Tekelec EAGLE® 5 Integrated Signaling System

Previously Released Features Manual

910-5073-001 Revision B

November 2007

Notice

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

Any export of Tekelec products is subject to the export controls of the United States and the other countries where Tekelec has operations.

No part of this documentation may be reproduced, translated, 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.

RoHS 5/6 - As of July 1, 2006, all products that comprise new installations shipped to European Union member countries will comply with the EU Directive 2002/95/EC "RoHS" (Restriction of Hazardous Substances). The exemption for lead-based solder described in the Annex will be exercised. RoHS 5/6 compliant components will have unique part numbers as reflected in the associated hardware and installation manuals.

WEEE - All products shipped to European Union member countries comply with the EU Directive 2002/96/EC, Waste Electronic and Electrical Equipment. All components that are WEEE compliant will be appropriately marked. For more information regarding Tekelec's WEEE program, contact your sales representative.

Trademarks

The Tekelec logo, EAGLE, G-Flex, G-Port, IP7, IP7 Edge, IP7 Secure Gateway, and TALI are registered trademarks of Tekelec. TekServer and A-Port are trademarks of Tekelec. 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:

5,732,213; 5,953,404; 6,115,746; 6,167,129; 6,324,183; 6,327,350; 6,456,845; 6,606,379; 6,639,981; 6,647,113; 6,662,017; 6,735,441; 6,745,041; 6,765,990; 6,795,546; 6,819,932; 6,836,477; 6,839,423; 6,885,872; 6,901,262; 6,914,973; 6,940,866; 6,944,184; 6,954,526;6,954,794; 6,959,076; 6,965,592; 6,967,956; 6,968,048; 6,970,542; 6,987,781; 6,987,849; 6,990,089; 6,990,347; 6,993,038; 7,002,988; 7,020,707; 7,031,340; 7,035,239; 7,035,387; 7,043,000; 7,043,001; 7,043,002; 7,046,667; 7,050,456; 7,050,562; 7,054,422; 7,068,773; 7,072,678; 7,075,331; 7,079,524; 7,088,728; 7,092,505; 7,108,468; 7,110,780; 7,113,581; 7,113,781; 7,117,411; 7,123,710; 7,127,057; 7,133,420; 7,136,477; 7,139,388; 7,145,875; 7,146,181; 7,155,206; 7,155,243; 7,155,505; 7,155,512; 7,181,194; 7,190,702; 7,190,772; 7,190,959; 7,197,036; 7,206,394; 7,215,748; 7,219,264; 7,222,192; 7,227,927; 7,231,024; 7,242,695; 7,254,391

Foreign Patent Numbers:

EP1062792; EP1308054; EP1247378; EP1303994; EP1252788; EP1161819; EP1177660; EP1169829; EP1135905; EP1364520; EP1192758; EP1240772; EP1173969; CA2352246

Ordering Information

To order additional copies of this document, contact your Tekelec Sales Representative.

Table of Contents

List of Figures

List of Tables

1

Introduction

About This Manual

This manual provides summaries of previously released EAGLE or EAGLE-related features at the time of their release.

Organization

This manual is organized into the following chapters:

- **Chapter 1, Introduction** provides information about this manual, how to contact the Customer Care Center, and a list of previously released features in alphabetical order.
- **Chapter 2, Features Num - E** describes features starting with numbers and letters from A to E.
- **Chapter 3, Features F - N** describes features starting with letters from F to K.
- **Chapter 4, Features L - Q** describes features starting with letters from L to O.
- **Chapter 5, Features P - Z** describes features starting with letters from P to Z.
- The **Glossary** provides a list of terms as well as acronyms and abbreviations.

References

The following document is referenced in this manual:

1. *TL-9000 "Quality System Problem Metric" Book Two, Release 3.0 QuEST Forum*.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

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

Documentation Availability, Packaging, and Updates

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

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

The electronic file of each manual is also available from the Tekelec Customer Support site. This site allows 24-hour access to the most up-to-date information.

Printed documentation is available for GA releases on request only and with a 4-week lead time. The printed documentation set includes pocket guides for commands and alarms. Pocket guides may also be ordered as a set or individually. Exceptions to printed documentation are:

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

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

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

Content changes are indicated with change bars, the revision of the manual part number is incremented, and the month of publication is updated.

Locate Product Documentation on the Customer Support Site

To view or download product documentation, log into the Tekelec Customer Support site at:

https://support.tekelec.com/index.asp

1. Log in with your user name and password. (Click on "Need an Account?" if you need to register).
2. Select EAGLE from the Product Support menu.
3. Select the release number from the Release menu.
4. Locate the Notices section to view the latest Feature Notice.
5. Locate the Manuals section to view all manuals applicable to this release.

   The documentation is listed in alphabetical order by the manual name. Only the first three manuals display. Click **more…** to see the remaining manuals.
6. Locate the latest revision of the manual name.

   Confirm the release number and last available revision.

   Select the 936-xxxx-x01 part number to download the complete documentation set with all linked files.

   NOTE: The electronic file for this part number is quite large.
7. To view a manual, double-click the manual name.
8. To download a manual, right-click and select Save Target As.

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

Customer Care Center

The Tekelec Customer Care Center offers a point of contact for product and service support through highly trained engineers or service personnel. The Tekelec Customer Care Center is available 24 hours a day, 7 days a week at the following locations:

- Tekelec, USA

  Phone:

  +1 888 367 8552 (US and Canada only)

  +1 919 460 2150 (international)

  Email: *support@tekelec.com*

- Tekelec, Europe

  Phone: +44 1784 467804

  Email:*ecsc@tekelec.com*

When a call is received, a Customer Service Report (CSR) is issued to record the request for service. Each CSR includes an individual tracking number.

Once a CSR is issued, the Customer Care Center determines the classification of the trouble. If a critical problem exists, emergency procedures are initiated. If the problem is not critical, information regarding the serial number of the system, COMMON Language Location Identifier (CLLI), initial problem symptoms (includes outputs and messages) is recorded. A primary Customer Care Center engineer is also assigned to work on the CSR and provide a solution to the problem. The CSR is closed when the problem is resolved.

Emergency Response

In the event of a critical service situation, emergency response is offered by Tekelec Technical Services twenty-four hours a day, seven days a week. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

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

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

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

Previously Released Features (Alphabetical Order)

The following features and enhancements were previously released under the EAGLE product (listed in alphabetical order):

- Disk Copy Fixed to Fixed (Release 20.0)
- Display Inhibited Alarms (Release 29.0)
- E1 Administration and Alarms (Release 26.3)
- E1 ATM High Speed Link (Release 28.1) (IP7 Release 6.0)
- E1/T1 MIM on EPM (E5-E1T1 Card) (Release 35.0)
- E1/T1 MIM on EPM (Release 35.1)
- E1/T1 Multi-Channel Interface Module (Release 28.0) (IP7 Release 6.0)
- E5-SM4G Card (Release 37.0)
- EAGLE Alarm Modifications for Synchronization with Harris (Release 31.5)
- EAGLE Frame Power Budget Alarm (Release 35.0)
- EAGLE Initiated OAP User Interface (Release 24.0)
- EAGLE Measurement Reports (Release 20.0)
- EAGLE OA&M IP Security Enhancements (EAGLE Releases 30.0, 30.2, IP7 Secure Gateway Release 8.0))
- EAGLE Support for Integrated Sentinel (Release 28.0)
- EDCM Support (IP7 Release 4.0)
- ELAP Network Address Translation (NAT) (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)
- Embedded OAP (Release 24.0)
- End Office Support (IP7 Release 5.0)
- Enhance GSM MAP Screening to add TC_Continue and End (Release 35.1)
- Enhance RTRV-LOG (Release 31.3)
- Enhanced Bulk Download (Release 25.0)
- Enhanced Database Status Reports (Release 20.0)
- Enhanced GPL Management (Release 25.0)
- Enhanced GSM Map Screening (Release 31.4)
- Enhanced GTT (Release 26.0)
- Enhanced Link Diagnostics (Release 22.0)

- GTT Error Reporting Enhancements (Release 21.0)
- GTT Loadsharing to 32 Destinations (Release 36.0)
- GTT Table Increase (Release 29.0)
- GTT UIM 21 Digit Length Enhancement (Release 29.0)
- GWS Error Reporting Enhancement (Release 21.0)
- Hex Digit Support for GTT (Release 35.3)
- High Capacity Multi-Channel Interface Module (HC MIM) (Releases 33.0 34.0)
- High Speed IMT Packet Router (HIPR) (Releases 33.0 34.0)
- High Speed Master Timing (Release 26.0)
- High-Speed Multiplexer (HMUX) (Release 27.2)
- Holdover BITS Clock Support (Release 21.0)
- Idle Terminal Port Logout (Release 21.0)
- IDP Screening for PrePaid (Release 34.3)
- IETF M3UA for “A” Link Connectivity (Release 28.1)
- IETF M3UA Support including IETF SUA (IP7 Release 5.0)
- IETF Protocol Update (Release 28.1) (IP7 Release 6.0)
- IETF SCTP for “A” Link Connectivity (Release 28.1)
- IETF SCTP Support (IP7 Release 5.0)
- IETF SUA for “A” Link Connectivity (Release 28.1)
- Implementation of SNMP Agent (IP7 Release 2.0)
- Improved Routing Management (Release 20.0)
- IMT Fault Isolation (Release 22.0)
- IMT Subsystem Alarms (Release 20.0)
- INAP-based Number Portability (INP) (Release 26.05)
- Increase Gateway Screening Screen Sets to 255 (Release 22.0)
- Increase GTT Entries per TT to 200,000 (Release 29.0)
- Increase in Time Zones (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0))

- Increase System-Wide IP Signaling Connections (Release 31.6)
- Increase System-Wide IPGWx TPS (Release 31.6)
- Increase the Number of Mated Application Entries (Release 22.0)
- Increased Linkset Capacity (Release 28.0)
- Increasing the Size of the Service Provider ID Table (Release 23.2)
- INP Number Normalization (Release 26.3)
- Integrated Monitoring for E5-E1T1 (Release 35.1)
- Interim Global Title Modification (IP7 Release 2.2)
- Intermediate GTT Loadsharing (Release 28.1)
- Intrusion Alert (Release 21.0)
- IP Signaling Serviceability (Release 35.0)
- IP7 Internationalization (IP7 Release 4.0)
- IP7 Transport Feature (Release 26.1)
- IPGWx Congestion Enhancement (Release 35.1))
- IPGWx Data Feed (Release 35.0)
- IPGWx Data Feed (Release 35.1)
- IPGWx TPS Control (Release 31.6)
- IPLIM Protocol Support Enhancement (Release 28.1) (IP7 Release 6.0)
- IPLIMx Data Feed (Release 35.0)
- IPLIMx to 8 Points (Release 29.1) (IP7 Release 7.1)
- IPLIMx/IPGWx on EPM (E5-ENET Card) (Release 35.0)
- IPLIMx/IPGWx on EPM (Release 35.1)
- IPMX/MCAP/TDM Replacement (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0))
- IP-SCP with LNP Capability (IP7Releases 1.0, 2.0)
- IP User Interface: Telnet Support (Release 29.0) (IP7 Release 7.0)
- IS-41 to GSM Migration (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)
- IS41 GSM Migration (Release 36.0))

- ISCC Interface Loopback Test (Release 22.0)
- ISUP Message Type Screening (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)
- ISUP Normalization Administration (IP7 Release 5.0)
- ISUP Normalization in the IP7 SG (IP7 Release 4.0)
- ISUP NP with EPAP (Releases 31.11, 34.0)
- ISUP-Over-IP Gateway for Connectivity to IP-SEPs (IP7 Release 1.0)
- ITU DTA (a.k.a. ITU Triggerless Message Screening) (Release 31.6)
- ITU Duplicate Point Code Routing (Release 26.05)
- ITU Gateway Measurements Enhancements (PR19536) (Release 26.05)
- ITU MTP Restart (Release 26.0)
- ITU SLS Enhancements (Release 26.0)
- ITUN-ANSI SMS Conversion (Release 37.0)
- ITU-TFR Procedure (Release 26.1)
- KSR Terminal Feature (Release 20.0)
- Large BICC MSU Support for IP Signaling (Release 37.0)
- Large System (Phase 3)—1500 Links (Release 29.0)
- Large System (Release 27.2)
- Large System—Phase 2 (Release 28.0)
- Last 10 Command Retrieval (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0))
- Link Failure Status Information (Release 22.0)
- Link Fault Sectionalization (Release 21.0)
- Link Maintenance Enhancements/LFS Increase for MPL-T and MIM (Release 31.3)
- Link Status Reporting (Release 21.0)
- Linkset ID to Measurements Report (EAGLE R30.0/IP7 SG R8.0)
- Linkset Name Increase—ANSI/ITU (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)
- Linkset Restricted Support (Release 31.9)
- LNP 96 Million TNs—EAGLE 5 (EAGLE Release 30.0, IP7 Secure Gateway Release 8.0)

- LNP—New LNP Input and Output Groups (Release 22.0)
- LNP—New Unsolicited Alarm Messages (UAMs) (Release 22.0)
- LNP—New Unsolicited Information Messages (UIMs) (Release 22.0)
- LNP—NPANXX Commands (Release 22.0)
- LNP—Query Routed as Final Global Title Translation (Release 22.0)
- LNP—Query Routed as Non-Final Global Title Translation (Release 22.0)
- LNP—Report LNP Status Command (Release 22.0)
- LNP—Rerouting Messages for the Local Subsystem (Release 22.0)
- LNP—Retrieve LNP Database Time Stamp Command (Release 22.0)
- LNP—SCCP Management on the LIMs (Release 22.0)
- LNP—Service Commands (Release 22.0)
- LNP—Service Provider Commands (Release 22.0)
- LNP—Split NPA Commands (Release 22.0)
- LNP—Subsystem Application Commands (Release 22.0)
- LNP—System Options Commands (Release 22.0)
- Login Failure Message (Release 21.0)
- Login Success or Failure Tracking (Release 21.0)
- Logout on Communications Failures (Release 22.0)
- LRN Table Increase (Release 26.1)
- M2PA on IPLIMx (Release 29.1) (IP7 Release 7.1)
- M2PA RFC Support (Release 34.3)
- M3UA Protocol Enhancements (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)
- Management of Unused User IDs (Release 21.0)
- Manual Deactivation of SRST Message (Release 21.0)
- MAP Table Increase (Release 29.0)
- Measurements Enhancements (Release 22.0)
- Measurements Platform Filename with CLLI (Release 31.3)

- Non-ANSI Point Code Support (Release 20.0)
- Non-Generation of Duplicate SEAS Autonomous Messages (Release 22.0)
- Non-SCCP/ISUP Routing (IP7 Releases 1.0, 2.0)
- Notification of Congestion Level Increase (Release 22.0)
- Notification of Inability to Perform a Global Title Translation (Release 22.0)
- Notification of Link Set Outage (Release 22.0)
- Notification of Link Set Recovery (Release 22.0)
- Notification of Locally Initiated Database Copy (Release 22.0)
- Notification of MTP-Level Routing Error (Release 22.0)
- Notification of Recovery from Link Congestion (Release 22.0)
- Number Pooling (Release 24.0)
- Number Pooling/Efficient Data Representation (EDR) (Release 26.1)
- OAP Upgrade Enhancement (Release 27.2)
- OCTRETRN in 30-Minute Measurements Reports (Release 31.4)
- Online Cartridge Formatting (Release 20.0)
- Option for Subsystem Prohibit (Release 29.0)
- Option for Turning on Class 1 Sequencing (Release 31.6.3)
- Origin-based MTP Routing (Release 35.0)
- Origin-based SCCP Routing (Release 35.0)
- Password Aging (Release 21.0)
- Password Encryption (Release 21.0)
- Password Requirements (Release 21.0)
- PCS 1900 LNP Query (Release 26.0)
- PDBA Proxy (EPAP 7.0)
- Per-Linkset Random SLS (Release 36.0)
- Performance Enhancements (IP7 Release 3.0)
- Persistent Device States (Release 29.0)

- Point-to-Point Connectivity for ITU Point Codes (IP7 Release 2.2)
- Portability Check for Mobile Originated SMS (Release 29.1)
- Prepaid Initial Detection Point Query Relay (Release 34.1)
- Prepaid SMS Intercept - Phase 1 (Release 28.1)
- Prevention of Congestion from Rerouted Traffic (Release 21.0)
- Prevention of Link Oscillation (Release 21.0)
- Preventive Cyclic Retransmission (PCR) (Release 20.0)
- Priority Processing of Network Management Messages (Release 21.0)
- Private Point Code (Releases 31.12, 34.0)
- Prohibit Removing the Last Route to a Destination if that Destination is being Referenced by Mated Applications or Concerned Signaling Point Code Groups (Release 22.0)
- Prohibit the Assigning of a Linkset with Linkset Types A or E to a Cluster Route (Release 22.0)
- Provisioning Range for Gateway Screening (Release 22.0)
- Quality of Service Enhancements (IP7 Release 3.0)
- Random SLS Generation (Release 28.0)
- REPT-STAT-CLK Enhancements for Clocking (Release 28.2)
- REPT-STAT-TRBL Enhancement (Release 29.0)
- Response to Commands Issued Prior to Login (Release 21.0)
- Revoking a User ID (Release 21.0)
- Routing Key Enhancements (IP7 Release 3.0)
- RTDB Retrieve (EPAP 9.0)
- RTRV-RTE/RTRV-DSTN: Support of PC Wildcards (Release 35.0)
- RTRV-STP on FTRA
- RTRV-TBL-CAPACITY Enhancement (Release 29.0)
- SCCP Loop Detection (Release 35.6)
- SCCP Message Type Screening (Release 22.0)
- SCCP Service Re-Route Capability (Release 34.3)

- SCCP/TCAP Over IP Gateway for Point-to-Multipoint Connectivity (IP7 Release 1.0)
- SCCS Interface Support (Release 21.0)
- SCTP Checksum Update (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)
- SCTP Retransmission Control (Release 28.1) (IP7 Release 6.0)
- SEAS Enhancements (Release 26.0)
- SEAS Enhancements, Autonomous Messages (Release 22.0)
- SEAS Gateway Audit Command (CHK-UNREF-ENT) (Release 22.0)
- SEAS Interface Support (Release 21.0)
- SEAS Verify Signaling Route-Set Status and SCCP Application Status Command (VFY-SRSAPST) (Release 22.0)
- Security Log Increase (Release 26.05)
- Selective Alarm Inhibiting (Release 22.0)
- Selective Homing of EPAP RTDBs (Release 29.0)
- Simplifying BIP (Board ID PROM) for EAGLE STP Boards (Release 23.1)
- Single Slot Enhanced DCM (Release 28.1) (IP7 Release 6.0)
- SLAN on E5-ENET Assembly (Release 37.0)
- Spare Point Code (Release 31.12)
- Split Allowed CGPA Table (Release 22.0)
- Split of Allowed SIO Table (Release 22.0)
- SS7 Message Rejection Due to Screening (Release 22.0)
- SS7 over High-Speed Signaling Link (Release 23.0)
- SS7-Over-IP Gateway for Point-to-Point Links (IP7 Release 1.0)
- SS7 SCCP-User Adaptation Layer (SUA) Request for Comment (RFC) (Release 31.10)
- STC on E5-ENET Assembly (Release 37.0)
- STP LAN Feature (Release 20.0)
- STPLAN Port to DCM (Release 26.0)
- STPLAN SSEDCM Capacity Increase (Release 34.0)

- STPLAN with Default Router (Release 23.0)
- SUA DAUD with SSN Support (Release 37.0)
- Support 12 Million Ported Numbers (Releases 24.0, 25.0)
- Support Changing the Linkset Name (Release 28.0)
- Support CHG-GTT to change the GTA (Release 35.0)
- Support for 2000 ITU Links per Node (Release 35.1)
- Support for 32 Prepaid SMS Intercept Platforms (Release 37.0)
- Support for 32 Prepaid SMS Intercepts (EPAP 9.0)
- Support for IP7 8.0 Gateway Features (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0))
- Support for LSMS Audit Enhancements (Release 26.1)
- Support for LSMS Split Provisioning (Release 26.1)
- Support for Matching Self-ID Rule in SEAS CHG-SID (Release 22.0)
- Support for MTP Status Functions (IP7 Release 2.0)
- Support for Provisioning Multiple EPAPs (Release 29.0)
- Support for SCCP XUDT/XUDTS Messsages, In-Sequence Delivery of Class 1 SCCP UDT/XUDT Messages (Release 31.6)
- Support for Secure Gateway Functionality through IP7 7.0 (Release 29.0)
- Support for TALI Architecture (IP7 Release 4.0)
- Support for the CLLI Parameter for Adding or Changing Linksets (Release 22.0)
- Support for the New Linkset Name Parameter for Changing the Attributes of a Route (Release 22.0)
- Support for Up to 41 IPLIMx DCMs (IP7 Release 2.2)
- Support G-Flex at 1700 TPS per DSM (ANSI only) (Release 31.6)
- Support Java 1.5 on EPAP (EPAP 9.0)
- Support LSMS Disaster Recovery (Release 23.1)
- Support of E1 Interface for SS7 Signaling Links (Optional) (Releases 22.2, 24.0)
- Support of E1 Master Clock Interface for SS7 Signaling Links (Optional) (Release 22.2)
- Suppression of Gateway Measurements on Non-Gateway Linksets (Release 25.0)

- Synchronous E1 High Speed Link (SE-HSL) (Release 34.0)
- TALI “A” Link Connectivity (Release 28.0)
- TALON Development Kit (IP7 Release 2.0)
- TDM Global Timing Interface (Release 31.6)
- Temporary Alarm Inhibiting and Offline Functions (Release 25.0)
- Thresholding of UIM Messages (Release 25.0)
- Time-Based Inhibit Alarm (Release 35.0)
- Time Stamps for rept-stat-trbl Report (Release 31.6)
- Translation Type Mapping (Release 21.0)
- Triggerless LNP (Release 24.0)
- TSM Warm Restart and Incremental Loading (Release 26.0)
- TT Independence for LNP Queries (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)
- TUP Message Type Screening (Release 31.6)
- Two-Point IPLIMx (EAGLE 27.1, IP7 Release 2.2)
- Unregistered Routing Key Treatment (IP7 Release 3.0)
- Update Validation (Release 34.0)
- Upgrade Procedure Enhancements (Release 22.0)
- Use IMT Bus Instead of MBUS (Release 23.0)
- User-Initiated Keyboard Locking (Release 22.0)
- Using the DPC/SSN Parameters and GTA Range in Displaying Global Title Translations (Release 22.0)
- Variable-Length Global Title Translation (Release 26.1) (IP7 Release 2.2)
- Warning Message When LIMs Added with Insufficient TSMs (Release 25.0)
- Weighted GTT Loadsharing (Release 36.0)
- Weighted SCP Load Balancing (Release 27.2)
- Wireless Number Portability (Release 23.1)
- X.25/SS7 Gateway Feature (Release 20.0)

- Year 2000 Compliance (Release 23.1)

2

Features Num - E

1100 TPS/DSM for ITU NP (Release 36.0)

Description

The 1100 TPS/DSM for ITU NP feature allows a DSM card to support up to 1100 transactions per second (TPS) for the EAGLE 5 ISS G-Port, A-Port, INP, IS41 GSM Migration, EIR, and ANSI-41 INP Query features.

The 1100 TPS/DSM for ITU NP feature increases the TPS capacity of each DSM card from the current 850 TPS to 1100 TPS per card when an EPAP-based ITU feature (G-Port, G-Flex, INP, EIR, Prepaid IDP Query Relay, A-Port, IS41 GSM Migration, or AINPQ) has been turned on. Increasing the TPS of each card increases the maximum capacity of an EAGLE 5 ISS, with 25 DSM cards in a 24 + 1 configuration, from 20,400 to 26,400 TPS. (The capacity of a DSM card is rated at 1700 TPS when features requiring EPAP-based database lookup have not been enabled or turned on.)

In most systems, only 50% or less of the traffic needs an EPAP-based database lookup while the rest of the traffic requires GTT-related database lookup. The 1100 TPS/DSM for ITU NP feature assumes that at most 70% of the traffic shall require EPAP-based database lookup.

A feature access key (FAK) for part number 893018001 is required to enable this feature.

- A temporary FAK is not allowed for this feature.
- This feature is an ON/OFF feature, it can be turned on and off after it has been enabled.
- At least one EPAP-based ITU feature (G-Port, G-Flex, INP, EIR, Prepaid IDP Query Relay, A-Port, IS41 GSM Migration, or AINPQ) must be on before this feature can be enabled.
- The **ansigflex** STP option cannot be used when this feature is enabled; this feature cannot be enabled when the **ansigflex** STP option is used.

Hardware Requirements

The 1100 TPS/DSM for ITU NP feature requires DSM cards running the VSCCP application

Limitations

When the 1100 TPS/DSM for ITU NP feature is on and more than 70% of the traffic requires EPAP-based database lookup, the DSM cards provisioned in the system for SCCP might not be able to support 1100 TPS.

120 Million LNP Numbers (Release 32.0)

Description

The 120 Million LNP number feature provides the capability to expand the maximum number of ported/pooled LNP numbers supported on one EAGLE platform from 96 million to up to 120 million LNP numbers. Local Service Management System (LSMS) _ EAGLE LNP Application Processor (ELAP) reload, audit and reconcile times increase proportionally to the size of the database. Aggregate times for Multi-Purpose Server (MPS) to DSM audit, reconcile, and reload increase slightly due to the increase in LNP database capacity, but the rate-per-time unit remain the same.

Hardware Requirements

The existing 4G DSM card is used for 120 Million LNP numbers.

Limitations

- This feature is only available for North American LNP customers.
- This feature is dependent on the LSMS 120 Million LNP number feature.
- If the Message Relay Group (MRG) Table exceeds 2 million entries then the Software Release Upgrade cannot occur. This is an incompatible situation and loss of data may occur if the upgrade is executed for either the EAGLE 5 ISS or ELAP.

15 Minute Measurements (Release 31.3)

The 15 minute Measurements feature is controlled by a feature access key and a measurement option. Turning on the feature requires a part number. The feature cannot be turned off once turned on. It is a Permanently ON feature. Upon turn on, the collection period defaults to the 30-minute option to maintain compatibility with the existing system capabilities.

The feature becomes operational when the collection period has been changed to 15 minutes. The collection period can be changed from 30 minutes to 15 minutes (and vice versa) by changing the 15 Minute Measurements collection option of the Measurements Platform options table. When the 15 Minute Measurements collection is disabled, measurements data will be collected and reported each half-hour at hh:00 and hh:30. When the 15 Minute Measurements collection option is selected to enabled, measurements data will be collected and reported four times each hour at hh:00, hh:15, hh:30, and hh:45. The current state of the option is displayed with the Measurements Platform options. Report types supported by 15 Minute measurements are: systot, comp, gtwy, and avl.

Turning on the feature requires a feature access key. This feature cannot be turned off once turned on, therefore it is a Permanently ON feature. When the feature is turned on, the collection period defaults to the 30-minute option to maintain compatibility with the existing system capabilities.

150,000 GTT TPS and 75,000 EPAP TPS (Release 37.0)

Description

The 150,000 GTT TPS feature increases the throughput capacity of the EAGLE 5 ISS from 52,700 to 150,000 TPS for a node in which the SCCP message throughput traffic is processed by the GTT feature.

The 75,000 EPAP TPS feature increases the throughput capacity of the EAGLE 5 ISS from 20,400 to 75,000 TPS for a node that processes part of the SCCP message throughput traffic by one or more of the EPAP-based features (e.g. G-Port, G-Flex, EIR, or INP) or for a node that processes a combination of GTT and EPAP traffic.

These features require the E5-SM4G card to be installed in the EAGLE 5 ISS. The E5-SM4G Throughput Capacity feature must be enabled and turned on in order to operate at 5000 TPS (if traffic is processed by GTT) or 3125 TPS (if traffic is processed by the EPAP-based features).

To achieve the maximum TPS rates, the following conditions must be met:

- All of the DSM cards must be replaced with E5-SM4G cards.
- The E5-SM4G Throughput Capacity feature must be enabled and turned on.

If all of the SCCP traffic is processed by GTT, then a maximum of 32 E5-SM4G cards can be provisioned in the EAGLE 5 ISS. If the E5-SM4G Throughput Capacity feature is enabled and turned on, then each E5-SM4G card can process traffic at a rate of 5000 TPS, and the 150,000 TPS rate can be reached.

If any of the SCCP traffic is processed by an EPAP-based feature, then a maximum of 25 E5-SM4G cards can be provisioned in the EAGLE 5 ISS. If all of the SCCP traffic is processed by EPAP-based features, and if the E5-SM4G Throughput Capacity feature is enabled and turned on, then the rate of 75,000 TPS can be reached.

E5-SM4G cards can co-exist with DSM cards in the EAGLE 5 ISS; however, if both kinds of cards are used, then the maximum TPS rates cannot be reached.

Feature Control Requirements

The E4-SM4G Throughput Capacity feature has the following feature control requirements:

- A FAK for part number 893-0191-01
- A temporary key cannot be used to enable the E5-SM4G Throughput Capacity feature.
- After the E5-SM4G Throughput Capacity feature has been turned on, it cannot be turned off.
- The E5-SM4G Throughput Capacity feature cannot be enabled if any of the following features or options are turned on:
  - E5IS (EAGLE 5 Integrated Monitoring) feature
  - LNP feature
  - ANSIGFLEX STP option

Hardware Requirements

The E5-SM4G Throughput Capacity feature requires HIPR cards to be installed in all the shelves in an EAGLE 5 ISS node.

Limitations

The 150,000 GTT TPS and 75,000 EPAP TPS features have the following limitations:

- The real time database entry capacity of the E5-SM4G card for the EPAP-based features is smaller than the capacity supported by the current DSM 4G card.
- If the E5IS IMF or LNP feature, or the ANSIGFLEX system option is enabled, then the TPS level is held to the level of a DSM card (1700 TPS). The E5-SM4G Throughput Capacity feature cannot be enabled, and the 150,000 GTT TPS feature cannot be used.

18 GB to 36 GB Hard Drive Upgrade (Release 29.1) (IP7 Release 7.1)

Description

EAGLE Release 29.1 requires that the EPAP databases accommodate 56 million G-Flex entries. Additional disk space is being provided by way of a hardware disk replacement, from 18 GB disks to 36 GB disks. All the new space on the data disk (18 GB minus overhead) will be appended to the database file system /usr/db. The additional space on the system disk (18 GB minus overhead) will be appended to the swap space. The disk upgrade will occur during a maintenance window, when no software upgrade is scheduled.

Although this feature has been developed specifically for the EPAP, it is not application-specific. This hard drive upgrade could be performed on any MPS server running any GA release.

Upgrade Procedure

The upgrade will be performed as follows:

- The technician will label the disks in the system and the disks in the upgrade kit.
- Using Disksuite functionality, half of the old disks will be replaced with the new disks, and will sync with the remaining old disks.
- Once the disks have been sync'd, the remaining old disks will be replaced with the remaining new disks. The new disks will then sync again.
- A script will expand the **`/usr/db`** and swap file systems to use all the space available.

A backout will be performed as follows:

- The MPS will be brought to run-level zero.
- The technician will remove the 36 GB disks, install all the old disks, and remove the new disks.
- The technician will boot the MPS.
- A script will re-mirror and repair the metadbs.

Hardware Requirements

This feature requires that all four 18 GB disks on an individual MPS be replaced with 36 GB disks. (New MPS's with the EPAP application will be manufactured with the 36 GB disks.)

192 Million LNP Numbers (Release 34.0, ELAP 5.0)

Description

The 192 Million LNP Numbers Support feature expands the maximum number of ported/pooled Local Number Portability (LNP) numbers supported on one EAGLE 5 ISS platform to 192 million LNP numbers. The feature supports feature access keys for 132, 144, 156, 168, 180, or 192 million ported/pooled numbers.

Configurable alarm thresholds indicate:

- When the transactions-per-second (TPS) for the EAGLE 5 ISS (as a whole) reaches the threshold value.
- When the number of LNP ported TNs and LRNs in the database is approaching the configured percent of the enabled maximum number allowed in the database.
- When the thermal limits of an HC-MIM card have been reached.

The 192 Million LNP Numbers Support feature requires the ELAP 5.0 database application. The ELAP 5.0 database application is installed and runs on the T1100 application server.

Hardware Requirements

The existing 4GB DSM card must be used for the 192 Million LNP Numbers feature.

The ELAP 5.0 database application that supports 192 million LNP numbers runs on the T1100 platform.

Limitations

- The 192 Million LNP Numbers feature is available only for North American LNP customers.
- This feature requires the LSMS 192 Million LNP Numbers feature.
- Prior to the upgrade, Tekelec will perform a pre-upgrade health check to access the compatibility of your current hardware and software configuration. If the Message Relay Group (MRG) table exceeds 2 million entries, the Software Release Upgrade cannot occur. This is an incompatible situation, and a loss of data may occur if the upgrade is executed for either the EAGLE 5 ISS or ELAP.
- 192 Million LNP Numbers feature activation on the EAGLE 5 ISS is based on the following conditions:
  - The ELAP LNP Configuration feature access key must be on.
  - 4-Gigabyte DSMs are required; at least one 4-Gigabyte DSM must be provisioned in the system.
  - The ELAP software version must be ELAP 4.0 if an EAGLE 5 ISS feature access key for 96-120 Million LNP Numbers is enabled.
  - The ELAP software version must be ELAP 5.0 if an EAGLE 5 ISS feature access key for more than 120 Million LNP Numbers is enabled.

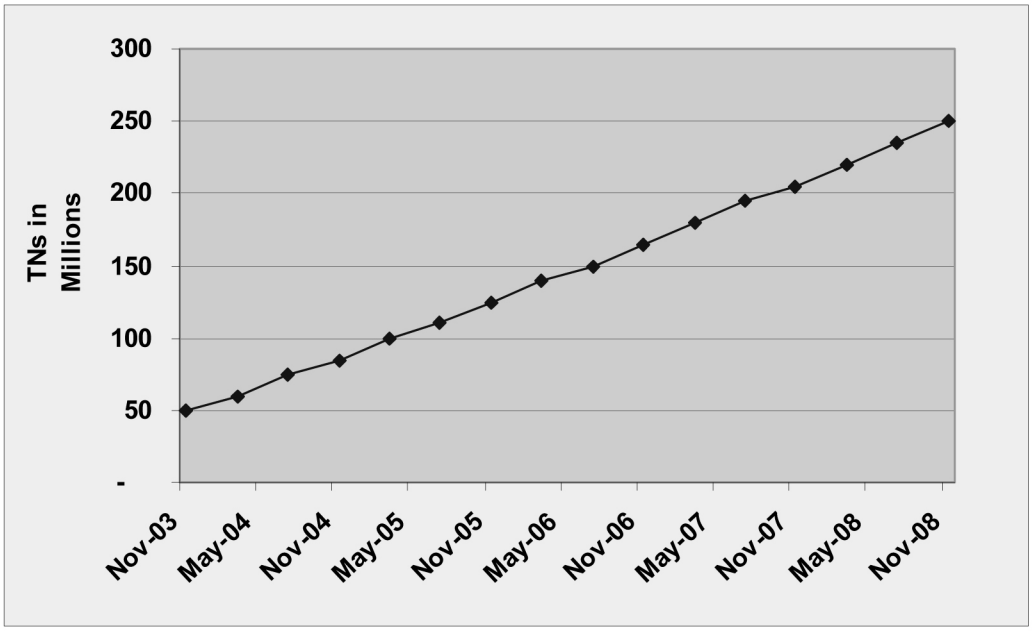
228 Million LNP Numbers (ELAP 6.0)

Description

As Local Number Portability becomes more established, competition increases, and number pooling becomes more widespread, the number of ported TNs continues to increase. Customers would like to manage a single LSMS that is capable of maintaining the national LNP database. Increased capacity is required on the ELAP.

Currently, Tekelec supports 192 Million LNP numbers per node on a 4 GB DSM card. With the advent of wireless portability and continued wireline LNP porting and pooling activity, it is anticipated that the 192 Million LNP numbers capacity will be exceeded sometime early-mid 2007 as shown in Figure FN-1.

Figure 2-1. Current LNP Growth Projections



The 228 Million LNP Numbers feature allows customers to use their existing hardware and remain in a centralized Eagle LNP architecture (all LNP numbers in one node).

The 228 Million LNP Numbers feature expands the maximum number of ported/pooled LNP numbers supported on one EAGLE node to 228 million LNP numbers in increments of 12 million numbers. Additional database improvements include faster MPS-to-DSM audit reconcile and reload times, and LSMS-to-ELAP audit times.

The 228 Million LNP Numbers feature expands the maximum number of ported/pooled Local Number Portability (LNP) numbers supported on one on the ELAP to 228 Million LNP Numbers. The feature supports feature access keys for increments from 204, 216, or 228 million ported/pooled numbers across all NPAC regions.

Hardware Requirements

The 228 Million LNP Numbers feature requires the existing 4 GB DSM card.

The 228 Million LNP Numbers feature runs on the T1100 platform.

Limitations

The 228 Million LNP Numbers feature is available only for North American LNP customers.

The 228 Million LNP Numbers feature requires the LNP 228 Million numbers feature on the LSMS.

228 Million LNP Numbers (Release 35.0)

Description

The 228 Million LNP Numbers feature allows the capacity of an EAGLE 5 ISS node to increase to 228 million LNP numbers without adding new hardware.

The increase is achieved by using existing 4GB DSM cards and enhancing the database. EAGLE 5 ISS supports the following feature access keys for LNP growth beyond 120 million LNP numbers on the existing 4GB DSM card:

- 132 Million LNP – 893-0110-15
- 144 Million LNP – 893-0110-16
- 156 Million LNP – 893-0110-17
- 168 Million LNP – 893-0110-18
- 180 Million LNP – 893-0110-19
- 192 Million LNP – 893-0110-20
- 204 Million LNP – 893-0110-21
- 216 Million LNP – 893-0110-22
- 228 Million LNP – 893-0110-23

The 228 Million LNP Number feature must be activated on the LSMS, ELAP, and EAGLE 5 ISS products. LSMS 8.5 and ELAP 6.0 with 228 Million LNP Numbers support are required to enable the feature on EAGLE 5 ISS.

Hardware Requirements

The 228 Million Numbers LNP feature has the following hardware requirement:

- The existing 4GB DSM card must be used for the 192 Million LNP Numbers feature.
- The ELAP 5.0 database application that supports 192 million LNP numbers runs on the T1100 platform.

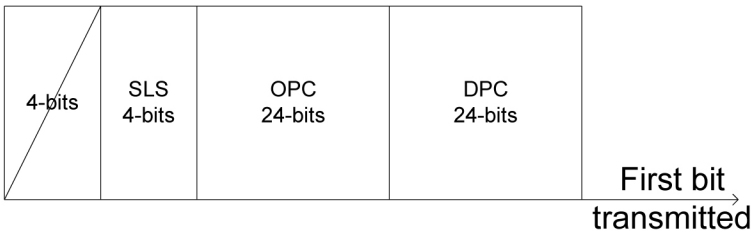
Limitations

The 228 Million LNP Numbers feature has no limitations.

24-Bit ITU-N Point Code Support Feature (Release 31.0)

The 24-bit ITU-N point code routing label structure consists of the Destination Point Code (DPC), Originating Point Code (OPC), and the Signaling Link Selection fields.

Both the DPC and OPC are 24 bits in length, and SLS is the code for signaling link selection for load sharing. Currently, only the least 4 bits of the SLS are used. The upper 4 bits are used as part of CIC in the telephone message label. For other messages, the upper 4 bits of the SLS are set to 0000.



2500 Routing Keys (IP7 Release 7.1)

Description

This feature increases the total number of routing keys on a SSEDCM IPGWx application from 1000 routing keys to 2500, while retaining the DCM IPGWx application to a maximum of 1000 routing keys. The total number of routing keys for each application may be all dynamic, all static, or a combination of both.

The SG supports two types of routing keys for use by the IPGWx application, Static Routing Keys and Dynamic Routing Keys. Both routing keys are stored in one routing key table which is located in RAM on the IPGWx application.

- Static Routing Keys. These routing keys are provisioned via administration commands and are stored in the OAM static database. The SS7IGWx application keeps a copy of the static routing keys in the SS7 Routing Key Table on-board in RAM for quick access.

- Dynamic Routing Keys. Dynamic Routing Keys are provisioned via a request sent over an IP connection and allows an IP connection to automatically direct traffic towards (or away from) themselves by sending messages to the Signaling Gateway.

Note that all IP connections (TALI/TCP, M3UA/SCTP and SUA/SCTP) on the IPGWx application use routing keys. Currently, only TALI sockets have the capability to create dynamic routing keys via dynamic registration. However, this feature makes no assumptions regarding an IP connection's ability to register dynamic routing keys.

New Auto-inhibit Facility

The System Configuration Manger (SCM) software is responsible for determining if the proper GPL should be fully loaded onto the requested card. For IPGWx applications, the SCM software will now calculate the sum of the **CHG-SG-OPTS** command parameters :**SRKQ** and :**DRKQ** to see if the total is over 1000.

If the sum is over 1000 and the IPGWx application board is a DCM, the card will be *automatically inhibited*, and the alarm message Insufficient memory for provisioning will be displayed. When a DCM IPGWx card is auto-inhibited, it will remain inhibited, unless the following sequence of events occurs.

- The number of routing keys on all IPGWx applications must be reduced to 1000 or less.
- Once the number of routing keys is reduced to 1000, the **CHG-SG-OPTS** command must be issued such that drkq + srkq <= 1000.
- The inhibited IPGWx card must be manually allowed.

Hardware Requirements

This feature requires the SSEDCM-based IPGWx GPLs (870-2372-xx).

40,000 GTT Capacity (Release 28.0) (IP^7 Release 6.0)

The EAGLE currently supports a maximum of 20,400 GTT/sec/system. For many customers, this GTT capacity is insufficient. This is especially true for customers who use a single node, or a single pair of nodes, to centralize GTT for their entire network. This feature allows the EAGLE to process a minimum of 40,800 GTT/sec/system.

The 40,000 GTT Capacity feature assumes the use of DSM cards for GTT functionality.

For more information on the GTT feature, refer to the *Database Administration Manual - Features*.

4000 Routesets (Release 23.0)

This feature increases the size of the routing table in the EAGLE database from 2000 entries to 4000 entries. With this feature turned on, the user can configure up to 4000 routesets in the database. The EAGLE requires that the destination point code of each routeset be entered in the database. So to enter 4000 routesets in the database, 4000 destination point codes must be entered in the database. The size of the destination point code table has been increased from 2000 destination point codes to 4000 destination point codes.

The 4000 routeset feature is activated using the **chg-feat** command. A new parameter, **DSTN4000**, has been added to the **chg-feat** command to turn the 4000 routeset feature on. Before the **chg-feat** command can be executed, the link interface modules (LIMs), both low-speed and high-speed, must have the proper memory installed.

