Tekelec EAGLE® 5 Integrated Signaling System

T1000 MPS Platform Software and Maintenance Manual

910-5391-001 Revision A
February 2009

Table of Contents

Chapter 4: MPS Platform and Application Alarms................55

List of Figures

List of Tables

Chapter

1

Introduction

Topics:

This chapter provides a brief description of the T1000-based Multi-Purpose Server. This chapter also includes the scope, audience, and organization of the manual; how to find related publications; and how to contact Tekelec documentation for assistance.

Overview

This manual contains the information necessary for the maintenance of the T1000-based Multi-Purpose Server (MPS) that supports the EAGLE 5 ISS Provisioning Application Processor (EPAP). Included are an overview of the MPS archtiecture and functions, routine operational procedures, preventative maintenance techniques, and corrective maintenance procedures.

Scope and Audience

This manual is written for system administrators of the MPS. The manual provides routine operating procedures, preventive maintenance procedures, and corrective maintenance procedures that aid administrators maintaining the MPS.

- *Preventive maintenance* procedures are routines implemented on a scheduled basis to prevent system faults. These tasks are industry-standard recommendations and are adaptable to any customer maintenance plan.

- *Corrective maintenance* procedures are used in response to a system alarm or output message. These procedures are MPS-specific and aid in the detection, isolation, and repair of faults.

Manual Organization

This document is organized into the following chapters:

- *Introduction* on page 1 contains general information about the T1000-based Multi-Purpose Server (MPS) documentation, the organization of this manual, and how to request technical assistance.

- *Platform Overview* on page 9 provides an overview of the T1000-based MPS platform, including terminology, hardware, software, network configurations, user administration, and fault tolerance.

- *MPS Maintenance* on page 29 describes preventative maintenance procedures, system health checks, problem detection, reporting, and recovery.

- *MPS Platform and Application Alarms* on page 55 consists of the platform and application alarm recovery procedures, grouped by alarm severity level.

- *MPS Field Replaceable Units* on page 107 consists of the hardware replacement procedures for the Field Replaceable Units (FRUs) of the T1000-based MPS.

- *General Procedures* on page 119 contains general procedures that are commonly used and referred to by other procedures.

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

  - **Columbia**

    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**

  - **Signaling**

    Phone:

    +44 1784 467 804 (within UK)

    TAC Regional Support Office Hours:

    8:00 a.m. through 7:00 p.m. (GMT), Monday through Friday, excluding holidays

  - **Software Solutions**

    Phone:

    +33 3 89 33 54 00

    TAC Regional Support Office Hours:

    8:00 a.m. through 7:00 p.m. (GMT), Monday through Friday, excluding holidays

- **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 (*support.tekelec.com*). 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 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 **new** Customer Support site at *support.tekelec.com*.

   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

Platform Overview

Topics:

This chapter describes the hardware, software, and network configuration of the T1000-based Multi-Purpose Server.

Introduction

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

The MPS platform supports the EAGLE 5 ISS Provisioning Application Processor (EPAP). The EPAP application includes the INP, G-Flex®, G-Port®, IS-41 to GSM Migration, and Equipment Identity Register (EIR) features. In addition to the software application, additional third-party software might be required to support the software application. *Figure 1: MPS/EAGLE 5 ISS Overview* on page 10 shows an overview of how the MPS is used with the EAGLE 5 ISS.

This chapter provides an overview of the hardware and platform software that comprises the MPS. For information about the EPAP application and how it interacts with the EAGLE 5 ISS, refer to the *EPAP Administration Manual* .

Figure 1: MPS/EAGLE 5 ISS Overview

Figure 2: Layered Design for MPS and Applications
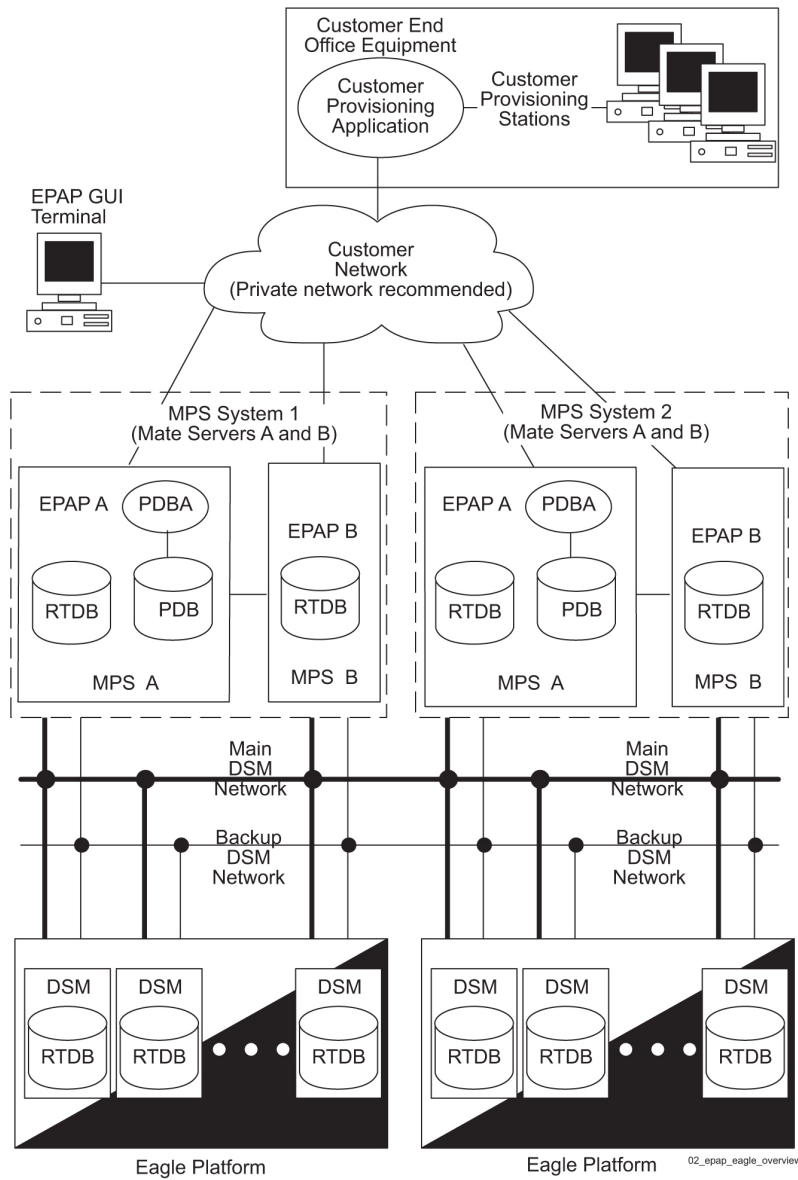
Layered Design

MPS is based on the Tekelec 1000 AS platform and uses a layered design with defined interfaces to enable application and platform changes to be made independently. This design provides an environment in which changes made to platform components do not require changes in application.

Figure 2: Layered Design for MPS and Applications on page 11 shows the layered design of the MPS and its supported application. In this manual, the application software is EPAP.

Figure 2: Layered Design for MPS and Applications

```
┌─────────────────────────────────┐
│                                 │
│      Application Software       │
│                                 │
├─────────────────────────────────┤
│                                 │
│     MPS Platform Software       │
│                                 │      Complete MPS
├─────────────────────────────────┤
│                                 │      Platform
│     Tekelec 1000 AS Hardware    │
│                                 │
└─────────────────────────────────┘
```
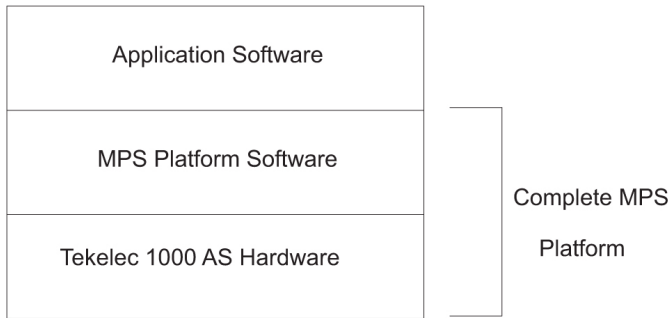
The MPS platform software is described in *MPS Platform Software Configuration* on page 18. For information about the other layers, refer to the following manuals:

- The Tekelec 1000 AS hardware layer is described in the *Tekelec 1000 Application Server Hardware Manual*.
- The application software is described in application documentation in the *EPAP Administration Manual*.

MPS Terminology

Table 2: MPS Terminology on page 12 defines the terminology used for MPS and the EPAP application.

Table 2: MPS Terminology

Term	Definition
MPS server	The Tekelec 1000 AS hardware and the MPS platform software comprise one MPS server.
Mate servers	Two MPS servers are located at an EAGLE 5 ISS site. An MPS server is referred to as a mate server by the other MPS server in the frame.
Upper server (also known as Server A)	This MPS server is installed above its mate.
Lower server (also known as Server B)	This MPS server is installed below its mate.
MPS system	Two MPS servers and their associated hardware are located at an EAGLE 5 ISS site. For more information about associated hardware, see *MPS System Hardware Configuration* on page 13.
Mated MPS systems	Two MPS systems are located at mated EAGLE 5 ISS sites.
EPAP A	This is the EPAP application running on MPS server A (the upper server).

Term	Definition
EPAP B	This is the EPAP application running on MPS server B (the lower server).

Tekelec 1000 AS Terminology

Table 3: Tekelec 1000 AS Platform Terminology on page 13 shows the terms used in describing the Tekelec 1000 AS platform.

Table 3: Tekelec 1000 AS Platform Terminology

Term	Definition
IPM	Initial Product Manufacture (IPM) is the process of installing Tekelec 1000 AS software platform on a *bare* server, which has no software installed, resulting in a state for which the server is ready for the installation of one or more applications.
Tekelec 1000 AS platform	The Tekelec 1000 AS platform is a combination of Tekelec 1000 AS hardware and Tekelec 1000 AS platform software.
TPD	Tekelec Platform Distribution (TPD) is the common platform Operating System packaged and distributed by Tekelec. TPD is the base installation for all products built on the Tekelec 1000 AS platform.

EAGLE 5 ISS Terminology

In this manual, Service Module card refers to either a DSM card or an E5-SM4G card unless a specific card is required. For more information about the supported cards, refer to the *EAGLE 5 ISS Hardware Manual*.

MPS System Hardware Configuration

Each MPS system requires the hardware shown in *Table 4: MPS Hardware Components* on page 14.

Table 4: MPS Hardware Components

Qty	Hardware Item	For more detail, see:	To replace, see:
2	Tekelec 1000 AS main unit; each unit has the following cards added during manufacturing: • Three dual-port gigabit Ethernet Peripheral Component Interconnect (PCI) cards • One Quad-Port serial PCI card • One PCI modem card, for use by only Customer Care Center Each Tekelec 1000 AS main unit has 2 gigabytes of Random Access Memory (RAM) installed and available.	*Tekelec 1000 Application Server Hardware Manual*	*Tekelec 1000 Application Server Hardware Manual*
4	Ethernet hubs: • Two for main DSM network • Two for backup DSM network	*Hubs* on page 14	*Hub Replacement Procedure* on page 114
2	Breaker panels	*Breaker Panels* on page 15	*Breaker Panel Replacement Procedure* on page 112
1	Power distribution panel (also called terminal block or terminal strip)	*Tekelec 1000 Application Server Hardware Manual*	Contact the *Customer Care Center* on page 3

The MPS system does not support additional peripheral devices, such as printers or tape drives.

Hubs

An MPS system contains four hubs. Two hubs support the main DSM network and two hubs support the backup DSM network. *Figure 3: MPS Hubs* on page 14 shows the location of the four hubs in the MPS frame and a magnified view of one hub.

Figure 3: MPS Hubs

MPS Frame

Hub Rear P/N 870-2224-01

Ethernet RJ-45

Rear View detail
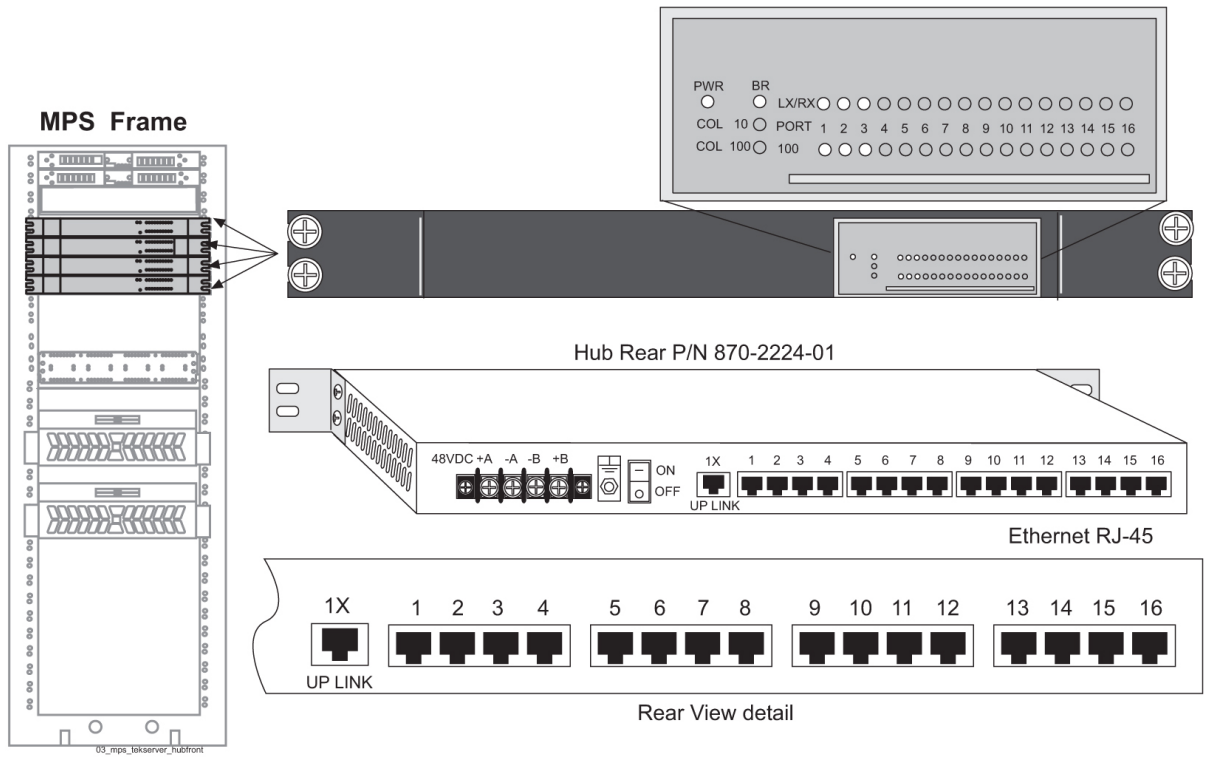
Breaker Panels

Figure 4: Front of Breaker Panel on page 15 shows the two circuit breaker panels used to provide redundant power paths:

- Upper circuit breaker panel (BP-1)
- Lower circuit breaker panel (BP-2)

Each circuit breaker panel has two sides: side A and side B. Each side has seven circuit breakers. Only the assigned or active circuit breakers on each side are *on* (closed). The *on* position of the circuit breaker is designated by **|**. The *off* (open) position of the circuit breaker is designated by **O**.

Figure 4: Front of Breaker Panel

Mounting screws Breaker Panel 1 Mounting screws
Breaker positions A1-A7 Front View Breaker positions B1-B7

Breaker positions A1-A7 Breaker Panel 2 Breaker positions B1-B7
Front View

Mounting screws Mounting screws
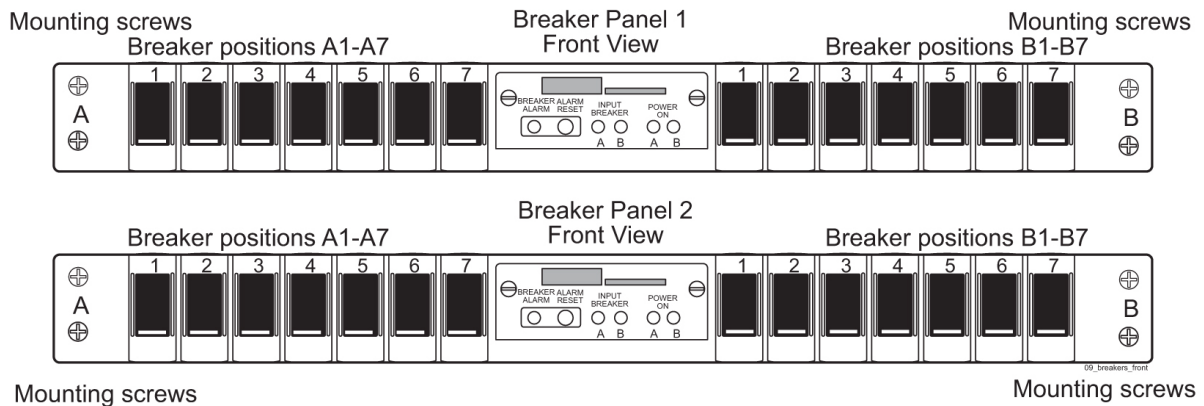
Breaker Panel LEDs

Figure 5: Breaker Panel LEDs on page 16 shows a detailed view of the power module, which is also called *Indicator Panel*, in the center of the front of each breaker panel.

Figure 5: Breaker Panel LEDs
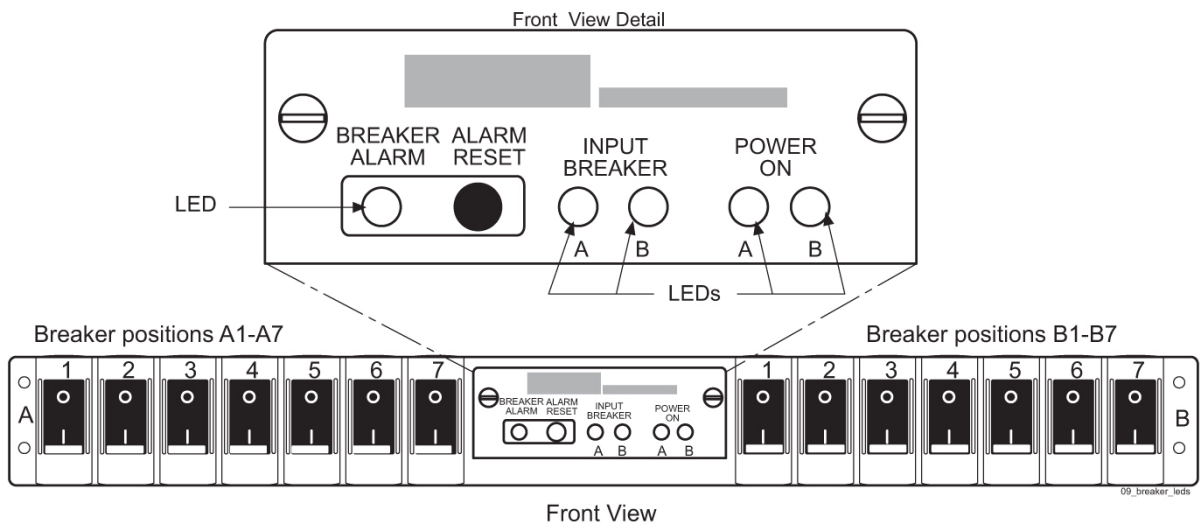
The power module contains two pairs of light-emitting diodes (LEDs). Each LED is labeled **A** and **B** to indicate which side of the breaker panel the LED represents:

- The two LEDs labeled **INPUT BREAKER** are illuminated (green) for normal operation. If one of the rear Input Breakers opens (pops out), its respective **INPUT BREAKER** LED is not illuminated.

- The two LEDs labeled **POWER ON** are illuminated (green) for normal operation. If power to the breaker panel fails, the affected **POWER ON** LED is not illuminated.

  Note: If one of the **POWER ON** LEDs is not illuminated, the respective **INPUT BREAKER** LED will not be illuminated and the **BREAKER ALARM** LED will be illuminated (red).

Breaker Panel Power Distribution

Power to the breaker panel is received from the customer power facility by the A and B input power feeds on the rear of the breaker panel. Power is distributed through the A and B side Input Breakers on the rear of the breaker panel to the circuit breakers located on the front of the breaker panel. Each Input Breaker controls the power from its corresponding input power feed and ensures that the input power level for its side is within an acceptable range.

From the Input Breakers, power is distributed to the circuit breakers on the front of the breaker panel. These circuit breakers control the power provided to the devices in the frame.

Power is distributed to the devices in the frame through terminal blocks, or terminal strips, which are mounted on the rear of the breaker panel. The circuit breakers on the front of the breaker panel control the power to these terminal blocks.

For more information about the cabling shown in *Figure 6: Rear of Breaker Panel* on page 17, refer to the *Tekelec 1000 Application Server Hardware Manual*.

Figure 6: Rear of Breaker Panel
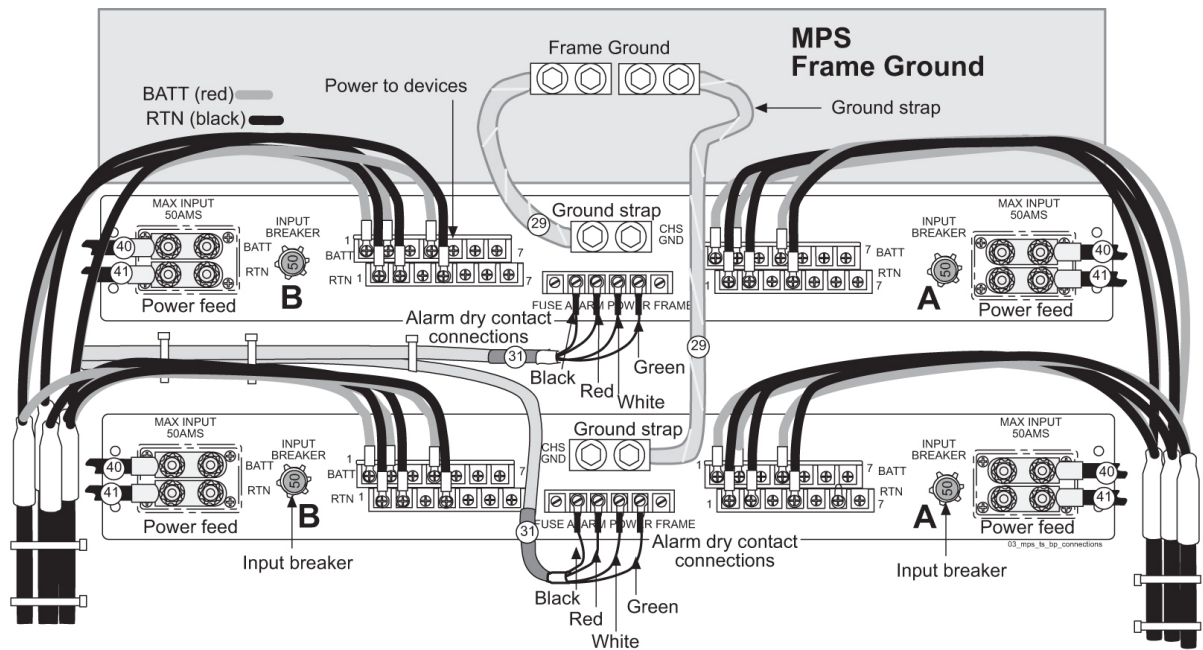
Mapping Breakers to Devices

Circuit breakers in positions 1, 2, and 4 on the A and B sides of the breaker panel are *on* (| position). The circuit breakers in positions 3, 5, 6 and 7 are not used, and may be in the *on* (|) or *off* (*O*) position. *Table 5: Mapping of Assigned (Closed) Circuit Breakers to Devices* on page 18 shows each assigned circuit breaker and the device it controls. The table shows the end-to-end connectivity from the breaker panel circuit breakers to the MPS.

Table 5: Mapping of Assigned (Closed) Circuit Breakers to Devices

Breaker Panel	Side	Breaker	Device
Upper (BP-1)	A	1	MPS A
		2	Hub 1
		4	Hub 2
	B	1	MPS B
		2	Hub 3
		4	Hub 4
Lower (BP-2)	A	1	MPS B
		2	Hub 3
		4	Hub 4
	B	1	MPS A
		2	Hub 1
		4	Hub 2

MPS Platform Software Configuration

MPS platform software is packaged and distributed as a Tekelec Platform Distribution (TPD). The following sections describe the features of the MPS platform software:

- *Kernel* on page 19
- *Serial Communication* on page 19
- *Remote Access* on page 21
- *Installation and Upgrade* on page 21
- *Diagnostics, Monitoring, and Alarming* on page 22
- *Disaster Recovery* on page 23
- *Security* on page 23

Kernel

The MPS platform uses an optimized kernel which supports:

- UNIX domain sockets
- TCP/IP version 4
- Integrated Drive Electronics (IDE)
- Universal Serial Bus (USB) version 1.1
- Point-to-Point Protocol (PPP) for dial-in access
- 10/100BASE-T and 1000BASE-T Ethernet cards

Serial Communication

The MPS provides the serial communication interfaces shown in *Figure 7: MPS Serial Port Connections* on page 19 and described in *Table 6: MPS Serial Port Assignments* on page 19.

Figure 7: MPS Serial Port Connections
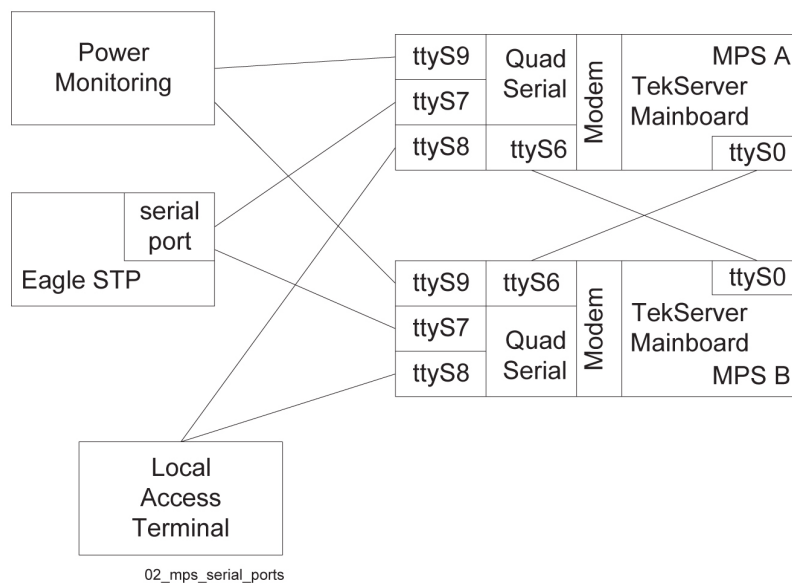
02_mps_serial_ports

Table 6: MPS Serial Port Assignments

Serial Port Name	Location	Access Through:	Serial Port Description
ttyS0	on Tekelec 1000 AS mainboard	Serial RS-232 port on rear of Tekelec 1000 AS chassis	Console port that is cable-crossed to mate, configured as: • 115200 baud • 8 data bits • 1 stop bit • No parity

Serial Port Name	Location	Access Through:	Serial Port Description
ttyS6	Quad-Serial card in PCI slot 8	Port 1 of DB44 to DB9 (X4) cable*	Cable from mate ttyS0 serial port, configured as: • 115200 baud • 8 data bits • 1 stop bit • No parity
ttyS7	Quad-Serial card in PCI slot 8	Port 2 of DB44 to DB9 (X4) cable*	Serial EAGLE 5 ISS connection port, configured by the MPS as: • 9600 baud • Parity 7E1 • Logins enabled
ttyS8	Quad-Serial card in PCI slot 8	Port 3 of DB44 to DB9 (X4) cable*	Local access terminal port, configured by the MPS as: • 9600 baud • Parity 7E1 • Logins enabled
ttyS9	Quad-Serial card in PCI slot 8	Port 4 of DB44 to DB9 (X4) cable*	Power monitoring port
Note: * For port assignments on the DB44 to DB9 (X4) cable, see *Figure 8: DB44 to DB9 (X4) Cable* on page 20. Port 0 of this cable connects to the Quad-Serial card in PCI slot 8.			

Figure 8: DB44 to DB9 (X4) Cable
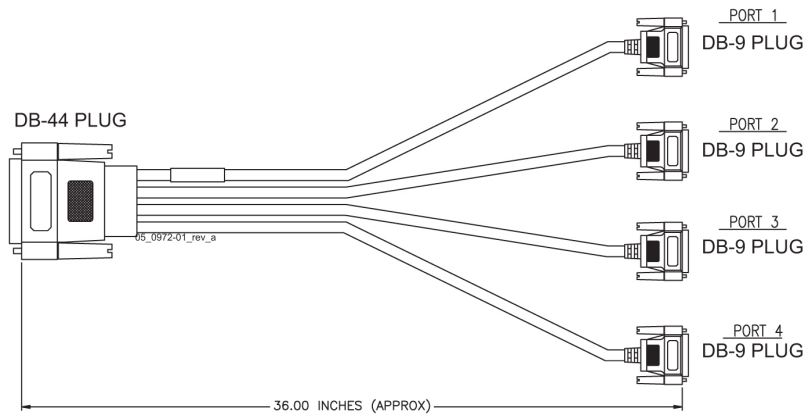
Remote Access

The MPS system provides the following remote access features.

- Remote network access is available through two Ethernet interfaces connected to the customer network. One of these interfaces is optional. For more information about the Ethernet interfaces, see *Table 7: MPS Network Interfaces* on page 24.

- A Web server provides hypertext transfer protocol (HTTP) access over Ethernet.

- The MPS does not support incoming connections that use non-secure services such as `rlogin`, `rsh`, `rexec`, `ftp`, and `telnet`. Any incoming connections using these services are dropped. The MPS supports secure protocols that provide similar features. The MPS enables the use of the following secure programs instead of the indicated non-secure programs:

  - The `ssh` program instead of `rlogin` and `telnet`
  - The `scp` program instead of `rcp`
  - The `sftp` program instead of `ftp`

  The MPS enables the use of secure protocols to access the MPS for troubleshooting. These secure protocols ensure that all traffic, including passwords, is encrypted, effectively eliminating eavesdropping, connection hijacking, and other network-level attacks. Additionally, several secure tunneling capabilities and a variety of authentication methods are provided.

Installation and Upgrade

This section provides an overview of MPS installation and upgrade.

Installation and upgrade of the MPS platform software and the applications that run on the MPS are coordinated by the *Customer Care Center* on page 3. Contact the *Customer Care Center* on page 3 to schedule an installation or upgrade.

Installation and Upgrade Media

The MPS operating system is installed or upgraded by either of the following methods:

- Locally install or upgrade from a CD-ROM (Compact Disk-Read Only Memory) that includes a checksum so that the contents are verified before loading. The mate server cannot be installed or upgraded from the CD-ROM in the local server; either the CD-ROM must be inserted into

the mate server or an International Standards Organization (ISO) image of the CD-ROM must be transmitted to the hard disk of the mate server.

- For an initial installation, two CD-ROMs are provided. One CD-ROM contains the platform software and one CD-ROM contains application software.
- For an upgrade, one CD-ROM contains all the software that needs to be upgraded. The CD-ROM contains platform software, application software, or both.

- Remotely install or upgrade from an ISO image of the CD-ROM that has been transmitted to and stored on the local hard disk.

  - For an initial installation, two images are provided. One image contains the platform software and one image contains application software.
  - For an upgrade, one image contains all of the software to be upgraded. This image includes platform software, application software, or both.

Upgrade Features

The upgrade design permits platform and/or application software upgrades to be performed easily and with minimal interruption of service. The following platform upgrade features are supported:

- Each server is upgraded independently and is brought offline during its upgrade. During the upgrade, the other server remains in service.
- If any package is not installed successfully during an upgrade, the entire upgrade is automatically backed out to leave the server in the same state as before the upgrade was initiated.
- A rollback mechanism is provided which can be executed at any time after a successful upgrade. The rollback of a server upgrade will undo all changes made to the server by the upgrade to leave the server in the same state as before the upgrade was initiated.

Diagnostics, Monitoring, and Alarming

The MPS provides the following diagnostic, monitoring, and alarming functions:

- Network diagnostic tools
- Monitoring of the following items:

  - Power
  - Fans
  - Hard drives for free capacity and faults
  - Logical integrity of meta-devices and filesystems
  - IP network core components
  - Operational status of core processes
  - Virtual Memory (VM) subsystem
  - Temperature

- Alarms, as Light-Emitting Diodes (LEDs) or messages, to report problems found by monitoring

For more information about MPS diagnostics, monitoring, and alarming, see *Detecting and Reporting Problems* on page 37.

Disaster Recovery

This section describes how the MPS platform is designed to prevent disastrous problems and to recover from them as efficiently as possible.

- The system disks are mirrored. A single disk failure does not cause system operation to stop.
- Installation is designed to prevent overwriting of existing application partitions.
- Journaling file systems are used for all general-purpose file system disk partitions. In addition to its meta-data, a journaling file system contains a log (or journal) of changes to meta-data. Before any meta-data changes, the changes to be attempted are written to this journal. If a non-clean shutdown occurs, this journal is played back upon reboot so that the meta-data changes occur.

Security

The MPS includes security features at several levels:

- Network access control

  - Only the network ports necessary for remote access or application use are enabled.
  - To reduce the risk of spoofing, all network name resolution occurs only through local files.

- Secure access for user accounts

  - The EPAP GUI displays a banner that explains that the system is for authorized users only and authentication is required for all accounts.
  - When stored, passwords are encrypted.
  - All connection attempts are logged.
  - The customer can assign users to different account types with varying levels of accessibility. For example, some users may be assigned access to only configuration data while others may be assigned access to both configuration data and diagnostic utilities.

- Remote administrative access, which always uses an encrypted protocol

MPS System Network Configuration

The following sections describe the MPS system network configuration.

MPS Network Interfaces

Each MPS server has three added dual-port gigabit Ethernet PCI cards to support network interfaces (see *MPS System Hardware Configuration* on page 13). The MPS software configures the Ethernet interfaces and modifies files to allow the network interfaces to be available to the EPAP application.

Figure 9: MPS Network Connections on page 23 shows the network connections for an MPS system.

