleshooting" chapter in the *Unsolicited Alarm and Information Messages Manual*.

Table 17: 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	LNP Ported LRNs approaching Feat. Capacity

UAM #	Alarm Level	Trigger	Message Text
		currently configured for the EAGLE 5 ISS.	
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
286	Major	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

UAM #	Alarm Level	Trigger	Message Text
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 18: 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 19: 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 LNP LRN measurements report will be truncated, and additional LRN measurements will not be collected or reported.	System Meas. Limit exceeded for LRN
1311	N/A	The Measurements Platform is not enabled and the number of provisioned NPANXXs exceeds 150,000. This UIM is notification that the LNP NPANXXs measurements report will be truncated, and additional NPANXX measurements will not be collected or reported.	System Meas. Limit exceeded for NPANXX

Chapter 5

ELAP Software Configuration

Topics:

This chapter describes the text-based user interface that performs ELAP configuration and initialization.

Overview of the ELAP User Interfaces

The EAGLE LNP Application Processor (ELAP) User Interface provides two user interfaces:

- The Graphical User Interface provides GUI menus that maintain, debug, and operate the platform; it and its associated error messages are described in *ELAP Graphical User Interface*.
- The text-based User Interface has a Configuration menu that performs the ELAP configuration and initialization; it is described in this chapter.

The GUI provides the user with menus and screens to perform routine operations. The text-based user interface provides the ELAP Configuration menu to perform the initial configuration.

To communicate with the ELAP graphical user interface, you use a PC with a network connection and a network browser. For information about using the ELAP GUI, see *ELAP Graphical User Interface*.

To configure ELAP, you use the ELAP text-based user interface. For information about configuring the ELAP and how to set up its PC workstation, continue with this chapter.

Setting Up an ELAP Workstation

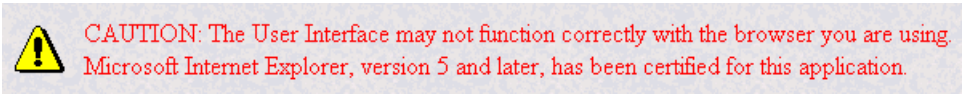
The customer workstation serving as a client PC (shown in *Figure 4: Process Architecture View of the ELAP UI*) must meet certain criteria, which are described next.

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 5.0 or later. The ELAP user interface is also compatible with Mozilla Firefox 1.0.2 or later. Do not use other browsers with the ELAP user interface. When using Firefox, you will encounter this message when logging into the ELAP GUI:



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 1.6 clients are supported, and backwards compatibility is maintained for Java 1.5 clients.

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 will not take effect.

1. Using the selected browser (Internet Explorer 5.0 or later or Mozilla Firefox 1.0.2 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:

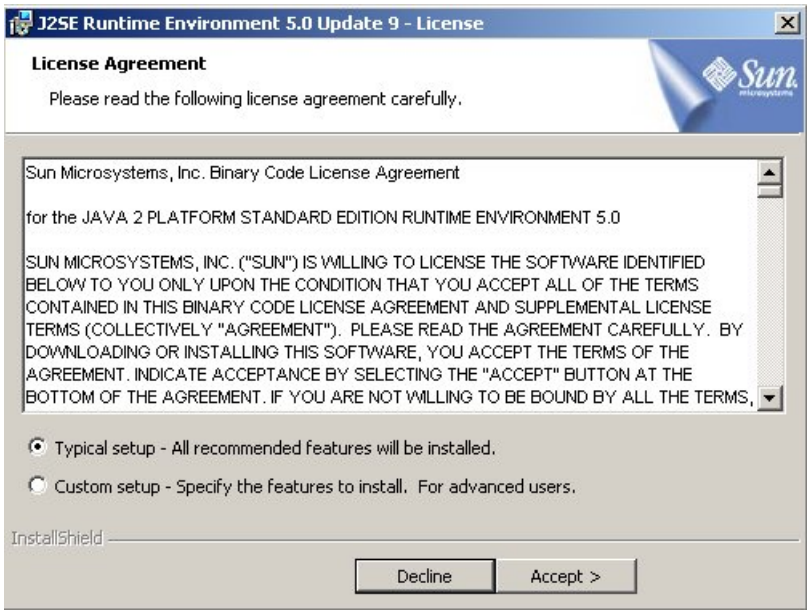
   ```
   The User Interface may not function correctly with the browser you are using.
   Microsoft Internet Explorer, version 5 and later, has been certified for this
   application
   ```

   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 32: Security Warning Window*.