All link interface modules (LIMs) running the **ss7ansi**, **ss7gx25**, and **ccs7itu** applications, the low-speed LIMs, must be equipped with one dual inline memory module (DIMM), containing 4 Mbytes of static RAM. All LIMATMs, the link interface module used for the high-speed ATM signaling link, must be equipped with two DIMMs providing a total of 8 Mbytes of memory. This additional memory is required so that the larger routing table can be downloaded to each LIM.

If the **DSTN4000** parameter is specified with the **chg-feat** command and even one LIM does not have the proper memory installed, the **chg-feat** command is rejected with this message, and the 4000 routeset feature will not be turned on:

48 Million Numbers (Release 27.0)

Overview

The 48 Million Number feature for EAGLE Release 27.0 provides the capability to expand the number of ported numbers supported on one EAGLE platform from 12 to 48 million numbers. This feature represents both an increase in the number of ported records a single EAGLE node can support and a re-architecture of the current LNP solution (i.e. the LSMS-OAP-OAM LNP interface) for increased database update performance.

The terms MPS and ELAP are used to describe the hardware and software that is replacing the EOAP and the LNP functions of the OAM. MPS refers to the hardware and OS software of the new platform. ELAP refers to the 48 million number application running on the MPS.

This feature is optional and requires a corresponding LSMS feature.

General Description

Customer databases of Local Number Portability (LNP) data are constantly growing. EAGLE Release 27.0 and LSMS Release 4.0 introduce the 48 Million Number feature to satisfy customer database size requirements. Because of the magnitude of the database size increase, several areas of the existing EAGLE/LNP architecture have been upgraded. The following functionality has been changed and improved for Release 27.0:

- Ownership of the "master" or "golden" real-time LNP database has moved from the EAGLE OAM to the ELAP.

  The data model for the new LNP solution closely resembles that of the International LNP solution. Data is collected at the LSMS from the NPAC (for subscription data) and from local provisioning on the LSMS (for default NPANXX, split NPANXX and other types of LNP records). This data is sent to the active ELAP at an EAGLE running Release 27.0 across a TCP/IP connection in the customer's network. The ELAP stores the data locally, and replicates it to the mate ELAP. The ELAP provides real-time database loading and provisioning functions for the EAGLE DSM cards, using two dedicated Ethernet networks between the MPS System and the EAGLE DSM cards.

  When the 48 Million Number feature is enabled, this new data model supersedes the existing EAGLE LNP model. The EAGLE OAM will not store LNP databases in Release 27.0. Also eliminated with the 48 Million Number feature are the BLM and DCM cards that previously were required to support EBD&A.

- The transmission rate of database updates from the LSMS to the EAGLE has increased from 2 TN/sec to 25 TN/sec.

  Prior to Release 27.0, LNP updates were sent from the LSMS to the OAP over the customer's network. The minimum OAP hardware in the field today runs on an 85MHz Sparc-4 platform. The OAP translates the data from the LSMS to character based commands resembling SEAS UPL commands for LNP. These commands are sent across a dedicated serial link to an EAGLE terminal port at 19,200 Kpbs. The command is then parsed and validated by the EAGLE before the real-time database is updated. Real-time updates are sent to SCCP cards serially using a card list.

  With Release 27.0, the 48 Million Number feature provides a much faster path for updates. LNP updates are sent from the LSMS to the ELAP over the customer's network. The ELAP performs minimal parsing and validation before updating the real-time database. Real-time updates are sent to the EAGLE DSMs in parallel using multicast technology.

- Enhanced Bulk Download and Audit (EBD&A) is supported directly by the ELAP.

The ELAP now provides all of the functionality of EBD&A.

- All cartridge-based bulk download operations have been eliminated.

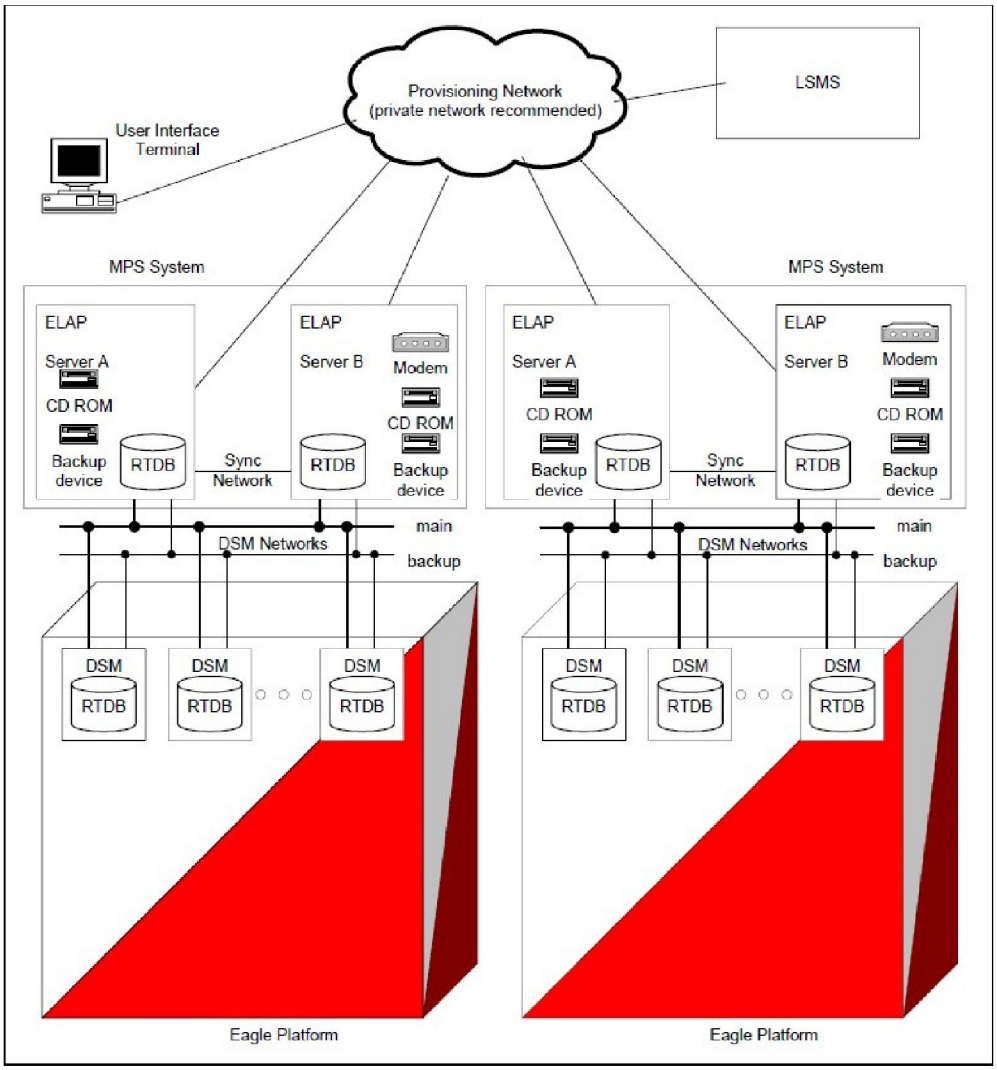
  Bulk loading is accomplished using the EBD&A functionality provided by the ELAP. Since EAGLE will not store the real-time database on disk, a cartridge based bulk load is no longer necessary.

- Real-time databases are recovered from one of the mate EAGLE's ELAPs in a disaster situation (ELAP failure at one EAGLE).

  In the unlikely event of a catastrophic failure of the complete MPS system at one EAGLE, resulting in the loss of the real-time database, it will be possible to copy the data from one of the MPS servers of the mated EAGLE node. After the MPS fault has been corrected, a craftsperson may gain access to it via a modem or through the customer's network. It will then be possible to initiate a connection to one of the MPS servers at the mate EAGLE site and initiate a transfer of the real-time database.

- The EAGLE security log functionality has been moved to the ELAP.

The following figure shows the system architecture supporting the 48 Million Number feature.



Attached to each EAGLE is an MPS System, consisting of two MPS Servers (Server A and B) and their associated platform software (e.g., Operating System, DBMS, etc.). The servers in the MPS System execute the software developed for the 48 Million Number feature, which is referred to as the "ELAP software."

Throughout the remainder of this description, when the term "ELAP" is used, it means "the ELAP software running on an MPS Server." Thus when we say that there are two ELAPs attached to each EAGLE, we mean that there are two MPS Servers attached to each EAGLE, both of which are running the ELAP software. These two ELAPs run in a mated-pair configuration, with one behaving as the "active ELAP" and the other as the "standby ELAP."

System-Level Requirements

When the 48 million number feature bit is on, the following attributes of the EAGLE change:

- OAM-based LNP commands are not be allowed (**`tt-serv`** is allowed).
- MPS-based LNP commands are allowed (**`rtrv-`** commands only).
- Enhanced Bulk Download (EBDA) functionality is implicitly inherited by the new architecture

The 48 million number architecture inherits all functionality of the 12 million number architecture (except for a separate bulkdownload component). This includes:

- Support DN to LRN mapping and up to six services for message relay. CLASS,LIDB,ISVM and CNAM message relay service are supported. (Customer-defined services are supported.)
- Support AIN/IN, IS-41 and PCS 1900 LNP query/response.
- Support Measurements (OAM can retain LNP Measurements).
- Support Transaction Log for LNP updates.
- Support for MPS alarming via EAGLE terminal.
- Support warm restart/incremental loading of the DSM card.
- Support loading the DSM card.
- Support Warm/Cold Restart of the DSM card
- Database storage of the LNP data from the LSMS.

  NOTE: The MPS architecture supports a real-time database only

- LNP Commands (**`tt-serv`** and **`rtrv-`** only)

There is one security log on the ELAP. The security log on the ELAP logs global (across all DSM cards) LNP updates as one entry, regardless of the number of DSM's provisioned. However, actions taken for a specific DSM card by the ELAP are logged on a per-DSM card basis.

The 48 million number architecture does not preclude the operation of the mate STP with the 12 million number architecture.

Required Hardware

To support 48 Million Numbers feature and the increased download rate from the NPAC/LSMS, the following new hardware is being introduced:

DSM

The Database Services Module (DSM) supports 48 million numbers by providing 1 GB daughterboard memory increments up to a total of 4GB. The DSM also provides TCP/IP connectivity directly to the MPS.

Table 2-1. Supported DSM Configurations

Name	Description	Maximum number of ported numbers supported
DSM1GB	DSM with 1GB populated memory	12,000,000
DSM2GB	DSM with 2GB populated memory	24,000,000
DSM3GB	DSM with 3GB populated memory	36,000,000
DSM4GB	DSM with 4GB populated memory	48,000,000

The DSM does not support the **`alloc-mem`** command to allocate daughterboard memory. Instead, the memory physically present on the board determines the number of ported records supported.

MPS

The Multi-Purpose Server (MPS) running the ELAP application is designed as a replacement not only for the LNP functionality contained in the EOAP, but also for the LNP database that currently resides on the OAM. The MPS fits into one general purpose frame (GPF).

Upgrade Considerations

ELAP

ELAP software is new software. All initial applications of this feature will be new installations. Future software upgrades will be addressed with the Solaris "pkgadd" utility. The following data must be preserved or re-generated for upgrade:

- Data configured through the user interface
- Security logs
- Data provisioned from the LSMS

Each of these must be addressed by any future upgrade.

Maintenance

Three upgrade considerations affect maintenance:

- Support the EPAP alarms defined in Release 26.05 and 26.1 during upgrade. This must be done for both UAMs and the **`rept-stat-mps`** output.

- Allow TSM cards to co-exist with DSM cards and support the output in all **rept-stat** reports.
- Allow for the conversion of DSMs from DSM operation to TSM operation via a database restore operation.

Measurements

Measurements data are not preserved from a prior release to the upgrade release during an upgrade. If the customer desires to retain a record of pre-upgrade measurements, a hardcopy of the measurements data can be obtained using the documented LNP measurement report procedures. Alternatively, measurements data can be copied to a Measurements removable cartridge using the **copy-meas** command. The data is then available for offline (non-EAGLE) processing. Measurements data cannot be restored to the upgraded EAGLE due to potential changes in data formats as a result of the upgrade.

LNP Measurements are preserved when the **LNP48MIL** feature bit is enabled after upgrade.

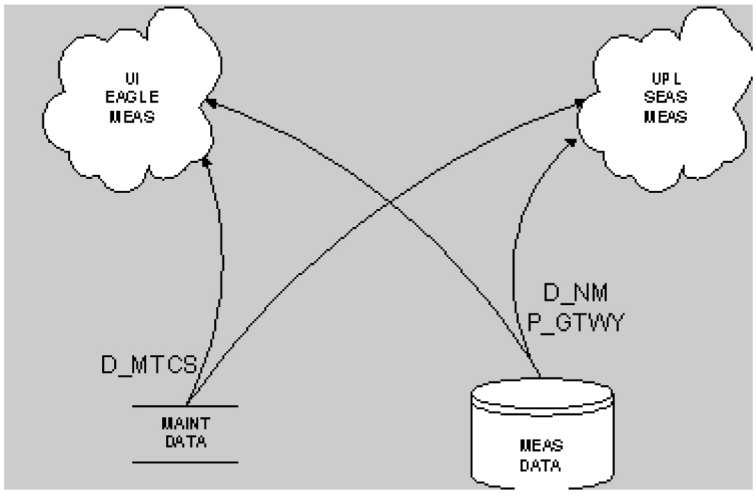
5 Minute Linkset Data (Release 25.0)

Release 25.0 adds two new schedules to the EAGLE reporting capabilities: D_NM and D_MTCS. Both schedules are available through the EAGLE terminal interface, and through the SEAS interface via the OAP.

The following figure provides a high-level diagram of the capabilities implemented by these new schedules. The D_MTCS schedule is a new capability for generating an on-demand maintenance status report using the **rept-meas** command (EAGLE) or the **send-dem-meas** command (SEAS). The report is generated from maintenance block data that is currently maintained within the OAM.

D_NM is a five-minute linkset schedule and supports the **lnkset** entity type. D_MTCS is a snapshot of the maintenance status indicators, and supports the **link** and **lnkset** entity types.

Figure 2-2. Concept Diagram



The D_NM schedule provides five-minute throughput measurements on a per-linkset basis, on demand. The schedule is available through the EAGLE HMI or the SEAS interface. Although the reporting of the D_NM schedule is new for Release 25.0, the mechanisms for collecting the data contained in the schedule are currently implemented in the EAGLE for link data collection. This feature reorganizes the link data collection to collect on a linkset basis. The linkset measurements are aggregated in a new data store over a five-minute period, and reported in the D_NM schedule. This feature does not impact per-link measurements data reporting.

The D_MTCS schedule provides the current maintenance state (active, out-of-service, or unavailable) of signaling links and linksets. The D_MTCS schedule is available on demand via the **rept-meas** command through the EAGLE HMI, or via the **send-dem-meas** command through the SEAS interface. Both interfaces support a parameter to specify reporting current data (**period=active**) for a link or linkset.

50,000 GTT Capacity (Release 35.1)

Description

The 50,000 GTT Capacity featur increases the GTT processing capability of EAGLE 5 ISS GTT-only nodes from 40,800 TPS to 52,700 TPS through the use of 32 DSMs per node (31 active and 1 for +1 redundancy), each running at 1700 TPS per card (31 x 1700 = 52,700).

Hardware Requirements

The 50,000 GTT Capacity feature requires 32 DSM cards exclusively for GTT functionality.

Limitations

The 50,000 GTT Capacity feature has the following limitations:

- The LNP, G-Flex, G-Port, INP, or EIR features cannot be activated if there are more than 25 DSM cards in the system. Therefore, these features are not supported in conjunction with the 50,000 GTT Capacity feature.
- The maximum number of SCCP cards allowed in a single EAGLE 5 ISS node is 32 (to provide n+1 functionality). 32 DSM cards are required to achieve 52,700 TPS: therefore, if any TSM cards are in the system, the total TPS rate will be less than the system maximum.
- The 50,000 GTT Capacity feature is not available on systems that are equipped with MPS.

5000 Routes (Release 26.1)

Some customers with large network configurations require more than 4000 routes, due to the expansion of link capability and/or collapsing networks. This feature is a continuation of route expansion for the EAGLE platform, and is intended to replace the 4000 route feature.

The maximum number of administered routes supported in the EAGLE STP has been increased from 4000 to 5000 as a system-wide option. The minimum number of x-list entries remains 500.

The EAGLE STP now supports, as a system-wide option, the administration and protocol changes required to support 5000 routes. The default for the routing option remains 2000 routes, and 500 x-list entries. No change in x-list capacity is required. Total routes table capacity is 5500 entries.

500 SS7 Links (Release 21.0)

In Release 21.0, the maximum number of SS7 signaling links the EAGLE can contain is being increased from 268 to 500. For the EAGLE to contain 500 SS7 signaling links (a maximum of 250 LIMs), the system configuration

has been increased from 3 frames to 6 frames. Each frame can contain 3 shelves, with the exception of the last frame which can contain only 1 shelf, for a maximum of 16 shelves. The numbering of the shelves is 1100 to 6100. This provides card location numbers from 1101 to 6118. Also in Release 21.0, card locations 1111 and 1112 are also configurable in the database. The following table shows the new numbering scheme for card locations.

Table 2-2. Release 21.0 Card Location Numbering Scheme

	Shelf 1	Shelf 2	Shelf 3
Frame 1	1101 - 1108, 1111 - 1118	1201 - 1208, 1211 - 1218	1301 - 1308, 1311 - 1318
Frame 2	2101 - 2108, 2111 - 2118	2201 - 2208, 2211 - 2218	3201 - 3208, 3211 - 3218
Frame 3	3101 - 3108, 3111 - 3118	2301 - 2308, 2311 - 2318	3301 - 3308, 3311 - 3318
Frame 4	4101 - 4108, 4111 - 4118	4201 - 4208, 4211 - 4218	4301 - 4308, 4311 - 4318
Frame 5	5101 - 5108, 5111 - 5118	5201 - 5208, 5211 - 5218	5301 - 5308, 5311 - 5318
Frame 6	6101 - 6108, 6111 - 6118	Not Equipped	Not Equipped

As a result of the change in the system configuration, the range of values specified for any command that uses the card location or the shelf location as a parameter (the **loc** parameter) have been changed. These commands are:

act-dlk	**act-file-trns**	**act-lpo**	**act-slk**
alw-card	**alw-slk**	**blk-slk**	**canc-dlk**
canc-lpo	**canc-slk**	**cdu**	**chg-bip-fld**
chg-bip-rec	**chg-x25-rte**	**chg-x25-slk**	**conn-imt**
dact-slk	**disc-imt**	**disp-bip**	**disp-bp**
disp-disk-dir	**disp-fta-dir**	**disp-lba**	**disp-mem**
dlt-bp	**dlt-card**	**dlt-dlk**	**dlt-fta**
dlt-ip-node	**dlt-shlf**	**dlt-slk**	**ent-bp**
ent-card	**ent-dlk**	**ent-ip-node**	**ent-shlf**
ent-slk	**ent-x25-rte**	**inh-card**	**inh-slk**
init-card	**rept-meas**	**rept-stat-card**	**rept-stat-db**
rept-stat-dlk	**rept-stat-slk**	**rept-x25-meas**	**rmv-card**
rst-card	**rtrv-bip**	**rtrv-card**	**rtrv-dlk**
rtrv-ip-node	**rtrv-obit**	**rtrv-shlf**	**rtrv-slk**
rtrv-trbl	**rtrv-x25-rte**	**rtrv-x25-slk**	**send-msg**
set-mem	**tst-bip**	**tst-dlk**	**tst-slk**
ublk-slk	**unhb-slk**		

If the EAGLE is using the gateway screening, global title translation, X.25 gateway, or STP LAN features, the card requirements to support these features will reduce the maximum number of SS7 signaling links the EAGLE can contain. The card requirements for these features are:

- For the gateway screening feature, the EAGLE can contain a maximum of 8 ASMs running the **gls** application.
- For the global title translation feature, the EAGLE can contain a maximum of 25 ASMs running the **sccp** application.
- There can only be one X.25 signaling link assigned to a LIM.
- For the STP LAN feature, the EAGLE can contain a maximum of 20 ACMs.

56 Million G-Flex Entries (Release 29.1) (IP7 Release 7.1)

Description

The 56 Million G-Flex Entries feature is a product of the 18GB (P/N 804-1282-01) to 36GB disk (P/N 804-1548-01) hard drive upgrade; see 18 GB to 36 GB Hard Drive Upgrade (Release 29.1) (IP7 Release 7.1) . As a result of this increased storage capacity, the existing EPAP and EAGLE software now can support 56 Million G-Flex entries.

Hardware Requirements

This feature requires the 36 GB disk hard drive (P/N 804-1548-01).

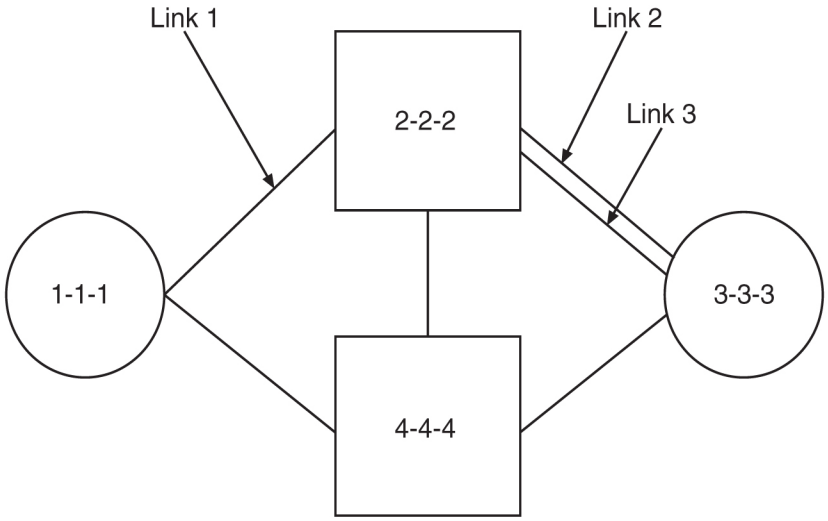
5-8 Bit Sequencing Assurance (Release 24.0)

Description

The signaling link selection field (SLS) in an MSU is used to balance traffic across the links in each linkset that a message passes through. The originator of the traffic can, by using the same SLS for a group of messages, guarantee that the same links are selected and guarantee that the traffic will be in sequence. In previous releases, the EAGLE evenly distributed traffic using a 5-bit SLS by using a 3-bit counter to fill in the three most significant bits in the SLS. This can result in missequencing of MSUs, as shown in the following example and figure:

1. Node 1-1-1 generates two messages with the same SLS, intending for them to be sequenced, and transmits them across link 1.
2. STP 2-2-2 converts the 5-bit SLS to an 8-bit SLS, resulting in two different SLS codes. The two messages leave STP 2-2-2 on links 2 and 3 and arrive out of order at node 3-3-3.

Figure 2-3. Example Network for Problem Description



This feature ensures that when a 5-bit SLS is converted to an 8-bit SLS, the MSUs arrive at the destination node in the order that they were generated by the originating node. The EAGLE also makes these SLS conversions:

- 5-bit ANSI SLS to 4-bit ITU SLS
- 4-bit ITU SLS to 5-bit ANSI SLS
- 8-bit ANSI SLS to 4-bit ITU SLS

The EAGLE does not convert a 4-bit ITU SLS to an 8-bit ANSI SLS.

The 5-bit to 8-bit SLS conversion takes place during the routing process, after the linkset is selected, but before the signaling link is selected. The ITU to ANSI SLS conversion takes place during the ANSI to ITU MSU conversion and after the outgoing signaling link is chosen.

Signaling Link Selection Conversion

5-bit to 8-bit SLS conversion is performed under these conditions:

- The incoming linkset is an ANSI linkset
- The **asl8=no** parameter is assigned to the incoming linkset
- The outgoing linkset is an ANSI linkset
- The outgoing linkset has either the **slscnv=on** and **slsci=yes** parameters, or the **slscnv=perls** and **slsci=yes** parameters assigned to it
- The three most significant bits of the SLS are zero.

When an ITU SLS is converted to an ANSI SLS, the ITU SLS is always converted to an ANSI 5-bit SLS. If the MSU containing the converted SLS is rerouted because of a link outage, the SLS may be converted from a 5-bit SLS to an 8-bit SLS.

When an ANSI SLS is converted to an ITU SLS, the ANSI SLS is always converted to an ITU 4-bit SLS.

When a 5-bit ANSI SLS is converted to an 8-bit ANSI SLS, the three most significant bits of the SLS are set using a function of originating point code and incoming port. This ensures that MSUs with the same originating point code, SLS, and incoming port will always have the same SLS after the conversion, guaranteeing that the MSUs arrive at the destination in the same sequence that they were sent.

All ANSI MSUs originating from the EAGLE will have an 8-bit SLS.

6000 Routesets (Release 29.0)

Description

The 6000 Routesets feature expands the SS7 routing connectivity between the EAGLE and other nodes by increasing the number of routesets supported by the EAGLE. This allows for the EAGLE to function in larger SS7 networks.

The functionality of this feature applies to all LIM types except LIMs running the GX25 GPL, which will continue to utilize the X.25 2000 Routeset feature. However, the increased 6000 SS7 routeset table will also be downloaded on GX25 card.

NOTE: There is a feature access key for the 6000 Routeset feature. It can not be activated unless the 5000 routeset feature bit is ON and the active and standby OAM is a GPSM-II running the EOAM GPL.

Hardware Requirements

This feature requires the GPSM-II in the active and standby OAM slot, and a TDM change (870-0774-10 or later).

CAUTION: Never install or initialize MCAP cards in MASP slots 1113 and 1115 after features that require GPSM-II cards are provisioned. Attempting to initialize MCAP cards with GPSM-II features provisioned will cause a system outage. Before replacing an existing GPSM-II card in a MASP slot (1113 and 1115) contact Tekelec Customer Service.

65,535 Entries per Translation Type (Release 22.0)

This feature improves the performance of the global title translation subsystem of the EAGLE to these levels.

- 850 messages per second
- 21,000 global title translations per second per system
- 65,536 entries per translation type

There is no mechanism to limit the number of global title translation entries to less than 65,537 per translation type. The maximum number of entries in the global title translation table has not changed and is still 270,000 entries. It is possible to enter all 270,000 entries under one translation type. The performance of the global title translation subsystem is not guaranteed when more than 65,536 translations are entered for a single translation type.

The **rtrv-gtt** command output has been changed to show the capacity of the global title translation table is as a percentage of the total number of entries in the system (270,000 entries).

8-Bit SLS Support (Release 21.0)

The signaling link selection (SLS) is a field in the routing label of the MSU. It is set by the originator of the MSU to a random value. It is used by EAGLE to pick which outgoing linkset and signaling link to use. MSUs with the same destination and the same SLS take the same path through the network, the same linksets and the same links. The MSUs are guaranteed to arrive at the destination in sequence.

The value of the SLS is used by the EAGLE to distribute traffic over the available signaling links in a linkset. The EAGLE uses only 16 SLS codes for assignment to linksets or combined linksets. For linksets containing 9 to 15 signaling links, some signaling links are assigned two SLS codes while other signaling links are assigned a single SLS code. This can create an imbalance in traffic distribution and inefficient link utilization. To overcome this problem, the EAGLE uses an 8 bit SLS code which provides the EAGLE with 256 SLS codes. More SLS codes means the traffic can be distributed more evenly.

Because some signaling points will still be generating messages with a 5 bit SLS, the EAGLE provides an option to convert 5 bit SLSs in messages to 8 bit SLSs. This option is set on an outgoing linkset basis. ITU messages continue to use 4 bit SLSs. Messages that go from ITU to ANSI are currently converted from a 4 bit SLS to a 5 bit SLS. If the outgoing linkset uses 5 to 8 bit conversion, the ITU messages are converted to 8 bit SLSs. If the linkset does not use 5 to 8 bit conversion, the ITU messages are converted from 4 bit to 5 bit SLS.

MSUs generated by the EAGLE (MTP management, SCCP management, and messages received from X25) will have an 8 bit SLS.

The **slsci** parameter, used with either the **ent-ls** or **chg-ls** commands, indicates whether the 5 bit to 8 bit SLS conversion feature is used to select signaling links for outgoing messages directed to the specified linkset. If the **slsci=yes** parameter is specified, the EAGLE replaces any 5 bit SLS value contained in received messages with a random 8 bit value before they are used by the EAGLE to select the outgoing signaling link in that linkset. The **slsci=yes** parameter can only be specified for linksets with ANSI SS7 adjacent point codes.

8,000 Routesets (Releases 31.8, 34.0)

Description

The 8,000 Routesets feature expands the SS7 routing connectivity between the EAGLE 5 ISS and other nodes by increasing the number of routesets supported by EAGLE 5 ISS from 6000 to 8000. This feature can be viewed as an extension to the 6000 Routesets feature, which expanded the EAGLE 5 ISS routesets from 5000 to 6000.

A Feature Access Key (FAK) allows the customer to set the routeset limit to either 7000 or 8000. With the exception of a routeset provisioning limit imposed by the 7000 FAK, the 7000 Routeset and 8000 Routeset implementations are identical.

Limitations

If the customer has more than 8000 aliases provisioned, then the 7000 or 8000 Routesets feature cannot be enabled. Aliases must be deleted from the system until the 8000 alias limit is met.

Hardware Requirements

The 8000 Routesets feature permits customers to add additional routesets without requiring hardware change.

Additional Integrated Sentinel Support (Release 28.2)

Description

This feature adds the following EAGLE cards to those supported by the EAGLE with Integrated Sentinel Feature introduced in EAGLE Release 28.0. Sentinel 8.1 supports monitoring for links on E1-ATM and LIM-ATM cards, and supports SS STC cards for monitoring:

- E1-ATM - With Release 28.2, the EAGLE supports Integrated Sentinel functionality for the E1-ATM card.
- LIM-ATM - With Release 28.2, the EAGLE supports Integrated Sentinel functionality for the LIM-ATM card.
- SS STC - With Release 28.2, the EAGLE supports the existing Sentinel routing functionality (EROUTE GPL) on a SS STC card.

New Hardware Required

No new hardware is required for this feature. Note, however, that the EAGLE with Integrated Sentinel feature does require the use of GPSM-II cards in place of MCAP cards, and HMUX cards in place of IPMX cards. Also, the EAGLE Time Synchronization feature must be active in conjunction with this feature. In addition, the timing requirements include the use of an external Bits clock.

CAUTION: Never install or initialize MCAP cards in MASP slots 1113 and 1115 after features that require GPSM-II cards are provisioned. Attempting to initialize MCAP cards with GPSM-II features provisioned will cause a system outage. Before replacing an existing GPSM-II card in a MASP slot (1113 and 1115) contact Tekelec Customer Service.

Administrable SLTMs (Release 20.0)

This feature allows the user to configure signaling link test messages (SLTMs). To test the coherency of a particular link, two signaling points can transmit periodic test messages. The signaling point initiating the test selects a link to test and then transmits an SLTM containing a test pattern. The other signaling point responds with an echo of the test pattern contained in the SLTM. The intervals between transmission of signal link test messages (SLTMs) are controlled by the sltm_enabled field in a corresponding SLTM table record. The SLTM table record also controls the following:

- the length of the test pattern in the SLTM
- automatic generation of SLTMs
- generation of periodic SLTMs when a link is put in service

The SLTMs can be sent to a signaling link that is in service whenever desired.

AINF Applique (Release 21.0)

The AINF is an integrated applique which supports the DSOA, DSCS and V.35 interfaces on the same applique. The AINF applique can be configured as either a DSOA, OCU, or V.35 interface from the user terminal.

Alarm Enhancements (Release 26.0)

NOTE: This is an engineering feature.

Currently, adding new UAMs to the system requires many modifications to the software. It requires adding ATH events, adding fields to the maintenance block (MB), changing ATH on the application card to set the new field in the MB, possibly updating the MB revision, and changing SCM to analyze the new field and generate the UAM.

Application Defined UAMs allow the application card to generate UAMs without modifying the OAM build. Initially, this capability will be given to every application using the Generic Maintenance Block. The application will then only be required to supply a message reference number (MRN), an output group, a device type, and element information (example: port number) to the Application Defined UAM software.

There will only be one Application Defined UAM allowed per card in the EAGLE. That is, only one Application Defined UAM may be active at any given time. Multiple Application Defined UAMs may be defined and sent by the application, but not simultaneously. There is only one slot in the MB for Application Defined UAM.

Allow a Mated Application to Work as Primary-Secondary and Secondary-Primary (Release 22.0)

There are two ways to load share global title translations.

1. A mated application in load shared mode.

2. Two mate applications in dominant mode. The global title translation addresses are split into two ranges such that half of the addresses translate to one mated application and the other half translates to the other.

This feature supports the second method of load sharing. This method of load sharing allows two replicated applications to load share and back each other up in the event of a network failure. Global title translation is load shared by splitting the range of global title addresses and have them work as two separate mated applications. If one application becomes prohibited, SCCP routing translates all the GTT messages in both address ranges to the mated application. The subsystem management messages (SBR/SNR) and SCCP management messages (SSP/SSA) are sent to the adjacent mated application and concerned signaling points.

The following example illustrates how this feature works using a split global title address range.

1. Enter two mated applications as a dominant point code/subsystem pair. In this example, mated application A is point code 001-001-001, **ssn** 10. Mated application B is point code 001-001-002, **ssn** 10.

   Input Example

```
ent-map:pc=001-001-001:ssn=10:mpc=001-001-002:mssn=10 :mult=dom:adj=yes
```

This mated application pair entered as A backed up by B, automatically creates an entry of B backed up by A. Either the primary or the backup point code and subsystem can be used as the preferred destination for a global title translation range. The other point code/subsystem is treated as the backup.

2. To split the global title ranges, enter two global title translation address ranges. One range uses mated application A and the other uses mated application B.

   Input Examples

```
ent-gtt:type=10:gta=800000:egta=800555:xlat=dpcssn:ri=ssn :pc=001-001-001:ssn=10
ent-gtt:type=10:gta=800556:egta=800999:xlat=dpcssn:ri=ssn :pc=001-001-002:ssn=10
```

   If mated application A becomes unavailable, all global title translation traffic for both address ranges is routed to mated application B. If mated application B becomes unavailable, the specified global title translation traffic is routed to mated application A. If both point code/subsystem pairs are available, the traffic is split according to the translation type and address ranges specified. Normally, the address range is split so that mated application A receives half the translated global title translation traffic and mated application B receives the other half.

   The adjacency, concerned signaling point code group, message routing under congestion and subsystem routing parameters in the **`ent-map`** command apply to both point code/subsystem pairs.

   The table shows how SCCP routing and subsystem management is handled according to the mated application parameters **`adj`** (adjacency), **`srm`** (subsystem routing messages), and **`mrc`** (message routing under congestion).

Table 2-3. SCCP Routing and SCCP Management Actions for a Primary-Secondary and Secondary-Primary Mated Application

Event	ADJ	SRM	MRC	SCCP Routing and SCCP Management Action
Preferred application fails because an MTP_PAUSE message for its point code has been received	yes	yes	yes or no	1. Send an SBR message to the next preferred application. 2. Reroute traffic to the next preferred application.
	no	yes	yes or no	1. Do not send an SBR message to the next preferred application. 2. Reroute traffic to next the preferred application.
	yes or no	no	yes or no	
Previously prohibited preferred application becomes available because an MTP_RESUME message for its point code has been received	yes	yes	yes or no	1. Send an SNR message to the next preferred application. 2. Route traffic back to the preferred application.
	no	yes	yes or no	1. Do not send an SNR message to the next preferred application. 2. Route traffic back to the preferred application.
	yes or no	no	yes or no	
Receive an SSP for the preferred application that is allowed.	yes	yes	yes or no	1. Send an SBR message to next the preferred application. 2. If the SSP came from the affected point code, broadcast SSP's to the list of concerned signaling point codes.

Event	ADJ	SRM	MRC	SCCP Routing and SCCP Management Action
				3. Reroute traffic to the next preferred application.
	no	yes	yes or no	1. Do not send an SBR message to the next preferred application. 2. Send SSP's to the list of concerned signaling point codes. 3. Reroute traffic to the next preferred application.
	yes or no	no	yes or no	
Receive an SSA for the preferred application that is prohibited.	yes	yes	yes or no	1. Send an SNR message to the next preferred application. 2. Send SSA's to the list of concerned signaling points. 3. Reroute traffic to the next preferred application.
	no	yes	yes or no	1. Do not send an SNR message to next preferred application. 2. Send SSA's to the list of concerned signaling points. 3. Reroute traffic to the next preferred application.
	yes or no	no	yes or no	
Preferred application becomes congested.	yes or no	yes or no	no	1. Do not reroute messages to the next preferred application.

Allowed Affected Destination Field Screen (Release 22.0)

Release 22.0 introduces a new gateway screening entity, the Allowed Affected Destination Field. The Allowed Affected Destination Field contains the affected destination point code of incoming MTP network management messages. This is also referred to as the concerned point code.

The current method of screening the affected point code in network management messages involves a check for the point code in the routing table, self point codes, and capability point codes. This check is applied after the message has passed all screenings in the configured screen set. This check is independent of the screen set. In order to provide the same capability as currently exists, this method of screening for the affected point code in network management messages is retained. The network management message can also be screened with gateway screening screensets. To screen the network management message with the existing capability, the **`destfld`** parameter with either the **`ent-scrset`** or **`chg-scrset`** command (a new parameter introduced in Release 22.0) must be set to **`yes`**.

If the **`destfld=yes`** parameter is specified, all MSU's with the service indicator of 0 (**`:si=0`**), including through switched messages, are screened by gateway screening against the routing table, self point codes, and capability point codes. This screening step is performed after the MSU has passed all other screening tables.

The advantage of using the configured Allowed Affected Destination Field screening table over the routing table is that it is now possible to reject messages containing point codes in the routing table. Previously, if a network management message concerned a point code in the routing table, it would pass this phase of screening and there was no way to prevent its entry into the network. An interconnecting network could then either accidentally or maliciously send a network management message for a destination in the home network.

The network management messages that require screening by the Allowed Affected Destination Field screen are:

- TFP, TFA, TFR
- TCP, TCA, TCR
- TFC
- UPU
- SRST (RSP, RSR)

All other network management messages are passed.

For cluster messages (TCP, TCA, and TCR), the member of the affected destination field is set to 0. If the affected cluster contains a point code with a member 0, the affected destination field for a TFx message for the member and a TCx message for the cluster will have the same affected destination. For example, a TFP concerning point code 007-007-000 and a TCP concerning cluster point code 007-007-* will both have an affected destination of 007-007-000. Typically, a user would provision an entry in the allowed affected destination field with these parameters, **:ni=007**, **:nc=007**, **:ncm=*,** all TFx messages concerning the member of the cluster and all TCx messages concerning the cluster are passed. If the user wants to screen TFx messages and TCx messages separately, the allowed SIO screen can be used to send TCx messages to one affected destination table, and send TFx messages to a different affected destination table.

The allowed affected destination field screen is configured with these commands.

- **ent-scr-destfld** - adding a new allowed affected destination field entry into the database
- **dlt-scr-destfld** - removing an allowed affected destination field entry from the database
- **chg-scr-destfld** - changing an existing allowed affected destination field entry in the database
- **rtrv-scr-destfld** - displaying the allowed affected destination field entries in the database

All these commands use these parameters.

- **sr** for the screening reference name of the allowed affected destination field screen
- **ni**, **nc**, **ncm** for ANSI point codes
- **zone**, **area**, **id** for ITU international point codes
- **npc** for ITU national point codes

The **chg-scr-destfld** command also uses these parameters for the point code values being changed.

- **nni**, **nnc**, **nncm** for new ANSI point code values
- **nzone**, **narea**, **nid** for new ITU international point code values
- **nnpc** for new ITU national point code values

The **rtrv-scr-destfld** command also uses the **all=yes** parameter to display a detailed output of the allowed affected destination field screen. The following is an example of the output of the **rtrv-scr-destfld:all=yes** command.

Output Example:

```
RLGHNCXA03W 97-06-07 13:14:18 EDT Rel 22.0.0
SCREEN = ALLOWED DESTFLD
SR    NI       NC       NCM      NSFI   NSR/ACT
IEC   240      001      010      STOP   -, -
IEC   241      010      *        STOP   -, -
SR    ZONE     AREA     ID       NSFI   NSR/ACT
IEC   1        003      4        STOP   -, -
IEC   1        003      5        STOP   -, -
SR    NPC                       NSFI   NSR/ACT
IEC   00235                     STOP   -, -
IEC   00240                     STOP   -, -
```

The allowed affected destination field screen can be referenced, the next screening function indicator (NSFI), by the allowed SIO, allowed DPC, and blocked DPC screens. If the allowed affected destination field screen is the NSFI of the allowed SIO screen, the service indicator of the allowed SIO entry must be 0, specified by the **:si=0** parameter with the **ent-scr-sio** and **chg-scr-sio** commands, and the entry **0** in the SI field in the **rtrv-scr-sio** command output.

The NSFI for the allowed affected destination field screen has only one value, STOP.

The redirect and copy functions, for the STP LAN and DTA features, (**:redirect=yes** and **:copy=yes** parameters with the **ent-scr-destfld**, **chg-scr-destfld**, and **rtrv-scr-destfld** commands) can be used with the allowed affected destination field screen.

Allowed CDPA Screen on SCCP Management Format ID (Release 22.0)

The allowed called party address (CDPA) screen can screen messages for the SCMG format ID (SCCP Management Format ID). A new parameter, **scmgid**, has been added to the **ent-scr-cdpa**, **dlt-scr-cdpa**, and **chg-scr-cdpa** commands to configure the allowed CDPA screen to screen for the SCMG format ID. A new field, SCMGID, has been added to the output of the **rtrv-scr-cdpa** command to show the SCMG format ID in the allowed CDPA screen. The following is an example of the new output.

Output Example:

```
RLGHNCXA03W 97-06-07 15:41:38 EDT Rel 22.0.0
SCREEN = ALLOWED CDPA
SR    NI       NC       NCM      SSN      SCMGID   NSFI    NSR/ACT
IEC   240      001      010      001      002      STOP    -, -
IEC   240      001      011      002      ------   STOP    -, -
IEC   240      001      010      12       ------   STOP    -, -
IEC   241      010      *        *        ------   AFTPC   IAFT
```

The value for the **scmgid** parameter is 1 - 255 or *. This parameter must be specified if the subsystem number of the called party address is set to 1 (**ssn=1**). An SCCP management message has the subsystem field of the called party address set to 1. The SCCP management format ID only applies to SCCP management messages.

The message type of the message being screened for the SCCP message format ID must be either a UDT, UDTS, XUDT or XUDTS message. All other message types are passed.

The wildcard value for the subsystem parameter (**ssn=***) indicates the range of values from 2 to 255. When the subsystem number is a wildcard, the next screening function identifier must be **stop (nsfi=stop)**. The SCMG format ID does not apply because messages with a subsystem of 2 to 255 are not SCCP management messages.

If the value of the **ssn** parameter is not a wildcard (1 - 255), the NSFI for the Allowed CDPA screen can be either the allowed affected point code screen (**aftpc**) or **stop**.

