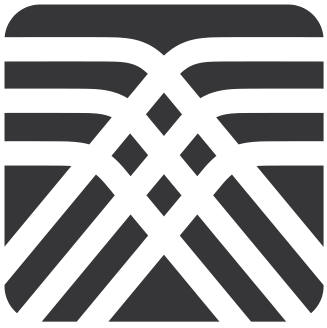
Tekelec Signaling Systems

Systems Overview

909-1021 Revision D
May 2005



TEKELEC

Notice
Information in this documentation is subject to change without notice. Unauthorized use or copying of this documentation can result in civil or criminal penalties.

No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of an authorized representative of Tekelec.

Other product names used herein are for identification purposes only, and may be trademarks of their respective companies.

Trademarks
The Tekelec logo, EAGLE, G-Flex, G-Port, IP^7, and IP^7 Secure Gateway are registered trademarks of Tekelec, Inc.

AS*i*, EAGLE 5, GenuOne, IP^7 Front End, SX*i*, TekServer, TekWare, and VX*i* are trademarks of Tekelec, Inc.

All other trademarks are the property of their respective owners.

Patents
This product is covered by one or more of the following U.S. and foreign patents:

U.S. Patent Numbers:
6,327,350 6,662,017 6,456,845 6,647,113 5,953,404 6,606379 6,167,129 6,324,183 6,639,981 5,008,929

Ordering Information
Additional copies of this document can be ordered from Tekelec Network Systems Division, 5200 Paramount Parkway, Morrisville, North Carolina, 27560.

Table of Contents

Chapter 1. Introduction

Purpose 1-1
Tekelec Signaling Systems 1-2
Conceptual Network Overview 1-2
Eagle 1-4
IP7 Secure Gateway 1-4
LNP 1-4
Sentinel 1-5
Supplemental Processing Systems 1-6

Chapter 2. SS7 Networks

Introduction 2-1
Common Channel Signaling Networks 2-1
SS7 Link and Message Types 2-2
Role of SSPs, STPs and SCPs in SS7 Networks 2-3
Service Switching Points (SSPs) 2-3
Signaling Transfer Points (STPS) 2-3
Service Control Points (SCPs) 2-6
STP System Link Administration 2-6

Chapter 3. EAGLE 5 SAS/IP7 Secure Gateway System Architecture

Introduction 3-1
Eagle and IP7 Secure Gateway Systems 3-2
Administration Subsystem 3-4
Communication Subsystem 3-5
Application Subsystem 3-7
Timing Systems Eagle/IP7 SG 3-12
Basic EAGLE 5 SAS Theory of Operation 3-14
SEAS Subsystem (Optional) 3-15
Embedded Operations Applications Processor (EOAP) 3-18
IP7 Secure Gateway 3-19

Chapter 4. LNP

Introduction to LNP 4-1
Query Methods for Wireless and Wireline Networks 4-2

Local Service Management System (LSMS) 4-4
EAGLE LNP Functional Capabilities 4-4
LNP Query Service (LNPQS) 4-4
Automatic Call Gapping (ACG) 4-5
LNP Message Relay (LNPMR) Function 4-5
EAGLE LNP Database 4-6
SCCP Subsystem Management 4-6
Messages for Local EAGLE LNP Subsystems 4-6
Database Audit 4-7
LNP Maintenance 4-7
Reporting Functions 4-7
Measurement and Billing Functions 4-8
LNP Hardware 4-9
LSMS 4-9
LSMS Hardware Configuration 4-10

Chapter 5. Sentinel

Sentinel 5-1
Sentinel Frames Overview 5-4
Site Collector Frames 5-4
Flight Recorders 5-4
Extended Services Platform (ESP) 5-5
Sentinel Server Frames 5-5
Integrated Sentinel 5-6
Probed Sentinel 5-9

Chapter 6. MPS

Introduction 6-1
MPS System Hardware 6-2
MPS on Tekelec 1000 6-2
Layered Design 6-3
MPS Platform Software Configuration 6-5
Serial Communication 6-6
Remote Access 6-6
Diagnostics, Monitoring, and Alarming 6-7
MPS System Network Configuration 6-7
MPS on Netra Platform 6-9
MPS on Netra System Features 6-10

Chapter 7. Tekelec 1000 Applications Server (APS)

Introduction 7-1
Tekelec 1000 Hardware Features 7-1
Hardware Components 7-2
Interfaces 7-3
Electrical Features 7-3
Mechanical Design 7-3
Alarm and Status Indicators 7-6
Installation and Replacement 7-6
Diagnostics 7-7
Reliability, Interoperability, and Scalability 7-7
Reliability 7-7
Interoperability 7-7
Scalability 7-8

Chapter 8. EOAP

Overview 8-2
Hardware 8-4
Shelf 8-4
Components 8-5
Asynchronous Maintenance Modem (Optional) 8-6
Terminal 8-7
Interfaces 8-7
EOAP-to-Eagle STP 8-8
EOAP-to-SEAS 8-10
Administration 8-12
IP7 Secure Gateway Provisioning 8-12
EOAP Retransmission Delay 8-13
Maintenance 8-13
Hardware 8-13
Software 8-14
Upgrade Considerations 8-14

List of Figures

Figure 1-1. Network Functions of Tekelec Signaling Systems 1-3
Figure 2-2. SS7 Common Channel Signaling Networks 2-2
Figure 3-1. EAGLE 5 SAS System Functional Diagram 3-2
Figure 3-2. Eagle/IP7 SG Subsystems 3-3
Figure 3-3. Maintenance and Administration Subsystem 3-5
Figure 3-4. Example EAGLE 5 SAS message flow 3-15
Figure 3-5. SEAS Subsystem 3-17
Figure 3-6. GR-376 EOAP in an Eagle System 3-19
Figure 3-7. IP7 Secure Gateway Network (STP Connectivity via MTP-over-IP) 3-21
Figure 3-8. IP7 Secure Gateway Network (SCP Connectivity via TCAP-over-IP) 3-22
Figure 3-9. IP7 Secure Gateway Network (SEP connectivity via ISUP, Q.BICC, and TUP-over-IP) 3-23
Figure 4-1. LNP Hardware Overview 4-9
Figure 4-2. Overview of LSMS Hardware Components 4-11
Figure 5-1. NOC in a Combined Probe-based and probe-less Configuration 5-2
Figure 5-2. Sentinel Components 5-3
Figure 5-3. Integrated Sentinel Block Diagram 5-7
Figure 5-4. probed Sentinel 5-10
Figure 6-1. MPS on Tekelec 1000/EAGLE Overview 6-3
Figure 6-1. Layered Design for MPS and Applications 6-4
Figure 6-2. MPS Hardware Configuration in Frame 6-5
Figure 6-2. Rear View of Tekelec 1000 6-5
Figure 6-3. MPS Serial Port Connections 6-6
Figure 6-4. MPS on Tekelec 1000 Network Connections 6-8
Figure 6-5. MPS NTP Configuration 6-9
Figure 6-3. MPS on Netra Hardware Overview 6-10
Figure 7-1. Tekelec 1000 in Tekelec Heavy-Duty Frame 7-2
Figure 7-2. Rear I/O Panel 7-5
Figure 7-3. Tekelec 1000 Status Indicators 7-6

Figure 8-1. EOAP Communication 8-3
Figure 8-2. EOAP Shelf 8-4
Figure 8-3. Operating Context of EOAP 8-8
Figure 8-4. EOAP-to-IP7 Secure Gateway Interface 8-9
Figure 8-5. EAGLE-to-SEAS Interface 8-11

List of Tables

Table 3-1. Example SS7 Routing Key Table 3-34
Table 4-2. Enterprise 450 Server Features 4-22
Table 5-3. ESP Frame Components Releases 8.0 and 8.1 5-17
Table 5-4. ESP Frame Components Release 9.0 5-18
Table 5-5. ESP Server 1A Release 9.0 5-19
Table 5-6. ESP Servers 1B through 1Q Release 9.0 5-19
Table 5-7. ESP Frame Components Release 10.0 5-20
Table 5-8. Site Collector Frame Components 5-34
Table 5-9. Sentinel Site Collector Server A 5-35
Table 5-10. Sentinel Site Collector Servers B and C 5-35
Table 5-11. EMS Frame Components 5-38
Table 5-12. MPS Server Specifications 6-8
Table 7-1. Basic Interfaces 7-4
Table 7-2. Optional Interfaces 7-5
Table 7-3. TekServer Chassis Dimensions 7-13
Table 8-13. Status LEDs of the EOAP System 8-5
Table 8-14. EOAP Port Labels and Functions 8-7
Table 8-15. SCSI Addresses 8-10
Table 8-16. EOAP Applications 8-11
Table 8-17. RFC1006 TCP Protocol Stack 8-20
Table 8-18. Performance Impacts of New EOAP Hardware 8-22

1

Introduction

Purpose 1–1
Tekelec Signaling Systems 1–2
Eagle 1–4
IP7 Secure Gateway 1–4
LNP 1–4
Sentinel 1–5
Supplemental Processing Systems 1–6
Manual Organization and Conventions 1–7
Acronyms 1–8

Purpose

The purpose of this *Systems Overview Manual* is to provide customers and system planners with a basic understanding of Tekelec Signaling systems and how those systems work together in a network. This manual also provides a high-level overview of each system and its subsystems. This manual does not describe how to install or replace hardware.

For installation information, refer to the *Installation Manual* included in your current documentation suite. For replacement procedures of existing hardware components, refer to the *Maintenance Manual* included in your current documentation suite.

Tekelec Signaling Systems

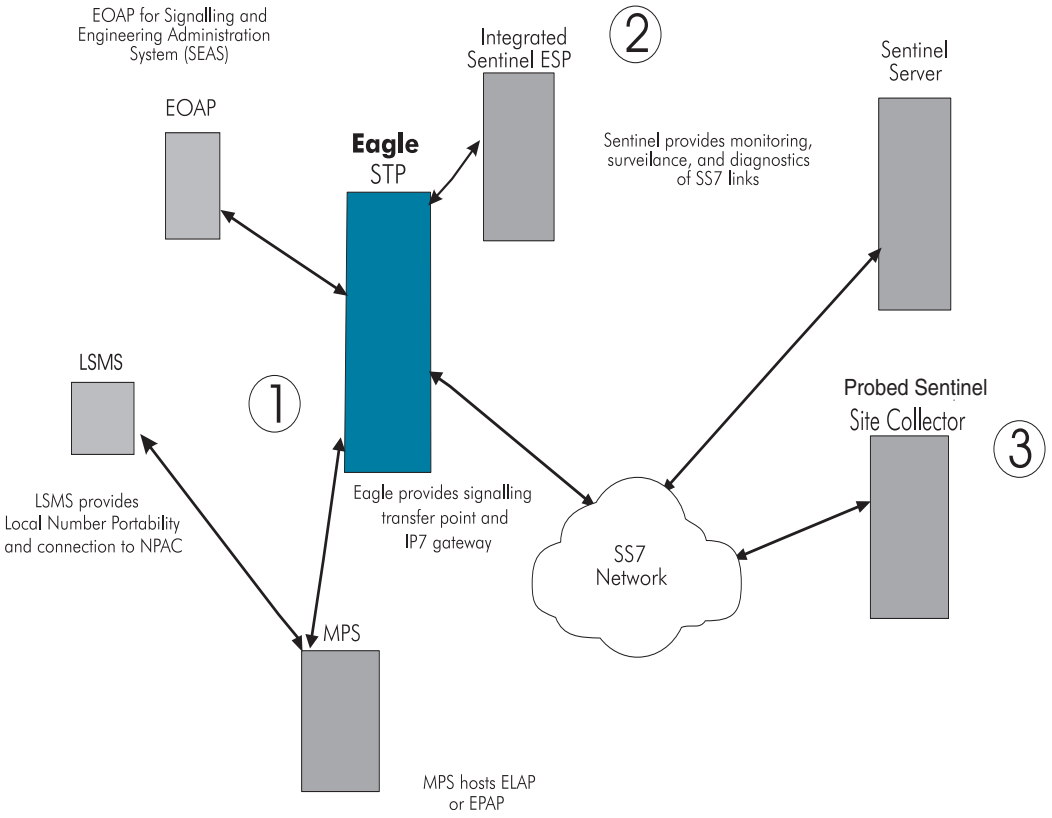
Tekelec uses different systems to support its processor and feature applications. This manual describes the following Tekelec systems:

- EAGLE 5 Signaling Application System (SAS) Signal Transfer Point (STP) and IP7 Secure Gateway (SG)
- Local Number Portability and LSMS
- Sentinel
- Supplemental Processing Systems
  - Multi-purpose Server (MPS)
  - Tekelec 1000 Applications Server (APS)
  - Embedded Operations Support System Applications Processor (EOAP)

Conceptual Network Overview

Figure 1-1 on page 1-3 outlines three scenarios that show how Tekelec Signaling products might work in a network.

Figure 1-1. Network Functions of Tekelec Signaling Systems



Some of the ways the EAGLE 5 SAS interacts with other Tekelec systems is illustrated in the following scenario descriptions:

1. A call is placed by a customer in North America who has just changed phone companies, but has retained the same phone number. SS7 data associated with the customer contained in the call is received by the EAGLE 5 SAS. The EAGLE 5 SAS needs Number Portability Administration Center (NPAC) data associated with the customer to transmit the call data properly. NPAC data gets to the EAGLE 5 SAS from Tekelec's Local Service Management System (LSMS) that has stored the NPAC data on a local database. The LSMS uses the Tekelec 1000-based MPS hosting ELAP software to pass the data to the EAGLE 5 SAS. This data transfer enables the customer to be associated with a specific phone number even though the customer has changed providers.

2. The EAGLE 5 SAS receives SS7 information in a phone call. Integrated Sentinel ESP servers monitor the SS7 links in the EAGLE 5 SAS directly (without the use of probes). Sentinel Transport Cards (STCs) in the EAGLE 5 SAS pass SS7 messaging data to the ESP. This data is processed by the ESP and sent to the Sentinel Server. The Sentinel Server further

processes the information and can then provide a wide array of data including billing infomation and fraud detection.

3. A non-EAGLE 5 SAS STP receives SS7 information in a phone call. Sentinel Site Collectors use external probes to connect to and monitor the SS7 links in the STP. This information including the call data record is passed to the base Sentinel Server for processing and reporting.

The following sections provide brief descriptions of the Tekelec Signaling systems used in these scenarios.

Eagle

Eagle is a large-capacity, multi-functional, fully scalable Signaling Transfer Point (STP). High capacity and scalability allow the Eagle to grow from a single-shelf, 80-link STP to a multi-frame, 1500-link STP.

EAGLE 5 SAS-based Products are NEBS-compliant (GR-63-CORE, Network Equipment-Building Systems). EAGLE 5 SAS -based products are configured in standard equipment frames to provide services to SS7 telephony networks.

Because of the distributed processor design, Eagle does not have a separate central processing unit to bottleneck traffic throughput. Application and interface cards are designed to provide plug and play type functionality that facilitates future growth. Eagle application and interface cards generally do not have specific shelf or frame limitations, allowing you to fully customize and define how your STP is configured. Eagle also supports a variety of interface cards to support connectivity to a wide range of network elements. Eagle provides connectivity interfaces for IP, ATM, DS0A, V.35, OCU, T1, and E1 protocols.

IP7 Secure Gateway

The IP7 Secure Gateway product is a subsystem of the EAGLE 5 SAS and provides connectivity between SS7 and IP networks, enabling messages to pass between the SS7 network domain and the IP network domain. It receives and sends switched circuit network (SCN) native signaling at the edge of the IP network. The signaling gateway function may relay, translate, or terminate SS7 signaling in an SS7-Internet gateway. The signaling gateway function may also be co-resident with the media gateway function to process SCN signaling associated with line or trunk terminations controlled by the media gateway.

LNP

Local Number Portability (LNP) allows a subscriber to change location, service provider, or service while keeping the same directory number. LNP ensures that subscribers receive the same freedom of choice for local service as

they do with long-distance service providers. The EAGLE 5 SAS with Local Number Portability (LNP) solution provides fully scalable transaction rates from 1,700 to 40,000 TPS.

Tekelec simplifies number portability by integrating advanced database management and signaling functions directly into its EAGLE 5 SAS platform. Using a memory-based approach, LNP functions are combined with EAGLE 5 SAS capabilities in a single network node.

Tekelec's LNP solution includes the Local Service Management System (LSMS). LSMS provides the interface between the number portability administration center (NPAC) service management system and the EAGLE 5 SAS's element management system (EMS). It maintains and distributes LNP data to the service provider's LNP databases. The LSMS is equipped with a graphical user interface to administer subscription, service provider, and network data.

Sentinel

The Sentinel product line provides the capability to monitor SS7 links. Sentinel is a network monitoring and diagnostic system that gives service providers visibility of and access to their SS7 networks. Sentinel includes the following components:

- Fault-management:
  - Problem re-creation
  - Problem analysis
  - Proactive surveillance
  - Problem resolution
- Business applications:
  - Loop detection
  - Mass call detection
  - Fraud detection
  - Billing verification

Supplemental Processing Systems

Multi-Purpose Server

The Multi-Purpose Server (MPS) hosts the EAGLE 5 SAS LNP Application Processor (ELAP) or EAGLE 5 SAS STP Provisioning Application Processor (EPAP) applications such as G-Flex and G-Port. When used to host ELAP or EPAP applications, the MPS provides an interface between the customer provisioning network and the Eagle DSM cards. As the customer's data is updated, the MPS stores the data and updates the DSM cards. An MPS is usually co-located with an Eagle, but can be installed remotely.

Beginning in release 30.1, MPS systems running EPAP 4.0 are hosted on the Tekelec 1000 Services Platform. Existing MPS systems running on SUN servers will continue to be supported. Customers wanting to upgrade to the functionality of MPS/EPAP 4.0 are required to install the Tekelec 1000 hardware.

Tekelec 1000 Applications Server (APS)

Tekelec 1000 provides a fully integrated application-hosting environment directly on top of the EAGLE 5 SAS platform. The Tekelec 1000 is a general-purpose application engine (AE) that offers high transaction rates with low latency. It supports a variety of application solutions for the wireless and wireline telecommunications infrastructure to provide the building blocks for next-generation signaling systems. The Tekelec 1000 supports a full suite of applications known as TekWare. The Tekelec 1000 is scalable and packaged in a compact-size, stand-alone enclosure.

EOAP

The Embedded Operations Support System Application Processor (EOAP) provides the Eagle STP system with a generic platform to develop and run OAP software for feature-specific interfaces to the Eagle STP. These interfaces, for example, include the optional Signaling and Engineering Administration System (SEAS) and the optional Local Service Management System (LSMS).

EOAP applications reside on redundant hardware processor modules in a chassis mounted in a Tekelec Operations Application Frame (OAF). Other applications such as the GR-376 can also be configured on an EOAP chassis. The OAP application residing on the EOAP replaces the older OAP.

Manual Organization and Conventions

This *Systems Overview Manual* is organized into the following chapters:

- *Chapter 1, "Introduction"*—contains general information about manual organization, the scope of this manual, its targeted audience, brief explanations of the various systems, typical content of a Documentation Suite delivered with each system, how to handle hardware repairs and returns, and how to get technical assistance.
- *Chapter 2, "SS7 Networks"*—provides an overview of common channel signaling networks, the role of STPs in those networks, the connectivity of STPs with other network elements, and the administration of STPs within a signaling network.
- *Chapter 3, "EAGLE 5 SAS/IP7 Secure Gateway System Architecture"* —describes the components of the EAGLE 5 SAS/IP^7 Secure Gateway system, and provides a high-level theory of its operation.
- *Chapter 4, "LNP"* —describes the EAGLE Local Number Portability (LNP) system, including the Local Service Management System (LSMS). It also provides a high-level theory of operation designed to assist maintenance personnel in troubleshooting the EAGLE 5 SAS LNP system.
- *Chapter 5, "Sentinel"* —describes both the integrated and probed Sentinel network monitoring and diagnostic systems.
- *Chapter 6, "MPS"* — describes the MPS hardware platform, MPS hardware components, and MPS disks and file systems.
- *Chapter 7, "Tekelec 1000 Applications Server (APS)"* — describes the Tekelec 1000 hardware platform.
- *Chapter 8, "EOAP"* — describes the Embedded Operations Support System Application Processor (EOAP) and the software for feature-specific interfaces to the Eagle STP.

The *Systems Overview Manual* uses the following conventions:

- Components used only in a specific system are clearly labeled, for example, (EAGLE 5 SAS only) or (IP7 SG only).
- Components that are specific to a release are labeled with the system and release number; for example, (IP7 SG 4.0 or later) or (EAGLE 27.2 or earlier).

Acronyms

A	Ampere
ACL	Application processor Code Loader
ACM	Applications Communications Module
AIN	Advanced Intelligent Networks. Set of standards for advanced intelligent services
AINF	Application Interface Applique
ANSI	American National Standards Institute.
AP	Application Processor
APD	Application Processor DCM bootstrap code
API	Application Interface
AS	Application server
ASM	Application Services Module
ATM	Asynchronous Transfer Mode
BHCA	Busy Hour Call Attempts
BITS	Building Integrated Timing System
BM	Buss Master (Cognitronics)
BOM	Bill Of Materials
BP	Boot Prom
BPDCM	Boot Prom DCM
Bps	Bit per second
CAP	Communication & Application Processor
CAR	Corrective Action Report
CCS7	Common Channel Signaling System #7
CE CISPR A	Compliance European, Comite Internationale Special des Perturbations Radioelectrique (European Compliance, International Special Committee on Radio Interference, Class A)
CDR	Call Detail Record
CDU	CAP Downloadable Utility
CLEI	Common Language Equipment Identifier
CF	Control Frame
CLLI	Common Language Location Identifier
CNAM	Calling Name Delivery Service

COTS ..... Commercial Off-the-Shelf

CP ..... Communications Processor

CSR ..... Customer Service Request

D1G ..... Database Communication 1 Gigabyte Expansion Memory Module

DCM ..... Database Communications Module

DMS ..... Disk Management Service

DRAM ..... Dynamic Random Access Memory

DS0 ..... Digital Signal Level-0 (64 Kbits/sec)

DS1 ..... Digital Signal Level-1 (1.544Mbits/sec)

DSM ..... Database Services Module

E1 ..... European Digital Signal Level-1 (2.048 Mbits/sec).

EBI ..... Extended Bus Interface

EDCM ..... Enhanced Database Communications Module

EF ..... Extension Frame

EILA ..... Enhanced Integrated LIM Applique

EMM ..... Extended Memory Management

EMP ..... EAGLE Monitor Protocol

EOAM ..... Enhanced OAM GPL

EOAP ..... Embedded Operation Support System Applications Processor

ESD ..... Electro-Static Discharge

ESP ..... Extended Services Platform

FAP ..... Fuse and Alarm Panel

FR ..... Flight Recorder

FTP ..... File Transfer Protocol

FTRA ..... FTP-based Table Retrieve Application

GB ..... GigaByte

GLS ..... Generic Loader Services

GPL ..... Generic Program Load

GPLM ..... GPL Management

GPSM-II ..... General Purpose Service Module

GTT ..... Global Title Translation

GWS ..... GTT Gateway Screening

HCAP ..... High-Speed Communications & Applications Processor

HCAP-T ..... Improved HCAP card

HDLC ..... High-Level Data Link Control

HIPR ..... High-speed IMT Router

HMUX ..... High-speed Multiplexer

IAD ..... Integrated Access Device

ICM ..... IMT configuration manager task

ILA ..... Integrated LIM-AINF module

ILDR ..... IMT loader task

IMT ..... Inter-processor Message Transport

IMTC ..... IMT Control task

IP ..... Internet Protocol

IP^7 ..... Tekelec's Internet Protocol to SS7 Interface

IPD ..... IMT Processor DCM operational code

IPMX ..... IMT Power and Multiplexer card

ISDN ..... Integrated Services Digital Network.

IS-NR ..... In Service – Normal

ISR ..... Interrupt Service Routine

ITU ..... International Telecommunications Union

IWF ..... Inter-Working Function

KHz ..... Kilohertz (1000 Hertz)

LAN ..... Local Area Network.

LFS ..... Link Fault Sectionalization

LIM ..... Link Interface Module

LNP ..... Local Number Portability

LIM-AINF ..... A LIM with a software-selectable interface

LOM ..... Lights out Management

LSMS ..... Local Service Management System

M256 ..... 256 Megabyte Memory Expansion Card

MAS ..... Maintenance and Administration Subsystem

MASP ..... Maintenance and Administration Subsystem Processor

MBUS ..... Maintenance Bus

MCAP ..... Maintenance Communications & Applications Processor

MDAL ..... Maintenance, Disk, and Alarm card

MG ..... Media Gateway

MGB ..... Master Ground Bar

MGC ..... Media Gateway Controller

MGCP ..... Media Gateway Controller Protocol

MIB ..... Maintenance Information Base utility

MIM ..... Multi-Channel Interface Module

MPL ..... Multi-Port LIM

MPS ..... Multi-Purpose Server

MSU ..... (SS7) Message signaling Unit

MS ..... Media Server

MTOS ..... Multi-Tasking Operating System, Industrial Programming Inc.