Figure 9: MPS Network Connections
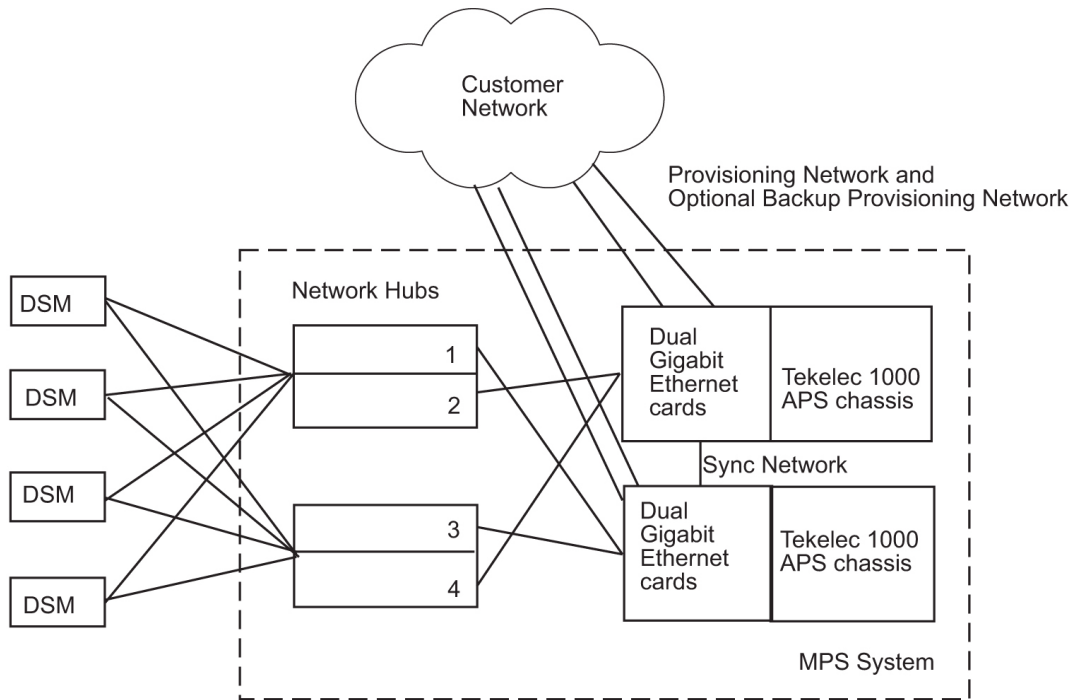
Table 7: MPS Network Interfaces on page 24 describes the network interfaces and how they are used.

Table 7: MPS Network Interfaces

Interface Number	Interface Function	Speed and Routing	Network Description
eth0 (lower port on PCI card 4)	Provisioning network	10/100 BaseT auto-sensing device: • Automatically runs as fast as the customer equipment allows • Precise bandwidth requirements are determined by the customer system configuration and performance requirements This is the only required network attached directly to the customer network. An optional backup provisioning network	This port is available for remote access and carries: • All provisioning information from the customer provisioning system • All traffic required to keep the Real-Time Databases (RTDBs) of the remote MPS systems synchronized

Interface Number	Interface Function	Speed and Routing	Network Description
		can be configured on **eth4**.	
eth1 (upper port on PCI card 4)	Main DSM network (A ports only)	100BaseT half-duplex Internal to EAGLE 5 ISS; not routed	Most of the traffic on this network is Reliable Multicast Transport Protocol (RMTP) II multicast traffic used to keep the Service Module card databases loaded and synchronized. This is the DSM A network.
eth2 (lower port on PCI card 1)	Backup DSM network (B ports only)	10BaseT: • Service Module cards run at 10BaseT • MPS interfaces run at 100BaseT • Ethernet hubs carry out the required rate conversion Internal to EAGLE 5 ISS; not routed	Negligible traffic travels across this network unless the main DSM network fails, in which case this network will carry all traffic normally carried by the main DSM network. This is the DSM B network.
eth3 (upper port on PCI card 1)	Sync network	Full-duplex Gigabit Ethernet Point-to-point network between MPS servers	This network provides a high-bandwidth dedicated communication channel for MPS data synchronization.
eth4 (lower port on PCI card 6)	Backup provisioning network (optional)	10/100 BaseT auto-sensing device: • Automatically runs as fast as the customer equipment allows • Precise bandwidth requirements are determined by the customer system configuration and performance requirements This is an optional network.	This network can be used as a limited backup network to be available for remote access and to carry all provisioning information from the customer provisioning system when the main provisioning network is down. This network path cannot be used as an alternate path for information that is replicated between

Interface Number	Interface Function	Speed and Routing	Network Description
			PDBs or information flowing from PDBs to RTDBs.
eth5 (upper port on PCI card 6)	NOT USED	N/A	N/A

Configuring Network Time Protocol

This section describes the network time protocol (NTP) features and how they are configured for the MPS platform.

Network Time Protocol Overview

Network Time Protocol (NTP) is an Internet protocol used to synchronize clocks of computers to Universal Time Coordinated (UTC) as a time reference. NTP reads a clock provided by a timeserver and transmits the reading to one or more clients; each client adjusts its clock as required. If left unchecked, the system time of a server will drift out of synchronization with other equipment with which it communicates.

Understanding Universal Time Coordinated

Universal Time Coordinated (UTC) is an official standard for determining current time. The UTC second 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.

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

Understanding Network Time Protocol

NTP primary servers provide their clients time that is accurate within a millisecond on a Local Area Network (LAN) and within a few tens of milliseconds on a Wide Area Network (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 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 explicitly 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.
- The stratum hierarchy continues up to the NTP network limit of stratum-15.

Normally, client workstations do not operate as NTP servers. NTP servers with a 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 failed software, hardware, or network links. NTP operates in one or more of the following association modes:

- Client/server mode - A client receives synchronization from one or more servers, but does not provide synchronization to the servers.
- Symmetric mode - Either of two peer servers can synchronize to the other to provide mutual backup.
- Broadcast mode - 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.

Network Time Protocol in the MPS

By default, the MPS A server of each mated MPS pair is configured as a free-running Network Time Protocol (NTP) server which communicates with the mate MPS servers on the provisioning network. Free-running refers to a system that is not synchronized to UTC and receives timing from its own clocking source. This allows mated MPS servers to synchronize their time. *Figure 10: MPS NTP Configuration* on page 27 shows the NTP configuration used by MPS.

Figure 10: MPS NTP Configuration
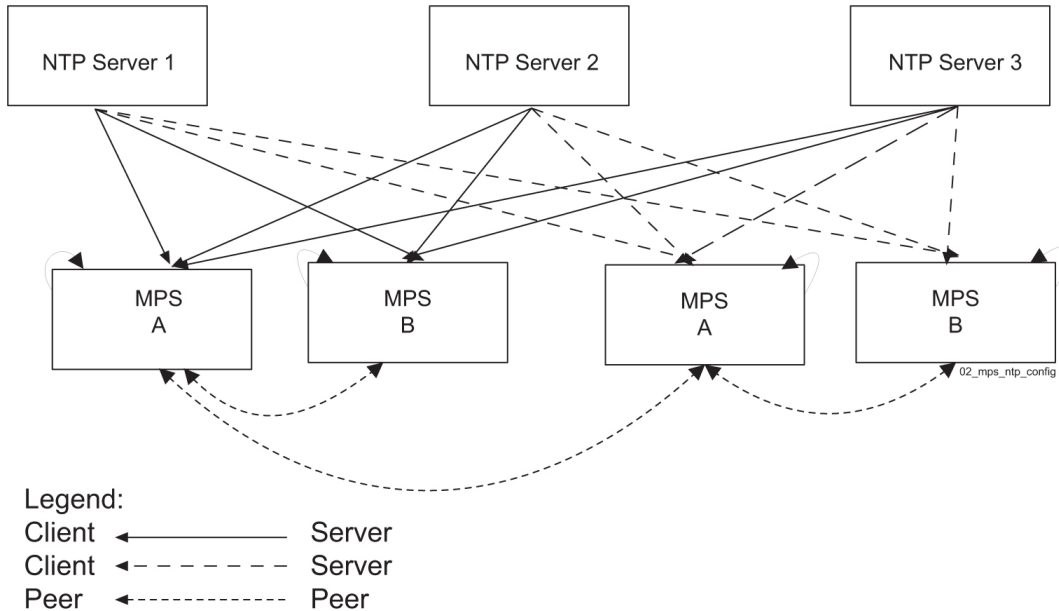
All MPS servers running the EPAP application have the option to be configured through the EPAP GUI to communicate and synchronize time with a customer-defined external NTP time server.

For information about defining an external NTP time server, refer to the *EPAP Administration Manual*.

User and Group Administration

The following users are created during the Initial Product Manufacture (IPM) process:

- `syscheck`

This account is used to execute the `syscheck` utility. The password is `syscheck`. When you log in as the syscheck user, the `syscheck` utility is executed in normal mode; when `syscheck` completes, the session is immediately logged off. This account does not have shell access.

- `tklcppp` (not used)

Fault Tolerance and High Availability

The MPS architecture is designed with the following features to ensure no single point of failure:

- The MPS system uses two MPS servers in an active/standby configuration. If the active server fails, the standby server can service all functions.
- Each frame in which the MPS servers are mounted has four power feeds. Each powered device in the frame has dual power feeds.
- Each MPS server is connected to the EAGLE 5 ISS with redundant networks.
- The EAGLE 5 ISS is replicated by a mate EAGLE 5 ISS, which has its own MPS system consisting of two MPS servers. These MPS servers are synchronized with the MPS servers of the mate EAGLE 5 ISS.

Chapter

3

MPS Maintenance

Topics:

This chapter provides maintenance information, problem detection description, and general recovery procedures for the T1000-based Multi-Purpose Server.

Introduction

This chapter provides preventive and corrective maintenance information. Customers perform a small number of daily and monthly preventive maintenance tasks. The MPS system and the EPAP application perform automatic monitoring and problem reporting.

This chapter also presents an overview of how to recover from reported problems. Detailed information about recovery procedures is contained in the remaining chapters of this manual.

Preventive Maintenance

Tekelec recommends using the Automatic PDB/RTDB Backup feature to backup all data stored in the PDB/RTDB. The Automatic PDB/RTDB Backup feature automates the process of creating backups of the PDB and RTDB databases at the time, frequency, and to the destination configured by the user. The Automatic PDB/RTDB Backup feature replaces all procedures listed under the Daily maintenance procedures. Refer to the EPAP *Administration Manual* to configure the Automatic PDB/RTDB Backup feature.

The recommended daily maintenance procedures are described in *Daily Maintenace Procedures* on page 30.

The maintenace procedures to perform monthly are described in *Monthly Maintenance Procedures* on page 36.

Daily Maintenace Procedures

Tekelec recommends that the Automatic PDB/RTDB Backup feature be used to backup all data stored in the PDB/RTDB. The manual backup procedures are included in this section if the database backup needs to be performed manually. Storing database backups in a secure off-site location ensures the ability to recover from system failures.

This section describes the following recommended daily maintenance procedures:

- *Backing Up the RTDB* on page 30
- *Backing Up the PDB* on page 34
- *Transferring RTDB and PDB Backup Files* on page 35

Backing Up the RTDB

Perform this procedure once each day. The estimated time required to complete this procedure is one hour.

1. Log in to the EPAP GUI on MPS A as the **epapall** user.

   For information about how to log in to the EPAP GUI, refer to *Accessing the EPAP GUI Interface* on page 120.

2. If you are not logged in to EPAP A, select the **Select Mate** option.

3. From the EPAP Menu, select **Process Control>Stop Software**.

4. In the Stop EPAP Software screen as shown in *Figure 11: Stop EPAP Software* on page 31, click **Stop EPAP Software**.

Note: DO NOT select the option to stop the PDB along with the EPAP software.

Figure 11: Stop EPAP Software
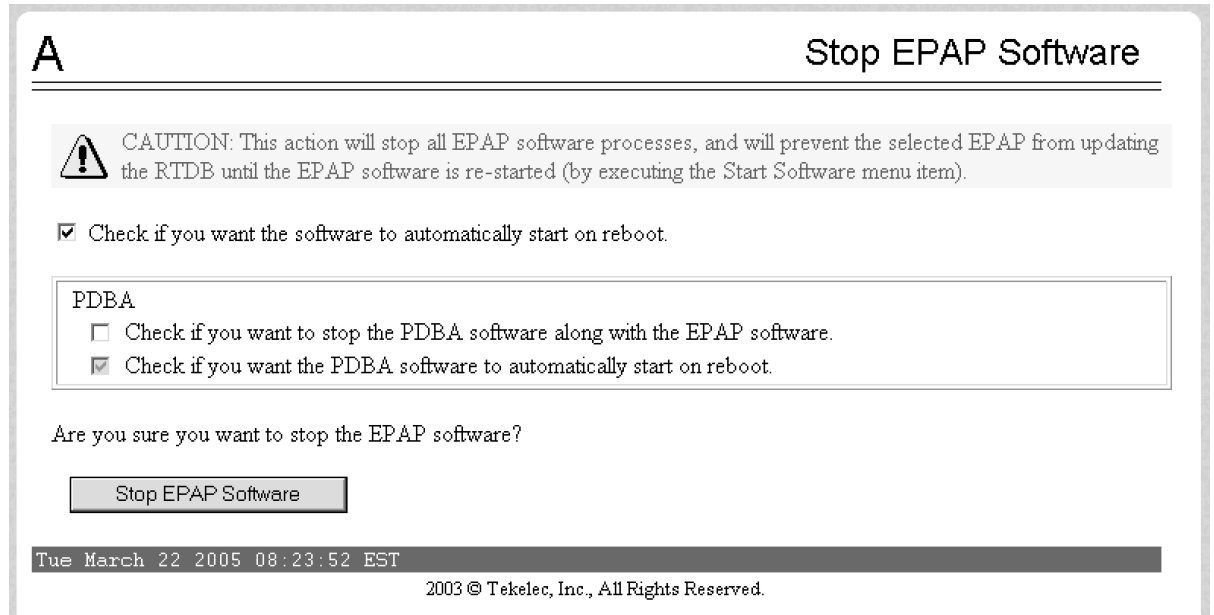
After the EPAP software has stopped successfully, the screen shown in *Figure 12: EPAP Software Successfully Stopped* on page 31 is displayed.

Figure 12: EPAP Software Successfully Stopped

5. From the EPAP menu, select **RTDB>Maintenance>Backup RTDB** .

The screen shown in *Figure 13: Backup the RTDB* on page 31 is displayed.

Figure 13: Backup the RTDB
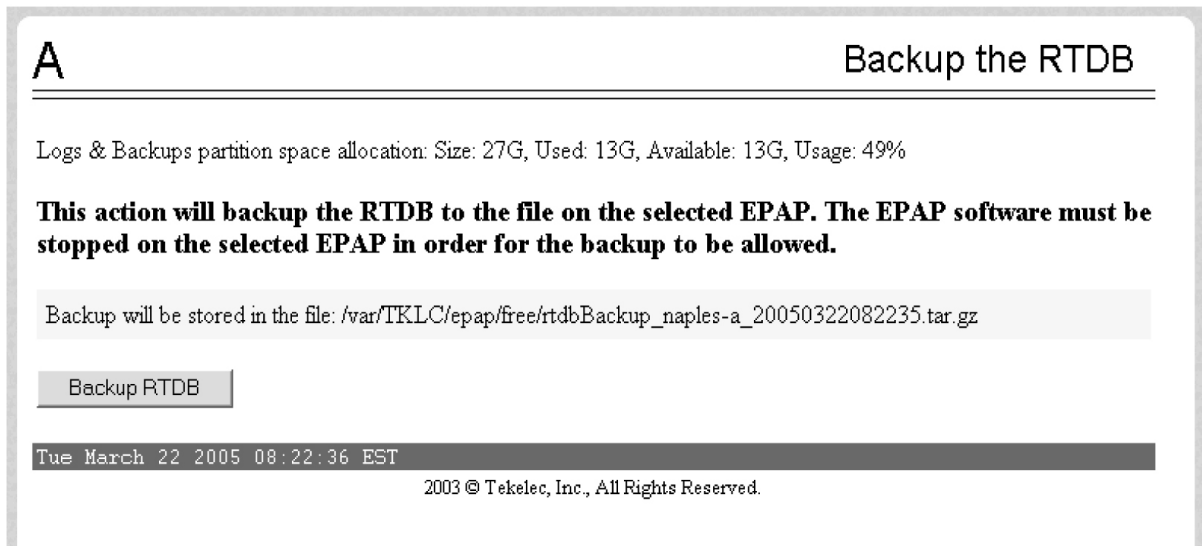
6. Record the file name as shown in this example:

```
/var/TKLC/epap/free/rtdbBackup_naples-a20050322082516.tar.gz
```

7. Click **Backup RTDB** .

The screen shown in *Figure 14: Backup the RTDB Confirmation* on page 32 displays a request for confirmation.

Figure 14: Backup the RTDB Confirmation
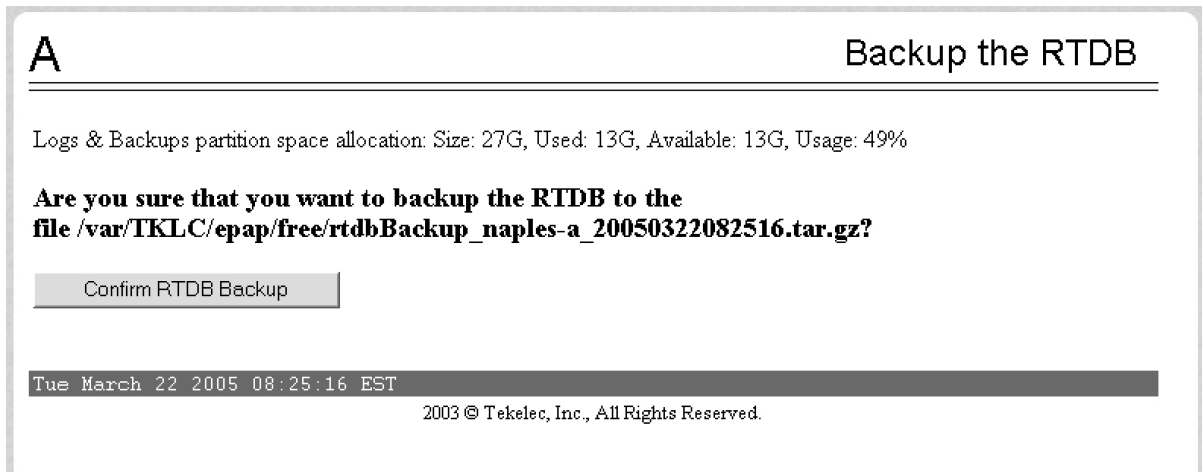
8. Click **Confirm RTDB Backup**.

If the backup starts successfully, the following message scrolls through the GUI banner:

```
Backup RTDB in progress.
```

After the backup completes successfully, the screen shown in *Figure 15: Backup the RTDB - Success* on page 32 is displayed.

Figure 15: Backup the RTDB - Success

9. Select **Process Control>Start Software** from the EPAP Menu.
10. On the Start EPAP Software screen shown in *Figure 16: Start EPAP Software* on page 33, click **Start EPAP Software**.

Figure 16: Start EPAP Software
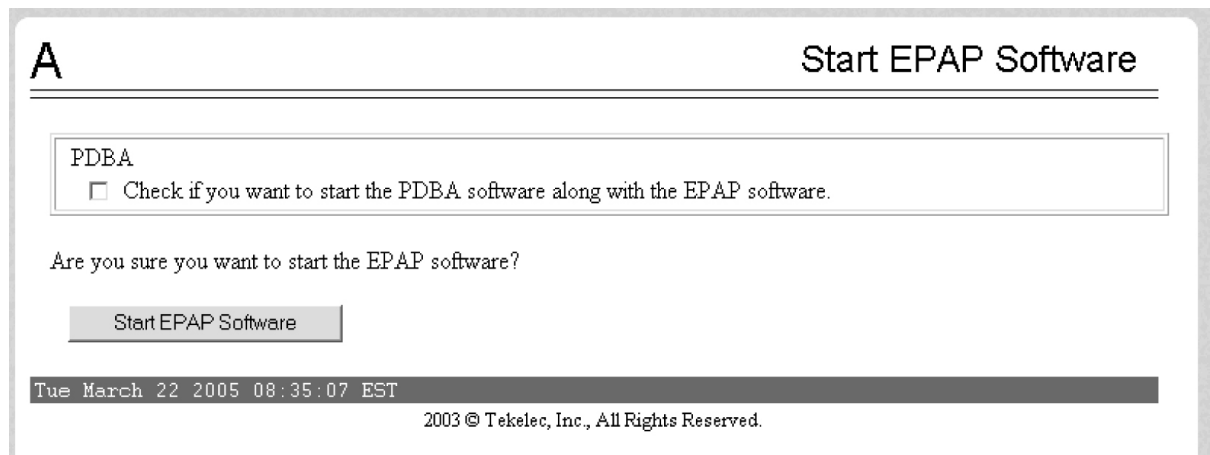
After the EPAP software has started successfully, the screen in *Figure 17: Start EPAP Software - Success* on page 33 is displayed.

Figure 17: Start EPAP Software - Success

11. This procedure is complete. Continue to *Backing Up the PDB* on page 34.

Backing Up the PDB

Perform this procedure once each day. The estimated time required to complete this procedure is one hour. PDB provisioning can take place while this procedure is being performed.

Note: Ensure that you perform this procedure on the same server on which you performed *Backing Up the RTDB* on page 30. Ensure that you performed *Backing Up the RTDB* on page 30 first so that the RTDB backup level will be lower than the associated PDB backup level.

1. Log in to the EPAP GUI on MPS A as the **epapall** user.

For information about how to log in to the EPAP GUI, refer to *Accessing the EPAP GUI Interface* on page 120.

2. If you are not logged in to EPAP A, select the **Select Mate** option.

3. From the EPAP Menu, select **PDBA>Maintenance>Backup>Backup the PDB**.

4. In the **Backup the PDB** screen shown in *Figure 18: Backup the PDB* on page 34, click **Backup PDB**.

Figure 18: Backup the PDB

The resulting screen, shown in *Figure 19: Backup PDB Confirmation* on page 34, displays a button to confirm the request to backup the PDB and the file name.

Figure 19: Backup PDB Confirmation

.
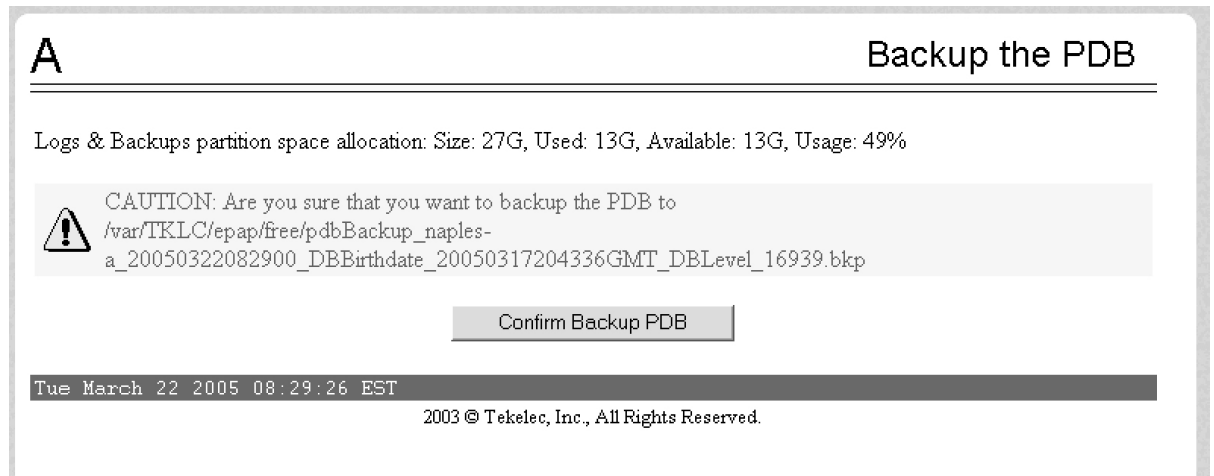
5. Record the file name.

   In this example, the file name is:

   `/var/TKLC/epap/free/pdbBackup_naples-a_20050322082900_DBBirthdate_20050317204336GMT_DBLevel_16939.bkp`

6. Click **Confirm Backup PDB**.

   While the backup is running, the following message scrolls through the GUI banner:

   `Backup PDB in progress.`

   After the backup completes successfully, the screen shown in *Figure 20: Backup the PDB - Success* on page 35 is displayed:

   Figure 20: Backup the PDB - Success

7. This procedure is complete. Continue to *Transferring RTDB and PDB Backup Files* on page 35.

Transferring RTDB and PDB Backup Files

Perform this procedure once each day. The time required to complete this procedure depends on network bandwidth. File sizes can be several gigabytes for each database.

1. Log in to the EPAP command line interface with user name `epapdev` and the password associated with that user name.

2. Use the Secure File Transfer Protocol (`sftp`) to transfer the following files to a remote, safe location:

   a) The RTDB backup file, whose name was recorded in *Step 6* on page 32 of *Backing Up the RTDB* on page 30

   b) The PDB backup file, whose name was recorded in *Step 5* on page 35 of *Backing Up the PDB* on page 34

Monthly Maintenance Procedures

Tekelec recommends performing the following procedures once a month.

- *Replacing Fan Filters* on page 36
- *Verifying Modems* on page 37

Replacing Fan Filters

Tekelec recommends replacing filters once a month. The filter may be replaced more often if the operating environment requires more frequent changes. Use the following procedure to replace a filter.

1. Using a Phillips screwdriver, remove the front fascia of the Tekelec 1000 AS chassis by loosening the four spring-loaded captive 1/4 turn screws.

   See *Figure 21: Tekelec 1000 AS Front Fascia Fasteners* on page 36.

   Figure 21: Tekelec 1000 AS Front Fascia Fasteners

Captive Fasteners
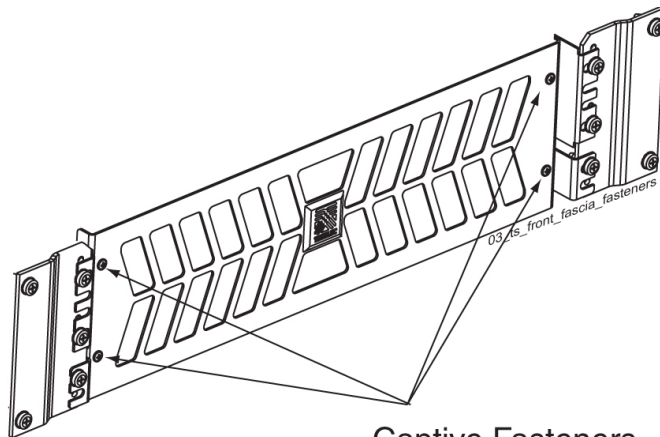
   Note: Fan filters can be removed from the chassis without turning off the power. A finger-safe perforated panel separates the moving fans from the filters. The Tekelec 1000 AS chassis does not have to be extended from the frame for this procedure.

2. Remove the old filter and discard it.

3. Insert the new filter (P/N 551-0022-01).

> **Note:** The filter has an arrow to indicated direction of airflow. The arrow points toward the rear of the chassis when installed correctly.

4. Using a Phillips screwdriver, replace the front fascia by tightening the four spring-loaded captive 1/4 turn screws.

> **Note:** Locate the TOP label, visible from the back of the fascia, to orient the fascia when replacing it on the chassis.

Verifying Modems

Use the following procedure once a month to verify that the modems are operational. Correct operation of the modems is necessary if a problem occurs that requires the attention of the *Customer Care Center* on page 3 and their ability to dial in to the MPS system.

1. Using dial-in/terminal emulation software, initiate a session to each server that contains a modem by dialing the access number assigned to the analog line connected to the internal modem card (in PCI slot 7).

    For information about which servers contain modems, see *MPS System Hardware Configuration* on page 13.

2. Log in with user name `syscheck` and password `syscheck` (see *Running syscheck Using the syscheck Login* on page 124).

    *   If the modem is operational, this login executes the System Health Check utility `syscheck`. When `syscheck` completes, it immediately logs out and disconnects the dial-up session.
    *   If the login does not work, contact the *Customer Care Center* on page 3.

3. Exit the terminal emulation software.

Detecting and Reporting Problems

Problems are detected and reported by the MPS platform and the EPAP application.

*   The MPS platform constantly monitors its operational status using the System Health Check utility `syscheck`. This utility can be initiated also by the user. For more details about `syscheck`, see *System Health Check Overview* on page 41.

    If `syscheck` detects a fault or error, the user is notified by:

    *   The appropriate alarm LED illuminated on the front of the MPS server (see *MPS Alarm LEDs* on page 38).
    *   An alarm message sent to the MPS application which:

        *   displays the alarm on the application GUI (see *Displaying Errors on EPAP GUI* on page 39).
        *   sends the alarm message to the EAGLE 5 ISS which sends a UAM to the operator screen to notify the user (see *MPS UAMs* on page 40).

- The `syscheck` test results logged to a file available for the *Customer Care Center* on page 3. If logs are to be saved to send to the *Customer Care Center* on page 3, see *Saving Logs Using the EPAP GUI* on page 125.

- The EPAP application running on the MPS server can detect application errors. If an application problem is detected, the user is notified by:

  - The appropriate alarm LED illuminated on the front of the MPS server (see *MPS Alarm LEDs* on page 38).

  - An error displayed on the graphical user interface (GUI) banner (see *Displaying Errors on EPAP GUI* on page 39).

  - An error sent to to the EAGLE 5 ISS, which reports the error as a UAM alarm (see *MPS UAMs* on page 40).

  - The error recorded in an application log file. If logs are to be saved to send to the *Customer Care Center* on page 3, see *Saving Logs Using the EPAP GUI* on page 125.

MPS Alarm LEDs

The front of the MPS server has three LEDs to indicate alarms, as shown in *Figure 22: MPS Alarm LEDs* on page 38.

Figure 22: MPS Alarm LEDs
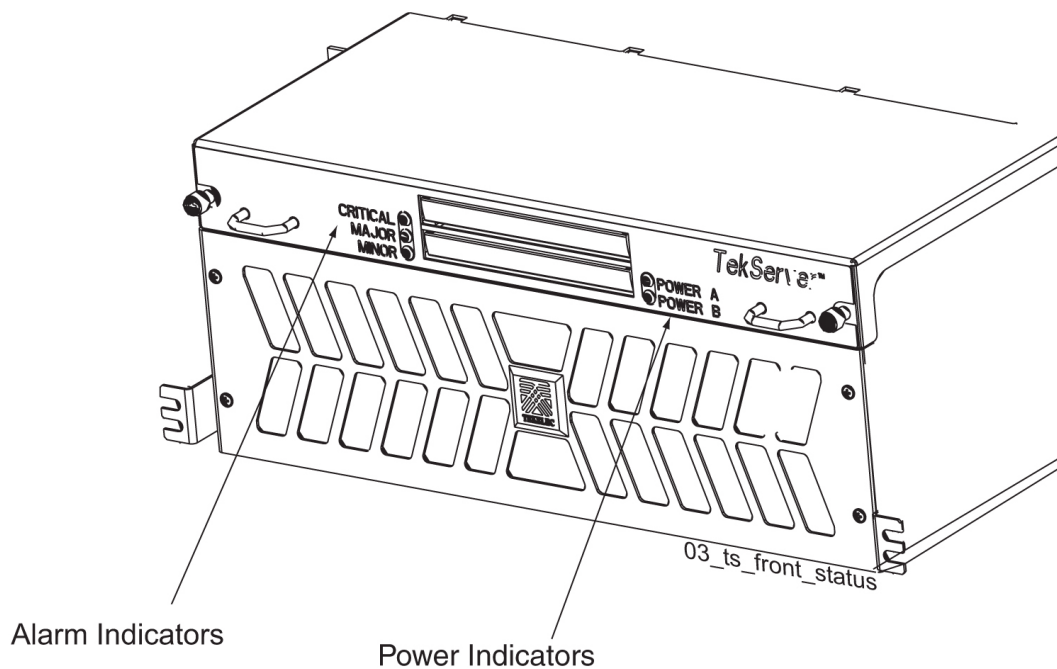
The alarms indicate the state of the MPS, as indicated in *Table 8: MPS Alarm LED Indications* on page 39.

Table 8: MPS Alarm LED Indications

Alarm LED	Color	Indication
Critical	Green	No critical platform or application alarms currently exist.
	Red	One or more critical platform or application alarms currently exist.
Major	Green	No major platform or application alarms currently exist.
	Red	One or more major platform or application alarms currently exist.
Minor	Green	No minor platform or application alarms currently exist.
	Amber	One or more minor platform or application alarms currently exist.

An alarm LED remains red or amber while an error condition remains active for that severity level. If alarm conditions are active for more than one platform alarm level, every applicable LED is illuminated red or amber, not only the most severe alarm level.

Figure 22: MPS Alarm LEDs on page 38 shows the LEDs that correspond to the platform alarm categories.

Displaying Errors on EPAP GUI

If the EPAP application detects an application error or receives an alarm message from the MPS platform layer, the EPAP application displays the error on the graphical user interface (GUI):

- With a text message running across the banner.
- By illuminating the alarm level indicator on the GUI that corresponds to the alarm level of the error. If that alarm level indicator is already illuminated, the number shown on the indicator is incremented. For details about the alarms represented by the indicator, click the alarm button.

Figure 23: Errors Displayed on EPAP GUI on page 39 shows an example of errors displayed on the EPAP GUI.

Figure 23: Errors Displayed on EPAP GUI
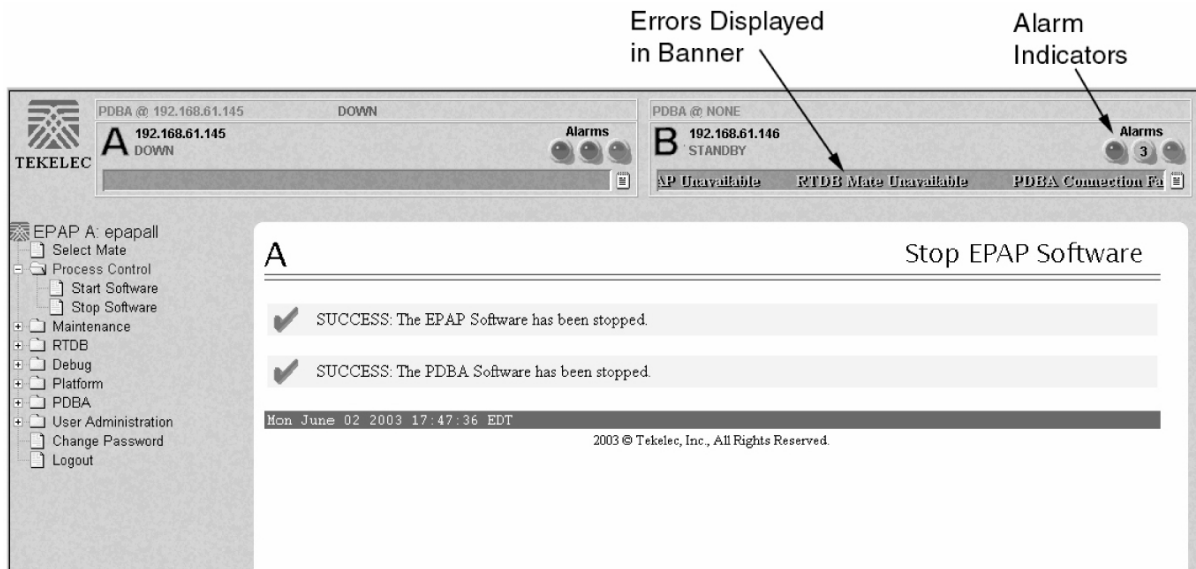
To obtain additional information about the alarms, click any lighted alarm indicator. A pop-up window is displayed, showing the number of each type of alarm and listing the text of each existing alarm in each type. *Figure 24: Viewing Alarm Details* on page 40 shows an example.