   Figure 32: Security Warning Window

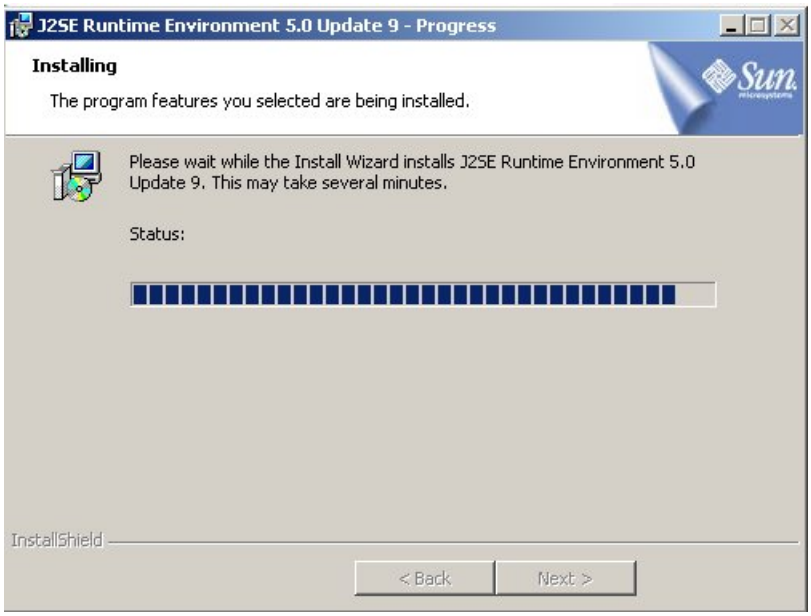
3. Click the **Install** button to begin the process of loading the Java plug-in.
4. Next, the Java installation presents a **License Agreement** screen as shown in *Figure 33: License Agreement*.

   Figure 33: License Agreement



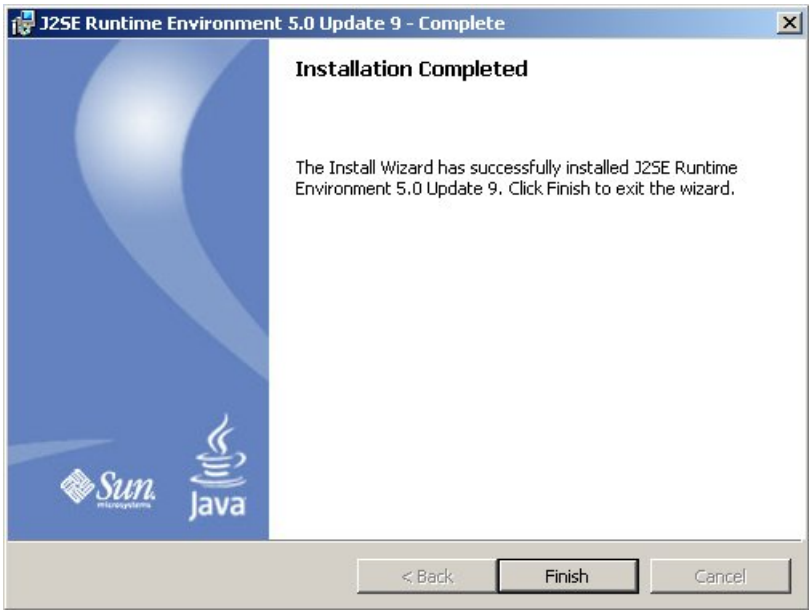
5. Ensure that the **Typical Setup** radio button is selected, and click the **Accept** button to accept the Sun Microsystems agreement.
6. The installation process starts, and a progress window appears as shown in *Figure 34: Java Installation Progress Window*.