NEBS ..... Network Equipment Building System

NOC ..... Network Operations Center

NS ..... Network Server

NSD ..... Tekelec's Network Systems Division

OAM ..... Operations, Administration, & Maintenance

OA&M ..... Operations, Administration, & Maintenance

OAP ..... Operations System Support/Applications Processor

OAPF ..... Operations System Support/Applications Processor Frame

OCU ..... Office Channel Unit

OEM ..... Original Equipment Manufacturer

OOS-MT-DSBLD ..... Out of Service –Maintenance Disabled

PMTC ..... Peripheral Maintenance task

PSTN ..... Public Switched Telephone Network

RAID ..... Redundant Array of Inexpensive Disks

RAM ..... Random Access Memory

RMA ..... Return Material Authorization

SAI/P ..... Serial Asynchronous Interface PCI Adapter

SCP ..... Service Control Point (SS7 Network)

SCCP	Signal Connection Control Part
SCM	System Configuration Manager
SCN	Switched Circuit Network
SCSI	Small Computer Systems Interface
SEAC	Signaling Engineering and Administration Center
SEAS	Signaling Engineering and Administration System
SG	Secure Gateway
SIP	Session Initiation Protocol
SS7	Signaling System Seven
SSP	Service Switching Point (SS7 Network)
STC	Sentinel Transport Card
STP	Signal Transfer Point (SS7 Network)
STPLAN	Signaling Transfer Point Local Area Network
T1	The North American telecommunications standard defining a circuit that multiplexes and switches 24 channels and operates at speeds of 1.544 Mbps
TCU	Table Creation Utility
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Terminal Disk Module
TEKCC	Tekelec Composite Clock
TEKOS	Tekelec Operating System
TMOAP	Texas Micro processor chassis hosting the OAP application
TOS486	Tekos Operating System for the 486
TOS4M	Tekos Operating System for the 486 implemented via MTOS
TSC	Time Slot Counter
TSM	Translation Services Module
UAM	Unsolicited Alarm Output
UD1G	Updated Database Communication 1 Gigabyte Expansion Memory Module
UIM	Unsolicited Information Messages
V.35	ITU Interface Recommendation, V.35
VPN	Virtual Private Network

WAN ..... Wide Area Network

2

SS7 Networks

Contents ..... Page

Introduction 2-1

Common Channel Signaling Networks 2-1

SS7 Link and Message Types 2-2

Role of SSPs, STPs and SCPs in SS7 Networks 2-3

STP System Link Administration 2-6

Introduction

This chapter provides an overview of common channel signaling networks, the role of STPs in those networks, the connectivity of STPs with other network elements, and the administration of STPs within a signaling network.

Common Channel Signaling Networks

Signaling System No. 7 (SS7) is a signaling protocol that has become a worldwide standard for modern telecommunications networks. The U.S. implementation is based on the International Telecommunications Union-Telecommunications Section (ITU-TS) and TIX I Committee of the Exchange Carriers Standards Association (ECSA). SS7 is a layered protocol following the OSI reference model. It offers all of the same call setup advantages as CCS6, but also enables network elements to share more than just basic call-control information through the many services provided by the SS7's Integrated Services Digital Network-User Part (ISUP), and the Transaction Capabilities Application Part (TCAP).

The functions of the TCAP and ISUP layers correspond to the Application Layer of the OSI reference model, and allow for new services such as User-to-User signaling, Closed-User Group, Calling Line Identification, various options on Call Forwarding and the rendering of services based on a centralized database (e.g., 800 and 900 service). All of these services may be offered between any two network subscribers, not just to subscribers served by the same telephone switch.

SS7 Link and Message Types

An *SS7* Network consists of a flat non-hierarchical configuration enabling peer-to-peer communication. Figure 2-2 depicts the makeup and connectivity of *SS7* common channel signaling networks currently installed and in use.

Figure 2-2. *SS7* Common Channel Signaling Networks

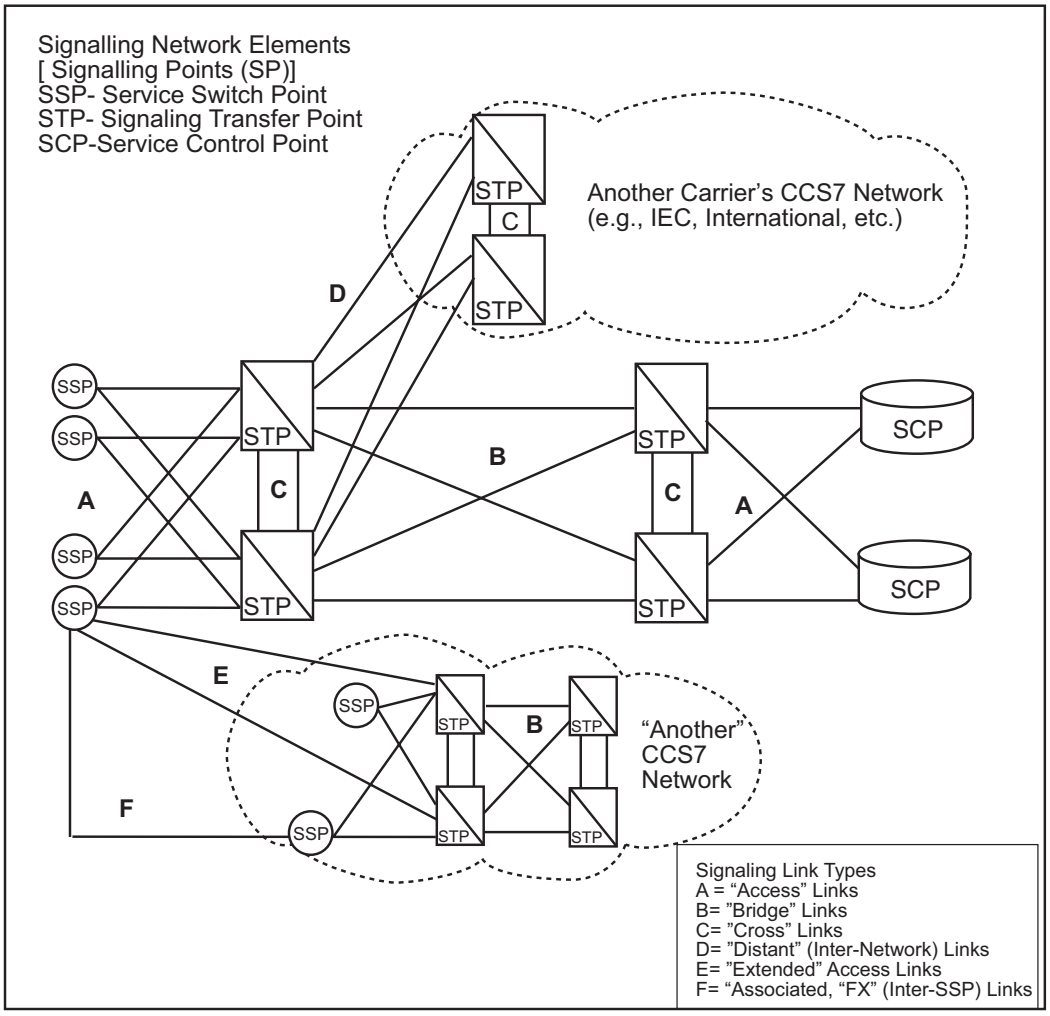


Figure 2-2 shows the three principal network elements of SS7 common channel signaling networks, interconnected by the six standard types of signaling links currently in use. Signaling links are data transmission links that ordinarily operate on digital carrier facilities at 56,000 bits per second in North America, and at 64,000 bits per second in most other regions of the world. High Speed Links (HSLs) at 1.54 M bps are beginning to be used in North America.

Signaling links between any two signaling network elements are deployed in groups called “link sets,” dimensioned to carry the estimated signaling traffic between two STPs. Because STPs like the EAGLE 5 SAS are deployed in pairs, as shown in Figure 2-2, an alternate route always exists between any two STPs.

One combination of the link sets interconnecting an SSP or SCP with both members of the STP pair is called a “Combined link set.” 'The traffic carried between any two signaling network elements is load-shared across links in a link set, rotating through all links available according to the rules of the SS7 protocol.

Traffic destined for any network element via the STP pair is further load-shared over the combined link set, unless restricted by network management rules also established by the SS7 protocol.

Role of SSPs, STPs and SCPs in SS7 Networks

Service Switching Points (SSPs)

In conventional telephone networks, Service Switching Points (SSPs) are usually telephone central offices, also known as “End-Offices,” or “Access Tandems.” In the cellular mobile or “wireless” communications environment, an SSP is frequently located at the Mobile Switching Center (MSC). In either case, the SSPs perform circuit switching functions, and are capable of using the SS7 protocol to signal other SSPs for call setup, or to query the centralized databases that are stored in Service Control Points (SCPs).

Signaling Transfer Points (STPS)

STPs like the EAGLE 5 SAS are ultra-reliable, high speed packet switches at the heart of SS7 networks, which terminate all link types except “F” links. For reliability reasons, they are nearly always deployed in mated pairs.

The primary functions of STPs are to provide access to SS7 networks and routing of signaling messages. The SS7 protocol itself defines destination routing for both circuit related signaling (inter-SSP) and non-circuit related data base inquiries (to SCPS). Many STPs contain additional routing information concerning the exact location of specific databases stored at different Service Control Points (SCP), so that a SSP can request information without knowing in which specific SCP it is stored.

STPs operate using the message transfer and signaling connection control parts (MTP and SCCP) of the SS7 protocol. The MTP provides basic message handling and network management procedures, and the SCCP adds the capability to transmit database queries and other non-circuit related signaling messages across the network. SCCP also provides a non-SS7 specific addressing interface (Global Title), as explained below.

In SS7 networks, STPs perform the following three basic functions:

- **Message routing** - by using the originating and destination point codes (OPC & DPC) contained in the MTP's "routing label," in a "datagram" environment (i.e. where a separate route may be chosen for each message packet). Routing tables, which are structured to allow message transport between any given pair of SSPs over different routes, are stored and maintained within STPS. The STP's signaling Network Management functions control message routing during periods of link congestion or failure.
- **Specialized routing (Global Title Translation)** - by using the SCCP to translate addresses (Global Titles) from signaling messages that *do not contain* explicit information allowing the MTP to route the message. For example, an STP translates a dialed "1+800" number to an SCP's DPC for MTP routing, and gives a subsystem number (SSN) for delivery to the "800" database application at the SCP. In case of congestion or failures, the STP's SCCP management takes responsibility for rerouting signaling traffic, based on information received via the MTP concerning the point code's routing status, and SSNs allowed or prohibited.
- **Carrier signaling access (Gateway Screening)** - by using the MTP and SCCP to allow or deny access to the "Home" SS7 network for transport of signaling messages from another network.

To establish and maintain trunk connections between two SSPs, and to notify both when the connection is to be released, a pre-defined sequence of SS7 messages is exchanged between the two SSPs. Except where "F-links" have been installed between the concerned SSPs, these messages are routed to one of a pair of STPs in the local ("Home") SS7 network over an "A- link," or to one of a pair of STPs in another SS7 network over an "E-fink." The STP function is illustrated by the following two cases:

- For an ordinary customer-dialed call to a 7- or 10-digit domestic station address (I±NPA+NXX+XXXX), the STP, after consulting its routing tables, will route its received SS7 messages towards the designated SSP over the

appropriate A, B or D-link. (Note: A message will be rerouted via a C-link only in cases of where use of the other B or D link sets are restricted or unavailable.)

- For calls to be given special billing or routing treatment, as indicated by other dialled prefix digits (e.g., I+NOO+..., IOXX +..., 0+..., etc.), an intermediate step requires the STP to retrieve routing information from a non-resident routing table or database. This retrieval process ordinarily involves translation of the signaling address and a completely separate message transaction with a SCP.

As shown in Figure 2-2, STPs are the hub of the signaling network infrastructure. A less efficient, and more expensive, signaling network might have each SSP connected to every other SSP via a ("F"-type) signaling link. This approach would be much more costly than the hubbed network shown in Figure 2-2, due to the total number of links that would be required. For example, a fully-connected, ten node network would require 45 "F-links," or 90 "F-links" if each link was redundant. The alternative hubbed network approach for ten SSPs utilizing STPs (deployed in pairs for increased availability) requires only 20 links, one link to each member of the STP pair.

One conspicuous drawback to the totally centralized signaling network as currently implemented is that it decreases the availability of the network. In the past, instances of this shortcoming have caused some carriers to lose whole networks. The optimal network implementation is somewhere between the fully connected and totally hubbed implementations. In an environment of relatively inexpensive high capacity, fiber-optic transmission systems, a fully connected network of smaller, more cost effective STPs can provide desired network diversity and diffusion.

Diversity is increasing the sectionalization of the network with the implementation of STPs in "communities of interest" or areas smaller than currently provisioned (i.e., large urban LATAs, statewide or multi-state regions). The savings from deploying this approach are two-fold: increased network availability (guaranteeing uninterrupted revenue streams), and reduction in the number of back-hauled "Inter-LATA," or inter-regional links to the larger, centralized STP. Increasing diversity positions multiple STPs within a network, as designated by the first three digits of the Point Code, and thus reduces the number of subscribers affected by a possible STP outage.

"Diffusion" increases the connectivity of the SSPs via E-links to STPs in adjacent networks. Diffusion may also increase the number of D-links between different STPs which were not previously connected due to a hierarchical network implementation. Perfusion of signaling connectivity in this manner decentralizes the role of signaling in network implementations, and decreases its impact on network availability.

Service Control Points (SCPs)

Service Control Points (SCPs) are network intelligence centers where databases of call processing information is stored. The primary function of SCPs is to respond to queries from other SCPs, by retrieving the requested information from the appropriate database within the SCP node, and sending it back to the originator of the request.

SCPs currently serve as centralized databases to translate logical numbers (e.g., 1+N00 numbers) into network physical addresses, or to verify credit card data and status. Future plans call for expanding the SCPs' centralized resource responsibilities to include greater interaction in call processing. This expansion of responsibilities will be attained through newly defined “call models” implemented in SSPs that may invoke assistance from SCPs more than once for the same call.

The information managed by an SCP can be modified or updated without affecting any other node in the SS7 network. This ease of data administration is a major appeal of SS7 implementation. The first applications of SCPS for 1+800 calls and Credit Card verifications could also have been implemented by storing the respective databases at each network switching node. This approach was rejected, however, due to the unmanageable task of administering multiple decentralized databases.

To appreciate the expediency and economy of centralized databases, consider adding a new service to a 100 node network by updating 100 databases. The ease of administration and greater control of new service offerings are obvious when one compares the two alternatives.

STP System Link Administration

After a STP is installed, system administration consists primarily of the following:

- Addition of signaling link hardware and software
- Creation and maintenance of data tables for links, link sets, and Routes
- Addition of hardware and software required for Global Title Translation
- Creation and maintenance of Global Title Translation tables
- Addition of hardware and software for Gateway Screening
- Creation and maintenance of Gateway Screening tables
- Updating software

When required, hardware must always be installed at the affected STP site. However, there are three methods that can be employed to load software and administer data tables:

1. Local administration via user interface(s) and portable storage media (disks/tapes)

2. Remote administration via modem using vendor-proprietary methods and commands to load and update data

3. Centralized, remote administration via modem or dedicated digital data link, using industry or network operator's standard operations support system (e.g., SCCS, SEAS, etc.).

3

EAGLE 5 SAS/IP^7 Secure Gateway System Architecture

Contents....Page

Introduction 3-1

Eagle and IP7 Secure Gateway Systems 3-2

- Administration Subsystem.... 3-4
- Communication Subsystem 3-5
- Application Subsystem 3-7
- Timing Systems Eagle/IP7 SG.... 3-12
- EAGLE Basic EAGLE 5 SAS Theory of Operation 3-14
- SEAS Subsystem (Optional).... 3-15
- Embedded Operations Applications Processor (EOAP) .. 3-18
- IP7 Secure Gateway.... 3-19

Introduction

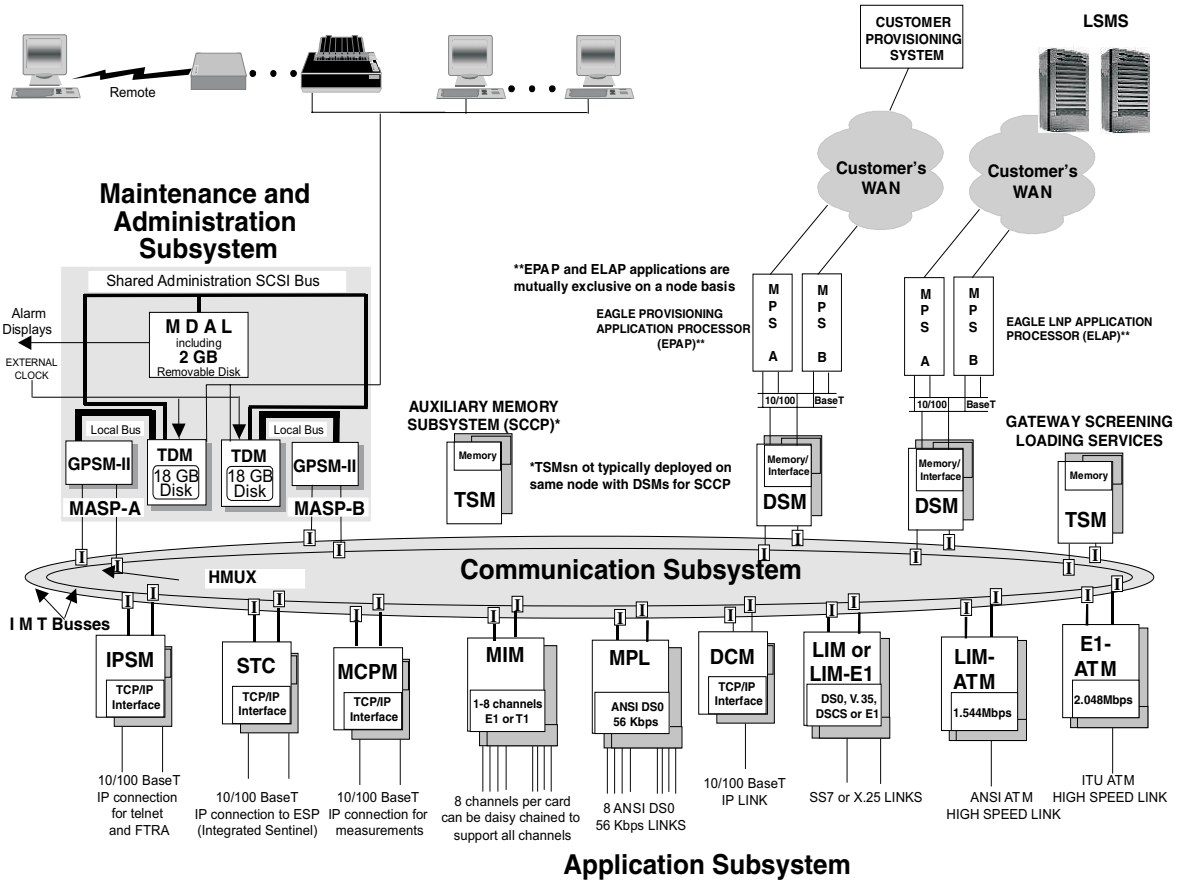
This chapter introduces the components of the EAGLE 5 SAS/IP^7 Secure Gateway system, and provides a high-level theory of its operation. For detailed descriptions of the EAGLE 5 SAS hardware, refer to the *Installation Manual*.

Eagle and IP7 Secure Gateway Systems

Eagle and IP7 SG systems are mounted in the same types of frames and are configured similarly. In the *Hardware Manual* specific component requirements or configurations for each system are explained in detail. Figure 3-1, on page 3-2 provides a high-level overview of the EAGLE 5 SAS subsystems and functions. These functions are described in the following sections of this chapter.

NOTE: In some cases in this manual EAGLE 5 SAS hardware card names are based upon the name of the software that is loaded on the card rather than the card type printed on the card label. Before servicing or configuring any EAGLE 5 SAS cards, be sure to physically inspect the card and read the card label to determine the card type.

Figure 3-1. EAGLE 5 SAS System Functional Diagram

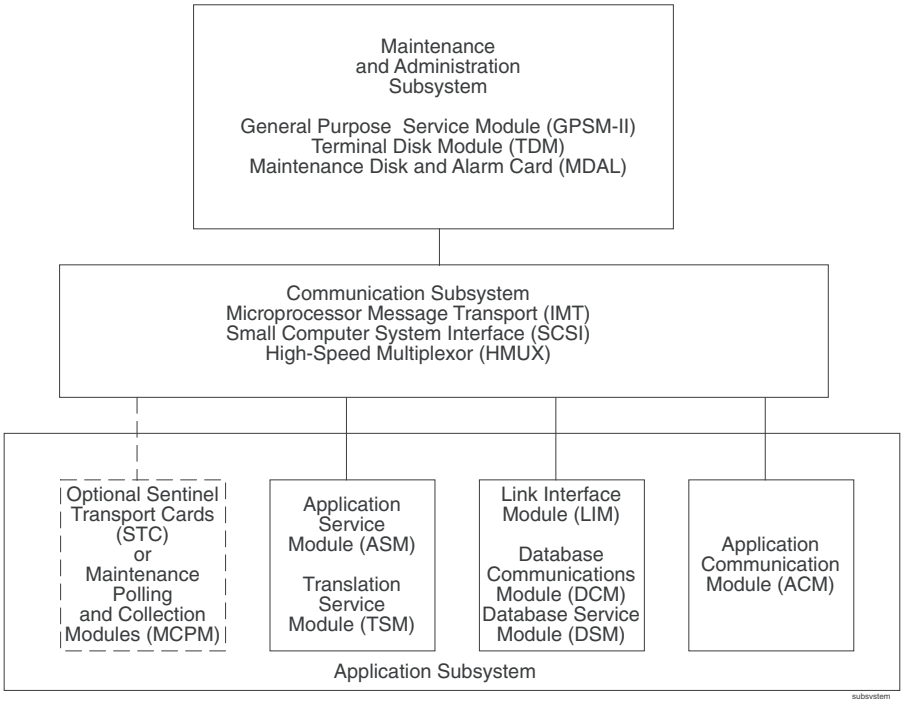


The EAGLE 5 SAS consists of the following subsystems:

- Maintenance and Administration Subsystem (MAS)
- Communication Subsystem
- Application Subsystem

In addition, Eagle and IP7 SG systems have a clock derived from the Building Integrated Timing System (BITS). This connects to the 64KHz composite BITS signal and distributes clock signals to the rest of the cards in the systems. See "Timing Systems Eagle/IP7 SG" on page 3-12 for information about High-Speed Master Timing and Time Slot Counter (TSC) Synchronization features.

Figure 3-2. Eagle/IP7 SG Subsystems



Administration Subsystem

The Maintenance and Administration Subsystem (MAS) provides services to other subsystems, and consists of the following:

- The General Purpose Service Module (GPSM-II)
- Terminal Disk Module (TDM)
- Maintenance Disk and Alarm (MDAL)

MASP

The Maintenance and Administration Subsystem Processor (MASP) function is a logical pairing of the GPSM-II card and the TDM card. The GPSM-II card is connected to the TDM card by means of an Extended Bus Interface (EBI) local bus.

The MDAL card contains the removable cartridge drive and alarm logic. There is only one MDAL card in the Maintenance and Administration Subsystem (MAS) and it is shared between the two MASPs.

The GPSM-II and TDM card combination performs the following functions:

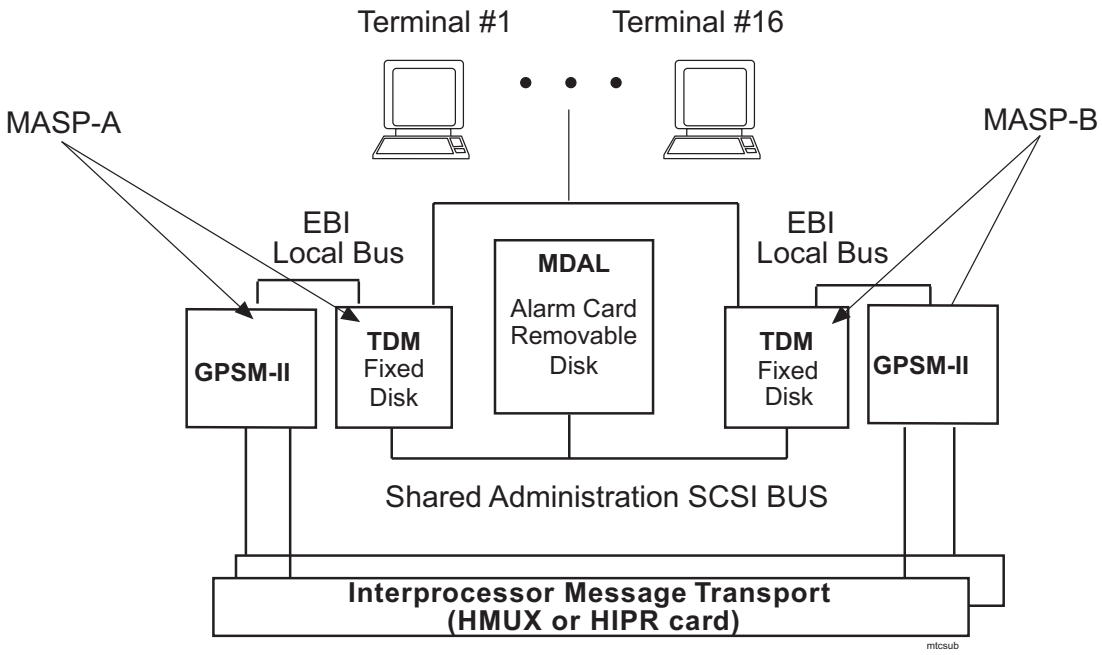
- Maintenance communication—Maintenance functions poll each application card and receives trouble reports. These are reported to the alarm function in the MASP to generate alarms, or to the event messaging function for output to the printer.
- Measurements—Collection and reporting of system performance data.
- Peripheral services—Provides access to all peripherals attached to the system, terminals, disks, alarms, clocks, and others.
- Alarm processing—Provides audible and visual alarms.
- System disks—Provides for storage of application or system software.

Software is downloaded to application cards from the MASP. The software provides the interface function depending on application requirements. The type of software the application processor receives depends on the function of the application board which is determined by provisioning the board.