Figure 24: Viewing Alarm Details
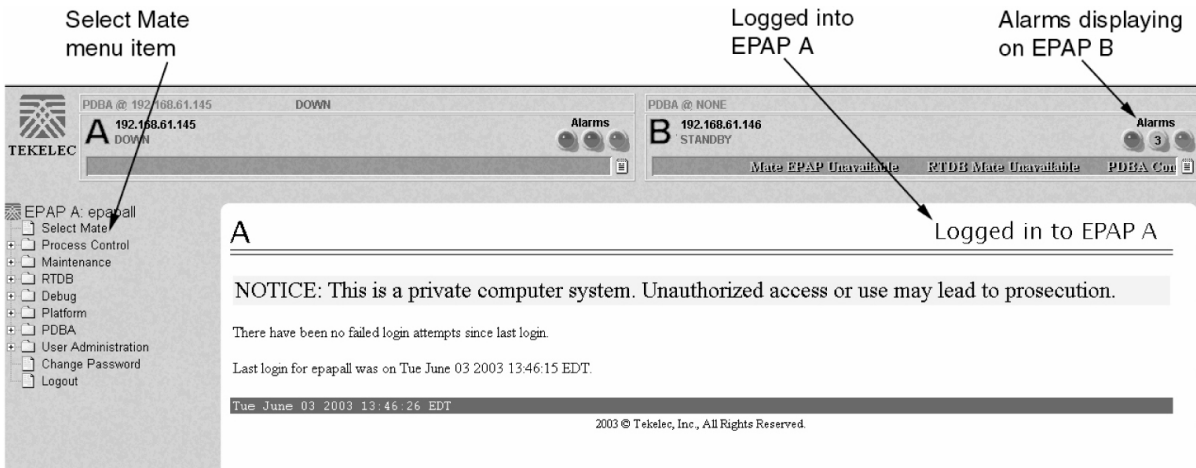
When an alarm value in the Alarm View popup window represents multiple alarms, as shown in *Figure 24: Viewing Alarm Details* on page 40, the text of each of the alarms being reported is displayed. The individual alarm text is found in *Table 10: Platform and Application Alarms* on page 56. To correct the alarm condition, perform the associated procedure described in *MPS Alarm Recovery Procedures* on page 60.

MPS UAMs

The EAGLE 5 ISS displays only one alarm per EPAP at a time based on the highest priority. If a single error is detected, the EPAP application sends an error message to the EAGLE 5 ISS terminal to report the active alarm category. If multiple errors are detected, the EPAP application sends an error message to the EAGLE 5 ISS terminal to report the most severe active alarm category.

If multiple alarms of the same severity exist and their severity is the highest alarm severity currently active, a combination alarm code is sent to the EAGLE 5 ISS. The EAGLE 5 ISS issues the appropriate UAM to the operator.

Errors detected in the MPS hardware and software are reported by the following UAMs, which are described in greater detail in *Unsolicited Alarm and Information Messages*.

- Critical Platform Alarms are reported by the EAGLE 5 ISS in UAM 0370.
- Critical Application Alarms are reported to the EAGLE 5 ISS in UAM 0371.
- Major Platform Alarms are reported to the EAGLE 5 ISS in UAM 0372.
- Major Application Alarms are reported to the EAGLE 5 ISS in UAM 0373.
- Minor Platform Alarms are reported to the EAGLE 5 ISS in UAM 0374.
- Minor Application Alarms are reported to the EAGLE 5 ISS in UAM 0375.

When all error conditions are corrected for all MPS platform errors and application errors, the operator receives this UAM:

```
UAM 0250 MPS available.
```

For information about the alarm data contained in UAMs, see *MPS Platform and Application Alarms* on page 55.

System Health Check Overview

The MPS runs a self-diagnostic utility program called `syscheck` to monitor itself. The system health check utility `syscheck` tests the server hardware and platform software. Checks and balances verify the health of the MPS server and platform software for each test, and verify the presence of required application software.

If the `syscheck` utility detects a problem, an alarm code is generated. The alarm code is a 16-character data string in hexadecimal format. All alarm codes are ranked by severity: critical, major, and minor. *Table 10: Platform and Application Alarms* on page 56 lists the platform alarms and their alarm codes.

The `syscheck` output can be in either of the following forms (see *Health Check Outputs* on page 44 for output examples):

- Normal— results summary of the checks performed by `syscheck`
- Verbose—detailed results for each check performed by `syscheck`

The `syscheck` utility can be run in the following ways:

- The operator can invoke `syscheck` :
  - From the EPAPGUI Platform Menu (see *Accessing the EPAP GUI Interface* on page 120). The user can request `Normal` or `Verbose` output.
  - By logging in as a `syscheck` user (see *Running syscheck Using the syscheck Login* on page 124). Only `Normal` output is produced.
- `syscheck` runs automatically by timer at the following frequencies:
  - Tests for critical platform errors run automatically every 30 seconds.

- Tests for major and minor platform errors run automatically every 60 seconds.

Functions Checked by syscheck

Table 9: System Health Check Operation on page 42 summarizes the functions checked by syscheck.

Table 9: System Health Check Operation

System Check	Function
Disk Access	Verify disk read and write functions continue to be operable. This test attempts to write test data in the file system to verify disk operability. If the test shows the disk is not usable, an alarm is reported to indicate the file system cannot be written to.
Smart	Verify that the smartd service has not reported any problems.
File System	Verify the file systems have space available to operate. Determine what file systems are currently mounted and perform checks accordingly. Failures in the file system are reported if certain thresholds are exceeded, if the file system size is incorrect, or if the partition could not be found. Alarm thresholds are reported in a similar manner.
Swap Space	Verify that disk swap space is sufficient for efficient operation.
Memory	Verify that 2 GB of RAM is installed.
Network	Verify that all ports are functioning by pinging each network connection (provisioning, sync, and DSM networks). Check the configuration of the default route.
Process	Verify that the following critical processes are running. If a program is not running the minimum required number of processes, an alarm is reported. If more than the recommended processes are running, an alarm is also reported. • sshd (Secure Shell daemon) • ntpd (NTP daemon) • syscheck (System Health Check daemon)
Hardware Configuration	Verify that the processor is running at an appropriate speed and that the processor matches what is required on the server. Alarms

System Check	Function
	are reported when a processor is not available as expected.
Cooling Fans	Verify that all fans are running within the expected revolutions per minute (rpm) range. Cooling fans ensure that the components on the server operate at the optimum temperature. Each server has six fans. All cooling fans are checked for fan failure.
Main Power Feeds	Verify that: • Main power is supplied to both server power inputs. • Power supplies are working properly.
Power Relay Unit	Verify that all configured power feeds are within specification. Verify that no breakers have opened (tripped). The breaker panel has a set of relays that allow information about the breaker panel status to be sent to all attached servers. The syscheck utility monitors this information. The following error conditions can be detected: • Breaker Panel Breaker Error: To recover, verify all breakers and power feeds (see *3000000002000000 - Breaker Panel Breaker Error* on page 79). • Breaker Panel Feed Error: To recover, verify that the breaker panel monitoring cable is installed correctly and is not damaged (see *3000000001000000 - Breaker Panel Feed Error* on page 76).
Voltages	Measure all monitored voltages on the server mainboard. Verify that all monitored voltages are within the expected operating range.
Temperature	Measure the following temperatures and verify that they are within a specified range. • Air temperature • Processors internal temperature
MPS Platform	Provide alarm if internal diagnostics detect any other error, such as MPSsyscheck script failures.

Health Check Outputs

System health check utility `syscheck` output can be Normal (brief) or Verbose (detailed), depending upon how `syscheck` was initiated. The following examples show Normal and Verbose output formats.

Normal Output

Following is an example of Normal output:

```
Running modules in class disk...
                                OK
Running modules in class hardware...
                                OK
Running modules in class net...
                                OK
Running modules in class proc...
                                OK
Running modules in class system...
                                OK
The log is available at:
  -->/var/TKLC/log/syscheck/fail_log
```

Verbose Output Containing Errors

If an error occurs, the system health check utility `syscheck` provides alarm data strings and diagnostic information for platform errors in its output. The following portion of Verbose output contains detected errors with the breaker panel and the numbers of running modules.

```
Running modules in class disk...
        fs: Current file space use in "/" is 38%.
        fs: Current Inode used in "/" is 38%.
        fs: Current file space use in "/boot" is 12%.
        fs: Current Inode used in "/boot" is 1%.
        fs: Current file space use in "/usr" is 25%.
        fs: Current Inode used in "/usr" is 9%.
        fs: Current file space use in "/var" is 20%.
        fs: Current Inode used in "/var" is 4%.
        fs: Current file space use in "/var/TKLC" is 21%.
        fs: Current Inode used in "/var/TKLC" is 1%.
        fs: Current file space use in "/tmp" is 4%.
        fs: Current Inode used in "/tmp" is 1%.
        fs: Current file space use in "/var/TKLC/epap/rt" is 3%.
        fs: Current Inode used in "/var/TKLC/epap/rt" is 1%.
        fs: Current file space use in "/var/TKLC/epap/db" is 65%.
        fs: Current Inode used in "/var/TKLC/epap/db" is 1%.
        fs: Current file space use in "/var/TKLC/epap/logs" is 2%.
        fs: Current Inode used in "/var/TKLC/epap/logs" is 1%.
        fs: Current file space use in "/var/TKLC/epap/free" is 1%.
        fs: Current Inode used in "/var/TKLC/epap/free" is 1%.
        fs: Return string: "OK"
      meta: Checking md status on system.
      meta: md Status OK, with 11 active volumes.
      meta: Checking md configuration on system.
      meta: Server md configuration OK.
      meta: Return string: "OK"
      swap: Checking amount of swap space on server.
      swap: Swap space is OK.
      swap: Swap available:  16736200
      swap: /sbin/swapon -s output ->
```

```
      swap: FilenameTypeSizeUsedPriority
      swap: /dev/md3                partition205624801000
      swap: /var/TKLC/swap/swap.1   file209713601
      swap: /var/TKLC/swap/swap.2   file209713602
      swap: /var/TKLC/swap/swap.3   file209713603
      swap: /var/TKLC/swap/swap.4   file209713604
      swap: /var/TKLC/swap/swap.5   file209713605
      swap: /var/TKLC/swap/swap.6   file209713606
      swap: /var/TKLC/swap/swap.7   file209713607
      swap: Return string: "OK"
     write: Successfully read from file system "/".
     write: Successfully read from file system "/boot".
     write: Successfully read from file system "/usr".
     write: Successfully read from file system "/var".
     write: Successfully read from file system "/var/TKLC".
     write: Successfully read from file system "/var/TKLC/swap".
     write: Successfully read from file system "/tmp".
     write: Successfully read from file system "/var/TKLC/epap/rt".
     write: Successfully read from file system "/var/TKLC/epap/db".
     write: Successfully read from file system "/var/TKLC/epap/logs".
     write: Successfully read from file system "/var/TKLC/epap/free".
     write: Return string: "OK"
     smart: Finished examining logs for disk: hdc.
     smart: Finished examining logs for disk: hda.
     smart: SMART status OK.
     smart: Return string: "OK"
                                    OK
Running modules in class hardware...
fancontrol: Return string: "OK"
breaker: Module is disabled.
cmosbattery: Return string: "OK"
       fan: Server Fan Status OK.
       fan: Return string: "OK"
    powera: Return string: "OK"
    powerb: Return string: "OK"
      temp: Return string: "OK"
   voltage: Return string: "OK"
                                    OK
Running modules in class net...
defaultroute: Module is disabled.
ping: Module is disabled.
                                    OK
Running modules in class proc...
       ntp: *mate            LOCAL(0)        14 u   14   64   377    0.229
0.579   0.062
       ntp: Return string: "OK"
       run: Checking smartd...
       run: Found 1 instance(s) of the smartd process.
       run: Checking atd...
       run: Found 1 instance(s) of the atd process.
       run: Checking crond...
       run: Found 1 instance(s) of the crond process.
       run: Checking sshd...
       run: Found 3 instance(s) of the sshd process.
       run: Checking syscheck...
       run: Found 1 instance(s) of the syscheck process.
       run: Checking syslogd...
       run: Found 1 instance(s) of the syslogd process.
       run: Checking maint...
       run: Found 1 instance(s) of the maint process.
       run: Checking rtdb...
       run: Found 1 instance(s) of the rtdb process.
       run: Checking topnode...
       run: Found 2 instance(s) of the topnode process.
       run: Checking prov...
```

```
        run: Found 1 instance(s) of the prov process.
        run: Checking provRMTP...
        run: Found 4 instance(s) of the provRMTP process.
        run: Checking provRcvr...
        run: Found 4 instance(s) of the provRcvr process.
         run: Checking pdba...  * run: ::MINOR:: 5000000000000002 -- Server
Application Process Error
        run: Only 0 instance(s) of pdba running. 1 instance(s) required!
        run: Checking exinit...
        run: Found 1 instance(s) of the exinit process.
        run: Checking gs...
        run: Found 1 instance(s) of the gs process.
        run: Checking mysqld...
        run: Found 16 instance(s) of the mysqld process.
        run: Checking httpd...
        run: Found 1 instance(s) of the httpd process.
      run: Return string: "Absolute threshold of running processes was not met."
One or more module in class "proc" FAILED
Running modules in class system...
        cpu: Found "4" CPU(s)... OK
        cpu: CPU 0 is on-line... OK
        cpu: CPU 0 speed: 1999.800 MHz... OK
        cpu: CPU 1 is on-line... OK
        cpu: CPU 1 speed: 1999.800 MHz... OK
        cpu: CPU 2 is on-line... OK
        cpu: CPU 2 speed: 1999.800 MHz... OK
        cpu: CPU 3 is on-line... OK
        cpu: CPU 3 speed: 1999.800 MHz... OK
        cpu: Return string: "OK"
        mem: Expected memory found
        mem: Skipping minimum expected memory check.
        mem: 2111262720 bytes (~2013.45703125 Mb) of RAM installed.
        mem: Return string: "OK"
                              OK
Failures occured during system check. The failure log is available at:
  -->/var/TKLC/log/syscheck/fail_log
```

Note: If an error occurs, the syscheck output also includes the alarm number and text that is generated. The example above highlights the alarm in bold text. For the explanation of alarm codes in the alarm strings and how to respond to them, refer to *MPS Platform and Application Alarms* on page 55.

Recovering from Problems

This section describes the following recovery procedures:

- *Restoring Databases from Backup Files* on page 46
- *Recovering From Alarms* on page 51

Restoring Databases from Backup Files

This section describes how to restore the RTDB, PDB, or both from backup files:

- *Restoring the RTDB from Backup Files* on page 47

- *Restoring the PDB from Backup Files* on page 49

Restoring the RTDB from Backup Files

To restore the EPAP RTDB from a backup file, contact the *Customer Care Center* on page 3.

Note: Tekelec recommends that the RTDB be backed up daily (see section, *Backing Up the RTDB* on page 30). The RTDB for EPAP Release 5.3 and later cannot be restored from backups made on an EPAP release earlier than 5.3.

Use the following procedure to restore the RTDB from a previously prepared backup file.

> ⚠ **CAUTION:** Contact the *Customer Care Center* on page 3 before performing this procedure.
> **CAUTION**

1. Log in to the EPAP command line interface with user name `epapdev` and the password associated with that user name.
2. Use the Secure File Transfer Protocol (`sftp`) to transfer the RTDB backup file, whose name was recorded in *Step 6* on page 32 of *Backing Up the RTDB* on page 30, to the following location:

```
/var/TKLC/epap/free/
```

3. Log in to the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120).
4. Select **Process Control>Stop Software** to ensure that no other updates are occurring.

    The screen shown in *Figure 25: Stop EPAP Software* on page 47 is displayed.

    Figure 25: Stop EPAP Software
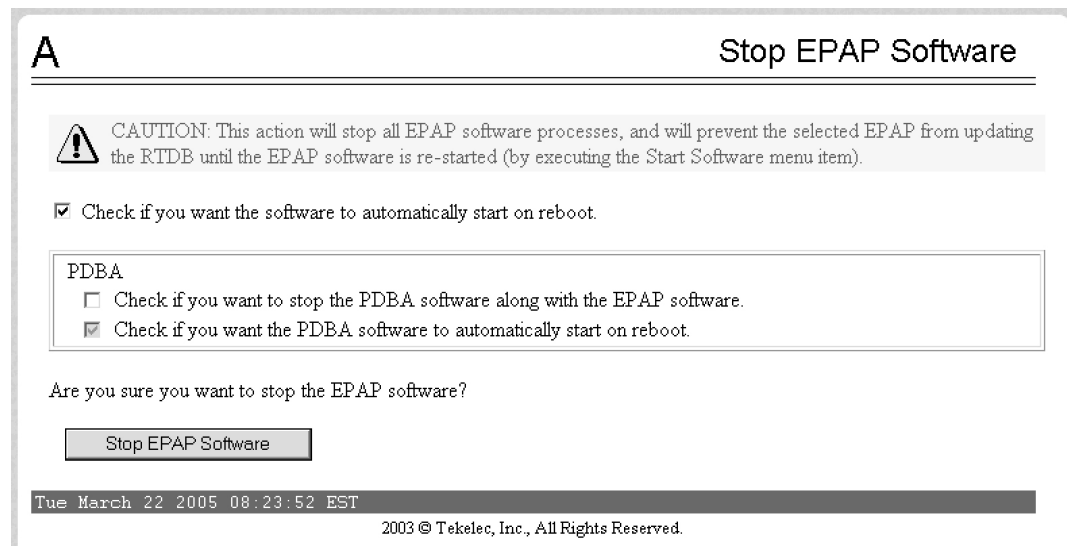
    When the software on the selected EPAP has stopped, the screen shown in in *Figure 26: Stop EPAP Software - Success* on page 47 is displayed.

    Figure 26: Stop EPAP Software - Success

5. Select **RTDB>Maintenance>Restore RTDB** .

   The screen shown in *Figure 27: Restoring the RTDB* on page 48 is displayed.

Figure 27: Restoring the RTDB
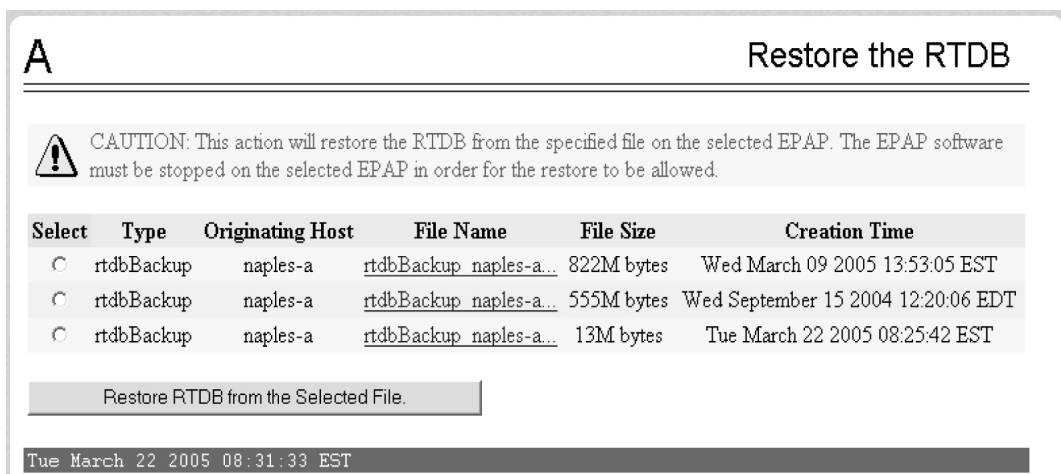
6. On the screen shown in *Figure 27: Restoring the RTDB* on page 48, select the file that was transferred in *Step 2* on page 47. Click **Restore the RTDB from the Selected File**.

7. To confirm restoring a file, click **Confirm RTDB Restore** as shown on the Restore the RTDB screen as shown in *Figure 28: Restore the RTDB Confirm* on page 48.

Figure 28: Restore the RTDB Confirm
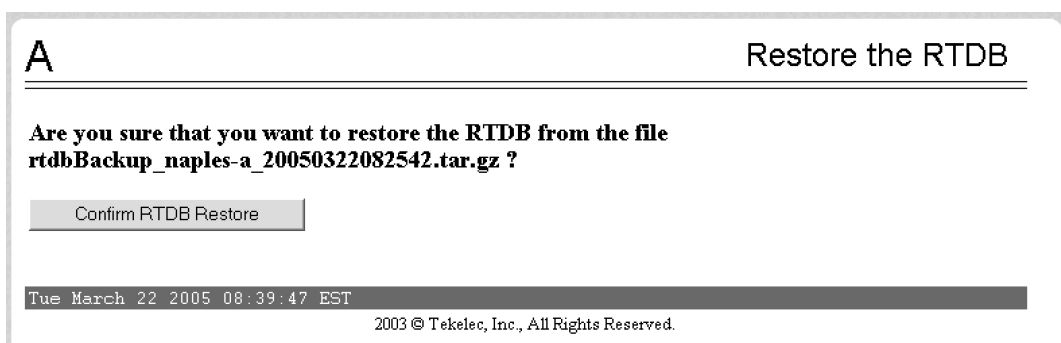
After the file is restored successfully, the screen shown in *Figure 29: Restore the RTDB - Success* on page 48 is displayed.

Figure 29: Restore the RTDB - Success

A   Restore the RTDB

✔ SUCCESS: Successfully started restore of RTDB from file rtdbBackup_naples-a_20050322082542.tar.gz.
   Restore status will be displayed on Banner message window.

Tue March 22 2005 08:40:13 EST
                              2003 © Tekelec, Inc., All Rights Reserved.
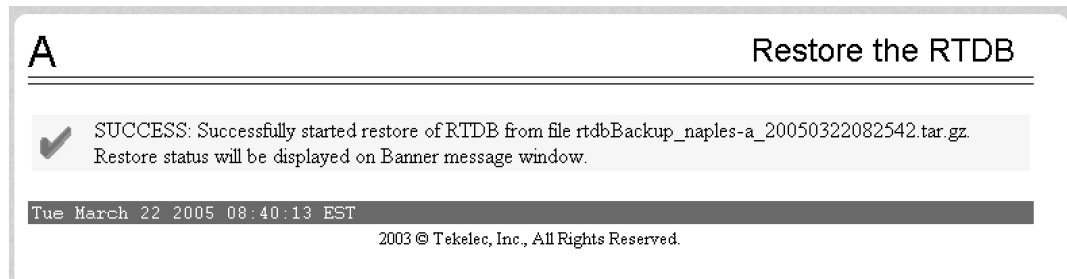
Restoring the PDB from Backup Files

To restore the EPAP PDB from a backup file, contact *Customer Care Center* on page 3.

Note: Tekelec recommends that the PDB be backed up daily (see section, *Backing Up the PDB* on page 34).

Use the following procedure to restore the PDB from a previously prepared backup file.

⚠ **CAUTION:** Contact the *Customer Care Center* on page 3 before performing this procedure.
CAUTION

1. Log in to the EPAP command line interface with user name `epapdev` and the password associated with that user name.
2. Use the Secure File Transfer Protocol (`sftp`) to transfer the PDB backup file, whose name was recorded in *Step 5* on page 35 of *Backing Up the PDB* on page 34, to the following location:

    ```
    /var/TKLC/epap/free/
    ```

3. Log in to the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120).
4. Select **Process Control>Stop Software** to ensure that no other updates are occurring.

    The screen shown in *Figure 30: Stop EPAP Software* on page 49 is displayed.

    Figure 30: Stop EPAP Software

When the software on the selected EPAP has stopped, the screen in *Figure 31: Stop EPAP Software - Success* on page 50 is displayed.

Figure 31: Stop EPAP Software - Success

5. Select **PDBA>Maintenance>Backup>Restore the PDB** .

   The screen shown in *Figure 32: Restoring the PDB* on page 50 is displayed.

Figure 32: Restoring the PDB

6. On the screen shown in *Figure 32: Restoring the PDB* on page 50 , select the file that was transferred in *Step 2* on page 49 Click **Restore the PDB from the Selected File**.

7. Click **Confirm PDB Restore**.
When the file is restored successfully, the success message screen is displayed.

Recovering From Alarms

Alarms are resolved in order of severity level from highest to lowest. When combination alarms are decoded into their individual component alarms, the customer can decide in which order to resolve the alarms because all alarms are of equal severity. For assistance in deciding which alarm to resolve first or how to perform a recovery procedure, contact the *Customer Care Center* on page 3.

Evaluate the following problems to find the appropriate recovery procedure as follows:

- If the problem being investigated **is no longer displayed** on the EPAP GUI, perform the following:

  1. Procedure *Decode Alarm Strings* on page 51
  2. Procedure *Determine Alarm Cause* on page 52
  3. Recovery procedure to which you are directed by procedure *Determine Alarm Cause* on page 52

- If the problem being investigated **is being reported currently** on the EPAP GUI, perform the following:

  1. Procedure*Determine Alarm Cause* on page 52
  2. Recovery procedure to which you are directed by procedure *Determine Alarm Cause* on page 52

Decode Alarm Strings

Use the following procedure to decode alarm strings that consist of multiple alarms.

1. Log in to the **User Interface** screen of the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120).
2. After logging in to the EPAP, select **Maintenance>Decode MPS Alarm** from the menu.
3. Enter the 16-digit alarm string into the window on the **Decode MPS Alarm** screen, as shown in *Figure 33: Decode MPS Alarm Screen* on page 51.

Figure 33: Decode MPS Alarm Screen
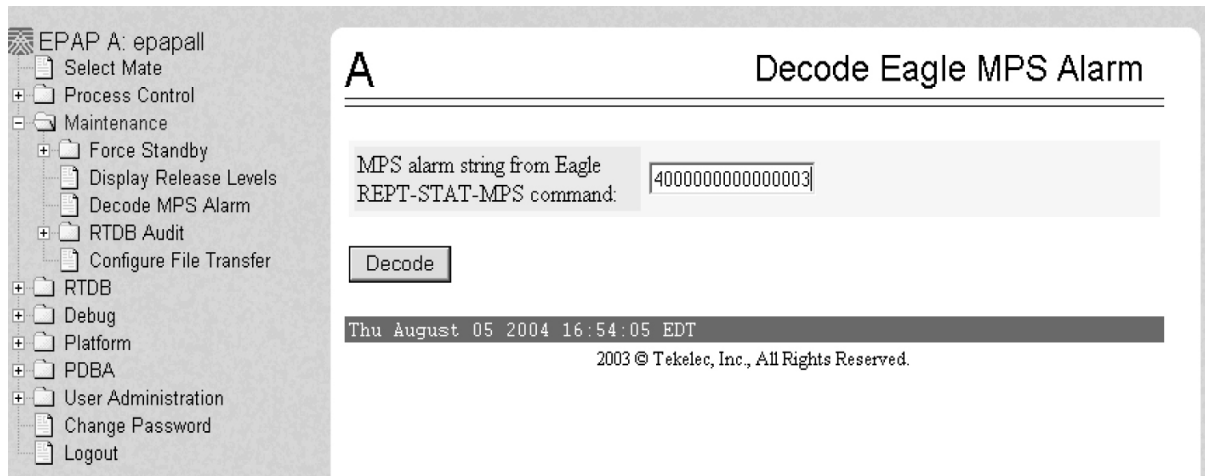
4. Click the **Decode** button.

   The system returns information on the Alarm Category (Critical Application, Major Platform)
   and error text, as shown in *Figure 34: Decoded MPS Alarm Information* on page 52.

   Figure 34: Decoded MPS Alarm Information
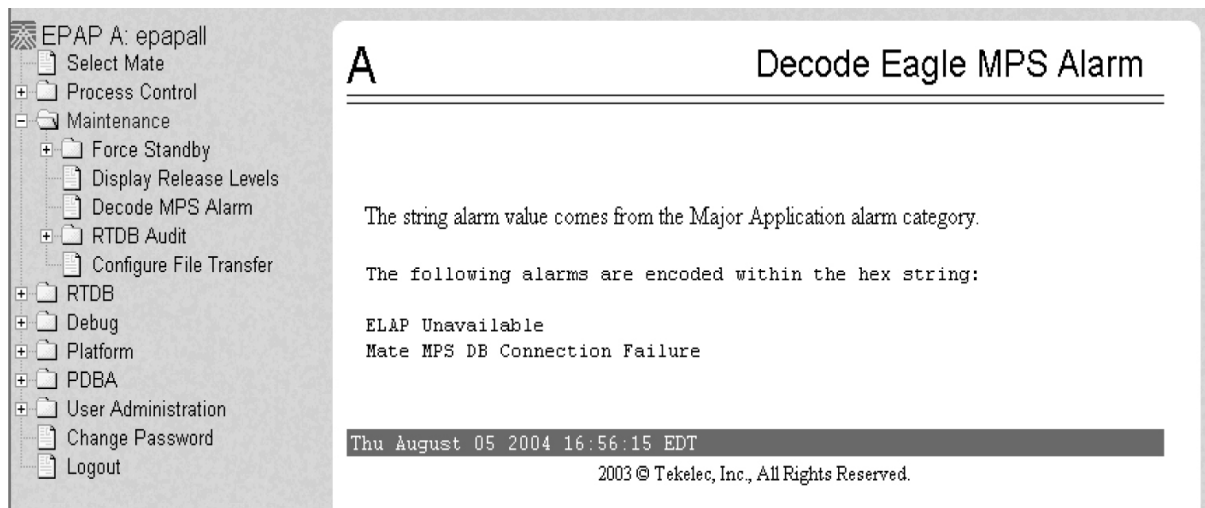
5. Find the alarm text string shown on the GUI in *Table 10: Platform and Application Alarms* on
   page 56. Note the corresponding alarm number change. Perform procedure *Determine Alarm
   Cause* on page 52.

   Note: For combination errors, multiple procedures may be required to resolve the problem.

Determine Alarm Cause

Use this procedure to find information about recovering from an alarm.

1. Record the alarm data string shown in the banner or the Alarm View on the EPAPGUI , or as
   decoded from *Decode Alarm Strings* on page 51.
2. Run `syscheck` in Verbose mode (see *Running syscheck Through the EPAP GUI* on page 123).

3. Examine the `syscheck` output for specific details about the alarm.

4. Find the recovery procedure for the alarm in the procedures shown in *MPS Platform and Application Alarms* on page 55. The alarms are ordered by ascending alarm number.

    Other procedures may be required to complete an alarm recovery procedure:

    *   Refer to procedures for replacing Field Replaceable Units (FRUs) in *MPS Platform and Application Alarms* on page 55 if instructed by an alarm recovery procedure to replace a FRU.
    *   Refer to general procedures used in a number of alarm recovery procedures in *MPS Platform and Application Alarms* on page 55

5. If the alarm persists after performing the appropriate procedure, call the *Customer Care Center* on page 3.

Chapter

4

MPS Platform and Application Alarms

Topics:

This chapter provides recovery procedures for platform and application alarms related to the T1000-based Multi-Purpose Server.

Introduction

This chapter describes recovery procedures to use when an alarm condition or other problem exists on the MPS system. For information about how and when alarm conditions are detected and reported, see *Detecting and Reporting Problems* on page 37.

When an alarm code is reported, locate the alarm in *Table 10: Platform and Application Alarms* on page 56. The procedures for correcting alarm conditions are described in *MPS Alarm Recovery Procedures* on page 60.

Note: Sometimes the alarm string may consist of multiple alarms and will have to be decoded in order to use the MPS Alarm Recovery Procedures in this manual. If the alarm code is not listed in *Table 10: Platform and Application Alarms* on page 56, "Platform and Application Alarms," see *Decode Alarm Strings* on page 51.

Platform and application errors are grouped by category and severity. The categories are listed from most to least severe:

- Critical Platform Alarms
- Critical Application Alarms
- Major Platform Alarms
- Major Application Alarms
- Minor Platform Alarms
- Minor Application Alarms

Table 10: Platform and Application Alarms on page 56 shows the alarm numbers and alarm text for all alarms generated by the MPS platform and the EPAP application. The order within a category is not significant.

Table 10: Platform and Application Alarms

Alarm Codes and Error Descriptor	UAM Number
Critical Platform Errors (There are no critical EPAP Platform Alarms)	
Critical Application Errors (There are no critical EPAP Application Alarms)	
Major Platform Errors	
3000000000000001 - Server Fan Failure on page 60	0372
3000000000000002 - Server Internal Disk Error on page 62	0372
3000000000000008 - Server Platform Error on page 62	0372
3000000000000010 - Server File System Error on page 62	0372

Alarm Codes and Error Descriptor	UAM Number
3000000000000020 - Server Platform Process Error on page 62	0372
3000000000000080 - Server Swap Space Shortage Failure on page 62	0372
3000000000000100 - Server Provisioning Network Error on page 62	0372
3000000000000200 - Server Eagle Network A Error on page 63	0372
3000000000000400 - Server Eagle Network B Error on page 65	0372
3000000000000800 - Server Sync Network Error on page 67	0372
3000000000001000 - Server Disk Space Shortage Error on page 69	0372
3000000000002000 - Server Default Route Network Error on page 70	0372
3000000000004000 - Server Temperature Error on page 74	0372
3000000000008000 - Server Mainboard Voltage Error on page 75	0372
3000000000010000 - Server Power Feed Unavailable on page 76	0372
3000000000020000 - Server Disk Health Test Error on page 76	0372
3000000000040000 - Server Disk Unavailable Error on page 76	0372
3000000001000000 - Breaker Panel Feed Error on page 76	0372
3000000002000000 - Breaker Panel Breaker Error on page 79	0372
3000000004000000 - Breaker Panel Monitoring Error on page 81	0372
Major Application Errors	
4000000000000001 - Mate EPAP Unavailable on page 82	0373
4000000000000002 - RTDB Mate Unavailable on page 83	0373

Alarm Codes and Error Descriptor	UAM Number
4000000000000004 - Congestion on page 84	0373
4000000000000020 - RMTP Channels Down on page 84	0373
4000000000000040 - Fatal Software Error on page 85	0373
4000000000000080 - RTDB Corrupt on page 85	0373
4000000000000100 - RTDB Inconsistent on page 85	0373
4000000000000200 - RTDB Incoherent on page 87	0373
4000000000001000 - RTDB 100% Full on page 87	0373
4000000000002000 - RTDB Resynchronization in Progress on page 87	0373
4000000000004000 - RTDB Reload Is Required on page 88	0373
4000000000008000 - Mate PDBA Unreachable on page 90	0373
4000000000010000 - PDBA Connection Failure on page 92	0373
4000000000020000 - PDBA Replication Failure on page 93	0373
4000000000040000 - RTDB DSM Over-Allocation on page 93	0375
4000000000080000 - RTDB Maximum Depth Reached on page 93	0375
4000000000100000 - No PDBA Proxy to Remote PDBA Connection on page 94	0375
4000000000200000 - DSM Provisioning Error on page 94	0375
Minor Platform Errors	
5000000000000001 - Server Disk Space Shortage Warning on page 95	0374
5000000000000002 - Server Application Process Error on page 96	0374
5000000000000004 - Server Hardware Configuration Error on page 96	0374

Alarm Codes and Error Descriptor	UAM Number
5000000000000020 - Server Swap Space Shortage Warning on page 97	0374
5000000000000040 - Server Default Router Not Defined on page 97	0374
5000000000000080 - Server Temperature Warning on page 99	0374
5000000000000100 - Server Core File Detected on page 100	0374
5000000000000200 - Server NTP Daemon Not Synchronized on page 100	0374
5000000000000400 - Server CMOS Battery Voltage Low on page 101	0374
5000000000000800 - Server Disk Self Test Warning on page 101	0374
5000000000004000 - Server Reboot Watchdog Initiated on page 101	0374
Minor Application Errors	
6000000000000001 - RMTP Channel A Down on page 101	0375
6000000000000002 - RMTP Channel B Down on page 101	0375
6000000000000008 - RTDB 80% Full on page 102	0375
6000000000000020 - Standby PDBA Falling Behind on page 102	0375
6000000000000040 - RTDB Tree Error on page 103	0375
6000000000000080 - PDB Backup failed on page 103	0375
6000000000000100 - Automatic PDB Backup failed on page 104	0375
6000000000000200 - RTDB Backup failed on page 105	0375
6000000000000400 - Automatic RTDB Backup failed on page 105	0375
6000000000001000 - SSH tunnel not established on page 106	0375
NOTE: The order within a category is not significant.	