Alternate Command Keywords (Release 20.0)

This feature provides an alternate set of keywords for current EAGLE commands. The following are the new, industry-standard keywords:

EAGLE Keyword	Alternate Keyword
cancel	deactivate
inhibit card	remove card
allow card	restore card
act lpo	block slk
allow slk	uninhibit slk
cancel lpo	unblock slk

ANSI G-Flex Support at 1700 TPS per DSM (Release 30.3)

The feature ANSI G-Flex Support at 1700 tps per DSM Card increases the current transaction-per-second (tps) capacity of the G-Flex application running on DSMs cards from 850 tps to 1700 tps in an ANSI environment.

- In an ITU environment, the capacity will remain at 850 tps per DSM card
- The Service Selector table cannot contain an ITU entry Only G-Flex is defined as a service (see the -srvsel commands)
- The G-Flex feature is turned on
- The ansigflex system option is enabled using the chg-stpopts command.

ANSI/ITU MTP Gateway (Release 20.0)

The EAGLE acts as a gateway to connect ANSI, ITU international, and ITU national networks. The EAGLE also continues to switch traffic that does not need to be converted when the origination network is the same network type as the destination network. In order to be able to perform these functions, the EAGLE does the following.

- Discriminates between MSUs originating from each type of network
- Converts MSUs to the appropriate format by converting the message transfer part (MTP) and ISDN user part
- Routes MSUs to the correct destinations

Level 3 MSU Discrimination

The EAGLE must determine whether an incoming MSU terminates at the STP or must be routed to another destination. To accomplish the discrimination task, the EAGLE does the following.

- Compares the network indicator (NI) of an MSU to a database of valid NIs. If the network indicator is not valid, the MSU is discarded.
- Extracts the network indicator and destination point code (DPC) information from the incoming MSU. If an MSU is transmitted to an ANSI linkset, the network indicator is forced to a binary pattern of “10” before being extracted.
- Determines whether an incoming MSU terminates at the EAGLE or must be routed to another destination by joining the network indicator and DPC to a list of self point codes. The self point code is a combination of the true point code and capability point code. The capability point code identifies a group of nodes that have similar capabilities.

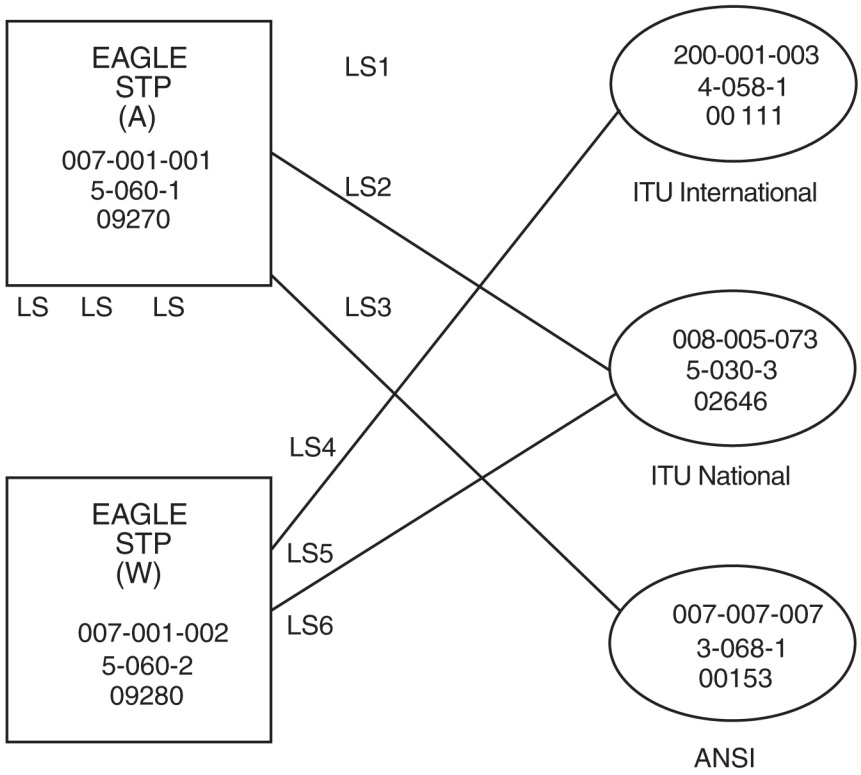
MSU Routing

MSU routing occurs after MSU discrimination and before MSU conversion (if conversion is necessary). The EAGLE selects an outgoing link on which to transmit the MSU. The MSU formats must be compatible with the linksets that transmit the MSUs.

EAGLEs are typically deployed in mated pairs. The EAGLE has a linkset for each supported network type. The EAGLE should have a unique adjacent point code. The EAGLE supports up to three self point codes—one for ANSI point codes, one for ITU international point codes, and one for ITU national point codes.

Figure 2-4 shows a sample network with mated gateway STPs. Note that there are different linksets for each network type. In the sample, STP (A) has an ANSI point code (007-001-001), an ITU National point code (09270), and an International point code (5-060-1).

Figure 2-4. Sample Gateway STP Network



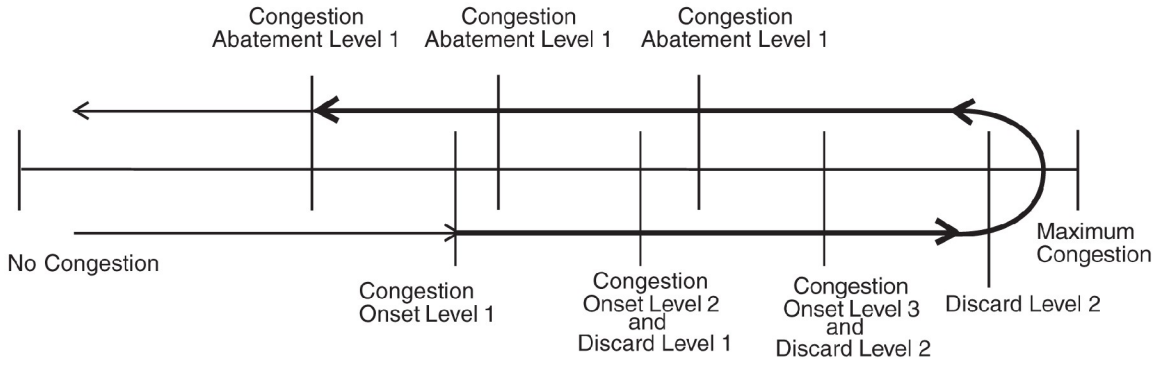
Administering Point Codes

The EAGLE can support multiple network types because each destination can be addressed by a true point code or by a list of alternate point codes. The list of alternate point codes contains from 0 to 2 alternates. The true point codes and alternate point codes are entered in the key table (by using the **ent-dstn** command). For example, an ANSI destination could have both a true point code and an alternate point code that point to the same routing translation in the routing table.

Local Link Congestion

When a link is congested, the EAGLE sends ANSI TFCs to the ANSI origination point code (OPC) and ITU TFCs to the ITU origination point code (OPC). **Figure 2-5** shows both an ANSI and an ITU network sending traffic to a congested link (the type of congested link does not matter). When an ANSI node is the source of the traffic to the congested link, the TFC contains a status. When an ITU node is the source of the traffic, the TFC does not contain a status.

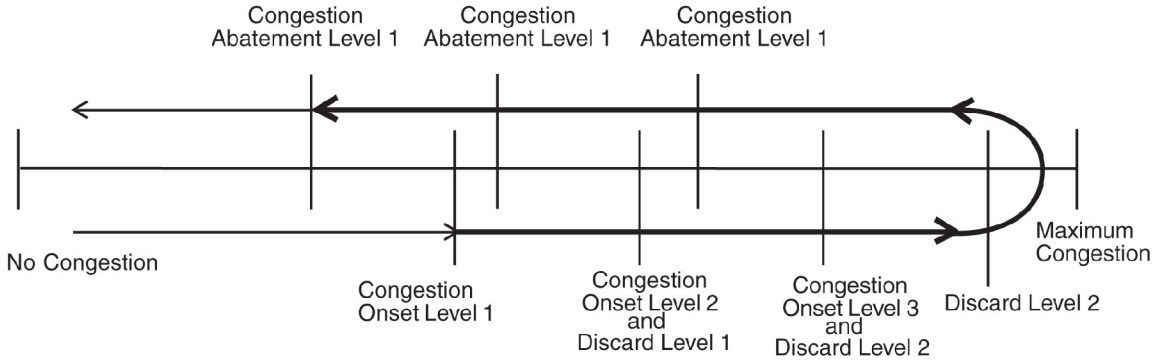
Figure 2-5. Traffic to and from a Congested Link



All links in the system operate with four levels of congestion. If the congestion level is “0”, there is no congestion, the EAGLE does not transmit TFCs, and no MSUs are discarded. At level 3 (indicating a maximum level of congestion), the EAGLE transmits TFCs, and discards MSUs.

Whenever the congestion onset status is above congestion onset level 1, and has not abated below congestion abatement level 1, the EAGLE generates a TFC. Whenever the congestion discard status is above discard level 1, and has not abated below discard level 1, the EAGLE discards the MSU. See **Figure 2-6** .

Figure 2-6. Congestion Levels



Remote Link Congestion

Table 2-4 shows the EAGLE’s response to remote congestion indicators.

Table 2-4. Remote Congestion Response

Event	EAGLE’s Response
EAGLE receives an ANSI TFC	When the EAGLE receives an ANSI TFC, the routing table is modified to discard lower priority MSUs being routed to the concerned point code. The TFC contains the congestion status of the concerned point code. The routeset congestion test mechanism is used to abate the congestion.
EAGLE receives an ITU TFC	When the EAGLE receives an ITU TFC, the routing table is modified to discard the lower priority MSUs being routed to the concerned point code. The TFC does not contain the congestion status of the concerned point code. Instead, the congestion status is user-configurable using the **chg-isup-stp:status** command. Once the routeset is identified as congested, a timer

Event	EAGLE's Response
	is used to abate the congestion. The timer is similar to the ANSI routeset congestion test mechanism.
EAGLE receives an ANSI RCT	There is no change in the EAGLE response when the EAGLE receives ANSI routeset congestion test messages.
EAGLE receives an ITU RCT	The H0H1 message codes are not contained in the ITU environment. These codes generate an invalid H0H1 MRN, and the message is discarded. This has no impact on the ITU network because the EAGLE uses a timer to abate congestion and does not rely on a reply to the RCT message.

ANSI/ITU SCCP and TCAP Conversion (Optional) (Release 22.2)

As an option for release 22.2, the ANSI/ITU SCCP and TCAP Conversion feature enables the EAGLE STP to convert MTP-routed SCCP and TCAP messages from ANSI to ITU format and to convert ITU formatted messages to ANSI. The following formatting and coding is supported:

- MTP routed Unitdata (UDT) non-segmented SCCP connectionless messages, including SCMG messages.
- MTP routed Unitdata Service (UDTS) messages (UDT messages returned due to error).

SCCP and TCAP conversion is turned on by way of two separate feature bits, one for the SCCP conversion and one for the TCAP conversion. The SCCP conversion feature must be turned on before, or at the same time as, the TCAP conversion feature.

ANSI/ITU SCCP and TCAP Conversion (Release 24.0)

As an option for release 24.0, the ANSI/ITU SCCP and TCAP Conversion feature enables the EAGLE STP to convert MTP-routed SCCP and TCAP messages from ANSI to ITU format and to convert ITU formatted messages to ANSI.

NOTE: This feature is a customized feature and does not conform to any known standard or specification.

The following formatting and coding is supported:

- MTP routed Unitdata (UDT) non-segmented SCCP connectionless messages, including SCMG messages.
- MTP routed Unitdata Service (UDTS) messages (UDT messages returned due to error).

SCCP and TCAP conversion is turned on by way of two separate feature bits, one for the SCCP conversion and one for the TCAP conversion. The SCCP conversion feature must be turned on before, or at the same time as, the TCAP conversion feature.

ANSI/ITU Translation (Release 35.0)

Description

The ANSI/ITU Translation feature allows any domain GTT selector to be assigned to a ‘cross’ domain GTT set. This allows access to GTA data within a GTT set that can be used to translate ANSI and ITU messages.

ANSI/ITU translation allows a user to provision a single cross domain GTT set with one set of GTA data and assign it to multiple GTT selectors, regardless of their domain. Since the user does not have to provision a GTT set with the same GTA data for each network domain GTT selector (gtia=2, gtii=2, gtii=4), GTA table space and user-provisioning activity is conserved.

The Enhanced GTT feature and ANSI-ITU-China SCCP Conversion feature must be on before the ANSI/ITU Translation feature can be enabled.

Hardware Requirements

The ANSI/ITU Translation feature has the following hardware requirements:

- Use of TSM or higher SCCP cards.
- LIM hardware types.

Limitations

The ANSI/ITU Translation feature has no associated limitations.

ANSI-41 INP Query (AINPQ) (Release 36.0)

Description

The ANSI-41 INP Query (AINPQ) feature adds support for using an ITU-N ANSI-41 NPREQ message for querying the INP database, in addition to the existing INP feature number portability query using the ITU-N and ITU-N24 INAP IDP message.

A feature access key (FAK) for part number 893017801 is required to enable the AINPQ feature.

- The GTT feature must be on before the AINPQ feature can be enabled.
- After the feature is enabled and turned on, it cannot be turned off.
- No temporary FAK is allowed for the feature.
- If any LNP quantity feature is enabled, the INP and AINPQ features cannot be enabled. If either the INP feature or the AINPQ feature is enabled, no LNP quantity feature can be enabled.
- The AINPQ feature and the EIR feature cannot be enabled in the system at the same time.

The AINPQ feature supports a mix of ITU and ANSI protocols in querying the INP database using the ANSI-41 NPREQ query.

Service selectors, INP options, and measurements are common to the INP and AINPQ features.

INP message relay functions operate when the INP feature, the AINPQ feature, or both features are turned on. The parameter values defined for INP query processing (through the INPQ service or PC/SSN) can apply to both the INP and AINPQ feature if both features are turned on.

INP query processing can be invoked by the following mechanisms (MTP routed NPREQ is not supported):

- For GTT-routed NPREQ query, INP query processing can be invoked using the **inpq** service selector that is defined using the SCCP Service Selector commands.

- For NPREQ-routed-based PC/SSN query, INP query processing can be invoked using the EAGLE 5 ISS point code and local subsystem number (PC/SSN) defined for the INP feature.

When the AINPQ featureis turned on,the INP query processing operates as follows:

- Handling of an ITU-N Point Code ANSI-41 NPREQ query encoded in ANSI-41 TCAP, ITU SCCP, and ITU MTP protocol stack is supported.

- ITU MTP/SCCP protocol validation and ANSI TCAP protocol validation for a received ANSI-41 NPREQ query are supported.

- For a received ANSI-41 NPREQ query subject to the INP query processing, the EAGLE 5 ISS uses the digits encoded in the DGTSDIAL parameter for database lookup.

- The EAGLE 5 ISS performs number conditioning on the DGTSDIAL value in preparation for database lookup. The Called Party Prefix, National Escape Code, Service Nature of Address, Nature of Number, and Country Codes are used to condition the number as a National or International number.

- Enhanced AINPQ and INP options for the Global Option for Connect on INP Query feature can be used to format information in the response that results from the database lookup.

- The AINPQ feature and the INP feature share the INP local subsystem, including SCCP subsystem management and service selection.

- The AINPQ feature and the INP feature share the CPCTYPE (Capability Point Code Type) state.

When the INP feature is turned on, the INP query processing operates as follows:

- Handling of the ITU-N and ITU-N24 INAP IDP message is supported.

- CDPN number conditioning is performed in preparation for database lookup.

- Enhanced AINPQ and INP options for the Global Option for Connect on INP Query feature can be used to format information in the response that results from the database lookup.

The INP options in the EAGLE 5 ISS have been enhanced to support the AINPQ feature.

- A new INP option is provided to define the National Escape Code (NEC) value, up to 5 digits, for each EAGLE 5 ISS node.

- The maximum number of Called Party Prefix entries allowed in the INPOPTS table has been increased from 5 to 40.

- AINPQ supports the Global Option for Connect on INP Query Response feature that was previously implemented for INP. The destination routing address (DRA) options have been enhanced for INP and AINPQ for formatting the ROUTDGTS parameter in the INP “Connect” message or AINPQ NPREQ “Return Result“ response message, as follows:

- Support RN + [CDPNPFX] + DN in INP “Connect” or AINPQ “Return Result” response messages

  — Support Routing Number in in INP “Connect” or AINPQ “Return Result” response messages

  — Support [CDPNPFX] + CC + RN + DN in INP “Connect” or AINPQ “Return Result” response messages

  — Support RN + [CDPNPFX] + NEC + DN in INP “Connect” or AINPQ “Return Result” response messages (the National Escape Code must be provisioned)

There are no new measurements pegs for NPREQ queries. The existing INP registers are pegged for the NPREQ query, the IDP query, or both; the peg for “IDP received” is a total count of the number of the IDP and NPREQ queries received if both the AINPQ and INP features are turned on.

Hardware Requirements

The ANSI-41 INP Query feature has the following hardware requirements:

- DSM card with at least 4G of memory running the VSCCP application

- After AINPQ is enabled, no DSM cards with less than 4G of memory can be provisioned. DSM cards installed with less than 4G of memory will be auto-inhibited if AINPQ is enabled.

Assumptions

The ANSI-41 INP Query feature assumes that an MSC will not initiate an NPREQ query for a call prefixed with International Escape Code (commonly defined as “00”) + CC+DN, as the call is intended for terminating to an international subscriber.

Limitations

None

ANSI-41 Mobile Number Portability (A-Port™) (Release 36.0)

Description

The ANSI-41 Mobile Number Portability (A-Port) feature enables an IS41 subscriber to change to a different service provider while retaining the same Mobile Dialed Number (MDN).

A-Port uses the EPAP (EAGLE Provisioning Application Processor) RTDB provisioning database to retrieve the subscriber portability status and provision directory numbers for exported and imported IS41 subscribers. This

database maintains information related to subscriber portability in the international E.164 format. A-Port uses RN and PT values to provision directory numbers (DNs) for exported subscribers. In addition, A-Port uses SP to provision DNs for imported subscribers. It is optional to provision the PT values for imported subscribers.

Service Selector Lookup

Service selector lookup is performed using the MTP/SCCP data. If the selectors match and MNP service is assigned, A-Port handling is performed.

To manage number portability, A-Port uses the MNP SCCP Service Selector to process LOCREQ and SMSREQ SCCP messages. The EAGLE ISS intercepts LOCREQ messages for the RTDB database lookup. An ANSI-41 LOCREQ message is initiated by a TDMA/CDMA MSC that queries the HLR for information regarding user subscription/location before terminating a voice call.

A-Port supports both GT- and MTP-routed messages.

- GT-routed messages support UDT and non-segmented XUDT message types and perform service selector lookup after SCCP verification.

- A-Port processes MTP-routed messages if the MTP Messages for SCCP Applications (MTP Msgs for SCCP Apps) feature is turned on (see "IS41 GSM Migration" for details of MTP-routed message processing).

MNP begins A-Port general TCAP/MAP verification if the message is ANSI TCAP and A-Port is turned on. TCAP/MAP verification is performed on all messages; A-Port supports only the ANSI TCAP format.

Database Lookup and Routing

The DN is used for database lookup.

- For LOCREQ messages, the DN is derived based on the setting of the LOCREQDN option (see the new **`chg-is41opts`** command).

- For non-LOCREQ messages, the DN is derived from the SCCP portion of the message.

- A-Port performs number conditioning upon successful decode and verification of the message. HomeRN and IEC or NEC prefixes are removed. The DN is conditioned to international number format based on the service nature of address (SNAI or TCAPSNAI or MTPLOCREQNAI).

A-Port performs RTDB lookup on the conditioned number, and routes or relays the message based on the lookup result.

- An SMSREQ message is relayed like any other non-LOCREQ message. No changes are performed to the TCAP/MAP portion of the message.

- A-Port modifies the TCAP information for LOCREQ messages only when a HomeRN was deleted from the TCAP DN and LOCREQRMHRN = YES. Any gaps in the data caused by a change in field length will be resolved by shifting the remaining information up. Any IEC or NEC code is left.

- A-Port falls through to GTT if number conditioning fails or does not find the DN in the RTDB database, or the DN is found with non-A-Port data.

- If a HomeRN is detected in the Called Party and a matching DN with RN is found in the database, the EAGLE 5 ISS generates UIM 1256, indicating detection of circular routing, and routes the message using normal routing if both the MNP Circular Route Prevention feature and the IS41 GSM Migration featureare turned on.

- Normal routing is performing GTT if the incoming message is sent to the EAGLE 5 ISS Self Point Code. Normal routing is routing the message to the MTP DPC if the incoming message is MTP-routed (the MTP DPC of the message is not the EAGLE 5 ISS Self Point Code).

A-Port shares the service state and re-route with the IS41 GSM Migration feature and the G-Port feature, under one service called the MNP service state. (The G-Port service state is used if only the G-Port feature is on.) A-Port supports re-route functions as part of MNP service re-route. Alternate PCs are shared by all three features.

Alarms and the **rept-stat-sccp** command output show MNP Service information if the A-Port feature is enabled.

Feature Access Key

A feature access key (FAK) for part number 893015501 is required to enable the A-Port feature.

- The GTT feature must be on before the A-Port feature can be enabled.
- After the feature is enabled and turned on, it cannot be turned off.
- No temporary FAK is allowed for the feature.
- An LNP quantity feature and the A-Port feature cannot be enabled in the system at the same time.

Measurements

The following enhancements support the collection and retrieval of measurements related to the A-Port feature. These new measurement registers are supported with and without the Measurements Platform feature enabled.

- New registers are added to the NP SSP reports: Hourly Maintenance Measurements on NP SSP (MTCH-SSP) and Daily Maintenance Measurements on NP SSP (MTCD-SSP).
  - — APLRACK—Number of call related LOCREQ messages acknowledged.
  - — APLRRLY—Number of call related LOCREQ messages relayed.
  - — APNOCL—Number of non-call non-LOCREQ related messages relayed.
  - — APNOCLGT—Number of non-call Non-LOCREQ related messages that fell through to GTT.

Feature Interactions

G-Port, A-Port, and IS41 GSM Migration solve the problem of number portability from one network to another or number migration from one mobile protocol to another. One, two, or all three features could be active on a single EAGLE 5 ISS node at a given point. Because all of these features could have same type of MTP and SCCP layers (ITU or ANSI), it may look like same kind of message at service selection, which looks at the network domain and SCCP parameters. Therefore, all three features share one service. Because of this, existing functions like SRVSEL, Service, Re-route, CPC and **rept-stat-sccp** command service snapshot counts are affected.

Hardware Requirements

The A-Port feature has the following hardware requirements:

- DSM cards with at least 4G of memory
- A-Port cannot be enabled if any DSM cards with less than 4G of memory or any TSM cards for SCCP are present in the system. When A-Port is enabled, no DSM cards with less than 4G of memory and no TSM cards for SCCP can be provisioned for SCCP.

Assumptions

Within a portability domain (ordinarily a country) a Mobile Directory Number (MDN) assigned to an IS41 subscriber will not overlap with an MSISDN assigned to a GSM subscriber (one dialed DN can either be an IS41 or a GSM subscriber). Therefore, IS41 and GSM subscriber data can co-exist in the same EPAP provisioning database.

Limitations

The A-Port feature has the following limitations:

- Communication between the SMSCs in the originating network (a calling party's home network or the network where the call was originated) and the SMSC in the terminating network is through SS7 and not SMPP.
- Number Portability across multiple countries is not supported.

ANSI-ITU-China SCCP Conversion (Release 31.3)

Since some ANSI and ITU SCCP parameters are incompatible in format and/or coding, subsequently the EAGLE has not historically supported SCCP traffic between ANSI and ITU networks. A specialized SCCP/TCAP conversion was previously implemented for MTP Routed UDT/UDTS messages. This feature will not interact with the Release 22.2 SCCP/TCAP conversion feature but will be mutually exclusive of it. Since the specialized SCCP/TCAP conversion was implemented, many improvements have been made to the EAGLE in regards to ITU SCCP compliance and features. (e.g. EGTT, MGTT). ANSI-ITU-China SCCP Conversion will provide a generic capability that will correctly format and decode/encode the following inter-network SCCP traffic:

- UDT and UDTS messages - includes SCMG messages, which are a specialized form of a UDT
- MTP routed
- GT routed

The feature also provides SCCP management (SCMG) across network type boundaries, i.e. concerned point codes for a mated application may be of a different network type than the mated application.

UDTS message return is controlled inherently by the SCCP layer protocol within the protocol class byte. If bits 5-8 indicate return message on error, a UDTS message will be sent when there is an error. Otherwise, no UDTS is returned to the originator.

ASM Obsolescence (Release 31.6)

The current Application Services Module (ASM) card is an aging board with limited functionality when compared with today's modern day processors. This feature removes ASM card support in EAGLE software. The ASM card currently supports only two application Generic Program Loads (GPLs), the Signaling Connection Control Part (SCCP) and Gateway Loading Services (GLS) applications. The TSM card already supports both of these applications. Supported GPLs by card type are shown in Table 2-5 .

Table 2-5. GPL Support for ASM and TSM Cards

GPL	ASM Card	TSM Card
Before ASM Obsolescence		
GLS Application supported	Yes	Yes
SCCP Application supported	Yes	Yes
After ASM Obsolescence		
GLS Application supported	No	Yes
SCCP Application supported	No	Yes

Hardware Required

Any ASM cards in the system must be replaced with TSM cards before the Release 31.6 upgrade can occur.

NOTE: Release 31.X baseline hardware includes GPSMIIs, HMUXs, -10s TDMs. If these modules are not equipped the act-upgrade command will be rejected.

Limitations

- Beginning with EAGLE software release 31.6, there will be no support for the ASM card and card type.

Auto Point Code Recovery (Release 35.6)

Description

The Auto Point Code Recovery feature enhances the EAGLE 5 ISS functionality for handling Circular Routing due to Far-End Loopback and automatically resets the Circular Route Detection (CRD) prohibited Destination Point Code (DPC).

The EAGLE 5 ISS detects Far-End Loopback in a link through the signaling link test control (SLTC) procedure. In this procedure, the EAGLE 5 ISS originating point code (OPC) sends a signaling link test message (SLTM) across a link to the STP and expects a signaling link test acknowledgement (SLTA) from the STP. If Far-End loopback occurs in the connecting link, the OPC receives the same SLTM instead of an SLTA. The OPC marks the link as failed as soon as it receives the SLTM.

Multiple MSUs can be returned to the OPC due to the circular route caused by the loopback. This can increase the congestion level on the link which then invokes Circular Route Detection (CRD) processing. CRD marks the link

as failed and marks the destination point codes (DPCs) as CRD-prohibited, meaning that the link cannot be used until the DPC is cleared. Clearing the DPCs requires manual execution of the **rst-dstn** command.

The Auto Point Code Recovery feature consists of the following features:

- Enhanced Far-End Loopback Detection
- Circular Route Auto-Recovery

The Enhanced Far-End Loopback Detection and the Circular Route Auto-Recovery features can be enabled and turned on separately. However, SLTMs must be enabled (**chg-slt** command) before either feature can operate.

Enhanced Far-End Loopback

The Enhanced Far-End Loopback feature significantly decreases the time required to take a link out of service. When a trigger event occurs that indicates Far-End Loopback may have occurred, the EAGLE 5 ISS sends an SLTM. Normal processing takes the link out of service if the SLTM is received. The Enhanced Far-End Loopback feature fails the link as quickly as possible. This rapid failure prevents the EAGLE 5 ISS from marking DPCs as CRD-prohibited.

Circular Route Detection

The Circular Route Detection feature automatically clears CRD when Far End Loopback is detected, and the failing link is part of the linkset that detected the circular route. Without the Circular Route Detection feature, CRD must be cleared by manually executing the **rst-dstn** command.

Hardware Requirements

No additional hardware requirements are required to support the Auto Point Code Recovery feature.

Automatic PDB and RTDB Backup (EPAP 7.0)

Description

The Automatic PDB/RTDB Backup feature allows for the scheduling of automated backups of EPAP PDBs and RTDBs. The PDB backup copy is created on the EPAP A server and the RTDB backup copy is created on the standby EPAP server (A or B). A specific destination for the backup copy can be configured at the users discretion.

From the EPAP GUI terminal (Web UI only), the user can access a graphical user interface screen and configure the time, frequency, and destination of the backup copy.

Tekelec recommends that an Automatic PDB/RTDB Backup be performed on a daily (24 hour) basis. Both the PDB and RTDB backups are scheduled together and cannot be scheduled separately. The **Time of the day to Start The Backup** is the time that the RTDB backup starts. The PDB backup automatically starts 1 hour later.

Backups can only be scheduled and created on a provisionable EPAP server pair. An automatic PDB/RTDB backup is not allowed and cannot be scheduled on a non-provisionable EPAP server pair.

Normal provisioning is allowed during the automatic PDB/RTDB backup. This includes provisioning from

- the customer network to the PDB,
- the PDB to the Active EPAP RTDB, and
- the Active EPAP RTDB to the DSM RTDB.

RTDB backups are always created from the standby EPAP RTDB (A or B). The RTDB can resume receiving updates when it is brought back on line.

Disk Space Limitations

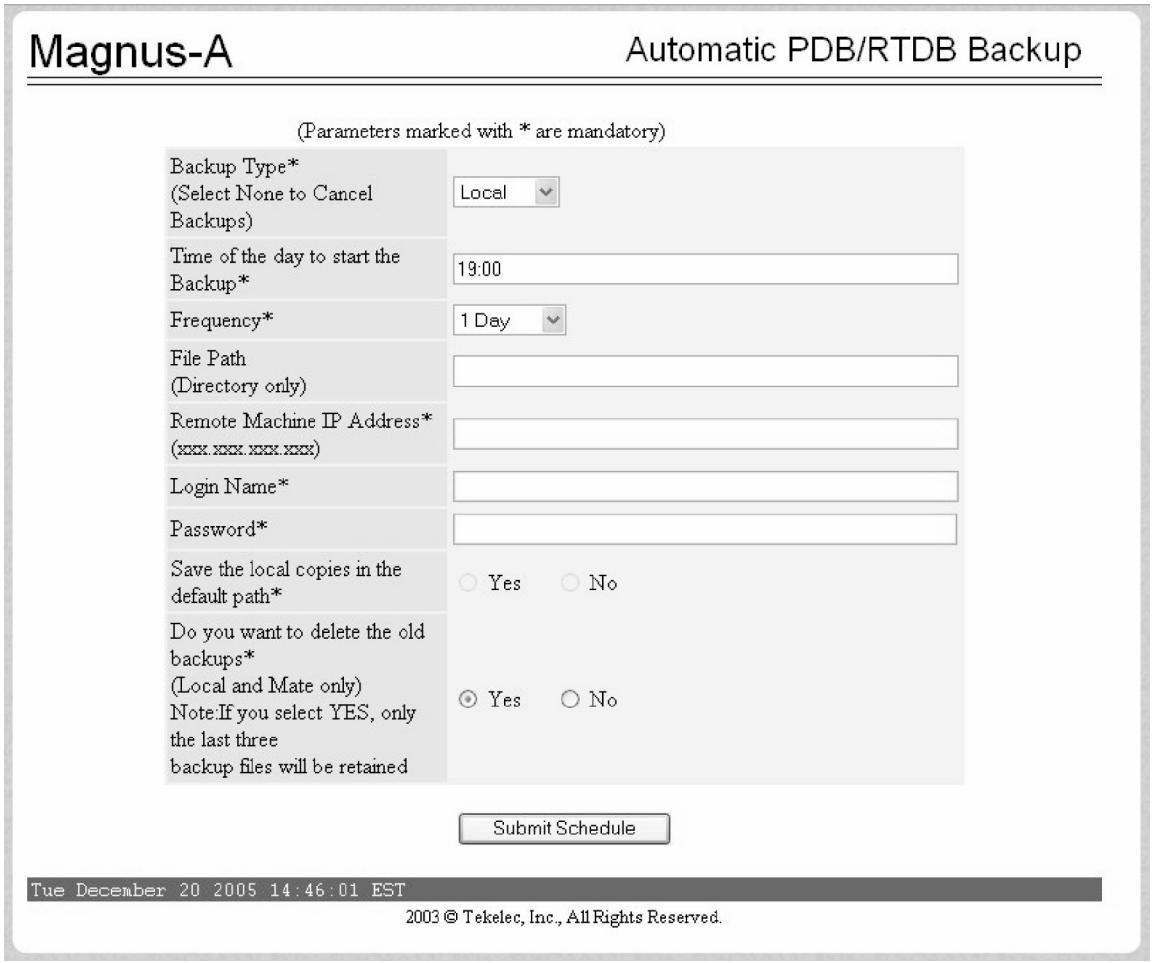
This feature supports the retention of three backup copies of the PDB and RTDB databases. However, the disk space in the EPAP free directory may not be sufficient to accommodate the retention of three backup copies on sites with large PDB and RTDB databases. When insufficient disk space exists, a dialog box appears asking the user “Do you want to delete the old backups”.

- If yes, the new database backup copy is written over the previous version.
- If no, the user must create a directory in a location with sufficient disk space and then specify the location of the backup directory to create the backup copy in.

Automatic PDB/RTDB Backup Screen

This feature adds to the list of EPAP Maintenance menu options, the item “Automatic PDB/RTDB Backup”. The scheduled time, frequency, and destination of the backup file can be configured by the user from the Automatic PDB/RTDB Backup screen.

Figure 2-7. Automatic PDB/RTDB Backup screen.



Most of the input parameters are self explanatory. The following options are configurable by the user:

The frequency of the backup copy can be any of the following increments:

- 12 hours (see Note below)
- 1 Day (daily)
- 2 Days
- 3 Days
- 5 Days
- 7 Days

The Backup Type parameter is the destination for the backup file:

- **Local -** A backup copy of the data is saved to the local disk on the same EPAP server as the PDB/RTDB being backed up.

- **Mate -** A backup copy of the data is created on the local server and then sent via SCP to the mate EPAP server.
- **Remote** - A backup copy of the data file is created on the local EPAP server and then sent via SFTP to a remote server configured by the user. This server may or may not run EPAP software and can be any machine on the network that is running an SFTP daemon or service.
- **None** - No backup is scheduled and cancel all previously scheduled backups. This will not affect a backup that is currently in progress.

The following table can be used as a guide when scheduling the Automatic PDB/RTDB Backup.

Table 2-6. Mandatory verses Optional Parameters

Parameter	Automatic PDB/RTDB Backup Type		
	Local	Mate	Remote
Time of day to start backup	Mandatory	Mandatory	Mandatory
Frequency	Mandatory	Mandatory	Mandatory
File Path	Optional	Optional	Mandatory
Remote Machine IP Address	N/A	N/A	Mandatory
Login Name	N/A	N/A	Mandatory
Password	N/A	N/A	Mandatory
Save the Local copies in the default path	N/A	Optional	Mandatory
Do you want to delete the old backups Note: If you choose Yes, only the last three backup files, including the current one are kept.	Mandatory	Mandatory	N/A

The default file path where subdirectories are created (on the mate and local servers) is /var/TKLC/epap/free/

The default file names that are used to designate the backup files are:

PDB	pdbBackup_<hostname>_<CurrentTime>_DBBirthdate_<DBBirthdate>_DBLevel_<level>.bkp.tar.gz
RTDB	rtdbBackup_<hostname>_<CurrentTime>.tar.gz

Automatic PDB Export Enhancement (EPAP 9.0)

Description

The Automatic PDB Export Enhancement feature provides more flexible scheduling for automatic PDBA exports.

With more options to choose from, scheduling an automatic PDB export is now very similar to the way tasks or appointments can be scheduled in a calendar manager.

In addition to the previously available choices for export format, mode, and data type, these enhancements allow the user to:

- View, modify, or delete existing reports
- Choose from multiple options for the frequency of the export:
  - Daily
  - Weekly
  - Monthly
  - Yearly
- Choose the time of day to start the export
- Add comments to describe the export

Hardware Requirements

None.

Limitations

None.

Backup Provisioning Network Interface (Release 29.0)

Currently, the MPS machines only make use of one interface to the customer network. There is an unused interface (QFE3) available. This feature allows for the configuring of a second interface to the customer network. This second interface must exist on a different subnet than the primary (HME0) interface. The customer can then use either interface to communicate with the MPS (WebUI, PDBI, telnet, etc).

NOTE: It is important to note that this backup interface could also be used for Versant's FTS replication, in the event that something is wrong with the HME0 path. However, this switch is not automatic. A user would have to manually make the change through the configuration text UI at both sites.

Hardware Requirements

No new hardware is needed to support this feature.

Calling Name Conversion Facility (CNCF) (Release 23.1)

This feature provides a conversion of ISUP IAM messages using two versions of calling name identification presentation (CNIP) for calling name information delivery. One version of the CNIP uses the nonstandard, proprietary ISUP party information (PIP) parameter. The other version uses the ANSI standard ISUP generic name (GN) parameter. The conversion will either replace the PIP parameter with the GN parameter or the GN parameter with the PIP parameter in the ISUP IAM message.

The gateway screening feature is used to select which ISUP messages are converted. The incoming messages are selected based on the OPC and DPC in the routing label of the message, and the message type in the service information octet. The message type is defined by the value of the service indicator (**`SI`**) field of the SIO. ISUP messages contain the value 5 in the service indicator field of the SIO. Screening rules for Allowed OPC, Allowed DPC, and the Allowed SIO entities must be configured in the database for this feature. The **`redirect=yes`**

parameter must be specified with the last entity in the screening process (**nsfi=stop**) to use the CNCF feature to convert the message.

This feature is an optional feature and must be turned on with the **chg-feat** command and the new parameter, **cncf=on**. Before this feature can be turned on, the gateway screening feature must be on. This is shown by the entry **GWS = on** in the output of the **rtrv-feat** command. If the gateway screening feature is not on when an attempt is made to turn the CNCF feature on, the **chg-feat** command is rejected with this message:

Error Message

```
E3646 Cmd Rej: GWS must be ON before CNCF can be ON
```

The **rtrv-feat** command output has been changed to add the **CNCF** field showing whether the CNCF feature is on or not.

If the CNCF feature is turned on, the DTA feature is disabled. There are no other command changes to support this feature.

Figure 2-8 shows an example network that contains these two separate ISUP versions. Based on this example, Table 2-8 shows when the ISUP IAM message conversion by the CNCF feature occurs.

Figure 2-8. PIP/GN Parameter Conversion

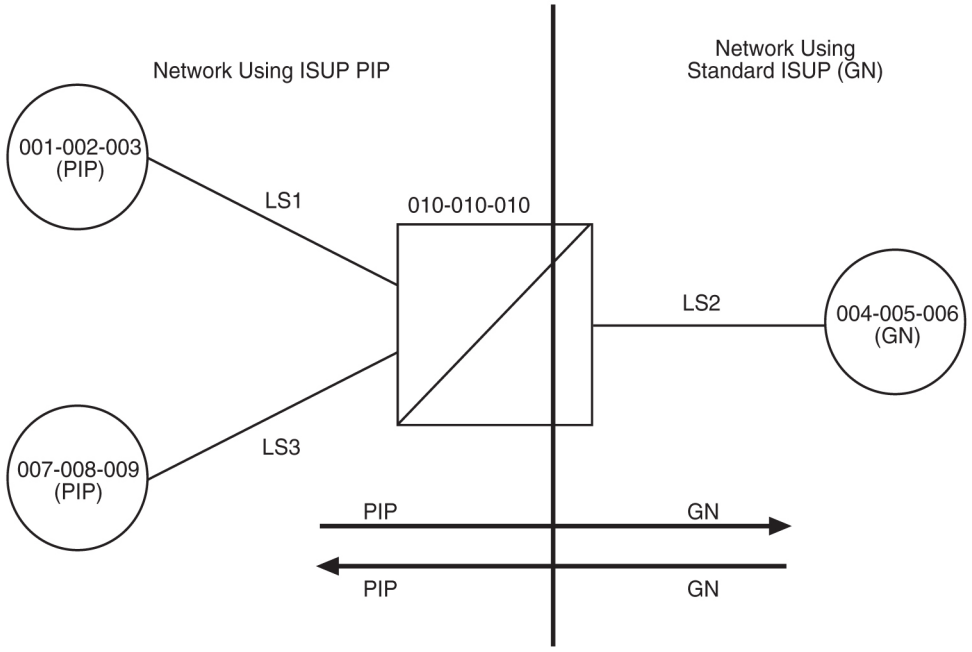


Table 2-7. ISUP IAM Message Conversion Examples

Origination Point Code	Destination Point Code	ISUP IAM Message Conversion
001-002-003	004-005-006	Yes
001-002-003	007-008-009	No
004-005-006	001-002-003	Yes
004-005-006	007-008-009	Yes

Origination Point Code	Destination Point Code	ISUP IAM Message Conversion
007-008-009	001-002-003	No
007-008-009	004-005-006	Yes

CAUTION: Take care when configuring the gateway screening rules for this feature. The CNCF feature has no way to validate the gateway screening rules to detect errors in converting messages between compatible networks. For example, using the example network in Figure 2-8 , the ISUP IAM message traffic from node 001-002-003 to node 007-008-009 does not need to be converted because they are using the same calling name delivery parameter, PIP. If the gateway screening rules are not carefully configured, these messages could be converted when they do not need to be.

Limitations

No measurements are collected showing the number of MSUs converted by this feature.

No error message is generated if an error occurs during the conversion of the PIP and GN parameters.

If the CNCF feature is turned on, the DTA feature is disabled. No message redirection using the DTA feature will be performed.

If the **copy=yes** parameter is specified with the **redirect=yes** parameter, the MSU is copied for the STP LAN feature after it has been converted by the CNCF feature.

If there are multiple PIP parameters or GN parameters with calling name information within a single ISUP IAM, only the first occurrence of the parameter in the ISUP IAM message is converted.

Messages on X.25 linksets cannot be converted with the CNCF feature.

Only GN IAM messages containing calling name information (Type of Name = Calling Name, Presentation = Allowed, Parameter Length >1) are converted to PIP IAM messages.

Only PIP IAM messages containing Calling Name Information (Sub-Parameter Code = Name Information, Name Element Indicator = Calling Party) are converted to GN IAM messages.

If the received IAM message contains both a GN and a PIP parameter with calling name information, the GN parameter is retransmitted and the PIP parameter is deleted.

Any MSU that is not converted is simply retransmitted. These MSUs include non-ISUP MSUs, non-IAM MSUs, and any IAM MSU received that does not contain either a GN or PIP parameter.

If the PIP parameter contains other information in addition to the calling party name information, only a GN parameter containing calling party name information is generated.

The linkset being screened for this feature should not contain C links (**lst=c** parameter of the **ent-ls** and **chg-ls** commands). This would result in the double conversion of the ISUP IAM messages.

IAM messages containing a GN parameter that are to be converted, must be 262 bytes or less. The ANSI SS7 MSU can contain a maximum of 272 bytes, including the Level 3 routing label. Without the routing label, the MSU can contain 265 bytes, starting at the Circuit ID code field. Since the PIP parameter has 3 bytes more than the GN parameter, the MSU can contain a maximum of 262 bytes.