Eagle System architecture provides Inter-processor Message Transport (IMT) connectivity directly to the maintenance and administration subsystem through the GPSM-II card. This allows the MASP to provide maintenance and administrative communication services to application cards.

Figure 3-3, “Maintenance and Administration Subsystem,” on page 3-5 shows relationships between different components of the maintenance and administration subsystem.

Figure 3-3. Maintenance and Administration Subsystem



Communication Subsystem

The communication subsystem consists of two separate sets of buses:

- Small Computer System Interface (SCSI) buses
- Inter-processor Message Transport (IMT) buses

Small Computer System Interface Buses

There are two independent Small Computer System Interface (SCSI) buses, one to the fixed disks on TDM cards and the other to the shared administration SCSI bus that runs on the backplane between TDMs and the MDAL card. Each SCSI bus has a block of memory that allows transfers from memory to occur without delaying the application processor.

Inter-processor Message Transport

The Inter-processor Message Transport (IMT) bus is the main communications artery for all subsystems in the system. This high-speed communications system is composed of two counter-rotating serial buses. The IMT bus uses load sharing, so messages from the various subsystems are divided evenly across both buses. If one bus should fail, the other immediately assumes control of all messages.

With EAGLE release 28.0 and later and Integrated Sentinel release 8.0 and later the IMT buses can function as an private LAN assigning internal IP address to LIM cards. By addressing cards on an internal LAN the EAGLE/Sentinel Integration feature allows monitoring of SS7 links without external connections. SS7 link information from the EagleLIM cards is collected by Sentinel Transport Cards (STC) and transferred to Expanded Service Platform (ESP) subassemblies. After processing in the ESP, the link information is forwarded to a Sentinel server.

The High-Speed IMT Packet Router

Beginning with EAGLE release 33.0, the High-Speed IMT Packet Router (HIPR) Module (P/N 870-2574-01) provides increased IMT bus bandwidth and individual high-speed card/server links. The HIPR enhances the IMT bus by introducing switched 125 Mbps interfaces to each slot within a shelf. HIPR acts as a gateway between the intra-shelf IMT BUS, running at 125 Mbps, and the inter-shelf ring operating at 1.0625 Gbps.

Traffic between cards on the same shelf will be switched directly to the destination slot and is not transmitted to any other cards in the shelf. Traffic between shelves is not required to pass onto an intra-shelf IMT channel.

Two HIPR modules are required in shelves equipped with high-performance LIMs, such as the High-Capacity MIM, and for interfacing to Tekelec 1000 Application Server through IMT Bridge and IMT PCI modules. HIPR requires all other shelves be equipped with either all HMUX cards or all HIPR cards (shelves cannot contain a mix of HMUX and HIPR).

The HIPR programmable logic is upgradeable and reprogrammable via the IMT inter-shelf interface. Updated images can be downloaded from the OAM to the HIPR and stored in FLASH memory on the HIPR.

With the improved bandwidth from the switched architecture, the HIPR card enables customers to use other higher performance cards from Tekelec such as the High Capacity MIM.

Beginning with EAGLE STP Software Release 30.0 all IPMX cards must be replaced by either High-Speed Multiplexer (HMUX) cards (P/N 870-1965-01) or High Speed IMT Router (HIPR) cards (P/N 870-2574-0). Beginning with EAGLE STP software release 33.0, IPMX cards must be replaced by either HMUX cards or High-Speed IMT Router Cards (P/N 870-2574-01). A mixture of HMUX and HIPR cards within one IMT ring is possible, provided HIPR is installed on both IMT A and IMT B on a given shelf. HMUX and HIPR

cards are installed at the factory or by Tekelec Technical Support and are not installed by customers.

High-Speed Multiplexer

High-Speed Multiplexer (HMUX) cards support requirements for up to 1500 links, allowing communication on IMT buses between cards, shelves and frames. HMUX cards interface to 16 serial links, creating a ring from a series of point to point links. Each HMUX card provides a bypass multiplexer to maintain the ring's integrity as cards are removed and inserted into an operational shelf. HMUX cards are installed at the factory or by Tekelec Technical Support and are not installed by customers.

Application Subsystem

The application subsystem consists of application cards. Application cards are capable of communicating with other cards through the redundant IMT buses. A Communications Processor (CP) on each application board provides control of communications from the cards to the IMT buses.

Software is downloaded to application cards on initial power-up from the Maintenance and Administration Subsystem Processors (MASP). Once Eagle and IP7 SG systems are loaded, software is downloaded to cards by the Generic Loader Services (GLS) and Operation Administration and Maintenance (OAM).

EAGLE 5 SAS Application Subsystem Modules

An Application Processor (AP) receives the software load on the application card. The type of software the AP receives depends on the function of the application board which is determined by the provisioning of the board. This combination of software and hardware card is known as a "module". The following are the application modules in the EAGLE 5 SAS:

- Link Interface Module (LIM)
- ACM - Application Communication Module
- TDM - Terminal Disk Module
- IPSM - IP Services Module
- DCM - Database Communication Module
- STC - Sentinel Transport Card
- DSM - Database Services Module
- GPSM-II - General Purpose Service Module
- MCPM - Measurements Collection and Polling Module
- ASM - Application Service Module
- TSM - Translation Service Module
- HCMIM - High-capacity MIM

Link Interface Module

The link Interface Module (LIM) provides the interface between the application subsystem and external services. Each LIM provides one or two SS7 links (depending on configuration), one X.25 link, or IP links. This assembly provides level one and some level two functions on SS7 signaling links.

The types of interfaces presently available through a LIM are:

- DS0A at 56 kbps
- OCU at 56 kbps
- V.35 at 56 kbps and 64 kbps for SS7
- T1-ATM at 1.544 Mbps
- E1-ATM at 2.048 Mbps
- E1 at 2.048 Mbps
- T1 at 1.544 Mbps
- TCP/IP at 10/100 MHz
- SCTP/IP at 10/100 MHz

Application Communication Module

The Application Communication Module (ACM) is an application card equipped with a main assembly and an Ethernet applique. It is used by the Signaling Transfer Point Local Area Network (SLAN) feature to access a remote host through an Ethernet LAN using TCP/IP.

The SLAN feature requires the gateway screening feature also be activated to control which messages are copied and sent to the remote host.

IP Services Module

The IP Services Module (IPSM) supports the optional IP User Interface feature introduced in EAGLE Release 29.0. This feature enhances the MAS features by providing a higher-speed Ethernet connection for EAGLE commands and responses. Up to three IPSMs can be deployed in a single EAGLE node. Each IPSM card supports up to eight simultaneous users over a 10/100BaseT Ethernet connection. The IPSM also provides IP connection for telnet and the FTRA application. Support for the Secure Shell (SSH) protocol was added to the IP User Interface in EAGLE Release 30.2 for added security. SSH clients and SFTP servers deployed by customers must be OpenSSH Version 2 Compatible.

The IPSM also supports the FTP Retrieve and Replace Feature. FTP-based Table Retrieve Application (FTRA) software package provides additional capability to the user for table data retrieval. The FTRA software maintenance and administration software is compatible with both Unix and Windows platforms supplied by the customer.

Database Communications Module

The Database Communications Module (DCM) provides STP Local Area Network (STPLAN) function, and 10/100Base-T ethernet links to EAGLE STP and IP7 SG systems.

General Purpose Service Module (GPSM-II)

The General Purpose Service Module (GPSM-II) is part of the Maintenance and Administration subsystem and supports the large system feature (up to 1500 links) in the Eagle. GPSM-II cards also support the Time Slot Counter (TSC) Synchronization and Integrated Sentinel Monitoring features.

Measurements Collection and Polling Module (MCPM)

The Measurements Collection and Polling Module (MCPM) is a EDSM-2G card loaded with the MCPM software. The MCPM provides comma delimited core STP measurement data to a remote server for processing. The MCPM card's ethernet ports can transfer measurements information directly to a FTP server.

Sentinel Transport Card (STC)

The Sentinel Transport card (STC) sends link monitoring data from the EAGLE 5 SAS to the Sentinel system. The STC functions as an IP router between the IMT bus internal to the EAGLE and the ethernet networks used to communicate with the Sentinel ESP servers.

Database Service Module (Eagle)

The Database Service Module (DSM) provides large capacity SCCP/database functionality used to support LNP, G-Port, G-Flex, and other functions. The DSM requires two slots for mounting and must be assigned to an odd numbered slot.

Application Service Module (Obsolete as of EAGLE 31.6)

The Application Service Module (ASM) provides an additional 16 MBytes of available memory for application processing. The ASM consists of a main assembly and a memory applique. The memory is used to store translation tables and screening data for applications such as Signaling Connection Control Part (SCCP), which is part of Global Title Translation (GTT), and Generic Load Services (GLS) which is part of Gateway Screening.

Generic Load Service (GLS) and Signaling Connection Control Part (SCCP) in systems without Local Number Portability (LNP), are provided by ASMs.

Beginning with EAGLE release 31.6, the ASM card will no longer be supported. The SCCP and GLS applications previously residing on the ASM card will be supported by the TSM card.

Translation Services Module

The Translation Services Module (TSM) performs global title translation functions required for Local Number Portability (LNP). For the Eagle system to perform LNP functions, all Signaling Connection Control Part (SCCP) Application Service Modules (ASMs) in the system must be replaced with TSMs or DSMs.

High-Capacity Multichannel Interface Module

The High-Capacity Multichannel Interface Module is a dual slot card providing eight trunk terminations processing signaling links of configurable channelized E1 or T1 connectivity. The eight E1/T1 ports reside on backplane connectors A and B.

Total system signaling link capacity depends on other cards within the system and must not exceed the provisioning limit of the EAGLE system. Since the HCMIM has the capacity to process a full T1 or E1 on a single card, daisy chaining or channel card operation is not needed. Interoperation with LIM-E1 or E1/T1 MIMs operating in channel mode is not supported

Generic Program Loads

Application software is downloaded to individual application cards by means of Generic Program Loads (GPLs). A GPL is a specific instance of an application for a specific piece of hardware. Hardware is defined to Eagle and IP7 SG systems by means of a series of administration commands. Software is then loaded from the fixed disk over the IMT bus directly to the cards. The type of the GPL loaded depends on the card and card function that is chosen.

The following are examples of GPLs:

- SCCP —Signaling Connection Control Part. This software allows the Translation Service Module (TSM/DSM) to be used as a memory board for Global Title Translation (GTT). Inbound SCCP messages from Link Interface Modules (LIMs) are sent to the TSM/DSM assigned to the LIM by system software. SCCP software on the TSM/DSM performs the translation, and sends messages through the IMT back to the appropriate LIM, which routes messages to the destination. The SCCP application can run on TSM and DSM cards.
- SLAN—Signaling Transfer Point Local Area Network. This software allows the system to support a TCP/IP interface to any external host with ACMs and DCMs.
- SS7—This software provides access to remote SS7 network elements.
- GX25—This software allows the system to send and receive traffic to and from an X.25 network, and convert the packet to an Signaling System #7 Message Signaling Unit (SS7 MSU).
- GLS—Gateway Loading Service (GLS) software controls download of Gateway Screening (GWS) data to Link Interface Modules (LIMs) and TSM when necessary. This ensures a fast download of gateway screening data when a card re-initializes.

  Gateway screening data is downloaded when a card is re-initialized, when Gateway screening is changed by database administration, or when there is manual intervention with commands being entered at a terminal.

- EROUTE—Ethernet Routing transfers link information messaging from the Eagle LIM cards to the Integrated Sentinel using TCP/IP and EAGLE Monitor Protocol (EMP). Implemented in Sentinel Transport Cards (STC).
- EOAM—Enhanced Operation Administration and Maintenance GPL for GPSM-II cards.
- IPLIM—The application software used by the DCM card for IP point-to-point connectivity for ANSI point codes.
- IPLIMI—The application software used by the DCM card for IP point-to-point connectivity for ITU point codes.
- SS7IPGW—The application software used by the DCM card for IP point-to-multipoint capability within an ANSI network.
- IPGWI—This application is used by the DCM card for IP point-to-multipoint connectivity for ITU point codes. The system allows a maximum of 64 cards to be assigned the ipgwi application.

Timing Systems Eagle/IP7 SG

Eagle and IP7 SG systems use synchronized timing systems to provide accurate reference standards to all cards on the IMT buses.

System Clock

Eagle and IP7 SG systems connect to the 64KHz composite Building Integrated Time System (BITS) clocks through two DB-15 style connectors on the backplane of the control shelf. The two clocks are labeled primary and secondary and are sent to both MASPs. Each MASP selects between two BITS clock signals to provide a system clock to the rest of the Eagle and IP7 SG systems. The system clock is used by Link Interface Modules (LIMs) for X.25 and Signaling System #7 (SS7) Digital Service level-0 Applique (DS0A) signaling links, with each LIM selecting either clock A or clock B for its own use.

Eagle and IP7 SG systems also distribute system clocks to all frames. All shelves, both extension shelves and control shelves, provide "clock in" and "clock out" connections. Clock cables from the control shelf connect to the "clock in" connector on the top shelf of each frame. From the "clock out" connector on the top shelf of each frame, the clock signals are connected to the "clock in" connector of the middle shelf of the frame and from that shelf to the bottom shelf.

The EAGLE 5 SAS Primary and Secondary system clock inputs are internally distributed by the TDM through the EAGLE as clocks A and B. The DB-15 connectors and the appropriate cables can accept up to three distinct types of clock signals:

- RS-422 High- Speed Master Timing clock running at 2.048Mhz or 1.544Mhz
- Clock reference signals in T1 or E1 formats
- 64KHz composite clock

  NOTE: Note: EAGLE systems equipped with TDM card 870-0774-15 or later and EAGLE software Release 31.6 or later can accommodate E1 and T1 formatted clock reference signals in addition to RS-422 signals.

Holdover Clock

An optional holdover clock can maintain clock synchronization for Eagle and IP7 SG system DS0A links during brief interruptions of the Building Integrated Timing System (BITS) clock signals. In accordance with Telcordia Technologies GR-1244-CORE, BITS clock outages of up to 15 seconds can be tolerated.

BITS Clock Routing

BITS clock signals A and B are routed through the holdover clock and then to the system, allowing the holdover clock to continue Stratum 3 clock signals to the Eagle and IP7 SG systems.

High-Speed Master Timing

The Eagle can be configured with high-speed master timing capabilities. High-speed master timing allows synchronization of LIM cards at E1 or T1 rates.

High-Speed clock input is required to support an EAGLE node serving as the Timing Master in a network. High-Speed clocks are not necessary if EAGLE high-speed signaling links (either channelized E1/T1, or ATM formatted E1 or T1) operate in “line” mode, meaning that each individual link derives timing from its incoming signal. Both High-speed Master Timing inputs and Composite Clock signals can be simultaneously accommodated by the EAGLE Control Shelf using the appropriate Tekelec cables.

For more information about installing or upgrading to high-speed timing see the section on Master Timing in the “*NSD Installation Manual*”.

Time Slot Counter Synchronization

Time Slot Counter Synchronization (TSC) Synchronization, an option for Eagle systems in release 28.0 and later, allows all cards in the system that contain a Time Slot Counter (TSC) to synchronize with one another. The ability to have synchronized timing between cards is used in applications such as system wide message time stamping.

Basic EAGLE 5 SAS Theory of Operation

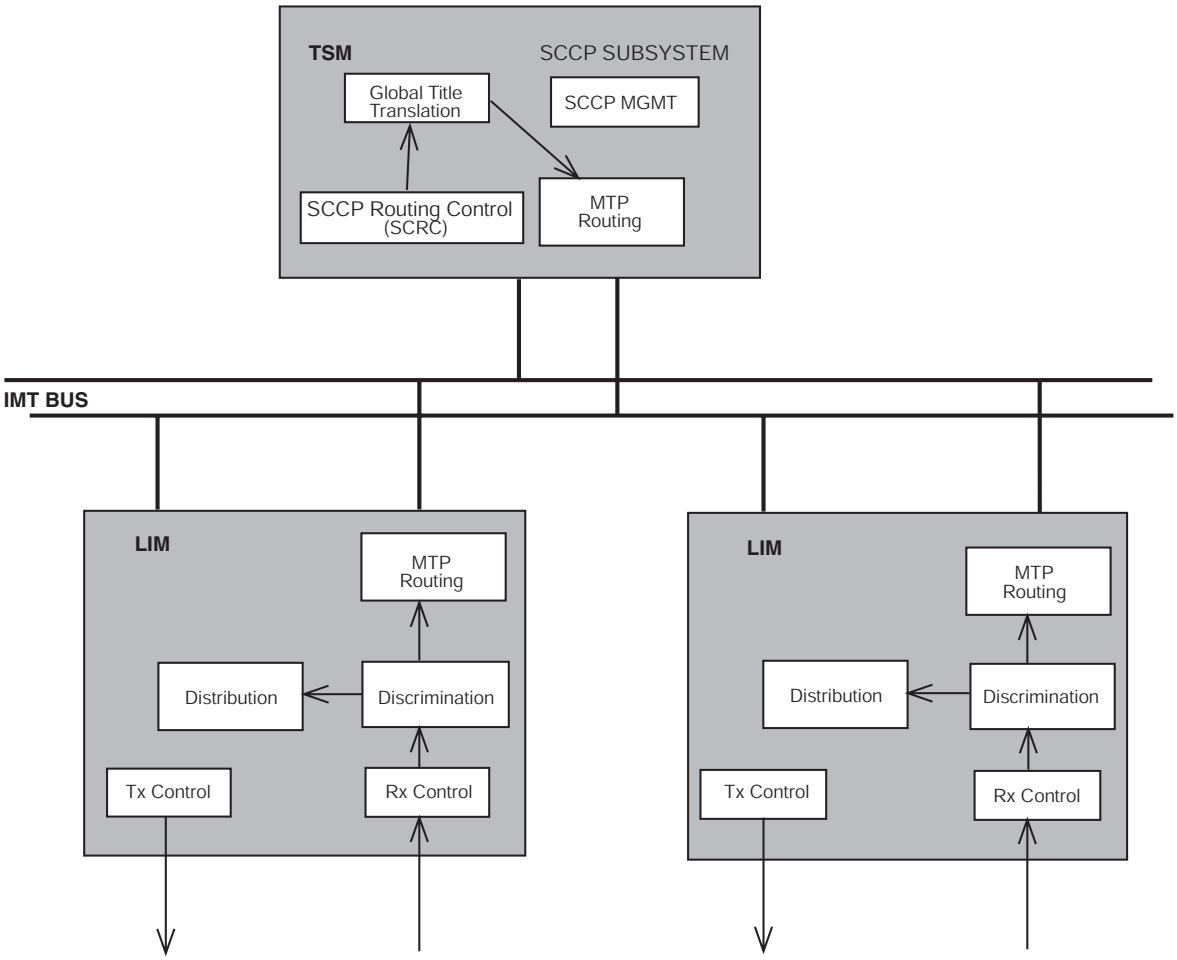
The EAGLE 5 SAS implements SS7 MTP function, level 2 and level 3, through software contained entirely within the LIMs. (No separate central processing unit exists within the EAGLE 5 SAS.) All message processing logic, including the links, link sets, and routes associated with each origination point code/destination point code in the signaling network are included within the MTP routing feature module. The STP offers full point code routing. (For rapid recovery from processor faults, copies of this software are also stored on the hard disk.) The LIMs can handle a 100% traffic load on each link, assuming a small MSU size.

The following illustrates incoming messages that are routed through an EAGLE 5 SAS. If gateway screening is activated, the messages are screened before they are examined for further processing. The message discrimination function determines whether the message can be routed based solely on the MTP routing label. If so, the outgoing link is identified with its equipment address (LIM), and the message is transferred through an IMT bus to that LIM for transmission to the designated destination point code (DPC).

If the discrimination function determines that a global title translation (GTT) is required, the message is sent, through the message distribution function, to SCCP routing that routes the message.

After the message arrives at the designated module, the destination point code (DPC) and subsystem number for this message are determined by global title translation, and the message is transferred through an IMT bus to the appropriate LIM for transmission to the designated DPC. See Figure 3-4.

Figure 3-4. Example EAGLE 5 SAS message flow



SEAS Subsystem (Optional)

The SEAS subsystem allows the EAGLE 5 SAS to connect to the Signaling Engineering and Administration System (SEAS). The Signaling Engineering and Administration System (SEAS) is an interface defined by Bellcore and used by the Regional Bell Operating Companies (RBOCs), as well as other Bellcore Client Companies (BCCs), to remotely administer and monitor the signaling points in their network from a central location.

SEAS provides a single, reliable, machine-to-machine interface by which commands are entered from a Signaling Engineering and Administration Center (SEAC) or a Signaling Network Control Center (SNCC) to various signaling points, such as STPs. These signaling points then provide command responses to the SEAC. The signaling points also provide automatic alarm and measurement data to the SEAC. Specifically, SEAS is used for the following functions.

- Memory Administration (Recent Change and Verification)
- Network Maintenance
- Network Data Collection (Measurements)
- Network Traffic Management Surveillance
- SEAS Application Control
- Supplier Specific Functions

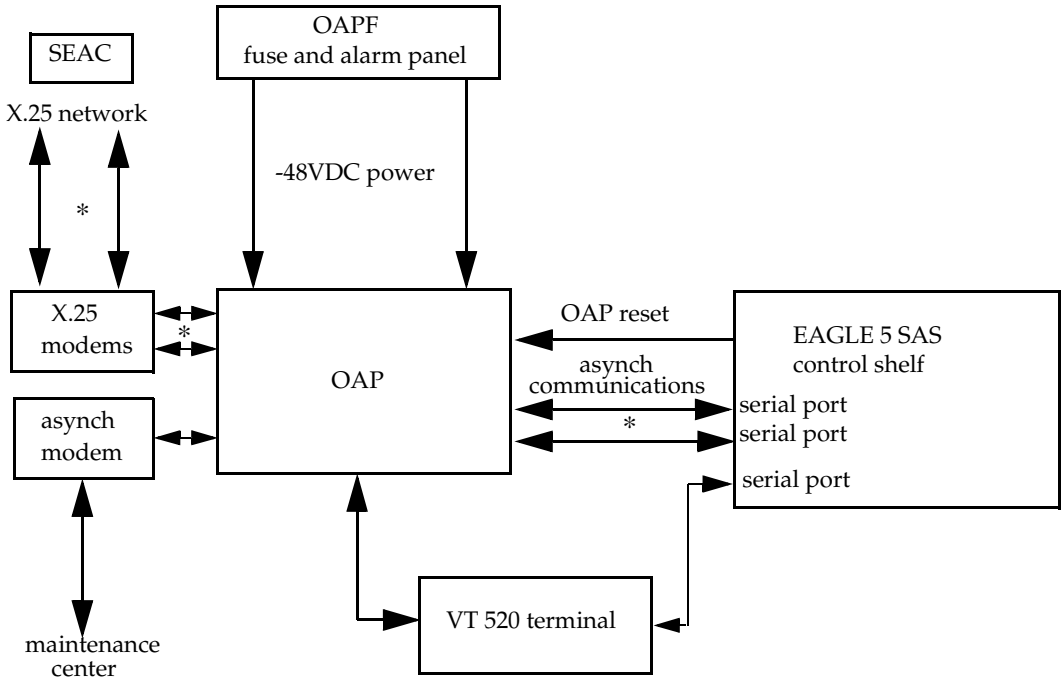
The SEAS interface has the following capabilities:

- Flow through messages - This allows any EAGLE 5 SAS command to be entered into the system from a SEAS console.
- Recent change and verify (immediate activation only) for following data entities:
  - MTP (routes, route sets, signaling links, linksets, point codes, and so forth)
  - GTT (global title translations, subsystems, and mated applications)
  - GWS (all gateway screening tables)
- Data collection (autonomous and on-demand) for existing measurement data
- On-occurrence output capability for existing reports
- Supports one active X.25 signaling link and one backup X.25 signaling link. Each X.25 signaling link supports a maximum of 10 PVCs at a data rate of 9.6 kbps on a per link basis.

The SEAC uses X.25 links to transmit data to and receive data from the signaling points it is monitoring. Terminal inputs to the EAGLE 5 SAS use asynchronous RS-232 ports. An operations system support applications processor (OAP) is used to allow the EAGLE 5 SAS to communicate with the SEAC.

The OAP is an adjunct processor that interfaces to a X.25 link and converts the data stream to an asynchronous serial format. All conversion from SEAS to EAGLE 5 SAS command sets takes place on the EAGLE 5 SAS. Two terminal disk module (TDM) ports (RS-232) running at 19,200 bps connect the OAP to the EAGLE 5 SAS. Two X.25 links connect the OAP to the SEAC. The OAP is mounted in a frame similar in design to the other frames used in the EAGLE 5 SAS, and is labeled as OAPF. See Figure 3-5.

Figure 3-5. SEAS Subsystem



* Two links are provided in a single OAP system. When two OAPs are installed in a system, each OAP has a single link.