MPS Alarm Recovery Procedures

This section provides recovery procedures for the MPS and EPAP alarms, listed by alarm category and Alarm Code (alarm data string) within each category.

Critical Platform Alarms

No critical EPAP alarms are generated.

Critical Platform Alarms

No critical EPAP alarms are generated.

Critical Application Alarms

No critical EPAP alarms are generated.

Major Platform Alarms

Major platform alarms involve MPS hardware components, memory, and network connections.

3000000000000001 - Server Fan Failure

This alarm indicates that one or more of the fans in the system has failed.

Note: For this alarm to clear, the underlying failure condition must be consistently undetected for a number of polling intervals. Therefore, the alarm may continue to be reported for several minutes after corrective actions are completed.

1. Refer to the procedure for replacing a fan assembly in the *Tekelec 1000* Application Server *Hardware Manual*.

    With the front lid open to access the fan assemblies, determine whether an object is interfering with the fan rotation. If an object is interfering with fan rotation, remove the object and go to *Step 3* on page 61.

2. If visual inspection does not indicate the presence of physical interference, perform the following substeps to determine which server fan assembly needs replacing and to replace the fan assembly:

    a) Run syscheck in Verbose mode (see *Running the System Health Check* on page 123).

Find the section of syscheck output about fans, which looks similar to the following:

```
      fan: Checking Status of Server Fans.
      fan: Fan is OK. mon0,Fan_C1: 1896 RPM (div = 8, min = 1394 RPM),
CHIP: lm87-i2c-0-2d
      fan: Fan is OK. mon0,Fan_C2: 2191 RPM (div = 8, min = 1394 RPM),
CHIP: lm87-i2c-0-2d
      fan: Fan is OK. mon1,Fan_A1: 1867 RPM (min = 1398 RPM), CHIP:
lm93-i2c-0-2e
      fan: Fan is OK. mon1,Fan_A2: 1867 RPM (min = 1398 RPM), CHIP:
lm93-i2c-0-2e
*     fan: ::MAJOR:: 3000000000000001 -- Server Fan Failure
      fan: Fan RPM is too low, mon1,Fan_B1: 0 RPM (min = 1398 RPM), CHIP:
 lm93-i2c-0-2e
*     fan: ::MAJOR:: 3000000000000001 -- Server Fan Failure
      fan: Fan RPM is too low, mon1,Fan_B2: 0 RPM (min = 1398 RPM), CHIP:
 lm93-i2c-0-2e
Return string: "One or more fans failed status check."
```

b) Use the `syscheck` output to determine the failed fan device from *Table 11: Mapping Fan Device Names to Server Fan Tray* on page 61 and determine which server fan assembly contains the failed fan.

For example, the sample `syscheck` output above lists the fans labeled as **Dev#: 1**; **mon0,Fan1**; and **mon1,Fan1** as failed, indicating that fan tray number 1 needs to be replaced.

Table 11: Mapping Fan Device Names to Server Fan Tray

Fan Device Name	Fan Tray #
Dev#: 1	1
mon0,Fan1	1
mon1,Fan1	1
Dev#: 2	2
mon0,Fan2	2
mon1,Fan2	2

c) Replace the indicated fan tray using the procedure for replacing a fan assembly in the *Tekelec 1000* Application Server *Hardware Manual* and continue to *Step 3* on page 61.

3. Run `syscheck` (see *Running the System Health Check* on page 123).
   a) If the alarm has been cleared, the problem is resolved.
   b) If the alarm has not been cleared, continue to the next step.

4. If the problem has not been resolved, call the *Customer Care Center* on page 3.

3000000000000002 - Server Internal Disk Error

This alarm indicates that the server is experiencing issues replicating data to one or more of its mirrored disk drives. This could indicate that one of the server disks has failed or is approaching failure.

1. Run `syscheck` in Verbose mode (see *Running the System Health Check* on page 123).
2. Call the *Customer Care Center* on page 3 and provide the system health check output.

3000000000000008 - Server Platform Error

This alarm indicates a major platform error such as a corrupt system configuration or missing files, or indicates that `syscheck` itself is corrupt.

1. Run `syscheck` in Verbose mode (see *Running the System Health Check* on page 123).
2. Call the *Customer Care Center* on page 3 and provide the system health check output.

3000000000000010 - Server File System Error

This alarm indicates that `syscheck` was unsuccessful in writing to at least one of the server file systems.

Call *Customer Care Center* on page 3 for assistance.

3000000000000020 - Server Platform Process Error

This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

Contact *Customer Care Center* on page 3 for recovery procedures.

3000000000000080 - Server Swap Space Shortage Failure

This alarm indicates that the server's swap space is in danger of being depleted. This is usually caused by a process that has allocated a very large amount of memory over time.

Note: In order for this alarm to clear, the underlying failure condition must be consistently undetected for a number of polling intervals. Therefore, the alarm may continue to be reported for several minutes after corrective actions are completed.

Call *Customer Care Center* on page 3 for assistance.

3000000000000100 - Server Provisioning Network Error

This alarm indicates that the connection between the server **eth0** interface and the customer network is not functioning properly. The **eth0** interface is the lower port of PCI 4 on the server.

1. Verify that the **eth0** cable is securely connected to the lower port of PCI 4 (see *Figure 35: Network Connections* on page 63).

2. Trace the cable to its connection point on the local network. Verify that this connection is secure.

3. Test the **eth0** cable with an Ethernet Line Tester.

   If the cable does not test positive, replace it.

4. Request that your network administrator verify that the network is functioning properly.

5. If no other nodes on the local network are experiencing problems and the fault has been isolated to the server or the exact origin of the problem cannot be determined, contact the *Customer Care Center* on page 3.

3000000000000200 - Server Eagle Network A Error

Note: If the three alarms 3000000000000200-Server Eagle Network A Error, 3000000000000400-Server Eagle Network B Error, and 3000000000000800-Server Sync Network Error exist, the probable cause is a failed mate server.

This alarm indicates an error in the Main DSM network, which connects to the DSM A ports. The error may be caused by one or more of the following conditions:

- One or both of the servers is not operational.

- One or both of the hubs is not powered on.

- The link between the hubs is not working.

- The connection between MPS server A and MPS server B is not working.

Figure 35: Network Connections on page 63 shows the connections between the servers and the hubs of the DSM networks (main and backup).

- The **eth1** interface is the upper port of PCI 4 on the server.

- Port 2 of hub 1 connects to the **eth1** interface on Server B.

- Port 2 of hub 2 connects to the **eth1** interface on Server A.

- Ports 3 through 16 on hubs 1 and 2 connect to the Main DSM ports (DSM A ports) on the EAGLE 5 ISS. To clearly display the location of these ports, *Figure 35: Network Connections* on page 63 does not include the connecting cables.

Figure 35: Network Connections
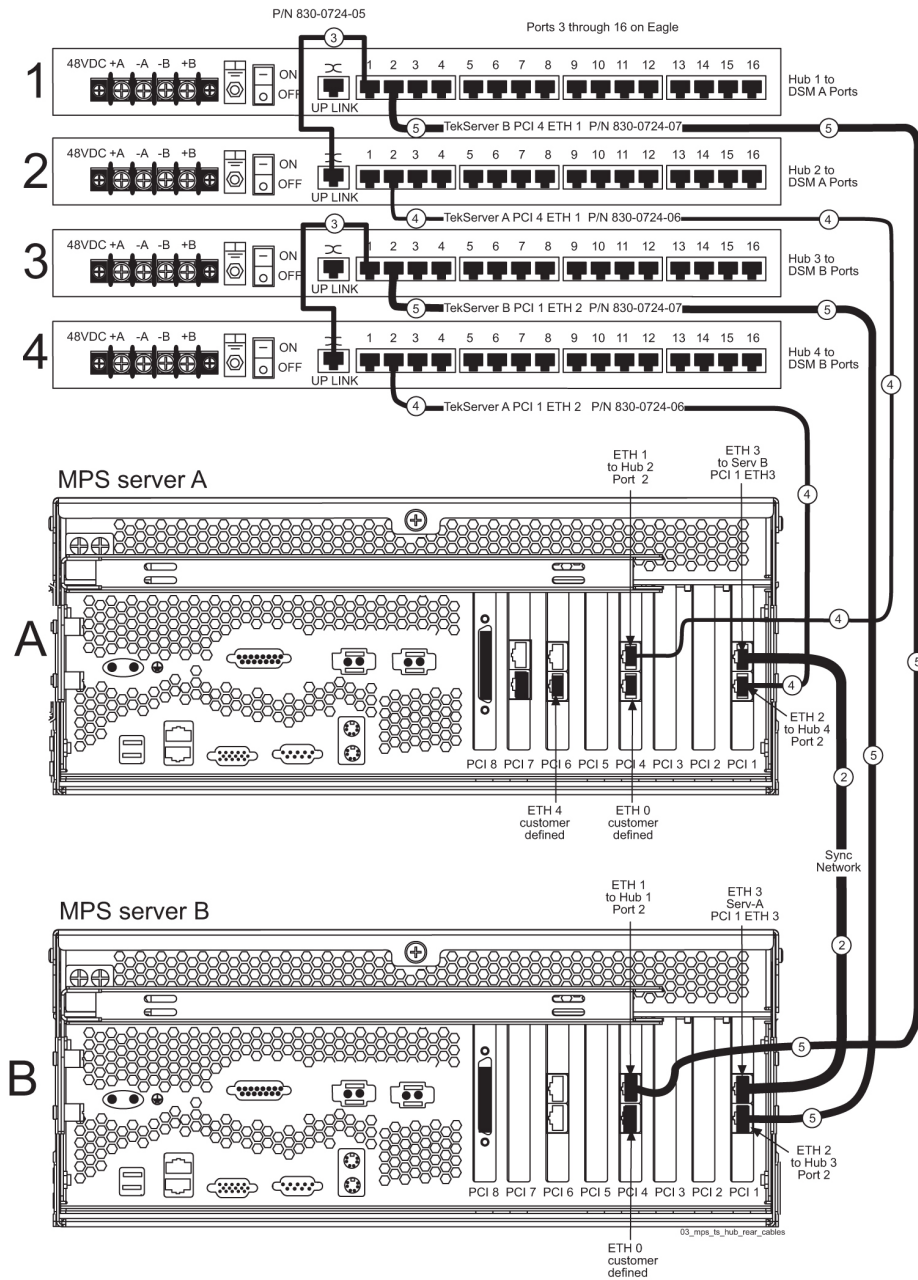
Note: The numbers shown in *Figure 35: Network Connections* on page 63 correspond to cable numbers described in the *Tekelec 1000 Application Server Hardware Manual*. Cables are referred to by number in this procedure.

1. Perform the following:

   a) Verify that both servers are powered on by confirming that the**POWER** LEDs on both servers are illuminated green.

   b) Verify that the hub is powered on.

   c) Verify that the hub does not have any fault lights illuminated.

    d) Verify that the **eth1** cable is securely connected to the upper port of PCI 4 on the server that is reporting the error.

    e) Trace the **eth1** cable to the hub. Verify that the **eth1** cable is securely connected at port 2 on the hub.

    f) Verify that the cable connecting the hubs (identified as cable 3 in *Figure 35: Network Connections* on page 63) is securely connected at both hubs.

2. Run `syscheck` (see *Running syscheck Through the EPAP GUI* on page 123).

    a) If the alarm is cleared, the problem is resolved.

    b) If the alarm is not cleared, continue with the next step.

3. Verify that the cable from **eth1** to the hub tests positive with an Ethernet Line Tester. Replace any faulty cables.

4. If the problem persists, call the *Customer Care Center* on page 3.

3000000000000400 - Server Eagle Network B Error

Note: If the three alarms 3000000000000200-Server Eagle Network A Error, 3000000000000400-Server Eagle Network B Error, and 3000000000000800-Server Sync Network Error exist, the probable cause is a failed mate server.

This alarm indicates an error in the Backup DSM network, which connects to the DSM B ports. The error may be caused by one or more of the following conditions:

• One or both of the servers is not operational.

• One or both of the hubs is not powered on.

• The link between the hubs is not working.

• The connection between MPS server A and MPS server B is not working.

Figure 36: Network Connections on page 65 shows the connections between the MPS servers and the hubs of the DSM networks (main and backup).

• The **eth2** interface is the lower port of PCI 1 on the server.

• Port 2 of hub 3 connects to the **eth2** interface on Server B.

• Port 2 of hub 4 connects to the **eth2** interface on Server A.

• Ports 3 through 16 on hubs 3 and 4 connect to the Backup DSM ports (DSM B ports) on the EAGLE 5 ISS. To clearly display the location of these ports, *Figure 36: Network Connections* on page 65 does not include the connecting cables.

Figure 36: Network Connections
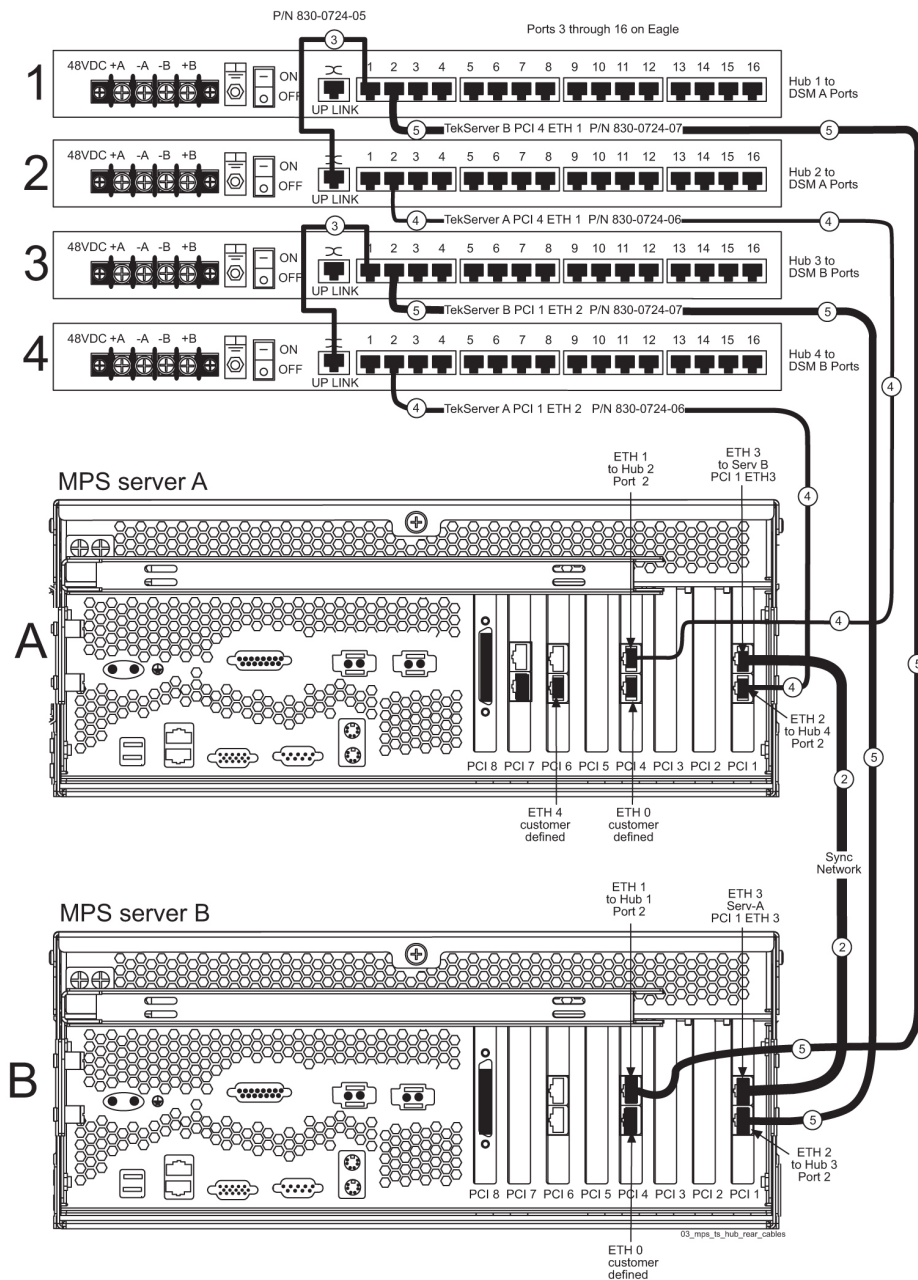
Note: The numbers shown in *Figure 36: Network Connections* on page 65 correspond to cable numbers in the *Tekelec 1000 Application Server Hardware Manual*. Cables are referred to by number in this procedure.

1. Perform the following:
   a) Verify that both servers are powered on by confirming that the **POWER** LEDs on both servers are illuminated green.
   b) Verify that the hub is powered on.
   c) Verify that the hub does not have any fault lights illuminated.

d) Verify that the **eth2** cable is securely connected to the lower port of PCI 1 on the server that is reporting the error.

e) Trace the **eth2** cable to the hub. Verify that the **eth2** cable is securely connected at port 2 on the hub.

f) Verify that the cable connecting the hubs (identified as cable 3 in *Figure 36: Network Connections* on page 65) is securely connected at both hubs.

2. Run syscheck (see *Running syscheck Through the EPAP GUI* on page 123).

   a) If the alarm is cleared, the problem is resolved.

   b) If the alarm is not cleared, continue with the next step.

3. Verify that the cable from **eth2** to the hub tests positive with an Ethernet Line Tester. Replace any faulty cables.

4. If the problem persists, call the *Customer Care Center* on page 3 for assistance.

3000000000000800 - Server Sync Network Error

Note: If the three alarms 3000000000000200-Server Eagle Network A Error, 3000000000000400-Server Eagle Network B Error, and 3000000000000800-Server Sync Network Error exist, the probable cause is a failed mate server.

This alarm indicates that the **eth3** connection between the two servers is not functioning properly. The **eth3** connection provides a network path over which the servers synchronize data with one another. The **eth3** interface is the upper port of PCI 1 on the server.

A direct connection is made between the two servers; no hub is used in this connection. A straight-through Ethernet cable (shown as cable 2 in *Figure 37: Network Connections* on page 67) must be used for this connection. All pairs are required.

Figure 37: Network Connections
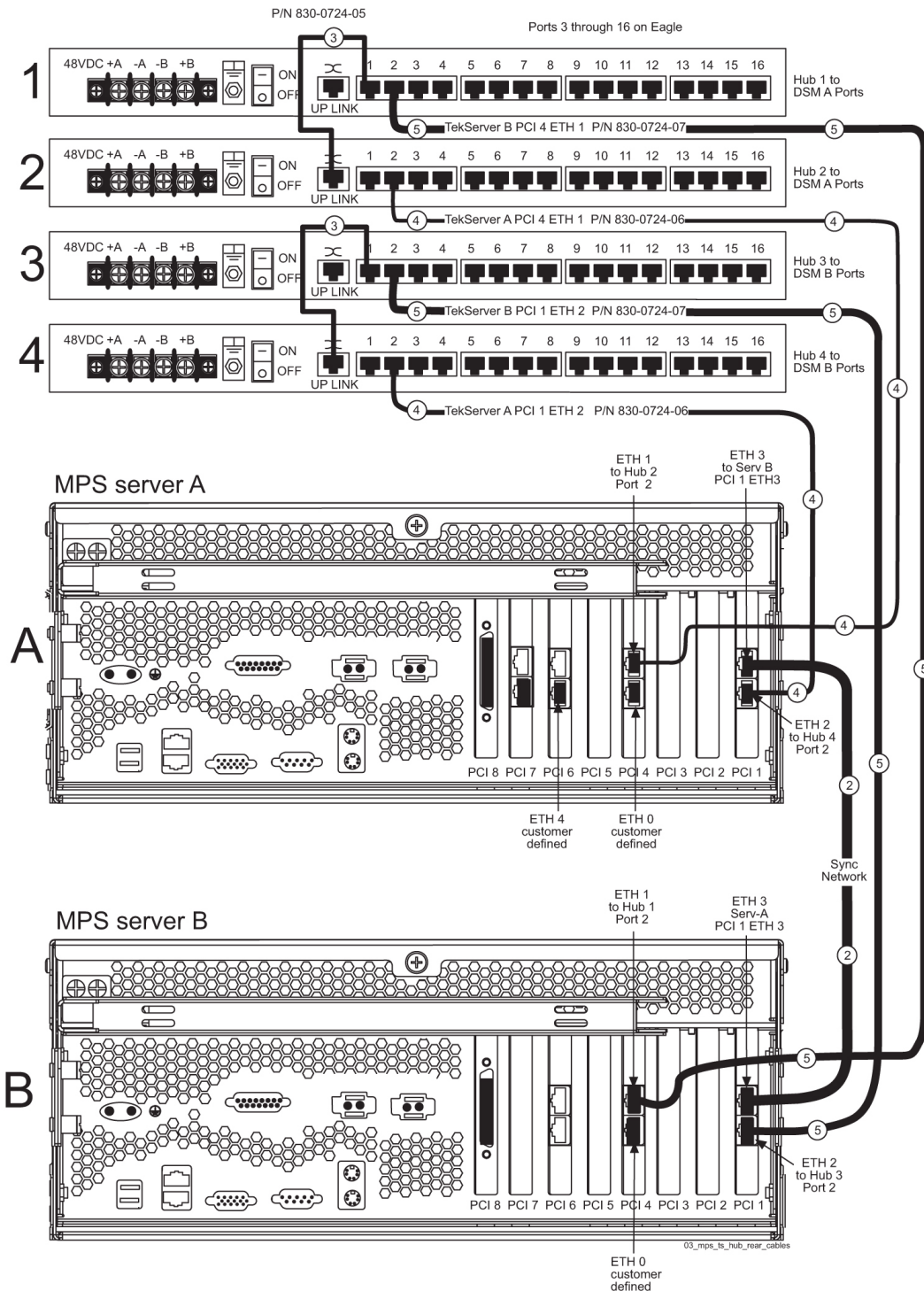
Note: The numbers shown in *Figure 37: Network Connections* on page 67 correspond to cable numbers described in the *Tekelec 1000 Application Server Hardware Manual*. Cables are referred to by number in this procedure.

1. Verify that both servers are powered on by confirming that the **POWER** LEDs on both servers are illuminated green.

2. Verify that the **eth3** cable (cable 2 in *Figure 37: Network Connections* on page 67) is securely connected to the upper port of PCI 1 on both Server A and Server B.

3. Test the **eth3** cable with an Ethernet Line Tester that is set to test a straight-through cable.

4. If the cable does not test positive, replace it.

5. If the problem persists, call the *Customer Care Center* on page 3 for assistance.

3000000000001000 - Server Disk Space Shortage Error

This alarm indicates that one of the following conditions has occurred:

- A filesystem has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the filesystem.

- More than 90% of the total number of available files have been allocated on the filesystem.

- A filesystem has a different number of blocks than it had when installed.

1. Run `syscheck` (see *Running syscheck Through the EPAP GUI* on page 123).

2. Examine the syscheck output to determine if the filesystem `/var/TKLC/epap/free` is low on space. If it is, continue to the next step; otherwise go to *Step 4* on page 70

3. If possible, recover space on the free partition by deleting unnecessary files:

   a) Log in to the EPAP GUI (see *Running syscheck Through the EPAP GUI* on page 123).

   b) Select **Debug>Manage Logs & Backups**.

   A screen similar to *Figure 38: Manage Logs and Backups* on page 69 is displayed. This screen displays the information about the total amount of space allocated for and currently used by logs and backups. The display includes logs and backup files which might be selected for deletion to recover additional disk space.

   Figure 38: Manage Logs and Backups
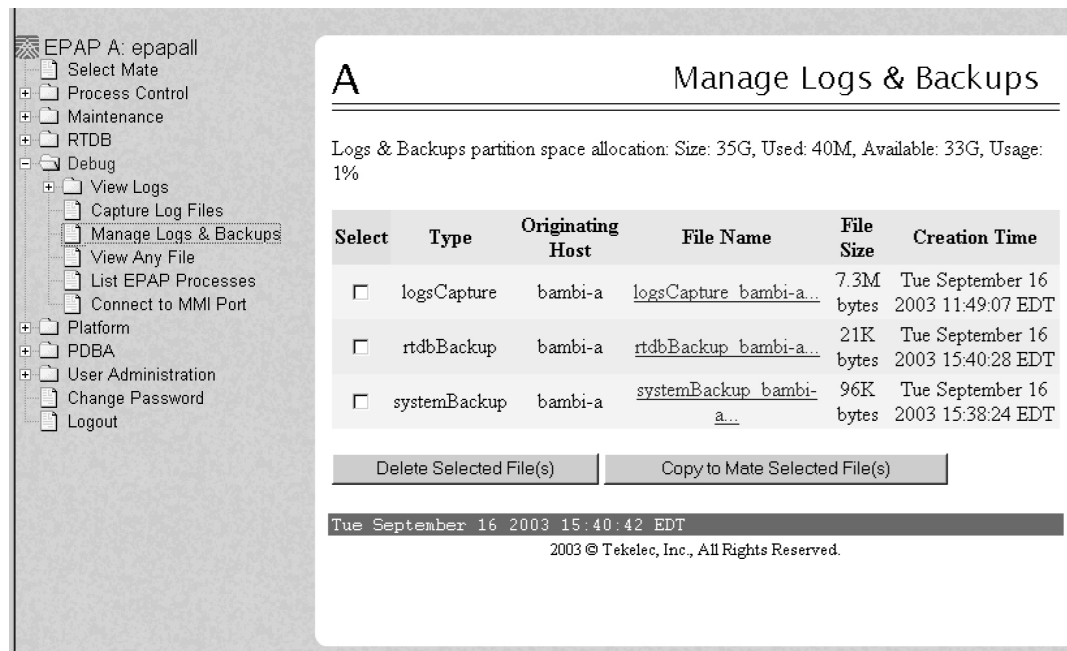
c) Click the checkbox of each file that you want to delete and then click **Delete Selected File(s)**.

4. Call *Customer Care Center* on page 3 for assistance.

3000000000002000 - Server Default Route Network Error

This alarm indicates that the default network route of the server is experiencing a problem. Running syscheck in Verbose mode will provide information about which type of problem is occurring.

CAUTION: When changing the network routing configuration of the server, verify that the modifications will not impact the method of connectivity for the current login session. The route information must be entered correctly and set to the correct values. Incorrectly modifying the routing configuration of the server may result in total loss of remote network access.

1. Run syscheck in Verbose mode.

   The output should indicate one of the following errors:

- `The default router at <IP_address> cannot be pinged.`

    This error indicates that the router may not be operating or is unreachable. If the `syscheck` Verbose output returns this error, go to *Step 2* on page 71.

- `The default route is not on the provisioning network.`

    This error indicates that the default route has been defined in the wrong network. If the `syscheck` Verbose output returns this error, go to *Step 3* on page 71.

- `An active route cannot be found for a configured default route.`

    This error indicates that a mismatch exists between the active configuration and the stored configuration. If the `syscheck` Verbose output returns this error, go to *Step 4* on page 73.

2. Perform the following substeps when `syscheck` Verbose output indicates:

    `The default router at <IP_address> cannot be pinged`

    a) Verify the network cables are firmly attached to the server, network switch, router, hub, and any other connection points.
    b) Verify that the configured router is functioning properly.

       Request that the network administrator verify the router is powered on and routing traffic as required.

    c) Request that the router administrator verify that the router is configured to reply to pings on that interface.
    d) Go to *Step 5* on page 74.

3. Perform the following substeps when `syscheck` Verbose output indicates:

    `The default route is not on the provisioning network`

    a) Obtain the proper Provisioning Network netmask and the IP address of the appropriate Default Route on the provisioning network.

       This information is maintained by the customer network administrators.

    b) Log in to the MPS with username `epapconfig` (see *Accessing the EPAP Text Interface* on page 122).

       The server designation at this site is displayed as well as **hostname**, **hostid**, **Platform Version**, **Software Version**, and date. Verify that the side displayed is the MPS that is reporting the problem. In this example, MPS A is reporting the problem. Enter option 2, `Configure Network Interfaces Menu`, from the EPAP Configuration Menu.

```
MPS Side A:  hostname: mpsa-d1a8f8  hostid: 80d1a8f8
             Platform Version: x.x.x-x.x.x
             Software Version: EPAP x.x.x-x.x.x
             Wed Jul 17 09:51:47 EST 2002
 /-----EPAP 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 | PDB Configuration Menu             |
|----|------------------------------------|
|  e | Exit                               |
\------------------------------------------/
Enter Choice:  2
```

c) Enter option 1, Configure Provisioning Network, from the Configure Network
   Interfaces Menu.

   The submenu for configuring communications networks and other information is displayed.

```
 /-----Configure Network Interfaces Menu----\
/--------------------------------------------\
|  1 | Configure Provisioning Network        |
|----|---------------------------------------|
|  2 | Configure Sync Network                |
|----|---------------------------------------|
|  3 | Configure DSM Network                 |
|----|---------------------------------------|
|  4 | Configure Backup Provisioning Network |
|----|---------------------------------------|
|  5 | Configure Forwarded Ports             |
|----|---------------------------------------|
|  6 | Configure Static NAT Addresses        |
|----|---------------------------------------|
|  7 | Configure Provisioning VIP Addresses  |
|----|---------------------------------------|
|  e | Exit                                  |
\--------------------------------------------/
Enter choice:  1
```

d) The following warning is displayed. Type Y and press **Enter**.

```
EPAP software and PDBA are running. Stop them? [N]  Y
```

e) The EPAP A provisioning network IP address is displayed.

```
Verifying connectivity with mate ...
Enter the EPAP A provisioning network IP Address [192.168.61.90]:
```

f) Press **Enter** after each address is displayed until the Default Route address is displayed.

```
Verifying connectivity with mate ...
Enter the EPAP A provisioning network IP Address [192.168.61.90]:
Enter the EPAP B provisioning network IP Address [192.168.61.91]:
Enter the EPAP provisioning network netmask [255.255.255.0]:
Enter the EPAP provisioning network default router IP Address: 192.168.61.250
```

g) If the default router IP address is incorrect, type the correct address and press Enter.

h) After you have verified or corrected the Provisioning Network configuration
   information, enter e to return to the Configure Network Interfaces Menu.

i) Enter e again to return to the EPAP Configuration Menu.

j) Go to *Step 5* on page 74.

4. Perform the following substeps to reboot the server if the `syscheck` output indicates the following error. Otherwise, go to *Step 5* on page 74:

```
An active route cannot be found for a configured default route
```

a) Log in as `epapconfig` on the MPS console.

Enter option 6, `Platform Menu`, from the EPAP Configuration Menu.

```
 /-----EPAP 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 |  PDB Configuration Menu          |
|----|---------------------------------|
|  e |  Exit                            |
\--------------------------------------/
Enter Choice:  6
```

b) Enter option 3, `Reboot MPS`, from the EPAP Platform Menu.

At the prompt, enter the identifier of the MPS to which you are logged in (`A` or `B`). In this example, `A` is used.

```
 /-----EPAP Platform Menu-\
/------------------------\
|  1 |  Initiate Upgrade  |
|----|-------------------|
|  2 |  Eject CD          |
|----|-------------------|
|  3 |  Reboot MPS        |
|----|-------------------|
|  4 |  Halt MPS          |
|----|-------------------|
|  5 |  File System Backup |
|----|-------------------|
|  6 |  MySQL Backup      |
|----|-------------------|
|  7 |  RTDB Backup       |
|----|-------------------|
|  8 |  PDB Backup        |
|----|-------------------|
|  e |  Exit              |
\------------------------/
Enter Choice:  3
Reboot MPS A, MPS B or BOTH? [BOTH]:  A
Reboot local MPS...
```

c) Wait for the reboot to complete.

d) Go to *Step 5* on page 74.

5. Run `syscheck`.

   - If the alarm is cleared, the problem is resolved.
   - If the alarm is not cleared, go to the next step.

6. Contact the *Customer Care Center* on page 3 with the `syscheck` output collected in the previous steps.

3000000000004000 - Server Temperature Error

This alarm indicates that the internal temperature within the server is unacceptably high.

1. Verify that nothing is blocking the fan intake (see *Figure 39: Server Fans* on page 74).
   Remove any blockage.

   Figure 39: Server Fans

2. Verify that the temperature in the room is normal (see *Table 12: Server Environmental Conditions* on page 74).
   If the room temperature is too hot, lower the temperature in the room to an acceptable level.

   Table 12: Server Environmental Conditions

Ambient Temperature	Normal Operating Temperature Range: 5 degrees C to 40 degrees C
	Exceptional Operating Limit: -5 degrees C to 50 degrees C (operation for no more than 96 hours duration at extremes and at elevations of less than 1800 meters)
	Storage: -20 degrees C to 60 degrees C

Relative Humidity	Operating: 5% to 85% non-condensing
	Storage: 5% to 95% non-condensing
Elevation	Operating: -300m to +300m
	Storage: -300m to +1200m
Heating, Ventilation, and Air Conditioning	Capacity must compensate for up to 5100 BTUs/hr for each installed frame.
	Calculate HVAC capacity as follows:
	Determine the wattage of the installed equipment.
	Use the formula: watts x 3.143 = BTUs/hr

Note: Be prepared to wait an appropriate period of time before continuing with the next step. Environmental conditions must be below alarm threshold levels consistently before the alarm clears. The alarm may take up to five minutes to clear after conditions improve. After the room temperature returns to an acceptable level, `syscheck` may not show the alarm cleared for up to ten minutes.