Figure 34: Java Installation Progress Window



7. When the installation is complete, the Installation Complete window appears as shown in *Figure 35: Java Installation Complete Window* .

Figure 35: 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.

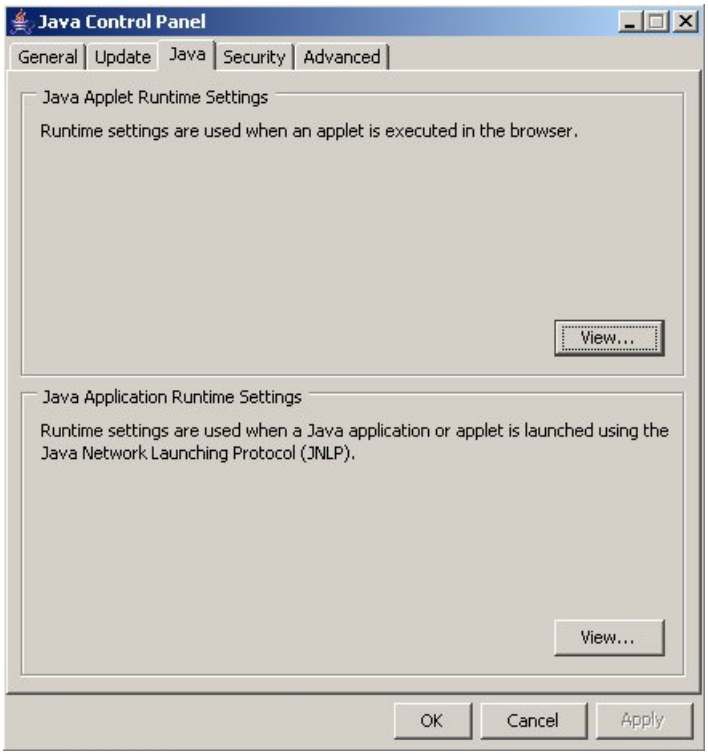
Note: The selected browser must be the only browser open on your PC when you modify or create the Java policy file, or else the change does not take effect.

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:

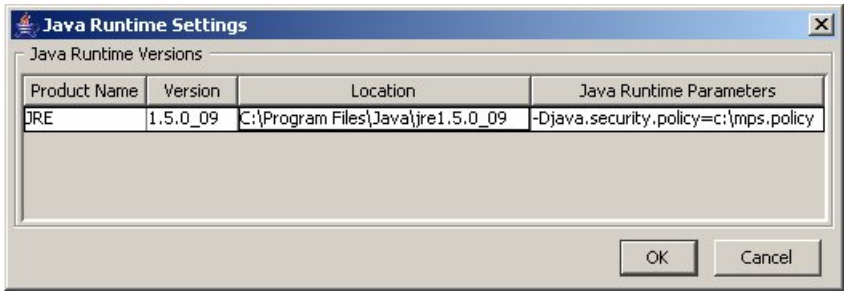
1. From the Windows **Start** menu, select **Control Panel**.
2. Select the **Java Control Panel**. When the **Java Control Panel** appears, click the **Java** tab as shown in *Figure 36: Java Control Panel, Java Tab*.

Figure 36: 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 37: Java Runtime Settings Dialog Box*.

Figure 37: 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 Diaglog 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 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 requirements 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 20: Information for MPS at EAGLE 5 ISS A* and EAGLE 5 ISS B *Table 21: Information for MPS at EAGLE 5 ISS B*). Fill in the following tables for reference during the installation procedure.

Table 20: 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 21: 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	

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. Before going into the details about the Configuration Menu, you need to know a few things about 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 38: Configuration Menu Header Format*.

Figure 38: Configuration Menu Header Format

```
MPS Side A:  hostname: mps-t1100-a  hostid: fd0a4767
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: ELAP 1.0.1-4.0.0_50.37.0
             Mon Sep 26 10:57:57 EDT 2005
```

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.

Initial “elapconfig” User Login

The first time the `elapconfig` user logs in to the system, the text screen is displayed as shown in *Figure 39: Initial Configuration Text Screen* .