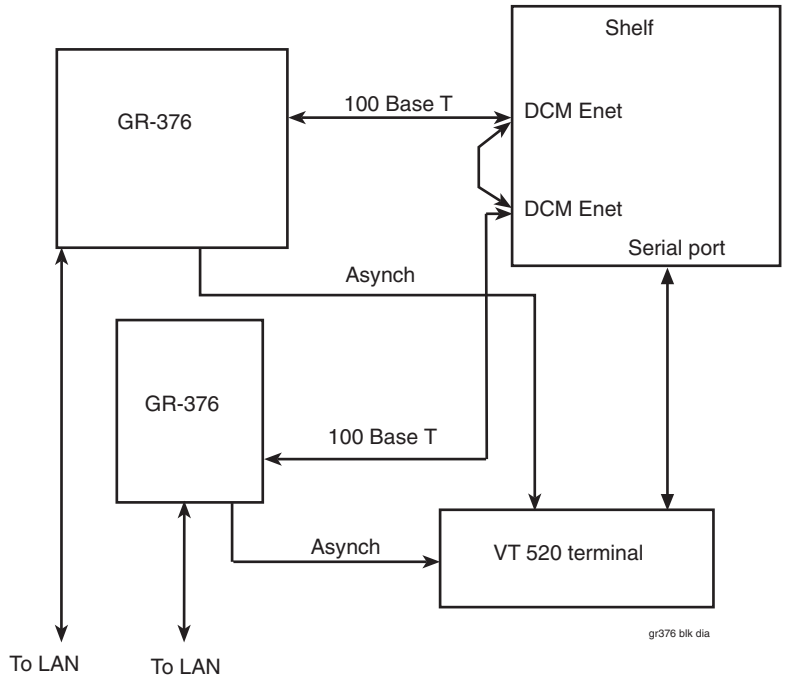
Embedded Operations Applications Processor (EOAP)

The Embedded Operation Support System Applications Processor (EOAP) is hosted in an assembly mounted in a dedicated EOAP Frame (OAPF). The EOAP and GR-376 applications run on the EOAP host assembly. More than one EOAP host shelf can be mounted in each OAPF. Each EOAP host shelf contains cards provisioned to support one or two EOAP systems. The EOAP application translates and converts higher layer protocols into asynchronous serial communications. The EOAP provides translation and async/X.25 conversion as part of the optional Signaling and Engineering Administration System (SEAS) interface for the Eagle system. An EOAP host shelf communicates with the Eagle system control shelf through two serial interface ports. The EOAP host replaces the older TMOAP assembly which is obsolete in the field but still supported by Tekelec. For more information see Chapter 8, "EOAP".

GR-376 EOAP

The GR-376 application runs on the EOAP host processor assembly mounted in a dedicated OAP Frame (OAPF). Two GR-376 EOAPs can be mounted in each OAPF. The GR-376 EOAP application communicates with the Eagle system through an Ethernet port (see Figure 3-6). The GR-376 EOAP hardware changes required to accommodate the GR-376 EOAP features include the addition of a second Ethernet port to the processor card, and use of 256MByte of memory instead of 64MByte. A Tekelec-designed drive bay provides connections and housing for a 3 1/2-inch Small Computer System Interface (SCSI) hard drive card and a 5 1/4-inch CD-ROM drive card.

Figure 3-6. GR-376 EOAP in an Eagle System



IP7 Secure Gateway

The IP7 Secure Gateway subsystem of the EAGLE 5 SAS provides connectivity between SS7 and IP networks, enabling messages to pass between the SS7 network domain and the IP network domain, as follows:

- When the IP7 Secure Gateway receives an SS7 formatted message over an SS7 link, it dynamically converts this message into TCP/IP format and routes the re-formatted message over an associated IP link to a destination residing within an IP network.

  The IP7 Secure Gateway uses sockets to access the IP domain. Sockets identify TCP/IP sessions.

- Conversely, when the IP7 Secure Gateway receives a TCP/IP formatted message over an IP link, it dynamically converts this message into SS7 format and routes the re-formatted message over an associated SS7 link to a destination residing within the SS7 signaling network.

  Address resolution is not performed in the IP to SS7 direction. It is the responsibility of the sending application to insert a point code into the SCCP Called and Calling Address message fields. The IP7 Secure Gateway uses the address fields to build the MTP routing label, to include the MTP3 portion, and route the message to the SS7 network.

IP7 Secure Gateway Hardware, Applications, and Functions

The IP7 Secure Gateway functions are provided by applications that run on IP cards. IP cards can be either a Database Communications Module (DCM) or an Enhanced-Performance Database Communications Module (EDCM). IP cards provide interfaces between the IMT bus and two 10/100 Base-Tx IEEE 802.3/Ethernet interfaces. The IP cards, similar to any other Link Interface Module (LIM) on the IP7 Secure Gateway, use the Interprocessor Message Transport (IMT) bus to communicate with the other cards in the system. The primary job of an IP card is to send and receive SS7 data on a network (in this case, an IP network), and to route that data to other cards in the system as appropriate.

The IP card can run any of the following applications:

- `iplim` or `iplimi` - Both applications support STP connectivity via MTP-over-IP functionality point-to-point connectivity (for more information, see "Connecting STPs Over the IP Network" on page 3-21).

  For these applications, the other end of the point-to-point connection is always another IP card running the `iplim` or `iplimi` application. This type of connection is essentially the same as that of a traditional SS7 point-to-point link, except that the traditional MTP2 and 56Kb/s technology is replaced by TCP/IP and Ethernet technology.

  The `iplim` application supports point-to-point connectivity for ANSI networks. The `iplimi` application supports point-to-point connectivity for ITU networks. With the optional ANSI/ITU MTP Gateway feature and proper configuration, the system could convert between any of the ANSI, ITU-N, and ITU-I networks, switch traffic between these networks, and perform network management for each of these networks.

  The IP7 Secure Gateway can support up to 41 100 cards with `iplim` and `iplimi` applications.

- `ss7ipgw` and `ipgwi` - These applications support the following types of point-to-multipoint connectivity for networks:

  – SCP connectivity via SCCP/TCAP-over-IP functionality (for more information, see "Connecting to SCPs with SCCP/TCAP Messages Sent Over the IP Network" on page 3-22)

  – SEP connectivity via ISUP, Q.BICC, and TUP-over-IP functionality (for more information, see "Connecting SEPs Using ISUP, Q.BICC, and TUP Messages Over the IP Network" on page 3-22)

  – SCP/SEP connectivity via non-ISUP, non-SCCP, non-Q.BICC, and non-TUP-over-IP functionality.

  The `ss7ipgw` application supports point-to-multipoint connectivity for ANSI networks. The `ipgwi` application supports point-to-multipoint connectivity for ITU networks.

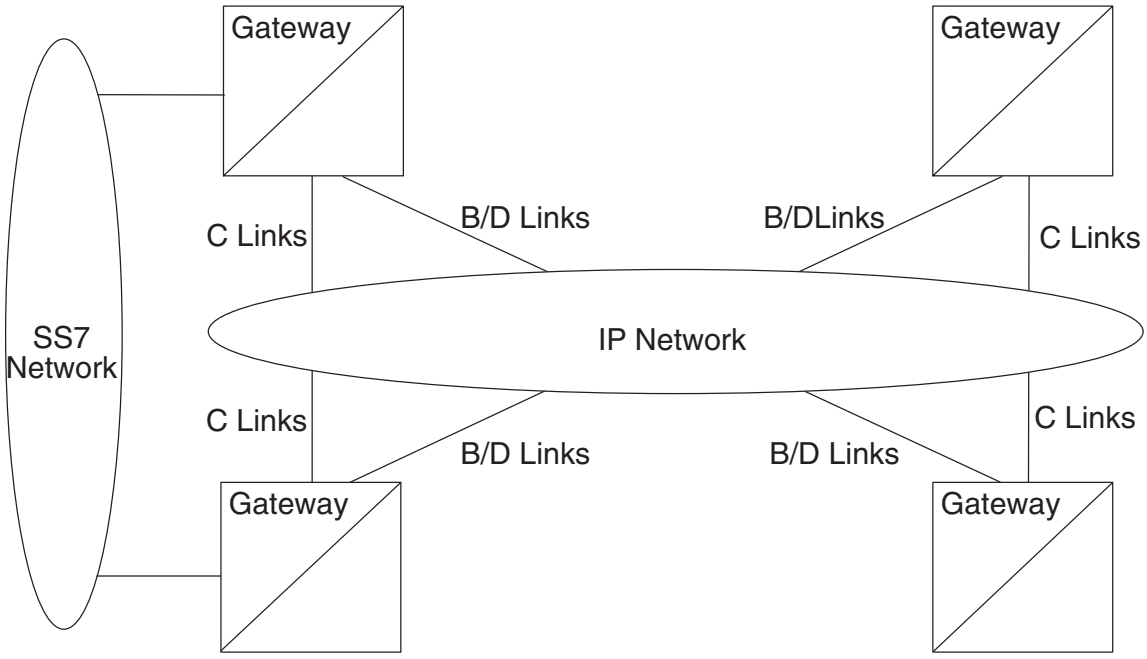
In addition to running an `iplim`, `iplimi`, `ss7ipgw`, or `ipgwi` application, each IP card supports the following functions:

- A Simple Network Management Protocol (SNMP) agent.
- Message Transfer Part (MTP) status. This function is available only on IP cards that support the `ss7ipgw` or `ipgwi` application. For more information, see "Support for MTP Status Functions" on page 3-23.

Connecting STPs Over the IP Network

This functionality allows the use of an IP network in place of point-to-point SS7 links to carry SS7 MSUs. Figure 3-7 shows a diagram of this type of IP7 Secure Gateway network. For example, the C links between the mated pair of STP or B/D Quad links between STPs can be replaced by an IP network. The IP7 Secure Gateways are deployed on both ends of the link (point-to-point connection). The IP7 Secure Gateway converts the SS7 MSUs to IP packets on one end of the link, and IP packets to SS7 MSUs on the other end of the link.

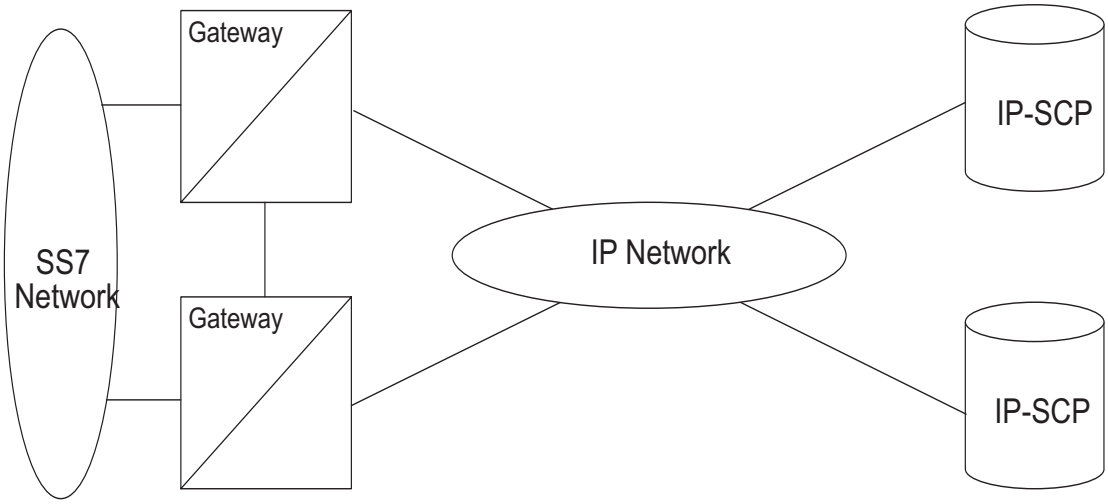
Figure 3-7. IP7 Secure Gateway Network (STP Connectivity via MTP-over-IP)



Connecting to SCPs with SCCP/TCAP Messages Sent Over the IP Network

This functionality allows SS7 nodes to exchange SCCP/TCAP queries and responses with an SCP residing on an IP network. Figure 3-8 shows a diagram of this type of IP7 Secure Gateway network.

Figure 3-8. IP7 Secure Gateway Network (SCP Connectivity via TCAP-over-IP)

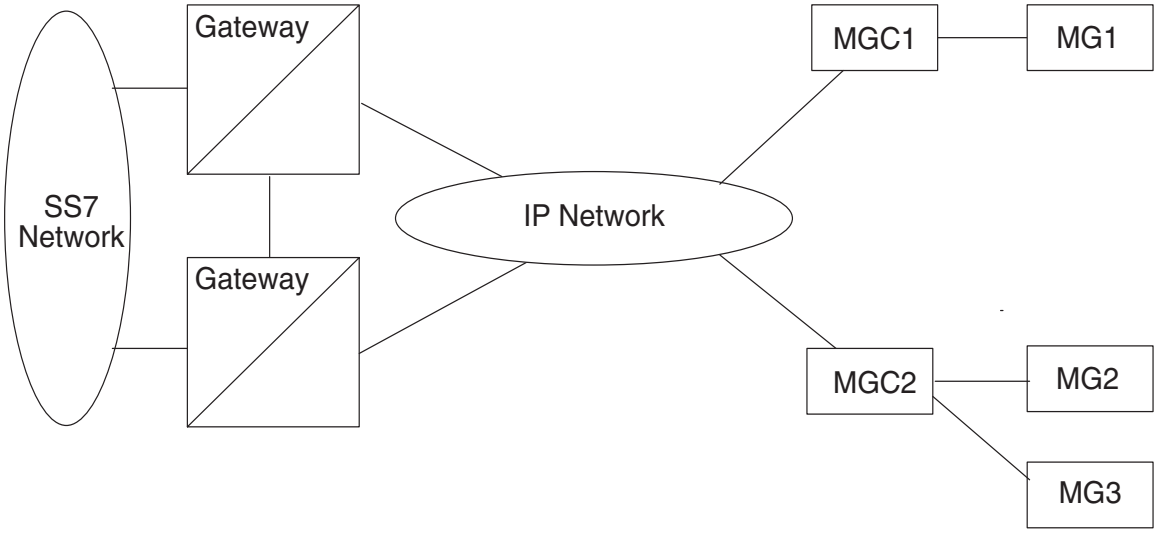


The IP7 Secure Gateway node manages the virtual point codes and subsystem numbers for the IP-SCP. From the SS7 network perspective, the TCAP queries are routed using these virtual point codes/SSNs. The IP7 Secure Gateway node maps the virtual point code/SSN to one or more TCP sessions (point-to-multipoint connection), converts the SS7 MSUs to TCP/IP packets by embedding the SCCP/TCAP data inside TCP/IP packets, and routes them over an IP network. The IP7 Secure Gateway also manages application subsystem status from an IP network's perspective and an SS7 network's perspective.

Connecting SEPs Using ISUP, Q.BICC, and TUP Messages Over the IP Network

This point-to-multipoint functionality allows SS7 nodes to exchange ISUP, Q.BICC, and TUP protocol messages with one or more signaling end points (class 4 switches, class 5 switches, VoIP gateways, Media Gateway Controllers, or Remote Access Servers) residing on an IP network. Figure 3-9 shows an example of this type of IP7 Secure Gateway network.

Figure 3-9. IP7 Secure Gateway Network (SEP connectivity via ISUP, Q.BICC, and TUP-over-IP)



The IP7 Secure Gateway node maps the originating point code, destination point code, and circuit identification code to a TCP/IP address and port. The SEP is provided the originating and destination point codes in the MTP level 3 routing label as part of the passed protocol.

Understanding Routing for `ss7ipgw` and `ipgwi` Applications

The **`ss7ipgw`** and **`ipgwi`** applications can use a single point code, called a virtual point code. This code is assigned to a set of TCP/IP devices that it connects to. The IP7 Secure Gateway distinguishes between the devices within the set by using application routing keys and application IP connections.

Application routing associates SS7 routes with IP connections. SS7 routes define a filter based on SS7 message data. Application IP connections define the connection between the IP local host/local port and IP remote host/remote port. If the routing keys filter matches the IP connection, the SS7 message is sent to the associated application IP connection.

Routing keys can be fully or partially specified, or specified by default.

Support for MTP Status Functions

This feature, available only on IP cards that support the `ss7ipgw` and `ipgwi` applications, allows the Message Transfer Part (MTP) status of point codes in the SS7 networks to be made available to IP-connected media gateway controllers (MGCs) and IP-SCPs. This feature is similar to the MTP3 network management procedures used in an SS7 network.

This feature enables an IP device to:

- Divert traffic from an SG that is not able to access a point code that the mated SG can access
- Audit point code status
- Build up routing tables before sending traffic
- Be warned about network congestion
- Abate congestion

4

LNP

Contents ..... Page

Introduction to LNP 4-1

EAGLE LNP Functional Capabilities 4-4

EAGLE LNP Functional Capabilities 4-4

LNP Hardware 4-9

Introduction to LNP

This chapter describes the EAGLE Local Number Portability (LNP) system, including the Local Service Management System (LSMS). It also provides a high-level theory of operation designed to assist maintenance personnel in troubleshooting the EAGLE LNP system. For detailed descriptions of EAGLE LNP hardware, refer to the *Installation Manual*.

LNP is a public switched telephone network capability that allows a user served by one switch (donor switch) to move their service to a different switch (recipient switch) while retaining their public directory number. Any user can call the ported subscriber using the unchanged directory number. The switch which recognizes that the call may be to a ported number (initiating switch) will route the call to the new recipient switch instead of old donor switch using a new Location Routing Number (LRN) instead of the dialed directory number (DN). The initiating switch may be the switch where the call originated (originating switch), an intermediate switch, or a terminating switch.

The LNP network capabilities described above are traditional STP (Signal Transfer Point) functions (for example, enhanced LNP Global Title Translation [GTT] routing services). However, there are certain application level functions which are traditional SCP functions (LRN query/Response), but are implemented as an extension to the EAGLE. This requires the EAGLE to emulate some of the service control point (SCP) behavior at Signaling Connection Control Point (SCCP) and Transaction Capabilities Application Part (TCAP) levels. The enhanced GTT functions consist of ported NPA-NXX detection and the message relay function.

Query Methods for Wireless and Wireline Networks

Tekelec's LNP solution provides two query methods to address the needs of wireline and wireless providers. For wireline, ANSI-41, and PCS-1900 networks, triggers in the originating exchange launch an LNP query to the EAGLE with LNP to determine whether the dialed number (DN) has been ported. The EAGLE queries its database and, if the number has been ported, returns the location routing number (LRN) to the originating exchange so the call can be routed. If the number has not been ported, a response indicating a non-ported number is returned.

The second query method is a triggerless solution, which delivers cost savings on switch upgrades and extends the mobile switching center's (MSC's) life. For triggerless queries, the LNP-equipped EAGLE receives the initial address message (IAM) with the dialed number from the MSC. It queries its LNP database to locate the LRN and determine whether the number has been ported. If the number has not been ported, the IAM is switched through to the tandem indicating a non-ported number has been detected. If the number has been ported, the triggerless-equipped EAGLE modifies the IAM to include the LRN. The converted IAM is then passed directly to the tandem.

EAGLE LNP features include:

- less than 75 mean millisecond processing delay (last bit in to first bit out)
- simplified data management and more efficient data storage
- supports up to 96 million ported numbers with five service (CNAM, LIDB, CLASS, ISVM, SMS)
- scalable solution (1,700 to 40,000 TPS)
- LRN query and message relay translation combined directly on the platform
- existing EAGLE platform users add LNP functionality with a simple hardware and software upgrade
- based on T1S1.6 Number Portability and Telcordia's GR-2936- CORE LNP Capability specifications
- supports AIN, IN, ANSI-41 and PCS 1900 query formats
- T1 high-speed and IP link capability
- supports triggerless LNP solution for wireless applications
- supports advanced global title translation (GTT) functions (including LNP message relay):
- 10 digit intermediate and final GTT
- 10 digit GTT for CLASS/LIDB/ISVM/CNAM/SMS
- 6 digit default GTT for non-ported DN in a ported NPA-NXX
- eliminates SCCP looping and circular routing
- provides subsystem management of remote applications
- supports routing of non-final GTT messages to an A-link
- performs GTT for LNP queries and LNP query processing on the same node
- supports coexisting databases for non-LNP GTT, LNP GTT, and LRN
- supports number pooling / efficient data representation

Local Service Management System (LSMS)

Tekelec's LNP solution includes the LSMS, which provides the interface between the number portability administration center (NPAC) service management system and the EAGLE's element management system (EMS). It maintains and distributes LNP data to the service provider's LNP databases. The LSMS is equipped with a graphical user interface to administer subscription, service provider, and network data.

LSMS features include:

- eight industry standard Q.3 NPAC interfaces
- supports administration of override data internal to the service provider's network
- supports up to eight EAGLE pairs
- ability to partition databases according to area of portability service (AOPS), eliminating the need for database replication on all nodes
- data auditing and reconciliation between EAGLE and the LSMS
- connection management for communications links, including automatic error detection and failure recovery
- enhanced security, including key management and firewall

Tekelec's LSMS operates on a SUN server system in an active and hot-standby configuration for high availability. Each Tekelec LSMS is configured with dual processors for fail-over conditions and shares a disk array capable of storing 96 million LNP data entries.

Normal updates are sent from the LSMS to the active EAGLE LNP Application Processor (ELAP) at a rate of 25 TNs per second over a connection that uses the proprietary High Speed Operations Protocol (HSOP) over TCP/IP protocol. The ELAP forwards the messages to all the DSMs using a IP multicast protocol (for more information, refer to the ELAP Administration Manual). No user action is required at the network element.

EAGLE LNP Functional Capabilities

LNP Query Service (LNPQS)

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

LNPQS task is divided into the following sub-tasks:

- Query verification
  All Queries are verified to conform to the encoding rules. If a query

does not conform to encoding standards, it is considered an invalid query and is either discarded or a TCAP error response is generated.

- Query decoding
  This is where the DN is decoded from query. This decoded dialed number (DN) is used to search for the provisioned LRN.
- Response generation
  Here a response message encoded with a DN or/and LRN is sent back to the generator of the query.

Automatic Call Gapping (ACG)

Automatic Call Gapping (ACG) procedures are used for overload control. ACG controls the rate at which location routing number (LRN) queries for a specified telephone number or a portion of a telephone number are received by the EAGLE LNP when predefined thresholds are reached. When conditions warrant, the LNP application will send ACGs as part of the AIN or IN LRN query response to throttle queries from the SSPs.

LNP Message Relay (LNPMR) Function

The LNPMR function performs enhanced GTT routing to support vertical services associated with portable numbers. This function performs 10-digit LNP GTT maintaining backward compatibility with existing non-LNP Operations Support Systems (OSSs). Currently, OSSs (and some switches) use 6-digit GTT for certain services. To minimize the impact of LNP on these systems, the EAGLE has to extract 10-digits from the TCAP portion of the message and use that as a Global Title Address (GTA). LNPMR is required to have a DN in the SCCP portion of the message.

Message Relay (MR) is an enhancement to existing GTT functions. Message relay involves the following main functions:

- Extraction of 10 digit dialed number from the TCAP portion of the message: If the MSU contains a 6-digit Called Party Address, MR will get the 10-digit dialed number from the TCAP portion of the MSU.
- Increased number of translations: For each 10 digit dialed number, up to 6 translations are possible. The number of dialed numbers that can be entered depends on the hardware.
- Replacement of GTA: MR provides the option of replacing the GTA in the Called Party Address with the LRN associated with the ported dialed number.

Message relay is performed in three stages:

1. The message arrives at the EAGLE LNP *route-on-gt*. The EAGLE performs 6-digit (NPA-NXX) translation. The result of this translation indicates if

message relay is required. If it is required, the result of this translation also gives the default data that may be used in stage 3.

2. If stage 1 indicates message relay is required, the EAGLE LNP then performs 10-digit message relay. If the 10 digit number is found, the translation data for the 10 digit number is used to route the message.

3. If the 10 digits are not found, the dialed number is not ported, and the default data from stage 1 is used to route the message.

EAGLE LNP Database

The database is partitioned between the EAGLE LNP and the EAGLE to eliminate the possibility of an LNP subsystem failure causing an EAGLE failure. The database provides fast real-time database access times (LNP 6 digit default GTT data, 10 digit ported GTT data, and LRN data all accessed within approximately 20ms). The EAGLE LNP database has the capability to increase the amount of database records in an incremental fashion without losing real-time performance. The EAGLE LNP database has the capability to provide different administrable views of database records (NPAC, LSMS, SEAS, EAGLE views), and also provides global database change capabilities (such as NPA-SPLITS, LRN Final GTT changes).

SCCP Subsystem Management

Messages for Local EAGLE LNP Subsystems

Messages for the local EAGLE LNP subsystem arrive *rt-on-ssn* or *rt-on-gt*. If they arrive *rt-on-ssn*, they contain an EAGLE true point code in the destination point code (DPC) field of the message, and an EAGLE LNP Subsystem number in the Called Party Subsystem field of the message. The EAGLE LNP processes the message if it has the EAGLE capability point code for the DPC, but will not be able to divert the message in the event of subsystem failure.

If messages arrive *rt-on-gt*, they contain a translation type and GTA that translates to the EAGLE True Point Code and the EAGLE LNP Subsystem. These messages also contain one of the EAGLE capability point codes in the DPC field. The EAGLE LNP processes the message if it has the EAGLE true point code for the DPC, but it will not be able to divert the message in the event of subsystem failure.

Database Audit

The EAGLE LNP audit is responsible for the following:

- Ensuring the contents of the current or backup LNP databases do not become altered by unapproved or unexpected mechanisms such as software bugs, COPY-TBL, etc.
- Ensuring the contents of the current LNP database are mirrored exactly on all cards which are maintaining a copy.

The ELAP to DSM interface is over TCP/IP Multicast to allow for rapid loading of the DSM cards. Auditing and reconciling LNP data is automatic and does not require any user intervention.

The ELAP downloads LNP data to the each DSM card with a checksum. After receiving the LNP data, the DSM recomputes the checksum and if the 2 checksums do not match, the DSM automatically requests a new update from the MPS.

The DSM(s) can continue to receive updates from the MPS when a particular DSM card needs to be reloaded. DSM(s) can also retain their RAM-based data as long as power is not removed from the card (warm restart). DSM(s) can reload LNP data rapidly in the event of the DSM loses power (cold restart).

The LNP database audit executes once every 24 hours. If a complete audit of the LNP database requires less than 24 hours (i.e. because the LNP database is not fully populated), then another audit cycle will not start until 24 hours have elapsed since the previous audit cycle started.