3. Run `syscheck` (see *Running syscheck Through the EPAP GUI* on page 123).

   a) If the alarm has been cleared, the problem is resolved.
   b) If the alarm has not been cleared, continue with *Step 4* on page 75.

4. Replace the filter by performing *Replacing Fan Filters* on page 36 .

   Note: Be prepared to wait an appropriate period of time before continuing with the next step. Environmental conditions must be below alarm threshold levels consistently before the alarm clears. The alarm may take up to five minutes to clear after conditions improve. After the room temperature returns to an acceptable level, `syscheck` may not show the alarm cleared for up to ten minutes.

5. Run `syscheck` (see *Running syscheck Through the EPAP GUI* on page 123).

   a) If the alarm is cleared, the problem is resolved.
   b) If the alarm is not cleared, continue with *Step 6* on page 75.

6. If the problem is not resolved, call the *Customer Care Center* on page 3 for assistance.

3000000000008000 - Server Mainboard Voltage Error

This alarm indicates that at least one monitored voltages on the server mainboard is not within the normal operating range.

Contact the *Customer Care Center* on page 3 for assistance.

3000000000010000 - Server Power Feed Unavailable

This alarm indicates that one of the power feeds to the server has failed. For more information about power feeds, see *Breaker Panels* on page 15.

If this alarm occurs in conjunction with any Breaker Panel alarm, a problem with the breaker panel may exist. Refer to the Breaker Panel alarm procedures: *3000000001000000 - Breaker Panel Feed Error* on page 76, *3000000002000000 - Breaker Panel Breaker Error* on page 79, and *3000000004000000 - Breaker Panel Monitoring Error* on page 81 .

1. Locate the server supplied by the faulty power feed. Verify that all connections to the power supply units are connected securely.
2. Run syscheck (see *Running syscheck Through the EPAP GUI* on page 123).
    a) If the alarm is cleared, the problem is resolved.
    b) If the alarm is not cleared, go to *Step 3* on page 76.
3. Trace the power feed to its connection on the power source.

    Verify that the power source is on and that the power feed is properly secured (see *Figure 40: Breaker LEDs* on page 77).
4. Run syscheck (see *Running syscheck Through the EPAP GUI* on page 123).
    a) If the alarm is cleared, the problem is resolved.
    b) If the alarm is not cleared, go to *Step 5* on page 76.
5. If the power source is functioning properly and all connections are secure, request that an electrician check the voltage on the power feed.
6. Run syscheck (see *Running syscheck Through the EPAP GUI* on page 123).
    a) If the alarm is cleared, the problem is resolved.
    b) If the alarm is not cleared, go to *Step 7* on page 76.
7. If the problem is not resolved, call the *Customer Care Center* on page 3 for assistance.

3000000000020000 - Server Disk Health Test Error

This alarm indicates that the hard drive has failed or failure is imminent.

Immediately contact the *Customer Care Center* on page 3 for assistance with a disk replacement.

3000000000040000 - Server Disk Unavailable Error

This alarm indicates that the smartd service is not able to read the disk status because the disk has other problems that are reported by other alarms. This alarm appears only while a server is booting.

Perform the recovery procedures for the other alarms that accompany this alarm.

3000000001000000 - Breaker Panel Feed Error

This alarm indicates that the server is not receiving information from the breaker panel relays.

1. Check the **POWER ON** LEDs (see *Figure 40: Breaker LEDs* on page 77).

Figure 40: Breaker LEDs
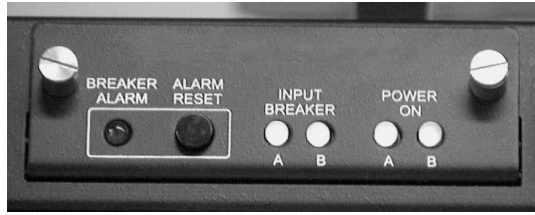
If one of the **POWER ON** LEDs is not illuminated, a problem has been detected with the corresponding input power feed (see *Figure 41: Breaker Panel Rear View* on page 77). Perform the following steps to correct this problem.

Figure 41: Breaker Panel Rear View
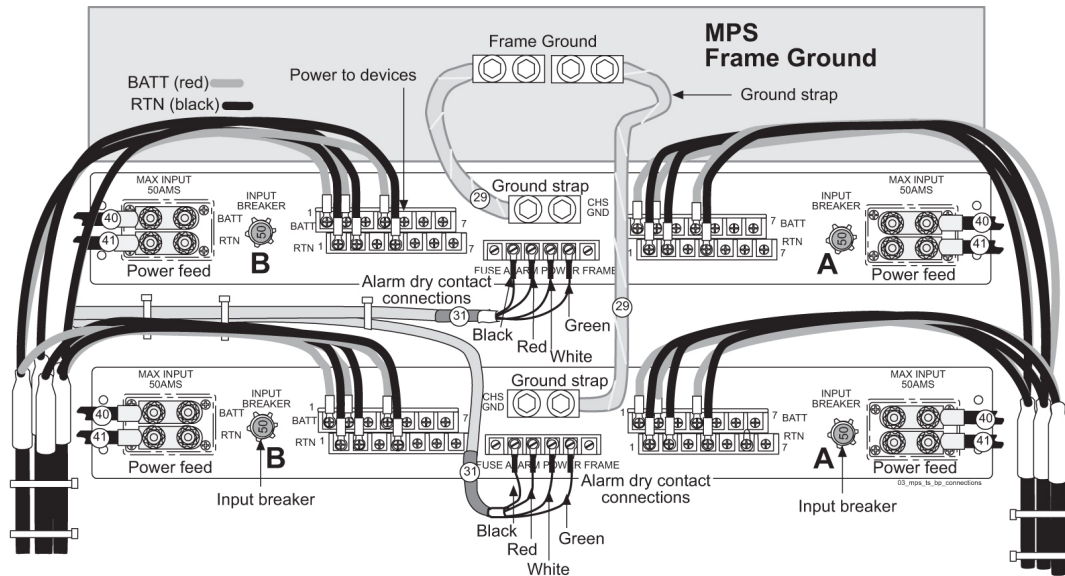
Note: The numbers shown in *Figure 41: Breaker Panel Rear View* on page 77 correspond to cable numbers in the *Tekelec 1000 Application Server Hardware Manual*. Cables are referred to by number in this procedure.

a) Verify that the customer-provided power source for the affected power feed is operational.

If the power source is properly functioning, request that an electrician remove the plastic cover from the rear of the breaker panel to verify the power source is securely connected to the input power feed connection on the rear of the breaker panel (see *Figure 41: Breaker Panel Rear View* on page 77). Correct any power connection deficiencies.

b) Check the **POWER ON** LED.

- If the **POWER ON** LED is illuminated, the issue is resolved. Proceed to *Step 4* on page 79 to verify that the alarm has cleared.

- If the **POWER ON** LED is not illuminated, continue to *Substep c* on page 77.

c) Request that an electrician verify the integrity of the input power feed.

The input voltage must measure -48VDC ± 7VDC. If the supplied voltage is not within the acceptable range (-41VDC and -55VDC), the input power source must be repaired or replaced.

Note: If the measured voltage is within the acceptable range, but the **POWER ON** LED is not illuminated, the LED may have failed or the breaker panel may be malfunctioning. For either failure, the breaker panel must be replaced (see *Breaker Panel Replacement Procedure* on page 112).

d) Check the **POWER ON** LED after the recommended actions have been performed to correct any deficiencies.

- If the **POWER ON** LED is illuminated, the issue is resolved. Proceed to *Step 4* on page 79 to verify that the alarm is cleared.

- If the **POWER ON** LED is not illuminated, go to *Step 5* on page 79 .

Figure 42: Breakers on Front Panel
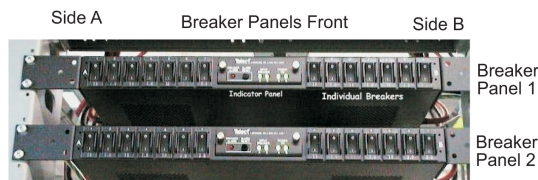
2. Check the **INPUT BREAKER** LEDs (see *Figure 42: Breakers on Front Panel* on page 78)

If one of the **INPUT BREAKER** LEDs is not illuminated, then the associated Input Breaker (see *Figure 40: Breaker LEDs* on page 77) is open (popped out). Perform the following steps to correct this problem:

a) Record the positions (**O** or **|**) of the breaker panel circuit breakers (see *Figure 42: Breakers on Front Panel* on page 78).

Refer to *Table 5: Mapping of Assigned (Closed) Circuit Breakers to Devices* on page 18 to determine which circuit breakers are assigned to control power to devices in the frame.

b) Switch all circuit breakers for the affected side of the breaker panel to the open (**O**) position (see *Figure 42: Breakers on Front Panel* on page 78).

c) After all circuit breakers on the affected side are in the open (**O**) position, reset by pushing in the Input Breaker for the affected side on the rear of the breaker panel (see *Figure 41: Breaker Panel Rear View* on page 77).

If the Input Breaker does not reset, or if it resets and within a few moments opens (pops out), go to *Step 5* on page 79.

d) Restore the circuit breakers on the affected side to their original settings. Switch only one circuit breaker at a time (see *Figure 42: Breakers on Front Panel* on page 78).

e) Check the **INPUT BREAKER** LEDs again.

If the LED is not illuminated, go to *Step 5* on page 79.

Note: The problem may recur after a delay. The server must be closely monitored for the recurrence of this alarm after performing corrective actions to repair the problem. If no recurrences are observed for 24 hours, the problem is considered resolved. If the problem recurs, contact the *Customer Care Center* on page 3.

3. If all **INPUT BREAKER** LEDs and **POWER ON** LEDs are illuminated, the probable cause is the serial connection between the server and the breaker panel.

The serial connection is used by the system health check to monitor the breaker panel for failures. Verify that both ends of the labeled serial cables (cable 31 in *Figure 41: Breaker Panel Rear View* on page 77) are securely connected. Correct any issues observed with these cables and continue to the next step to verify that the alarm has been cleared; otherwise, go to *Step 5* on page 79.

4. Run `syscheck` (see *Running the System Health Check* on page 123).

    a) If the alarm is cleared, the problem is resolved.

    b) If the alarm is not cleared, continue with the next step.

5. If the problem is not resolved, call the *Customer Care Center* on page 3 for assistance.

3000000002000000 - Breaker Panel Breaker Error

This alarm indicates that one or more of the active circuit breakers on the front of the breaker panel is in the open position (**O**). Inactive circuit breakers are labeled **NOT USED** and should be in the open (**O**) position. The circuit breaker configuration is determined by the specific product installation. See *Breaker Panels* on page 15 for details regarding breaker panel configuration.

Note:

The problem may recur after a delay. The server must be closely monitored for the recurrence of this alarm after performing corrective actions to repair the problem. If no recurrences are observed for 24 hours, the problem is considered resolved. If the problem recurs, contact the *Customer Care Center* on page 3 for assistance.

1. Inspect the **BREAKER ALARM** LED, which is the red LED in the center of the front of the breaker panel (see *Figure 43: Breaker Panel LEDs* on page 79).

    a) If the **BREAKER ALARM** LED is illuminated, one or more of the active breakers is in the open position, go to *Step 3* on page 79.

    b) If the **BREAKER ALARM** LED is not illuminated, the probable cause is the serial connection between the server and the breaker panel.

    The serial connection is used by the system health check to monitor the breaker panel for failures. Continue to *Step 2* on page 79 to verify the serial connection.

    Figure 43: Breaker Panel LEDs
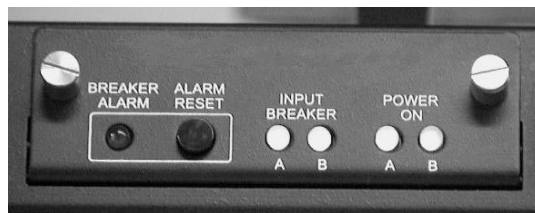
2. Verify that both ends of the labeled serial cables (cable 31 in *Figure 45: Breaker Panel Rear View* on page 80) are securely connected.

    Correct any issues observed with these cables and go to *Step 6* on page 81 to verify that the alarm has been cleared; otherwise go to *Step 7* on page 81.

3. Carefully examine all circuit breakers on the breaker panel (see *Figure 44: Breaker Positions* on page 80).

Unused circuit breakers are labeled **NOT USED** and should always be in the open (**O**) position. If an assigned (active) circuit breaker is in the open (**O**) position, switch it to the closed (**|**) position.

Figure 44: Breaker Positions
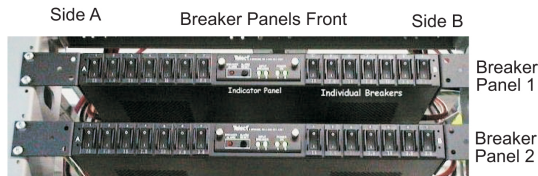
Check the **BREAKER ALARM** LED (see *Figure 43: Breaker Panel LEDs* on page 79).

a) If the**BREAKER ALARM** LED is not illuminated, the problem may be resolved.

   Go to *Step 6* on page 81 to verify that the alarm is cleared.

b) If the **BREAKER ALARM** LED is illuminated, continue to the next step.

4. Depress and release the **ALARM RESET** button located in the center on the front of the breaker panel, beside the **BREAKER ALARM** LED (see *Figure 43: Breaker Panel LEDs* on page 79).

   After releasing the **ALARM RESET** button, examine the **BREAKER ALARM** LED again.

a) If the **BREAKER ALARM** LED is no longer illuminated, the problem may be resolved.

   Go to *Step 6* on page 81 to verify the alarm is cleared.

b) If the **BREAKER ALARM** LED is illuminated and this is the first attempt at resetting the **ALARM RESET** button, continue to *Step 5* on page 80.

c) If the **BREAKER ALARM** LED is illuminated and this step is being repeated, go to *Step 7* on page 81.

5. Request that an electrician verify that all terminal connections are tightly secure for the circuit breakers which are assigned to control power to devices in the frame (see *Figure 45: Breaker Panel Rear View* on page 80).

Figure 45: Breaker Panel Rear View
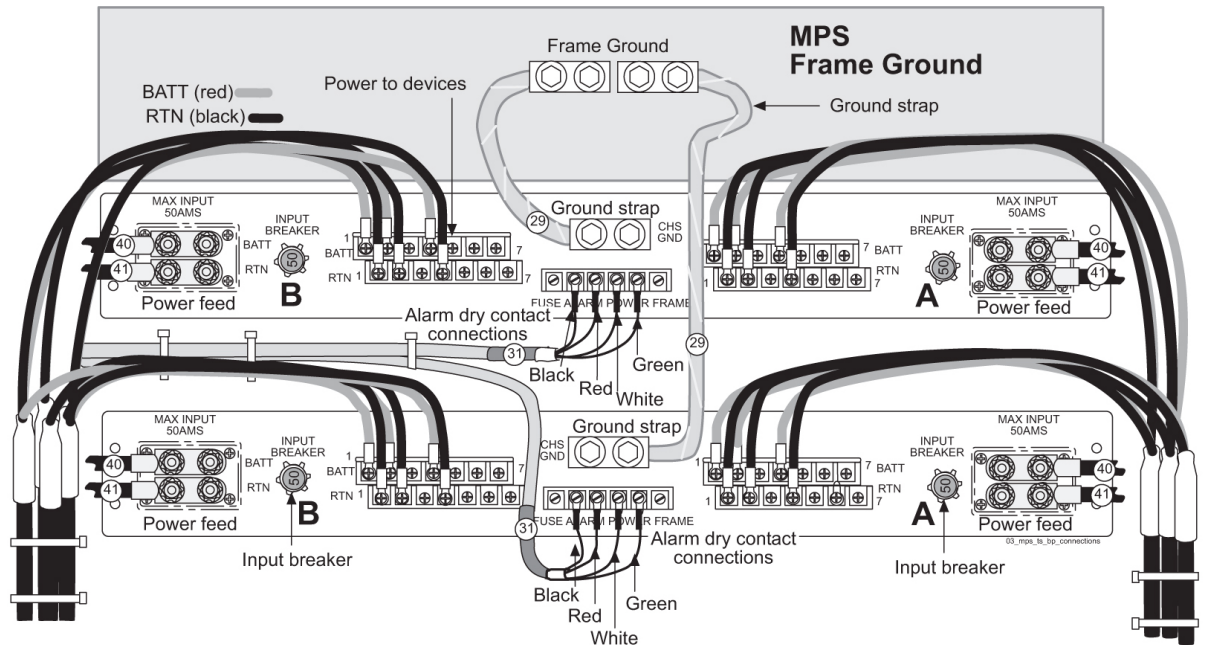
Note: The numbers shown in *Figure 45: Breaker Panel Rear View* on page 80 correspond to cable numbers in the *Tekelec 1000 Application Server Hardware Manual*. Cables are referred to by number in this procedure.

After all connections are verified as secure, return to *Step 4* on page 80.

6. Run `syscheck` (see *Running the System Health Check* on page 123).

   a) If the alarm is cleared, the problem is resolved.
   b) If the alarm is not cleared, continue to the next step.

7. If the problem is not resolved, contact call the *Customer Care Center* on page 3 for assistance.

3000000004000000 - Breaker Panel Monitoring Error

This alarm indicates a failure in the hardware, software, or both that monitors the breaker panel. A problem may exist with the file I/O libraries, the serial device drivers, or the serial hardware.

Note: When this alarm occurs, the system health check is unable to monitor the breaker panel for faults. If this alarm is detected, the breaker panel must be carefully examined for the existence of faults. The LEDs on the breaker panel will be the only indication of the occurrence of either alarm *3000000001000000 - Breaker Panel Feed Error* on page 76 or *3000000002000000 - Breaker Panel Breaker Error* on page 79 until the Breaker Panel Monitoring Error is corrected.

1. Verify that both ends of the labeled serial cables (cable 31 on *Figure 46: Breaker Panel Rear View* on page 81) are securely connected.

   Figure 46: Breaker Panel Rear View
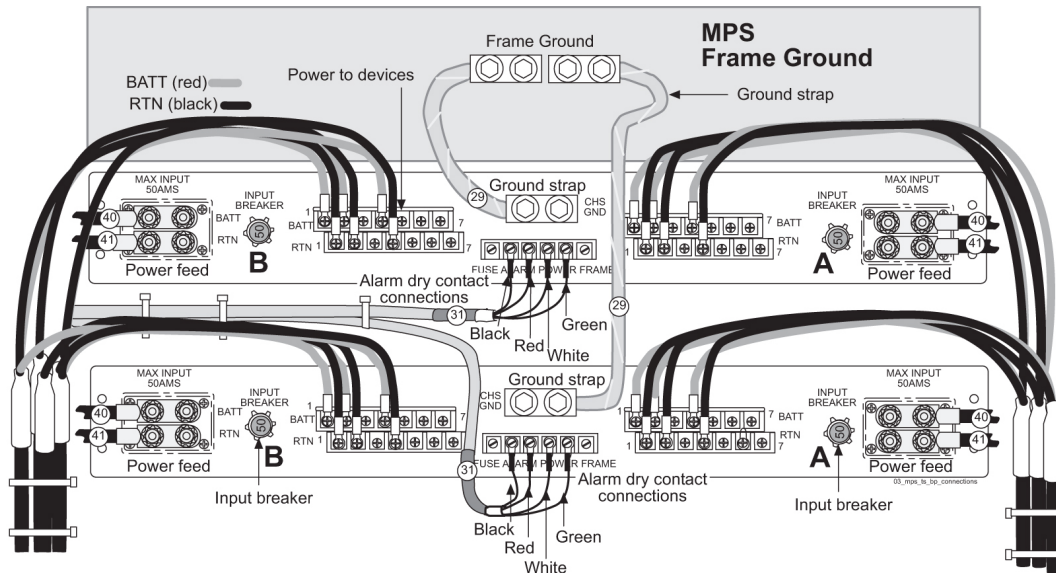
Note: The numbers shown in *Figure 46: Breaker Panel Rear View* on page 81 correspond to cable numbers described in the *Tekelec 1000 Application Server Harware Manual*. Cables are referred to by number in this procedure.

2. Run `syscheck` (see *Running the System Health Check* on page 123).

   a) If the alarm is cleared, the problem is resolved.

   b) If the alarm is not cleared, continue to the next step.

3. If the problem is not resolved, call the *Customer Care Center* on page 3 for further guidance.

Major Application Alarms

The major application alarms involve the EPAP software, RTDBs, file system, JRS connection, and logs.

4000000000000001 - Mate EPAP Unavailable

One EPAP has reported that the other EPAP is unreachable.

1. Log in to the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120).

2. View the EPAP status on the banner.

   - If the mate EPAP status is DOWN, go to*Step 4* on page 82 .
   - If the mate EPAP status is ACTIVE or STANDBY, go to *Step 7* on page 83.

3. Select the **Select Mate** menu item to change to the mate EPAP.

4. Select **Process Control>Start Software** to start the mate EPAP software.

5. View the EPAP status on the banner.

   - If the mate EPAP status is ACTIVE or STANDBY, the problem is resolved.

- If the mate EPAP status is still DOWN, continue with *Step 6* on page 83.

6. Select the **Select Mate** menu item to change back to the side that reported the alarm.

7. Stop and start the software on the side that is reporting the alarm (see *Restarting the EPAP Software* on page 130).

8. If the problem persists, run `savelogs` to gather system information for further troubleshooting (see *Saving Logs Using the EPAP GUI* on page 125), and contact the *Customer Care Center* on page 3.

4000000000000002 - RTDB Mate Unavailable

The local EPAP cannot use the direct link to the Standby for RTDB database synchronization.

1. Log in to the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120).

2. View the EPAP status on the banner.

- If the mate EPAP status is DOWN, go to *Step 4* on page 83.
- If the mate EPAP status is ACTIVE or STANDBY, go to *Step 7* on page 83.

3. Select the **Select Mate** menu item to change to the mate EPAP.

4. Select **Process Control>Start Software** to start the mate EPAP software.

5. Determine whether the alarm has cleared by verifying whether it is still being displayed in the banner or in the Alarm View window.

- If the alarm has cleared, the problem is resolved.
- If the alarm has not yet cleared, continue with *Step 6* on page 83.

6. Ensure that you are logged into the side opposite from the side reporting the alarm.

If it is necessary to change sides, select the **Select Mate** menu item to change to the side opposite the side that reported the alarm.

7. Stop and start the software on the side that is reporting the alarm (see *Restarting the EPAP Software* on page 130).

8. Select **RTDB>View RTDB Status** to verify that the RTDB status on both sides is coherent, as shown in *Figure 47: Coherent RTDB Status* on page 83.

Figure 47: Coherent RTDB Status

9. If the problem persists, run `savelogs` to gather system information for further troubleshooting (see *Saving Logs Using the EPAP GUI* on page 125), and contact the *Customer Care Center* on page 3.
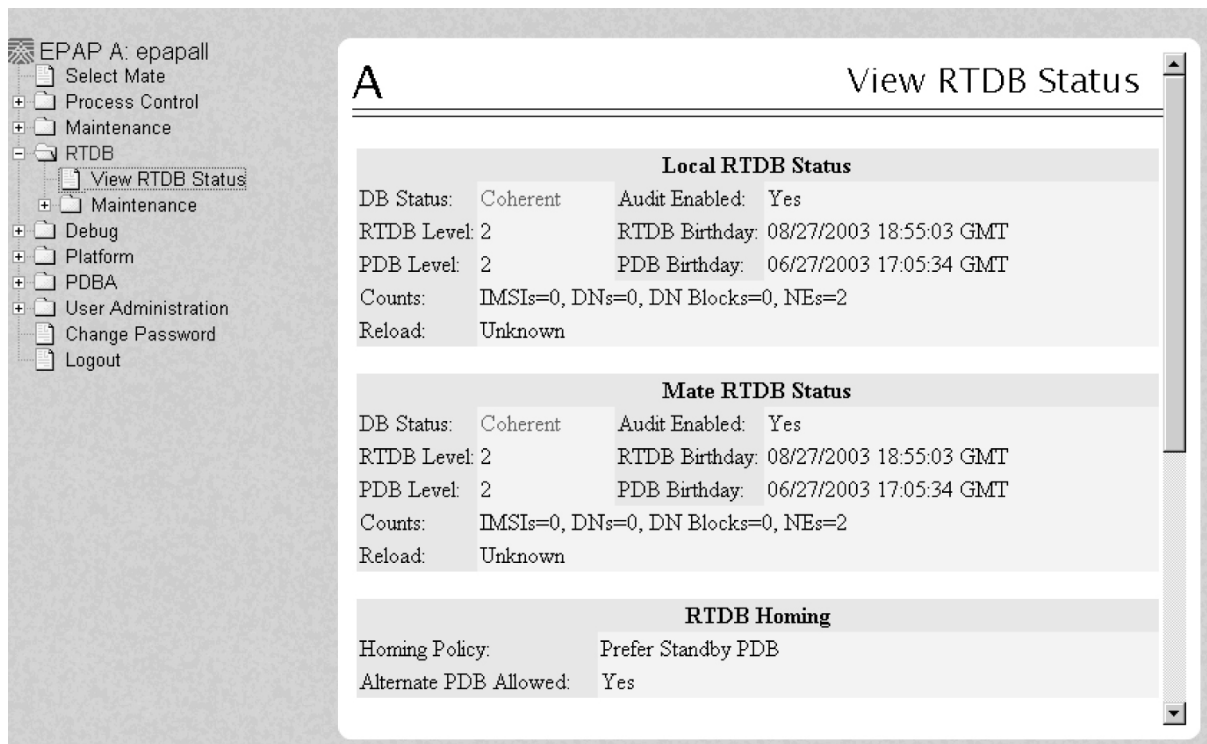
4000000000000004 - Congestion

The EPAP RTDB database record cache used to keep updates currently being provisioned is above 80% capacity.

1. At the EAGLE 5 ISS input terminal, enter the `rept-stat-mps` command to verify the status.

   Refer to the *Commands Manual* to interpret the output.

2. If the problem does not clear within 2 hours with an "EPAP Available" notice, capture the log files on both EPAPs (see *Saving Logs Using the EPAP GUI* on page 125) and contact the *Customer Care Center* on page 3.

4000000000000020 - RMTP Channels Down

Both IP multicast mechanisms are down.

1. Check the physical connections between the local MPS and the Service Module cards on the EAGLE 5 ISS.

   Make sure the connectors are firmly seated.

2. Stop and restart the software on the side that is reporting the alarm (see *Restarting the EPAP Software* on page 130).

3. Capture the log files on both EPAPs (see *Saving Logs Using the EPAP GUI* on page 125) and contact the *Customer Care Center* on page 3.

4000000000000040 - Fatal Software Error

A major software component on the EPAP has failed.

1. Perform *Restarting the EPAP Software* on page 130
2. Capture the log files on both EPAPs (see *Saving Logs Using the EPAP GUI* on page 125) and contact the *Customer Care Center* on page 3.

4000000000000080 - RTDB Corrupt

A real-time database is corrupt. The calculated checksum did not match the checksum value stored for one or more records.

Capture the log files on both EPAPs (see *Saving Logs Using the EPAP GUI* on page 125) and contact the *Customer Care Center* on page 3.

4000000000000100 - RTDB Inconsistent

This message indicates one or more of the following conditions:

- The real-time database for one or more Service Module cards is inconsistent with the current real-time database on the Active EPAP fixed disks

- RTDBs detect that it is ahead of an ACTIVE PDBA that it just connected to (probably a PDBA switchover has occurred, or a restore from a backup of PDB with a previous db level)

- RTDB timestamp of most recent level does not match the PDBAs record of that timestamp.

1. Log in to the User Interface screen of EPAP A (see *Accessing the EPAP GUI Interface* on page 120)
2. Check the banner information above the menu to verify that you are logged into the EPAP A that is reporting the problem.

   If it is necessary to switch to EPAP A, click the **Select Mate** menu item.

3. From the menu, select **RTDB>View RTDB Status** to display status information about the RTDBs.

   Figure 48: RTDB Status on page 85 shows an example.

   Figure 48: RTDB Status
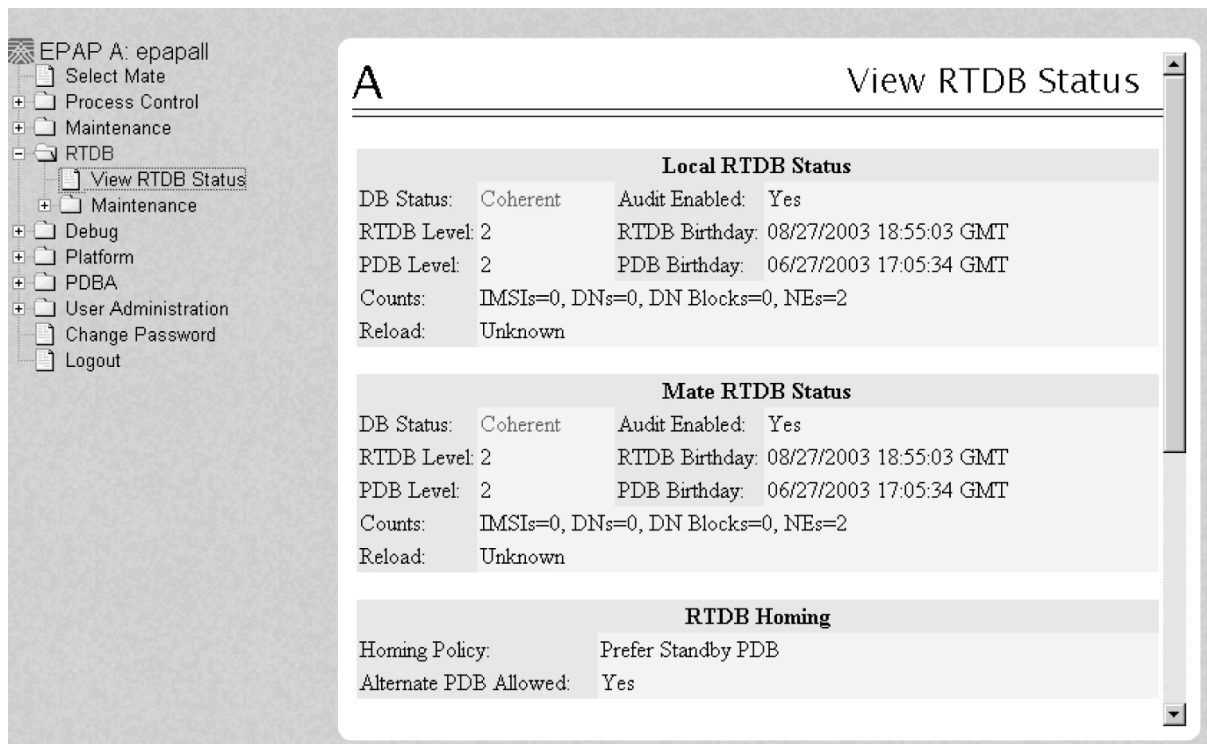
4. Verify the PDB information on the RTDB Status view is correct before continuing.

5. Before attempting to copy the RTDB, the EPAP A software must be stopped by doing the following:

CAUTION: If the software is not stopped as directed in *Substep a* on page 86 through *Substep c* on page 86, the RTDB will become corrupted.

CAUTION

a) Select **Process Control>Stop Software** to stop the software.

The following warning appears:

```
CAUTION: This action will stop all EPAP software processes, and will prevent
 the selected EPAP from updating the RTDB until the EPAP software is
re-started (by executing the Start Software menu item).
```

b) On the **Stop EPAP Software** screen, make sure the following item on the screen is checked: **Check if you want the software to automatically start on reboot.**

c) Select the **Stop EPAP Software** button to stop the software.

6. Select **RTDB>Maintenance>Reload RTDB from PDBA** .

The screen shown in *Figure 49: Reload RTDB from PDBA* on page 86 is displayed.

Figure 49: Reload RTDB from PDBA

4000000000004000 - RTDB Reload Is Required

This message indicates that the RTDB reload is required for one of the following reasons:

- The PDB Birthday on the EPAP reporting the error does not match the mate EPAP's PDB Birthday.

- The transaction logs did not contain enough information to resynchronize the databases (the transaction logs may be too small).

CAUTION:

If both sides are reporting this error, contact the *Customer Care Center* on page 3.

CAUTION

If only one side is reporting this error, use the following procedure.

1. Log in to the User Interface screen of the EPAP (see *Accessing the EPAP GUI Interface* on page 120)

2. Check the banner information above the menu to verify that you are logged into the EPAP that is reporting the problem.

   If it is necessary to switch to the problem EPAP, click the **Select Mate** menu item.

3. From the menu, select **RTDB>View RTDB Status** to display status information about the RTDBs.

   Figure 50: RTDB Status on page 88 shows an example.

   Figure 50: RTDB Status

4. If the RTDB birthdays for both the local RTDB and the mate RTDB are the same, you can copy the mate's RTDB to the local RTDB.

   If the RTDB birthdays are not the same, go to step *Step 11* on page 90.

5. Before attempting to copy the RTDB, you must stop the software on both sides by doing the following:

   ⚠ **CAUTION:** If you do not stop the software on both sides, as directed in substeps *Substep a* on page 89 through *Substep f* on page 89, the RTDBs will become corrupted.

   CAUTION

   a) Select **Process Control>Stop Software** to stop the software.
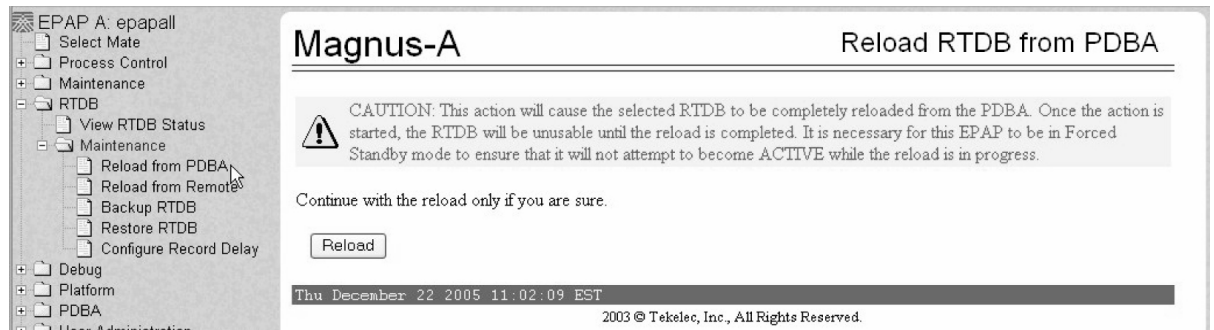
      The following warning appears:

      ```
      CAUTION: This action will stop all EPAP software processes, and will prevent
       the selected EPAP from updating the RTDB until the EPAP software is
      re-started (by executing the Start Software menu item).
      ```

   b) On the **Stop EPAP Software** screen, make sure the following item on the screen is checked:

      Check if you want the software to automatically start on reboot.

   c) Select the **Stop EPAP Software** button to stop the software.

   d) Select **Select Mate** from the menu.

   e) Repeat substeps *Substep a* on page 89 through *Substep c* on page 89 on the other side.

   f) Select **Select Mate** from the menu to return to the EPAP that is reporting the problem.