Table 2-8 summarizes the conversion action performed based on the optional parameters found within the MSU.

Table 2-8. CNCF Conversion Actions

PIP Parameter Content	GN Parameter Content		
	GN Parameter with Calling Name Information	GN Parameter without Calling Name Information	GN Parameter Not Found
PIP Parameter with Calling Name Information	The PIP parameter is deleted. The GN parameter is retransmitted without conversion. No network-specific parameters (0xFD and 0xFE) are deleted.	The PIP parameter is converted to a GN parameter. The GN parameter is retransmitted if it is present. Network-specific parameters (0xFD and 0xFE) are deleted.	The PIP parameter is converted to a GN parameter. The GN parameter is retransmitted if it is present. Network-specific parameters (0xFD and 0xFE) are deleted.
PIP Parameter without Calling Name Information	The PIP parameter is deleted. The GN parameter is retransmitted without conversion. No network-specific parameters (0xFD and 0xFE) are deleted.	The PIP parameter is deleted. The GN parameter is retransmitted if it is present. Network-specific parameters (0xFD and 0xFE) are deleted.	The PIP parameter is deleted. The GN parameter is retransmitted if it is present. Network-specific parameters (0xFD and 0xFE) are deleted.
PIP Not Found	The PIP parameter is not involved. The GN parameter is converted to PIP. No network-specific parameters (0xFD and 0xFE) are deleted.	No parameters are converted. No parameters are deleted.	No parameters are converted. No parameters are deleted.
NOTE: Parameters with calling name information have precedence over parameters without calling name information. For example, an MSU that has both a GN parameter with calling name information and a GN parameter without calling name information is treated as if it were an MSU with a GN parameter with calling name information.			

PIP and GN Parameters

The PIP format contains a parameter name (0xFC), parameter length and optional sub-parameters. The format is shown in **Table 2-9** . The Name Element Indicator, Name Element Length and Name Information fields can be repeated within a single PIP.

Table 2-9. PIP Parameter Format

Field	Length	Bits Value HGFE DCBA	Comments
Parameter Name	1 octet	1111 1100	Party Information
Parameter Length	1 octet	—	Length of the parameter excluding the parameter name and the parameter length octet
Sub-Parameter Code	1 octet	1111 1110	Name Information
Sub-Parameter Length	1 octet	—	Sum of the number of octets in the Name Element Indicator, Name Element Length, and Name Information fields

Field	Length	Bits Value HGFE DCBA	Comments
Name Element Indicator	1 octet	0000 0001	Calling party name
		0000 0010	Connected party name
		0000 0011	Redirecting party name
Name Element Length	1 octet	—	Number of characters in the name information field (maximum of 15)
Name Information	up to 15 octets	—	Maximum of 15 IA5 characters

The GN format contains a parameter name (0xC7), parameter length and up to 16 additional octets. The format is shown in **Table 2-10** .

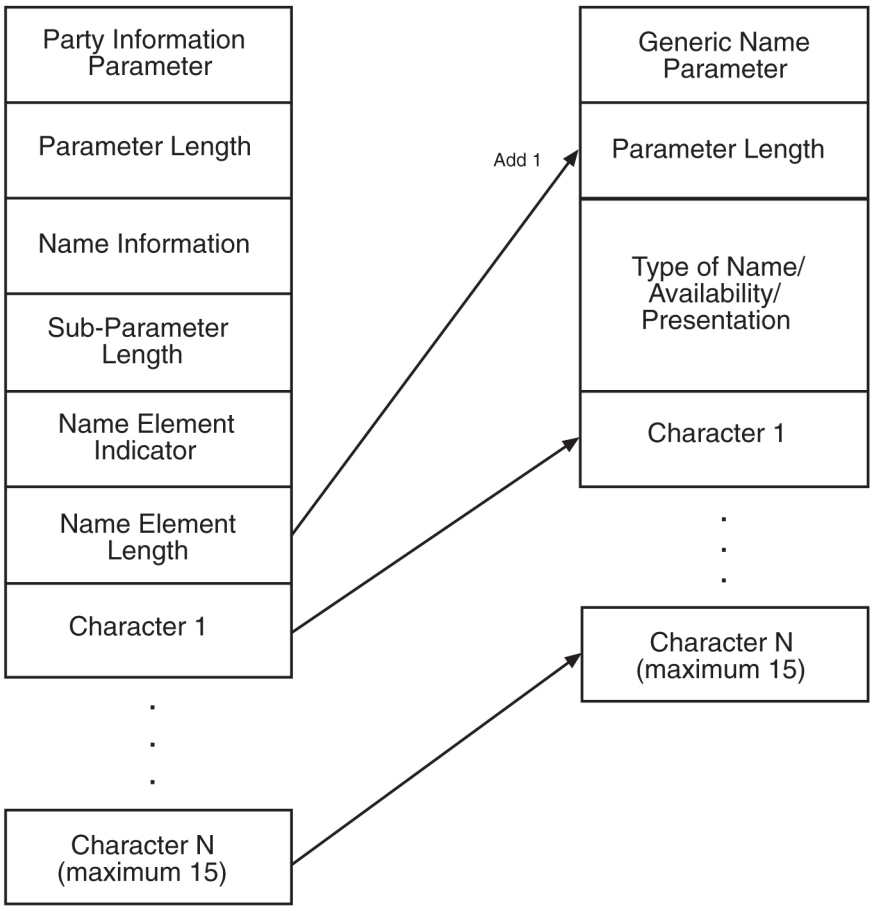
Table 2-10. GN Parameter Format

Field		Bits Value HGFE DCBA	Comments
Parameter Name		1100 0111	Generic Name
Parameter Length		—	Length of the parameter excluding the parameter name and length fields
Octet 1	Presentation	XXXX XX00	Presentation Allowed
		XXXX XX01	Presentation Restricted
		XXXX XX10	Blocking Toggle
		XXXX XX11	No indication
	Spare	XXXX 00XX	Not Used
	Availability	XXX0 XXXX	Name available or name availability unknown
		XXX1 XXXX	Name not available
	Type of name	000X XXXX	Spare
		001X XXXX	Calling name
		010X XXXX	Original called name
		011X XXXX	Redirecting name
		100X XXXX	Connected name
		101X XXXX to 111X XXXX	Spare
		Octets 2-n	— Maximum of 15 IA5 characters

Conversion of PIP to GN

The mapping of PIP parameters to GN parameters for this conversion is shown in Figure 2-9 . The new GN parameter length field is computed based on the PIP name element length and not the PIP parameter length or Sub-Parameter length fields.

Figure 2-9. PIP to GN Parameter Mapping



Conversion of GN to PIP

The mapping of GN parameters to PIP parameters for this conversion is shown in Figure 2-10 .

Figure 2-10. GN to PIP Parameter Mapping

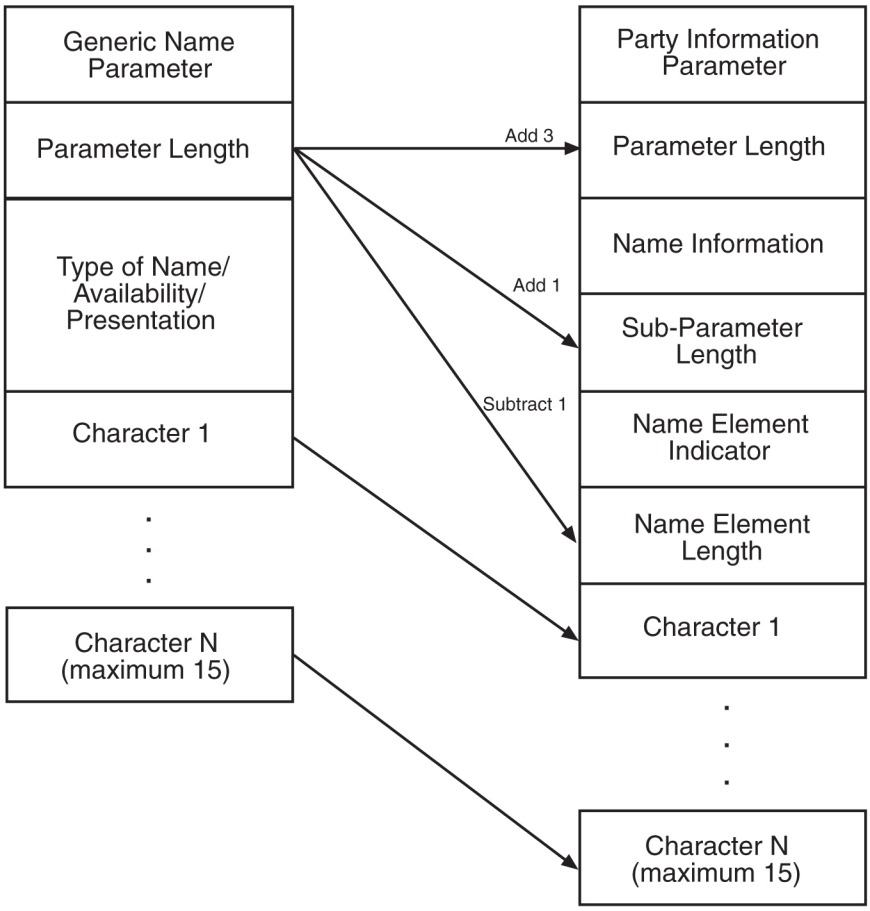


Table 2-11 shows how the PIP and GN parameters are mapped during the conversion process.

Table 2-11. PIP/GN Parameter Mapping

Party Information Parameter		Generic Name Parameter	
Field Name	**Value**	**Field Name**	**Value**
Parameter Name	Party Information (0xFC)	Parameter Name	Generic Name (0xC7)
Parameter Length	as calculated	Parameter Length	as calculated
Sub-Parameter Code	Name Information (0xFE)	—	no mapping
Sub-Parameter Length	as calculated	—	no mapping
Name Element Indicator	Calling Party Name (1)	Type of Name	Calling Name (HGF=001)
—	no mapping	Presentation	Allowed (BA=0)
—	no mapping	Availability	Name Available (E=0)
Name Element Length	as calculated	—	no mapping

Party Information Parameter		Generic Name Parameter	
Field Name	**Value**	**Field Name**	**Value**
Name Information	Calling Party Name (maximum 15 characters)	Characters	Calling Party Name (maximum 15 characters)

Message Conversion

The conversion process only occurs in ISUP Initial Address Messages (IAM) with either the PIP or GN optional parameters that contain calling party name information. The conversion either replaces PIP parameters with GN parameters or GN parameters with PIP parameters. In some cases, network-specific optional parameters are also deleted from the message. The Level 2 Length Indicator is also updated since the MSU length is changing. The sections shown in bold type show which fields of an IAM with the GN parameter are effected by the CNCF feature.

Output Example

```
Protocol Flavor: ANSI-SS7
Total Message Length: 56
*** Start of MTP Level 2 ***
                MTP
000 00000000 00
    -0000000    Backward Sequence Number                0
    0-------    Backward Indicator Bit                  0
001 00000000 00
    -0000000    Forward Sequence Number                 0
    0-------    Forward Indicator Bit                   0
002 00110101 35
    --110101    Length Indicator                        53
    00------    Spare                                   0
*** Start of MTP Level 3 ***
                MSU
003 10000101 85
    ----0101    Service Indicator                       0101 - ISDN User Part
    --00----    Network Priority                        00 - priority 0
    10------    Network Indicator                       10 - National Network
004 00000110 06 Destination Point Code                  4-5-6
005 00000101 05
006 00000100 04
007 00000011 03 Origination Point Code                  1-2-3
008 00000010 02
009 00000001 01
010 00000000 00 Signaling Link Selection                0
*** Start of ISDN User Part ***
                Initial address Message
011 00000000 00 Circuit Identification Code             0
012 00000000 00
    --000000
    00------    Spare                                   0
013 00000001 01 Message Type                            01
                Nature of connection indicators
014 00000000 00
    ------00    Satellite Indicator                     00 - no satellite in the connection
    ----00--    Continuity check indicator              00 - continuity check not required
    ---0----    Echo Control Device Indicator           0 - outgoing half echo cntrl dev not inc
    000-----    Spare                                   0
                Forward call indicators
015 00000000 00
    -------0    Incoming International Call Indicator   0 - not an incoming international call
    -----00-    End-to-End Method Indicator             00 - no end-to-end method available
    ----0---    Interworking Indicator                  0 - no interworking encountered -all SS7
    ---0----    IAM Segmentation Indicator              0 - no indication
    --0-----    ISDN User Part Indicator                0 - ISDN user part not used all the way
    00------    ISDN User Part Preference Indicator     00 - ISDN-UP preferred all the way
016 00000000 00
    -------0    ISDN Access Indicator                  0 - originating access non-ISDN
```

```
    -----00-    SCCP Method Indicator                  00 - no indication
    ----0---    Spare                                  0
    0000----    Reserved for National Use              0
                Calling party's category
017 00000010 02 Calling party's category               00000010 - operator, language English
                Variable Portion
018 00000011 03 User service information Pointer       Offset 021
019 00000101 05 Called party number Pointer            Offset 024
020 00010001 11 Optional Portion Pointer               Offset 037
                User service information
021 00000010 02 User service information Length        2
                Octet 3
022 11000000 c0
    ---00000    Information transfer capability        00000 - speech
    -10-----    Coding Standard                        10 - national standard
    1-------    Extension                              01
                Octet 4
023 10010000 90
    ---10000    Information transfer rate              10000 - 64 kbit/s
    -00-----    Transfer mode                          00 - circuit mode
    1-------    Extension 4                            Excluded
                User information layers
                Called party number
024 00001100 0c Called party number Length             12
025 00000011 03
    -0000011    Nature of address indicator            national (significant) number
    0-------    Odd/even indicator                     0 - even number of address signals
                Octets 2-10
026 00010000 10
    ----0000    Spare                                  00
    -001----    Numbering plan                         001 - ISDN(Telephony) numbering plan
    0-------    Spare                                  00
027 00100001 21 Address                                12345678901234567890
028 01000011 43
029 01100101 65
030 10000111 87
031 00001001 09
032 00100001 21
033 01000011 43
034 01100101 65
035 10000111 87
036 00001001 09
                Optional Portion
                Generic Name
037 11000111 c7 Generic Name Type                      199
038 00010000 10 Generic Name Length                    16
039 00100000 20
    ------00    Presentation                           00 - Presentation Allowed
    ----00--    Spare                                  00
    ---0----    Availability                           0 - Name available, or unknown
    001-----    Type of Name                           01
040 01000001 41 NAME                                   ABCDEFGHIJKLMNO
041 01000010 42
042 01000011 43
043 01000100 44
044 01000101 45
045 01000110 46
046 01000111 47
047 01001000 48
048 01001001 49
049 01001010 4a
050 01001011 4b
051 01001100 4c
052 01001101 4d
053 01001110 4e
054 01001111 4f
055 00000000 00 End of optional parameters             00
```

The sections shown in bold type show which fields of an IAM with the PIP parameter are effected by the CNCF feature.

Output Example

```
Protocol Flavor: ANSI-SS7
Total Message Length: 59
*** Start of MTP Level 2 ***
                MTP
000 00000000 00
    -0000000    Backward Sequence Number                0
    0-------    Backward Indicator Bit                  0
001 00000000 00
    -0000000    Forward Sequence Number                 0
    0-------    Forward Indicator Bit                   0
002 00111000 38
    --111000    Length Indicator                        56
    00------    Spare                                   0
*** Start of MTP Level 3 ***
                MSU
003 10000101 85
    ----0101    Service Indicator                       0101 - ISDN User Part
    --00----    Network Priority                        00 - priority 0
    10------    Network Indicator                       10 - National Network
004 00000110 06 Destination Point Code                  4-5-6
005 00000101 05
006 00000100 04
007 00000011 03 Origination Point Code                  1-2-3
008 00000010 02
009 00000001 01
010 00000000 00 Signaling Link Selection                0
*** Start of ISDN User Part ***
                Initial address Message
011 00000000 00 Circuit Identification Code             0
012 00000000 00
    --000000
    00------    Spare                                   0
013 00000001 01 Message Type                            01
                Nature of connection indicators
014 00000000 00
    ------00    Satellite Indicator                     00 - no satellite in the connection
    ----00--    Continuity check indicator              00 - continuity check not required
    ---0----    Echo Control Device Indicator           0 - outgoing half echo cntrl dev not inc
    000-----    Spare                                   0
                Forward call indicators
015 00000000 00
    -------0    Incoming International Call Indicator   0 - not an incoming international call
    -----00-    End-to-End Method Indicator             00 - no end-to-end method available
    ----0---    Interworking Indicator                  0 - no interworking encountered -all SS7
    ---0----    IAM Segmentation Indicator              0 - no indication
    --0-----    ISDN User Part Indicator                0 - ISDN user part not used all the way
    00------    ISDN User Part Preference Indicator     00 - ISDN-UP preferred all the way
016 00000000 00
    -------0    ISDN Access Indicator                   0 - originating access non-ISDN
    -----00-    SCCP Method Indicator                   00 - no indication
    ----0---    Spare                                   0
    0000----    Reserved for National Use               0
                Calling party's category
017 00000010 02 Calling party's category                00000010 - operator, language English
                Variable Portion
018 00000011 03 User service information Pointer        Offset 021
019 00000101 05 Called party number Pointer             Offset 024
020 00010001 11 Optional Portion Pointer                Offset 037
                User service information
021 00000010 02 User service information Length         2
                Octet 3
022 11000000 c0
    ---00000    Information transfer capability         00000 - speech
    -10-----    Coding Standard                         10 - national standard
    1-------    Extension                               01
                Octet 4
023 10010000 90
    ---10000    Information transfer rate               10000 - 64 kbit/s
    -00-----    Transfer mode                           00 - circuit mode
```

```
    1-------    Extension 4                              Excluded
                User information layers
                Called party number
024 00001100 0c Called party number Length               12
025 00000011 03
    -0000011    Nature of address indicator              national (significant) number
    0-------    Odd/even indicator                       0 - even number of address signals
                Octets 2-10
026 00010000 10
    ----0000    Spare                                    00
    -001----    Numbering plan                           001 - ISDN(Telephony) numbering plan
    0-------    Spare                                    00
027 00100001 21 Address                                  12345678901234567890
028 01000011 43
029 01100101 65
030 10000111 87
031 00001001 09
032 00100001 21
033 01000011 43
034 01100101 65
035 10000111 87
036 00001001 09
                Optional Portion
                Party Information Parameter
037 11111100 fc Party Information Parameter Type         252
038 00010011 13 Party Information Parameter Length       19
039 11111110 fe Sub-Parameter Code                       254 - Name Information
040 00010001 11 Sub-Parameter Length                     17
041 00000001 01 Name Element Indicator                   01 - Calling Party Name
042 00001111 0f Name Element Length                      15
043 01000001 41 Name Information                         ABCDEFGHIJKLMNO
044 01000010 42
045 01000011 43
046 01000100 44
047 01000101 45
048 01000110 46
049 01000111 47
050 01001000 48
051 01001001 49
052 01001010 4a
053 01001011 4b
054 01001100 4c
055 01001101 4d
056 01001110 4e
057 01001111 4f
058 00000000 00 End of optional parameters               00
```

Calling Name Conversion Facility (CNCF) with Redirect Capability (Release 24.0)

Description

This feature provides a conversion of ISUP IAM messages using two versions of calling name identification presentation (CNIP) for calling name information delivery. One version of the CNIP uses the nonstandard, proprietary ISUP party information (PIP) parameter. The other version uses the ANSI standard ISUP generic name (GN) parameter. The conversion will either replace the PIP parameter with the GN parameter or the GN parameter with the PIP parameter in the ISUP IAM message.

The gateway screening feature is used to select which ISUP messages are converted. The incoming messages are selected based on the OPC and DPC in the routing label of the message, and the message type in the service information octet. The message type is defined by the value of the service indicator (**SI**) field of the SIO. ISUP

messages contain the value 5 in the service indicator field of the SIO. Screening rules for Allowed OPC, Allowed DPC, and the Allowed SIO entities must be configured in the database for this feature.

Refer to the *Database Administration Manual - Gateway Screening* for details on using this feature.

Unsolicited Information Messages

The commands **chg-scr-aftpc**, **chg-scr-cdpa**, **chg-scr-cgpa**, **chg-scr-tt**, **ent-scr-aftpc**, **ent-scr-cdpa**, **ent-scr-cgpa**, and **ent-scr-tt** cannot use any entry shown in the **rtrv-gws-actset** command output that contains the redirect stop action (**RDCT**) or the CNCF stop action (**CNCF**). This restriction is not enforced when the **chg-gws-actset** and the **chg-scr-aftpc**, **chg-scr-cdpa**, **chg-scr-cgpa**, **chg-scr-tt**, **ent-scr-aftpc**, **ent-scr-cdpa**, **ent-scr-cgpa**, and **ent-scr-tt** commands are entered into the database. The database will accept these commands using entries from the gateway screening stop action table, but when the EAGLE encounters MSUs that pass gateway screening at the AFTPC, CDPA, CGPA or TT screens, these UIMs (unsolicited information messages) are generated indicating that gateway screening received a MSU that could not be redirected or converted.

UIM 1125 – Gateway Screening received a Called Party Address that could not be Redirected for the DTA feature

```
RLGHNCXA03W 99-01-07 00:57:31 EST Rel 24.0.0
1001.1125    CARD 1103,A  INFO         GWS rcvd CDPA that could not be RDCTd
             SIO=03   OPC=001-001-001  DPC=002-002-002
             SCCP MT= 18
             CDPA:  AI=10  PC=003-003-003  SSN=005  TT=250  ADDR=1234567890
             CGPA:  AI=10  PC=004-004-004  SSN=005  TT=251  ADDR=1234567890
             SR=scrb  LSN=A1234567
      Report Date: 98-09-07  Time: 16:27:19
```

UIM 1126 – Gateway Screening received a Calling Party Address that could not be Redirected for the DTA feature

```
RLGHNCXA03W 99-01-07 00:57:31 EST Rel 24.0.0
1002.1126    CARD 1103,A  INFO         GWS rcvd CGPA that could not be RDCTd
             SIO=03   OPC=001-001-001  DPC=002-002-002
             SCCP MT= 18
             CDPA:  AI=10  PC=003-003-003  SSN=005  TT=250  ADDR=1234567890
             CGPA:  AI=10  PC=004-004-004  SSN=005  TT=251  ADDR=1234567890
             SR=scrb  LSN=A1234567
      Report Date: 98-09-07  Time: 16:27:19
```

UIM 1127 – Gateway Screening received an Affected Point Code that could not be Redirected for the DTA feature

```
RLGHNCXA03W 99-01-07 00:57:31 EST Rel 24.0.0
1003.1127    CARD 1103,A  INFO         GWS rcvd AFTPC that could not be RDCTd
             SIO=03   OPC=001-001-001  DPC=002-002-002
             SCCP MT= 18
             CDPA:  AI=10  PC=003-003-003  SSN=005  TT=250  ADDR=1234567890
             CGPA:  AI=10  PC=004-004-004  SSN=005  TT=251  ADDR=1234567890
             SR=scrb  LSN=A1234567
      Report Date: 98-09-07  Time: 16:27:19
```

UIM 1128 – Gateway Screening received a Translation Type that could not be Redirected for the DTA feature

```
RLGHNCXA03W 99-01-07 00:57:31 EST Rel 24.0.0
1004.1128    CARD 1103,A  INFO         GWS rcvd TT that could not be RDCTd
             SIO=03   OPC=001-001-001  DPC=002-002-002
             SCCP MT= 18
             CDPA:  AI=10  PC=003-003-003  SSN=005  TT=250  ADDR=1234567890
```

```
             CGPA:  AI=10  PC=004-004-004  SSN=005  TT=251  ADDR=1234567890
             SR=scrb  LSN=A1234567
      Report Date: 98-09-07  Time: 16:27:19
```

UIM 1215 – Gateway Screening received a Called Party Address that could not be processed by the Calling Name Conversion Facility feature

```
RLGHNCXA03W 99-01-07 00:57:31 EST Rel 24.0.0
1005.1215    CARD 1103,A  INFO         GWS rcvd CDPA that could not be CNCFd
             SIO=03   OPC=001-001-001  DPC=002-002-002
             SCCP MT= 18
             CDPA:  AI=10  PC=003-003-003  SSN=005  TT=250  ADDR=1234567890
             CGPA:  AI=10  PC=004-004-004  SSN=005  TT=251  ADDR=1234567890
             SR=scrb  LSN=A1234567
      Report Date: 98-09-07  Time: 16:27:19
```

UIM 1216 – Gateway Screening received a Calling Party Address that could not be processed by the Calling Name Conversion Facility feature

```
RLGHNCXA03W 99-01-07 00:57:31 EST Rel 24.0.0
1006.1216    CARD 1103,A  INFO         GWS rcvd CGPA that could not be CNCFd
             SIO=03   OPC=001-001-001  DPC=002-002-002
             SCCP MT= 18
             CDPA:  AI=10  PC=003-003-003  SSN=005  TT=250  ADDR=1234567890
             CGPA:  AI=10  PC=004-004-004  SSN=005  TT=251  ADDR=1234567890
             SR=scrb  LSN=A1234567
      Report Date: 98-09-07  Time: 16:27:19
```

UIM 1217 – Gateway Screening received an Affected Point Code that could not be processed by the Calling Name Conversion Facility feature

```
RLGHNCXA03W 99-01-07 00:57:31 EST Rel 24.0.0
1007.1217    CARD 1103,A  INFO         GWS rcvd AFTPC that could not be CNCFd
             SIO=03   OPC=001-001-001  DPC=002-002-002
             SCCP MT= 18
             CDPA:  AI=10  PC=003-003-003  SSN=005  TT=250  ADDR=1234567890
             CGPA:  AI=10  PC=004-004-004  SSN=005  TT=251  ADDR=1234567890
             SR=scrb  LSN=A1234567
      Report Date: 98-09-07  Time: 16:27:19
```

UIM 1218 – Gateway Screening received a Translation Type that could not be processed by the Calling Name Conversion Facility feature

```
RLGHNCXA03W 99-01-07 00:57:31 EST Rel 24.0.0
1008.1218    CARD 1103,A  INFO         GWS rcvd TT that could not be CNCFd
             SIO=03   OPC=001-001-001  DPC=002-002-002
             SCCP MT= 18
             CDPA:  AI=10  PC=003-003-003  SSN=005  TT=250  ADDR=1234567890
             CGPA:  AI=10  PC=004-004-004  SSN=005  TT=251  ADDR=1234567890
             SR=scrb  LSN=A1234567
      Report Date: 98-09-07  Time: 16:27:19
```

In order to stop these UIMs from being generated, the gateway screening rule shown in the UIM must be identified. Once the gateway screening rule has been identified, a gateway screening change command can be used either to remove the gateway screening action set name or change the gateway screening action set name to a different gateway screening action set not containing the CNCF or redirect gateway screening stop actions. The gateway screening stop action set can also be changed with the **chg-gws-actset** command to remove the redirect or CNCF gateway screening stop actions. However, this could keep other gateway screening rules from redirecting or converting MSUs passing gateway screening from the BLKOPC, BLKDPC, SIO, OPC, DPC, or DESTFLD screens.

CDU for DSM (Release 26.05)

CDU (CAP Downloadable Utility) is an existing software platform for diagnostics used by manufacturing in identifying and isolating expansion memory problems in the EAGLE cards quickly and reliably. This feature ports the existing CDU and provides an efficient “go/no go” memory test for the DSM/DCM card.

CDU Port

The existing CDU utility has been ported for the DSM/DCM card, and a new GPL VCDU has been created. The new GPL has all the existing functionality. The DSM board can hold up to 4GB of memory. The CDU or the VCDU utility is downloaded automatically, depending on the type of the board. For the DSM, the VCDU utility is downloaded; for the other boards, the CDU utility is downloaded.

The CDU or the VCDU can be downloaded into any card with the following command:

```
 alw-card:loc=xxxx:code=utility
```

The following **act-memtst** command used with the parameter set to "**fast**" lets the VCDU utility test 4GB of memory in 4 hours:

```
 cdu:loc=xxxx:cmd=
" ACT-MEMTST:BEG=H'100000:END=H'200000 :TYPE=FAST
"
```

Quick Test

The quick go/no go test is implemented with the **ACT-QCKTST** command in CDU/VCDU. Using this command, the VCDU utility can check the basic integrity of the memory within 10 minutes. This test includes verifying the address and data lines to the memory, and verifying accessibility of each memory chip of 4GB.

Ping Test

The VCDU utility uses a new command, **act-pingtst**, to test the network. The ping test applies to the DCM/DSM card only.

```
 cdu:loc=xxxx:cmd=
" act-pingtst:port=<a/b>:dest=<ip_address> :router=<router>:loop=n
"
```

This command activates the ping test. The **port** parameter specifies the origination address. The **dest** parameter specifies the destination address to be pinged. The **router** parameter is an optional parameter that specifies the router through which the network interface can be tested. The **loop** parameter specifies the number of times the test should be run before termination.

CgPA GWS Routing Indicator Enhancement (Release 31.3)

The wildcarding of the CgPA routing indicator (RI=*) produced 2 entries in the GWS database on the LIM card; that reduced the number of CgPA rules available to the customer from 4000 to 2000 per screenset.

The wildcarding has been changed to produce a single database entry for wildcard (*) of the routing indicator in CgPA GWS screening rules. The EAGLE does not expand the provisioned wildcard routing indicator into multiple rules in the bound screenset.

Upgrade to Release 31.3 auto consolidates existing entries that were provisioned with RI=*.

Change Default ATM CLP Bit for Data Cells from 1 to 0 (Release 31.3)

The Cell Loss Priority (CLP) bit is in the ATM packet header and is used by ATM network elements to determine which messages are discarded when an ATM network element is in congestion. Should there be congestion in an ATM network element, it will first start to discard ATM packets with a CLP bit of 1 first before discarding any ATM packets with a CLP bit of 0. The CLP bit has the following characteristics:1. The CLP bit for ATM-SS7 signaling (data cells) is specified to be either be 0 or 1 and is not specifically assigned a default value in GR-2878 CORE (ANSI) nor I.361 (ITU). The CLP bit for ATM unassigned/idle (filler) cells is specified to be 0 for T1 interfaces and 1 for E1 interfaces. ATM equipment is required to discard these cells upon receipt and therefore the CLP bit for unassigned/idle (filler) cells will remain unchanged.2. The CLP bit for ATM-SS7 signaling (data cells) is used by ATM network equipment much in a similar fashion as the priority field is used by TDM SS7 equipment 3. The CLP bit determines how important a message is when an ATM network node is in congestion and needs to discard messages/packets. Currently, the CLP bit for ATM-SS7 signaling (data cells) is a non-configurable value in the EAGLE ATM header that is defaulted to 1 for both LIM-ATM (ANSI) and E1-ATM (ITU) cards. Effective in Release 31.3, this default will be changed to 0 (higher priority). The new CLP bit value of 0 has a higher priority than the current CLP bit value of 1.

Changeover and Changeback Procedure for Processor Outage and LIN (Release 21.0)

Currently, the EAGLE performs a sequence controlled changeover instead of a time-controlled changeover when the signaling link gets locally or remotely inhibited or when a local or remote processor outage condition is entered. In these cases, sending a changeover order could result in failure of the signaling link. The EAGLE also sends SIPOs when a signaling link is remotely or locally inhibited and also performs a sequence controlled changeover by sending a changeover order to the remote end.

With this release, the EAGLE now performs a time controlled changeover under these conditions. The EAGLE behaves in the following manner:

- When the signaling link is inhibited locally or remotely, the EAGLE does not send SIPOs. Instead a time diversion changeover procedure is started for the inhibited signaling link.
- When the signaling link is unavailable because of a remote or local processor outage, a time controlled changeover is performed instead of sequence controlled changeover.

If a changeover order is received for the unavailable link, while the level 3 T1 timer is in progress, the buffer updating procedure and sequence controlled changeover is performed. The EAGLE responds with an emergency changeover acknowledgment if the changeover order is received after the level 3 T1 timer has expired.

This feature applies to both ANSI and ITU signaling links. This feature has no impact on X.25 gateway signaling links since the inhibit and processor outage procedures are not used in the X.25 protocol.

Cluster Routing and Management Diversity (Release 21.0)

Description

The cluster routing and management diversity feature eliminates the need for a full point code entry in the routing table to route to every signaling point in every network. The cluster routing and management diversity feature allows the EAGLE to configure one route set to a entire cluster of destinations. This allows the EAGLE to manage and switch traffic to more end nodes.

A cluster is defined as a group of signaling points whose point codes have identical values for the network and cluster fields of the point codes. A cluster entry in the routing table is shown with an asterisk (*) in the member field of the point code, for example, 111-011-*. Cluster entries can only be provisioned as ANSI destination point codes. ANSI destination point codes can be specified as either a full point code, for example, 123-043-045, or as a cluster of signaling point codes, for example, 111-011-*.

Provisioning of clusters as well as full point codes that belong to the same cluster as destination point codes is also supported. The point codes 111-011-*, 111-011-005 and 111-011-045 entries can be provisioned. The cluster destination point code 111-011-* represents all the point codes of the cluster except for point codes 111-011-005 and 111-011-045. Cluster entries in the destination point code table can also be used as a destination point code (DPC) for a route. A group of such routes with varying relative cost forms a routeset to a cluster just like a routeset to a full point code.

Exception Lists (X-lists)

An exception list for a cluster is a list of point codes in a cluster whose route status is more restricted than the corresponding route status of that cluster. The term “more restricted” is used when comparing the route status of a cluster member to the route status of the cluster. A PROHIBITED status is more restrictive than a RESTRICTED status and a RESTRICTED status is more restrictive than an ALLOWED status. This list contains point codes that are not assigned to any individual routeset and the only routesets to that node is through a cluster routeset. The exception list is a dynamic list that changes when the status of the cluster routeset or any member routesets in that cluster changes.

For each cluster, the user can specify an exception list exclusion indicator (ELEI) when configuring the cluster point code with the **ent-dstn** command. When the ELEI is **yes**, the EAGLE does not maintain exception list entries. When the ELEI is **no**, the EAGLE maintains exception list entries.

Exception list entries are stored as an extension of the destination point code table, which can contain up to 2500 entries. The EAGLE allows the user to specify the number of entries reserved for the exception list, between 500 to 2000 entries. The remainder of the 2500 entries in the destination point code table are reserved for the full and cluster point codes.

The outputs of the **ent-dstn**, **dlt-dstn**, **chg-dstn**, and **rtrv-dstn** commands display the following destination point code usage information.

- The number of configured full point codes
- The number of configured cluster point codes
- The sum of configured destinations (full and cluster point codes)
- The number of entries reserved for configured destinations (full and cluster point codes). This number is 2500 minus the number of entries reserved for the exception list.

- The number of entries reserved for exception list

There is an STP-wide expiration time value for exception list entries. This timer specifies the amount of time an idle exception list entry can be in the exception list before it is discarded. When this timer expires, unsolicited information message (UIM) 1146, REPT-SLST-TIMO: X-LIST entry expired, is displayed on the terminal and the specified exception list entry is discarded. The following is an example of UIM 1146.

Output Example:

```
RLGHNCXA03W 96-04-16 16:21:11 EDT Rel 21.0.0
1234.1146    CARD 1101    INFO  REPT-XLST-TIMO: X-LIST entry expired
             DPC=011-212-033
Report Date: 96-04-16  Time: 16:20:19
```

In this example, the point code (DPC) 011-212-033 was in the exception list, the timer expired, and the point code was discarded from the exception list.

The value of the exception list timer is shown in the MTPXLET field of the **rtrv-stpopts** command output and is configured with the **mtpxlet** parameter of the **chg-stpopts** command.

The **rtrv-stpopts** command output contains three other fields that show the parameters of the exception list, MTPXLQ, MTPXLOT, and MTPDPCQ.

The MTPXLQ field shows the maximum number of entries the exception list (x-list) can contain. This value is configured with the **mtpxlq** parameter of the **chg-stpopts** command.

The MTPXLOT field shows the exception list (x-list) occupancy threshold (in terms of the percentage of the exception list space being used). The percentage of occupancy threshold is configured with the **mtpxlot** parameter of the **chg-stpopts** command. The default value for the threshold is 90%. For example, if there are 1500 entries configured for the exception list and the exception list contains 1000 entries, the percentage of the exception list space being used is 66%. If this threshold is exceeded, a minor alarm, unsolicited alarm message (UAM) 321, X-LIST occupancy threshold exceeded, is displayed. The following is an example of UAM 321.

UAM Messages

```
    RLGHNCXA03W 96-04-16 16:21:11 EDT Rel 21.0.0
*   0061.0321  * XLIST                X-LIST occupancy threshold exceeded
```

The MTPDPCQ field shows the maximum number of destination point codes that can be configured in the EAGLE.

The EAGLE raises a major alarm, UAM 338, X-LIST space full-entry(s) discarded, when the exception list becomes completely full and the EAGLE fails to create any more exception list entries. The following is an example of UAM 338.

```
    RLGHNCXA03W 96-04-16 16:21:11 EDT Rel 21.0.0
**  0055.0338 ** SYSTEM               X-LIST space full-entry(s) discarded
```

An exception list entry's expiration timer is restarted when an exception list entry gets created, updated, or used for routing. This expiration timer can be set for a minimum of 20 minutes to a maximum of 24 hours. The default value for the expiration timer upon system start-up is 60 minutes. If the timer expires before it is restarted, the exception list entry is removed. The expiration timer allows the EAGLE to save resources if the exception list entry is sitting idle for a specified period of time.

An exception list entry can be created for three distinct set of conditions.

1. The first set of conditions creates exception list entries based on the status of the route (allowed, restricted, or prohibited) and are marked as “exception list due to routing.”

2. The EAGLE creates an exception list entry to maintain the congestion status of a non-provisioned, cluster routed destination point code. These entries are marked “exception list due to congestion.”

3. The EAGLE also creates an exception list to prohibit routing to a member of a cluster when circular routing to that member is detected. These exception list entries are marked “exception list due to circular routing.”

An exception list entry for a particular cluster can be removed from the exception list when the following conditions are met:

1. The status of all routes to the specified point code changes to a status that is less or equally restrictive than corresponding status of cluster’s routes. This can happen for two reasons.

    a. A **dact-rstst** command was issued. The **dact-rstst** command changes the route’s status to allowed.

    b. A network management message (TFA or TFR) was received indicating the new status of the route to the specified point code.

2. The expiration timer for the exception list entry expires.

3. When a **chg-dstn** command is issued and changes the ELEI to **yes** for the cluster; the EAGLE removes all exception list entries created for that cluster.

4. The **chg-stpopts** command was issued with the **mtpxlet** parameter and the new value for the **mtpxlet** parameter was smaller than the original value. This command can change allocation of routing table entries for exception lists. If the size of the exception list is reduced and the number of entries in the exception list is now greater than the new value of the **mtpxlet** parameter, the EAGLE will remove excess exception list entries at random.

5. When a user allows a circular routed “exception list due to circular routing” entry after fixing the problem. The **rst-dstn** command is used to allow the routing.

6. When congestion abates for an “exception list due to routing” entry.

Cluster Routing

When the EAGLE receives an MSU to route, the routing function looks for the MSUs destination point code as a full point code entry in the routing table. If found, the full point code entry is used to find the corresponding routeset and the outgoing route. If a full point code entry is not found, the routing function uses the destination point code’s network and cluster values to find a cluster entry to which a destination point code belongs. If found, the cluster entry is used to find the corresponding routeset and the outgoing route. If neither a full point code entry or cluster point code entry is found, the EAGLE generates UAM 1004, “MTP rcvd unknown DPC.”

Compatibility with Non-Cluster Routing STPs

It is possible that not all STPs in the network that the EAGLE is operating in are cluster routing STPs. In such a situation, those STPs not doing cluster routing will interpret TCx messages and apply them to each individual

point code belonging to the concerned cluster. This may cause an inconsistency in the status records for exception listed point codes in different STPs. In order to avoid this situation, the EAGLE takes the following steps:

1. After broadcasting a TCR message for a cluster, the EAGLE enables TFPs for the cluster's exception listed prohibited member point codes by stopping the level 3 T8 timer. This allows TFPs to be sent for prohibited members immediately after a TCR is broadcast.

2. After broadcasting a TCA message for a cluster, the EAGLE enables a one-time TFR for the cluster's exception listed restricted member point codes by stopping the level 3 T18 timer and enables the TFPs for the cluster's exception listed (prohibited) member point codes by stopping the level 3 T8 timer. This allows TFPs to be sent for prohibited members and TFRs for restricted members immediately after a TCA is broadcast.

Compatibility with the ITU Network and X.25 Gateway

ITU SS7 networks do not use the concept of clusters of point codes and cluster network management messages. The EAGLE does not generate TCx messages towards ITU nodes. The EAGLE does not send TCx messages to adjacent ITU point codes during the broadcast phase of TCx messages when the EAGLE is acting as an STP between an ITU network and an ANSI network. It is possible that messages may be lost in such a case. In order to reduce message loss and quickly notify the sending ITU node about the status, the EAGLE enables TFPs or TFRs immediately (with the level 3 T8 or T18 timers stopped) and relies on the TFPs or TFRs to convey the status information.

While sending response method network management messages in response to a received MSU, the EAGLE checks the MSU's originating point code. If the MSU's originating point code is an ITU point code, a TFx message is returned.

Cluster entries can only be provisioned as ANSI destination point codes. Cluster entries cannot be provisioned for ITU international or ITU national destination point codes. The ANSI alias point code for an ITU international or ITU national destination point code must be a full point code. Cluster routing is not supported for X.25 destinations. X.25 destinations and any alias point codes used for X.25 destinations must be full point code entries.

Cluster Management When the Cluster Routing Feature is Turned Off

Cluster routing is an optional feature and can be turned on with the **chg-feat:crmd=on** command. Once this feature is turned on, it cannot be turned off. If this feature is turned off, the EAGLE does not send any cluster management messages or allow cluster destination point codes to be added to the destination point code table. The EAGLE is capable of processing incoming cluster management messages even though the feature is turned off. When a cluster management message is received, the EAGLE treats this message as though network management messages were received for each full point code, configured in the destination point code table, belonging to that cluster.

Command Class Management (Release 29.0)

Description

The Command Class Management feature allows the user to place EAGLE commands into 32 new configurable command classes. The craftsperson can provision any of these configurable command classes to contain any of the EAGLE commands. The command classes can then be assigned to a user and/or terminal, thus allowing the

user or terminal the privilege of executing any command in the class. This allows users and terminals to fully configure custom command classes. This capability is controlled via a feature access key.

NOTE: The result is each user/terminal will have access to a set of commands tailored to a specific need. The new configurable command classes are in addition to the existing non-configurable command classes. The current basic and non-configurable command classes will remain.

Refer to the *Commands Manual* for current detailed information on this feature.

Hardware Requirements

No new hardware is needed to support this feature.

Limitations

There is a limitation on the feature's operation regarding the use of the **ENT-USER**, **CHG-USER**, **CHG-SECU-TRM** and **CHG-CMD** commands. These commands can assign a maximum of eight command classes per command execution. However, subsequent command executions can be used to readily assign the full number of required configurable command classes.