Figure 39: 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...
```

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 40: Initial Configuration Continues* shows the continuation of the screen information. The installer enters `y` if the installation is to continue.

Figure 40: Initial Configuration Continues

```
Are you sure you wish to continue? [N]: y
```

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 41: Entering the elapdev Password* shows sample output that is generated after the correct password is entered.

Figure 41: Entering the elapdev Password

```
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.
```

At this point, the first appearance of the Configuration Menu occurs.

Text-based Configuration Menu

Following the report appearing in *Figure 41: Entering the elapdev Password*, the ELAP Configuration Menu is displayed as shown in *Figure 42: ELAP Configuration Menu* . The `elapconfig` user can now begin configuring the MPS local and remote servers.

Figure 42: ELAP Configuration Menu

```
MPS Side A:  hostname: mps-t1100-a  hostid: 0
             Platform Version: 3.0.2-8.0.0_80.4.0
             Software Version: ELAP 3.0.2-8.0.0_80.4.0
             Wed Apr 16 13:32:15 EDT 2008

 /-----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
```

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 43: Example of Display Configuration Output*.

Figure 43: Example of Display Configuration Output

```
MPS Side A:  hostname: mps-t1100-a  hostid: 0
             Platform Version: 3.0.2-8.0.0_80.4.0
             Software Version: ELAP 3.0.2-8.0.0_80.4.0
             Wed Apr 16 13:40:38 EDT 2008

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...
```

Addresses that you choose should not conflict with your internal network addresses. The class C networks you choose should not conflict with the class C network used in your network scheme. *Table 22: Sample IP Addresses Used in Configuration* shows an example of IP addresses used in the configuration process.

Table 22: 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 44: Configure Network Interfaces Menu*. It supports the configuration of all the network interfaces for the ELAP.

Figure 44: 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:
```

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 45: Configure Provisioning Network Output* for the option **1** output.

Figure 45: Configure Provisioning Network 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...
```

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 46: Configure DSM Network* for the option **2** output.

Figure 46: Configure DSM Network

```
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]:
```

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 21: Information for MPS at EAGLE 5 ISS B* and *Table 20: 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 47: Configuring NAT Addresses Prompt* shows an example of a resulting prompt.

Figure 47: Configuring NAT Addresses Prompt

```
ELAP A Static NAT Address:
```

Select Time Zone

Note: Do not perform the Select the Time Zone function on a running system. Contact Tekelec Customer Care Center 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 48: Select Time Zone Menu* for the option 3 output.

Figure 48: Select Time Zone Menu

```
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:
```

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 49: Exchange Secure Shell Keys Output* for the option 4 output.

Figure 49: Exchange Secure Shell Keys Output

```
Are you sure you wish to exchange keys? [N]: y
```

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 50: Change Password* for the option 5 output.

Figure 50: Change Password

```
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...
```

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 51: Platform Menu Output* for the option 6 output.

Figure 51: Platform Menu Output

```
MPS Side A:  hostname: mps-t1100-a  hostid: fd0a4767
             Platform Version: 2.0.2-4.0.0_50.26.0
             Software Version: ELAP 1.0.1-4.0.0_50.37.0
             Mon Sep 26 10:57:57 EDT 2005

/-----ELAP Platform Menu-\
/-------------------------\
|  1 | Initiate Upgrade   |
|----|--------------------|
|  2 | Eject CD           |
|----|--------------------|
|  3 | Reboot MPS         |
|----|--------------------|
|  4 | Halt MPS           |
|----|--------------------|
|  5 | MySQL Backup       |
|----|--------------------|
|  6 | RTDB Backup        |
|----|--------------------|
|  e | Exit               |
\-------------------------/

Enter choice:
```

Initiate Upgrade

The Initiate Upgrade menu option 1 initiates an upgrade on the selected ELAP. For upgrade procedures, contact *Customer Care Center*.

Eject CD

The Eject CD menu option 2 initiates an ejection of the CD media on the selected ELAP. The default is 'BOTH'.