6. Verify that you are logged in to the side that is reporting the problem.

7. Select **RTDB>Maintenance>Reload from Remote**.

   The screen shown in *Figure 51: Reload RTDB from Mate EPAP* on page 89 shows this function.

   Figure 51: Reload RTDB from Mate EPAP
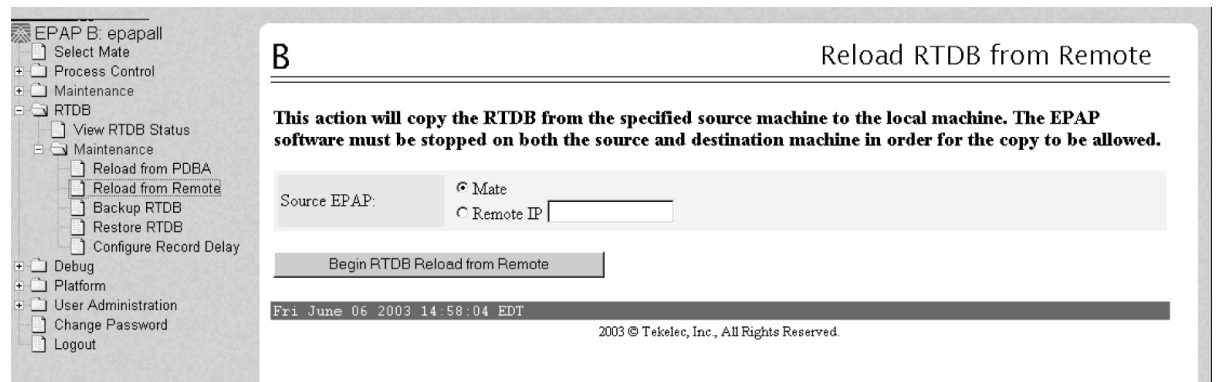
8. Ensure that the Mate radio button is filled in, as shown in *Figure 51: Reload RTDB from Mate EPAP* on page 89 and click the **Begin RTDB Reload from Remote** button.

9. When the reload has completed, start the software on both sides by doing the following:

   a) Select **Process Control>Start Software** to start the software again.

      Make sure the following item on the screen is checked (this item applies only if performing this procedure on Side A):

      Check if you want to start the PDBA software along with the EPAP software.

b) Select the **Start EPAP Software** button to start the software.

c) Select **Select Mate** from the menu.

d) Repeat substeps *Substep a* on page 89 and *Substep b* on page 90 on the other side.

10. If you wish to increase the size of the transaction logs, select **PDBA>Maintenance>Transaction Log Params>Change Params** as shown in *Figure 52: Changing Transaction Log Parameters* on page 90.

Figure 52: Changing Transaction Log Parameters
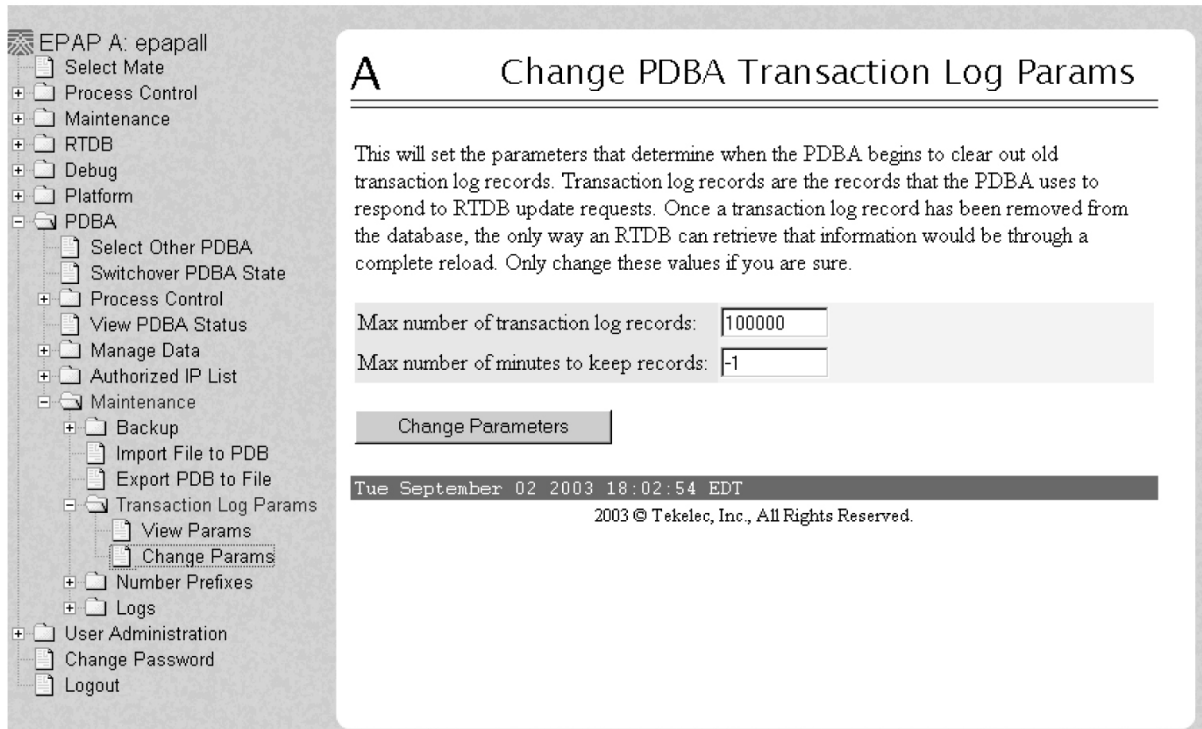
11. If the problem persists, contact the *Customer Care Center* on page 3.

4000000000008000 - Mate PDBA Unreachable

This message indicates that the other PDBA is unreachable.

1. Login to the **User Interface** screen of the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120).

2. Check the banner information above the menu for the PDBA status.

a) If neither PDBA status is DOWN, go to *Step 7* on page 92.

b) If status of one of the PDBAs is DOWN, continue with *Step 3* on page 91.

Figure 53: PDBA Down on page 90 shows an example in which the PDBA on EPAP B is DOWN.

Figure 53: PDBA Down
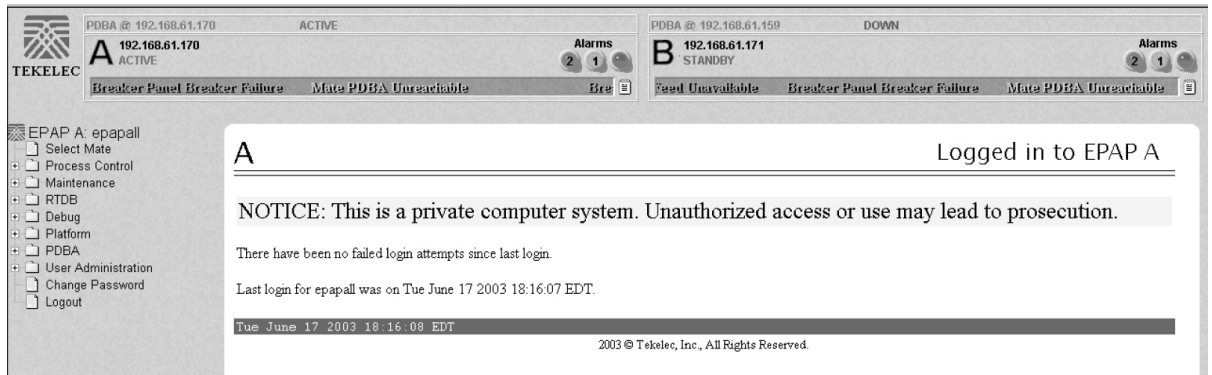
3. Check the banner information above the menu to verify that you are logged into the EPAP whose PDBA is DOWN.

   If it necessary to switch to the other PDBA, select **PDBA>Select Other PDBA** .

4. Attempt to start the PDBA by selecting **PDBA>Process Control>Start PDBA Software**.

   The window shown in *Figure 54: Start PDBA* on page 91 is displayed.

   Figure 54: Start PDBA
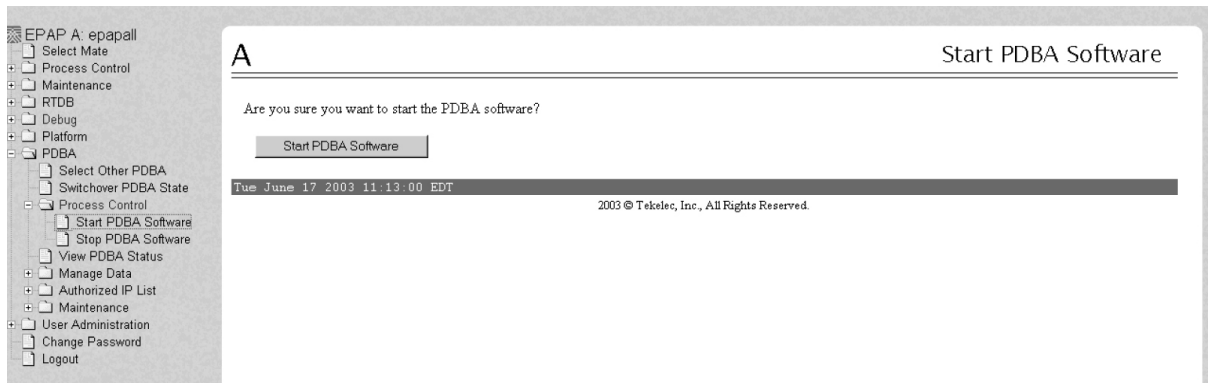
5. Click the **Start PDBA Software** button.

6. When the PDBA software has been started, the window shown in *Figure 55: PDBA Started* on page 91 displays, and within moments the banner will show the PDBA status as ACTIVE or STANDBY.

   If the status does not change to ACTIVE or STANDBY, continue to *Step 7* on page 92.

   Figure 55: PDBA Started
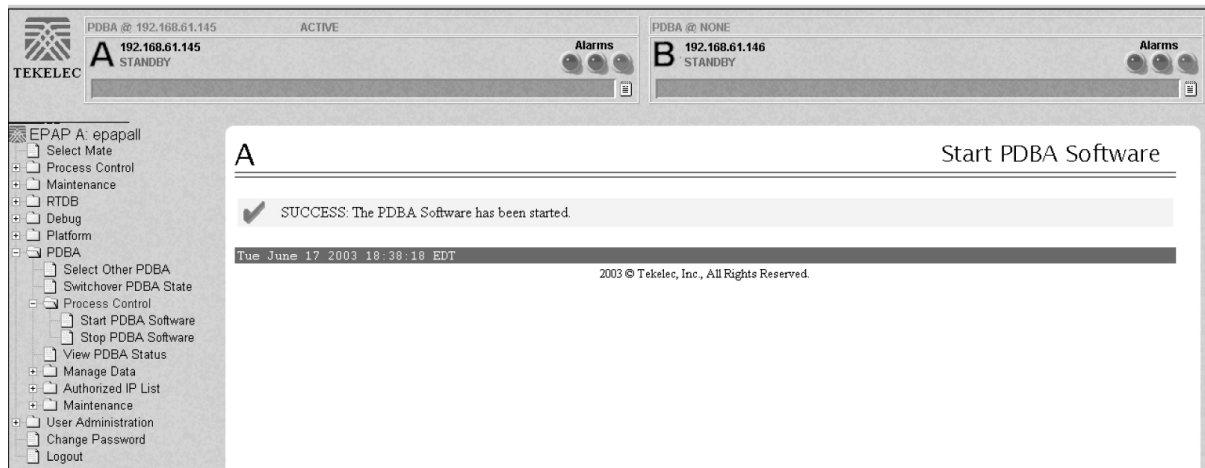
7. Check the status of the provisioning network.

   If problems exist in the provisioning network, fix them.

8. If the problem persists, run `savelogs` (see *Saving Logs Using the EPAP GUI* on page 125), and contact the *Customer Care Center* on page 3.

4000000000010000 - PDBA Connection Failure

The local EPAP RTDB process cannot connect to the local PDBA.

1. Login to the **User Interface** screen of the EPAP (see *Accessing the EPAP GUI Interface* on page 120).

2. Check the banner information above the menu to verify that you are logged into the problem EPAP indicated in the UAM.

   Select **Select Mate** if necessary to switch to the problem EPAP.

3. Perform *Restarting the EPAP and PDBA* on page 127.

4. Select **RTDB>View RTDB Status** and determine the homing policy for the PDBA.

   In the example shown in *Figure 56: Determining the Homing Policy* on page 92, the Homing Policy shows that the Standby PDB is preferred for homing.

   Figure 56: Determining the Homing Policy
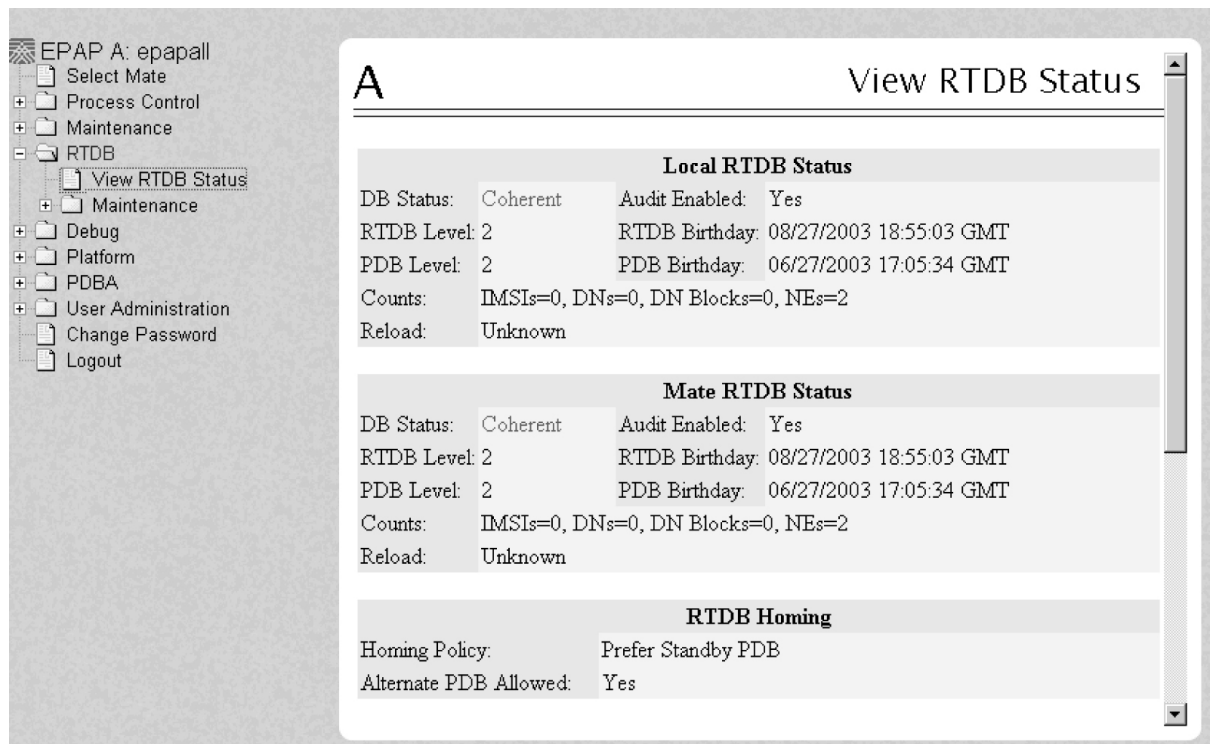
5. At the EPAP indicated by the Homing Policy, repeat *Step 3* on page 92 and *Step 4* on page 92 to restart the PDBA.

6. If the problem persists, run `savelogs` (see *Saving Logs Using the EPAP GUI* on page 125), and contact the *Customer Care Center* on page 3.

4000000000020000 - PDBA Replication Failure

Provisioning data is no longer being exchanged from the Active PDB to the Standby PDB.

1. Run `savelogs` (see *Saving Logs Using the EPAP GUI* on page 125).

2. Contact the *Customer Care Center* on page 3.

4000000000040000 - RTDB DSM Over-Allocation

At least one Service Module card in the attached EAGLE 5 ISS has insufficient memory to provision the RTDB entry. No more provisioning will be allowed to the RTDB until this issue is resolved.

Install Service Module cards in the attached EAGLE 5 ISS with sufficient memory to accommodate the expected size of the RTDB.

4000000000080000 - RTDB Maximum Depth Reached

This alarm indicates that the maximum depth has been reached for a tree. If the alarm was initiated during a data update, the update will continually fail until there is manual intervention. RTDB data is stored as inverse tree structures. The trees have a maximum depth allowed.

Contact the *Customer Care Center* on page 3.

4000000000100000 - No PDBA Proxy to Remote PDBA Connection

This message indicates that the PDBA Proxy feature is disabled or the software is down.

1. Log in to the User Interface screen of EPAP A (see *Accessing the EPAP GUI Interface* on page 120)

2. Select **PDBA>View PDBA Status** to verify that the PDBA proxy feature is enabled.

   The Local Proxy Status items only appear if the PDBA Proxy feature is enabled (See *Figure 57: View PDBA Status Screen* on page 94).

Figure 57: View PDBA Status Screen

3. Refer to *Restarting the EPAP and PDBA* on page 127 to restart the PDBA.

4. If the problem persists, capture the log files on both EPAPs (see *Saving Logs Using the EPAP GUI* on page 125) and contact the *Customer Care Center* on page 3.

4000000000200000 - DSM Provisioning Error

A coherent DSM RTDB is more than 1000 levels behind the EPAP RTDB.

Monitor this situation.

If it does not improve, contact the *Customer Care Center* on page 3 for guidance.

Minor Platform Alarms

Minor platform alarms involve disk space, application processes, RAM, and configuration errors.
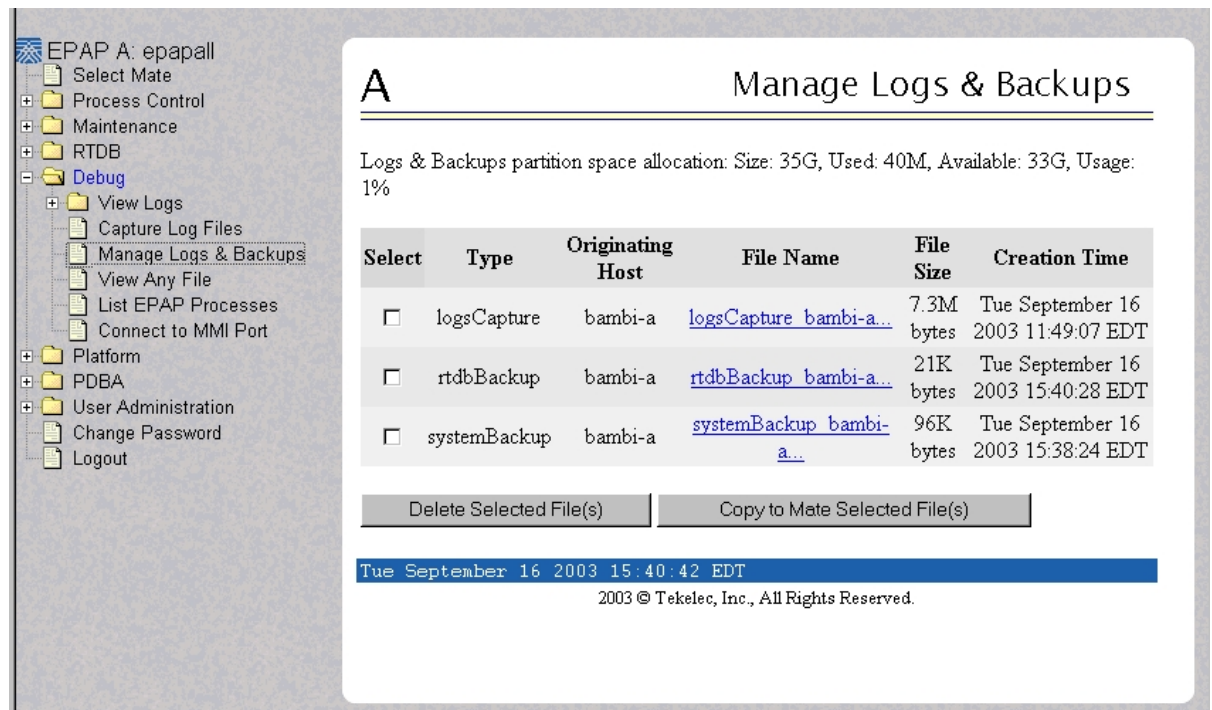
5000000000000001 - Server Disk Space Shortage Warning

This alarm indicates that one of the following conditions has occurred:

- A filesystem has exceeded a warning threshold, which means that more than 80% (but less than 90%) of the available disk storage has been used on the filesystem.

- More than 80% (but less than 90%) of the total number of available files have been allocated on the filesystem.

1. Run `syscheck` (see *Running syscheck Through the EPAP GUI* on page 123)
2. Examine the syscheck output to determine if the filesystem `/var/TKLC/epap/free` is the one that is low on space, if so, continue to *Step 3* on page 95; otherwise skip to *Step 4* on page 96.
3. You may be able to free up space on the free partition by deleting unnecessary files, as follows:
   a) Log in to the EPAPGUI (see *Accessing the EPAP GUI Interface* on page 120)
   b) Select **Debug>Manage Logs & Backups**.

      A screen similar to *Figure 58: Manage Logs and Backups* on page 95 displays. This screen displays the information about the total amount of space allocated for, and the amount of space currently used by logs and backups, and it lists logs and backup files that you might choose to delete, freeing up additional disk space.

      Figure 58: Manage Logs and Backups

c) Click the checkbox of each file that you want to delete and then click **Delete Selected File(s)**.

4. Call the *Customer Care Center* on page 3 for assistance.

5000000000000002 - Server Application Process Error

This alarm indicates that either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.

1. If a *3000000000000020 - Server Platform Process Error* on page 62 alarm is also present, execute the recovery procedure associated with that alarm before proceeding.

2. Log in to the User Interface screen of the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120)

3. Check the banner information above the menu to verify that you are logged into the problem EPAP indicated in the UAM.

   If it is necessary to switch to the other side, select **Select Mate**.

4. Open the Process Control folder, and select the **Stop Software** menu item.

5. Open the Process Control folder, and select the **Start Software** menu item.

6. Capture the log files on both EPAPs (see *Saving Logs Using the EPAP GUI* on page 125) and contact the *Customer Care Center* on page 3.

5000000000000004 - Server Hardware Configuration Error

This alarm indicates that one or more of the server's hardware components are not in compliance with Tekelec specifications (refer to the Tekelec Application Server Hardware Manual).

1. Run `syscheck` in verbose mode (see *Running syscheck Through the EPAP GUI* on page 123).

2. Call the *Customer Care Center* on page 3 for assistance.

5000000000000020 - Server Swap Space Shortage Warning

This alarm indicates that the swap space available on the server is less than expected. This is usually caused by a process that has allocated a very large amount of memory over time.

Note: In order for this alarm to clear, the underlying failure condition must be consistently undetected for a number of polling intervals. Therefore, the alarm may continue to be reported for several minutes after corrective actions are completed.

Call the *Customer Care Center* on page 3 for assistance.

5000000000000040 - Server Default Router Not Defined

This alarm indicates that the default network route is either not configured or the current configuration contains an invalid IP address or hostname.

⚠️ **CAUTION**

CAUTION: When changing the server's network routing configuration it is important to verify that the modifications will not impact the method of connectivity for the current login session. It is also crucial that this information not be entered incorrectly or set to improper values. Incorrectly modifying the server's routing configuration may result in total loss of remote network access.

1. Perform the following substeps to define the default router:

   a) Obtain the proper Provisioning Network netmask and the IP address of the appropriate Default Route on the provisioning network.

   These are maintained by the customer network administrators.

   b) Log in to the MPS with username `epapconfig` (see *Accessing the EPAP GUI Interface* on page 120).

   The server designation at this site is displayed, as well as **hostname**, **hostid**, **Platform Version**, **Software Version**, and the date. Ensure that the side displayed is the MPS that is reporting the problem. In the following example, it is MPS A.

   c) Enter option 2, `Configure Network Interfaces Menu`, from the EPAP `Configuration Menu`.

```
MPS Side A:  hostname: mpsa-d1a8f8  hostid: 80d1a8f8
             Platform Version: x.x.x-x.x.x
             Software Version: EPAP x.x.x-x.x.x
             Wed Jul 17 09:51:47 EST 2002
 /-----EPAP 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 | PDB Configuration Menu            |
|----|-----------------------------------|
|  e | Exit                              |
\-----------------------------------------/
Enter Choice:  2
```

d) Enter option 1, Configure Provisioning Network from the Configure Network Interfaces Menu.

This displays the following submenu for configuring communications networks and other information.

```
 /----Configure Network Interfaces Menu-----\
/--------------------------------------------\
|  1 | Configure Provisioning Network        |
|----|---------------------------------------|
|  2 | Configure Sync Network                |
|----|---------------------------------------|
|  3 | Configure DSM Network                 |
|----|---------------------------------------|
|  4 | Configure Backup Provisioning Network |
|----|---------------------------------------|
|  5 | Configure Forwarded Ports             |
|----|---------------------------------------|
|  6 | Configure Static NAT Addresses        |
|----|---------------------------------------|
|  7 | Configure Provisioning VIP Addresses  |
|----|---------------------------------------|
|  e | Exit                                  |
\--------------------------------------------/
Enter choice:  1
```

The following warning appears:

```
EPAP software and PDBA are running. Stop them? [N]
```

e) Type Y and press Enter.
The EPAP A provisioning network IP address displays:

```
Verifying connectivity with mate ...
Enter the EPAP A provisioning network IP Address [192.168.61.90]:
```

f) Press Enter after each address is displayed until the Default Route address displays:

```
Verifying connectivity with mate ...
Enter the EPAP A provisioning network IP Address [192.168.61.90]:
Enter the EPAP B provisioning network IP Address [192.168.61.91]:
Enter the EPAP provisioning network netmask [255.255.255.0]:
Enter the EPAP provisioning network default router IP Address: 192.168.61.250
```

g) If the default router IP address is incorrect, correct it, and press Enter.

h) After you have verifying or correcting the Provisioning Network configuration information, enter **e** to return to the Configure Network Interfaces Menu.

i) Enter **e** again to return to the EPAP Configuration Menu.

2. Rerun `syscheck`. If the alarm has not been cleared, go to *Step 3* on page 99 .

3. Contact *Customer Care Center* on page 3 for assistance.

5000000000000080 - Server Temperature Warning

This alarm indicates that the internal temperature within the server is outside of the normal operating range. A *3000000000000001 - Server Fan Failure* on page 60 may also exist along with this warning.

1. Ensure that nothing is blocking the fan's intake (see *Figure 59: Server Fans* on page 99) and remove any blockage.

Figure 59: Server Fans

2. Verify that the temperature in the room is normal (see *Table 13: Server Environmental Conditions* on page 99). If it is too hot, lower the temperature in the room to an acceptable level.

Table 13: Server Environmental Conditions

Ambient Temperature	Normal Operating Temperature Range: 5 degrees C to 40 degrees C
	Exceptional Operating Limit: -5 degrees C to 50 degrees C (operation for no more than 96 hours duration at extremes and at elevations of less than 1800 meters)
	Storage: -20 degrees C to 60 degrees C
Relative Humidity	Operating: 5% to 85% non-condensing
	Storage: 5% to 95% non-condensing

Elevation	Operating: -300m to +300m
	Storage: -300m to +1200m
Heating, Ventilation, and Air Conditioning	Capacity must compensate for up to 5100 BTUs/hr for each installed frame.
	Calculate HVAC capacity as follows:
	Determine the wattage of the installed equipment.
	Use the formula: watts x 3.143 = BTUs/hr

Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. The alarm may take up to five minutes to clear after conditions improve. It may take about ten minutes after the room returns to an acceptable temperature before syscheck shows the alarm cleared.

3. Run syscheck (see *Running syscheck Through the EPAP GUI* on page 123). If the alarm has not been cleared, continue with *Step 4* on page 100

4. Replace the filter by performing *Replacing Fan Filters* on page 36 .

   Note: Be prepared to wait the appropriate period of time before continuing with the next step. Conditions need to be below alarm thresholds consistently for the alarm to clear. The alarm may take up to five minutes to clear after conditions improve. It may take about ten minutes after the filter is replaced before syscheck shows the alarm cleared.

5. Run syscheck (see *Running syscheck Through the EPAP GUI* on page 123). If the alarm has not been cleared, continue with *Step 6* on page 100.

6. If the problem has not been resolved, call *Customer Care Center* on page 3 for assistance.

5000000000000100 - Server Core File Detected

This alarm indicates that an application process has failed and debug information is available.

1. Run savelogs to gather system information (see *Running syscheck Through the EPAP GUI* on page 123")

2. Contact the *Customer Care Center* on page 3.

   They will examine the files in /var/TKLC/core and remove them after all information has been extracted.

5000000000000200 - Server NTP Daemon Not Synchronized

This alarm indicates that the NTP daemon (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.

Contact the *Customer Care Center* on page 3.

5000000000000400 - Server CMOS Battery Voltage Low

The presence of this alarm indicates that the CMOS battery voltage has been detected to be below the expected value. This alarm is an early warning indicator of CMOS battery end-of-life failure which will cause problems in the event the server is powered off.

Contact the *Customer Care Center* on page 3.

5000000000000800 - Server Disk Self Test Warning

A non-fatal disk issue (such as a sector cannot be read) exists.

Contact the *Customer Care Center* on page 3.

5000000000004000 - Server Reboot Watchdog Initiated

This alarm indicates that the server has been rebooted due to a hardware watchdog.

Contact the *Customer Care Center* on page 3.

Minor Application Alarms

Minor application alarms involve the EPAP RMTP channels, RTDB capacity, and software errors.

6000000000000001 - RMTP Channel A Down

Channel A of the IP multicast mechanism is not available.

1. Check the physical connections between the local EPAP(s), and the EPAP(s) and the Service Module cards on the EAGLE 5 ISS. Make sure the connectors are firmly seated.
2. Run `syscheck` (see *Running syscheck Through the EPAP GUI* on page 123)

   If you cannot log in, go to *Step 5* on page 101.
3. Perform *Restarting the EPAP Software* on page 130.
4. Capture the log files on both EPAPs (see *Saving Logs Using the EPAP GUI* on page 125")
5. Contact the *Customer Care Center* on page 3.

6000000000000002 - RMTP Channel B Down

Channel B of the IP multicast mechanism is not available.

1. Check the physical connections between the local EPAP(s), and the EPAP(s) and the Service Module cards on the EAGLE 5 ISS.

   Make sure the connectors are firmly seated.
2. Run `syscheck` (see *Running syscheck Through the EPAP GUI* on page 123).

If you cannot log in, go to *Step 5* on page 102.

3. Perform *Restarting the EPAP Software* on page 130.

4. Capture the log files on both EPAPs (see *Saving Logs Using the EPAP GUI* on page 125).

5. Contact the *Customer Care Center* on page 3.

6000000000000008 - RTDB 80% Full

The RTDB on the EPAP or DSM is approaching capacity (80%).

Note: This is an indication to the user to immediately make plans for an EPAP upgrade or upgrade the Service Module card to add more memory.

1. At the EAGLE 5 ISS input terminal, enter the `rept-stat-mps` command.

2. Refer to the output to determine which specific database (for an EPAP or for a Service Module card) is approaching its capacity.

3. Run `savelogs` on each EPAP (see *Saving Logs Using the EPAP GUI* on page 125), and contact the *Customer Care Center* on page 3.

6000000000000020 - Standby PDBA Falling Behind

This is an indication that there is a congestion condition affecting updates to the standby PDBA. The amount of time between an update being committed in the Active PDB and the same update being committed in the Standby PDB has reached an unacceptable level.

The EPAP attempts to automatically recover from this situation. This error can result from one of the following conditions:

• Provisioning activity is very heavy

• The provisioning network is experiencing errors or latency

• Server maintenance functions (such as backups, restores, imports, exports, etc) are occurring

1. Periodically, verify that the level of the standby PDBA is catching up by selecting **PDBA>View PDBA Status** and comparing the Level of the Standby PDBA (on EPAP A in the example shown in *Figure 60: View PDBA Status* on page 102) to the Level of the Active PDBA (on EPAP B in the example).

Figure 60: View PDBA Status

PDBA @ 192.168.61.170 STANDBY PDBA @ 192.168.61.159 ACTIVE

TEKELEC

A 192.168.61.170
ACTIVE

Alarms
2

B 192.168.61.171
STANDBY

Alarms
2

anel Feed Unavailable   Breaker Panel Breaker Failure   eaker Panel Breaker Failure   Break

EPAP A: epapall
Select Mate
Process Control
Maintenance
RTDB
Debug
Platform
PDBA
  Select Other PDBA
  Switchover PDBA State
  Process Control
  View PDBA Status
  Manage Data
  Authorized IP List
  Maintenance
User Administration
Change Password
Logout

A   View PDBA Status

PDBA@192.168.61.170 Status

Status:	STANDBY	Version:	1.0
Level:	1448036	Birthday:	06/10/2003 17:40:17 GMT
DN Prefix:		IMSI Prefix:	
Counts:	IMSIs=5324496, DNs=10362100, DN Blocks=1, NEs=426		
RTDB Clients:	Address	Level	

PDB@192.168.61.170 Status

Status:	Database daemon is running
Counts:	IMSIs=5324496, DNs=10362100, DNBlocks=1, NEs=426

PDBA@192.168.61.159 Status

Status:	ACTIVE	Version:	1.0
Level:	1448036	Birthday:	06/10/2003 17:40:17 GMT
DN Prefix:		IMSI Prefix:	
Counts:	IMSIs=5324496, DNs=10362100, DN Blocks=1, NEs=426		
RTDB Clients:	Address	Level	
	192.168.2.200 (mate)	1448036	
	192.168.61.170	1448036	
	192.168.61.171	1448036	
	192.168.61.159	1448036	

PDB@192.168.61.159 Status

Status:	Database daemon is not running

Sat June 14 2003 17:09:42 EDT

2003 © Tekelec, Inc., All Rights Reserved.

2. If the problem persists for more than two hours, run `savelogs` (see *Saving Logs Using the EPAP GUI* on page 125), and contact *Customer Care Center* on page 3 for assistance.

6000000000000040 - RTDB Tree Error

This alarm indicates either that the depth is greater than the theoretical maximum or that some other general problem has been found with a tree. RTDB data is stored as inverse tree structures. The trees have maximum theoretical depths based on the number of records in the tree.

Contact the *Customer Care Center* on page 3.

6000000000000080 - PDB Backup failed

The PDB backup failed because of at least one of the following conditions:

- A manual backup script was not able to create PDB backup successfully
- A PDB backup was already in progress when Automatic PDB backup attempted to start
- A PDB restore was in progress when the Automatic PDB backup attempted to start

To verify the exact failure condition, refer to the error string in the log file.