Command Output Changes (Release 22.0)

The method of displaying whether the **copy=yes** or **redirect=yes** parameters have been specified for a given screening entry in the gateway screening retrieve commands has been changed. The heading of the NSR field of the output has been changed to NSR/ACT to display either the next screening reference name (NSR) or the next action that is to be performed (ACT). The same field can be used to display both of these items, because in previous releases, the NSR field is blank when the **copy=yes** and **redirect=yes** parameters have been specified. These parameters can only be specified when the NSFI is set to **stop** and the **nsr** parameter cannot be specified.

If the NSFI of the screen is not **stop** or **fail**, the NSR/ACT field displays the name of the next screening table to be used in the gateway screening process.

When NSFI of the screen is **stop**, the NSR/ACT field contains the following entries.

- -, - — if neither the **copy=yes** or **redirect=yes** parameters have been specified. This entry is also displayed if the NSFI of the screen is **fail** (only with the **rtrv-scr-blkdpc** and **rtrv-scr-blkopc** commands)
- C, - — if only the **copy=yes** parameter has been specified
- -, R — if only the **redirect=yes** parameter has been specified
- C, R — if both the **copy=yes** and **redirect=yes** parameters have been specified

Refer to the *Commands Manual* for current command information..

The outputs of these commands have been changed to this new format.

- **rtrv-scr-opc**

- **rtrv-scr-dpc**
- **rtrv-scr-blkdpc**
- **rtrv-scr-blkopc**
- **rtrv-scr-destfld**
- **rtrv-scr-sio**
- **rtrv-scr-cgpa**
- **rtrv-scr-cdpa**
- **rtrv-scr-aftpc**
- **rtrv-scr-tt**
- **rtrv-scrset**

Configuring the Frequency of RST Messages on Low Priority Routes (Release 22.0)

This feature allows the configuring of a timer to specify the frequency of signaling-route-set-test messages for routes of lower priority than the current route.

In earlier releases, the routeset test messages were sent for every route to every destination for a period of time equal to the value of the level 3 timer T10. With this feature, the EAGLE only sends the routeset test messages for routes of equal or higher priority that the current route.

Parameters

To send routeset test messages for lower priority routes, new parameters (**mtplprst** and **mtpt10alt**) have been added to the **chg-stpopts** command to turn this capability on and to set the timer to control the frequency that the routeset test messages are sent.

mtplprst — turns on or off the routeset test message for lower priority routes capability. The values for this parameter is **yes** or **no**. The default value for this parameter is **yes**.

mtpt10alt —the timer to control the frequency at which the routeset test messages are sent. The values for this parameter are from 30 to 10,000 milliseconds. The default value for this parameter is equal to the value of the level 3 T10 timer.

When the **mtplprst=no** parameter is specified with the **chg-stpopts** command, the EAGLE does not send routeset test messages for the lower priority routes. When the **mtplprst=yes** parameter is specified, the EAGLE sends routeset test messages at intervals specified by the value of the **mtpt10alt** parameter.

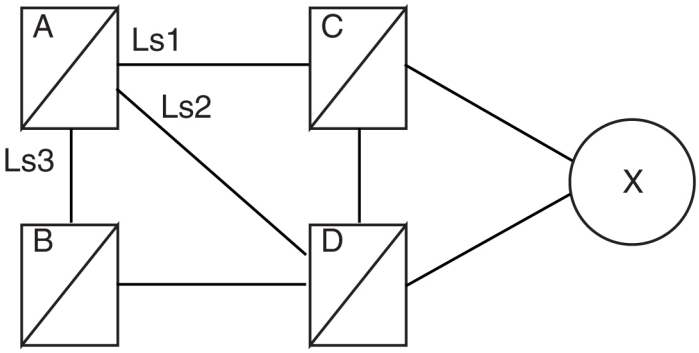
The network example shown in Figure *Route Set Test Example* shows how this feature works. The following table shows the priorities of the routesets to destination X.

Table 2-12. Routeset Priorities

Routesets to Destination X	Cost
Ls1 (high priority route)	10
Ls2 (current route)	20
Ls3 (low priority route)	30

Destination X is currently accessible from STP A using route Ls2. STP C and STP B have sent TFP messages for destination X to STP A. STP C is on higher priority route than the current route while STP B is on lower priority route than the current route. By default, the EAGLE polls STPs B and C by sending RSP messages for destination X at intervals defined by the level 3 timer T10. The polling frequency to STP B can be changed by changing low priority route set test time interval with the **mtpt10alt** parameter of the **chg-stpopts** command and setting it to a value greater than the value of the level 3 timer T10. RSP messages for destination X are sent to STP C at intervals defined by the level 3 timer T10 and RSP message for destination X are sent to STP B at intervals defined by the **mtpt10alt** parameter.

Figure 2-11. Route Set Test Example



The level 3 T10 timer and **mtpt10alt** parameter of the **chg-stpopts** command are configured independently. The EAGLE requires that the value of the **mtpt10alt** parameter is greater than or equal to the value of the level 3 T10 timer. If the value of the level 3 T10 timer is increased to a value greater than the current value of the **mtpt10alt** parameter, the value of the **mtpt10alt** parameter is adjusted to be equal to the new value of the level 3 T10 timer and the following message is displayed in the scroll area of the terminal.

MTP T10alt Timer in STP Options Table adjusted to correspond with T10 Timer.

If the value of the level 3 T10 timer is decreased, the value of the **mtpt10alt** parameter is not adjusted.

Any changes in the values of the level 3 T10 timer and the **mtpt10alt** parameter of the **chg-stpopts** command take affect only after these timers have expired.

Configuring the Unauthorized Use Warning Message (Release 22.0)

Currently, the EAGLE displays the following message immediately after successfully logging into the EAGLE.

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

In Release 22.0, the user can now configure their own warning message that follows a successful login. The message can contain up to 20 lines of text with each line of text containing up to 70 characters.

When a login attempt is successful, the user sees the warning message (0 - 20 lines) and then 2 lines of login history information. The administrator can configure the warning message so that it and the login history information will not all fit into the scroll area of the EAGLE terminal. The user can use scroll area locking (F8) key so the login warning message can be read before it scrolls out of view.

NOTE: When the EAGLE is delivered to the user, the database will contain the following login warning message. This complies with the suggested Bellcore default values.

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

The **chg-secu-dflt** and **rtrv-secu-dflt** commands have been modified to configure this warning message.

Two parameters have been added to the **chg-secu-dflt** command to configure the login warning message, **wrnln** and **wrntx**.

The **wrnln** parameter specifies the line number of the login warning message that is being changed. The values for this parameter are from 1 to 20.

The **wrntx** parameter specifies the text for the line number of the login warning message. The text line can contain up to 70 alphanumeric characters and must be enclosed in quotes (“). A text line with no characters can be specified with this text string, “”. This prevents the text line from being displayed in the login warning message. A blank line is specified with this text string, ““.

The following is an example of how the login warning message can be configured.

Input Examples:

```
CHG-SECU-DFLT:WRNLN=1:WRNTX="*******************************************************"
CHG-SECU-DFLT:WRNLN=2:WRNTX="*  NOTICE: This is a private computer system.       *"
CHG-SECU-DFLT:WRNLN=3:WRNTX="*  UNAUTHORIZED ACCESS OR USE WILL BE PROSECUTED    *"
CHG-SECU-DFLT:WRNLN=4:WRNTX="*                                                   *"
CHG-SECU-DFLT:WRNLN=5:WRNTX="*                                                   *"
CHG-SECU-DFLT:WRNLN=6:WRNTX="* 06/07/97 Notice!!! EAGLE will be upgraded between *"
CHG-SECU-DFLT:WRNLN=7:WRNTX="*                 the hours of 2am-3am on 06/15/97. *"
CHG-SECU-DFLT:WRNLN=8:WRNTX="*                                                   *"
CHG-SECU-DFLT:WRNLN=9:WRNTX="*                                                   *"
CHG-SECU-DFLT:WRNLN=10:WRNTX="*******************************************************"
CHG-SECU-DFLT:WRNLN=11:WRNTX=" "
CHG-SECU-DFLT:WRNLN=12:WRNTX=""
CHG-SECU-DFLT:WRNLN=13:WRNTX=""
CHG-SECU-DFLT:WRNLN=14:WRNTX=""
CHG-SECU-DFLT:WRNLN=15:WRNTX=""
CHG-SECU-DFLT:WRNLN=16:WRNTX=""
CHG-SECU-DFLT:WRNLN=17:WRNTX=""
CHG-SECU-DFLT:WRNLN=18:WRNTX=""
CHG-SECU-DFLT:WRNLN=19:WRNTX=""
CHG-SECU-DFLT:WRNLN=20:WRNTX=""
```

The following is an example of what this example login warning message would look like after a successful login attempt.

Output Example:

```
**************************************************
*NOTICE: This is a private computer system.
**UNAUTHORIZED ACCESS OR USE WILL BE PROSECUTED
**
**
**06/07/97 Notice!!! EAGLE will be upgraded between

**the hours of 2am-3am on 06/15/97
```

```
**
**
******************************************************
0 LOGIN failures since last successful LOGIN
Last successful LOGIN was on port 3 on 97-06-07 @ 12:12:35
```

The parameter **msg** (with the values **yes** or **no**) has been added to the **rtrv-secu-dflt** command to display the text of each line of the login warning message. If the **msg=yes** parameter is specified, the security defaults for user IDs and passwords and the 20 lines of text for the login warning message are displayed. If the **msg=no** parameter (the default value for this parameter) is specified, the security defaults for user IDs and passwords are displayed, but the login warning message text lines are not displayed. The following is an example of the **rtrv-secu-dflt:msg=yes** command output.

Output Example:

```
RLGHNCXA03W 97-06-07 16:02:05 EDT  Rel 22.0.0
SECURITY DEFAULTS
-----------------
PAGE           60
UOUT           90
MULTLOG        NO
MINLEN          8
ALPHA           1
NUM             1
NC              1
WARNING MESSAGE
---------------
1:"******************************************************"
2:"*  NOTICE: This is a private computer system.       *"
3:"*  UNAUTHORIZED ACCESS OR USE WILL BE PROSECUTED    *"
4:"*                                                   *"
5:"*                                                   *"
6:"* 06/07/97 Notice!!! EAGLE will be upgraded between *"
7:"*                 the hours of 2am-3am on 06/15/97. *"
8:"*                                                   *"
9:"*                                                   *"
10:"******************************************************"
11:" "
12:""
13:""
14:""
15:""
16:""
17:""
18:""
19:""
20:""
```

Congestion Abatement Reporting (Release 21.0)

When a signaling link's congestion level changes, these changes are reported to the user as UAMs (unsolicited alarm messages), whether the congestion level increases or decreases. The UAMs show how the signaling link congestion level has changed. The following table shows the changes in the signaling link congestion level changes and the UAM that reports these changes. No alarms are associated with these UAMs.

Table 2-13. Signaling Link Congestion Messages

From Level	To Level	Output Messages	UAM
0	1	REPT-LINK-CGST: congestion level 0 to 1	0264
0	2	REPT-LINK-CGST: congestion level 0 to 1	0264

From Level	To Level	Output Messages	UAM
		REPT-LINK-CGST: congestion level 1 to 2	0265
0	3	REPT-LINK-CGST: congestion level 0 to 1 REPT-LINK-CGST: congestion level 1 to 2 REPT-LINK-CGST: congestion level 2 to 3	0264 0265 0266
1	0	RCVRY-LINK-CGST: congestion has cleared	0269
1	2	REPT-LINK-CGST: congestion level 1 to 2	0265
1	3	REPT-LINK-CGST: congestion level 1 to 2 REPT-LINK-CGST: congestion level 2 to 3	0265 0266
2	0	RCVRY-LINK-CGST: congestion level 2 to 1 RCVRY-LINK-CGST: congestion has cleared	0268 0269
2	1	RCVRY-LINK-CGST: congestion level 2 to 1	0268
2	3	REPT-LINK-CGST: congestion level 2 to 3	0266
3	0	REPT-LINK-CGST: congestion level 3 to 2 RCVRY-LINK-CGST: congestion level 2 to 1 RCVRY-LINK-CGST: congestion has cleared	0267 0268 0269
3	1	REPT-LINK-CGST: congestion level 3 to 2 RCVRY-LINK-CGST: congestion level 2 to 1	0267 0268
3	2	REPT-LINK-CGST: congestion level 3 to 2	0267

Cost Factor on Routing (Release 20.0)

This feature allows the assignment of a weighting factor to a route. The weighting factor is then used by MTP routing to determine which is the primary route, and which are the alternate routes. By using this feature, multiple routes may be assigned to a destination, with a primary route selected for all routing unless congestion or some other condition should be encountered, at which point one of the alternate routes would be chosen.

Each routeset (which is a combination or routes) may be assigned six routes, with each route assigned a different cost factor. The range for cost factors is 0 to 99, with 99 being the least favorable route (highest cost).

Combined linksets may be assigned the same cost factor, allowing equal load sharing over the two linksets. Alternate combined linksets may also be created by assigning a higher cost factor to subsequent linksets.

Consistent Command Response Conversion (Releases 22.0, 24.0)

The consistent Command Response Conversion feature enables GUI software to read a consistent command response from the EAGLE STP and display the information in a suitable format and language on Keyboard Send/ Receive (KSR)-mode-provisioned ports. This requirement fulfills the GUI’s requirement to know when an EAGLE-initiated command is completed.

Command Execution

To ensure reliability and uniqueness of pattern, a sequence of eight End of Transmission (EOT) characters (h'04) is used to indicate that the entered command has completed. These End of Transmission characters are not visible on the terminal display. This sequence, in most cases, means that all associated data output in response to the command entered has been displayed. Exceptions in which data output between the start of a command and the receipt of the EOTs may differ from the norm include the following:

- Commands with delayed completion that allow other output to be displayed (for example, **copy-disk** and **format-disk**).
- Commands that report completion but actually continue displaying results for some amount of time (for example, **rept-meas**).
- Commands entered in midstream of unsolicited output via Ctrl-A. For example:

Output Example for Release 22.2:

```
lnpstp 97-12-30 18:02:07 EST Rel 22.2.0.0
Error writing table 206:   on standby TDM (A);
>set-date:date=971201
Command Accepted - Processing
      DMS0002:table not found on disk[H'290e].
;
   lnpstp 97-12-30 18:02:07 EST Rel 220.18.0.0    set-date:date=971201    Command entered at terminal
#5.
;
   lnpstp 97-12-30 18:02:07 EST Rel 220.18.0.0    Date set complete. ;(Response Ended - string of
EOTs here)
```

Output Example for Release 24.0:

```
RLGHNCXA03W 99-01-07 00:57:31 EST Rel 24.0.0
Error writing table 206:
  on standby TDM (A);
>set-date:date=990301
Command Accepted - Processing
  DMS0002:table not found on disk[H'290e].
;
RLGHNCXA03W 99-01-07 00:57:31 EST Rel 24.0.0
set-date:date=990301
Command entered at terminal #5.
;
RLGHNCXA03W 99-03-01 00:57:31 EST Rel 24.0.0
Date set complete.
;(Response Ended - string of EOTs here
```

CSPC Increase in Groups (Release 34.0)

The maximum number of point codes that can be provisioned in a Concerned Signaling Point Code (CSPC) group is increased from 32 to 96.

Customer Definable Alarms (Release 20.0)

This feature allows the user to connect up to 10 external devices to the EAGLE for alarm reporting. These are defined in the EAGLE database as customer defined troubles. These external devices are monitored and any

changes in the state of these devices is reported to the user as an unsolicited alarm message (UAM). Two of these UAMs generate critical alarms, two UAMs generate major alarms, six UAMs generate minor alarms. The following table lists the UAM, the alarm level, and the trouble ID.

Table 2-14. Customer Definable Troubles Alarm Levels

Customer Trouble ID	Alarm Detected UAM	Alarm Clearing UAM	Customer Trouble ID	Alarm Detected UAM	Alarm Clearing UAM
1	Reserved	N/A	9	Reserved	N/A
2	Reserved	N/A	10	Reserved	N/A
3	0058 - Critical	0062 - Normal	11	0060 - Minor	0062 - Normal
4	0058 - Critical	0062 - Normal	12	0060 - Minor	0062 - Normal
5	Reserved	N/A	13	0060 - Minor	0062 - Normal
6	Reserved	N/A	14	0060 - Minor	0062 - Normal
7	0059 - Major	0062 - Normal	15	0060 - Minor	0062 - Normal
8	0059 - Major	0062 - Normal	16	0060 - Minor	0062 - Normal

The following messages are examples of these UAMs.

UAMs

```
    ralncstp01  95-05-12  12:14:59 EST  Rel 20.0.0
*C  4054.0058 *C CDT    4                 Critical Customer Trouble detected
    ralncstp01  95-05-12  12:14:59 EST  Rel 20.0.0
**  4055.0059 ** CDT    8                 Major Customer Trouble detected
    ralncstp01  95-05-12  12:14:59 EST  Rel 20.0.0
*   4056.0060  * CDT   11                 Minor Customer Trouble detected
    ralncstp01  95-05-12  12:14:59 EST  Rel 20.0.0
    4058.0062    CDT    9                 Customer Trouble cleared
```

The status of these UAMs are displayed with the **`rept-stat-cdt`** command.

When the alarm condition that displayed these UAMs is cleared, UAM number 0062 is displayed.

Database Integrity Enhancements (Release 20.0)

With this feature, the system audits the actual data in each module, provides checksum information, and verifies the checksum information against the original checksum that was downloaded to the module.

Database Management Command Functions (Release 20.0)

Description

In this feature, the database management commands are used to perform the following operations.

- Backing up the database to the fixed disk and to the removable cartridge
- Restoring the database from the fixed disk and from the removable cartridge

- Copying the approved GPLs from the active fixed disk onto a removable cartridge
- Copying the measurements data from the fixed disk onto a removable cartridge
- Displaying the directories and files on either the fixed disks or the removable cartridge

These five operations are discussed separately, below.

Backup

This command makes a backup copy of the administered data that can later be used to restore the data. The backup is made onto both the fixed disks or onto the removable cartridge according to a parameter of the command. The original data is taken from the current partition on the fixed disk.

If the backup is made to the fixed disks, the current partition on a fixed disk is copied to the backup partition on the same fixed disk.

If the backup is made to the removable cartridge, it is taken from the current partition of the fixed disk of the active MASP and copied to the removable cartridge. There is only one data partition on the removable cartridge, and this is defined to be the backup partition.

Restore

This command allows the user to bring back onto the fixed disk a set of known good tables, which had been previously backed-up on a disk (either fixed or removable). This command only restores the administered data tables, not the GPLs or measurement tables.

When the restore is from the fixed disk, the backup partition is copied into the current partition.

When the restore is done from the removable cartridge, the backup partition on the removable cartridge is copied onto the current partition on the fixed disk. This command modifies the data tables on the fixed disks of both the active and standby MASPs.

When the restore is from the removable cartridge, the tables are copied to the fixed disks on both TDMs. It does not propagate any data changes to the SCCP cards, LIMs, and so forth. To propagate the changes resulting from the restored database, the EAGLE must be reinitialized.

Copy GPL

This command copies the set of approved GPLs from the active fixed disk on the TDM onto a removable cartridge. This is typically done after the installation of a new GPL on the system, when the GPLs have been approved, and will allow the user to keep one removable cartridge with a copy of all the approved GPLs in use on the system.

These GPLs may be brought back into the system from the removable cartridge using change GPL commands if there is a need to bring a system back to a prior state, or if a spare fixed disk needs to be brought up to date.

Copy Measurements

When there is a need to perform offline analysis of the raw measurements data, this command copies that data onto the removable cartridge. The data is copied from the active fixed disk on the TDM to the removable cartridge.

Measurements collection is not allowed to continue while this command is copying the tables, since this may result in data from one collection period spilling over into data from another collection period. Measurements cannot be

copied if measurement collection is turned on. Measurement collection must be turned off if you wish to copy the measurements tables.

Since there are two formats for removable cartridges, and only one of these is valid for measurements, the command will give a clear error message if the wrong type of removable cartridge is mounted in the drive.

Disk Directory

This command displays the directory on the specified disk. It can be used to display the creation date for each file or selected files and to verify that the correct version of files are on the fixed disks or the removable cartridge.

NOTE: Wildcards "*" and "?" can be used for filename matching. The "*" will match any number of characters, and any "?" will match any single character.

Database Transport Access (DTA) (Release 20.0)

This feature interconnects the X.25 and SS7 network protocols. This connection enables the interworking of several telephony and financial database application protocols carried within the X.25 and SS7 messages.

Refer to the *Database Administration Manual - Features* for current details of this feature.

Delay Vs. Throughput (IP^7 Release 5.0)

Description

This feature provides some level of user control over the TCP retransmission behavior that an individual TALI socket exhibits. Several aspects of TCP retransmissions need to be introduced in order to understand how this delay versus throughput feature will work.

As far as this feature is concerned, there are three primary aspects of TCP retransmissions that need to be understood.

- Retransmission timer
- Retransmission mode
- Congestion window

Retransmission Timer

Conceptually, the TCP retransmission timer is a timer that is started when a TCP data segment is sent on a socket. The TCP data segment is encapsulated in an IP packet (we will refer to this data segment being sent as a TCP packet, even though TCP is a byte oriented transport layer that does not typically send 'packets'). If an acknowledgement for the TCP packet arrives before the timer expires, the timer is stopped. If the timer expires before an acknowledgement arrives, the original packet is assumed to be lost/corrupted and a retransmission of that packet occurs.

In practice, most TCP implementations do not start a separate timer for each packet, rather an internal timer expiration occurs at a fixed interval and upon each internal timer expiration the data related to outstanding transmit packets without acknowledgements is analyzed to determine which retransmissions occur. It may take multiple

expirations of the internal timer until the overall timeout exceeds the retransmission timer. Therefore the actual time delay for each initial retransmission falls within a range determined by the frequency of the fixed timer expiration. For example, if a 50 millisecond internal timer is used, and it takes three expirations of the internal timer until a retransmission occurs, the actual timeout used varies from 101 milliseconds to 150 milliseconds.

In this document, the term 'internal retx timer' refers to the internal TCP timer that expires at a fixed interval regardless of how many transmit packets are outstanding. Upon each internal retx timer expiration, retransmissions are analyzed and possibly sent.

In this document, the term 'initial retransmission timeout' refers to the minimum amount of time that passes from when a packet is first transmitted until the initial retransmission occurs. It is important to note that the timeout refers to the minimum time before retransmission (not the maximum or average).

In this document, the term 'retransmission timeout' refers to the minimum amount of time that passes until the next retransmission occurs. The pending retransmission may or may not be the first retransmission based on the condition being described. The 'retransmission timeout' always refers to the current timeout.

In this document, the terms 'previous retransmission timeout' and 'next retransmission timeout' refer to the minimum timeouts before and after the current retransmission timeout.

Retransmission Mode

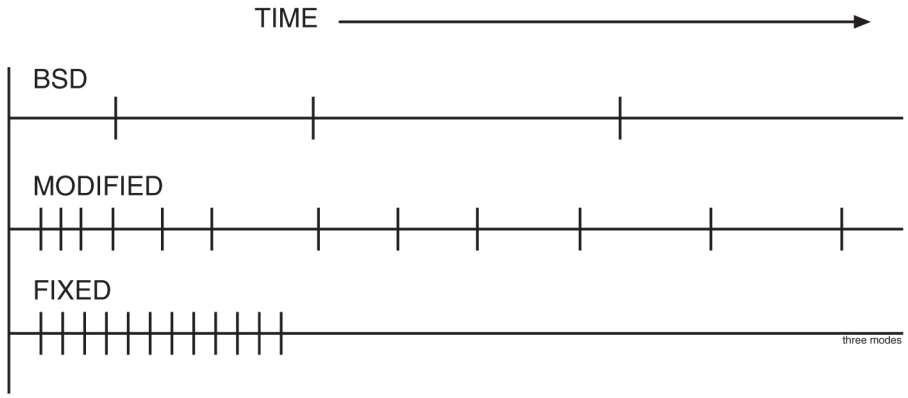
The retransmission mode refers to how the timeout varies from previous to current to next retransmission timeout.

There are several modes discussed in this document.

- BSD mode refers to exponential growth of the timeout. Upon each timeout the next retransmission timeout is equal to 2 x the current retransmission timeout. Usually there is an upper limit on the exponential growth (exponential up to a threshold, then stays at the threshold).
- FIXED mode refers to a constant timeout that does not change as subsequent retransmissions of the same packet occurs.
- MODIFIED mode refers to a combination of the above two modes. One implementation of this mode may use a fixed mode for two out of every three consecutive retransmissions, shifting to the BSD mode on every third retransmit.

The following figure shows the relative spacing of timeouts for the three different retransmissions modes. Note that the spacing for BSD mode is incomplete due to its relatively long sequence

Figure 2-12. Spacing of Retransmissions in the Three Modes



- The TCP protocol uses a sliding window to determine how much transmit data can be sent at one time, based on the minimum of the node's transmit window size and the far end's receive window size. The default TCP sliding window size is 8K bytes. Once 8K bytes of transmit data have been sent, with no acknowledgements received, the transmitter is prohibited from sending more until the far end sends acknowledgments for some portion of the window. The TCP window is said to slide when acknowledgments arrive, allowing packets with higher sequence numbers to be sent as packets with lower sequence numbers are acknowledged.

- Even though a particular socket within a TCP stack is configured for an 8K sliding window size, there are times when the TCP protocol does not take advantage of the entire 8K sliding window. One of these times is when retransmissions occur.

- When the TCP layer needs to retransmit one or more packets on a socket, the TCP protocol uses the minimum congestion window size rather than the TCP sliding window size to limit how much traffic can be sent until it must wait for acknowledgments. The minimum congestion window size is typically much less than the TCP sliding window size. As acknowledgments arrive from the far end after a retransmission event, the node slowly grows the congestion window up from the minimum congestion window to the size of the TCP sliding window.

- Another way of looking at this aspect of retransmission is to state that when a retransmission occurs, a transmitter intentionally lowers its own throughput until enough evidence from the far end arrives to assure the transmitter that the network is not congested. This phenomena is also referred to as congestion avoidance.

Socket Connection Dropped due to Retransmission Timeouts

- One other aspect of TCP retransmissions that should be mentioned is what happens when the same packet gets retransmitted over and over. When multiple retransmissions occur for a single packet, the TCP layer counts the number of retransmissions that is performed, and when this count gets too high the TCP socket is closed due to excessive retransmission timeouts. This shows up in the netstat -p tcp output in the 'connection dropped by rexmit timeout' row.

- In the BSD TCP stack, when a packet has been retransmitted 12 times, the socket is closed. Given the use of the exponential retransmit mode in standard BSD, the 12 retransmissions correspond to a time period of approximately 205.5 seconds where the packet was not able to sent/ack'd. (205.5 is based on 500 ms x 511, 511 is the sum of the tcp_backoff[] array which governs how the exponential backoff occurs and when the top threshold is reached).

- In the IP ^{7} SG stack, when a packet has been retransmitted 12 times, the socket is closed. Given the use of fixed retransmission mode with a 125ms timer, the 12 retransmissions correspond to a time period of approximately 1.5 seconds where the packet was not able to be send/ack'd.

Behavior of Standard BSD Sockets

The following table summarizes the TCP retransmission characteristics of a standard BSD socket.

Table 2-15. BSD Socket Retransmission Characteristics

Characteristic	Setting or Behavior (not configurable, applies to all sockets)
initial retransmission timeout	500 milliseconds
tcp window size	8k
retransmission mode	exponential
minimum congestion window	2 x the maximum segment size
how does cong window grow	initially grows exponentially via 1 MSS per ack. past a certain threshold, the growth is linear up to the point where the window is fully open
socket dropped due to retransmission timeout	after approx 205.5 seconds
RTO	500 ms default, algorithm to "learn" RTO by averaging recent round trip times, with software imposed upper bound

BSD sockets are extremely tolerant of poor network conditions and continue to wait for longer and longer time periods before performing subsequent retransmissions. These characteristics are not very well suited for time sensitive data such as SS7.

Behavior of IP^7 SG Release 4.0 IPLIMX & IPGWX Sockets

The following table summarizes the IPLIMX & IPGWX retransmission characteristics present in the IP ^{7} SG Release 4.0 product.

Table 2-16. IPLIMX Socket Retransmission Characteristics on IP^7 SG 4.0

Characteristic	Setting or Behavior (not configurable, applies to all sockets)
initial retransmission timeout	125 milliseconds
tcp window size	192k
retransmission mode	fixed
minimum congestion window	32k
how does cong window grow	grows exponentially via 1 MSS per ack up to the point where the window is fully open
socket dropped due to retransmission timeout	after approx 1.5 seconds
RTO	fixed, no dynamic information about actual round-trip times used

IPLIMX & IPGWX sockets have been tuned to handle time sensitive data and expect network conditions with low RTT and few transmission errors. The configuration shown above is not tolerant of networks with RTT above a certain threshold (approximately 100ms) or with too many transmission errors. The 4.0 implementation does not expect packet loss due to congestion. The only loss that is expected is due to hardware and/or transmission errors, bad checksums, and so forth. The 4.0 implementation expects little or no congestion on the network, and does not react in a fair manner (with respect to congestion avoidance) when congestion does occur.

Behavior of IP^7 SG Release 5.0 IPLIMX & IPGWX Sockets

The following table summarizes the IPLIMX and IPGWX retransmission characteristics that are available in the IP ^{7} SG Release 5.0 product.

Table 2-17. IPLIMX Socket Retransmission Characteristics on IP^7 SG 5.0

Characteristic	Setting or Behavior (configurable on a per socket basis)
initial retransmission timeout	as low as 125 milliseconds, settable in 125ms increments
tcp window size	192k
retransmission mode	fixed | bsd | modified
minimum congestion window	32k
how does cong window grow	exponential when mode = fixed | modified exponential followed by linear when mode = bsd
socket dropped due to retransmission timeout	varies from 1.5 to 205.5 seconds based on the mode and retransmission timeout configured
RTO	fixed, no dynamic information about actual round-trip times used

As seen in the tables above, the Delay vs. “Throughput for TALI Sockets” feature allows the end user to tune the retransmission characteristics of individual sockets. Sockets can be set so that they can function in a variety of network conditions (for example, LAN connection vs. a trans-Pacific WAN connection).

Upgrade Considerations

The addition of two new parameters in the entry (in the Socket Table) for each TCP/IP Socket necessitates the need for changes to the Upgrade Procedures for Engineering Release 37. These two new fields, Retransmission Mode and Round Trip Time Value, must be initialized to default values. The Retransmission Mode is initially set to "FIXED", with the Round Trip Time set to 60 milliseconds. A third field, the Congestion Window Lower Limit must be set to a calculated value using the default Round Trip Time (60 milliseconds). These fields must be set up for every assigned socket. The upgrade applies to both the OAM and Application copies of the Socket Table.

Limitations

The TCP/IP Protocol Stack timing mechanism has been modified by Tekelec software engineers. These changes enable the protocol to support TCP timers with resolutions as low as 125 milliseconds. It is not within the scope of the "Delay Vs. Throughput for TALI Sockets" feature to implement any other TCP timer resolutions than those currently supported. Each value entered as part of the Round Trip Time parameter is mapped to a corresponding Retransmission Timer, with a resolution of 125 milliseconds.

DigitAction Expansion (Releases 31.11, 34.0)

Description

G-Port and G-Flex allow the SCCP CdPA GTA field to be overwritten if G-Port determines the call should be relayed to its destination after a PDB lookup is performed.

G-Port and G-Flex support options that can be selected to overwrite or not to overwrite the SCCP CdPA GTA field. These options are defined by the DigitAction field of the PDBI Enter Network Entity command and Update Network Entity command. The user can also set these options to format the SCCP field before the EAGLE relays the message to the destination.

The rules for formatting the SCCP CdPA GTA field are based on the value specified in the DigitAction field. If digitaction = none, the EAGLE 5 ISS does not overwrite the SCCP CdPA GTA field. For all other values, the EAGLE 5 SAS formats the SCCP CdPA GTA field according to the value assigned to DigitAction field.

The following table provides samples of the format of the SCCP CdPA GTA field of an outgoing message using RN/SP ID= 1404 and default country code=886.

Table 2-18. DigitAction Applications

DigitAction	Value in Incoming CdPA GTA	Value in Outgoing CdPA GTA
none	886944000213	886944000213 (no change is made)
prefix	886944000213	1404886944000213
replace	886944000213	1404
insert	886944000213	8861404944000213
delccprefix	886944000213	1404944000213
delcc	886944000213	944000213
spare1	886944000213	is treated as "none"
spare2	886944000213	is treated as "none"

This feature expands the DigitAction field in PDBI and the EPAP GUI to support additional values "delcc," "delccprefix," "spare1," and "spare2." If the DigitAction value is "delccprefix," the SCCP CdPA GTA field of an outgoing message is formatted by prepending the RN/SP ID to the incoming SCCP CdPA GTA field and deleting the default country code if present. If the DigitAction value is "delcc," the SCCP CdPA GTA field of an outgoing message is the incoming SCCP CdPA GTA field without the default country code if present. The result of specifying the DigitAction field values “spare1” and “spare2” is the same as specifying the value “none.”

Hardware Requirements

Refer to the hardware baseline.

Disallow Simultaneous Logins Sessions with the Same User ID (Release 21.0)

In Release 21.0, the EAGLE does not allow more than one login session to be active at any given time for a specific user ID. During **login** command processing, a check is made to see if the user ID is associated with any currently active login session, or is in the process of logging on to another port. If the user ID is found to be already in use on some other EAGLE terminal port, then the login is rejected and the error message (the duplicate login error message) is displayed.

```
E2750 Cmd Rej: UserID already logged on (or is logging on) another port
```

The following message is also displayed in the scroll area of the terminal that gives the terminal port (port yy) that the user (UserID xxxxxxxx) is already logged to.

```
Info: UserID xxxxxxxx is currently logged on to port yy.
```

The check for multiple login sessions is made after the user ID and password have been successfully validated and before any password aging or force password change checking is done. As a result, the following events can occur.

1. If the user specifies an invalid login or password, this message is displayed and the duplicate login error message is not displayed.

E2757 Cmd Rej: Invalid userID/password combination

1. If the user ID and password is valid, but the user's password requires changing, they do not see the messages or prompts to change the password. Instead, they see the duplicate login error message.

This feature can be disabled by specifying the **chg-secu-dflt** command with the **multlog=yes** parameter

Discard TFC Traffic

The **chg-ss7opts** command includes the **discardtfci** and **discardtfcn** parameters to enable and disable the discarding of TFC traffic. The **rtrv-ss7opts** command displays the current setting of the parameters.

Disk Coherency Tests (Release 20.0)

This feature checks that the information in the database contains the correct pointers. The system can determine whether an update to the database failed and whether the information in the database was corrupted.

Disk Copy Fixed to Fixed (Release 20.0)

This feature allows maintenance personnel to create a mirror image from the active TDM fixed disk drive to the standby TDM fixed disk drive. This is used when replacing or updating a TDM.

If more than one message is sent to the EOAP without the LSMS waiting for a response, the LSMS must manage retries and the sequencing of messages.

The EOAP must be configured locally with the LSMS OSI-Address information necessary for association establishment. The EOAP will initiate association connections with the LSMS.

Display Inhibited Alarms (Release 29.0)

Description

This feature enhances the **`rept-stat-alm`** report to show all the devices that are alarm-inhibited, at what level and duration they are inhibited, and their current alarm level, if any.

Use of the Display Parameter

- If DISPLAY=INHB is used, a plus sign (+) seen in the "Alarm Inhibit Report" (i.e. in the CUR ALM LVL column) indicates that the current alarm is not inhibited, because the level of the inhibit is less than the level of the alarm.
- Column description:
  - — Device and element is listed first. Only devices that are alarm inhibited are shown.
  - — Duration shows whether the device is alarm inhibited permanently or temporarily.
  - — The "alm inh lev" shows the level in which devices are alarm inhibited. The inh-alm command defaults level to major. Devices cannot be alarm inhibited at a critical level unless the stpopt critalminh is turned on.
  - — The "current alm lev" shows the level of the current alarm on that device. "None" means there is no alarm currently on that device. If there is no alarm currently on that device, the Duration should show "Perm."

Hardware Requirements

No new hardware is needed to support this feature.

E1 Administration and Alarms (Release 26.3)

Description

Instead of a card having to be removed to change the configuration, each card can be configured using new commands and extensions to existing commands. This capability allows customers ease of configuring and updating their network using the EAGLE. Also, since the DIP switches are no longer required, they can be removed from future production E1 appliques.

NOTE: This feature is backward compatible with the E1 hardware, with or without the DIP switches.

With the introduction of this feature, the administration of the E1 will be done by EAGLE commands. Thus various EAGLE commands have been created or modified.

Currently E1 cards are "provisioned" via dip switches on the LIM board. Although this method of provisioning is functional, customers desire to integrate the provisioning of E1 functionality similar to other LIM cards, via software. This feature enhances the current 2-Port E1 feature by allowing the customer to configure the E1 hardware without using the DIP switches on the applique. This feature also provides support for E1 Master Timing.

Description of E1 Operation within an EAGLE

The introduction of this feature brings complete product support for the E1 line interface into the EAGLE, thereby concluding the E1 effort begun during Release 22.2. Along with V.35, the E1 interface is a primary interface used outside of North America. Thus, this large market base is a large market potential for an EAGLE with an E1 interface.

The E1 cards are provisioned and operate in a fashion very similar to the current DS0/OCU/V.35 signaling links:

- E1 cards and links must be configured in the EAGLE in a manner similar to how existing signaling links are configured. These configuration activities include entering cards, entering links, assigning links to link sets, and activating cards and links, in addition to entering E1 parameters. Changes to existing EAGLE commands, and new EAGLE commands, to perform these configuration activities are required.
- Two new card types, 'LIME1' and 'LIMCH', are used to define the E1 card and Channel cards, respectively, in the EAGLE.
- A set of E1-specific interface parameters must be maintained on a per-E1 basis. These parameters include:
  - which E1 port is used (either #1 or #2)
  - CRC4, CAS/CCS, HDB3/AMI, master/slave clocking options
  - signaling bits settings
- A set of E1-specific interface parameters must be maintained on a per-signaling link basis. These parameters include:
  - which E1 card is the card dropping timeslots
  - which timeslots are being used
- The current E1 implementation provisions E1 cards as either DS0 or OCU, based on master/slave timing. This feature provisions the cards as E1 or channel with either master or slave timing.
- Building Integrated Timing System (BITS) clock alarms must be supported when E1 cards with master timing are provisioned in the EAGLE. Currently, this is the reason that E1 cards are provisioned as DS0 cards.

The **TST-SLK** command will continue to support local transceiver loopback using the ISCC, just like the DS0/OCU/V.35 cards; no changes are necessary.

EAGLE Application Support for E1

Currently the SS7 application software initializes the hardware completely based on DIP switch values. With the new E1 Administration and Alarms feature allowing E1 cards to be provisioned, the SS7 application software needs to only initialize the hardware to a benign state until provisioning information is provided. This initial hardware state is similar to the other link interface module (LIM) cards' initial state.

Hardware Requirements

This feature is dependent upon the EAGLE E1 hardware, consisting of the LIM E1 backplane kit (P/N 890-1037-01), which allows connectivity between the E1 LIM card(s) and the corresponding E1 channel card(s) (both P/N 870-1379-01).

Upgrade Considerations

- The system release containing the E1 Administration and Alarms feature must be field-upgradable, with the EAGLE in an in-service mode.
- The new current and backup tables for E1 link interface parameter values must be created.
- A new phase is needed in the upgrade procedure to update the database with E1 information retrieved from the network cards after the network cards have been loaded with the latest GPL.
- Prior to collecting E1 information, cards will be loaded with the latest GPL with data from the database, including link information. Cards containing existing E1 links must load and bring up their SS7 links using the DIP switches instead of downloaded E1 data in this case.
- Card type field in the current and backup IMTA tables needs to be corrected from DS0/OCU based on information received from each card.
- E1 parameter information needs to be updated in current and backup E1LINK tables.
- E1 timeslot information needs to be updated in current and backup LINK and XLINK tables.
- Since upgrade must be able to be performed remotely, there must be an automated way to map the E1/Channel card relationship via some method such as far-end loopback detection.
- Since TS0 and TS16 (when CAS is enabled) may be assigned using the DIP switches, the upgrade must detect and report this condition. However, no change can be made to the timeslots.

Limitations

The E1 Administration and Alarms feature has these limitations:

- The configuration of the various E1/channel cards via the E1 backplane is not validated with the E1 parameter set information.
- There is no verification that the E1 and channel cards are connected to the E1 backplane.

E1 ATM High Speed Link (Release 28.1) (IP^7 Release 6.0)

Description

International customers desire increased signaling bandwidth by utilizing Asynchronous Transfer Mode (ATM). This capability requires EAGLE software to support ATM, as well as some hardware modifications to the existing LIM-ATM card that currently supports ATM over T1. The existing HCAP design for the LIM-ATM, with some modifications to the appliqué, is being used to accommodate the E1 ATM connectivity to the EAGLE.

This feature provides a new E1 interface capability on the EAGLE. This new capability is provided using the existing LIM-ATM via an HCAP card, a new Applique' ATM (AATM) daughterboard, and a new GPL. A modified LIM-ATM supporting 2.048 Mb/sec is here referenced as an E1 ATM card. The E1 ATM capability supports a single ATM Virtual Channel Connection (VCC) at a line speed of 2.048 Mbps. The E1 ATM replaces the MTP layers 1 and 2, (ITU-T Q.702 and ITU-T Q.703) with an ATM-based protocol (ITU-T Q.2110, Q.2140 and Q. 2144). ATM is used as the transport technology for carrying the signaling information via PDU's between network nodes.

Refer to the *NSD Hardware Manual* for detailed hardware information.

New Hardware

E1 ATM LIM provides one Asynchronous Transfer Mode over E1 Interface at 2.048 Mbps, (P/N 870-1293-xx). This module uses an E1 Asynchronous Transfer Mode Applique (E1 ATM) installed on a High Capacity Application Processor (HCAP) main assembly. The E1 ATM applique provides a new communications capability on the EAGLE, a High Speed Link (HSL) using ATM over E1. This capability is provided using the existing HCAP card, a new applique, and a new GPL (ATMITU).

Refer to the *NSD Hardware Manual* for detailed hardware information.

Limitations

OAM F5 Performance Monitoring

ATMANSI does not provide OAM F5 performance monitoring. This capability has not been added for this feature. Because the anticipated deployment of this feature is as a direct connection, performance monitoring of the network is not anticipated to supply any additional information that SAAL does not.

OAM F5 Fault Management

ATMANSI only provides OAM F5 fault management for OAM loopback. It does not provide support for alarm surveillance and continuity check. These capabilities have not been added for this feature. Because the anticipated deployment of this feature is as a direct connection, fault management of the network is not anticipated to supply additional functionality. Connection issues will be detected by the SAAL and the link will be deactivated if appropriate.