```
Eject CD tray of MPS A, MPS B or BOTH? [BOTH]:
```

Reboot MPS

The Reboot MPS menu option 3 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: Rebooting the MPS stops all ELAP processes. Databases cannot be updated until MPS is fully booted.

Halt MPS

The Halt MPS menu option 4 initiates a halt of one MPS or both. The default is BOTH.

CAUTION: Halting an MPS stops all ELAP processes. Selecting the default (halt both MPS A and MPS B) requires a person to be physically present in order to reboot MPS and allow for further access!

Note: The `elapconfig` user can abort the MPS Halt by pressing the **Escape** key at the displayed prompt.

MySQL Backup

The MySQL Backup menu option 5 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 6 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-t1100-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 5 ISS A and MPS A side of EAGLE 5 ISS B. Attempting to perform initial configuration on MPS B of EAGLE 5 ISS 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 5 ISS A and MPS A on EAGLE 5 ISS 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. Tekelec recommends that you do not change the default network values.

- 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 [ ].
- It is the customer's decision about the timing and frequency of performing a back-up of his databases. 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 it will dictate the frequency of database back-up.
- 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 5 ISS pairs.
- The ELAP terms 'local' and 'remote' are relative with respect to the ELAP configuration software. In other words, if the installer is running the configuration software on the physical MPS (that is, the MPS that the installer is physically on-site and has his terminal connected to), the configuration software refers to that MPS as 'local'. However if the installer connects through the network into the MPS A on EAGLE 5 ISS B, the configuration software executing at EAGLE 5 ISS B sees itself as 'local', referring to the MPS that the installer is physically connected to as the 'remote'.

  Remember that 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 5 ISS A is the first MPS to which the installer 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 5 ISS A is considered to be the on-site MPS to which the installer has the physical connection. This document refers to the MPS to which the installer does not have the physical connection as MPS A on EAGLE 5 ISS 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 23: 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.

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 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 *ELAP Administration Manual - 8.0* or *ELAP Administration Manual - 9.0* .

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 21: 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 ISS A to configure it, then uses `ssh` to connect to the MPS at EAGLE 5 ISS B and configure it.

1. Upon connecting to the MPS on EAGLE 5 ISS A, login to the ELAP.
   a) Log in as `elapconfig`.
   A caution appears.

```
SunOS 5.7
mpsa-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 ISS B. While the MPSs on EAGLE 5 ISS 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-t1100-a  hostid: a8c0683d
             Platform Version: 3.0.2-8.0.0_80.4.0
             Software Version: ELAP 3.0.2-8.0.0_80.7.0
             Wed Apr 16 13:44:58 EDT 2008


/-----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 ISS A.

```
MPS Side A:  hostname: mps-t1100-a  hostid: 0
             Platform Version: 3.0.2-8.0.0_80.4.0
             Software Version: ELAP 3.0.2-8.0.0_80.4.0
             Wed Apr 16 13:44:58 EDT 2008
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 20: Information for MPS at EAGLE 5 ISS A* and *Table 21: 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 20: Information for MPS at EAGLE 5 ISS A* and *Table 21: 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 20: Information for MPS at EAGLE 5 ISS A* and *Table 21: 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...
```

a) Press **Return** to continue.
   You are prompted for confirmation on setting the time zone for MPS A and MPS B at his site.
b) 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.

Upon 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: bonaire-a  hostid: a8c0d03d
             Platform Version: 3.0.3-8.0.0_80.8.0
             Software Version: ELAP 3.0.12-8.0.0_80.12.0
             Fri Jul 25 09:29:35 EDT 2008

 /-----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 B:  hostname: bonaire-b  hostid: a8c0d13d
             Platform Version: 3.0.3-8.0.0_80.8.0
             Software Version: ELAP 3.0.13-8.0.0_80.14.0
             Mon Jul 28 10:21:15 EDT 2008

 /-----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 B:  hostname: bonaire-b  hostid: a8c0d13d
             Platform Version: 3.0.3-8.0.0_80.8.0
             Software Version: ELAP 3.0.13-8.0.0_80.14.0
             Mon Jul 28 10:21:15 EDT 2008