Note: This alarm will also clear if the Automatic PDB/RTDB backup executes successfully during the next scheduled backup time.

To clear this alarm immediately, perform one of the following:

- Cancel the Automatic PDB / RTDB backup via the EPAP GUI as follows:

    Note: Automatic PDB / RTDB Backup will have to be rescheduled if it is cancelled.

    1. Log in to the User Interface screen of the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120).

    2. From the menu, select **Maintenance>Automatic PDB/RTDB Backup** to display the automatic backup screen.

    3. From the **Automatic PDB/RTDB Backup** screen, select **None** as the **Backup Type.**

    4. Select the **Schedule Backup** button to complete the cancellation.

        Automatic PDB/RTDB Backup will have to be rescheduled. Refer to the EPAP *Administration Manual* to reschedule the Automatic PDB / RTDB Backup.

- Perform a manual backup via the EPAP GUI (see *Backing Up the RTDB* on page 30).

6000000000000100 - Automatic PDB Backup failed

The PDB backup failed because of at least one of the following conditions:

- The mate machine was not reachable.
- The SCP command to transfer of PDB backup file to mate fails
- The transfer of Automatic PDB Backup to Mate fails
- The transfer of Automatic PDB Backup to mate failed due to disk space shortage on mate
- The remote machine was not reachable
- The connection to remote host failed for SFTP of the PDB Backup file
- The SFTP to the remote host failed for Automatic PDB Backup
- The login or password configured for the Remote machine is wrong for the configured user
- The Destination File Path to store the PDB Backup file in Remote machine configured by the user does not exist
- The transfer of the Automatic PDB Backup to the remote failed due to disk space shortage on the remote

To verify the exact failure condition, refer to the error string in the log file.

Note: This alarm will clear if the Automatic PDB / RTDB backup executes successfully during the next scheduled backup time.

To clear this alarm immediately, cancel the Automatic PDB/RTDB backup via the EPAP GUI, as described in *Substep a* on page 104 through *Substep d* on page 104.

Note: Automatic PDB/RTDB Backup will have to be rescheduled if it is cancelled.

a) Log in to the User Interface screen of the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120).
b) From the menu, select **Maintenance>Automatic PDB/RTDB Backup** to display the **Automatic PDB/RTDB Backup** screen.
c) From the **Automatic PDB/RTDB Backup** screen, select **None** as the **Backup Type.**
d) Select the **Schedule Backup** button to complete the cancellation.

Note: Automatic PDB/RTDB Backup will have to be rescheduled. Refer to the *EPAP Administration Manual* to reschedule the Automatic PDB/RTDB Backup.

6000000000000200 - RTDB Backup failed

The RTDB backup failed because of at least one of the following conditions:

- The manual backup script (backupRtdb.pl) was not able to create RTDB Backup successfully.
- The EPAP software could not be successfully stopped in order for Automatic RTDB Backup to start.
- Another user has already stopped the EPAP Software before the script stops the EPAP Software for Automatic RTDB Backup
- Another user is currently stopping the EPAP Software. The Automatic RTDB Backup script cannot stop the EPAP Software.
- The GUI Server returned an error when trying to get a lock from it for Automatic RTDB Backup.
- Not able to connect to GUI server for Automatic RTDB Backup
- The EPAP software was not running when it was to be stopped for Automatic RTDB Backup
- The mate machine is not reachable.

To verify the exact failure condition, refer to the error string in the log file.

Note: This alarm will clear if the Automatic PDB/RTDB backup executes successfully during the next scheduled backup time.

To clear this alarm immediately, perform one of the following:

- Cancel the Automatic PDB/RTDB backup via the EPAP GUI.

  Note: Automatic PDB/RTDB Backup will have to be rescheduled if it is cancelled.

  1. Log in to the User Interface screen of the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120).
  2. From the menu, select **Maintenance>Automatic PDB/RTDB Backup** to display the **Automatic PDB/RTDB Backup** screen.
  3. From the **Automatic PDB/RTDB Backup** screen, select **None** as the **Backup Type.**
  4. Select the **Schedule Backup** button to complete the cancellation. Automatic PDB/RTDB Backup will have to be rescheduled. Refer to the *EPAP Administration Manual* to reschedule the Automatic PDB/RTDB Backup.

- Perform a manual backup via the EPAP GUI as described in *Backing Up the RTDB* on page 30.

6000000000000400 - Automatic RTDB Backup failed

The RTDB backup failed because of at least one of the following conditions:

- The mate machine is not reachable.
- Automatic RTDB Backup file transfer to the Mate failed.

- Unable to connect to Remote host IP Address for Automatic RTDB Backup.

- Automatic RTDB Backup file transfer to the Remote failed.

- The incorrect login or password configured for Automatic RTDB Backup.

- The destination path does not exist in remote machine IP Address for Automatic RTDB Backup.

To verify the exact failure condition, refer to the error string in the log file.

Note: This alarm will clear if the Automatic PDB/RTDB backup executes successfully during the next scheduled backup time.

> To clear this alarm immediately, cancel the Automatic PDB / RTDB backup via the EPAP GUI as described in *Substep a* on page 106 through *Substep d* on page 106.
>
> **Note:** Automatic PDB/RTDB Backup will have to be rescheduled if it is cancelled.
>
> a) Log in to the User Interface screen of the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120).
> b) From the menu, select **Maintenance>Automatic PDB/RTDB Backup** to display the **Automatic PDB/RTDB Backup** screen.
> c) From the **Automatic PDB/RTDB Backup** screen, select **None** as the **Backup Type.**
> d) Select the **Schedule Backup** button to complete the cancellation. Automatic PDB/RTDB Backup will have to be rescheduled. Refer to the *EPAP Administration Manual* to reschedule the Automatic PDB/RTDB Backup.

6000000000001000 - SSH tunnel not established

One or more SSH tunnels has been enabled in the past, but the cron job was not able to re-establish the SSH tunnel with all of the Authorized PDBA Client IP addresses.

- Verify that the Customer Provisioning Application (CPA) machine is up and running.

  - If the CPA machine is not running, restart it and wait for the alarm to clear.
  - If the CPA machine is running, or if the alarm does not clear, contact *Customer Care Center* on page 3.

Chapter

5

MPS Field Replaceable Units

Topics:

This chapter includes guidelines and procedures for field replaceable units of the T1000-based Multi-Purpose Server.

Introduction

Field Replaceable Units (FRUs) are units of hardware that the customer can replace in the field. The following type of FRUs are described in this section:

- *Table 14: MPS-Specific FRUs* on page 108 lists the FRUs that are specific to the MPS. The procedures to replace these FRUs are described in the referenced manuals.
- *Table 15: Tekelec T1000 AS FRUs (No Further Action Required)* on page 109 lists the FRUs that are common to Tekelec 1000 AS implementations and for which replacement is described in the referenced manuals.
- *Table 16: Tekelec T1000 AS FRUs (Further Action Required)* on page 110 lists FRUs that are common to all Tekelec 1000 AS implementations, but for which additional recovery actions must be performed by *Customer Care Center* on page 3.

General FRU Guidelines

Use the following guidelines when you replace any FRU:

- When unpacking, check the shipping carton for damage.
- Always use a static strap when handling the components.
- Read the instructions prior to performing the replacement or maintenance.
- Do not use excessive force when installing or removing the component. Damage to a connector may result. Apply even pressure when installing the component.
- When the procedures instruct you to install a component, you can also remove an existing component for replacement purposes.
- Always test the installed or replaced component to ensure correct operation.

Locating FRU Replacement Procedures

Table 14: MPS-Specific FRUs on page 108 through *Table 16: Tekelec T1000 AS FRUs (Further Action Required)* on page 110 list the FRU part numbers and replacement procedures to perform.

Table 14: MPS-Specific FRUs

FRU	Vendor Part Number	Tekelec Part Number	Replace with	Replacement Procedure
Breaker Panel	Telect T009-5010F1F1A33	804-1423-01[*] or 804-1423-R01	804-1423-R01	*Breaker Panel Replacement Procedure* on page 112
Breaker Panel Alarm Card	Telect 400185	0804-1489-01[*] or 804-1489-R01	804-1489-R01	For detailed installation and replacement procedures, refer

FRU	Vendor Part Number	Tekelec Part Number	Replace with	Replacement Procedure
				to the *Telect* ATO *Configurable Breaker Panel User Manual*, part number 118267, Issue A, Rev 0. Section 6 provides detailed information on "Operation."
Hub	Garrett DS8016R-48VDC	804-1198-01[*] or 804-1198-R01	804-1198-R01	*Hub Replacement Procedure* on page 114

[*] This FRU is functionally equivalent to the one specified by the replacement part number

Table 15: Tekelec T1000 AS FRUs (No Further Action Required) on page 109 lists the FRUs whose replacement procedures are described in the *Tekelec T1000* Application Server *Hardware Manual*. Because replacing fan filters is recommended as regular preventive maintenance, the procedure for replacing fan filters is included in this manual and in the *Tekelec T1000 Application Server Hardware Manual*.

Note: All steps needed to replace the FRUs shown in *Table 15: Tekelec T1000 AS FRUs (No Further Action Required)* on page 109 are contained in the referenced procedure. No other action is required.

Table 15: Tekelec T1000 AS FRUs (No Further Action Required)

FRU	Vendor Part Number	Tekelec Part Number	Replace with	Replacement Procedure
Fan Filter	N/A	551-0022-01	551-0022-01	*Replacing Fan Filters* on page 36 (This replacement can be performed while the MPS is in service.)
Fan Assembly	N/A	840-1125-02	840-1125-02	*Tekelec T1000* Application Server *Hardware Manual* (This replacement can be performed

FRU	Vendor Part Number	Tekelec Part Number	Replace with	Replacement Procedure
				while the MPS is in service.)
CD/DVD Drive Assembly	N/A	870-2746-01[*] or 870-2746-02	870-2746-02	*Tekelec T1000*Application Server *Hardware Manual* (this replacement can be performed while the MPS is in service)

[*] This FRU is functionally equivalent to the one specified by the replacement part number

Table 16: Tekelec T1000 AS FRUs (Further Action Required) on page 110 lists the FRUs whose replacement procedures are described in the *Tekelec T1000 Application Server Hardware Manual.*

CAUTION: Replacing one of the FRUs in *Table 16: Tekelec T1000 AS FRUs (Further Action Required)* on page 110 usually requires additional action to ensure that system and application data is also properly restored. Although general guidelines are shown here, always contact the *Customer Care Center* on page 3 for assistance with a complete replacement procedure.

Table 16: Tekelec T1000 AS FRUs (Further Action Required)

FRU	Vendor Part Number	Tekelec Part Number	Replace with	Outline of Replacement Procedure
MPS Server (Tekelec T1000 AS)	N/A	870-2640-01[*] or 870-2640-03	870-2640-03	1. Contact the *Customer Care Center* on page 3 to perform the remaining steps. 2. Shut down the software, as described in *MPS Server Power Down Procedure* on page 115 3. Replace the server, as described in

FRU	Vendor Part Number	Tekelec Part Number	Replace with	Outline of Replacement Procedure
				the *Tekelec T1000*Application Server *Hardware Manual* . 4. Ensure that system and application data is properly restored.
Disk Drive	N/A	804-1804-01* or 804-1804-R01	804-1804-R01	1. Contact *Customer Care Center* on page 3 to perform the remaining steps. 2. Prepare for removing the disk by removing from the mirroring software all references to the failed disk. 3. Replace the disk drive, as described in the *Tekelec T1000*Application Server *Hardware Manual.* 4. Ensure that system and application data is properly restored.
PCI cards	N/A	Varies	Varies	1. Contact the *Customer Care*

FRU	Vendor Part Number	Tekelec Part Number	Replace with	Outline of Replacement Procedure
				Center on page 3 to perform the remaining steps. 2. Shut down MPS server using *MPS Server Power Down Procedure* on page 115. 3. Replace PCI card, as described in the *Tekelec T1000 Applications Server Hardware Manual*. 4. Reboot the MPS using *Rebooting the MPS* on page 134.
Always contact *Customer Care Center* on page 3 when attempting to replace a FRU in this table.				
[*] This FRU is functionally equivalent to the one specified by the replacement part number.				

Fan Replacement Procedure

The Tekelec T1000 AS fan assembly can be replaced while the MPS is in service. For detailed replacement procedures, refer to the *Tekelec T1000*Application Server *Hardware Manual* .

Breaker Panel Replacement Procedure

This procedure explains how to remove the breaker panel. For more information about how the breaker panels are configured, see *Breaker Panels* on page 15.

It is recommended that one panel remain powered while removing the other panel. This will enable the MPS to remain in-service while replacing a panel.

DANGER:

Breaker panels contain high current capacities which can be dangerous to personnel and equipment. Before replacing a breaker panel, contact the *Customer Care Center* on page 3.

DANGER

1. Turn off the breakers for the MPS Server and the hubs at the failed breaker panel.

   See *Table 17: Breaker Panel Assignments* on page 113 to identify the appropriate breakers.

Table 17: Breaker Panel Assignments

Breaker Position	Breaker Value	BP-1 Panel A	BP-1 Panel B	BP-2 Panel A	BP-2 Panel B
1	15.0A	MPS Server A Feeds	MPS Server B Feeds	MPS Server A Feeds	MPS Server B Feeds
2	1.0A	Hub 1 A Feed	Hub 3 B Feed	Hub 3 A Feed	Hub 1 B Feed
3	15.0A	Reserved	Reserved	Reserved	Reserved
4	1.0A	Hub 2A Feed	Hub 4 B Feed	Hub 4 A Feed	Hub 2 B Feed
5	10.0A	Not Used	Not Used	Not Used	Not Used
6	3.0A	Not Used	Not Used	Not Used	Not Used
7	3.0A	Not Used	Not Used	Not Used	Not Used

2. Turn off the breakers at the main power panel for the "A" and "B" power sources to the failed breaker panel.
3. Verify that power is not present on the leads by checking with a Volt Ohm Meter at the "A" and "B" power input leads on the back of the failed breaker panel.
4. Disconnect the BATT and RTN leads from the power source for "A" and "B" at the breaker panel you want to remove.
   Mark or label each cable as you remove it. Tape or insulate all disconnected power leads.
5. Disconnect from the failed breaker panel all BATT and RTN leads for the hubs and MPS Servers A and B.
6. Disconnect the alarm cable from the failed breaker panel.
7. Disconnect the frame ground from the failed breaker panel.
8. Remove the screws that hold the failed breaker panel in the frame.
9. Remove the failed breaker panel.

10. To install the replacement panel, refer to the *Signaling Products Integrated Applications Installation Manual*.

Hub Replacement Procedure

This procedure explains how to remove a hub. For more information about the hubs, see *Hubs* on page 14.

Refer to the "Hub Installation Procedure" in the *Signaling Products Integrated Applications Installation Manual* to install the replacement hub.

1. Turn off the power switch on the rear of the hub to be replaced and on the rear of the other hub on the same network as the hub to be replaced.

> ⚠️ **CAUTION:** Always turn off the power to both the hub to be replaced and to the other hub on its network. That is, turn the power off to both hubs 1 and 2 (main network) or to both hubs 3 and 4 (backup network)—but not to both pairs of hubs **CAUTION** at once.

2. Turn off the hub breakers at the breaker panel.

   Table 18: Hub Breakers (Main Network) on page 114 and *Table 19: Hub Breakers (Backup Network)* on page 114 show the breakers for the hubs.

Table 18: Hub Breakers (Main Network)

Hub	Breaker Panel	Breaker
Hub 1 (A leads)	BP-1	A2
Hub 1 (B leads)	BP-2	B2
Hub 2 (A leads)	BP-1	A4
Hub 2 (B leads)	BP-2	B4

Table 19: Hub Breakers (Backup Network)

Hub	Breaker Panel	Breaker
Hub 3 (A leads)	BP-2	A2
Hub 3 (B leads)	BP-1	B2
Hub 4 (A leads)	BP-2	A4

Hub	Breaker Panel	Breaker
Hub 4 (B leads)	BP-1	B4

3. Remove the power terminal strip cover.
4. Disconnect the BATT and RTN leads from the breaker panel for "A" and "B".
5. Disconnect the frame ground.
6. Make sure that all RJ45 cables are labeled, and disconnect all the RJ45 cables.
7. Remove the screws that hold the hub in the frame.
8. Remove the hub.
9. To install the replacement hub, use the "Hub Installation Procedure" in the *Signaling Products Integrated Applications Installation Manual* .
10. Make sure that the other hub on the same network is also powered up.

MPS Server Power Down Procedure

Use the following procedure to shut down the MPS software and turn off power to the MPS server. For more information about the Halt MPS interface menu item, refer to the *EPAP Administration Manual*. Use this procedure before performing the following replacement procedures:

- Replacing a Tekelec T1000 AS main unit (after shutting down the MPS server, refer to the *Tekelec T1000*Application Server *Hardware Manual* for the procedure for replacing the server)

- Replacing a disk drive (after shutting down the MPS server, refer to the *Tekelec T1000*Application Server *Hardware Manual* for the procedure for replacing the disk drive)

Note: After the replacement is complete, power up and test the MPS Server.

The following procedure includes details on how to shut down the MPS Server from the EPAP GUI. For more information about the Halt MPS interface menu item, refer to the *EPAP Administration Manual*.

CAUTION: Performing this procedure will cause interruption of service.

warning: DONOT perform the last step (to turn off the breakers) until *Step 1* on page 115 through *Step 5* on page 116 are complete.

1. Login to the User Interface screen of the EPAP (see *Accessing the EPAP GUI Interface* on page 120).
2. Check the banner information above the menu to verify that you are logged into the problem EPAP indicated in the UAM.

   If it is necessary to switch to the proper EPAP associated with the MPS to be powered down, select the **Select Mate** menu item.

3. When you are logged into the MPS to be powered down, select **Platform>Halt the MPS** menu item to stop the MPS.

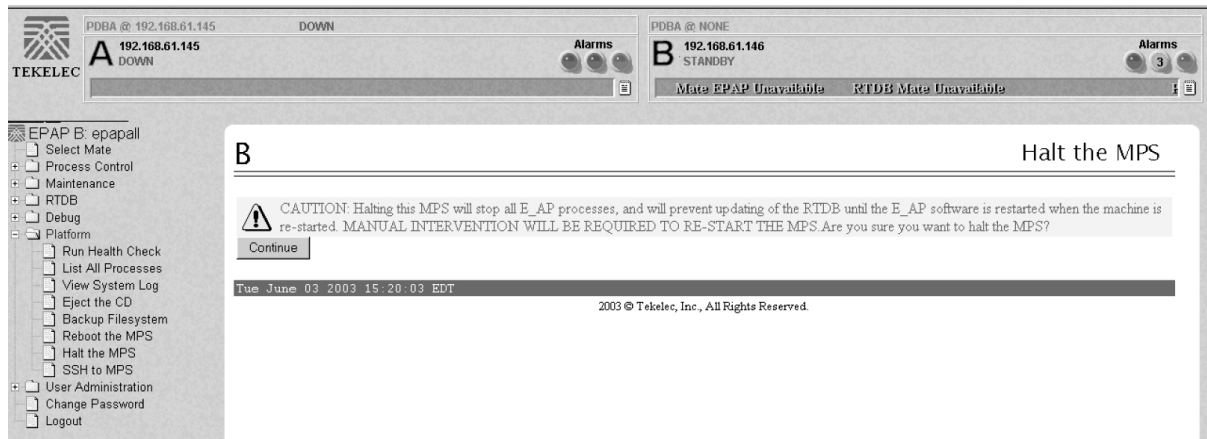The screen shown in *Figure 61: Halting the MPS* on page 116 is displayed:

Figure 61: Halting the MPS

4. Click the **halt_MPS** button.

The confirmation message shown in *Figure 62: Halting the MPS Confirmation* on page 116 appears:

Figure 62: Halting the MPS Confirmation

5. Click the **Continue** button.

Note: The EPAP software and the MPS Server are now shut down. The MPS Server can be powered down.

⚠️ **WARNING**

warning: DO NOT continue with *Step 6* on page 116 to turn off the breakers until *Step 1* on page 115 through *Step 5* on page 116 are complete.

6. To power down the MPS Server, turn off breakers A1 and B1 on the appropriate breaker panels for the MPS Server that is to be shut down (see *Table 20: MPS Server A Breaker Locations* on page 117 and *Table 21: MPS Server B Breaker Locations* on page 117).

For more information about breaker panels, see *Breaker Panels* on page 15 .

Table 20: MPS Server A Breaker Locations

MPS Server	Breaker Panel	Breaker
A	BP-1	A1
A	BP-2	B1

Table 21: MPS Server B Breaker Locations

MPS Server	Breaker Panel	Breaker
B	BP-1	B1
B	BP-2	A1

The selected MPS Server is shut down and powered down.

Disk Drive Replacement Procedure

warning: Disk drive replacement should be performed only by the *Customer Care Center* on page 3. If a disk drive needs to be replaced, contact the *Customer Care Center* on page 3.

When the *Customer Care Center* on page 3 replaces a disk drive, they perform the following functions:

1. Once the disk that is failed has been determined, prepare for removing the disk by removing from the mirroring software all references to the failed disk.
2. Shut down the MPS Server, using *MPS Server Power Down Procedure* on page 115.
3. Replace the disk drive hardware, as described in the *Tekelec T1000* Application Server *Hardware Manual*.
4. Reboot the MPS, see *Rebooting the MPS* on page 134.
5. Configure the new disk.

PCI Card Replacement Procedure

warning:

PCI card replacement should be performed only by the *Customer Care Center* on page 3. If a PCI card needs to be replaced, contact the *Customer Care Center* on page 3.

When the *Customer Care Center* on page 3 replaces a PCI card, they perform the following functions:

1. Contact the *Customer Care Center* on page 3 to perform the remaining steps.
2. Shut down the MPS Server using *MPS Server Power Down Procedure* on page 115.
3. Replace the PCI card hardware as described in the *Tekelec 1000* Application Server *Hardware Manual*.
4. Reboot the MPS using *Rebooting the MPS* on page 134.

Tekelec T1000 AS Main Unit Replacement Procedure

Prior to replacing the main unit, the MPS Server must be shut down (see *MPS Server Power Down Procedure* on page 115).

For a detailed procedure for replacing the main unit, refer to the *Tekelec T1000* Application Server *Hardware Manual*. Contact the *Customer Care Center* on page 3) to perform the steps to configure the new disk.

Appendix

A

General Procedures

Topics:

This chapter includes general procedures for the T1000-based Multi-Purpose Server.

Introduction

This chapter contains miscellaneous general procedures that are referred to within this manual.

Accessing the EPAP GUI Interface

EPAP 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 will encounter the following message when logging into the EPAP GUI:

```
CAUTION: 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
```

Use the following procedure to access the main screen of the EPAP GUI interface.

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 EPAP application.

    The login screen shown in *Figure 63: EPAP User Interface Screen* on page 120 appears.

    Figure 63: EPAP User Interface Screen
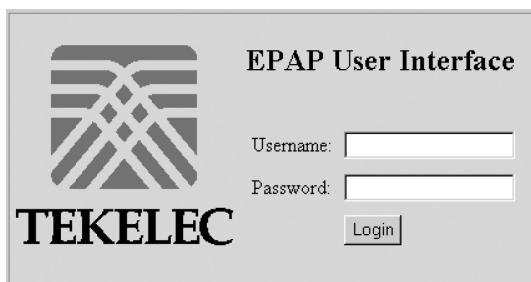
    If using Firefox, the following message will be displayed when logging into the EPAP GUI:

```
CAUTION: 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
```

    Note: *Figure 63: EPAP User Interface Screen* on page 120 does not show the release number that appears on the EPAP User Interface Login window because this manual covers multiple EPAP releases.

2. Enter the appropriate username and password.

    Specify a username that has permission to access the menu items indicated in the procedure to be performed. *Table 22: Usernames* on page 121 shows the default usernames. Additional usernames can be defined by selecting the User Administration menu item. For more information about assigning usernames, refer to the *EPAP Administration Manual*.

Table 22: Usernames

EPAP UI Login Name	Access Granted
epapmaint	Maintenance menu and all sub menus
epappdba	Database menu and all sub menus
epapdebug	Debug menu and all sub menus
epapplatform	Platform menu and all sub menus
uiadmin	User Administration menu
epapall	All of the menus in this Table

3. Continue with the procedure that invoked this procedure.
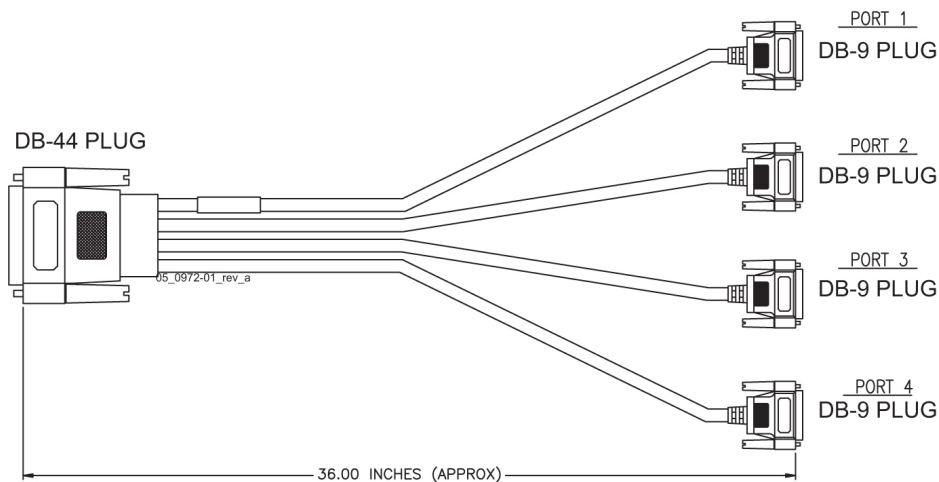
Connecting the Local Access Terminal

The Local Access Terminal can be used for the following purposes:

- Accessing the EPAP text interface
- Running `syscheck`

Use the following procedure to connect the Local Access Terminal.

1. Connect the workstation you will use as the Local Access Terminal to Port 3 of the DB44 to DB9 (X4) cable (P/N 830-0972-01), shown in *Figure 64: DB44 to DB9 (X4) Cable* on page 121.

Port 0 of this cable connects to PCI card 8. (For more information about the location of PCI card 8, refer to the *Tekelec 1000* Application Server *Hardware Manual*; for more information about this cable, refer to the *Signaling Products Integrated Applications Installation Manual*.

Figure 64: DB44 to DB9 (X4) Cable

PORT 1
DB-9 PLUG

DB-44 PLUG

PORT 2
DB-9 PLUG

05_0972-01_rev_a

PORT 3
DB-9 PLUG

PORT 4
DB-9 PLUG

36.00 INCHES (APPROX)

2. When the prompt appears on the Local Access Terminal, enter either of the following usernames and associated passwords:

   a) To access the EPAP text interface, enter the `epapconfig` username and the password provided by your system administrator.

      For more information about the EPAP text interface, see *Accessing the EPAP Text Interface* on page 122.

   b) To run the `syscheck` utility, enter `syscheck` as the username and `syscheck` as the password.

      For more information about running syscheck from this interface, see *Running syscheck Using the syscheck Login* on page 124.

Accessing the EPAP Text Interface

The EPAP text-based user interface is accessed through the Local Access Terminal. The text-based user interface is used for initial configuration of the EPAP application. Some errors described in this manual result from errors in the initial configuration, and recovery from them requires that you access the text interface.

For information about the initial configuration of the EPAP application, refer to the *EPAP Administration Manual*.

1. Connect the Local Access Terminal to the MPS server you need to access (see *Connecting the Local Access Terminal* on page 121).

2. Log in with username epapconfig and the password provided by your system administrator.

3. Continue with the procedure that invoked this procedure.

Running the System Health Check

The operator can run `syscheck` to obtain the operational status of the MPS platform with one of the following procedures:

- *Running syscheck Through the EPAP GUI* on page 123
- *Running syscheck Using the syscheck Login* on page 124

Running syscheck Through the EPAP GUI

Refer to the   EPAP *Administration Manual* for more details and information about logins and permissions.

1. Log in to the User Interface of the EPAPGUI (see *Accessing the EPAP GUI Interface* on page 120).
2. Check the banner information above the menu to verify that the EPAP about which system health information is sought is the one that is logged into.

   The example in *Figure 65: Login window* on page 123 shows a user is logged into EPAP A , while alarms are showing on EPAP B. To find out more information about conditions on the B server, run `syscheck` on that server.

   Figure 65: Login window
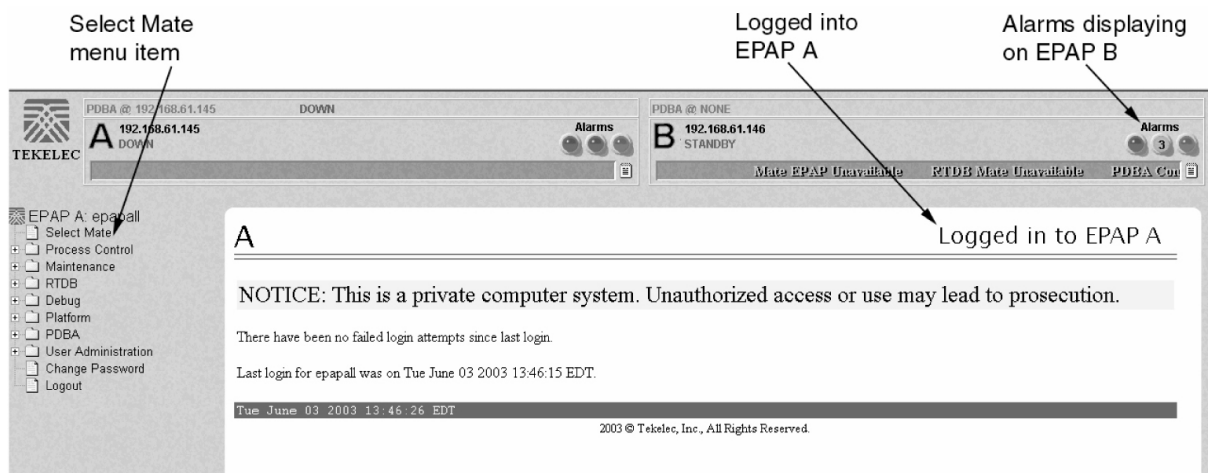
3. If it is necessary to switch to the other EPAP, click the **Select Mate** menu item.
4. When the GUI shows you are logged into the EPAP about which you want system health information, select **Platform>Run Health Check**. as shown in the following window.

   Figure 66: Run Health Check
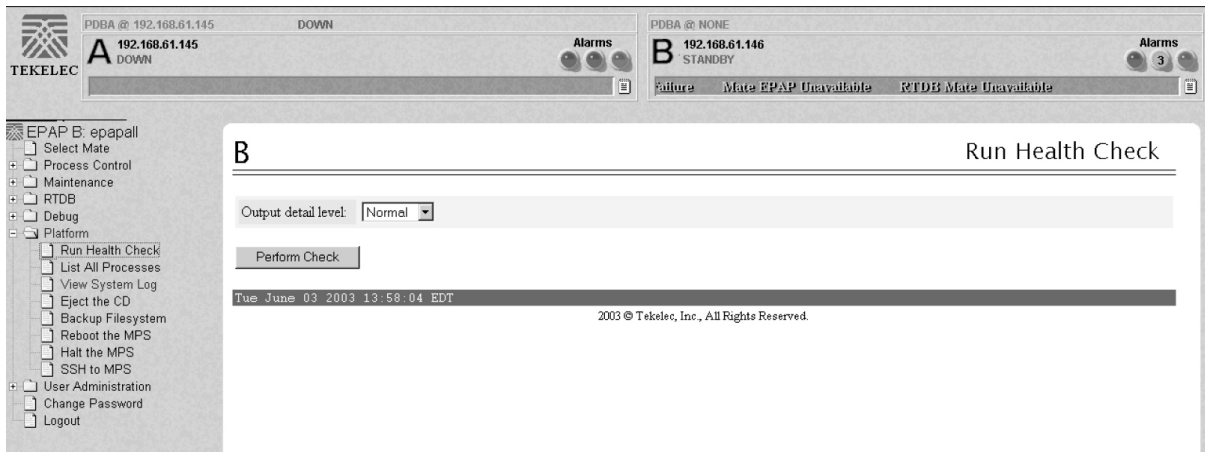
5. On the Run Health Checkwindow, use the pull-down menu to select Normal or Verbose for the **Output detail level** desired.

6. Click the **Perform Check** button to run the system health check on the selected MPS.

The system health check output data is displayed. The example shown in *Figure 67: Displaying System Health Check on EPAP GUI* on page 124 shows Normal output with errors.

Figure 67: Displaying System Health Check on EPAP GUI
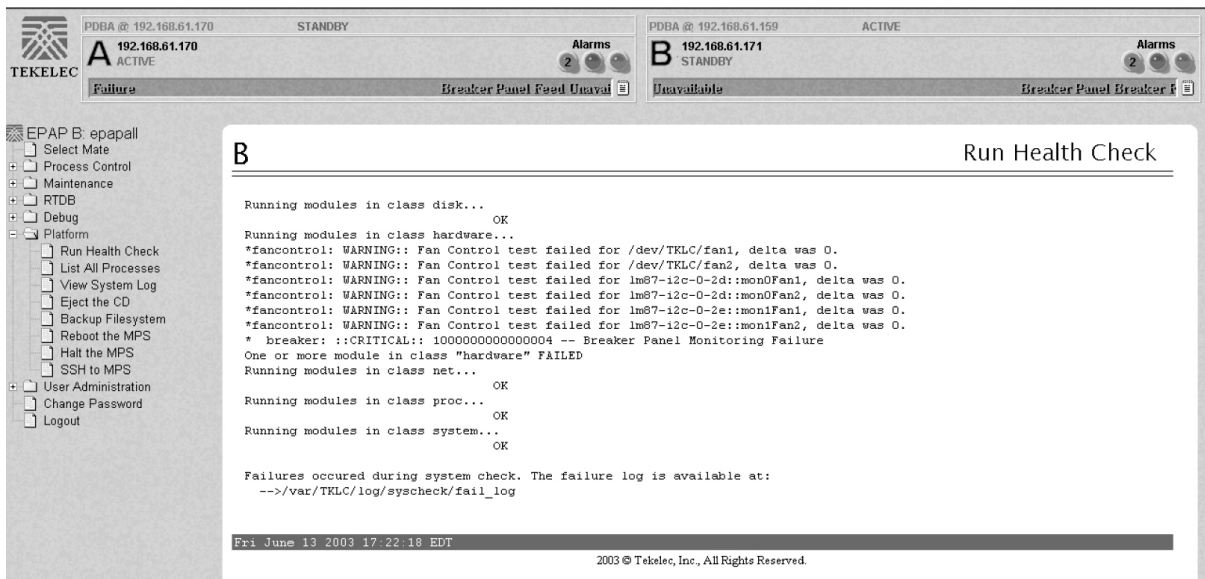
Running syscheck Using the syscheck Login

If the EPAP application has not been installed on the MPS or you are unable to log in to the EPAP user interface, you cannot run `syscheck` through the GUI. Instead, you can run `syscheck` from the `syscheck` login, and report the results to the *Customer Care Center* on page 3.