Traffic Size

Traffic size will have a definite impact on MSU throughput of the system; see table.

Table 2-19. Comparison of MSU Size to Throughput

MSU Size	ATM Packet Overhead	Cells/MSU	Max MSU/Sec
20	62%	1	2000
30	43%	1	2000
40	24%	1	2000
50	52%	2	1800
60	43%	2	1800
70	33%	2	1800
80	24%	2	1800
90	43%	3	1200
100	36%	3	1200
150	29%	4	900
200	24%	5	720
250	21%	6	600

AMI

AMI is not supported in this release. HDB3 is the only supported encoding option for the E1 ATM card.

OVERSIZE MESSAGES

Oversize messages (>272 octets) will not be supported in this release. This limitation is a holdover from ATMANSI.

A general purpose implementation of the ATM HSL protocol stack would allow for 'Large MSUs' to be transferred across the physical link. The SSCOP layer is capable of handling data from SSCF that is up to 4096 byes long. Since SSCF does not add a trailer to MTP3 data, this equates to an MTP3 packet of 4096 bytes.

However, the current implementation of the ATM HSL stack restricts the largest MSU size to 272 bytes of MTP3 data. This restriction will be used for this feature, and as in the ATMANSI gpl, a the same UIM will be generated with a Large MSU is received.

E1/T1 MIM on EPM (E5-E1T1 Card) (Release 35.0)

Description

The E1/T1 MIM on EPM feature provides a single-slot, high-density E5-E1T1 card for channelized E1 and T1 link solutions. This card can be operated with a 40 Amp frame-level power budget and does not require a fan.

The E5-E1T1 card can be assigned a maximum of 32 signaling links of configurable channelized T1 connectivity. The links on the card can operate in a linkset with other links running at different speeds. The total number of provisioned T1 links cannot exceed the allowed system maximum (the quantity shown for the Large System # Links entry in the rtrv-ctrl-feat command output).

The E5-E1T1 card terminates 8 E1/T1 ports (trunks) and routes them to the A and B ports of the EAGLE 5 ISS backplane. These ports can be configured to select which E1/T1 ports are active and which channels on each port are used for signaling links.

The E5-E1T1 card supports one SE-HSL signaling link on one of the eight ports. Channelized operation is not possible on any E5-E1T1 card that is provisioned for SE-HSL. SE-HSL requires a Feature Access Key on a system level basis. The E5-E1T1 card provides copying and time-stamping of MSUs for all provisioned signaling links (up to 32 LSLs or 1 SE-HSL) simultaneously when the EAGLE 5 Integrated Monitoring Support (E5IS) feature is turned on.

NOTE: EAGLE 5 ISS Release 35.0 supports only the T1 functions on the card. The E1 functions will be available in EAGLE 5 ISS Release 35.1.

Modes of Operation

The E5-E1T1 card can be provisioned to operate in the E1 or T1 mode. The mode of operation defines the trunk format for the 8 ports on the card.

Along with the T1 mode, the E5-E1T1 card provides a Channel Bridging function that allows users to utilize T1 bandwidth that is not used by EAGLE 5 ISS signaling links. T1 ports 1, 3, 5, and 7 (master ports) can be independently channel bridged with their adjacent even-numbered (slave) T1 ports 2, 4, 6, and 8 to allow non-signaling data pass-through.

In T1 mode, the E5-E1T1 card generates an idle code in idle (unused) time slots. If the Channel Bridging function is used, idle codes are inserted into timeslots on even ports corresponding to the reflected signaling channels on the odd port.

EAGLE 5 ISS supports the Channel Bridging function for all combinations of master/line timing modes invoked by the adjacent equipment. Internal clock selection criteria ensure synchronous data paths through the bridged channels.

Thermal Management

The E5-E1T1 card includes and alarming provisions to protect the card from damage if environmental conditions hinder thermal stability. The EAGLE 5 ISS responses to increasing temperatures are as follows:

- Temp1 Exceeded—Major alarm raised
- Temp2 Exceeded—Critical alarm raised; failover initiated, traffic rerouted
- Temperature abated. Normal operation restored

Hardware Requirements

The E1/T1 MIM on EPM feature has the following hardware requirement::

- HIPR cards are required on each shelf that contains E5-E1T1 cards.

Limitations

The E1/T1 MIM on EPM feature has the following limitation:

- The E1 functions are not supported in EAGLE 5 ISS Release 35.0.

E1/T1 MIM on EPM (Release 35.1)

Description

The E1/T1 MIM on EPM feature enhances the E1/T1 MIM on EPM feature from Release 35.0 by adding EAGLE 5 ISS support for E1 functionality and SE-HSL links. This Feature Notice documents only these enhancements. Refer to the EAGLE 5 ISS 35.0 Feature Notice for a detailed discussion of the E1/T1 MIM on EPM feature.

With support for the E1 functionality, the E5-E1T1 card can terminate 8 E1/T1 ports (trunks) and route them to the A and B ports of the EAGLE 5 ISS backplane. These ports can be configured to select which E1/T1 ports are active and which channels on each port are used for signaling links.

The E5-E1T1 card supports one SE-HSL signaling link on one of the 8 ports. Support for SE-HSL requires a system-level Feature Access Key.

The E5-E1T1 card provides copying and time-stamping of MSUs for all provisioned signaling links (up to 32 low-speed links) simultaneously when the EAGLE 5 Integrated Monitoring Support (E5IS) feature is turned on.

Modes of Operation

The E5-E1T1 card can be provisioned to operate in the E1 or T1 mode. The mode of operation defines the trunk format for the 8 ports on the card.

In T1 mode, a port represents a time-division-multiplexed data stream of 24 channels with an aggregate data rate of 1.544 Mbps. In E1 mode, a port represents a time-division-multiplexed data stream of 32 channels with an aggregate data rate of 2.048 Mbps.

E1 and T1 port configurations cannot be mixed on a single card. The E5-E1T1 card provides a Channel Bridging function that allows use of E1T1 bandwidth that is not used by EAGLE 5 ISS signaling links. E1 and T1 ports 1, 3, 5, and 7 (master ports) can be independently channel bridged with their adjacent even-numbered (slave) E1 and T1 ports 2, 4, 6, and 8 to allow non-signaling data pass-through.

In the E1 or T1 mode, the E5-E1T1 card generates an idle code in idle (unused) time slots. If the Channel Bridging function is used, idle codes are inserted into timeslots on even ports corresponding to the reflected signaling channels on the odd port.

EAGLE 5 ISS supports the Channel Bridging function for all combinations of master/line timing modes invoked by the adjacent equipment. Internal clock selection criteria ensure synchronous data paths through the brIdged channels.

NOTE: Channelized operation cannot be performed on any E5-E1T1 card that is provisioned for SE-HSL.

Hardware Requirements

The E1/T1 MIM on EPM feature requires HIPR cards on each shelf that contains E5-E1T1 cards.

Limitations

The E1/T1 MIM on EPM feature has the following limitations:

- E1 and T1 port configurations cannot be mixed on a single card.
- Channelized operation cannot be performed for any E5-E1T1 card that supports SE-HSL links.

E1/T1 Multi-Channel Interface Module (Release 28.0) (IP^7 Release 6.0)

The E1/T1 Multi-Channel Interface Module (MIM) provides increased E1 signaling connectivity and a channelized T1 connection to the EAGLE STP.

The MIM increases the number of SS7 links (ports) the EAGLE handles per E1 card. This allows the EAGLE to interact in larger SS7 networks, as well as decreases the footprint of an EAGLE (i.e. previously 250 cards were required to support 500 links; now only 63 cards are required). The E1/T1 MIM can be used in systems equipped with either the IPMXor the HMUX board. The MIM also provides a new channelized T1 connection to the EAGLE. The MIM can replace an existing LIME1/LIMCH card (as an E1 terminating card or E1 channel card), with no reprovisioning required. E1 MIM is hot-swappable with LIM-E1.

NOTE: For existing E1 customers, the E1 Administration feature will be activated after upgrading to Release 28.0, unless the source release is 26.3.

The E1/T1 Multi-Channel Interface Module (MIM) card has 2 physical backplane port connections, as other LIM cards do. These are referred to here as interface A and interface B. For the E1/T1 MIM, as with the existing LIM-E1 card, interface A has 2 ports of E1/T1 connectivity. These 2 ports are referred to as port #1 and port #2. Interface B provides the expansion port to service channel cards.

Refer to the Database Administration Manual - SS7 for detailed and configuration information.

Hardware Requirements

No new hardware other than the new MIM card itself (870-2198-01) is needed to support this feature.

For detailed information on hardware, refer to the *NSD Hardware Manual*.

E5-SM4G Card (Release 37.0)

Description

The E5-SM4G card enhances the EAGLE 5 ISS support for the EPAP and ELAP-based features by providing performance improvement over the DSM cards that currently run the **vsccp** application. DSM cards will continue to be supported, but are being replaced with E5-SM4G cards for new initial and extension shipments.

The E5-SM4G card requires the E5-SM4G Throughput Capacity feature to be enabled to achieve maximum processing. A FAK is required to enable the E5-SM4G Throughput Capacity feature.

The new E5-SM4G card running the **sccphc** GPL and the **vsccp** application performs the same functions as the current DSM card for EPAP-based and ELAP-based features.

The E5-SM4G card is provisioned with card type **dsm** and the **vsccp** application, allowing the E5-SM4G card to replace a DSM card in the control or extension frame without re-provisioning.

The E5-SM4G Throughput Capacity feature performs the following functions:

- Allows each E5-SM4G card to operate at a rate of 5,000 TPS for SCCP traffic that is processed entirely by GTT.
- Allows each E5-SM4G card to operate at a rate of 3,125 TPS if part of the SCCP traffic is processed by EPAP-based features.
- Allows achievement of the maximum system TPS capacity provided by the 150,000 GTT TPS feature and the 75,000 EPAP TPS feature. See “150,000 GTT TPS and 75,000 EPAP TPS” on page FN-8.

If the E5-SM4G Throughput Capacity feature is not enabled, then the E5-SM4G card continues to operate at the DSM-equivalent capacities:

- GTT only mode=1700 TPS per E5-SM4G card
- EPAP-based feature node if the 1100 TPS/DSM feature is not enabled = 850 TPS per E5-SM4G card
- EPAP-based feature node if the 1100 TPS/DSM feature is enabled = 1100 TPS per E5-SM4G card

HIPR cards must be installed in any shelf that contains an E5-SM4G card. HIPR cards must be installed in all shelves in the system before the E5-SM4G Throughput Capacity feature can be enabled to increase the card and system TPS capacity.

The E5-SM4G card cannot be inserted into a node that is provisioned to process more than 192 million LNP numbers. If the E5-SM4G card is inserted into a node that can process more than 192 million LNP numbers, the card auto-inhibits.

The E5-SM4G card can co-exist with DSM cards and operate at a capacity of 5,000 TPS. The E5-SM4G card can co-exist with TSM cards that are used for GTT and GLS only, and can co-exist with two channel LIM cards per node.

The E5-SM4G card provides two physical 10/100 Mbps Ethernet ports.

The E5-SM4G card supports thermal management and alarming provisions.

Feature Control Requirements

If the E5-SM4G Throughput Capacity feature is used, then the following feature control requirements apply:

- A FAK for part number 893-0191-01
- A temporary key cannot be used to enable the feature.
- After the feature has been turned on, it cannot be turned off.
- The feature cannot be enabled if any of the following features or options is turned on:
  - E5IS (EAGLE 5 Integrated Monitoring Support) feature
  - LNP feature
  - ANSIGFLEX STP option

Hardware Requirements

The E5-SM4G card requires HIPR cards in card locations 9 and 10 in the shelf in which it is installed.

Limitations

The E5-SM4G card provides 3.1 GB of memory while the DSM card provides approximately 3.6 GB of memory. This reduction in memory limits the number of entries to a maximum of 84 million for EPAP applications and 192 million for LNP. Additional E5-SM4G cards may be required to match the processing capacity of DSM for these applications.

EAGLE Alarm Modifications for Synchronization with Harris (Release 31.5)

Description

There is an issue between the Harris monitoring system and the alarm generation/clearing shown by the EAGLE. There are multiple instances where the EAGLE will either silently clear an alarm, or silently refresh an alarm to a different alarm. Since the Harris system is relying on the EAGLE output to set or clear alarms on EAGLE devices, the two systems alarming counts are frequently out of sync.

Limitations

If a customer is only using a normal KSR terminal for monitoring, there is a potential to drop alarms from the terminals output if the output buffers fill up with data such as hourly reports, IMT reports, Measurements reports, excessive UIM output, etc. There are ways to minimize this extra output to significantly reduce the likelihood of such a buffer overflow:

- Turn off Traffic output group (TRAF) for the terminal used by Harris
- Use UIM thresholding

NOTE: using the new EMSALM terminal solves this limitation

Due to the sheer number of Alarms that are potentially generated during link alignments for an EAGLE with a large number of signaling links, the multiple signaling link alarm states continue to be done without output. The first Signalling Link alarm is output but subsequent alarms for that device transition silently. This suppression of output is OK for signaling links, in that all the signaling link silent alarm transitions are within the same alarm level, MAJR. When the signaling link alarms are cleared, there is an appropriate clearing alarm issued for each affected link. To cycle through and issue each overtaking signaling alarm for every link over an "init-sys" on a large system output overwhelms the output buffer, and alarms would be lost.

In the event that the Harris system's alarms get out of Sync with the EAGLE's alarms, it is up to the Harris system both to detect and correct its alarm counts to match that of the EAGLE.

EAGLE Frame Power Budget Alarm (Release 35.0)

Description

The EAGLE Frame Power Budget Alarm feature issues an alarm if the power consumption of cards in a frame nears the frame-level power capacity. The power capacity value can be provisioned in the Frame Power Threshold (FPT) table or a default value of 30 Amps can be used.

NOTE: The value in the FPT table would be provisioned based on FAP configuration and power feed.

The feature identifies the type of cards in a frame, calculates potential power consumption based on the frame-level population of cards, compares calculated power consumption to a frame-level power capacity figure, and raises alarms based on provisioned thresholds.

The new **rtrv-stp** command can be used to display the power consumption and power threshold values for all frames or a specific frame in the system.

Hardware Requirements

None

Limitations

The EAGLE Frame Power Budget Alarm feature has the following limitation:

- During initialization and switchover, frame power consumption is calculated using information from the various cards; therefore, the correct power consumption value is calculated only after information from all of the cards have been processed by the Frame Power Budget Alarm task.

EAGLE Initiated OAP User Interface (Release 24.0)

Description

In Release 24.0, the OAP configuration information is entered from the EAGLE terminals into the EAGLE database. When the configuration of an OAP needs to be updated, the OAP configuration data in the EAGLE database is sent to the specified OAP.

OAP Commands

The EAGLE uses these commands to configure and display the OAP data in the database and send this data to the OAP. Refer to the *Commands Manual* for current usage information.

- **chg-oap-config**
- **chg-oap-lkeys**
- **act-oap-config**

- **rtrv-oap-config**

This feature can be used to configure and update the Texas Micro OAPs currently being used or the Embedded OAPs introduced in Release 24.0. This feature cannot be used to upgrade the OAP software. Upgrading the OAP software must be performed by a terminal connected directly to the OAP.

CHG-OAP-CONFIG

The **chg-oap-config** command is used to configure the EAGLE database with the OAP configuration information. This information is sent to the specified OAP with the **act-oap-config** command.

CHG-OAP-LKEYS

The **chg-oap-lkeys** command is used to enter the license keys of the DSET APLI, DSET DSGRuntime, Solstice OSI, and Solstice X.25 third party OAP software into the EAGLE database. The license keys are not sent to the OAP with the **act-oap-config** command, but are used when auditing the OAP and EAGLE configuration data.

ACT-OAP-CONFIG

The **act-oap-config** command is used to update the OAPs with the configuration data entered into the EAGLE database with the **chg-oap-config** command.

RTRV-OAP-CONFIG

This command displays the OAP configuration information in the EAGLE database that has been configured with the **chg-oap-config** and **chg-oap-lkeys** commands.

CHG-SID

When the EAGLE's CLLI has been entered into the database or changed with the **chg-sid** command, the OAP configuration must be changed to include the new CLLI value. When this change to the EAGLE's CLLI has been made, the following warning message is displayed in the scroll area of the terminal display, reminding the user that the OAP configuration must be updated with the **act-oap-config** command.

LNP Service Commands

When the LNP feature is on, the LNP services CLASS, CNAM, LIDB, and ISVM must be in the OAP configuration in the EAGLE database. When these services are added to the database (with the **ent-lnp-serv** command), removed from the database with the **dlt-lnp-serv** command, or changed with the **chg-lnp-serv** command, the OAP configuration must be updated with the **act-oap-config** command. When any of these changes to the LNP services have been made, the following warning message is displayed in the scroll area of the terminal display, reminding the user that the OAP configuration must be updated with the **act-oap-config** command.

Auditing the OAP Database

In order to keep OAP database synchronized with the EAGLE, a checksum is created using all of the OAP configuration data stored on the EAGLE. The OAP also calculates this checksum based on the data it has. This checksum is returned by the OAP with every forced maintenance poll allowing the EAGLE to compare and act on the result. If the checksum values do not agree, the EAGLE generates a minor alarm (UAM 0364) within 10 seconds:

UAM 0364 is cleared within five seconds after the EAGLE detects that the databases are synchronized again, and the checksum values of the databases agree, with UAM 0365:

EAGLE Measurement Reports (Release 20.0)

EAGLE STP measurements provide support for STP performance management, SS7 traffic monitoring and engineering, and Specific feature performance analysis (STPLAN).

Refer to the *Maintenance Manual* for current EAGLE measurement information.

EAGLE OA&M IP Security Enhancements (EAGLE Releases 30.0, 30.2, IP7 Secure Gateway Release 8.0)

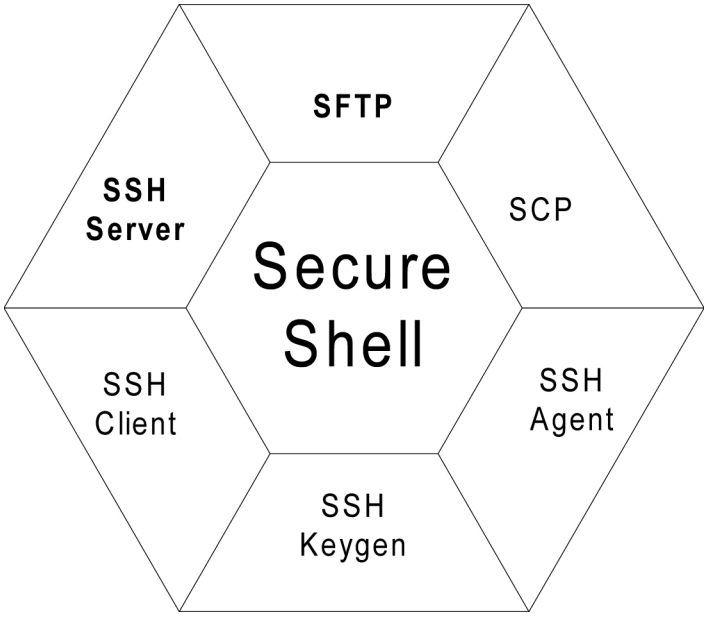
Description

The EAGLE OA&M IP Security Enhancements feature provides tools to securely pass data across an otherwise non-secure network. Once the EAGLE OA&M IP Security Enhancements Feature is turned on, the EAGLE allows only secure connections from approved clients, and protects sensitive passwords and information while in transit between the EAGLE and a host.

The EAGLE OA&M IP Security Enhancements feature uses a software package called Secure Shell. Secure Shell (SSH) is a protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE IPUI traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.

SSH consists of several component applications, two of which are relevant for IPUI enhancements: SSH client program for secure remote login (an enhancement for telnet), and SFTP, the secure file transfer protocol (which replaces FTP); refer to the **bold** components in the following figure.

Figure 2-13. The Secure Shell Package



Both applications support strong encryption of passwords and data, using widely accepted cipher routines. In addition, they provide authentication to reliably determine the source of any connection attempt. Lastly, SSH provides a guarantee of data integrity, which ensures data cannot be tampered with, even while in transit over the network. These security features, once implemented, are transparent to the users.

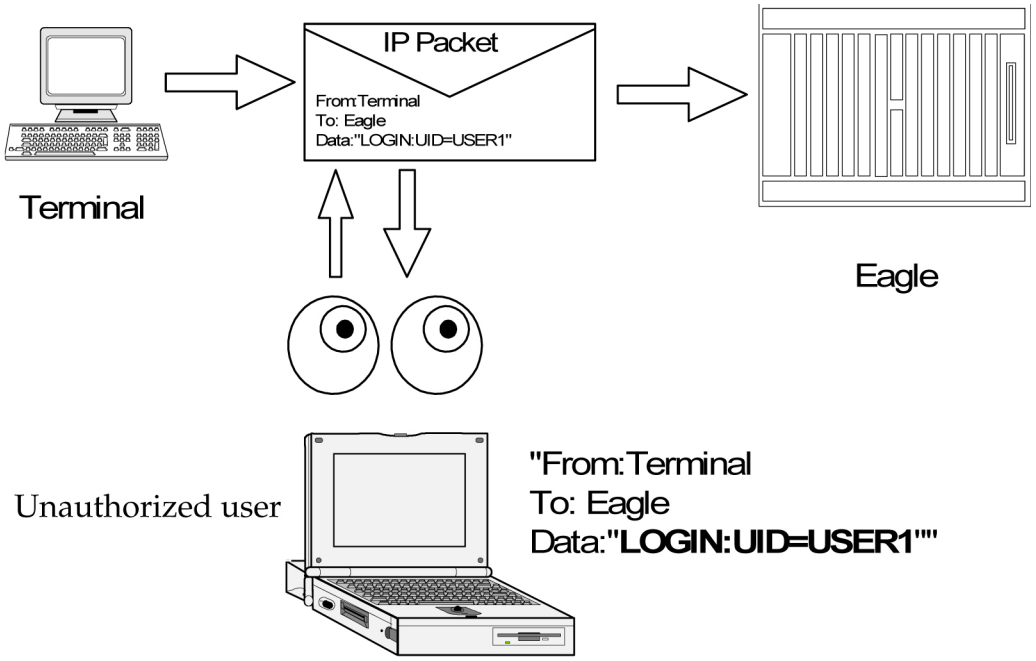
IP Network Security

A non-secure network is vulnerable to several types of electronic attacks. IP protocol itself provides limited inherent capability for confidentiality or security. Because of this, networks that depend on IP are subject to relatively simple attacks; these include eavesdropping on an IP transmission, recording or even modifying data. A protocol analyzer, for instance, can record network traffic, and then the packet's data contents are open to view. Another type of IP attack involves a third-party taking over a session and masquerading as one of the original parties involved in the communication.

IP-based security vulnerabilities include:

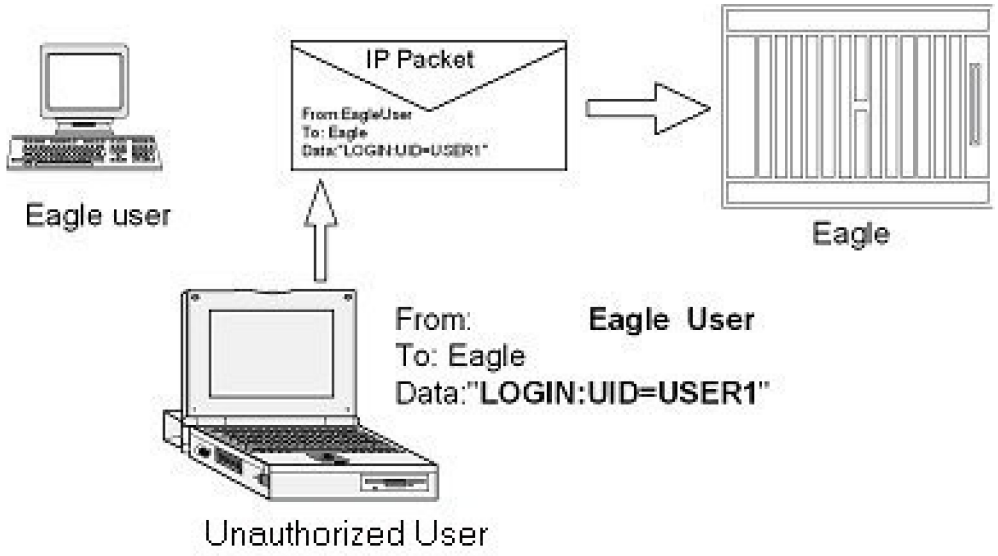
- *Snooping*, or eavesdropping on a connection, which is especially damaging while passwords are being transmitted (see next figure).

Figure 2-14. Example of Snooping



- IP *spoofing*, in which an intruder tries to gain access by changing a packet's IP address to make it appear that the packet came from another, trusted host (see next figure).

Figure 2-15. Example of Spoofing



- IP source routing, where a host can pretend that an IP packet comes from another, trusted host
- DNS spoofing, where an attacker forges name server records
- Interception of clear text passwords and other data by intermediate hosts
- Manipulation of data by people in control of intermediate hosts
- Attacks based on listening to authentication data and spoofed connection to the server.

Addressing IP Security

The EAGLE Secure Shell package developed for this feature addresses the network vulnerabilities as follows:

Identification

Identification occurs on many levels during a telnet or FTP terminal session. User identification is not only via username, but also through the originating IP address, and also by the Secure Shell client session ID. During the establishment of a secure connection, the host and client go through a process of key exchange and verification, to firmly establish a session identity. Secure Shell is in effect, providing a secure pipe between the client and host for the duration of that connection. All subsequent messages can be verified as originating from that known and established source.

Authentication

Authentication, at the user level, is provided for by the EAGLE login (username and password). This establishes the users identity. Secure Shell provides for authentication at the message level, to ensure incoming messages have originated from a known and verified source, while the session is in effect. This prevents network attacks based on spoofing or modifying the IP packets addressing headers, or originator ID.

Confidentiality

Confidentiality is enforced via message encryption. The Secure Shell tools encrypt each packet of data, before being exchanged in the process of either file transfer, or an interactive session. This encryption prevents snooping-type LAN attacks, where a hostile party intercepts and attempt to read messages in transit.

Data Integrity

Encryption also protects the data contained in the message or the message header from being altered or modified (either maliciously or accidentally) while in transit. Any message that fails an integrity test would be discarded, and the protocol would request the originator to resend the lost message. Data integrity is protected by including a Message Authentication Code (MAC) with each packet. The MAC is computed from a shared secret (key), packet sequence number, and the contents of the packet. The message authentication algorithm and key are negotiated when the connection is established.

Encryption

The secure connection and data encryption is established *before* the password or other authentication is ever sent, so all data remains protected. The client determines the encryption cipher; one of several is used, such as 3DES, IDEA, or Blowfish. Once the cipher has been determined (generally within the client preferences), the client and server exchange encryption keys.

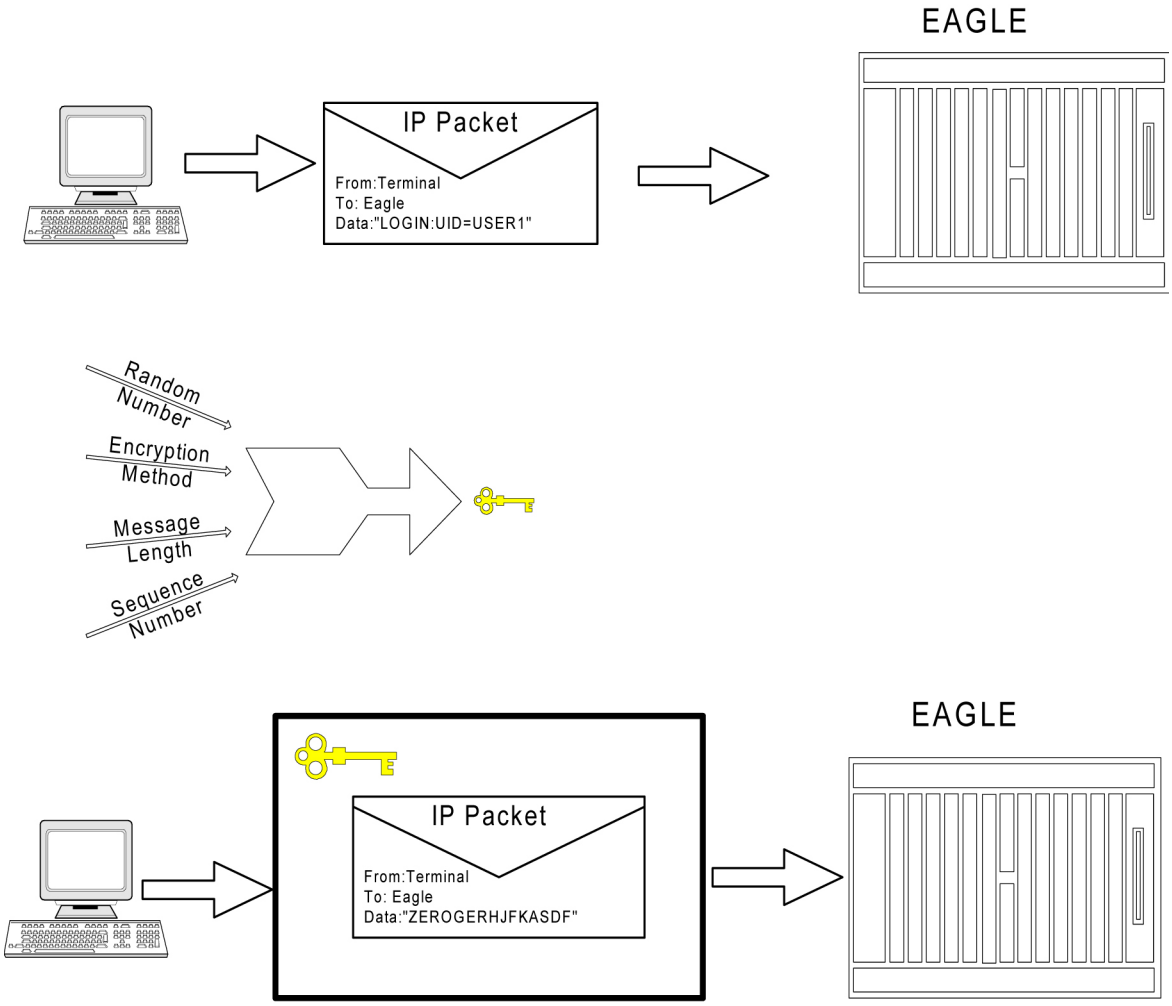
Strong Authentication

Strong authentication on a per-user basis would entail the use of public/private key pairs, generated at runtime and distributed to each user's client, along with a pass code that was user specific. These keys could not be pre-generated and stored in a table (with user names and passwords), since that would compromise any security advantage they were meant to impart. This would also entail an administrator account on each IPSM or MCPM card, along with a key server agent, to track user keys. Neither the IPSM nor MCPM platform currently supports administrator shell access, or a file system to store keys generated at runtime. This feature does not address Strong Authentication.

Secure Shell Summary

The top drawing in the following figure depicts a standard IP packet traveling over a LAN connection to the server. A packet header contains the destination address, the sender's address, etc. The packet contains data. An IP sniffer could open this packet from the IP stream, examine the contents, change the source or destination address, or change the contents. Security tools prevent the originator's address from being altered, the destination address from being altered, and the data is both unreadable, and protected from modification while in transit.

Figure 2-16. IP Network Security



EAGLE Secure Shell Solution

The EAGLE communicates over IP using two methods: Telnet and File Transfer. Telnet is the remote interactive terminal session. FTP Retrieve and Replace and Measurements Platform use file transfer, for performing bulk data transfer to remote servers.

Secure Shell uses encryption and authentication to protect sensitive data as it passes from one system to another in either scenario. SSH, a terminal connection program, and SFTP, a file transfer program, use an encryption algorithm for protecting all data transmitted over a session, including initial login and password, files and commands sessions.

All data passed through a Secure Shell session is secure: Secure Shell encrypts and authenticates all traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.

Secure Shell works through three fundamental stages:

- **Integrity** - Guarantees the data traveling over a network arrives unaltered.

- **Encryption** - Scrambles data to render it unintelligible, except to the intended recipients. A network sniffer could not read the enclosed data, as it cannot be decrypted without the key.

- **Authentication** - A secure protocol authenticates the source and destination addresses, as well as encrypts and data contained. Authentication protects against several security problems, e.g., IP spoofing, fakes routes, and DNS spoofing. Nor could false data be substituted, since authentication would reject any but known client's packets.

Applying Secure Shell to EAGLE

This feature applies Secure Shell Version 2.0 to EAGLE OA&M IP Interfaces. Secure Shell defines a protocol for secure remote login and other secure network services over any non-secure network. It provides an encrypted terminal session with authentication of both the server and client. It provides authentication and secure communications over unsecured channels. In other words, Secure Shell never trusts the net; somebody hostile who has taken over the network can only force Secure Shell to disconnect, but cannot decrypt or play back the traffic, or hijack the connection. Secure Shell contains two separate utilities for IP OA&M connections: SSH and SFTP.

- SSH is the terminal session utility of the Secure Shell package. SSH is a secure replacement for telnet clients.

- SFTP is the file transfer utility that is part of the Secure Shell package.

  SSH and SFTP share the same security features, which include:

  — A variety of data authentication methods.

  — A secure session established between clients and hosts.

  — Support for data encryption.

EAGLE IP Features

The EAGLE OA&M IP Security Enhancements feature affects these features:

- IPUI User Interface (Telnet), introduced in EAGLE Release 29.0/IP ^{7} Secure Gateway Release 7.0

- FTP Retrieve and Replace, introduced in EAGLE Release 29.0/IP ^{7} Secure Gateway Release 7.0

- Measurements Platform (EAGLE Release 28.0)

Hardware Requirements

No new hardware is needed to support this feature.

Upgrade Considerations

FTRA (FTP-based Table Retrieve Application) software must be upgraded to support the EAGLE OA&M IP Security Enhancements feature.

Limitations

Security is a process, not a product. EAGLE OA&M IP Security Enhancements will not assist any activity that compromises a host's security in some other way. This feature provides secure access to the EAGLE IPUI terminals, and while the EAGLE is transferring data off-board to remote SFTP servers. Vigilance still is required in protecting username/password combinations, and in controlling system access to EAGLE commands (via the configurable command class feature) to prevent violation of access privilege. This feature does not provide the remote Secure Shell client or server applications (SSH, SFTP).

If this feature is enabled with a temporary key, the key can expire while telnet (SSH) or FTP (SFTP) connections are up and in progress. In this scenario, all existing (legacy) connections remain up, and new connections follow the state of the feature: ON or OFF. Both secure and non-secure connections are possible for the duration of the 'legacy' connection.

EAGLE Support for Integrated Sentinel (Release 28.0)

Description

The EAGLE STP and the Sentinel Network Maintenance and Diagnostics tool are both existing Tekelec products. Without the EAGLE Support for Integrated Sentinel feature, the Sentinel requires physical, clamp-on connections to the EAGLE's SS7 signaling links, in order to monitor SS7 traffic. This monitoring method involves costs for cable installation and maintenance for each SS7 link that is to be monitored.

The EAGLE Support for Integrated Sentinel feature eliminates the need for intrusive hardware for each link to be monitored; instead, monitoring is via an Ethernet connection. Message Signaling Units (MSUs), alarms and events can be copied to the ESP over the Ethernet link to provide the same network traffic monitoring.

For more information on the EAGLE Support for Integrated Sentinel feature, refer to the *Database Administration Manual - Features*.

Hardware Requirements

The EAGLE Support for Integrated Sentinel feature requires GPSM-II cards in place of MCAP cards. Also, the EAGLE Time Synchronization feature (TSC Sync) must be active in conjunction with this feature. In addition, the timing requirements include the use of an external nits clock.

CAUTION: The EAGLE Support for Integrated Sentinel feature also requires the STC cards (870-1945-xx) and HMUX (870-1965-01 Rev A). For EAGLE 28.0, DCM cards (870-1945-xx) will serve as STC cards.

NOTE: The TSC feature requires GPSM-II; the EAGLE Support for Integrated Sentinel feature requires the TSC feature.

For detailed hardware information, refer to the *NSD Hardware Manual*.

EDCM Support (IP^7 Release 4.0)

As the IP ^{7} SG applications add new features and their throughput increases, more memory storage and CPU performance is required from the hardware platform. The Enhanced-Performance DCM (EDCM) is a new version of the DCM that includes more main memory and better processing performance. Additional memory is added,

doubling the amount of application SRAM. Some memory is replaced with higher performance chips. The following list highlights the changes embodied by the EDCM:

- The application processor is the AMD K6-IIIe+, which is an embedded version of the AMD K6-III high-performance processor that is used on the DCM 870-1945-xx. This processor consumes less power and produces less heat, leading to increased reliability.
- The application processor operates with an internal clock frequency of 396MHz rather than the 298MHz of the DCM, thereby increasing application performance and reliability.

The following elements of the EDCM are unchanged from the DCM:

- The EDCM requires two frame slots, like the DCM.
- The communication processor is unchanged.
- The amount of communication processor main memory is unchanged (2MB).

Refer to the *NSD Hardware Manual* for current hardware information.

ELAP Network Address Translation (NAT) (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)

NOTE: The ELAP NAT feature is only available at the preproduction level.

Description

Customers need to support communication between an ELAP system and a remote browser that may be on the public side of an IP firewall or router that employs Network Address Translation (NAT).

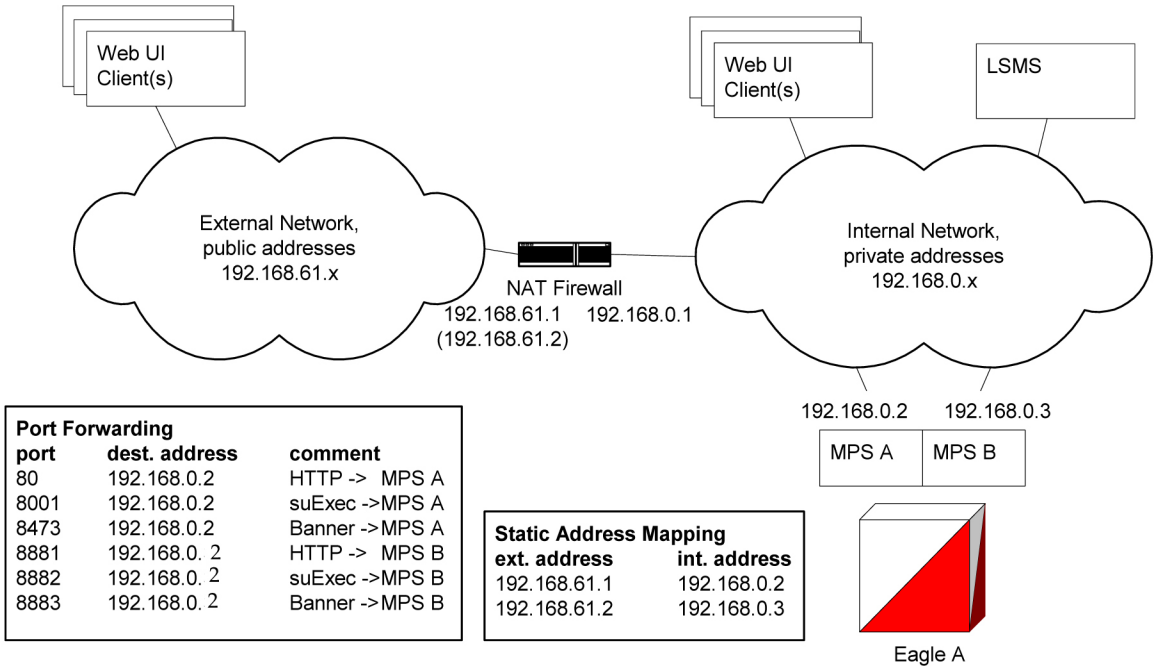
With the ELAP Network Address Translation (NAT) feature, the MPS platform (ELAP/EPAP) supports communications on networks where Network Address Translation (NAT) is employed. This means that the two MPS systems (A and B) can intercommunicate using IP addresses on a private network, yet also support IP addressing and communication with a remote browser that may be on the public or "other" side of a firewall or router employing NAT that is performing the IP address translation.

Network Address Translation (NAT) on MPS

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

The addresses in the following figure are examples. Addresses are not restricted to particular classes/ranges.

Figure 2-17. Network Address Translation on MPS



Port Forwarding

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

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

CAUTION

CAUTION: Do not change the default values for these ports.

Static Address Mapping

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

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

Hardware Requirements

No new or additional hardware is required to support this feature.

Enhancements to the ELAP Text-Based Interface

This section describes the enhancements to the text-based ELAP Configuration interface made to accommodate this feature. For more information, see the *ELAP Administration Manual*.

ELAP Configuration Menu

Entering '1' from the ELAP Configuration Menu provides a configuration report of the ELAP. The following figure illustrates an example configuration that includes NAT Address information (see arrows):

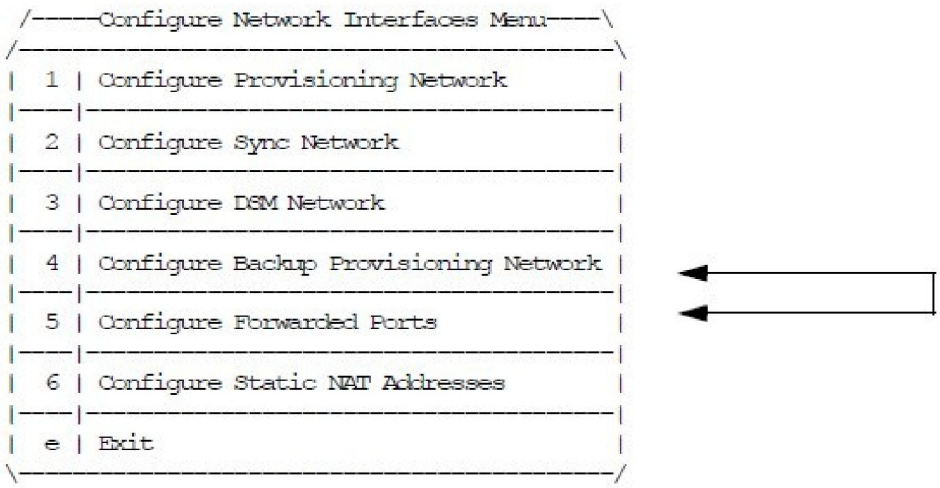
Figure 2-18. Display Configuration

```
MPS Side A:  hostname: mpsa-d1c48f  hostid: 80d1c48f
             Platform Version: 3.0.0-22.13.0
             Software Version: ELAP 3.0.0-30.19.0
             Mon Dec 16 16:42:32 EST 2002

ELAP A Provisioning Network IP Address = 192.168.61.90
ELAP B Provisioning Network IP Address = 192.168.61.91
Provisioning Network Netmask           = 255.255.255.0
Provisioning Network Default Router    = 192.168.61.250
ELAP A Backup Prov Network IP Address  = Not configured
ELAP B Backup Prov Network IP Address  = Not configured
Backup Prov Network Netmask            = Not configured
Backup Prov Network Default Router     = Not configured
ELAP A Sync Network Address            = 192.168.2.100
ELAP B Sync Network Address            = 192.168.2.200
ELAP A Main DSM Network Address        = 192.168.128.100
ELAP B Main DSM Network Address        = 192.168.128.200
ELAP A Backup DSM Network Address      = 192.168.129.100
ELAP B Backup DSM Network Address      = 192.168.129.200
ELAP A HTTP Port                       = 8888
ELAP B HTTP Port                       = 80
ELAP A HTTP SuExec Port                = 8001
ELAP B HTTP SuExec Port                = 8001
ELAP A Banner Connection Port          = 8473
ELAP B Banner Connection Port          = 8473
ELAP A Static NAT Address              = 10.25.50.10
ELAP B Static NAT Address              = 10.25.50.11
ELAP A LSMS Connection Port            = 7402
ELAP B LSMS Connection Port            = 7403
ELAP A EBDA Connection Port            = 1030
ELAP B EBDA Connection Port            = 1030
Time Zone                              = US/Eastern

Press return to continue…
```

Configure Network Interfaces Menu

This menu allows for the configuration of all of the possible network interfaces for the ELAP. When this menu item is selected, the menu shown in the following figure is displayed (see arrows).