 /-----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 B:  hostname: bonaire-b  hostid: a8c0d13d
             Platform Version: 3.0.3-8.0.0_80.8.0
             Software Version: ELAP 3.0.13-8.0.0_80.14.0
             Mon Jul 28 10:21:15 EDT 2008

 /-----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 B:  hostname: bonaire-b  hostid: a8c0d13d
             Platform Version: 3.0.3-8.0.0_80.8.0
             Software Version: ELAP 3.0.13-8.0.0_80.14.0
             Mon Jul 28 10:21:15 EDT 2008

 /-----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 t*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 the 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 ISS 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...
```

a) Press **Return** to return to the ELAP Configure NTP Server Menu.
b) 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 ISS 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 ISS A and on EAGLE 5 ISS B must be rebooted.

- If you do not need to reboot the MPS pairs on EAGLE 5 ISS A and on EAGLE 5 ISS B, continue with *Step 21*.
- If you must reboot the MPS pairs on EAGLE 5 ISS A and on EAGLE 5 ISS 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 **3**, Reboot MPS, from the ELAP Platform Menu.

```
/-----ELAP Platform Menu-\
/-------------------------\
|  1 | Initiate Upgrade    |
|----|---------------------|
|  2 | Eject CD            |
|----|---------------------|
|  3 | Reboot MPS          |
|----|---------------------|
|  4 | Halt MPS            |
|----|---------------------|
|  5 | MySQL Backup        |
|----|---------------------|
|  6 | 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 ISS 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 ISS B is now complete. Both MPSs on EAGLE 5 ISS A and MPSs on B are now configured and rebooted.

Appendix A

Time Zone File Names

Topics:

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 24: 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 B

ELAP Local Provisioning Utility

Topics:

This appendix provides user guide information for the ELAP Local Provisioning Utility (LPU) batch command language.

Introduction

This chaper 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 = *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 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 = *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 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 = *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 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 = *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 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 25: 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 26: 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 = oc1
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 = oc1
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.
```

Miscellenous Commands

ELAP supports the following miscellenous 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, a template is used to avoid repeating the message text for each possible service.

The templates are as follows:

- *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 xNeed to insert the missing mandatory argument.
```