LNP Maintenance

The EAGLE LNP requires a DSM card for GPL and data loading. In addition, the SCCP GPL's application data loader will register all tables for loading, independent of the LNP feature provisioning and motherboard / daughterboard hardware configuration.

As a result, load requests are always identical. During loading, multiple SCCP load requests are combined into a single download, reducing the overall download time. The SCCP card will store or discard LNP table data based on whether it has LNP capable hardware or not.

Reporting Functions

The EAGLE LNP solution provides users on-demand status of the LNP subsystem. The EAGLE displays a detailed status of LNP information for the LNP system as a whole or for a given DSM. The system wide detailed report includes information for each of the GTT, LNP message relay (LNPMR), LNP query service (LNPQS), Wireless (IS-41) LNP query service (WNPQS), PCS 1900 LNP query service (PLNPQS) and automatic call gapping (ACG) functions.

The EAGLE also provides a set of measurements related to LNP query and message relay traffic. These measurements include queries for ported numbers per LRN, queries for non-ported numbers per NPA-NXX, and ported and non-ported message relay GTTs received for CLASS, LIDB, CNAM, ISVM and WSMSC. These measurements are available hourly and daily. Daily measurements are maintained for one week.

Measurement and Billing Functions

Measurement data is provded by the Measurement Collection and Polling Module (MCPM). This dedicated processor platform consists of multiple MCPM (EDSM-2G) cards in a primary/secondary configuration, in which a single primary MCPM performs all collection and reporting functions. The secondary MCPM cards serves as backup for the primary MCPM.

The primary MCPM monitors the status of all secondary MCPM cards. If the primary MCPM fails before or during collection, the secondary MCPM card assumes the primary role, and begins/continues collection. Legacy GR310/778 measurements are still supported.

The Measurements Platform collects and stores the collected data in MCPM RAM. Following collection, comma delimited scheduled reports are automatically generated and transferred to the customer's FTP server via the FTP interface.

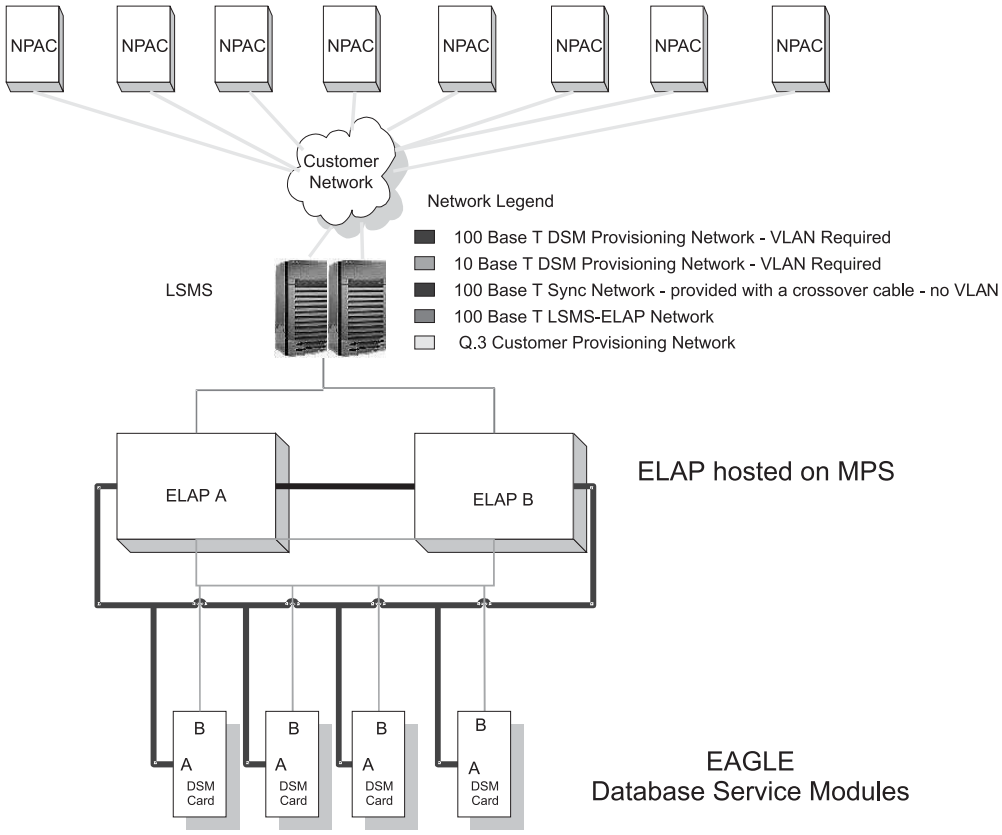
The reports are always transferred to the configured Primary FTP Server or, if the Primary server is down, to the configured Secondary FTP Server. The filename of the report contains the CLLI name of the EAGLE to easily identify the source of the data. Measurement collection periods of 15 minute, 30 minute, hourly, and daily are provided.

On-demand report requests are also generated and transferred to the customer's FTP server, or output to the terminal. A command to enable the user to transfer missed scheduled reports is also available. Its purpose is to enable the customer to recover any scheduled reports within the last 24 hours that may not have transferred to the FTP Server. If these measurements are used for the billing function, aggregation, formatting and other billing functions must be performed on an external device.

LNP Hardware

Figure 4-1 provides an overview of the hardware components needed to support LNP. ELAP servers transmit data from the EAGLE to LSMS servers. ELAP Servers use Tekelec's Multi-purpose Server (MPS) platform. For information on MPS, see Chapter 6, "MPS".

Figure 4-1. LNP Hardware Overview



LSMS

The Local Service Management System (LSMS) provides an interface between the Number Portability Administration Center (NPAC) Service Management System (SMS) and the service provider's Element Management System (EMS). The LSMS maintains a service provider's LNP data.

The LSMS is composed of hardware and software components that interact to create a secure and reliable LNP system. This section gives an overview of the LSMS hardware and describes the LSMS hardware components.

Standard and Optional Hardware Components

This section lists the standard and optional hardware components for the LSMS Release 6.1 Enterprise 450 platform.

Standard Hardware Components

- Two Sun Enterprise 450 servers
- Two Sun StorEdge D1000 Disk Systems
- Twelve external hard disks (six per storage array)
- Two internal hard disks
- One Fast Ethernet switch
- Two HP SureStore Optical 5200ex (MO) disk drives
- Two 3Com U.S. Robotics 56K modems
- Two expansion cabinets (with power sequencers) housing the servers, disk systems, switch, optical disk drives, and modems
- One Sun Ultra 5 with 17" monitor, keyboard, and mouse
- Two Sun DDS-3 Autoloader tape drives

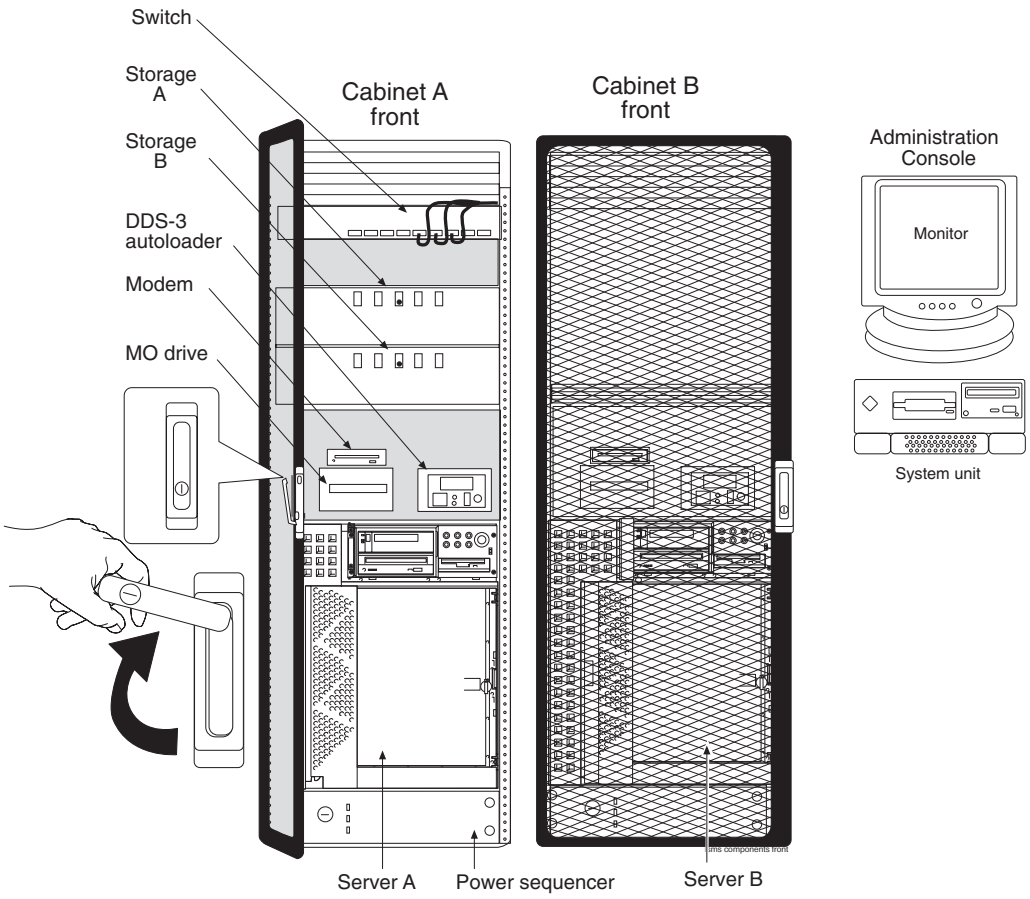
Optional Hardware Components

- 96 Million Numbers Option
  - Two external hard drives (one per storage array) as hot-spare disks.
  - Four external hard drives (two per storage array) as mirrored shared storage.

LSMS Hardware Configuration

The physical layout of the Tekelec LSMS hardware platform server components is shown in Figure 4-2 on page 2-11.

Figure 4-2. Overview of LSMS Hardware Components



5

Sentinel

Sentinel 5-1
Integrated Sentinel 5-6
Probed Sentinel 5-9
Site Collector Frames 5-4
Flight Recorders 5-4
Extended Services Platform (ESP) 5-5
Sentinel Server Frames 5-5

Sentinel

Sentinel™ is a complete network monitoring and diagnostic system that gives service providers total visibility of and access to their Signaling System 7 (SS7) and Internet protocol (IP) networks.This section describes Sentinel hardware products from Sentinel Release 8.1 and later. Sentinel products use some commercial off-the-shelf components and Tekelec proprietary products configured in heavy-duty frames.

Some of the hardware server components are based upon the Tekelec 1000 Applications Server (Tekelec 1000 APS) introduced with Sentinel Release 11.x. For information on Sentinel components that are based on the Tekelec 1000 platform, including assembly drawings, interconnect diagrams, and installation instructions, see the *Tekelec 1000 Applications Server Hardware Manual*.

A Sentinel system is comprised of two major system components: distributed site collectors located at remote sites and centralized servers located at the Network Operations Center (NOC). Site collectors are for remote deployments within a carrier's switching offices. For a probe-based configuration, one or more Probe and server systems are deployed at remote sites as site collectors. For the probe-less (Integrated) configuration, EAGLE STP and the ESP servers are the site collectors. Typically, Sentinel includes a Base System Server, Alarm Server and optional Traffic Database Server as well as one or more Data Gateway Servers in the NOC. User workstations are typically located either in the NOC or in a Technical Assistance Center (TAC). The Site Collectors are connected to the NOC via the customer WAN.

The Sentinel system can simultaneously support both probe-based and probe-less configurations. In a combined probe-based and probe-less configuration, the same NOC can be used to simultaneously monitor MSU data sent by an EAGLE STP or via the probes as shown in the Figure 5-1 on page 5-2.

Figure 5-1. NOC in a Combined Probe-based and probe-less Configuration

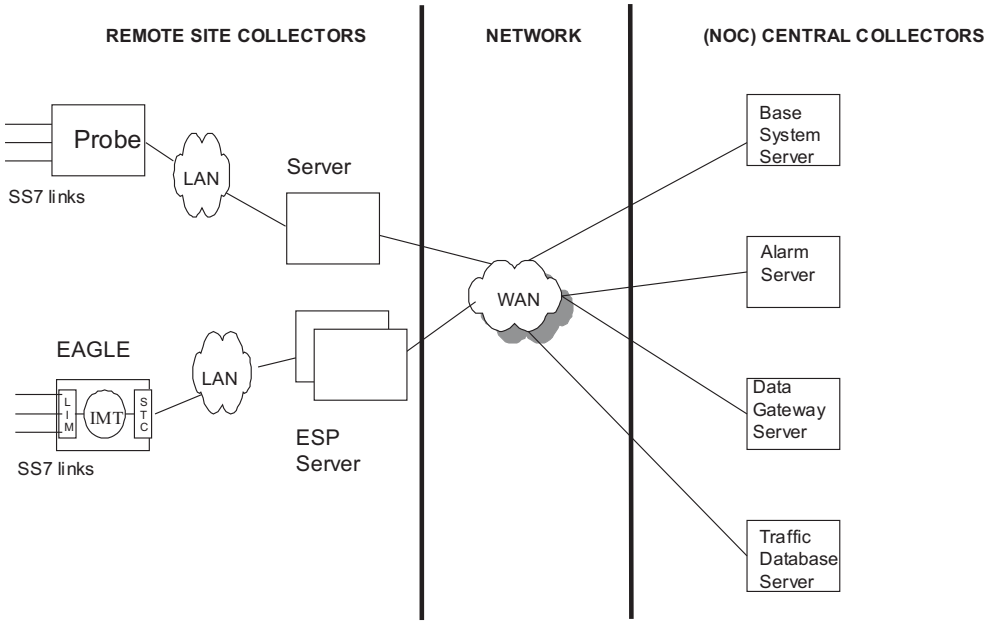
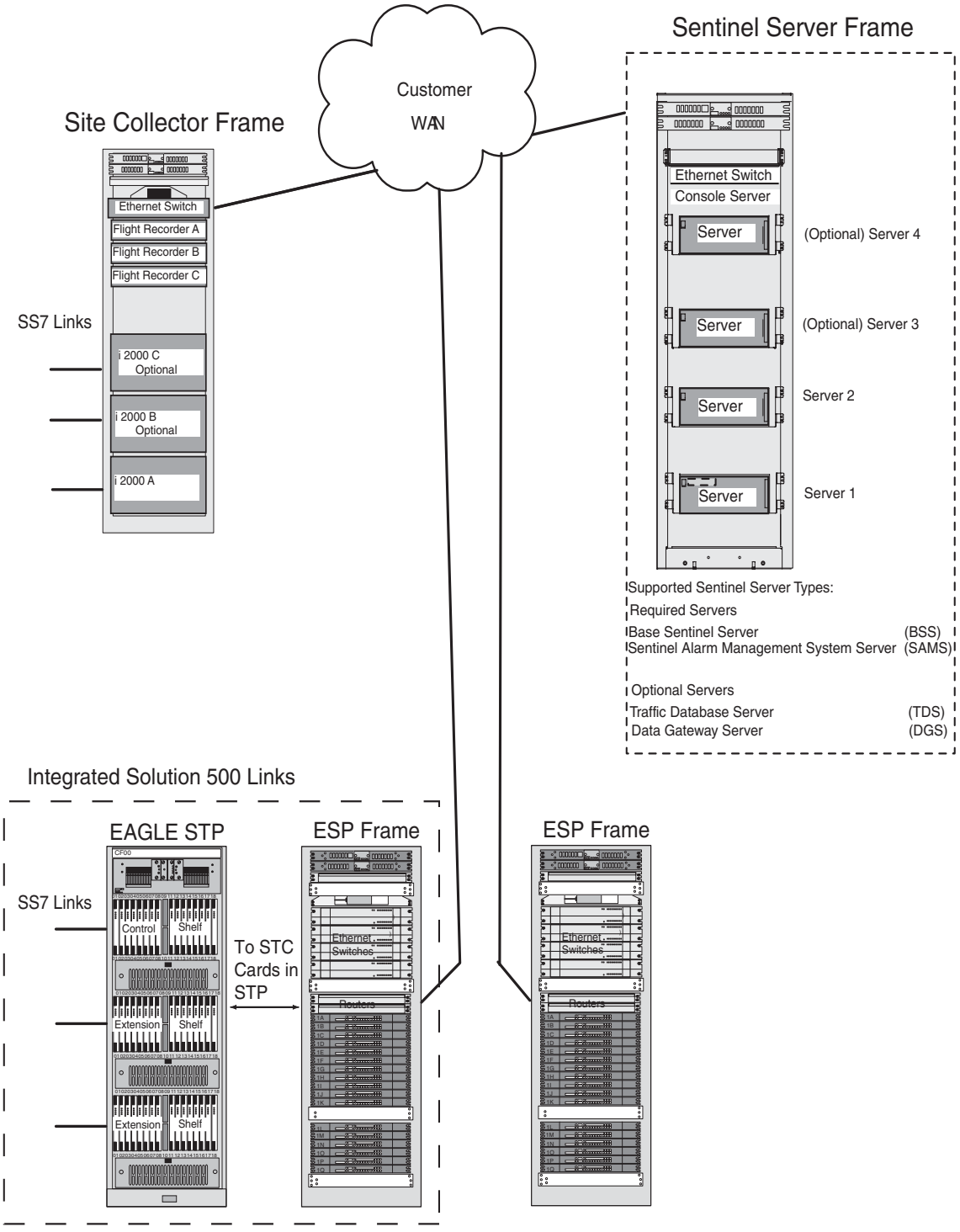


Figure 5-2 on page 5-3 shows the major components of a Sentinel system.

Figure 5-2. Sentinel Components



Sentinel Frames Overview

Both the integrated and probed Sentinel products use some commercial off-the-shelf components and Tekelec proprietary products configured in heavy-duty frames. Sentinel frames typically are configured with dual breaker panels and are cabled with redundant power busses for reliability. Sentinel products support application specific services that monitor SS7 network links.

Sentinel systems are mounted in standard seven-foot high, 23-inch wide frames. For information on unpacking and installation of Sentinel frames see the *Installation Manual* included in this documentation set. Sentinel systems use the following Frames:

- Site Collector
- Flight Recorder
- Extended Services Platform
- Sentinel Server

Site Collector Frames

All Sentinel site collectors consist of the following three basic functional components:

- Data Acquisition - External probe-based connections to SS7 links using monitoring shelves (probed solution) or internal connections to the Eagle (integrated solution).
- LAN Transport - Connects all components of a Sentinel site collector, routers, ethernet switches, hubs, and servers.
- Processing and Storage - Site collector servers process monitored SS7 link information and call detail record (CDR) data, storing data and forwarding to Base Sentinel Servers.

Flight Recorders

The Tekelec's Flight Recorder (FR) is responsible for maintaining a history buffer of MSUs that can be forwarded to the Base Sentinel Server for historical call trace. It prepares MSUs and forwards them to the Data Gateway Server for use in various data collection applications. It is a multiprocessor-based probe used to monitor TALI links carrying SS7 traffic. The flight recorder transmits MSUs to the Base Sentinel Server for real-time link monitoring, PA, and call trace.

An FR connects to a Tekelec i2000 shelf to provide processing and storage for a probed Sentinel solution. Flight Recorders are not used in the Integrated Sentinel. The FR functions are similar to the Integrated Sentinel Extended Services Platform (ESP) server described in the following section.

Extended Services Platform (ESP)

The ESP is also a Sentinel site collector server that can work in conjunction with the EAGLE. ESPs are responsible for receiving MSUs directly from an EAGLE STP. The ESP prepares MSUs for transmission to the Base Sentinel Server for protocol analysis, link monitoring, and call trace functions. ESPs are also responsible for maintaining traffic statistics and forwarding those statistics to the traffic subsystem on the Base Sentinel Server.

Sentinel Server Frames

Both the integrated and probed Sentinel systems use Sentinel Server frames for processing of message link information. The Sentinel server frames described in this manual operate in conjunction with Sentinel site collector systems. Sentinel Server Frames are generic server frames, located at a central location, for example a Network Operations Center (NOC), and have servers configured to operate as the following Sentinel server types for specific system functions.

- Base Sentinel Server (BSS)

  Responsible for administrative provisioning of all other network elements within the Sentinel system; responsible for running the links monitoring, call trace, and protocol analysis applications.

- Data Gateway Server (DGS)

  Responsible for receiving message signal units (MSUs) from ESPs and flight recorders; for creating Call Detail Records (CDRs), Transaction Detail Records (TDRs), and Usage Measurment Data Feeds from the MSUs; for running the optional loop detection and mass call detection applications; and for delivering data feeds to back-office applications running on application servers.

- Sentinel Alarm Management Server (SAMS)

  Provides an extensive alarms management package to collect system-wide Sentinel alarms information and make it available to alarms C\clients. It includesa topology application as well as an alarm browser.

- Traffic Database Server (TDS)

  Provides user the option to use any SQL (Structured Query Language)-based interface (Oracle Forms, Crystal Reports, etc.) to access the traffic pegs stored in a database and generate customized reports.

The following sections describe how these frames work together with the EAGLE in a network.

Integrated Sentinel

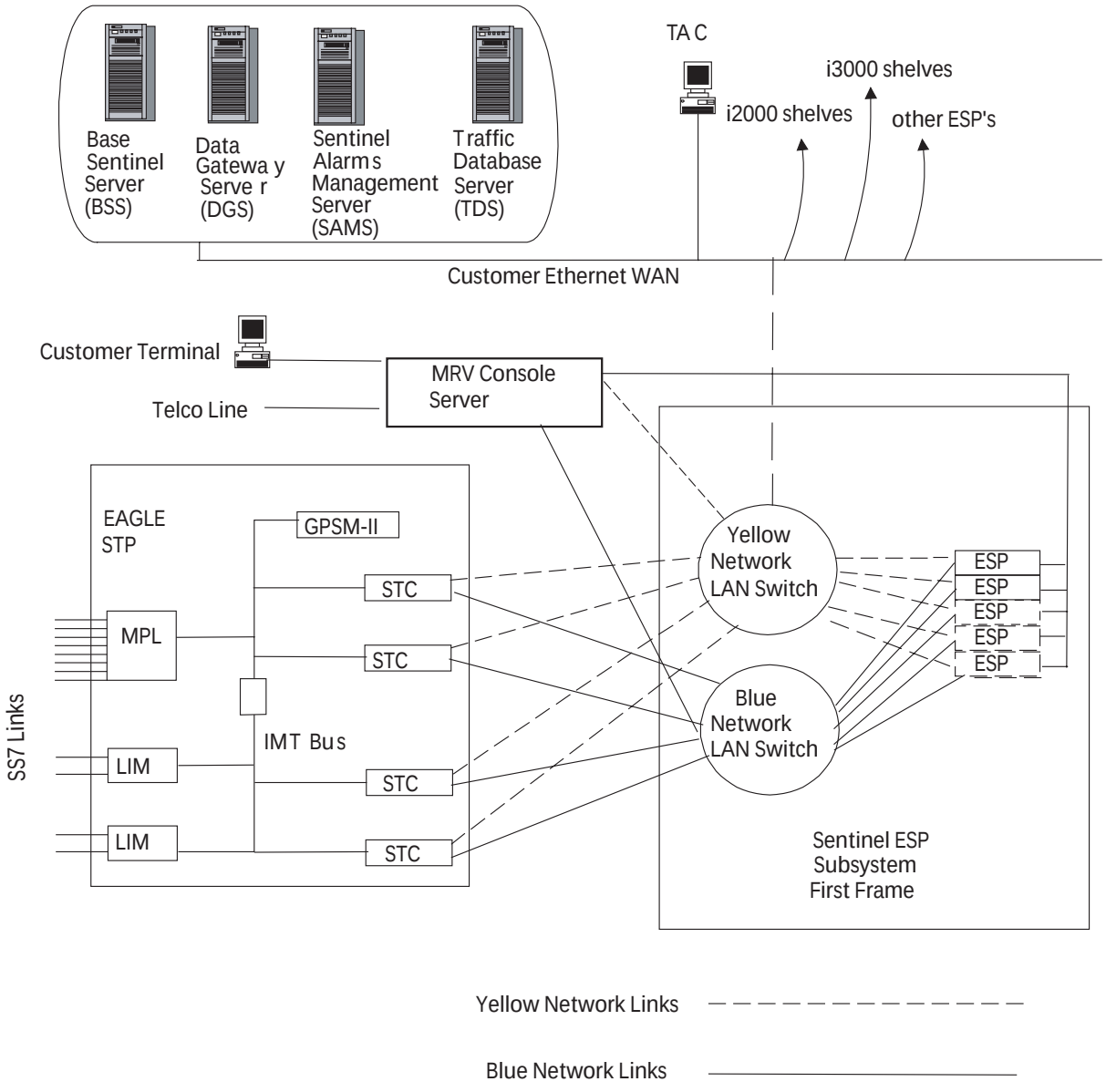
The Integrated Sentinel product includes network surveillance capabilities and fault-management functions. Integrated Sentinel features a call detail record (CDR) generation system that uses raw network traffic on the links to generate CDR data for use in various business intelligence applications.

The Integrated Sentinel monitors EAGLE STP links internally to eliminate hardware connections such as cabling, bridge amplifiers, and patch panels. The Integrated Sentinel can receive all acknowledged message signal units (MSU) as well as other important information from the Eagle. The Eagle monitors SS7 links at the LIM, and connects to ESP LAN interfaces using the dual-port Sentinel Transport Card (STC). The STC card acts as a router to route TCP/IP traffic from Eagle ports to ESP servers.

In Integrated Sentinel, site collector processing and storage tasks are hosted on ESP servers, providing all of the relevant site collector functions for data processing and storage of collected SS7 data. Integrated Sentinel ESP servers are connected to an associated Eagle using redundant LAN interfaces. The internal local area network (LAN) traffic is isolated to keep monitored data separate from the customer's wide area network (WAN).