Figure 2-19. Configure Network Interfaces Menu



Configure Forwarded Ports

Entering a choice of '5' from the Configure Network Interfaces Menu provides the functionality to configure ELAP ports for the Web UI and PDBI interfaces. When this menu item is selected, the menu shown in the following figure is displayed.

Figure 2-20. Configure Forwarded Ports Menu

```
 /-----Configure Forwarded Ports Menu------\
/-----------------------------------------\
|  1  | Change ELAP A HTTP Port             |
|-----|-------------------------------------|
|  2  | Change ELAP B HTTP Port             |
|-----|-------------------------------------|
|  3  | Change ELAP A HTTP SuExec Port      |
|-----|-------------------------------------|
|  4  | Change ELAP B HTTP SuExec Port      |
|-----|-------------------------------------|
|  5  | Change ELAP A Banner Connection Port |
|-----|-------------------------------------|
|  6  | Change ELAP B Banner Connection Port |
|-----|-------------------------------------|
|  7  | Change ELAP A LSMS Connection Port  |
|-----|-------------------------------------|
|  8  | Change ELAP B LSMS Connection Port  |
|-----|-------------------------------------|
|  9  | Change ELAP A EBDA Connection Port  |
|-----|-------------------------------------|
| 10  | Change ELAP B EBDA Connection Port  |
|-----|-------------------------------------|
|  e  | Exit                                |
\-----------------------------------------/
```

Each numbered item on the Configure Forwarded Ports menu allows the user to specify a port number used for remote access to the MPS.

Configure Static NAT Addresses

Entering a choice of '6' from the Configure Network Interfaces Menu provides the functionality to configure the static NAT addresses of the ELAP. When this menu item is selected, the menu shown in the following figure is displayed.

Figure 2-21. Configure Static NAT Addresses Menu

```
 /-----Configure Static NAT Addresses Menu-\
/-----------------------------------------\
|  1 | Change ELAP A Static NAT Address    |
|----|-------------------------------------|
|  2 | Change ELAP B Static NAT Address    |
|----|-------------------------------------|
|  e | Exit                                |
\-----------------------------------------/
```

Each numbered item of the Configure Static NAT Addresses menu allows the user to specify an IP Address used outside of the firewall for remote access to the MPS. The values entered here must match the configuration of the firewall.

Embedded OAP (Release 24.0)

Description

The OAP is a stand alone processor that acts as an interface between the EAGLE and operation support system (OSS) devices using standard interfaces and converting the communications to the EAGLE proprietary serial interface. The OAP can be used as an interface between the EAGLE and the SEAC (Signaling Engineering and Administration Center), for the SEAS feature, and as an interface between the EAGLE and the SMS (Service Management System), for the LNP feature. The OAP is installed in the OAP frame of the EAGLE.

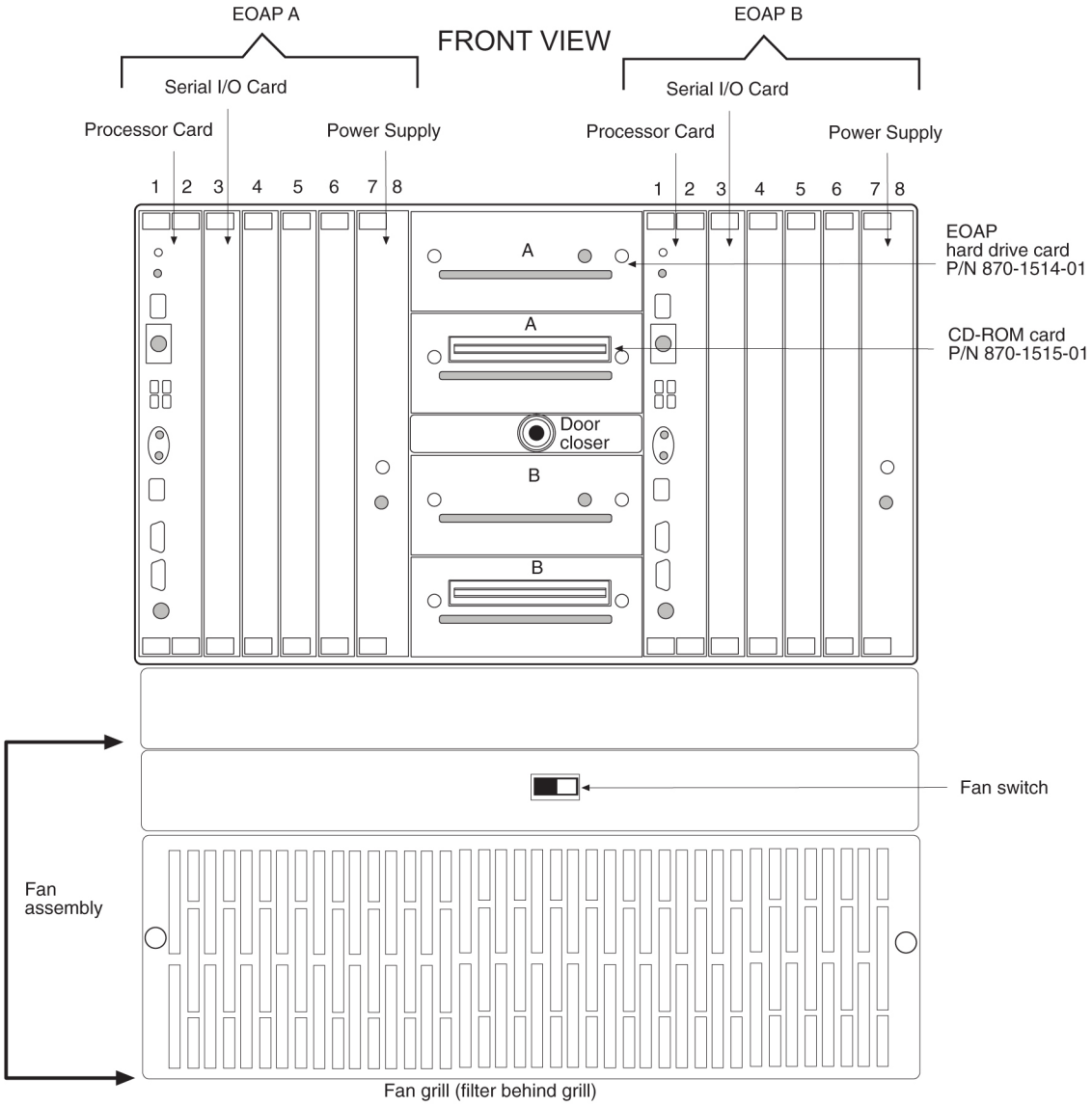
When used as an interface between the SEAC and the EAGLE, the OAP processes SEAS commands into EAGLE commands and EAGLE commands into SEAS commands.

When used as an interface between the SMS and the EAGLE, the OAP receives LNP data and commands from the SMS and converts the SMS commands into EAGLE commands and the LNP data is loaded onto the EAGLE.

The Embedded OAP (EOAP) replaces the existing Texas Micro OAP with a modular unit with field replaceable components which meet or exceed all of the OAP's current capabilities. In addition, the EOAP provides for the future enhancement of the OAP's responsibilities.

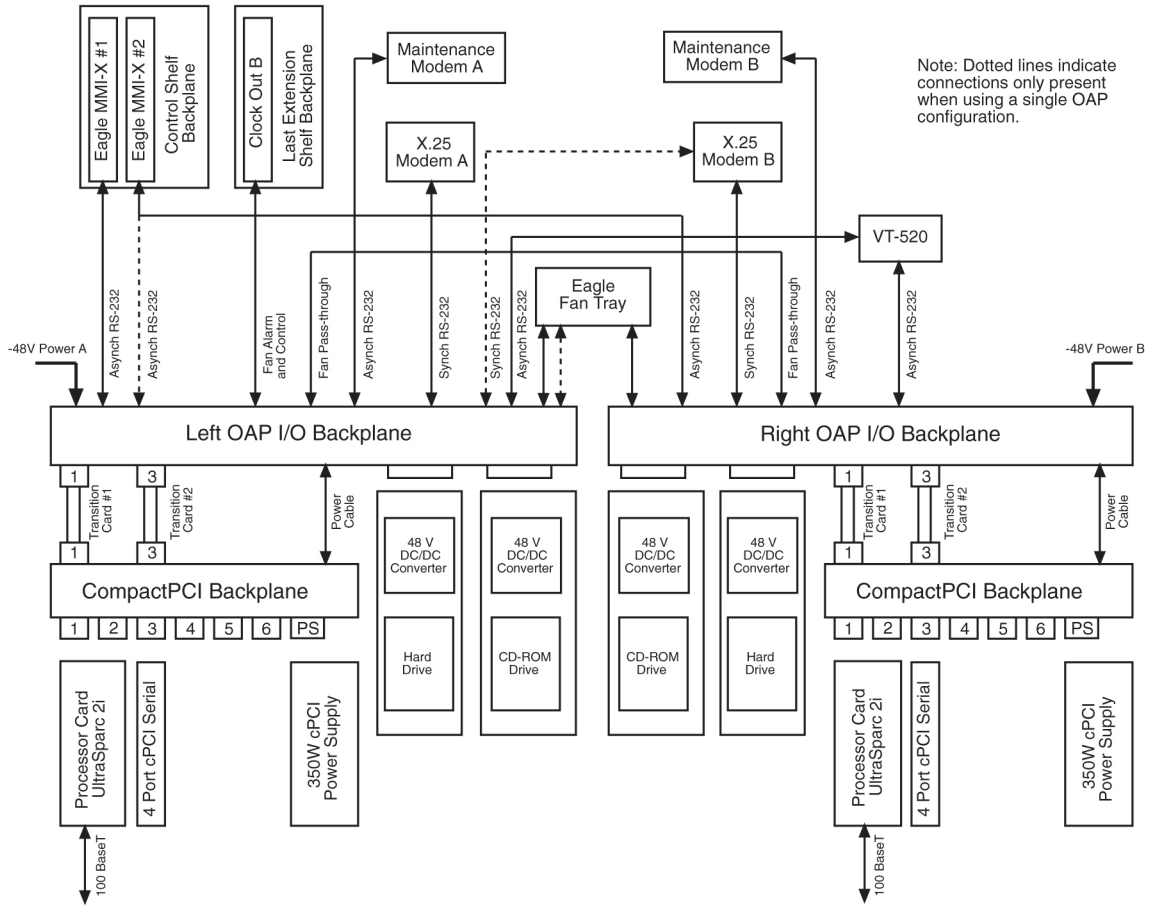
There are two EOAPs in the system, EOAP-A and EOAP-B. The EOAP is in the EOAP shelf which is located in the OAP frame. Each EOAP in the dual configuration consists of a processor card, an interface card, a power supply card, and a center bay containing a removable hard drive and a CD-ROM drive for each EOAP. Figure *Embedded OAP* illustrates the layout of the system. For a functional block diagram, see figure *Functional Block Diagram of the EOAP*.

Figure 2-22. Embedded OAP



The following figure shows a functional block diagram of the EOAP.

Figure 2-23. Functional Block Diagram of the EOAP



The following table shows the hardware components of the EOAP.

Table 2-20. Hardware Requirements of the EOAP

Component	Part Number
Processor Card with the UltraSparc 2I processor and 64 MB of RAM (expandable to 1 GB)	800-0271-01
4-Port Serial I/O Card	800-0272-01
350W 48V DC/DC Power Supply	800-0274-01 800-0267-01
CompactPCI Backplane	850-0489-01
Tekelec APC SCSI Hard Drive - 4 GB minimum	870-1514-01
Tekelec APC 32X SCSI CD-ROM Drive	870-1515-01
Tekelec Right OAP I/O Backplane	850-0487-01
Tekelec Left OAP I/O Backplane	850-0488-01

Component	Part Number
Tekelec Transition Card - Processor Card to the OAP I/O Backplane	850-0496-01
Tekelec Transition Card - Serial I/O Card to OAP I/O Backplane	850-1514-01

EOAP Processor Card - P/N 800-0271-01

Slots 1 and 2 of the EOAP contains the processor card using the UltraSparc 2i processor. This card provides two serial ports, A and B, for connecting the EOAP to the EAGLE. Serial port A is accessible from the EOAP backplane and from an RS232C mini-DIN8 serial interface on the front panel. Serial port B is accessible from the EOAP backplane. Both serial ports provide RS232 asynchronous modem support.

CAUTION

CAUTION: The front panel interface on serial port A is provided for monitor output. However, no provision has been made to safeguard the processor card against data entry from the front panel interface. Data input through the front panel serial port is allowable so long as serial port A is not accessed from the rear panel while this occurs. Unpredictable events will occur on the processor card if data is simultaneously input on serial port A through the front panel and back panel connectors.

An RJ-45 Ethernet port on the front of the card provides a negotiated 10/100BaseT network access for LNP support using the LSMS.

The processor card also contains a seven-segment LED, a system status LED, a user configurable alarm LED, and abort and reset capabilities through both manual and software intervention.

The seven segment LED displays the numeric values 0 through 9 and the alphabetic values A through F and H. If the seven-segment LED is displaying a number zero, the processor has been halted. If the seven-segment LED is displaying a number one, the processor is operating normally. If the seven-segment LED is blank, the processor is being reinitialized. The other values for the seven-segment LED have not been defined in Release 24.0.

The processor card is a field replaceable unit. If the processor card is replaced, new license keys must be installed on the hard drive through the EAGLE initiated OAP user interface. This is due to the change in the Host ID that will occur with the new processor card.

The processor card is equipped with 64 MB of RAM, and is expandable to 1 GB of RAM.

4-Port Serial I/O Card - P/N 800-0272-01

Slot 3 of the EOAP contains the 4-port serial I/O card, which supplies four RS-232C serial ports. These ports are accessible from the backplane. Two of these ports are used for interfacing the EOAP with SEAS. The other two ports are used to connect the EOAP to a VT-520 console or to an RS232C asynchronous modem. The 4-port serial I/O card is a field replaceable unit.

350W Power Supply - P/Ns 800-0274-01 and 800-0267-01

The power supply for the EOAP is a field replaceable unit that occupies slots 7 and 8 of the EOAP. One of two power supplies can be used on the EOAP. P/N 800-0274-01 is the preferred power supply to use with the EOAP. This power supply is a DC-DC switcher-style power supply. Power supply P/N 800-0276-01 is an alternate power supply that can be used on the EOAP and is based on Astec DC-DC converters.

Two LEDs are located on the front of the power supply. The **POWER GOOD** LED (a green LED) should be on when input voltage falls within the allowable range of -48 to -72 VDC. The **FAULT** LED (a 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 following table shows the specifications of both power supplies.

Table 2-21. Power Supply Specifications

Specification	Power Supply P/N 800-0274-01	Power Supply P/N 800-0267-01
Input Range	36VDC - 72VDC	40VDC - 72VDC
Efficiency	75% Typical, derated 2.5% per degree above 40 degrees C	75% typical, derated 10W per degree over 50 degrees C
Ripple/Noise	greater of 1% peak-peak or 50mV	50mV max. for all outputs, peak-peak, dc to 20MHz with coaxial probe and 0.1uF/22uF capacitors at the connector
Connector	Positronics P/N PCI38M 400A1	Positronics P/N PCI38M 400A1
Outputs	+3.3 V - 40A maximum * +5.0 V - 50A maximum * +12.0V - 12A maximum -12.0 V - 2A maximum * - Combined 3.3V and 5.0V current not to exceed 50A	+3.3 V - 25A maximum +5.0 V - 50A maximum +12.0V - 9A maximum -12.0 V - 2A maximum
Inrush Current	60 A maximum @ 72V 40 A maximum @ 48V 20 A maximum @ 36V	15 A maximum
Internal Fuse	15A replaceable fuse	15 A replaceable fuse

Hard Drive and CD-ROM Drive

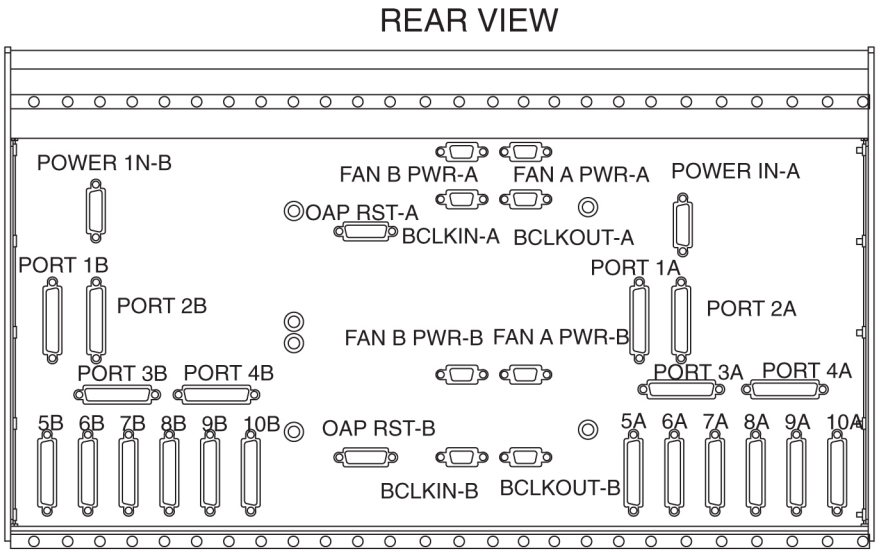
The center section of the dual EOAP system contains four individual drive bays. The first and third drive bays contain a SCSI hard drive (P/N 870-1514-01) with a minimum capacity of 4 GB, and is a field replaceable unit. The first drive bay is hardwired to EOAP-A and the third drive bay is hardwired to EOAP-B. If the hard drive is replaced, all site specific information must be reloaded on the EOAP from the EAGLE.

The second and fourth drive bays contain a 32X SCSI CD-ROM drive (P/N 870-1515-01). The second drive bay is hardwired to EOAP-A and the fourth drive bay is hardwired to EOAP-B. The CD-ROM drive is a field replaceable unit.

EOAP Connectors

The cards in slots 1 through 8 for each EOAP are connected to the CPCI backplane (P/N 850-0489-01) as shown in figure *Functional Block Diagram of the EOAP*. The interface from the EOAP to the EAGLE is provided through another set of backplanes, the left and right backplanes (P/Ns 850-0488-01 for the left backplane and 850-0487-01 for the right backplane). The layout of the left and right backplanes is shown in figure *EOAP Backplane and Connectors*. The hard disk and CD-ROM drive for each EOAP connect directly to the left and right backplanes. The CPCI backplane connects to the right and left backplanes with the APC Transition Cards, one for the processor card - P/N 850-0496-01, and one for the serial I/O card - P/N 850-1514-01. The transition cards only provides an electrical connection between the CPCI backplanes and the left and right backplanes for the EOAP assembly. The transition cards do not perform any processing of the signals from either backplane.

Figure 2-24. EOAP Backplane and Connectors



External Interface Descriptions

The next two tables show the connectors used on the backplanes of the EOAP and on the front of the processor card.

Table 2-22. External Interfaces - OAP A

Connector (Silkscreen Label)	Signal	DESCRIPTION (Software name in parenthesis)	TYPE	Usage/Destination
POWER IN-A	System Power	-48VDC, CHASSIS GND, -48VDCRTN	N/A	From Fuse Panel
FAN A-PWR-A	Fan A Power	FAN POWER, ALARM, CONTROL	N/A	To Fan Assembly
FAN B-PWR-A	Fan B Power	Fan Power, Alarm, Control	N/A	To Fan Assembly
OAP RST-A	Oap Reset	OAP Hard Reset Lines	N/A	Currently Unused
BCLKIN-A	B Clock Input	Provides Fan Alarm/Control From EAGLE to Fan A	N/A	From Last Extension Shelf Backplane
BCLKOUT-A	B Clock Output	Provides Fan Alarm/Control to Fan B	N/A	To System B BCLKIN
1A	RS-232	Processor Card - Slots 1 and 2 (/dev/term/a)	Asynchronous	EAGLE Terminal Port
2A	RS-232	Processor Card - Slots 1 and 2 (/dev/term/b)	Asynchronous	EAGLE Terminal Port
3A	RS-232	Serial I/O Card - Slot 3 (/dev/term/0)	Asynchronous	VT-520 Terminal

Connector (Silkscreen Label)	Signal	DESCRIPTION (Software name in parenthesis)	TYPE	Usage/Destination
4A	RS-232	Serial I/O Card - Slot 3 (/dev/term/1)	Asynchronous	Maintenance Modem
5A	RS-232	Serial I/O Card - Slot 3 (hih0)	Synchronous	X.25 Port
6A	RS-232	Serial I/O Card - Slot 3 (hih1)	Synchronous	X.25 Port
7A	RS-232	Reserved for future expansion through Slot 4	Asynchronous or Synchronous	Currently Unused
8A	RS-232	Reserved for future expansion through Slot 4	Asynchronous or Synchronous	Currently Unused
9A	RS-232	Reserved for future expansion through Slot 4	Asynchronous or Synchronous	Currently Unused
10A	RS-232	Reserved for future expansion through Slot 4	Asynchronous or Synchronous	Currently Unused
Front Ethernet Port (RJ-45)	100BsT	LAN Connection	10/100BaseT	Connection to LSMS via LAN
Front Serial A/B Port	RS-232	Not used, CANNOT be used while rear serial ports are in use.	Asynchronous	Not to be used in standard configuration
RESET Switch	POR	Mechanical reset key, when enabled and toggled, generates a push-button Power On Reset (POR) to the UltraSPARC-2I. Same affect as a Power On Reset from the power supply, except set status bit B_POR in the Reset_Control Register.	Mechanical switch.	To be used when a hard reset is required. System must be halted prior to execution to ensure disk integrity.
ABORT Switch	XIR	Mechanical abort key, when enabled and toggled, generates XIR (externally initiated reset) without resetting the whole system. Sets B_XIR in Reset_Control register.	Mechanical Switch	To be used when abort is required. System must be halted prior to execution to ensure disk integrity.
Front SCSI Port	SCSI-2	Auto-terminating narrow SCSI-2	SCSI-2	Reserved for use by manufacturing
Front Keyboard Port	Sun Keyboard and Mouse	8-pin mini-DIN	Asynchronous	Supports Sun Keyboard and Mouse (Unused)

Table 2-23. External Interfaces - OAP B

Connector (Silkscreen Label)	Signal	DESCRIPTION (Software name in parenthesis)	TYPE	Usage/Destination
POWER IN-B	System Power	-48VDC, CHASSIS GND, -48VDCRTN	N/A	From Fuse Panel
FAN A-PWR-B	Fan A Power	FAN POWER, ALARM, CONTROL	N/A	To Fan Assembly
FAN B-PWR-B	Fan B Power	Fan Power, Alarm, Control	N/A	To Fan Assembly
OAP RST-B	Oap Reset	OAP Hard Reset Lines	N/A	Currently Unused
BCLKIN-B	B Clock Input	Provides Fan Alarm/ Control From EAGLE to Fan A	N/A	From Last Extension Shelf Backplane
BCLKOUT-B	B Clock Output	Provided for future expansion of additional Fan Assemblies	N/A	Currently Unused
1B	RS-232	Force Processor - Slot 1 (/dev/term/a)	Asynchronous	EAGLE Terminal Port
2B	RS-232	Force Processor - Slot 1 (/dev/term/b)	Asynchronous	EAGLE Terminal Port
3B	RS-232	Aurora Serial I/O - Slot 3 (/dev/term/0)	Asynchronous	VT-520 Terminal
4B	RS-232	Aurora Serial I/O - Slot 3 (/dev/term/1)	Asynchronous	Maintenance Modem
5B	RS-232	Aurora Serial I/O - Slot 3 (hih0)	Synchronous	X.25 Port
6B	RS-232	Aurora Serial I/O - Slot 3 (hih1)	Synchronous	X.25 Port
7B	RS-232	Reserved for future expansion through Slot 4	Asynchronous or Synchronous	Currently Unused
8B	RS-232	Reserved for future expansion through Slot 4	Asynchronous or Synchronous	Currently Unused
9B	RS-232	Reserved for future expansion through Slot 4	Asynchronous or Synchronous	Currently Unused
10B	RS-232	Reserved for future expansion through Slot 4	Asynchronous or Synchronous	Currently Unused
Front Ethernet Port (RJ-45)	100BsT	LAN Connection	10/100BaseT	Connection to LSMS via LAN
Front Serial A/B Port	RS-232	Not used, CANNOT be used while rear serial ports are in use.	Asynchronous	Not to be used in standard configuration

Connector (Silkscreen Label)	Signal	DESCRIPTION (Software name in parenthesis)	TYPE	Usage/Destination
RESET Switch	POR	Mechanical reset key, when enabled and toggled, generates a push-button Power On Reset (POR) to the UltraSPARC-2I. Same affect as a Power On Reset from the power supply, except set status bit B_POR in the Reset_Control Register.	Mechanical switch.	To be used when a hard reset is required. System must be halted prior to execution to ensure disk integrity.
ABORT Switch	XIR	Mechanical abort key, when enabled and toggled, generates XIR (externally initiated reset) without resetting the whole system. Sets B_XIR in Reset_Control register.	Mechanical Switch	To be used when abort is required. System must be halted prior to execution to ensure disk integrity.
Front SCSI Port	SCSI-2	Auto-terminating narrow SCSI-2	SCSI-2	Reserved for use by manufacturing
Front Keyboard Port	Sun Keyboard and Mouse	8-pin mini-DIN	Asynchronous	Supports Sun Keyboard and Mouse(Unused)

Asynchronous Maintenance Modem

Although not provided with the EOAP, a Hayes compatible modem can be connected to the EOAP to provide connectivity for remote monitoring and maintenance. This allows access to the EOAP as required by Tekelec Technical Services. The modem is connected to the EOAP through the 4-Port Serial I/O Card through connectors 4A or 4B on the EOAP backplanes. The modem must be configured as shown in table *Modem Configuration.* See tables *External Interfaces - OAP A*, *External Interfaces - OAP B*, and figure *EOAP Backplane and Connectors* for the designation and location on the backplanes of each connector.

Table 2-24. Modem Configuration

Modem Parameter	Value
Baud Rate	9600 bits per second
Data Bits	7
Parity	Even
Stop Bits	1

EOAP User Console

The user console for the EOAP is provided by a Digital Equipment Corporation VT520 terminal. The VT520 is connected to the EOAP using an RS232C terminal cable attached to connectors 3A or 3B on the EOAP backplanes. See tables *External Interfaces - OAP A*, *External Interfaces - OAP B*, and figure *EOAP Backplane and Connectors* for the designation and location on the backplanes of connectors 3A or 3B. This terminal allows for monitoring and direct interfacing capabilities to the EOAP and must be set up for VT100 emulation.

Fans

To help keep the EOAP cool, the EAGLE fan assembly is mounted underneath the EOAP. The fan assembly consists of eight fans, two LEDs, and a three-way switch. The fan assembly is powered from the A and B power sources on the EOAP backplanes (connectors FAN A-PWR-A, FAN A-PWR-B, FAN B-PWR-A, and FAN B-PWR-B2, see tables *External Interfaces - OAP A*, *External Interfaces - OAP B*, and figure *EOAP Backplane and Connectors*.

The three-way switch allows the user to specify how the fans are controlled. The normal position of the switch allows the system software to control when the fans are turned on and off. The **ON** and **OFF** positions of the switch turns the fans on and off and overrides any control by the system software.

One of the LEDs shows whether the fans are on (LED is green) or off (LED is off). The second LED (see table *Fan Alarm Status*) shows the alarm status of the fans.

Table 2-25. Fan Alarm Status

LED	Alarm Status
Green	No Fan Alarm
Red	Fan Alarm
Off	No Power

UAMs

If there is a failure of any of the fans, or if the three-way switch is in the **OFF** position, the alarm status LED is red, and a minor alarm (unsolicited alarm message 302) is generated at the EAGLE.

```
RLGHNCXA03W 99-01-07 00:57:31 EST Rel 24.0.0
*   0055.0302 *  SYSTEM               Cooling Fan Failure
```

When the fan failure is cleared, or when the three-way switch is placed in either the ON or normal position, the fan alarm is cleared, the alarm status LED is green, and unsolicited alarm message 303 is generated at the EAGLE.

```
RLGHNCXA03W 99-01-07 00:57:31 EST Rel 24.0.0
    0056.0303    SYSTEM               Cooling Fans Normal
```

The fan alarm and control input and output are obtained from the Clock Out B connector on the last EAGLE extension shelf and connected to the BCLKIN-A, BCLKIN-B, BCLKOUT-A, and BCLKOUT-B connectors on the EOAP backplanes. See tables *External Interfaces - OAP A*, *External Interfaces - OAP B*, and figure *EOAP Backplane and Connectors* for the designation and location on the backplanes of each connector.

Third Party Software

The following table shows the third party software and the versions of the software required by the EOAP.

Table 2-26. Third Party Software for the EOAP

Product	Vendor	Embedded OAP Version
DSET APLI	DSET	4.1.3f compiled for Solaris version 2.5.1
DSET DSGRuntime	DSET	4.1.3f compiled for Solaris version 2.5.1
Solstice OSI	Sun	8.1.1
Solaris	Sun	2.5.1
SunLink HSI/S	Sun	2.0
Solstice X.25	Sun	9.1
NetPilot UAL Software	Bellcore	8.2
Performance Technologies Driver	Performance Technologies	810P027930

EOAP to EAGLE Interface

The EOAP is connected to the EAGLE through the EOAP backplane. The two serial ports on the processor card are used for this connection. The cables are connected to any two of the terminal ports (MMI 0-MMI 15) on the EAGLE control shelf backplane.

The EOAP connected to the lower numbered terminal port is considered by the EAGLE to be OAP A, and the EOAP connected to the higher numbered terminal port is considered by the EAGLE to be OAP B.

The terminal port being used by the EOAP must be configured in the EAGLE with the **type=oap** parameter of the **chg-trm** command. When the **type=oap** parameter is specified with the **chg-trm** command, none of the communication attribute parameters, **baud** (the baud rate of the terminal port), **prty** (the parity of the terminal port), **sb** (the number of stop bits for the terminal port's RS-232 connection), and **fc** (the type of flow control for the terminal port's RS-232 connection) can be specified. These parameters are defaulted to the values shown in the following table.

Table 2-27. EAGLE Terminal Port Configuration for the EOAP

Terminal Port Parameter	Value
Baud Rate (**baud**)	19200 bits per second
Parity (**prty**)	even
Stop Bits (**sb**)	1
Flow Control (**fc**)	hw - hardware flow control

To allow the user to reset the EOAP from the EAGLE terminal, an alarm/reset cable connects to the EOAP at the OAP RST-A and OAP RST-B connectors and on the EAGLE at the OAPALM connector on the control shelf backplane. The EAGLE **init-oap** command is used to initiate the reset of the EOAP. The **init-oap** command uses the parameters **oap** and **force**.

- **oap** – Specifies which OAP is being initialized, as considered by the EAGLE.

— **a** – OAP A

— **b** – OAP B

— **both** – Both OAPs

- **force** – Forces the reset of the specified OAP if that OAP is operational (its state is either IS-NR, in-service normal, or IS-ANR, in-service abnormal) and it is the only operational OAP. The values for this parameter are either **yes** or **no**. If the specified OAP is not operational, the **force=yes** parameter is not required. The default value for the **force** parameter is **no**.

If the specified OAP is the only operational OAP and the **force=yes** parameter is not specified for the **init-oap** command, the **init-oap** command is rejected with this message.

```
E2813 Cmd Rej: FORCE=YES must be specified to initialize the last OAP
```

The **init-oap** command requires that the SEAS feature is on, or the **init-oap** command is rejected with this message.

```
E2812 Cmd Rej: SEAS feature or LNP feature is not configured
```

EOAP to SEAS Interface

The EOAP is connected to the SEAC using these connectors on the EOAP backplanes: 5A, 5B, 6A, and 6B. From one of these ports, an RS232C cable is connected to a 9600 bps synchronous modem, which in turn is connected to the SEAS system. If only a single EOAP is being used, both ports on that EOAP are connected to two separate modems. If both EOAPs are being used, only one port on each EOAP is connected to a modem that is connected to the SEAS system. See tables *External Interfaces - OAP A*, *External Interfaces - OAP B*, and figure *EOAP Backplane and Connectors* for the designation and location of each connector on the backplanes.

EOAP to LSMS Interface

The EOAP is connected to the LSMS through the Ethernet port (an RJ-45 connection) located on the front of the Processor Card using a 10/100BaseT cable.

The EOAP handles eight messages from the LSMS at a time (process and respond to the LSMS), although multiple messages may be sent to the EOAP. No more than eight messages should be sent from the LSMS to the EOAP without a response being returned by the EOAP. If more than one message is sent to the EOAP without the LSMS waiting for a response, the LSMS must manage retries and the sequencing of messages.

The EOAP must be configured locally with the LSMS OSI-Address information necessary for association establishment. The EOAP will initiate association connections with the LSMS.

End Office Support (IP^7 Release 5.0)

Description

Customers see the IP ^{7} Secure Gateway product as a means by which they can take advantage of next generation network technology by migrating existing signaling end points from the PSTN to the IP network. The fact that the

SG is a signaling transfer point and has its own point code, however, presents a significant network management issue for them. Some customers do not want to obtain a new point code and reconfigure their network in order to introduce the SG and an IP end office node. This feature provides such customers the means to perform the migration without using a new point code or reconfiguring their network.

Refer to the *Database Administration Manual - Features* for current information on this feature.

Upgrade Considerations

The upgrade of fielded SG software will take into account the changes introduced by End Office Support, and no degradation of system capability will occur from such an upgrade. This feature adds the new Remote Application Table.

Limitations

- The APC assigned to an IPGW linkset should not be used as an IPC for an EO Node. The IPGWx application is to be used as a redundant pair of cards. Proper use would involve having equal cost routes to each linkset of a pair of IPGWx cards. This scheme prevents the use of the IPGWAPC since only one route should exist to that point code. In addition, the IPGWx application currently expects to receive only SNMs for the IPGWAPC. All messages received for the IPGWAPC are discarded, though SNMs may generate MTP primitives. This feature will not prevent the IPGW APC being provisioned as an IPC, but IPGWx will discard the traffic destined to the IPC for this configuration.

- A third point code, the IPC, must be assigned to the EO Node, in order to allow two equal cost routes to be provisioned.

- The End Office Support feature allows one or more IP network elements to share the SG's true and secondary point codes. IP nodes having their own point code are also supported, but not as end office nodes. This feature eliminates one and only one point code for a given network type.

- This feature provides no method for a mated pair of SGs to share an End Office Node. An End Office Node shares the true or secondary point code of the SG. Each SG of a mated pair continues to require a unique true point code. There are no benefits of redundancy if mated SGs share an IPNE operating as two EO Nodes.

- This feature prevents an IP end office node from receiving through-switched messages having SI=0, SI=1, and SI=2, with the exception of UPUs. If such messages are desired, then the IP network element cannot be configured as an end office node.

- An end office node cannot share a SCCP subsystem other than SCMG with the SG. An end office node's SCCP subsystem takes priority over the SG's local SCCP subsystems.

- An end office node must not generate non-UPU, non-TFC, and non-RCT network management messages having OPC=TSPC or CPC=TSPC. The IPGWx application will discard such messages that it receives.

- There are no new measurements specific to the End Office feature. Existing per-socket measurements can be used to see the number of MSUs going to and received from each socket.

- Messages arriving at the SG from the network and having DPC=IPC shall be routed, just as if the message had arrived having DPC=TSPC and an assigned remote application. Such a message will bypass the new discrimination algorithm and be immediately forwarded to the EO Node.

- This feature shall not prevent a user from provisioning a routing key having DPC=IPC. The IPGWx will not generate network management when such a routing key changes states. Messages arriving at the IPGWx cards with DPC=IPC are changed to have DPC=TSPC prior to routing key lookup, and so a routing key having DPC=IPC will never be a match for a message. If no matching routing key having DPC=TSPC is available, then MSUs with DPC=IPC arriving at the IPGWx for transmission will be silently discarded with private pegs.

Enhance GSM MAP Screening to add TC_Continue and End (Release 35.1)

Description

The Enhance GSM MAP Screening to add TC_Continue and End feature enhances the GSM MAP Screening, Enhanced GSM MAP Screening, and MTP-based GSM Screening features by enabling MAP screening to be performed on non-segmented TC_Continue and TC_End messages.

In order for MAP screening to occur, the messages must meet the following requirements:

- TCAP-CONT messages must have an Invoke component type.
- TCAP-END messages must have a Return-Result (Test) type.

Screening is not performed on messages that do not meet these requirements.

Hardware Requirements

The Enhance GSM MAP Screening to add TC_Continue and End feature has no hardware requirements.

Limitations

The GSM Map Screening feature must be on before the Enhance GSM MAP Screening to add TC_Continue and End can be enabled.

Enhance RTRV-LOG (Release 31.3)

This enhancement will allow the customer to customize RTRV-LOG output. The following list contains examples of customized reports of the logs:

- Filtered for a particular Output Group
- Separated between UIMs and Alarms and further separated by Output Group
- Filtered by a given alarm number or range of numbers.

In addition, this command is modified to become a cancelable command, allowing a user or sysadmin to stop the processing of the command at any time during its execution.

The RTRV-LOG enhancement feature also includeds a new command (rtrv-trbltx) that allows the craftsperson to display information from the trbltx table, which contains all of the UIMs and Alarms for each EAGLE release. The information displayed for each entry of the trbltx table will be the MRN, alarm severity (for Alarms), Output Group and text. Optional parameters for rtrv-trbltx allow the craftsperson to display a subset of the information available to them. The optional parameters for rtrv-trbltx allow an Output Group or TYPE to be specified or a range of MRN numbers to be specified. Additionally, all Output Groups may be displayed with a list of MRNs that match each Output Group.

Enhanced Database Status Reports (Release 20.0)

The database level (resident on every card in the system) and the “coherency” indicator are displayed with this feature. The coherency indicator identifies corrupt database files, which can be corrected using database management commands.

Enhanced Bulk Download (Release 25.0)

The EAGLE Enhanced Bulk Download (EBD&A) feature adds “infrastructure” to the EAGLE that supports the implementation of higher functionality at the LSMS.

For current details of this feature, refer to the *LNP Database Synchronization Manual*.

Hardware Requirements

As previously stated, this feature requires the following additional EAGLE hardware, which is devoted to the EBD&A function:

- One (1) DCM card and FANS.
- One (1) BLM card. This BLM card must be equipped with enough applique memory cards to be able to load the entire LNP DB. Specifically, the applique requirements for the EBD&A BLM card are exactly the same as the memory requirements for a TSM card running the SCCP application.

Additional memory is required on the SCCP cards to support the addition of 12 million ported numbers. Memory may be added in 256 MByte increments to the TSMs, up to a maximum of 1024 Mbytes of memory.

The following TSM configurations are supported:

- TSM256: TSM with 256 MB populated memory. Maximum number of ported numbers supported: 2,000,000.
- TSM512: TSM with 512MB populated memory. Maximum number of ported numbers supported: 4,000,000.
- TMS768: TSM with 768MB populated memory. Maximum number of ported numbers supported: 6,000,000.
- TSM1024: TSM with 1024MB populated memory. Maximum number of ported numbers supported: 8,000,000 without optional software feature, 12,000,000 with optional software feature. In addition, the parameter **`lnp12mil=on`** must be set.

Refer to the *NSD Hardware Manual* for current hardware information.

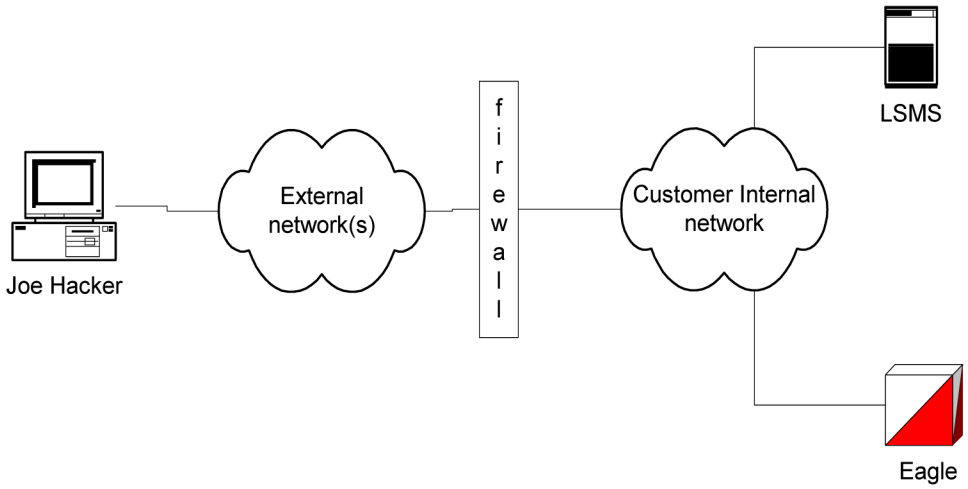
Serviceability

LSMS↔DCM Ethernet Security

Security of the LSMS↔DCM ethernet connection is the customer's responsibility. Neither the EAGLE nor the LSMS will provide any type of security to thwart unauthorized attempts to access the EAGLE and/or LSMS by “hijacking” the connection.

If the customer is concerned about security (e.g. a hacker who gains access to the EAGLE by masquerading as an LSMS, and downloading a faulty database to EAGLE via the bulk download facility), he should take steps to ensure that security is not compromised. One such method would be to provide the LSMS↔DCM connection totally within the customer's own internal network, and install a firewall between the customer's internal network and the "outside world,", as illustrated in the following figure.

Figure 2-25. LSMS↔DCM Connection with Firewall



Administration of the EBD&A Feature

Provisioning of Necessary BLM and DCM Components

For the EBD&A feature to operate, a dedicated BLM and DCM must be present and running the new GPLs developed for this feature.

- Associating the new EBD&A GPLs with the DCM and BLM card types is accomplished by the existing **`ent-card:appl=`** command to accept new GPL types (EBDADCM, EBDABLM).