The parameter's mnemonic (e.g. 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 LSMSmay 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.
```

Glossary

A

ACK	Data Acknowledgement
ACT	Activate
AIN	Advanced Intelligent Network 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.
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.
AS	Application Server A logical entity serving a specific Routing Key. An example of an Application Server is a virtual switch element handling all call processing for a unique range of PSTN trunks, identified by an SS7 DPC/OPC/CIC_range. Another example is a virtual database element, handling all HLR transactions for a particular SS7 DPC/OPC/SCCP_SSN combination.

A

	The AS contains a set of one or more unique Application Server Processes, of which one or more normally is actively processing traffic.
	Application Simulator
	Test tool that can simulate applications and/or SMSCs.

C

CD	Carrier Detect
	Compact Disk
CET	Customer Environment Test
CLASS	Custom Local Area Signaling Service
	Custom Local Area Subscriber Services
CNAM	Calling Name Delivery Service
CTS	Clear to Send

D

Database	All data that can be administered by the user, including cards, destination point codes, gateway 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
	Daughter Board
	Documentation Bulletin

D

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 5 ISS, but does not have to be.
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).

E

ECC	Error Correction Coded
ELAP	EAGLE Local Number Portability Application Processor

F

FTA	File Transfer Area A special area that exists on each OAM hard disk, used as a staging area to copy files to and from the EAGLE 5 ISS using the Kermit file-transfer protocol.
FTP	File Transfer Protocol A client-server protocol that allows a user on one computer to transfer files to and from another computer over a TCP/IP network.

G

GB	Gigabyte — 1,073,741,824 bytes
GMT	Greenwich Mean Time
GPS	Global Positioning System
GT	Global Title Routing Indicator
GTT	Global Title Translation A feature of the signaling connection control part (SCCP) of the SS7 protocol that the EAGLE 5 ISS uses to determine which service database to send the query message when an MSU enters the EAGLE 5 ISS 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.
GUI	Graphical User Interface The term given to that set of items and facilities which provide the user with a graphic means for manipulating screen data rather than being limited to character based commands.

H

HS	High Speed
HSOP	High Speed Operation Protocol

I

ID	Identity, identifier

I

IN	Intelligent Network A network design that provides an open platform for developing, providing and managing services.
IP	Internet Protocol IP specifies the format of packets, also called datagrams, and the addressing scheme. The network layer for the TCP/IP protocol suite widely used on Ethernet networks, defined in STD 5, RFC 791. IP is a connectionless, best-effort packet switching protocol. It provides 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 a number in dotted decimal notation which looks something like [192.168.1.1].
IPM	Implementation Project Management IMT Power and Multiplexer Card Initial Product Manufacture
IS-ANR	In Service - Abnormal The entity is in service but only able to perform a limited subset of its normal service functions.
IS-NR	In Service - Normal
ISS	Integrated Signaling System

L

L

LAN	Local Area Network 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. See also STP LAN.
LED	Light Emitting Diode An electrical device that glows a particular color when a specified voltage is applied to it.
LIDB	Line Information Database
LIM	Link Interface Module Provides access to remote SS7, IP and other network elements, such as a Signaling Control Point (SCP) through a variety of signaling interfaces (DS0, MPL, E1/T1 MIM, LIM-ATM, E1-ATM, IPLIMx, IPGWx). The LIMs consist of a main assembly and possibly, an interface appliqué board. These appliqués provide level one and some level two functionality on SS7 signaling links.
LNP	Local Number Portability
LRN	Location Routing Number 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.

L

LSMS	Local Service Management System

M

MEA	Memory Extension Applique Mismatch of Equipment and Attributes
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.
MR	Message Relay
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

M

signaling information octet of the message.

- The routing information for the message, shown in the routing label of the message, with the 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 5 ISS uses to pick which link set and signaling link to use to route the message.

N

NAK	Negative Acknowledgment
NAT	Network Address Translation
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).
NPAC	Number Portability Administration Center
NTP	Network Time Protocol

O

OAM	Operations, Administration, and Maintenance The application that operates the Maintenance and Administration Subsystem which controls the operation of the EAGLE 5 ISS.

O

OOS-MT — Out of Service - Maintenance

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.

OS — Operations Systems

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**).

P

PMTC	Peripheral Maintenance
PPP	Point-to-Point Protocol

R

RAID	Redundant Array of Independent Disks A group of disks presented to clients as one or more large virtual disks, with accesses coordinated among multiple disks concurrently to increase performance, reliability, or both.
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 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
RMTP	Reliable Multicast Transport Protocol
Route	A signaling path from an LSP to an RSP using a specified Link Set

R

RTDB	Real Time Database
RTS	Ready to Send Request to Send

S

SCCP	Signaling Connection Control Part
SCM	System Configuration Manager System Configuration Matrix.
SERVDI	Support ELAP Reload via Database Image
Service Module card	DSM card or E5-SM4G card that contains the Real Time Database (RTDB) downloaded from an EPAP or ELAP system.
SP	Signaling Point A set of signaling equipment represented by a unique point code within an SS7 domain.
SPID	Service Provider ID
Split NPA	Split Number Planning Area 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

S

	being split is copied to the new NPANXX.
SSH	Secure Shell A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE 5 ISS IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.
SSN	Subsystem Number The subsystem number of a given point code. The subsystem number identifies the SCP application that should receive the message, or the subsystem number of the destination point code to be assigned to the LNP subsystem of the EAGLE 5 ISS. 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.
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.

T

TCP/IP	Transmission Control Protocol/Internet Protocol
TN	Telephone Number

T

A 10 digit ported telephone number.

Translation Type — See TT.

U

UAM — Unsolicited Alarm Message

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.

UDP — User Datagram Protocol

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.

V

VIOL — A value displayed on an application GUI that indicates that the client brower'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.

V

VSCCP	VxWorks Signaling Connection Control Part The application used by the Service Module card to support EPAP-related features and LNP 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
WSMSC	Wireless Short Message Service Center

X

XLAT	Translate Indicator