Figure 5-3 shows a block diagram of a SS7 monitoring network incorporating the Integrated Sentinel.

Figure 5-3. Integrated Sentinel Block Diagram



Integrated Sentinel with Eagle

To implement the Integrated Sentinel solution on with the EAGLE STP, the following hardware and software is required:

- Installation of HMUX or HIPR cards in all shelves
- Activation of HMUX Group Ticket Voucher (TVG)
- Upgrade to Sentinel release 8.1 and EAGLE Release 28.2 or later
- GPSM-II cards in OAM slots (1113 and 1115) of the control shelf
- Installation of two TDM boards (P/N 870-0774-10 and later)
- Installation of Sentinel Transport Cards (STC) in the EAGLE STP
- Activation of the Time Slot Counter (TSC) Synchronization feature
- Activation of the Integrated Sentinel feature
- Activation of the MSU copy feature

Sentinel Transport Cards

The STC functions as an IP router between the IMT bus internal to the EAGLE and the ethernet networks used to communicate with the ESP servers.

Time-Slot Counter Synchronization

Time Slot Counter (TSC) Synchronization is an option for the EAGLE that will allow all cards in the system that contain a Time Slot Counter to synchronize with one another. The ability to have synchronized timing between cards is used in applications such as system wide message time stamping.

Integrated Sentinel ESP

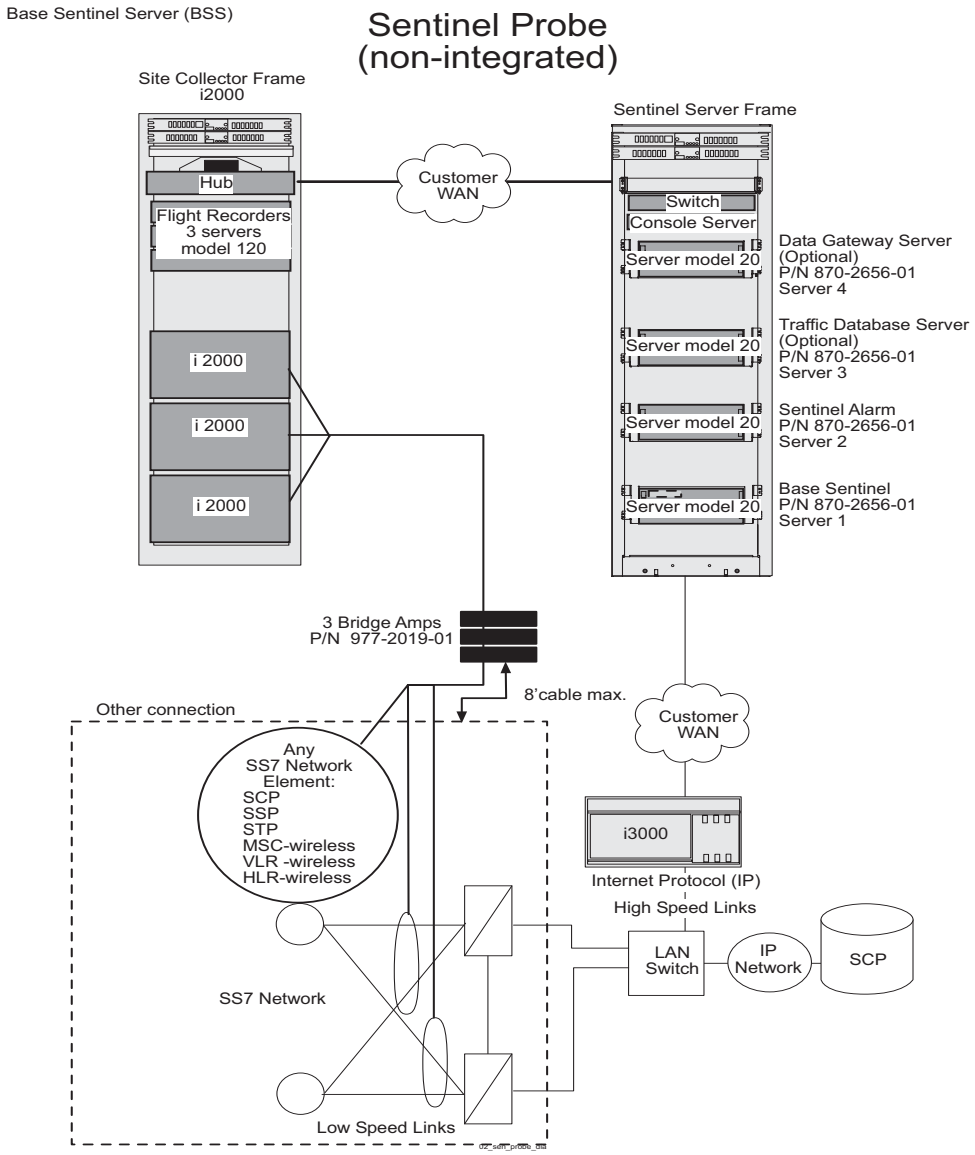
The Extended Services Platform (ESP) is the Integrated Sentinel software bundle and the required software platform that provides the interface from the EAGLE STP to the Integrated Sentinel monitoring system. All ESP servers located at one EAGLE location are an ESP subsystem.Each ESP server is considered a separate processing element with respect to communications to the downstream Sentinel servers and therefore needs its own IP address. As shown in Figure 5-3 on page 5-7, a single demarcation point is provided for the Customer's network at the ESP frame's ethernet switch.

The Integrated Sentinel ESP subsystem interfaces to the monitored links in the EAGLE through ethernet connections to the Sentinel Transport Cards (STC) located in the EAGLE frame. In the Eagle the information being copied from LIM cards and sent to the ESP subassembly is transported by TCP/IP using a custom proprietary protocol called EAGLE Monitor Protocol (EMP).

Probed Sentinel

The Probed Sentinel product provides external monitoring of SS7 links without direct connection to an EAGLE. In the probed Sentinel, SS7 traffic is processed by a series of processes collectively referred to as a Sentinel Site Collector. A Sentinel Site Collector System consists of user workstations, the Eagle Shelves, Signaling Transfer Points (STPs) or other SS7 Network Equipment and a Site Collector Frame. Figure 5-4 shows the components of the probed Sentinel.

Figure 5-4. probed Sentinel



Site Collector is a collective term for either ESPs or Flight Recorders (FR) that collect MSUs and forward them on to the Sentinel Server system for processing. FRs are connected to mated i2000 shelves in the Sentinel Site Collector Frame. Sentinel i2000 shelves are connected by probes to the SS7 links that are monitored.

The Flight Recorder (FR) refers to a subsystem composed of hardware and software components that comprise the platform for a particular Sentinel site collector. The FR platform functions very similar to the ESP platform used in the integrated solution for a Sentinel site.

NOTE: A Sentinel Site Collector Frame can be ordered without i2000 shelves to inter-connect with existing Sentinel systems.

Probed Sentinel Server Frame

The Sentinel Server Frame is configured with one to four Sun Netra servers to support Data Gateway servers (DGS), Traffic Database servers (TDS), Sentinel Alarm Management System (SAMS) servers or Base Sentinel servers (BSS).

6

MPS

Introduction 6-1

MPS System Hardware 6-2

MPS on Tekelec 1000 6-2

MPS on Netra Platform 6-9

Introduction

Tekelec's Multi-purpose Server (MPS) is a hardware and software platform that can be configured as an EAGLE Local Number Portability (LNP) Application Processor (ELAP) or EAGLE Provisioning Application Processor (EPAP) server.

The MPS provides an interface between the customer provisioning network and the Eagle DSM cards. As the customer's data is updated, the MPS stores the data and updates the DSM cards. An MPS is usually co-located with an Eagle. If you need to install an MPS at a distance from the EAGLE, contact "Tekelec Technical Services" for assistance.

Currently, the MPS supports the following features:

- MPS running the EAGLE Provisioning Application Processor (EPAP) software supports the GSM Flexible Numbering (G-Flex), GSM Mobile Number Portability (G-Port), and INAP-based Number Portability (INP) features.

  These features allow a subscriber to change location, service provider, or service while keeping the same directory number and ensures that subscribers receive the same freedom of choice for local service as they do with long-distance service providers.

- MPS running the EAGLE LNP Application Processor (ELAP) software supports the LNP 96 Million Numbers Feature.

  The Local Number Portability (LNP) 96 Million Numbers feature increases the number of provisionable telephone numbers (TNs) from 18 million to 48 million. The LNP 96 Million Numbers feature also relocates the LNP database from the OAM (Operation Administration and Maintenance) to the MPS.

  The MPS is composed of hardware and software components that interact to create a secure and reliable system. This chapter includes an overview of the MPS hardware platform and a description of MPS hardware components.

MPS System Hardware

The MPS is based on Tekelec's Tekelec 1000. Earlier deployments of MPS are based on Netra servers.

Tekelec 1000-based MPS is required for the LNP application EPAP 4.0. Tekelec 1000-based MPS configuration are comprised of:

- 2 breaker panels
- 4 hubs
- 2 Tekelec 1000 processing systems.

The Netra-based MPS is comprised of:

- 2 breaker panels
- 4 hubs
- 2 Sun Microsystems Netra t 1400 processing systems.

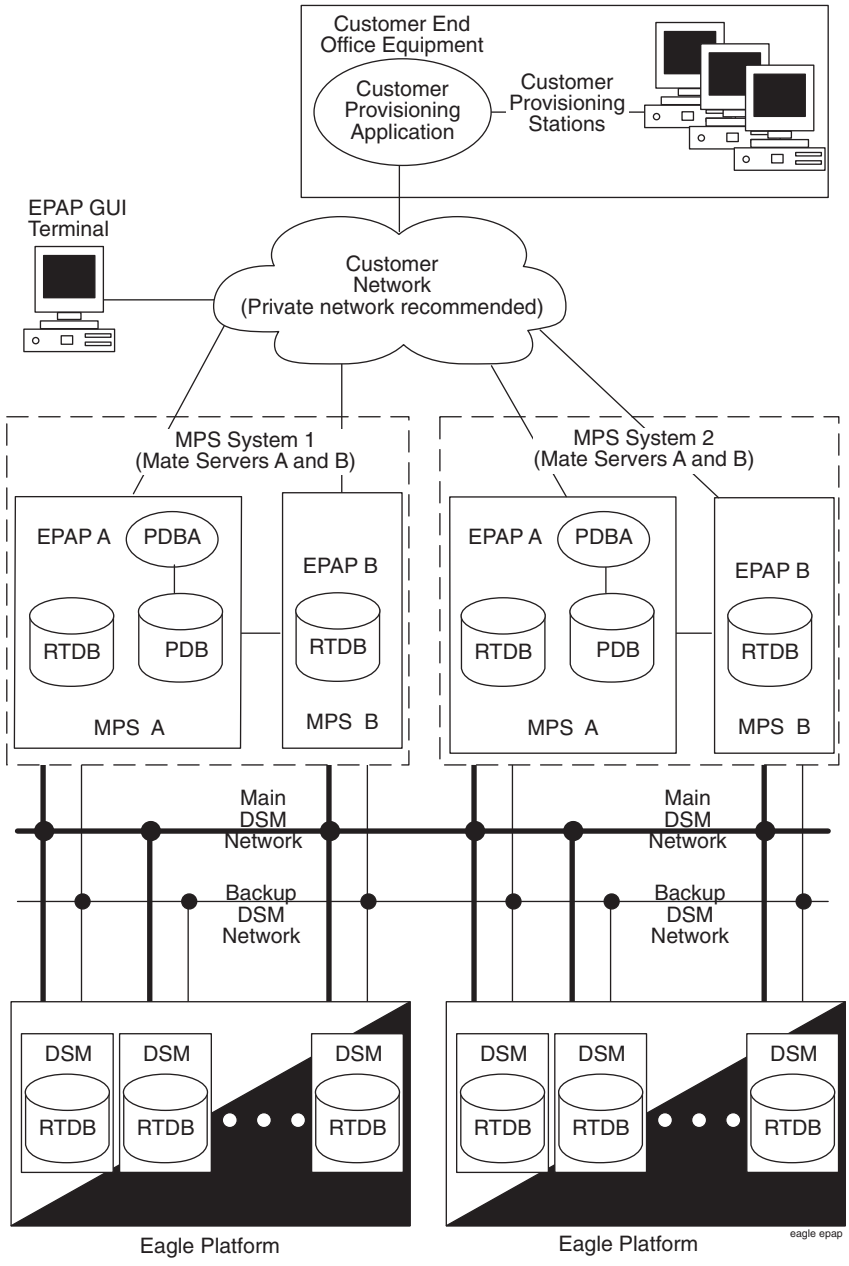
MPS on Tekelec 1000

MPS on Tekelec 1000 supports the EAGLE Provisioning Application Processor (EPAP) The EPAP application includes the INP, G-Flex, and G-Port® features. In addition to the software application, additional third-party software might be required to support the software application.

Figure 6-1 on page 6-3 shows an overview of how the MPS on Tekelec 1000 is used with the EAGLE system.

This section provides an overview of the hardware and platform software that comprises the MPS on Tekelec 1000. For information about the EPAP application and how it interacts with the EAGLE, refer to the *EPAP Administration Manual*.

Figure 6-1. MPS on Tekelec 1000/EAGLE Overview



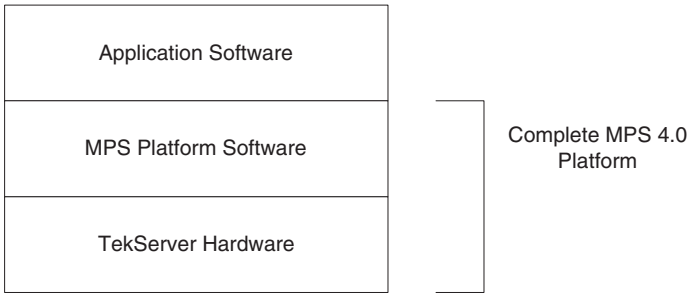
Layered Design

MPS Release 4.0 is based on the Tekelec 1000 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 need not cause changes in application.

Figure 6-1 on page 6-4 shows the layered design of the MPS and the application it supports.

Figure 6-1. Layered Design for MPS and Applications

MPS System Hardware Configuration



Each MPS system requires the hardware shown in Table 6-1.

Table 6-1. Tekelec 1000 Main Unit

Qty	Hardware Item
2	Tekelec 1000 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 Each Tekelec 1000 main unit has 2 gigabytes of Random Access Memory (RAM) installed and available.
4	Ethernet hubs: • Two for main DSM network • Two for backup DSM network
2	Breaker panels
1	Power distribution panel (also called terminal block or terminal strip)
2	PCI modem card located in MPS servers A and B

Figure 6-2 on page 6-5 shows the MPS hardware configuration in a frame and a magnified view of the Tekelec 1000 main unit.

Figure 6-2. MPS Hardware Configuration in Frame

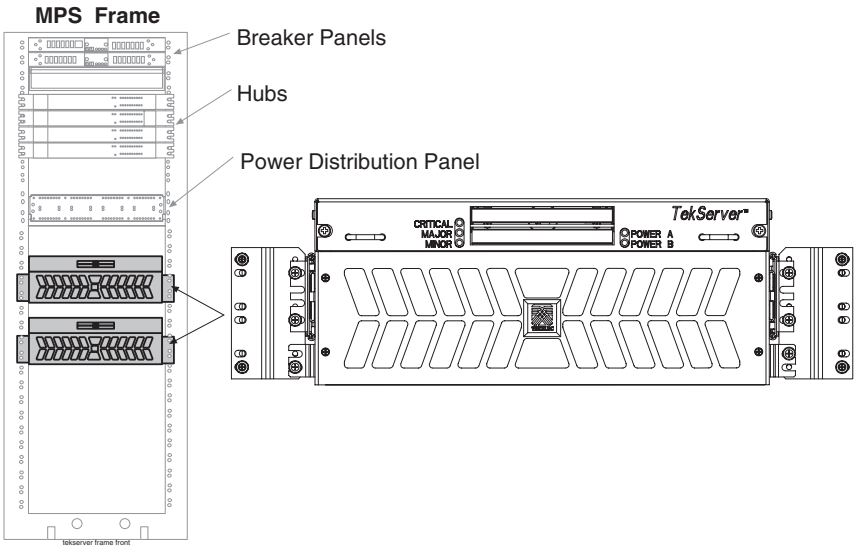
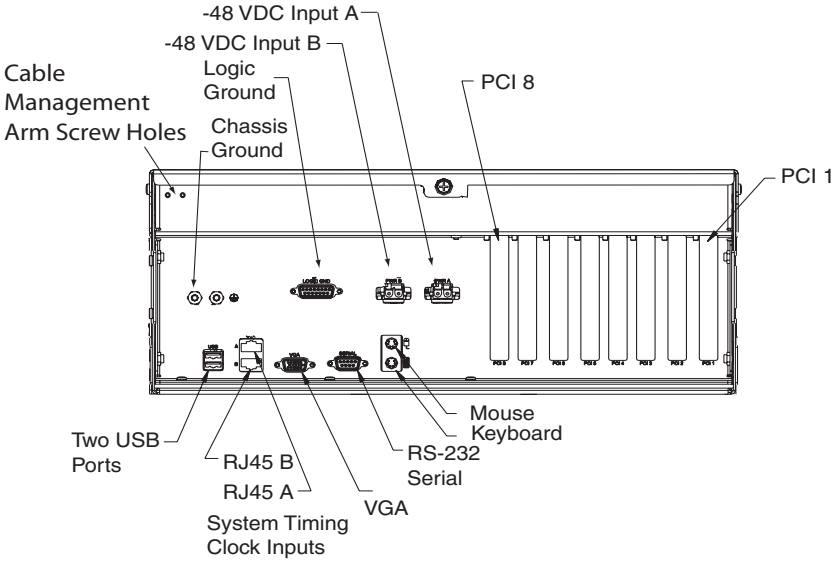


Figure 6-2. Rear View of Tekelec 1000



For more detailed information about the main unit, refer to the *Tekelec 1000 Applications Server Hardware Manual*.

MPS Platform Software Configuration

MPS Release 4.0 platform software is packaged and distributed as a Tekelec Platform Distribution (TPD).

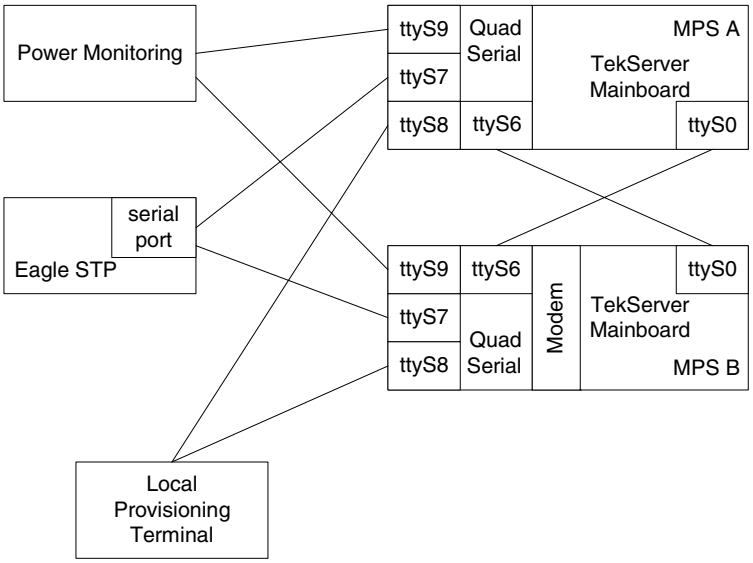
The MPS platform uses an optimized kernel which supports:

- 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 on Tekelec 1000 provides the serial communication interfaces shown in Figure 6-3 on page 6-6:

Figure 6-3. MPS Serial Port Connections



Remote Access

The MPS on Tekelec 1000 system provides the following remote access features.

- Five Ethernet interfaces are provided; each interface can support 10 megabits per second (Mbps), 100 Mbps, or 1 gigabit per second (Gbps).
- A web server provides hypertext transfer protocol (HTTP) access over both Ethernet and PPP.

- The MPS does not support incoming connections that use services such as **`rlogin`**, **`rsh`**, **`rexec`**, **`ftp`**, and **`telnet`**. Any incoming connections using these services are dropped. Instead, the MPS supports secure protocols that provide similar features.
- A dial-in modem, installed in PCI slot 7 on MPS B, provides access for both Microsoft® Windows® and Linux® clients using the Point to Point Protocol (PPP). The modem is for use only by Tekelec Technical Services.

Diagnostics, Monitoring, and Alarming

The MPS on Tekelec 1000 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's core components
  - — Whether core processes that should be running are running
  - — Virtual Memory (VM) subsystem
  - — Temperature
- Alarms, in the form of Light-Emitting Diodes (LEDs) or messages, to report problems found by monitoring

MPS System Network Configuration

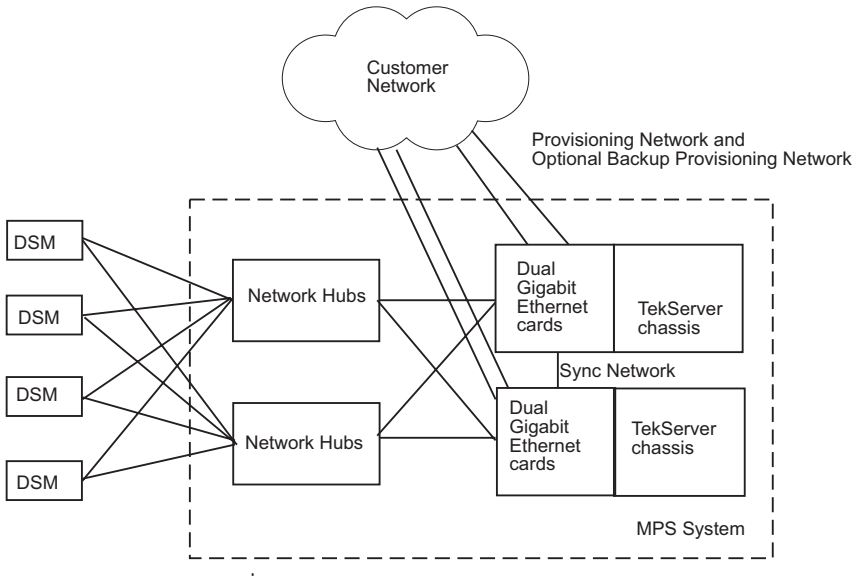
The following sections describe the MPS system network configuration.

Network Interfaces

Each MPS server has three added dual-port gigabit Ethernet PCI cards to support network interfaces. The MPS software configures the Ethernet interfaces and modifies files to make the network interfaces available to the EPAP application.

Figure 6-4 shows the network connections for an MPS system.

Figure 6-4. MPS on Tekelec 1000 Network Connections

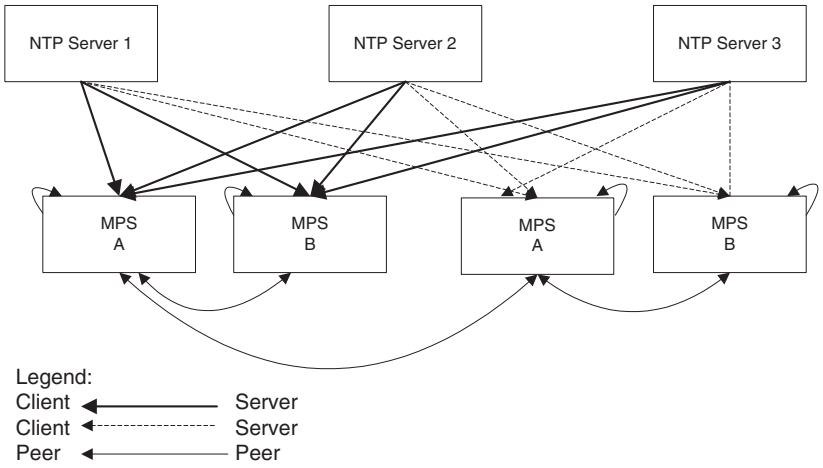


Network Time Protocol (Core)

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 Tekelec 1000 will drift out of synchronization with other equipment that it communicates with.

All Tekelec 1000 servers can optionally be configured to communicate with customer-defined NTP timeservers. Tekelec 1000 servers at a given site will also be configured to communicate with each other, so they will stay synchronized even if contact to other NTP servers within the customer network is lost.

Figure 6-5. MPS NTP Configuration



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

MPS on Netra Platform

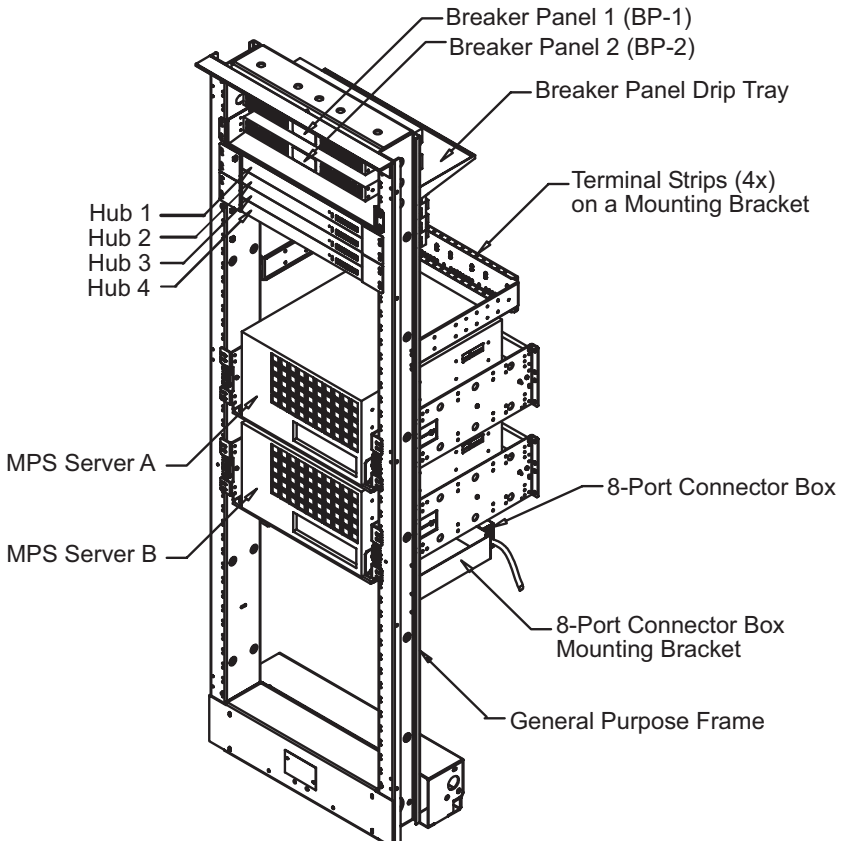
The following section provides overview information and describes the parts of the Netra-based MPS.