1. Connect the Local Access Terminal to the MPS server whose status you want to check (see *Connecting the Local Access Terminal* on page 121).

2. Log in as the `syscheck` user.

```
Login:  syscheck
Password:  syscheck
```

The `syscheck` utility runs and its output is displayed to the screen.

Saving Logs Using the EPAP GUI

During some corrective procedures, it may be necessary to provide Tekelec with information about the MPS for help in clearing an alarm. These log files are used to aid the *Customer Care Center* on page 3 when troubleshooting the MPS.

Use the following procedure to save logs using menu selections from the EPAP GUI.

1. Login to the User Interface screen of the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120).

2. Check the banner information above the menu to verify that you are logged into the problem EPAP indicated in the UAM.

   If it is necessary to switch to the problem EPAP, click the **Select Mate** menu item.

3. From the menu, select **Debug>Capture Log Files.**

4. Deselect (if necessary) the box labeled `Check if you want to capture core files with the Logs`, as shown in *Figure 68: Capture Logs File Screen* on page 125.

   Note: Contact the *Customer Care Center* on page 3 for assistance before capturing core files with the log files.
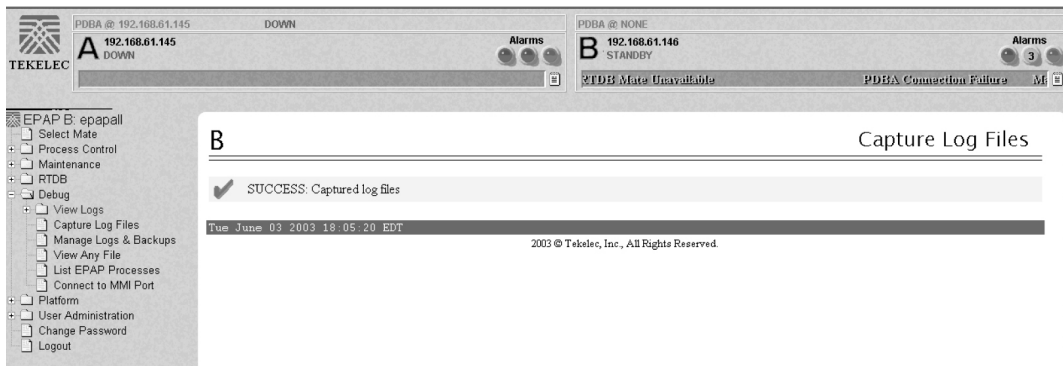
   Figure 68: Capture Logs File Screen
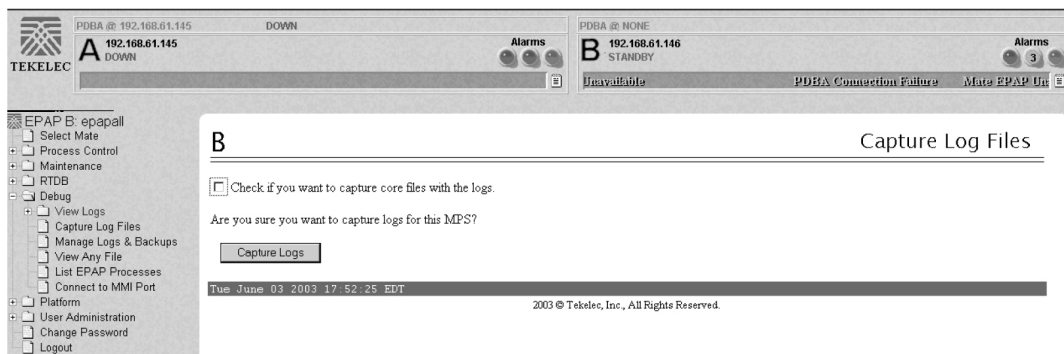
5. Click the **Capture Logs** button to capture the log files.

   After completion, verify the following response:

   Figure 69: Capture Logs Success

6. Contact the *Customer Care Center* on page 3 to analyze and check the log files.

7. When the *Customer Care Center* on page 3 has finished analyzing the logs files, delete them from the MPS by selecting **Debug>Manage Logs Files and Backups** to open the **Manage Logs and Backups** Screen.

8. Click the checkboxes for the files you want to delete and then click the **Delete Selected File(s)** button.
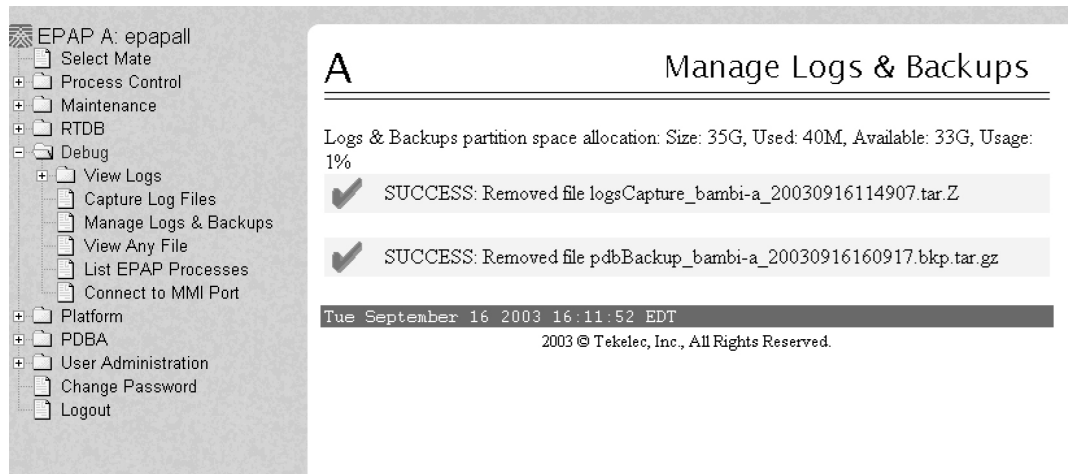
   An example is shown in *Figure 70: Deleting Captured Log Files* on page 126.

Figure 70: Deleting Captured Log Files

.
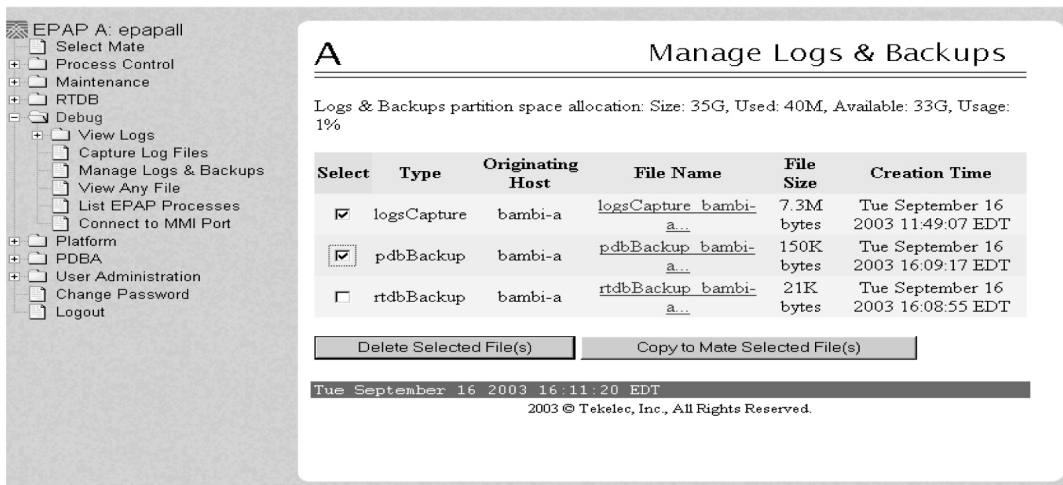
When the log files have been deleted, the GUI displays confirmation, as shown in *Figure 71: Delete Log Files Success* on page 126.

Figure 71: Delete Log Files Success

Restarting the EPAP and PDBA

This procedure is invoked by procedures in *MPS Platform and Application Alarms* on page 55.

CAUTION: Perform this procedure only when directed to by one of the procedures in *MPS Platform and Application Alarms* on page 55. This is not a standalone procedure.

CAUTION

1. Log in to the User Interface screen of the EPAP GUI (see *Accessing the EPAP GUI Interface* on page 120).

2. Check the banner information above the menu to verify that you are logged into the problem EPAP indicated in the UAM.

   If it is necessary to switch to the problem EPAP, select **Select Mate**.

3. From the **epapmaint** screen, select **Process Control>Stop Software**.

   The screen shown in *Figure 72: Stop Software Confirmation* on page 127 appears:

   Figure 72: Stop Software Confirmation

4. On the **Stop EPAP Software** screen, make sure the following checkboxes are all checked, so that the PDBA software is stopped along with the EPAP software and so that both the PDBA and EPAP software are automatically restarted on reboot (see *Figure 73: Stop Software* on page 128 for an example):

a) **Check to cause the software to automatically start on reboot**

This checkbox causes the EPAP software to automatically reboot.

b) **Check to stop the PDBA software along with the EPAP software**

c) **Check to cause the PDBA software to automatically start on reboot**
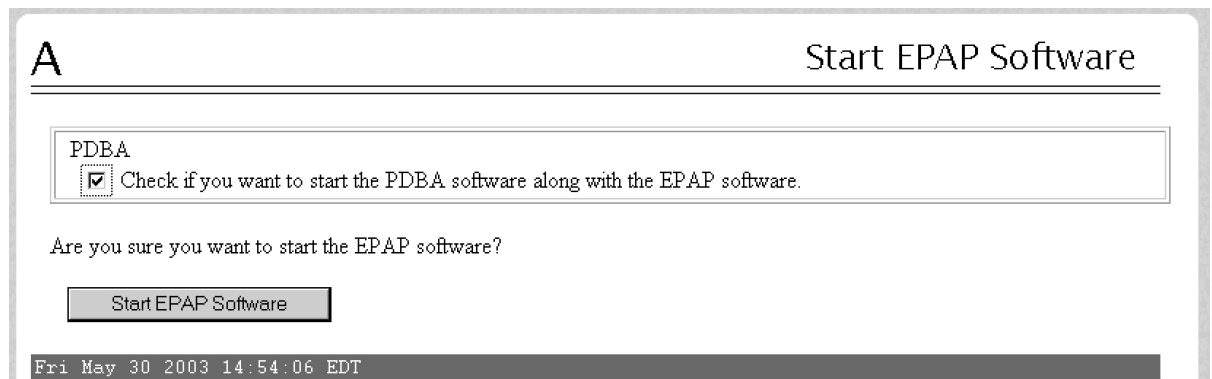
Figure 73: Stop Software

5. Click the **Stop EPAP Software** button to stop the software.

The screen shown in *Figure 74: Stop Software Completion Screen* on page 128 appears (the PDBA item appears only if performing this procedure on Side A).

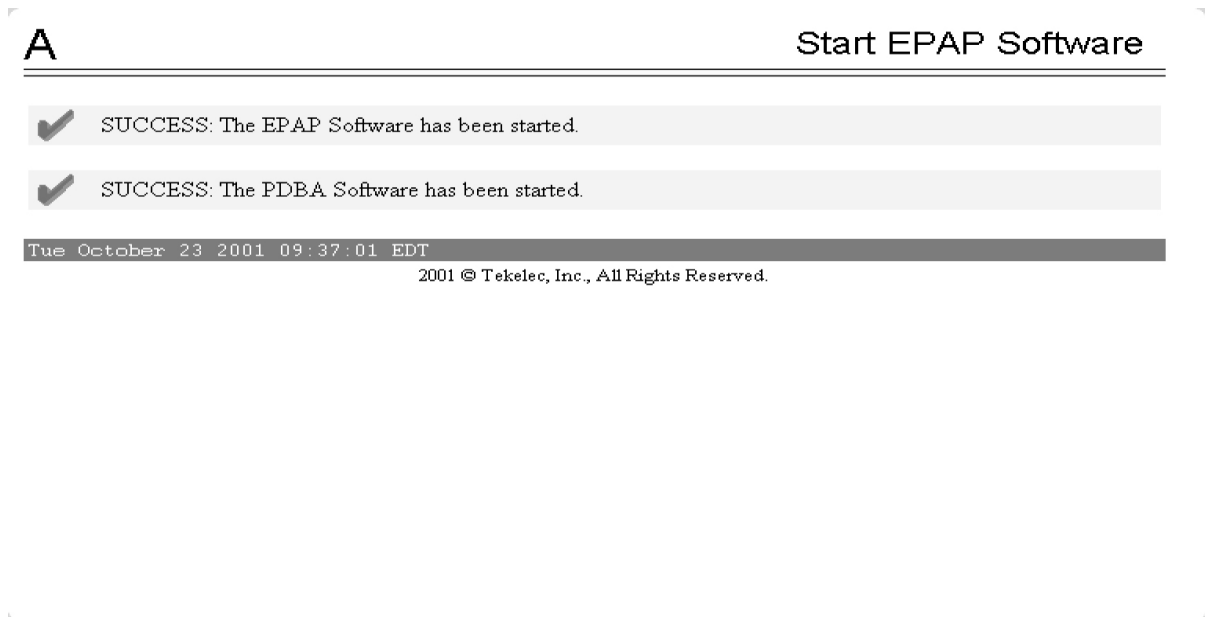**Figure 74: Stop Software Completion Screen**

6. Select **Process Control>Start Software**.

7. From the **Start EPAP Software** screen, make sure the checkboxes are checked as shown in *Figure 75: Start EPAP Software* on page 129 (this item applies only if performing this procedure on Side A):

Figure 75: Start EPAP Software

8. Click the **Start EPAP Software** button to start the software.
   The screen shown in *Figure 76: Start Software Completion Screen* on page 129 confirms that the software has started (the PDBA item appears only if performing this procedure on Side A):

Figure 76: Start Software Completion Screen

Restarting the EPAP Software

This procedure is used when referenced by one of the procedures in *MPS Platform and Application Alarms* on page 55.

CAUTION: Perform this procedure only when directed to by one of the procedures in *MPS Platform and Application Alarms* on page 55. This is not a standalone procedure.

CAUTION

1. Log in to the User Interface screen of the EPAPGUI (see *Accessing the EPAP GUI Interface* on page 120).

2. Check the banner information above the menu to verify that you are logged into the problem EPAP indicated in the UAM.

    If it is necessary to switch to the problem EPAP, select **Select Mate**.

3. From the **epapmaint** screen, select **Process Control>Stop Software**.

    The screen shown in *Figure 77: Stop Software Confirmation* on page 130 appears:

    Figure 77: Stop Software Confirmation
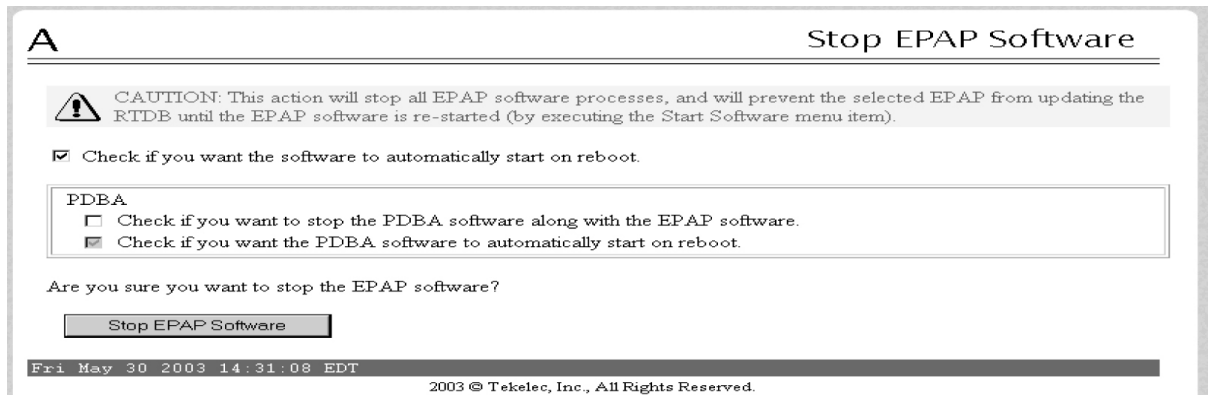
4. On the **Stop EPAP Software** screen, make sure the checkboxes are checked as shown in *Figure 77: Stop Software Confirmation* on page 130.

5. Click the **Stop EPAP Software** button to stop the software.

   The screen shown in *Figure 78: Stop Software Completion Screen* on page 131 appears.

   Figure 78: Stop Software Completion Screen
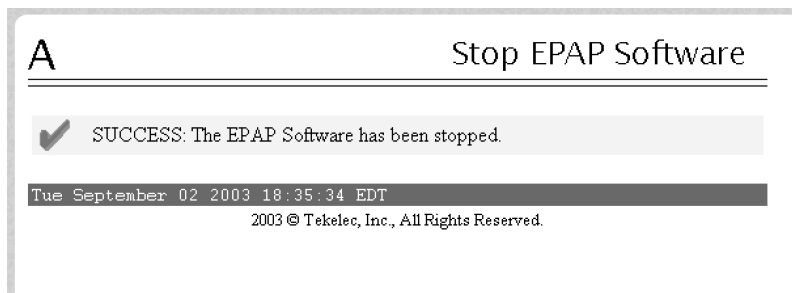
6. Select **Process Control>Start Software**.

7. From the **Start EPAP Software** screen, make sure the checkboxes are checked as shown in *Figure 79: Start EPAP Software* on page 131:

   Figure 79: Start EPAP Software
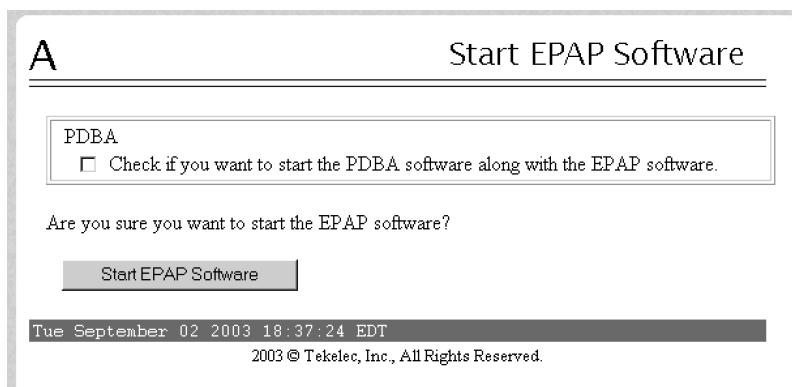
8. Click the **Start EPAP Software** button to start the software.

The screen shown in *Figure 80: Start Software Completion Screen* on page 132 confirms that the
software has started:

Figure 80: Start Software Completion Screen

Restarting the PDBA Software

This procedure is used when referenced by one of the procedures in *MPS Platform and Application
Alarms* on page 55.

CAUTION: Perform this procedure only when directed to by one of the procedures
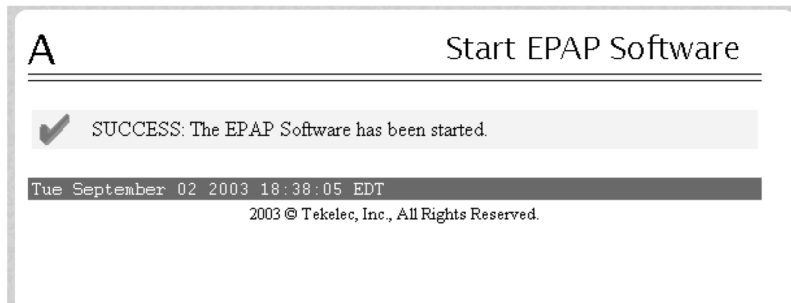in *MPS Platform and Application Alarms* on page 55. This is not a standalone procedure.

1. Log in to the User Interface screen of the EPAP GUI (see *Accessing the EPAP GUI Interface* on
   page 120).
2. Check the banner information above the menu to verify that you are logged into the MPS A
   at the site reporting the problem.

   If it is necessary to switch to the other side to be on MPS A, select **Select Mate**. Ensure that you
   are logged into MPS A at the site reporting the problem. If it is necessary to switch to the other
   site, select **PDBA>Select Other PDBA**.
3. Select **PDBA>Process Control>Stop Software** to stop the PDBA process.

   The window shown in *Figure 81: Stop PDBA* on page 132 is displayed.

Figure 81: Stop PDBA
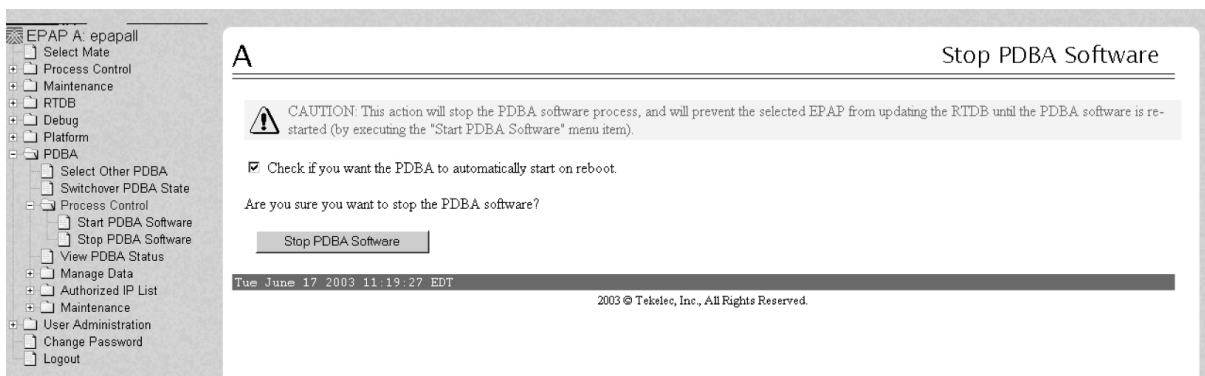
4. Ensure the checkbox is filled in as shown in *Figure 81: Stop PDBA* on page 132.

   Click the **Stop PDBA Software** button. When the software has stopped, a confirmation window is displayed, as shown in *Figure 82: PDBA Software Stopped* on page 133.

   Figure 82: PDBA Software Stopped
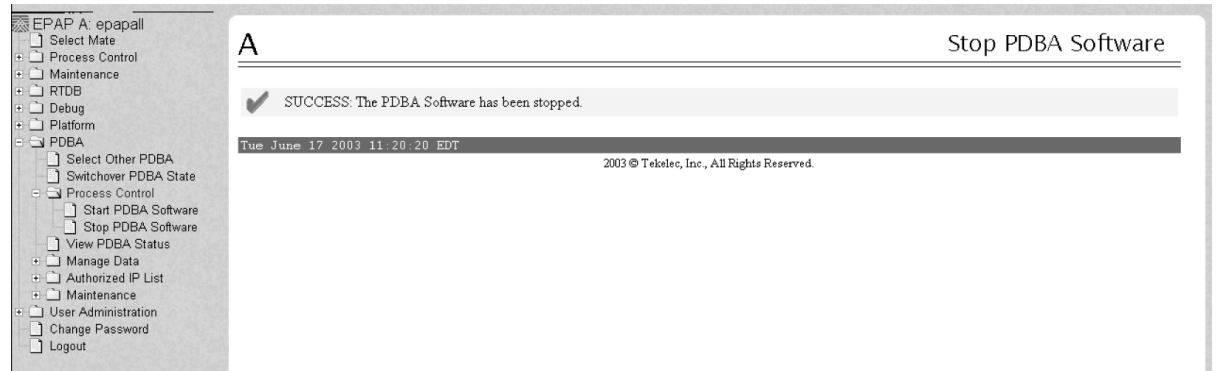
5. Restart the PDBA software by selecting **PDBA>Process Control>Start Software**.

   The window shown in *Figure 83: Start PDBA* on page 133 is displayed.

   Figure 83: Start PDBA

6. Click the **Start PDBA Software** button.

   When the PDBA software has started, the window shown in *Figure 84: PDBA Software Started* on page 133 is displayed.

   Figure 84: PDBA Software Started
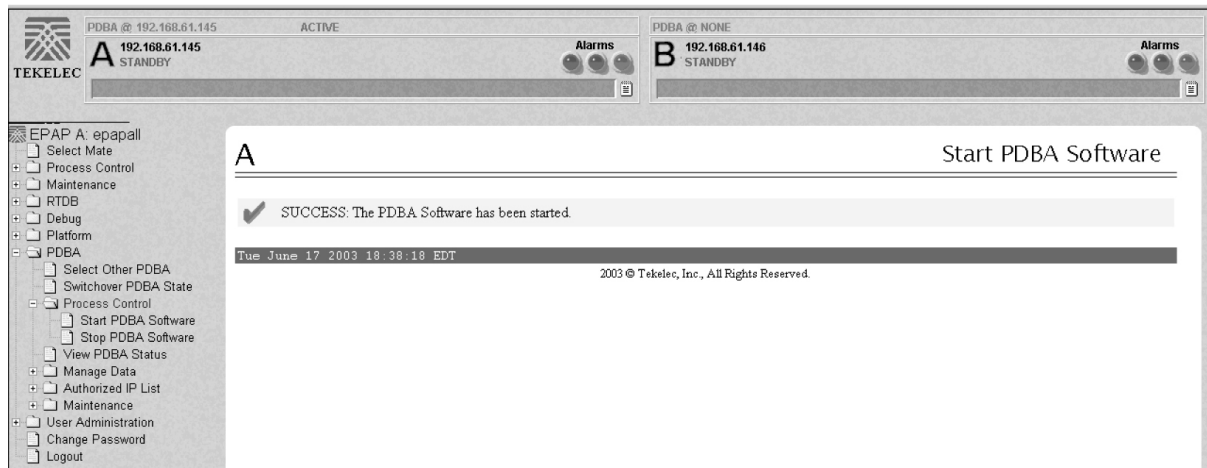
Rebooting the MPS

This procedure is used when referenced by one of the procedures in *MPS Platform and Application Alarms* on page 55.

 CAUTION: Perform this procedure only when directed to by one of the procedures in *MPS Platform and Application Alarms* on page 55. This is not a standalone procedure.
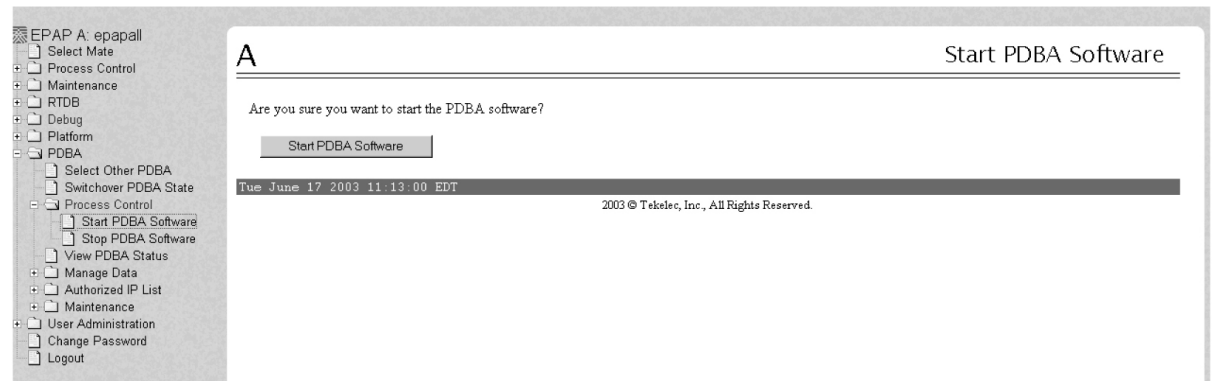
1. Login to the **User Interface** screen of the EPAPGUI (see *Accessing the EPAP GUI Interface* on page 120).
2. Check the banner information above the menu to verify that you are logged into the problem EPAP indicated in the UAM.

   Select **Select Mate** if necessary to switch to the problem EPAP.
3. Select **Platform>Reboot the MPS** .

   The screen shown in *Figure 85: Request Reboot of the MPS* on page 134 appears:

   Figure 85: Request Reboot of the MPS

4. Click the **Reboot the MPS** button to restart the MPS.

The screen shown in *Figure 86: Confirm Requested Reboot the MPS* on page 135 is displayed.

Figure 86: Confirm Requested Reboot the MPS
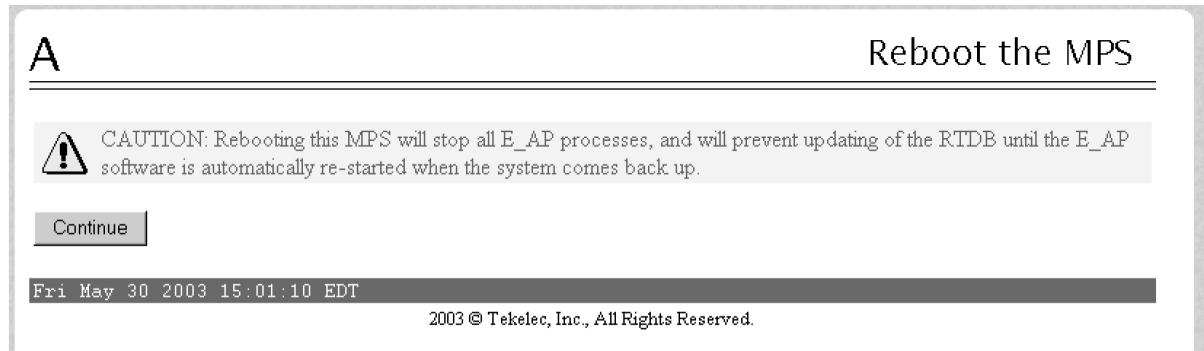
5. Click the **Continue** button.

The screen shown in *Figure 87: Reboot Information* on page 135 is displayed.

Figure 87: Reboot Information

This will reboot the EPAP and also start the EPAP software. The connection to the EPAP will be lost.

6. At the EAGLE 5 ISS input terminal, enter the `rept-stat-mps` command to verify the status of the EPAP.

Refer to the *Commands Manual* to interpret the output.

7. If the problem has not been resolved, contact the *Customer Care Center* on page 3 for assistance.

Have the system health check data available.

8. Return to the procedure that directed you to perform this procedure.

Glossary

A

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. The AS contains a set of one or more unique Application Server Processes, of which one or more normally is actively processing traffic.

B

BATT

Battery, including power supply cable.

BP

Board Prom

C

CD

Carrier Detect

Compact Disk

Channel

A single Time-Division-Multiplexed (TDM) timeslot within a channelized E1/T1 port. Generically, channels can be used for transporting signaling, digitized voice, or data information. Unused channels typically are filled with defined idle codes designed to maintain sufficient ones density to ensure frame-level synchronization.

C

CMOS	Complementary Metal Oxide Semiconductor
	CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor.

D

daemon	A process that runs in the background and performs a specified operation at predefined times or in response to certain events.
DO	Derived Object
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).
DVD	Digital Versatile Disk

E

EIR	Equipment Identity Register
	A network entity used in GSM networks, as defined in the 3GPP Specifications for mobile networks. The entity stores lists of International Mobile Equipment Identity (IMEI) numbers, which

E

correspond to physical handsets (not subscribers). Use of the EIR can prevent the use of stolen handsets because the network operator can enter the IMEI of these handsets into a 'blacklist' and prevent them from being registered on the network, thus making them useless.

EPAP   EAGLE Provisioning Application Processor

F

FRU   Field Replaceable Unit

G

GB   Gigabyte — 1,073,741,824 bytes

GMT   Greenwich Mean Time

G-Port   GSM Mobile Number Portability

A feature that provides mobile subscribers the ability to change the GSM subscription network within a portability cluster, while retaining their original MSISDN(s).

GSM   Global System for Mobile Communications

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.

I

I

INP	INAP-based Number Portability
	Tekelec's INP can be deployed as a stand-alone or an integrated signal transfer point/number portability solution. With Tekelec's stand-alone NP server, no network reconfiguration is required to implement number portability. The NP server delivers a much greater signaling capability than the conventional SCP-based approach.
	Intelligent Network (IN) Portability
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-41	Interim Standard 41, same as and interchangeable with ANSI-41. A standard for identifying and

I

authenticating users, and routing calls on mobile phone networks. The standard also defines how users are identified and calls are routed when roaming across different networks.

ISO   International Standards Organization

ISS   Integrated Signaling System

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.

M

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.

N

NTP   Network Time Protocol

P

P

PCI	Peripheral Component Interface
	Point Code International
	Protocol Control Information
	Peripheral Component Interconnect
PDB	Provisioning Database
PDBA	Provisioning Database Application
	There are two Provisioning Database Applications (PDBAs), one in EPAP A on each EAGLE 5 ISS. They follow an Active/Standby model. These processes are responsible for updating and maintaining the Provisioning Database (PDB).
PPP	Point-to-Point Protocol

R

RAM	Random Access Memory
	A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes.
RMTP	Reliable Multicast Transport Protocol
ROM	Read Only Memory
Route	A path to another signaling point.
RS	Requirement Specification

R

RTDB   Real Time Database

S

SCP   Service Control Point

T

TCP/IP   Transmission Control
                                      Protocol/Internet Protocol

TPD   Tekelec Platform Development

U

UAM   Unsolicited Alarm Message.

UI   User Interface

UIM   Unsolicited Information Message

W

WAN   Wide Area Network

Index

A

admonishments, documentation 3
alarm card, breaker panel
    FRU 108
    replacement procedure 109
alarm LED 37
alarm LEDs 38
application, detecting problems 38
Automatic PDB/RTDB Backup 30
availability, documentation 6

B

breaker panel
    alarm card FRU 108
    alarm card replacement procedure 109
    FRU 108
    replacement procedure 112

C

card 108, 109
    FRU, breaker panel alarm 108
CAUTION admonishment 3
Cooling Fans 43
corrected errors 41
Critical Platform Errors 56
CSR, See Customer Service Request (CSR)
Customer Care Center
    contact information 3
    emergency response 5
Customer Service Request (CSR) 3
Customer Support site
    how to access 7

D

DANGER admonishment 3
Disk Access 42
documentation 3, 6, 7
    availability, packaging, and updates 6
    Documentation Bulletins 7
    electronic files 6
    locate on Customer Support site 7
    printed 6
    Related Publications 6
    Release Notice 6

E

electronic files, documentation 6
emergency response, Customer Care Center 5
error conditions corrected 41

F

File System 42
Firefox 120

H

hub
    FRU 109
    replacement procedure 114

L

LED, alarm 37
locate documentation on Customer Support site 7

M

main power feeds, checking 43
Major Platform Errors 56
manual
    audience 2
    scope 2
Memory 42
Minor Application Errors 59
Minor Platform Errors 58
Mozilla Firefox 120
MPS Platform 43
MPS Server, power down procedure 115

N

network
    syscheck 42

P

packaging, documentation 6
Power Relay Unit 43
power, checking main feeds 43
printed documentation 6
procedure
    breaker panel alarm card replacement 109