The MPS Server is a one- to four-processor device that uses the family of UltraSPARC™ II processors. Housed within a rack-mounting enclosure, the MPS Server provides the following:

- High performance processors
- Extensive I/O expansion and a wide range of options
- Modular internal design
- High performance disk, system, memory, and I/O subsystems
- High performance peripheral component interconnect (PCI) I/O
- Redundant hot swap power supply units
- Alarm function for remote management
- Powered by –48V DC supplies

The following sections provide a brief description of the MPS Server I/O devices and a detailed overview of the system features.

Figure 6-3. MPS on Netra Hardware Overview



MPS on Netra System Features

System components are housed in a rack-mounting enclosure. The motherboard contains the CPU module(s), memory, system control application-specific integrated circuits (ASICs), and I/O ASICs.

The system has these additional features:

- Rack mounting enclosure with n+1 redundant, hot-swap –48VDC power supplies
- UltraSPARC Port Architecture (UPA) coherent memory interconnect
- Use of Dual Inline Memory Module (DIMMs), with an interleaved memory system. Populating with two pairs of identical capacity DIMMs enables the memory controller to interleave and overlap, providing optimal system performance. There are a total of 16 DIMM slots supplying

a minimum of 256 MB (4 x 64 MB) and a maximum of 4 GB (16 x 256 KB) of memory.

- 40 Mbps Fast-20 (UltraSCSI) disk subsystem supporting up to four 18 GB disk drives
- Two RS232/423 DB-25 serial ports (asynchronous protocols)
- Parallel port
- External Fast-20 (UltraSCSI) 68-pin port
- Two SCSI removable media drives (CD-ROM or DVD-ROM, and Tape Drive)
- Alarm card

  The alarm card has a non-volatile buffer to record recent events, monitors internal hardware devices, and controls the front panel alarm, fault, and system LEDs.
- Quad FastEthernet Network Interface Card
- Serial Asynchronous Interface/PCI adapter (SunSAI/P card with 8-Port Connector Box) on Server B only

7

Tekelec 1000 Applications Server (APS)

Introduction 7-1

Tekelec 1000 Hardware Features 7-1

- Hardware Components 7-2
- Interfaces 7-3
- Electrical Features 7-3
- Mechanical Design 7-3
- Alarm and Status Indicators 7-6

Introduction

The Tekelec 1000 Applications Server (APS) provides a fully integrated application-hosting environment directly on top of the EAGLE platform. The Tekelec 1000 is a general-purpose application engine (AE) that offers high transaction rates with low latency. It supports a variety of application solutions for the wireless and wireline telecommunications infrastructure to provide the building blocks for next-generation signaling systems. The Tekelec 1000 software is comprised of a POSIX compliant, Open System Environment.The Tekelec 1000 supports a full suite of applications known as TekWare. Also, the Tekelec 1000 is used to host the MPS, and Sentinel ESPs and Traffic Database Servers.

Tekelec 1000 Hardware Features

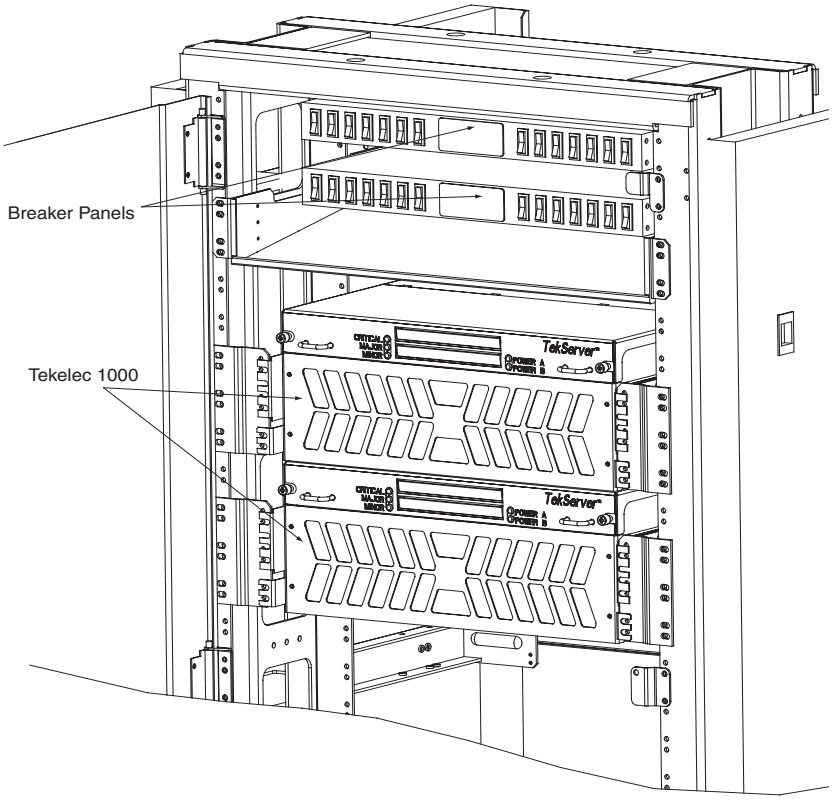
The TekServer Services Platform is a scalable computing platform constructed with state-of-the-art components packaged in a compact-size, stand-alone enclosure. The TekServer chassis utilizes dual processors, and has eight PCI slots, four internally mounted media devices, and expandable memory.

NOTE: Tekelec 1000 servers are normally configured in an (n+1) configuration to achieve 99.999% availability. Some applications may not require the redundant configuration.

Figure 7-1 on page 7-2 shows a Tekelec 1000 configured in a Tekelec heavy-duty frame.

NOTE: The Tekelec 1000 shown in Figure 7-1 on page 7-2 is at the top of the frame; this is the typical position when the Tekelec 1000 is part of a new installation at the customer location. The Tekelec 1000 can also be located at other positions in the frame.

Figure 7-1. Tekelec 1000 in Tekelec Heavy-Duty Frame



Hardware Components

The TekServer platform offers the following standard hardware components:

- Intel® E7501 chipset
- Dual Intel Pentium® 4 Xeon™ processors
- Redundant BIOS architecture
- 266-MHz DDR RAM, registered, with ECC and Chipkill™ support
- 533 megahertz (MHz) processor bus speed

- Light Emitting Diode (LED) diagnostic display
- Battery-backed real-time clock
- Hardware monitors that read and report:
  - — Supply, battery, and core voltages
  - — Fan speed inputs
  - — Ambient and processor temperatures
- E1/T1 composite clock signals
- Four devices for storage media (for example, fixed media disk drives and CD-RW/DVD ROMs) for internally supporting persistent storage

In addition, the TekServer platform has a variety of internal and external interfaces, as described in "Interfaces" on page 7-3.

Interfaces

The TekServer platform includes interfaces for accommodating expansion, control and configuration, network connectivity, and peripheral support. See the *Tekelec 1000 Applications Server Hardware Manual* for details.

Electrical Features

The TekServer platform offers the following standard electrical features:

- Operates from -48 VDC +/- 5% power input according to Network Equipment Building System (NEBS) requirements in accordance with typical telecommunications applications
- Includes short-circuit protections and safety precautions in accordance with common standards

Mechanical Design

The TekServer mechanical design meets all applicable NEBS requirements and is designed to protect all of the active components. The design has efficient component cooling using low-impedance air paths, and its compact size allows multiple units to be configured in a frame with zero top and bottom clearance when stacked.

The TekServer hardware has been designed for easy maintenance. The following components are field-replaceable units (FRUs):

- Fans
- Fan filters
- Disk drives (located on the removable lid)

- Peripheral Component Interconnect (PCI) cards
- Complete Tekelec 1000 Chassis

The fans, filters, and disk drives have lower mean time between failures (MTBF) and can be easily replaced, so they have been grouped together. The disk drives are located in the removable lid (for more information, see "Component Access Front Lid" on page 7-4). The PCI cards are located at the rear of the Tekelec 1000 chassis and plug into the main board.

All other components, which are less likely to fail and are more difficult to replace, are located in the TekServer main unit. If one of the components in the main unit fails, you can remove the disks (preserving your data which is stored on the disk drives in the lid), replace the entire main unit, and then install the disk drives in the replacement chassis.

Use the procedures in the *Tekelec 1000 Applications Server Hardware Manual* when removing or replacing FRUs. Always perform a soft shutdown of the Tekelec 1000 chassis before switching OFF both circuit breakers supplying redundant power. For more information about troubleshooting systems and performing soft shutdowns see the appropriate maintenance manual for your application.

Component Access Front Lid

The TekServer platform has a hinged lid at the front that is locked in place by captive screws during normal operation. This lid allows access to the fan trays, BIOS select switch, reset button, and two USB ports that are located under the lid. The front lid also has the following features:

- Light emitting diode (LED) alarm indicators, mounted to the front surface of the lid.
- Space for routing and strain relief of cables to the media device, LED's, and fan trays.
- Constant torque hinges, which are a safety feature to protect the attached components from shock by preventing sudden closure of the lid.
- The following devices, mounted to the bottom side:
  - — Two 3.5 disk drives (HDD) mounted separately. Each HDD is mounted to a bracket. This assembly is then mounted to the front lid.
  - — Two slimline drives (for removable media devices) and drive adapter board, mounted together with a dual CD-RW/DVD ROM bracket. These assemblies are then mounted to the front lid.

Rear I/O Panel

The rear input/output (I/O) panel is perforated to facilitate airflow and forms the back wall of the TekServer enclosure. It has openings for:

- Eight peripheral component interface (PCI) cards' I/O panels

- The I/O connectors on the rear edge of the main board (mouse, keyboard, VGA, serial port, E1 or T1 clock inputs, and two USB ports)
- The power board I/O (logic ground connection)

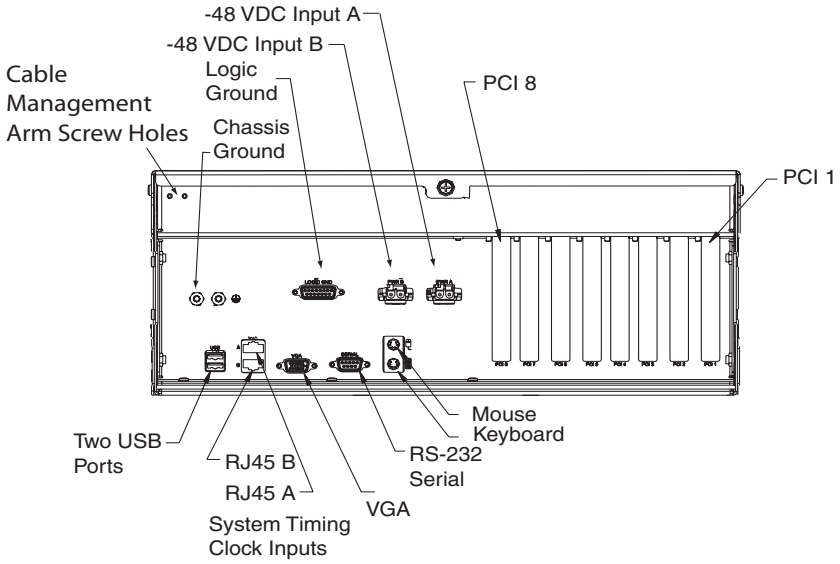
Power entry is at the rear of the TekServer platform. There are two right angle power connectors (A and B feeds) on the power board that are accessible through the rear I/O panel. The power input connectors are keyed and have positive locking features.

Logic ground is carried on a 15-position, right-angle connector on the power board. The connector is bulkhead-mounted to the rear I/O panel. There are also two frame ground connector studs on the rear I/O panel. See Figure 7-2 on page 7-5 for a detailed view of the rear I/O panel.

NOTE: The rear I/O panel is shown without the perforated air panel for clarity.

Figure 7-2. Rear I/O Panel

TekServer Main Board



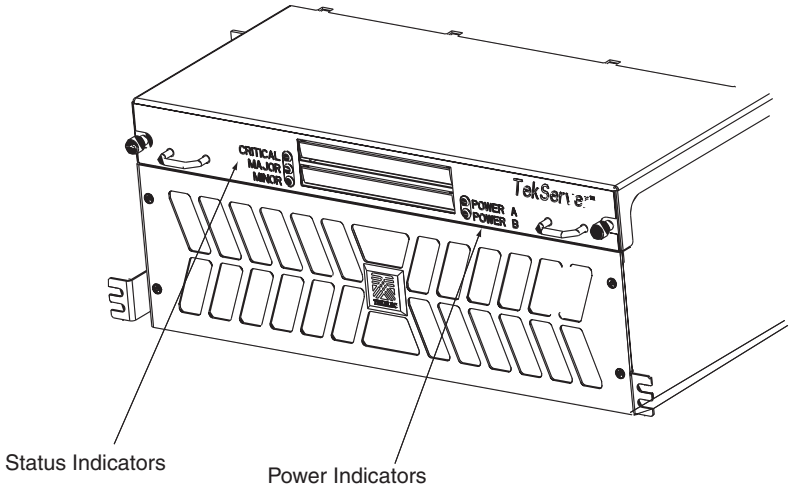
The main board has eight PCI card slots. PCI cards are plugged directly into the main board, and the PCI cards bulkhead panels are fixed to the Rear I/O Panel with screws. Slots one through six support full length (12.283 inch) PCI cards, slots seven and eight support cards 6.875 inches long, or less.

Alarm and Status Indicators

The Tekelec 1000 platform provides the following alarm and status indicators:

- Critical, Major, and Minor visual alarm indicators located on the front panel of the TekServer platform.
- Status indicators provide additional information regarding the operational condition of the TekServer platform, including status of the major subsystems: processors, volatile memory, non-volatile memory (disk drives, etc.), and interfaces. Front panel light-emitting diode (LED) indicators for primary and secondary power inputs are provided.

Figure 7-3. Tekelec 1000 Status Indicators



For more information about the diagnostics that manage these alarm and status indicators, see the *Tekelec 1000 Applications Server Hardware Manual*.

Installation and Replacement

The Tekelec 1000 chassis is field installable in a Tekelec Heavy Duty Frame. The slides are constructed such that the telescoping portion can be installed in the frame and the inner slide rail can be attached to the TekServer chassis. The TekServer chassis can then be loaded into the frame without having to support it while installing hardware.

The TekServer chassis is also field replaceable. TekServer replacement, including disconnecting cables, mounting a replacement system (of identical configuration), and reconnecting cables requires no more than 30 minutes. See the *Tekelec 1000 Applications Server Hardware Manual* for installation and replacement procedures.

Diagnostics

All components that comprise the TekServer platform are designed for testability to ensure that operational status can be accurately determined and that appropriate levels of fault detection and isolation are possible with a minimum of effort.

The following levels of diagnostics are provided:

1. Power-On Self Test (POST) diagnostics run once at start-up to determine whether all required devices are installed and functional. POST can also be run by Tekelec Technical Services to verify that the TekServer platform is operational.
2. Online diagnostics actively monitor the health of a running TekServer platform. When online diagnostics encounter a problem, an alarm is raised and front panel light-emitting diodes (LEDs) are illuminated to indicate a problem. Online diagnostics can be run while maintaining in-service operation of node. Individual links undergoing tests will be out-of-service.
3. Offline diagnostics can be used by Tekelec Technical Services to detect system hardware problems that POST cannot detect. Offline diagnostics can also provide load simulation and stress testing

Diagnostics enable troubleshooting of installed systems by verifying:

- Operational capability of Field Replaceable Units (FRU).
- Operational status of peripheral system components (such as cables and connectors) through automated testing initiated by FRU components. Examples are loop-back and Bit Error Rate Test (BERT) tests.

Reliability, Interoperability, and Scalability

Reliability

The primary market for the TekServer platform is traditional telecommunications signaling environments requiring robust performance and 99.999% availability. The TekServer platform is designed to maximize reliability and include redundancy of critical systems (such as the primary power modules and fans) that may detract from reliability expectations

Interoperability

The TekServer platform interoperates with a variety of IP enabled and SS7 compliant devices in accordance with the standard interfaces and protocols supported.

Scalability

The TekServer platform is scalable to provide for price/performance ratios best suited to specific customer applications. Tekelec provides scalability through insertion and/or depopulation of the following components.

- Processors -Two
- RAM - Scalable from 2Gbytes to 16Gbytes in 2Gbyte increments.
- Ethernet components
- Expansion cards
- Bay-mounted devices

Additional E1/T1 interfaces can be configured.

8

EOAP

Overview 8-2

Hardware 8-4

- Shelf 8-4
- Components 8-5
- Components 8-5
- Asynchronous Maintenance Modem (Optional) 8-6
- Asynchronous Maintenance Modem (Optional) 8-6
- Terminal 8-7

Interfaces 8-7

- EOAP-to-Eagle STP 8-8
- EOAP-to-SEAS 8-10

Administration 8-12

- IP7 Secure Gateway Provisioning 8-12

EOAP Retransmission Delay 8-13

- EOAP Retransmission Delay 8-13

Maintenance 8-13
Hardware 8-13
Software 8-14
Upgrade Considerations.....8-14

Overview

The Embedded Operations Support System Application Processor (EOAP) is a general purpose interface module that provides the Eagle STP system with a generic platform to develop and run software for feature-specific interfaces to the Eagle STP. These interfaces, for example, include the optional Signaling and Engineering Administration System (SEAS).

The EOAP translates and converts higher layer protocols into asynchronous serial communication. It communicates with the Eagle STP system through a serial interface port. For the SEAS interface, the EOAP provides translation and asynchronous-to-X.25 communication conversion. For the LSMS interface, the EOAP processes input from the LSMS.

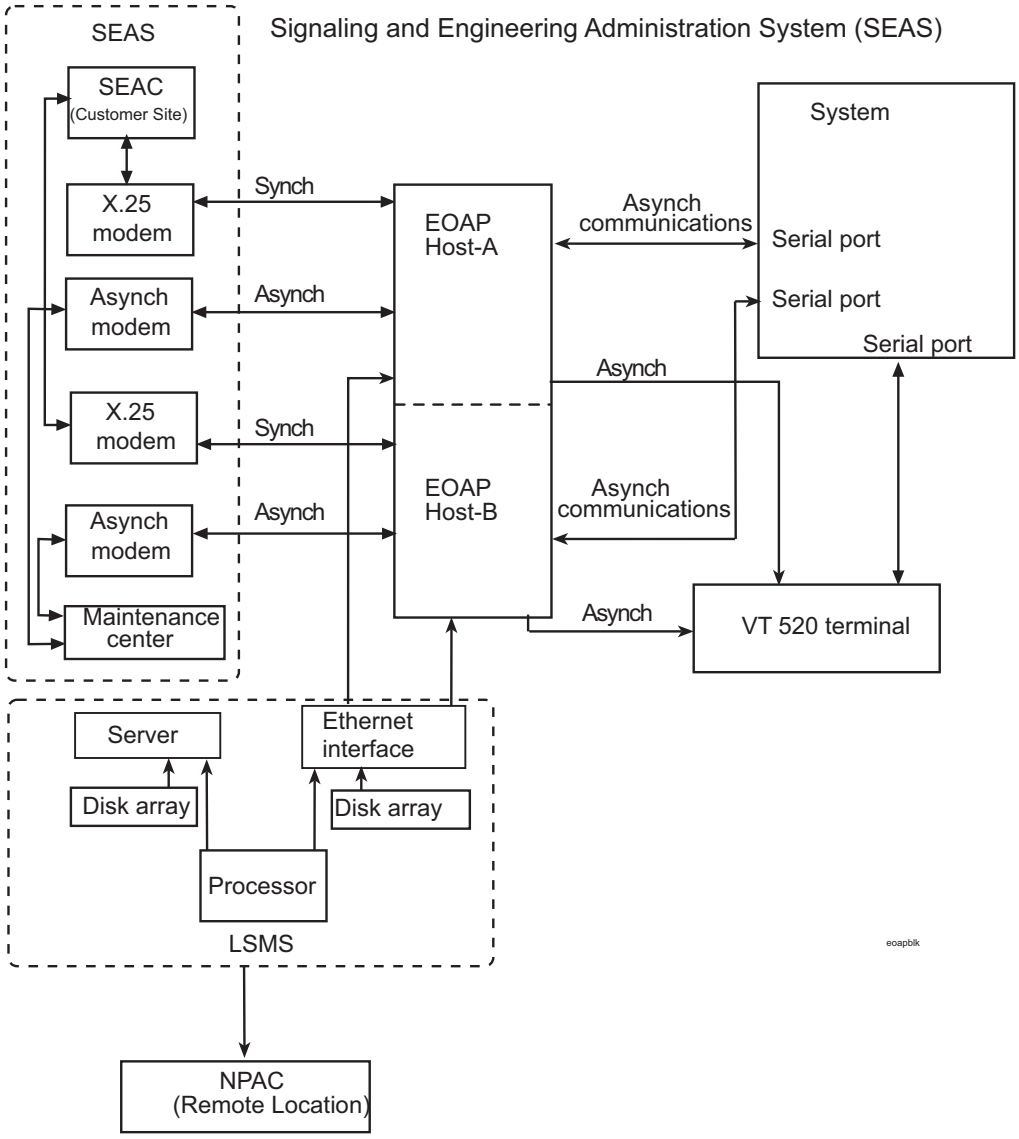
Each EOAP reports to the Eagle STP its general status as well as the status of its User Application Layer (UAL), X.25 links, PVCs on those links, and Q.3 associations. The Eagle STP can then report the status of the EOAP and its components to the user through the Eagle STP's HMI.

You can configure most aspects of the EOAP through the Eagle STP terminal. For upgrade, debug, and maintenance functions, use a VT-520 terminal directly connected to the EOAP.

The EOAP is a modular unit with field-replaceable components. For upgrade purposes, the EOAP can replace an existing Texas Micro OAP.

The EOAP shelf is designed for a split system consisting of an EOAP-A and an EOAP-B. Each EOAP system in the dual configuration consists of a processor card, a serial interface card, a power supply card, a removable hard drive, and a removable CD-ROM drive.

Figure 8-1. EOAP Communication



Hardware

Shelf

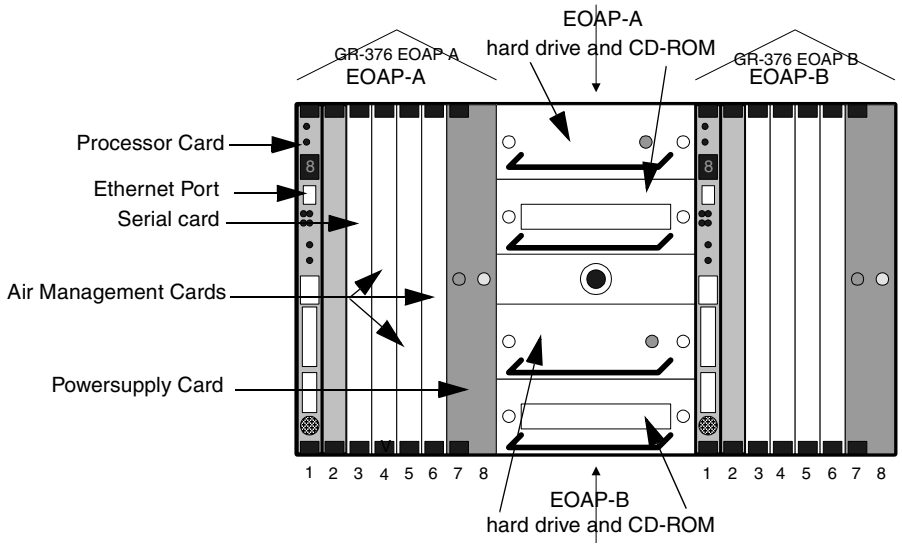
The EOAP shelf is designed for a split system consisting of an EOAP-A and an EOAP-B. Each EOAP in the dual configuration consists of the following components:

- Air management card (P/N 870-1524-01)
- CD-ROM drive card (P/N 870-1515-03)
- Hard drive card (P/N 870-1514-03)
- Power supply card (P/N 870-1521-01)
- Processor card (P/N 870-1523-01)
- Serial card (P/N 870-1522-01)

Figure 8-2 illustrates the layout of the system.

The center section of the dual EOAP system (both EOAP-A and EOAP-B) contains four individual drive bays. The top two drive bays are hard wired to EOAP-A and the bottom two drive bays are hard wired to EOAP-B. The top drive bay for each EOAP is occupied by the hard drive for that unit. The hard drive must be a SCSI II device, set to SCSI ID#0, with a minimum capacity of 9 GB.The factory pre-loaded hard drive is a field replaceable unit. If the hard drive card is replaced, the platform followed by all site-specific information must be reloaded on the EOAP.

Figure 8-2. EOAP Shelf



Components

Processor Card

The processor card occupies slots 1 and 2 of the EOAP. This card is a 300 MHz or faster CompactPCI card with 64 MB on-board RAM (expandable to 1 GB). The processor card is the main computational component of the EOAP system. On the front of the card are system status LEDs (see Table 8-1) and an Ethernet port. The card also provides abort and reset capabilities through both manual and software intervention.

Table 8-1. Status LEDs of the EOAP System

Value	Meaning
0	Normal Operation
1	Halted

The processor card is a field-replaceable unit. It provides two serial ports, which are accessible through the EOAP backplane, for connecting to a VT-520 terminal and an asynchronous maintenance modem. An RJ-45 Ethernet port on the front of the card provides negotiated 10/100BaseT network access for Local Number Portability (LNP) support using the LSMS.

The card provides the following usable front panel fixtures: abort and reset switches, a rotary mode switch, microphone and headphone jacks, a SCSI connector, and a keyboard connector.

Serial port A is used for direct console connection (vt100, PC, etc.) and port B is used for the maintenance modem connection (when required).

The processor card provides one 10/100 Mbits/s Ethernet port. It is routed to the front panel where it can be accessed via a TPE-RJ45 interface. The processor card incorporates an auto-negotiate feature to auto-detect 10Mbits/s or 100 Mbits/s. The bit rate auto-configures itself during operation.

Serial Card

The serial card occupies slot 3 of the EOAP. This card is a CompactPCI with four serial ports accessible from the EOAP backplane. These ports support full RS-232C capabilities in both synchronous and asynchronous modes. The first two ports are used for EOAP-to-Eagle STP connections. The other two ports are used for connecting the EOAP with SEAS. The serial card is a field-replaceable unit.

Power Supply Card

The power supply card occupies slots 7 and 8 of the EOAP. This card is a 48V input CompactPCI card. When powered by 48V central office power, the card provides +5, +12 and -12V outputs used by various components of the EOAP system. Two LEDs are located on the front of the card. The green LED indicates that the input voltage falls within the allowable range of 48 to 72 VDC, 12A max. The red LED indicates than an internal fault has occurred. These faults include over-voltage, input DC fail warning, loss of output power, and temperature exceeding set limits. The power supply card is a field-replaceable unit. Each EOAP I/O backplane contains a single input power connector.

Hard Drive Card

The center section of the dual EOAP system (both EOAP-A and EOAP-B) contains four individual drive bays. The top two drive bays are hard wired to EOAP-A and the bottom two drive bays are hard wired to EOAP-B. The top drive bay for each EOAP is occupied by the hard drive for that unit. The hard drive must be a SCSI II device, set to SCSI ID#0, with a minimum capacity of 9 GB. The factory pre-loaded hard drive is a field-replaceable unit. If the hard drive card is replaced, the platform followed by all site-specific information must be reloaded on the EOAP from the IP7 Secure Gateway.

CD-ROM Drive Card

The center section of the dual EOAP system (both EOAP-A and EOAP-B) contains four individual drive bays. The top two drive bays are hard wired to EOAP-A and the bottom two drive bays are hard wired to EOAP-B. The bottom drive bay for each EOAP is occupied by the CD-ROM drive card for that unit. The CD-ROM drive card must be a Solaris-compatible SCSI device and is currently configured as a 32X CD-ROM drive. The CD-ROM drive card is a field-replaceable unit.

Asynchronous Maintenance Modem (Optional)

CAUTION: The EOAP's open system architecture allows access to the operating system. Any undocumented changes to the files may cause the system to become corrupted and unusable. Making any undocumented changes on the EOAP, including changes to the hardware, operating system and/or the components found therein will void the warranty.

WARNING: EOAP hardware components, including disk drives, may be removed and (re)inserted with the power on, but they are NOT HOT SWAPPABLE at the operating system level.

Before any hardware component is removed from the EOAP, the operating system MUST BE HALTED. To halt the system, log in as

root, then at the command line, type: /usr/sbin/init 0. When the ok prompt appears, it is safe to remove the component.

After a component is (re)inserted, the system must be reset for Solaris to successfully detect the component. To reset the system, at the ok prompt type: reset-all. The system should boot up. If the system returns to the ok prompt after the reset-all command has executed, type: setenv auto-boot? true. Then type: reset-all.

WARNING: If the system still does not boot, as a LAST RESORT, perform a hardware reset by using a paperclip to press the ABORT and then RESET buttons on the faceplate, or by removing and reinserting the cPCI power supply from slot 7. Performing a hardware reset runs a HIGH RISK of corrupting the operating system to the point of rendering it unusable. If this occurs, the operating system and system software must be reloaded. A hardware reset also runs the RISK of causing the hard drive to fail. If this occurs, the hard drive must be replaced.

Although not provided with the EOAP, you can connect a Hayes-compatible modem to the EOAP to provide connectivity for remote monitoring and maintenance. This allows access to the EOAP as required by Tekelec Technical Services. If used, the modem is connected to the EOAP through the processor card's second serial port. The modem must be configured for 9600 bps, 7 bits, Even parity, and 1 stop bit (7-E-1).

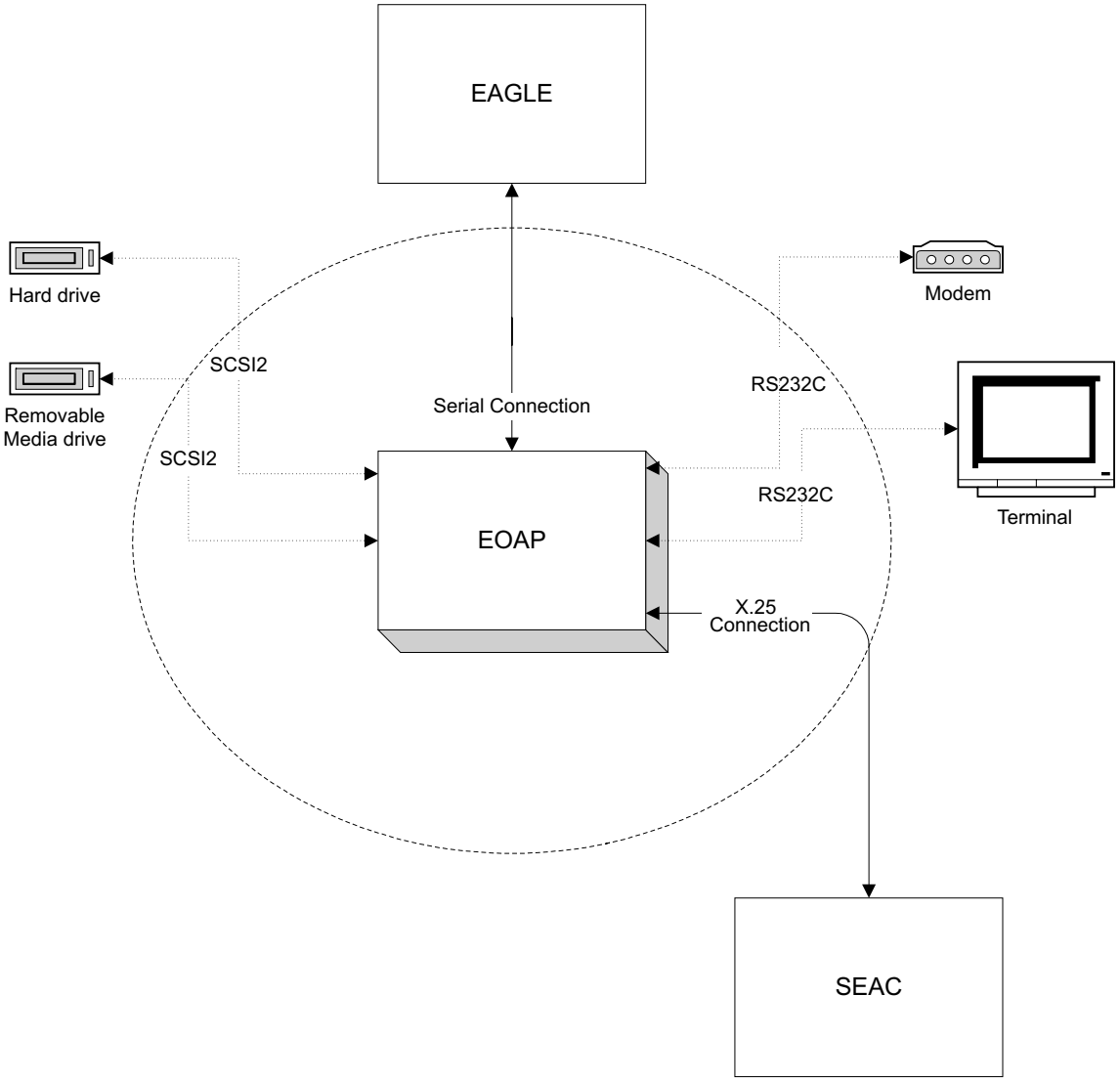
Terminal

The user console for the EOAP is a Digital Equipment Corporation VT-520 terminal. The VT-520 is connected to the EOAP through an RS232C terminal cable attached to the first serial connector of the processor card through the EOAP backplane. The terminal allows monitoring and direct interfacing capabilities to the EOAP. To ensure that the terminal and EOAP interact correctly, the terminal must be setup for vt100 emulation.

Interfaces

The EOAP is a general purpose interface module that provides the Eagle STP system with a generic platform to develop and run software for feature-specific interfaces to the Eagle STP. These interfaces include the optional Signaling and Engineering Administration System (SEAS) and the optional Local Service Management System (LSMS). Figure 8-3 shows the EOAP's operation context.

Figure 8-3. Operating Context of EOAP



EOAP-to-Eagle STP

Function

Each EOAP reports to the Eagle STP its general status as well as the status of its User Application Layer (UAL), X.25 links, PVCs on those links, and Q.3 associations. The Eagle STP can then report the status of the EOAP and its components to the user through the Eagle STP's HMI.

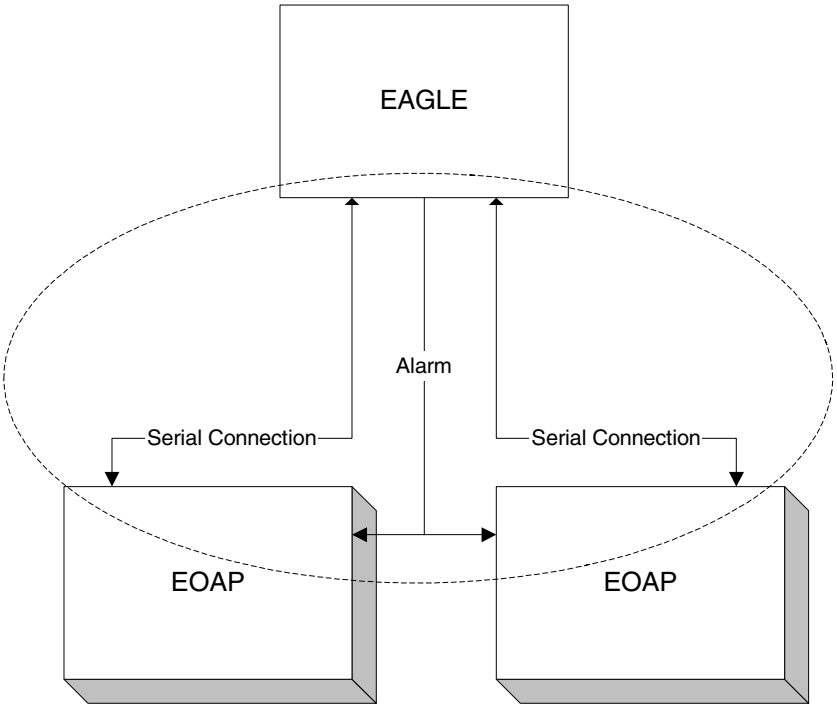
You can configure most aspects of the EOAP through the Eagle STP terminal. For upgrade, debug, and maintenance functions, use a VT-520 terminal directly connected to the EOAP.

The Eagle STP cannot perform a reset of the EOAP with the `init-oap` command from the Eagle STP terminal as it does with the OAP.

Interface

This section details the overall connections and setup required for the EOAP to Eagle STP interface. This includes the physical connection and a brief look at the messaging that occurs between the two.

Figure 8-4. EOAP-to-IP7 Secure Gateway Interface



Physical Connection

The EOAP is connected to the Eagle STP through the EOAP backplane using one of the two serial ports assigned to the processor card (only one port is used in a dual EOAP configuration). On the Eagle STP backplane, the cables are connected to any two of the MMI ports (MMI 0-MMI 15). By convention, if there are two EOAPs connected to the IP7 Secure Gateway (dual configuration), EOAP-A is connected to the lower numbered MMI port and EOAP-B is connected to the higher numbered MMI port. Regardless of their configuration, at any given moment, the EOAP connected to the lowest port is reported as OAP A by the Eagle STP. Any Eagle STP port connected to an EOAP must be configured as type "OAP" from the Eagle STP terminal.

Testing the Connection

Once the EOAP has been connected to any external device, it must be tested to ensure the connection was made correctly and is working as designed. For the EOAP-to-Eagle STP connection, this involves testing the ability for the EOAP to send maintenance information to the Eagle STP and have that information reported, verifying that the EOAP can communicate with the EOAP backplane serial ports, and test the ability of the IP7 Secure Gateway to perform a restart of the EOAP from the Eagle STP terminal.

EOAP-to-SEAS

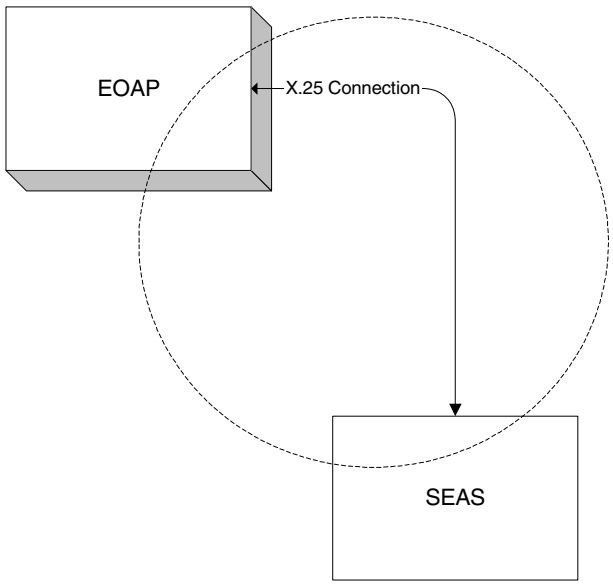
Function

The EOAP provides connectivity between the Signaling Engineering and Administration Center (SEAC) and the Eagle STP by implementing the UAL and X.25 layers of the SEAS protocol.

Each EOAP is configured according to customer specifications. Configurations for the EOAP support for SEAS include X.25 and UAL parameters.

This section details the overall connections and setup required for the EOAP to SEAS interface. This includes the physical connection and a brief look at the messaging that occurs between the two. It will also include a list of the components (hardware and software) necessary for its implementation, which will also include the EOAP-to-IP7 Secure Gateway connections.

Figure 8-5. EAGLE-to-SEAS Interface



Physical Connection

The EOAP is connected to the SEAS through the serial card. Port 3A/B and port 4A/B are reserved for SEAS communication. From these port(s), an RS232C cable is connected to a 9600 bps synchronous modem or other equivalent device necessary to connect to the SEAS system. If the configuration is for a single EOAP, the connection is made from both ports to two separate modems or other equivalent devices (X.25 connection). If the configuration is for a dual EOAP configuration, only one of the two serial ports is used per EOAP.

Messaging

Communication between the EOAP and the SEAS involves three message types:

- SEAS commands
- STP responses
- STP autonomous messages

These messages may involve one-way or two way communication between the SEAS and the EOAP. The actual messages are from the SEAC to the Eagle STP, however, the EOAP receives and transmits these messages between the two in a format that each can understand.

SEAS Commands

SEAS commands are messages originating from the SEAC that request the Eagle STP to perform a specific action. A response to this messages is returned by the Eagle STP within a required amount of time. These commands may specify when the command is to take place: either immediately upon receipt, upon receipt of a subsequent SEAS order-activation command, or automatically at a specified date and time. The default activation time for a SEAS command is immediately unless otherwise specified. At this time, the EOAP does not support time-delayed commands.

STP Responses

STP responses are messages sent from the Eagle STP to the SEAC in response to a SEAS command. The three basic types of STP responses are: completion responses, acceptance acknowledgments without completion, and exception responses.

STP Autonomous Messages

STP autonomous messages are messages sent from the Eagle STP automatically to the SEAC. These messages contain either scheduled measurement reports or on-occurrence event reports. Although these messages are logged by the SEAC, no acknowledgment is sent back to the Eagle STP confirming receipt.

Administration

The IP7 Secure Gateway administration supports the EOAP by providing the means to provision the EOAP at the IP7 Secure Gateway

IP7 Secure Gateway Provisioning

Administration provides support for the EOAP as follows:

- `chg-oap-config` command

  This command allows the configuration of the host name, IP address, netmasks, SEAC CLLI. X.25 mode and packet size, and EOAP configuration.

- `act-oap-config` command

  This command allows the update of the EOAP configuration.

- `rtrv-oap-config` command

  This command displays the IP address, netmasks, default router, SEAC CLLI. X.25 configuration, and X.25 packet size and DTE/DCE.

EOAP Retransmission Delay

Performance of this feature is affected by the requirement that the EOAP buffer an IP7 Secure Gateway message before transmission. It is a SEAS requirement that the STP knows the total length of a message before transmission of the message to SEAS. The IP7 Secure Gateway currently is not aware of message length before transmission. This requires the EOAP to buffer the entire message before it retransmits the message to the SEAS.

The Eagle STP/EOAP interface baud rate is 19200. The X.25 EOAP SEAS interface baud rate is 9600. To transfer a 12,000-character report (approximately 150 lines) from the Eagle STP to the EOAP, for example, takes approximately 5 seconds. The EOAP must buffer all 12,000 characters before retransmission. The EOAP would require another 10 seconds to retransmit the message. Total transmission time is 15 seconds.

The SEAS computers do not receive any response from the Eagle STP until EOAP retransmission begins. In the example above, SEAS does not receive any response for 5 seconds. This response delay increases for longer reports, assuming that SEAS will not time-out during the delay.

Maintenance

Hardware

Hardware maintenance for the EOAP consists of the replacement of any defective EOAP field-replaceable component. These components are the processor card, the the serial card, the power supply card, the hard drive card, and the CD-ROM drive card.

You must halt the Solaris operating system and remove power from the chassis before executing any hardware replacement procedures. You may have to power down one or both sides depending on what is replaced.

CAUTION: The EOAP's open system architecture allows access to the operating system. Any undocumented changes to the files may cause the system to become corrupted and unusable. Making any undocumented changes on the EOAP, including changes to the hardware, operating system and/or the components found therein will void the warranty.

If the hard drive is replaced, all site-specific information must be reloaded on the EOAP from the IP7 Secure Gateway. If other hardware items are replaced, no software changes will be required as long as they are replaced with identical items.

Software

Software maintenance is not required. The IP7 Secure Gateway performs all required configuration. Should a failure occur that cannot be corrected through the IP7 Secure Gateway, Tekelec Technical Services has the ability to access the EOAP through a modem or a direct terminal connection. If the operating system has been corrupted beyond the ability for Technical Services to perform a recovery, the hard drive will be replaced in the field.

Although the capability does exist for an on-site full re-install of all software packages found on the EOAP, this maintenance must only be performed under close supervision of Tekelec Customer Services.

CAUTION: The EOAP's open system architecture allows access to the operating system. Any undocumented changes to the files may cause the system to become corrupted and unusable. Making any undocumented changes on the EOAP, including changes to the hardware, operating system and/or the components found therein will void the warranty.

Alarm Interface

The EOAP provides a programmable seven-segment display on the front panel of the processor card. Additionally, the power supply card provides "Input OK" and Fault LEDs.

Upgrade Considerations

A detailed procedure for configuring the Eagle STP when upgrading from OAPs to EOAPs is described in the Eagle STP Installation Manual. The entire upgrade is performed either by a terminal connected directly to the EOAP or by an external connection through a modem.

Index

48 Million Numbers feature
see LNP 48 MIllion Numbers feature

A
administration
EOAP 8-12
alarm card, MPS Server
description 6-11
Application Communication Module 3-9
Application Service Module 3-10
Application Subsystem 3-7
Applications 3-20
Automatic Call Gapping 4-5

B
Billing Functions 4-8

C
card
MPS Server alarm 6-11
Communication Subsystem 3-5
components, MPS
list of hardware 6-2
specifications 6-10

D
Database Audit 4-7
Database Communications Module 3-9
Database Service Module (Eagle STP) 3-10
disk systems 4-10

E
Eagle LNP Functional Capabilities 4-4
Eagle STP 1-4
Eagle STP and IP7 Secure Gateway Systems 3-2
ELAP
supports LNP 48 Million Numbers feature 6-2
Embedded Operations Applications Processor 3-18
Enterprise 450
servers 4-10
EOAP 1-6
administration 8-12
EPAP
support of GSM features 6-1
equipment, MPS hardware 6-2
expansion cabinets 4-10

F
Fast Ethernet switch 4-10
features
G-Flex 6-1
G-Port 6-1
GSM 6-1
INP 6-1
LNP 48 MIllion Numbers 6-2
MPS system additional 6-10
MPS system supported 6-1
FTP Retrieve and Replace Feature 3-9
FTRA 3-9

G
G-Flex feature 6-1
G-Port feature 6-1
GR-376 EOAP 3-18
GSM features 6-1

H
hardware
platform 4-10
hardware, MPS
list of equipment 6-2
hardware, MPS system configuration 6-4
High Speed Operations Protocol 4-4
High-Capacity Multichannel Interface Module 3-11
High-Speed IMT Packet Router 3-6
High-Speed Master Timing 3-13
High-Speed Multiplexer 3-7
HIPR 3-6
HSOP 4-4

I
INP feature 6-1
Integrated Sentinel 5-6
Integrated Sentinel (ESP Frame Side) 5-8

Inter-processor Message Transport 3-5
IP7 Secure Gateway 1-4
ipgwi 3-20
iplim 3-20
iplimi 3-20

L

layered design 6-3
LEDs
  MPS Server 6-11
Link Interface Module 3-8
LNP
  measurements 4-8
LNP 48 Million Numbers feature 6-2
LNP Database 4-6
LNP Maintenance 4-7
LNP Query Service (LNPQS) 4-4
LSMS
  hardware platform 4-10

M

Maintenance and Administration Subsystem 3-4
MASP 3-4
Message Relay (MR) Function 4-5
MO drive 4-10
modems 4-10
MPS
  overview
    layered design 6-3
  system hardware configuration 6-4
  system software configuration 6-5
MPS hardware
  list of equipment 6-2
MPS on Netra 6-9
MPS on TekServer 6-2
MPS Server
  see also MPS system
  alarm card
    description 6-11
  component specifications 6-10
  LEDs 6-11
  overview 6-9
MPS system
  see also MPS Server
  additional features 6-10
  component specifications 6-10
  list of hardware components 6-2
  supported features 6-1
MPS/EPAP 4.0 1-6
Multi-Platform Server (MPS) Systems 6-1
Multi-Purpose Server 1-6

N

network
  configuration 6-7
  interfaces 6-7
network time protocol
  in TekServer platforms 6-8
NTP
  in TekServer platforms 6-8

O

optical disk drives 4-10
Overview of LSMS Hardware Components 4-11

P

platform 4-10
power sequencers 4-10

R

remote access 6-6
Reporting Functions 4-7

S

SCCP Subsystem Management 4-6
Scope and Audience 1-1
Sentinel Frames 5-4
Sentinel Server Frames 5-5
Sentinel Transport Cards 5-8
serial communication 6-6
server 4-10
Server, MPS
  see MPS Server
Site Collector Frames 5-4
Small Computer System Interface Buses 3-5
software, MPS system configuration 6-5
specifications
  MPS Server component 6-10
ss7ipgw 3-20

Sun StorEdge
D1000 Disk Systems 4-10
Sun Ultra
Enterprise 450 servers 4-10
Sun Ultra 5
standard hardware component 4-10
System Clock 3-12

T

T-1000 5-1
Tekelec 1000 1-6
Tekelec 1000 Applications Server 1-6, 5-1
Tekelec Signalling Products Systems 1-2
TekServer 1-6
Theory of Operation 3-14
Time Slot Counter Synchronization 3-14
Timing Systems Eagle STP/IP7 SG 3-12
Translation Services Module 3-10

IntroductionEAGLE STP/LNP Overview1-1
Common Channel signaling NetworksEAGLE STP/LNP Overview1-1
SS7 Link and Message TypesEAGLE STP/LNP Overview1-3
Role of SSPs, STPs and SCPs in SS7 NetworksEAGLE STP/LNP Overview1-7
STP System Link AdministrationEAGLE STP/LNP Overview1-11
IntroductionEAGLE STP/LNP Overview2-1
EAGLE SubsystemsEAGLE STP/LNP Overview2-1
Theory of OperationEAGLE STP/LNP Overview2-15
IntroductionEAGLE STP/LNP Overview3-2
EAGLE LNP SubsystemsEAGLE STP/LNP Overview3-2
EAGLE LNP Functional CapabilitiesEAGLE STP/LNP Overview3-8
OverviewEAGLE STP/LNP Overview4-2
HardwareEAGLE STP/LNP Overview4-4
SoftwareEAGLE STP/LNP Overview4-10
InterfacesEAGLE STP/LNP Overview4-13
AdministrationEAGLE STP/LNP Overview4-20
PerformanceEAGLE STP/LNP Overview4-21
MaintenanceEAGLE STP/LNP Overview4-22
Upgrade ConsiderationsEAGLE STP/LNP Overview4-23