- Other commands that could affect the loading or monitoring of these BLM and DCM components of EBD&A have been modified to accommodate the new GPL types as necessary.

Provisioning of EBD&A DCM Ethernet Details

Provisioning of this information is performed by new commands. The following scenario shows the minimum number of steps required to configure the DCM card, so that it is functional for EBD&A purposes:

1. **`chg-ip-card:loc=xxxx:`**

This command provides little information for the EBD&A DCM, but is a pre-requisite for the command to follow. Since the EBD&A DCM card will be acting as a sockets server, additional parameters that this command provides (such as domain name server IP address) are not needed.

2. **`ent-ip-host:host=dcm_name:ipaddr=a.b.c.d`**

   This command tells the DCM card what hostname is associated with the DCM card's IP address. The value for the **`host=`** parameter is required in order to associate the TCP/IP port (specified in the next step) with the TCP/IP address (specified on the previous step), but its value is unimportant to the EBD&A DCM: specify any unique value. The **`ipaddr=`** value must be the same value that was specified on the **`chg-ip-lnk`** command.

3. **`chg-ip-lnk:loc=xxxx:port=x:ipaddr=a.b.c.d:submask=x.x.x.x:…`**

   This command tells the DCM card at **`loc=`** to assign the IP address (**`ipaddr=`**) to the indicated port (port in this context is the physical port 'A' or 'B' on the DCM card: it does not refer to the TCP/IP port number). The DCM card now knows what its IP address is for the indicated physical port. Additional parameters available for this command can be used if necessary to configure the operational parameters of the DCM's ethernet link (e.g. link speed).

NOTE: The EBD&A feature is designed to use only the 'A' port of the DCM card. Be sure to attach the physical ethernet connection (i.e. the wire) only to the 'A' port, and then configure the 'A' port accordingly. The 'B' port is ignored by the EBDADCM GPL, even if provisioned via the CHG-IP-LNK command. The 'B' port can be configured and used to allow source-level debugging of the DCM card via the VxWorks "Tornado" debugging tool.

Selection of DCM Card Slot

The DCM card currently takes up 2 slots in the EAGLE shelf card cage due to the large heat sink on the top of the DCM card. Because of this, the DCM cannot be provisioned in any arbitrary slot. Certain slots in the card cage are adjacent to the cage sides, and/or are adjacent to metal supports welded into the card cage. These slots cannot be used to house a DCM card.

Also, the DCM card requires a substantial amount of power. Due to the way the EAGLE fuses power pairs of card slots, the DCM should always be provisioned into an odd-numbered card slot. For example, fuse 1A provides power to both slots 1101 and 1102. The combined current draw for both of these slots must not exceed 3A, or the fuse may blow. Inserting a DCM into slot 1102 when there is another card in 1101 could cause the total current requirements for both of these slots to exceed 3A.

Additionally, the shelf equipped with the DCM card must be equipped with fans in order to keep the card from overheating.

Minimum LSMS↔EAGLE Ethernet Facility

The customer is responsible for selecting and providing a connection between the EAGLE and LSMS locations so that the LSMS and DCM components may communicate via ethernet.

Unless the speed of the communications line is very poor, the maximum processing speed of the EBD&A feature will most likely be limited by the performance of the BLM card, which has a maximum rate of » 400 DB inserts/second as previously stated; providing communications facilities of very high capacity will not make the EBD&A feature perform its work any faster.

However, selection of an extremely slow communications line will result in EBD&A performance degradation.

Assuming the following:

- Maximum BLM DB insert rate = 400 entries/second.
- Average size of a DB record passed from LSMS à DCM over ethernet = 95 bytes/entry (Note: maximum size would be 120 bytes/entry).
- LSMS is able to extract DB entries from its database (Versant) and present them across the ethernet connection to the EAGLE as fast as the BLM can process them.

In order to keep the BLM card 100% busy during bulk download, the ethernet connection must have a transmission rate of:

400 entries/second * 95 bytes/entry = 38,000 bytes/second

During high-speed audit, it is estimated that the BLM can extract and present 3400 TN/checksum pairs/second. The LSMS, however, has a measured maximum performance of 1,666 extracts from its database/second, therefore the LSMS will most likely be the limiting bottleneck during audits:

1666 entries/second * 9 bytes/entry = 14,994 bytes/second

Therefore, Tekelec recommends that the LSMS↔EAGLE communications link installed for the EBD&A feature have a transmission capacity of » 38,000 bytes/second.

Upgrade Considerations

New EBD&A GPLs

The EBD&A feature introduces two new GPL types to Release 25.0. However, upgrades from previous releases to Release 25.0 need not include steps to create these new GPLs on the system being upgraded, since Release 25.0 introduces functionality to create feature-specific GPLs at the time the feature is installed at the customer site.

Modifications to EAGLE LNP Subscription Records on Disk

A new 4-byte field has been added to each LNP subscription record in the EAGLE LNP DB. This field is created from unused pad area already present in the record. This new field holds the CRC-32 checksum for the record, enabling the high-speed audit of the subscription record contents by the LSMS. There is no need to obsolete existing LNP DB tables, or create new ones, in order to accommodate the new checksum.

Enhanced GPL Management (Release 25.0)

Description

This feature minimizes the effort required to add new GPLs (applications) to EAGLE by updating a table of GPL attributes. The table makes each application available to all existing commands which contain the "**appl = <xyz>**" parameter. Likewise, all commands that display an application also have the parameter available.

All commands that use an **appl=** parameter, as well as the commands that administer GPLs, must check the existence of the GPL definition in the table as part of their semantic validation.

All commands that display an APPL as part of their output must retrieve the application name from the new table.

All processes that download applications must retrieve the GPL DOS filename from the new table.

Upgrade Considerations

In order to provide access to new GPLs, the APPL Definitions Table must be updated. Most of this table is filled in at compile time, which means that an updated OAM GPL must be provided in order to support new GPLs. During the upgrade process, new GPLs are available once the updated OAM is running.

The feature does not change any DCBs or maintenance blocks; thus no on-the-fly conversion of data structures is required.

There are no new DMS tables defined by the feature, and no existing DMS tables are modified; therefore, no database conversion is required.

Enhanced GSM Map Screening (Release 31.4)

Description

The Enhanced GSM MAP Screening Feature is an enhancement to the existing GSM MAP Screening feature that adds the ability to perform screening based on the Called Party Address Global Title Digits (CdPA) including NP and NAI. In addition, wild card entries are supported for the MAP Operation Code, CgPA and CdPA.

Prior to this feature, GSM Map Screening was limited to the combinations of MAP Operation Codes and Calling Party Address Global Title Digits (CgPA GTA). With this feature, the screening is extended to include the ability to a combine the CgPA and CdPA, each including NP and NAI information, along with a new wild card option for the MAP Operation Code, CgPA, and CdPA.

The supported screening actions will continue to be: Discard, Route, Duplicate, Forward , Pass, Duplicate and Discard, and Error (ATI only).

The Enhanced GSM MAP Screening Feature allows the screening to be extended to include the ability to a combine the CgPA and CdPA, each including NP and NAI information, along with a new wild card option for the MAP Operation Code, CgPA, and CdPA.

Limitations

- Since there is a 150 characters limit on PROCOMM terminal, sometimes a single ENT/CHG-GSMMAP-SCRN command does not fit in a single line when ACTION is FORWARD, DUPLICATE or DUPDISC. If an ENT-GSMMAP-SCRN command doesn't fit in one line, execute the same with less number of parameters, then run CHG-GSMMAP-SCRN command(s) to modify the rule. If CHG-GSMMAP-SCRN command doesn't fit in one line, break the same into multiple commands.

- NPV and NAIV values can't be modified, as they are part of the CgPA and CdPA keys, after implementing this feature.

- If a single entry (CgPA or CdPA) is created which falls into existing range in range entry, then the range entry is not split into two range entries.

- Mass deletion of CgPAs and CdPAs is not allowed.

- If an existing EAGLE with 2000 CgPA entries is upgraded to this release, then a default wildcard CdPA entry is created for each CgPA entry, thus utilizing all of the 2000 CdPA entries. Thus the table remains full and no additional entries will be allowed.
- Measurements data are not be collected for screening rules containing ranged CgPA or CdPA entries.
- The Measurements Platform are provisioned and enabled before EGMS measurements can be collected or reported. EGMS can be turned on without measurements platform installed but EGMS measurements data are not available.
- DSM or later revision card running the VSCCP GPL is required before the EGMS feature can be turned on.
- GTT\GFlex must be turned on and passed prior to this feature.
- If an upgrade to the new release is performed, EGMS remains off, and OAM measurements are being used to report normal GMS data, then the ordering of individual entities within the MEAS MAP Screening Per-Server report will change.
- The retrieve output screens on the EAGLE appear differently after the upgrade, even if the EGMS FAK is not turned ON.
- GSM MAP Screening and Enhanced GSM MAP Screening do not perform best-fit, longest-match searches in the database. Therefore, a match is only found if the digits received in the message exactly match digits in the database. This is true for both individual and range entries. For example, if a number is received containing 15 digits, and a 14 digit database entry exists which exactly matches the first 14 digits of the received number, this does NOT result in a match. The database entry would also have to be 15 digits long.

Enhanced GTT (Release 26.0)

Description

EGTT is an enhancement to the existing GTT function. EGTT provides the following main enhancements to EAGLE's current GTT:

- Increased number of selectors:
- Relaxed GTT rules:
- Deletion of GT:
- Inclusion of SSN in the CDPA:
- Inclusion of OPC in the CGPA:

Refer to the *Database Administration Manual - Features* for current details of this feature.

Upgrade Considerations

After the upgrade and the EGTT feature is enabled, any ITU selectors added with GTI=4 that match any pre-upgraded entries will be an exception to the numbering plan and/or nature of address indicator of the pre-upgraded entry. The pre-upgrade entry will now match on any set of numbering plan-nature of address combinations, other than the added post-EGTT-enabled entries.

Enhanced Link Diagnostics (Release 22.0)

Enhanced Link Diagnostics provides improved information reporting to aid in the investigation of link failures. SS7 Level 2 status information is buffered before and after a link failure has occurred. This feature provides the capability to loop the internal transmit and receive data on the ISCC chip. Link failures can occur on the near end node, far end node or the wire connecting the two nodes. This capability either confirms or eliminates a portion of the near end node as the reason for the link failure.

Enhanced Load Distribution (Release 21.0)

This feature improves the load distribution of traffic on a combined linkset when a signaling link in one of the linksets in the combined linkset fails.

Before Release 21.0, if a signaling link in a combined linkset fails, the traffic is redistributed to the other links in the same linkset. With this feature, the traffic is redistributed over the signaling links in the combined linkset. This feature applies to both ANSI and ITU signaling links.

Traffic is distributed over the combined linkset using the signaling link selection (SLS) values assigned to the signaling links in each linkset. When a signaling link in the combined linkset fails, the system uses the SLS values assigned to the signaling links, the number of signaling links in each linkset, and the number of failed signaling links in the combined linkset to determine which of the remaining signaling links in each linkset will carry the failed signaling link traffic.

To evenly distribute the traffic on all the signaling links in a combined linkset, each linkset in the combined linkset must contain the same number of signaling links.

Enhanced Routing Key Support (IP^7 Release 2.0)

Release 2.0 offers several enhancements for the routing key table that the IP ^{7} Secure Gateway uses to route SS7 Message Signaling Units (MSUs) over the IP network. The routing table is used for SCCP/TCAP-over-IP, ISUP-over-IP, and non-SCCP/non-ISUP connectivity, each of which uses the **`ss7ipgw`** application.

Understanding the Routing Key Table Used in Release 1.0

The routing key table maps SS7 Routing Keys to TCP/IP socket names, as illustrated by the example in table *Example SS7 Routing Key Table*. MSUs that match the parameters in a given row are sent over one of the sockets shown for that row (up to 16 socket associations can be defined for a single routing key). Multiple sockets for a given row allow load sharing. In addition, multiple routing keys can be used to send traffic to a single socket.

Table 2-28. Example SS7 Routing Key Table

SS7 Routing Keys						TCP/IP Sockets that carry traffic for that Routing Key
SS7 DPC	**SS7 SI**	**SS7 SSN**	**SS7 OPC**	**CIC START**	**CIC END**	**Socket Name**
DPC-SI-SSN routing key for SSCP/TCAP-over-IP connectivity						
5-5-5	03	6	-	-	-	KC_HLR1_1201 KC_HLR2_1201 KC_HLR1_1203 KC_HLR2_1203
ISUP-CIC rouiting key for ISUP-over-IP connectivity						
5-5-6	05	-	4-4-4	1	100	DN_MSC1_1201 DN_MSC2_1201 DN_MSC1_1203 DN_MSC2_1203
DPC-SI routing key for non-SCCP/non-ISUP connectivity						
5-5-7	02					SF_HLR1_1204

IP 7 Secure Gateway release 1.0 required the user to use the **`ent-appl-rtkey`** and **`dlt-appl-rtkey`** commands to configure the routing key table, which could hold a maximum of 250 keys. For more information about using these commands, refer to the *IP 7 Secure Gateway Database Administration Manual - Features*.

Enhancements to the Routing Key Table in Release 2.0

IP 7 Secure Gateway release 2.0 provides the following enhancements for routing keys:

- Routing keys can be dynamically configured by the receipt of a TALI message from the IP network.
- Routing keys that are statically defined (using the **`ent-appl-rtkey`** command) can be changed by using a new command **`chg-appl-rtkey`**.
- Up to 1000 routing key entries per DCM card are supported. The customer can specify the maximum number of static keys and dynamic keys to be supported, as long as the total is less than or equal to 1000.

Dynamic Routing Key Registration

This enhancement allows a socket to automatically direct traffic towards, or away from, itself by sending a message to the IP 7 Secure Gateway. This enhancement allows customers to add IP 7 routing key intelligence to their IP applications rather than requiring user entry of static routing keys.

When transmitting Message Signaling Units (MSUs), the IP 7 Secure Gateway routing code looks for a dynamic routing key before searching for a static routing key. When a socket fails, all dynamic entries associated with it are deleted. A dynamic routing key entry can have the same parameters as a static key entry.

Adjusting Static Routing Key Entries

IP 7 Secure Gateway release 2.0 allows the use of the new **chg-appl-rtkey** command to make one of following adjustments to a routing key that has already been statically defined:

- Any existing static entry's socket associations can be overwritten by a new socket association. If the **chg-appl-rtkey** command assigns a new socket name to a routing key has multiple socket associations, all socket associations are replaced with the new socket name.
- Any existing ISUP-CIC entry (an entry whose SI is equal to 05) can be split into two entries by naming a SPLIT value. One entry uses the original CIC START value and makes the CIC END value equal to one less than the SPLIT value. The other entry uses the SPLIT value as its CIC START value and the original CIC END value for its CIC END value. Each entry retains the OPC, DPC, SI, and socket name associations from the original entry.
- Any existing ISUP-CIC entry (an entry whose SI is equal to 05) can have its CIC range extended and/or decreased as long as the new range does not overlap the range on any other key.

Only one of these changes can be made with each use of the **chg-appl-rtkey** command. If additional changes are needed, enter the command again for each change needed.

Support of Additional Routing Keys

IP 7 Secure Gateway release 2.0 supports up to 1000 routing key entries (increased from the previous limit of 250) for each DCM card. These 1000 key entries may be either dynamic entries (added by receipt of a request from the IP network) or static entries (configured using the **ent-appl-rtkey** and **dlt-appl-rtkey** commands) or a combination of both. The user can specify the maximum number of static entries and dynamic entries allowed using the **chg-sg-opts** command.

An additional change is a parameter added to the **rtrv-appl-rtkey** command to allow the user to specify the maximum number of routing key entries to be displayed.

Understanding the Use of Dynamic and Static Routing Entries for ss7ipgw Routing

The IP 7 Secure Gateway has two DCM cards, each of which contains a routing table of up to 1000 entries. The static entries in one table are identical to the static entries in the other table; the dynamic entries may differ depending on messages received from other IP nodes. The following table provides a summary of the characteristics of static and dynamic entries.

Table 2-29. Comparison of Static and Dynamic Entries in Routing Key Table

Characteristic	Static Entries	Dynamic Entries
Provisioned by:	**ent-appl-rtkey**, **dlt-appl-rtkey**, and **chg-appl-rtkey** commands, entered through the OAM, saved on disk, and reloaded to each DCM card upon reset	Receipt of message over socket; purged when socket fails or DCM card is reset
Option of **chg-sg-opts** command used to set maximum number of entries	**srkq**	**drkq**
Same on both DCMs?	Yes	Not necessarily

Characteristic	Static Entries	Dynamic Entries
Used for routing:	Used only if no matching dynamic entry exists	Used first for routing

Enhanced Software Loading (Release 20.0)

This feature reduces the EAGLE's reload time during system initialization or restart to less than 5 minutes. To meet this requirement, the system is reloaded from the fixed disk drives on both the active and standby TDMs (terminal disk modules). Some subsystems are loaded from one fixed disk drive and other subsystems are loaded from the other fixed disk drive. The system operating software determines which subsystems are loaded from each fixed disk drive.

The following conditions are assumed.

- That no cards fail during the loading process.
- All cards remain aligned on the IMT bus which allows the clock to start (no bus transition).
- The loading of gateway screening data is not included in the loading process.

CAUTION: All LIMs are of one application type. The 5 minute loading requirement does not apply if both the SS7ANSI and CCS7ITU applications are being used on the EAGLE.

Enhanced STC Card Performance (Release 35.0)

Description

The Enhanced STC Card Performance feature increases the capacity of the STC card to 4,800 TVG grants per second. This allows MSUs on IP, low-speed, and high-speed links to be monitored for data feed to the Integrated Message Feeder (IMF). This feature applies to both the K6-II and K6-III variants of the SSEDCM card.

Hardware Requirements

The Enhanced STC Card Performance feature has the following hardware requirements:

- A minimum of 2 STC cards must be provisioned in an EAGLE 5 ISS.
- A maximum of 32 STC cards can be provisioned in an EAGLE 5 ISS.
- A maximum of 3 STC cards can be provisioned in shelves that contain HMUX cards.
- The STC capacity of shelves that contain HMUX cards should be provisioned in adjacent shelves. Half of the STC capacity should be provisioned on the current shelf and the other half on either the previous or next shelf.
- Shelves where monitoring of IP links is performed must contain HIPR cards. The STC cards should be provisioned in the same shelf as the HIPR cards. If this does not occur, data feed is inhibited for IPLIMx/ IPGWx, and an alarm is generated for each monitored link on the card.

Limitations

The Enhanced STC Card Performance feature has no limitations.

Enhancement to Backup TFR/TCR Procedures (Release 21.0)

TFR/TCR messages may be lost or not processed at a node due to a signaling link failure, congestion or other error conditions. Because of this, other nodes continue to send traffic over a restricted route. This results in C-link congestion. To help prevent this problem, the TFR/TCR procedures have been improved to send a second backup TFR/TCR once per linkset in response to messages received after the first TFR/TCR.

This feature is currently supported in the EAGLE (Release 3.3 and later) for TFRs with one exception.

When a TFR is generated because of internal congestion, as opposed to normal route failure, the EAGLE responds with one TFR for every 10 messages received. In Release 21.0, this has been changed so that after the first TFR/TCR is sent, the level 3 T18 timer is started. When the level 3 T18 timer expires, the EAGLE sends only one backup TFR/TCR.

This feature applies only to ANSI signaling links.

t a response being returned by the EOAP. If more than one message is sent to the EOAP without the LSMS waiting for a response, the LSMS must manage retries and the sequencing of messages.

The EOAP must be configured locally with the LSMS OSI-Address information necessary for association establishment. The EOAP will initiate association connections with the LSMS.

Enhancement to GTT Failure Messages (Release 25.0)

Description

This feature enhances the current SEAS REPT-NOTRNS messages to include four optional parameters currently not supported in the EAGLE version of these messages.

- **c4** - "Called Party Global Title Address"
- **d1** - "Calling Party Address Type"
- **d2** - "Calling Party Subsystem Number"
- **d3** - "Calling party Address Point Code"

Effect on Existing UIMs

Implementation of this feature involves a minor change to one of the existing EAGLE UIM formats. To add the CgPA information to the SEAS REPT-NOTRANS message, 6 bytes of the DATA field I16 have been deleted. The format before and after the change is shown below; changes are shown in **bold**.

```
xxxx.xxxx    CARD cccc,p  INFO  'test'
             SIO=xx   OPC=###-###-###  DPC=###-###-###
             CDPA LENGTH=###   MSG TYPE=##
```

```
                CDPA:  AI=xx  PC=###-###-###  SSN=###  TT=###  ADDR=##########
                DATA=xx xx xx xx xx xx xx xx xx xx xx xx
                     xx xx xx xx xx xx
                LSN=[lnkset]
Format with new feature:
    xxxx.xxxx   CARD cccc,p  INFO  'test'
                SIO=xx   OPC=###-###-###  DPC=###-###-###
                CDPA LENGTH=###   MSG TYPE=##
                CDPA:  AI=xx  PC=###-###-###  SSN=###  TT=###  ADDR=##########
                DATA=xx xx xx xx xx xx xx xx xx xx
                    xx xx xx xx xx xx
                LSN=[lnkset]
```

NOTE: The DATA field that is output begins with the CdPA part of the MSU. The CdPA part of the MSU is of variable length, but in most cases is organized as follows:

1st Byte - CdPA Length

2nd Byte - Address Indicator

3rd Byte - SSN

4th Byte - Translation Type

Last 11 Bytes - CdPA Address

The following table lists the UIMs affected by this change, and use UIM format I16.

Table 2-30. Affected EAGLE UIMs

UIM #	Trouble Text
1029	SCCP rcvd inv Cld Party - bad GT ind
1033	SCCP rcvd inv Cld Party - bad network
1034	SCCP rcvd inv Cld Party - no SSN
1042	SCCP rcvd inv GT - bad Translation Type
1043	SCCP did not route - bad translation

Enhancements to GWS Reject Messages (Release 25.0)

Description

This feature enhances the current SEAS REPT-SCRREJ message to include two optional parameters currently not supported in the EAGLE version of these messages. The two optional parameters are:

- **rec** - "Rejection Error Code"
- **z** - "Supplier-Specific Parameter Text"

SEAS Compliance

The following table maps EAGLE rejection reasons to the SEAS rejection error codes.

Table 2-31. EAGLE-to-SEAS GWS Rejection Mapping

EAGLE Gateway Screening Reject Reason (RPT_ MRN_GWS_…)	EAGLE Supplier-Specific Parameter Text in the "z" Field	SEAS Code	SEAS Reject Code Meaning (per GR-778)
OPC_NOT_ALLOWED OPC_BLOCKED	"GWS rcvd OPC that is not allowed" "GWS rcvd OPC that is blocked"	ONNV	OPC not valid
DPC_NOT_ALLOWED DPC_BLOCKED	"GWS rcvd DPC that is not allowed" "GWS rcvd DPC that is blocked"	DNNV	DPC not valid
SIO_FAILED	"GWS rcvd SIO that is not allowed"	SINV	SI not valid
	No EAGLE Equivalent	NINV	NIC not valid
PRIORITY_FAILED	"GWS rcvd a priority that is not allowed"	PRNV	PRI not valid
H0H1_FAILED	"GWS rcvd H0/H1 that is not allowed"	HCNV	H0 or H1 not valid
CLG_FAILED	"GWS rcvd Clg Party that is not allowed"	CGNV	CgPA PC or SSN not valid
	No EAGLE Equivalent	LGNV	CgPA/link set combination not valid
	No EAGLE Equivalent	RINV	CdPA routing indicator not valid
CLD_FAILED	"GWS rcvd Cld Party that is not allowed"	CDNV	CdPA SSN or DPC not valid
DESTFLD_NOT_ALLOWED	"GWS rcvd AFTPC that is not allowed"	DFNV	Affected destination field not valid
SCMG_APC_FAILED	"GWS rcvd SCMG with not allowed AFTPC"	AFNV	Affected PC/SSN not valid
	No EAGLE Equivalent	FINV	SCMG format ID not valid
GT_TYPE_FAILED ALLOWED_ TT_FAILED	"GWS rcvd Translation Type not allowed" "GWS rcvd invalid GTI in TT Screening"	TTNV	TT not valid
	No EAGLE Equivalent	ISNV	ISUP message type not valid
TFC_ APC_FAILED RSP_ APC_FAILED RSR_ APC_FAILED TCA_ APC_FAILED TCP_APC_FAILED TCR_ APC_FAILED TFA_ APC_FAILED TFP_ APC_FAILED TFR_APC_FAILED UPU_ APC_FAILED	"GWS rcvd TFC, AFTPC not in routing tbl" "GWS rcvd RSP, AFTPC not in routing tbl" "GWS rcvd RSR, AFTPC not in routing tbl" "GWS rcvd TCA, AFTPC not in routing tbl" "GWS rcvd TCP, AFTPC not in routing tbl" "GWS rcvd TCR, AFTPC not in routing tbl" "GWS rcvd TFA, AFTPC not in routing tbl" "GWS rcvd TFP, AFTPC not in routing tbl" "GWS rcvd TFR, AFTPC not in routing tbl" "GWS rcvd UPU, AFTPC not in routing tbl"	OTNV	Message rejected for a reason not identified by any of the other "rec" field values.

Enlarged LNP SPID and NPANXX Support (Release 24.0)

The Enlarged LNP SPID and NPANXX Support increases the maximum number of service provider IDs (SPID) and NPANXXs that can be configured in the database.

The maximum number of service provider IDs is increased to 10,000. If you try to enter more than 10,000 service provider IDs with either the **ent-lnp-sp**, **ent-lnp-sub**, or **ent-lnp-lrn** commands, the attempt will be rejected with this message.

Error Messages

```
E3133 - LNP Service Provider Table is full
```

The maximum number of NPANXX entries is increased to 150,000. If you try to enter more than 150,000 NPANXXs with either the **ent-lnp-npanxx**, **ent-split-npa**, **ent-lnp-sub**, or **ent-lnp-lrn** commands, the attempt will be rejected with this message.

```
E3138 - LNP NPANXX Table is full
```

RTRV-LNP-SP Command

The parameters **num**, **force**, and **sp** have been added to the **rtrv-lnp-sp** command to control the number of entries in the service provider ID table that are displayed. Refer to the *Commands Manual* for current usage information.

Entering a Global Title Translation to a Non-Mated Application without Adding the Application as Mated Application (Release 22.0)

In Release 22.0, a global title translation can be entered to a non-mated (solitary) application, either through an EAGLE terminal or the SEAS interface, without requiring the application to be defined by the EAGLE's **ent-map** command.

The **force** parameter (valid values **yes** or **no**) has been added to the EAGLE's **ent-gtt** command that allows the user to override the rules that make sure that the application is defined in the mated application table. The default value for the force parameter is **no** for the EAGLE's **ent-gtt** command. If a global title translation is being added from the SEAS interface, the default value for this parameter is **yes**. When a global title translation is entered on the SEAS interface, the EAGLE does not check to see if the specified application is defined in the mated application table.

If the global title translation is a final global title translation, the application being referenced by the global title translation must be in the mated application entity set. If the global title translation is being entered on an EAGLE terminal with the **ent-gtt** command, the **force=yes** parameter is not specified, and the mated application is defined the mated application table, the command is rejected with the following error messages.

```
E2450 Cmd Rej : PC/SSN does not exist as a mated application
```

```
E2419 Cmd Rej : Point code does not exist in the remote point code table
```

If the **force=yes** parameter is specified with the **ent-gtt** command and the specified application is required to be defined in the mated application table, the following warning messages are displayed.

```
CAUTION - DPC-SSN does not exist in the Mated Application table.

CAUTION - DPC does not exist in the Mated Application table.
```

If the final global title translation is entered on the SEAS interface, the rules checking the mated application table do not apply.

EOAP/OAP Support of HSOP Protocol (Release 28.0)

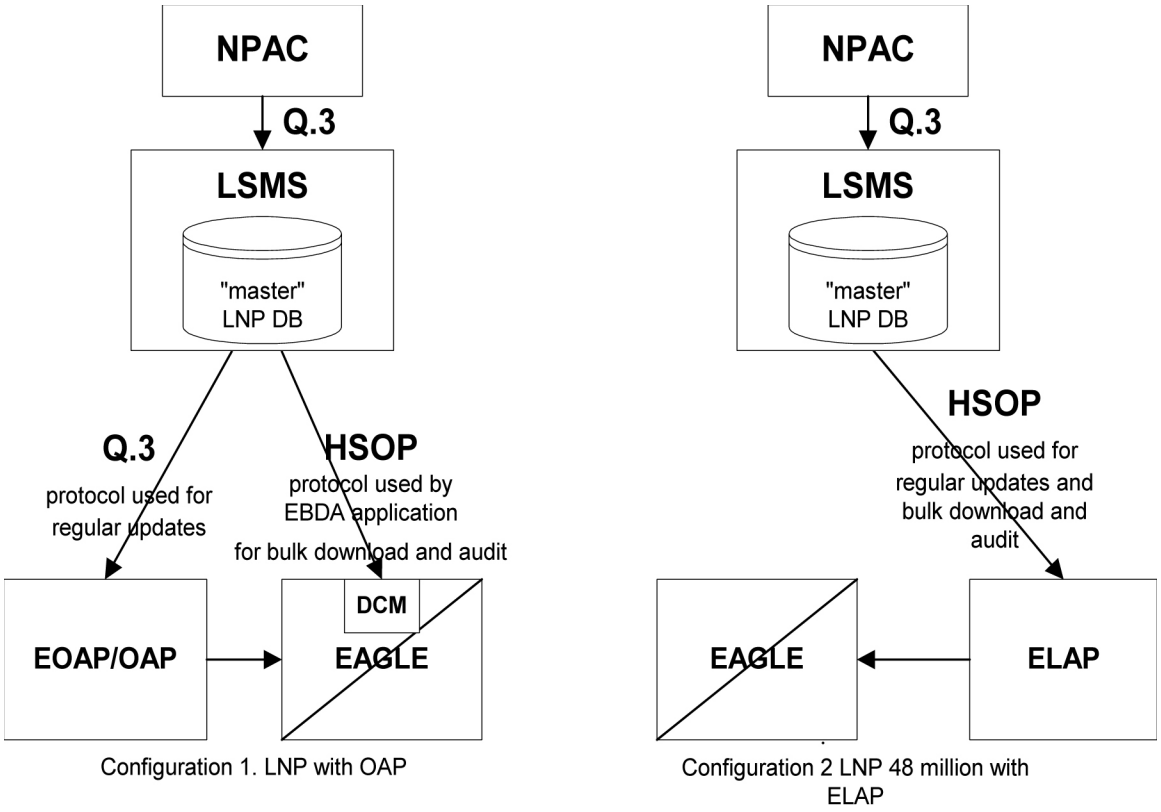
The EOAP/OAP currently supports only the Q.3 interface to the LSMS. The ELAP supports the HSOP interface to the LSMS. From an internal perspective, it is advantageous for the LSMS to support a single interface to the EAGLE, regardless of the architecture deployed. This feature achieves a single interface by requiring the OAP/EOAP to support the HSOP protocol.

HSOP is a fast, reliable protocol developed by Tekelec. LSMS Release 5.0 will support one HSOP protocol to communicate with EAGLE release 28.0 and future EAGLE releases.

LSMS EAGLE Communication Overview

Prior to release 5.0, LSMS supported two different protocols to communicate with pre-28.0 EAGLE releases.

Figure 2-26. LSMS EAGLE Protocol Interface for Pre-5.0 LSMS Releases and pre-28.0 EAGLE Releases



The Q.3 protocol is used by LSMS to communicate with EOAP/OAP. HSOP protocol is used by the EBDA process to send information to DCM cards on EAGLE. Enhanced HSOP protocol is used to communicate with the ELAP when the 48 Million feature is enabled.

EOAP/OAP Overview

EOAP/OAP (OSS Application Processor) was developed to provide telephone company network management systems access to the EAGLE STP. SEAS (Signaling Engineering and Administration System) provides network management functionality. EOAP/OAP interfaces with SEAS using Telcordia standards and licensed code.

EOAP/OAP software consists of few a processes running on the Solaris 2.5.1 UNIX operating system. With the introduction of the LNP (Local Number Portability) feature, EOAP/OAP was extended to provide the communication channel for updates sent from LSMS to EAGLE LNP database using Q.3 protocol.

EOAP/OAP consists of 11 processes. Some processes provide SEAS access to EAGLE; others process LNP database updates sent from LSMS to EAGLE. LNP database updates are sent from LSMS using the Q.3 protocol to the EOAP/OAP emsAgent process.

The purpose of emsAgent process is to translate Common Management Information Protocol (CMIP) messages from the LSMS M-Actions into TL-1 commands that can be interpreted on the EAGLE by the UPL parser.

HSOP replaces the Q.3 protocol, and hsopAgent replaces the emsAgent (see figure). The hsopAgent process translates LSMS HSOP commands to TL-1 commands that can be interpreted on the EAGLE by the UPL parser. The new hsopAgent provides the same interface to the ysTTy process and the ysT1mnt process. It is seamlessly integrated with current EOAP/OAP software; it does not require special configuration to run properly.

New Hardware Required

No new hardware is required for this feature.

EPAP 2.0 Alarm Migration from ELAP (EAGLE 28.0)

This EAGLE 28.0 feature converts EPAP message notification and alarming from the type previously used in EPAP 1.0 to the type used in ELAP 2.0.

As revised, EPAP 2.0 employs different EAGLE UAMs, uses the MPS System Health Check (*syscheck*) utility to diagnose and report MPS/EPAP platform problems, and uses MPS LEDs more completely.

For additional details, refer to the *EPAP Administration Manual* and the *Maintenance Manual*.

EPAP Automated Database Recovery (EPAP 7.0)

Description

The EPAP Automated Database Recovery (ADR) feature is used to restore the EPAP system function and facilitate the reconciliation of PDB data following the failure of the Active PDBA.

The automated recovery mechanism provided by this feature allows 1 PDBA to become Active when 2 PDBAs think they are active and have updates that have not been replicated to the mate PDBA. The software selects the PDBA that received the most recent update from it's mate to become the Active PDBA (the PDBA that was the Standby most recently will become the Active). No automatic reconciliation is performed because the system has insufficient information to ensure that the correct actions are taken.

In order to return the system to normal functionality, a manual PDB copy from the PDBA the software picked to be Active to the PDBA that is in the replication error (ReplErr) state must be performed. However, provisioning can resume until a maintenance period is available to do this.

This feature uses a replication error list that consists of updates that exist as a result of a failure during the database replication process from the active-to-standby PDB. These updates have not been propagated (reconciled) throughout the system and require manual intervention to ensure the EPAP systems properly process the updates.

Limitations

1. The EPAP ADR feature can be turned on or off. The default setting is off.

2. The EPAP ADR feature must be turned on for both MPS-A boxes of an MPS pair.

3. The EPAP ADR feature requires Standby-homing to be active. If Active-homing is being used by the customer, DSM re-boots may be required if they have taken updates from the Active PDB that are different from what has been replicated to the Standby PDB.

4. Each EPAP can support a minimum of two replication error lists.

EPAP Command Response Enhancement (Release 31.6)

This feature provides users of the PDBI with the ability to retrieve information about the status of the DSMs in their network. This information includes, but is not limited to, the database level of each card. The DSM database level is of specific importance because the customer can use it to determine when a specific update has made its way to most or all of the DSM cards.

This new information will be made available to PDBI clients through new asynchronous notifications and synchronous requests/responses. New WebUI screens that utilize the new PDBI messages are also created for displaying the DSM information.

In order to propagate the DSM information up from the DSM to being available through the PDBI, the DSM code as well as several processes in the EPAP are changed.

EPAP PDB-RTDB Level Threshold (Release 31.6)

Currently, the amount of time used to determine if the RTDB is too slow on getting updates (alarm is raised) is configurable using the RTDB->Maintenance->Configure Record Delay menu. uiEdit or the cgi script interface can be used to change this value from the default value of 15 to any value between 1 and 300.

The mate PDBA is configurable via the new menu (PDBA->Maintenance->Configure PDBA Record Delay.) The PDBA threshold may also be changed (by development/cust service only) by using uiEdit to change the value of PDBA_MAX_STANDBY_DELAY - which is defaulted to 300.

EPAP Provisioning Blacklist (EPAP 7.0)

Description

TheEPAP Provisioning Blacklist feature helps prevent provisioning of protected address strings in the EPAP database. Provisioning a protected address string as a DN, DN Block, or IMSI may result in unintended and incorrect routing of messages by the EAGLE 5 ISS DSM. The EPAP Provisioning Blacklist feature allows the user to define a list of address strings that cannot be provisioned as DN, DN Block or IMSI address strings. The addresses of all HLRs must be provisioned in the provisioning blacklist in order for the EPAP Provisioning Blacklist feature to work as intended.

A maximum of 150 blacklist ranges is supported by EPAP. A blacklist range is defined by two address strings. The beginning and ending address strings used to define a blacklist range must be between 5 and 15 HEX digits. In addition, both address strings must be of the same length.

The ending address must be greater than or equal to the beginning address and must not conflict with DN, DN block, or IMSI values in the PDB.

Limitations

The EPAP Provisioning Blacklist feature has the following limitations:

- The blacklist ranges are stored in the PDB database. Since modification of blacklist data is not supported via the PDBI (Provisioning Database Interface), support of PDBI export and import is not possible. In addition, modification of existing blacklist data is not supported.
- If the blacklist does not include all protected address strings in a customer network, and one of the protected address strings is provisioned as a DN, DN Block, or IMSI, unintended message routing occurs, and may cause network outages.

EPAP RTDB Level Auto Refresh (Release 31.6)

This feature provides a configurable auto refresh rate for the viewPDBAStatus.cgi and viewRtdbStatus.cgi screens. Users are able to halt the refreshing without losing the information displayed on the screen at the time (for debugging or capturing data).

A new field is added to the Modify Defaults screen that takes a value of 0 or 5-600 seconds. This determines if (0 means no refreshing) the PDBA and RTDB View Status pages are refreshed and how often. On the screen, this value can be modified, but reloading the screen using the left-most menu links causes the system default to be changed. The system default applies to both screens.

EPAP Security Enhancements (Release 29.0)

Description

The EPAP Security Enhancements feature implements a database table of IP addresses that can be added to, deleted from, and retrieved by an authorized user.

The Admin user or user possessing IP action privileges can at any time add, delete, and retrieve IP addresses. Deletion of an IP would cause that IP address to no longer reside in the IP table, and therefore would no longer be able to connect to the EPAP 3.0 GUI. While each of the IP action privileges can be assigned individually to a user, the IP action privileges of add and delete should only be granted to those users with knowledge of the customer network.

The functionality for addition, deletion, retrieval of client IP addresses, and toggling of IP authorization checking are individually assignable and accessible only through the EPAP 3.0 GUI. The IP mechanism implemented in this feature will provide a foundation for further enhancements in privilege control.

The new IP actions of add, delete, retrieval, and toggling of IP authorization checking are available only through the EPAP 3.0 GUI, and added initially to the Admin group only. The privilege of viewing IP addresses on the customer's network should be a security consideration made only by a user with Admin Group privilege. Privileged users can add a custom message in place of the standard 403 Forbidden site error.

NOTE: The IP actions of this function that allow for adding, deleting, retrieving authorized IP Addresses, and the toggling of authorized IP checking are NOT accessible from the EPAP 3.0 text-based UI. They are accessible from the EPAP 3.0 GUI only. No IP addresses are restricted from accessing the EPAP 3.0 GUI until the Admin user toggles IP authorization to enabled. When IP authorization checking is enabled, all IP addresses not present in the IP authorization list will be refused access to the EPAP 3.0 GUI.

Hardware Requirements

No new hardware is needed to support this feature.

Upgrade Considerations

This feature will impact the EPAP 1.x/2.x to 3.0 upgrade.

Limitations

IP access and range constraints provided by web server and EPAP 3.0 IP address checking functionality will not protect against IP spoofing . The customer must rely on the security of the customer intranet network to protect against spoofing.

EPAP Support for HTTPS on GUI (EPAP 9.0)

Description

The EPAP Support for HTTPS on GUI feature allows users to configure whether the GUI can be accessed only by standard HTTP (Hypertext Transfer Protocol) or only by HTTPS (Secure Hypertext Transfer Protocol) or by both.

In previous releases of EPAP, the EPAP GUI used only standard HTTP protocol. The data transfer between the web server and the GUI is not encrypted with standard HTTP protocol; therefore, it can be captured by any network analyzer and viewed. Secure HTTP (HTTPS) supports encryption of data exchanged between the web server and the browser. This facilitates data privacy.

With the addition of this feature, the EPAP now allows the user to configure the use of either HTTP or HTTPS, or both, for the EPAP GUI. The user can disable HTTP. The ability to configure HTTP and HTTPS and the ability to disable HTTP can be limited to a specific user class or group.

When the HTTPS interface is used for the first time, the security certificate needs to be imported to the client machine. For information about importing the secure certificate, refer to the *EPAP Administration Manual*.

Hardware Requirements

None.

Limitations

None.

EPAP Support for SSH on PDBI (EPAP 9.0)

Description

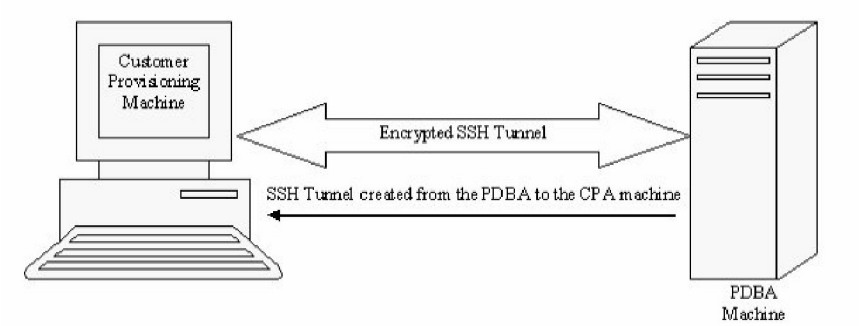
The EPAP Support for SSH on PDBI feature provides support for Secure Shell (SSH) on the EPAP Provisioning Database Interface (PDBI) for customers who want additional security protection.

SSH is a robust, commercial-grade, and full-featured toolkit that implements security and network encryption.

In previous EPAP releases, the customer provisioning application (CPA) connected to the EPAP only through a non-secure TCP/ IP connection. Provisioning sent by the CPA was non-secure, because the data was not encrypted and could be seen by packet sniffers in the network.

To make the data transfer between the CPA and the PDBA (Provisioning Database Application) machine secure, SSH tunneling (also called remote port forwarding) is used to securely connect the PDBA machine to the CPA machine.

Figure 2-27. SSH Tunnel Between the CPA and PDBA Machines



Remote Port Forwarding

Remote Port Forwarding refers to the SSH tunneling approach where the SSH tunnel is created from the client side of the tunnel towards the server side. In the EPAP implementation, the CPA machine is the server and the PDBA machine is the client.

The PDBA machine user specifies a particular port number (configurable from GUI) to be opened on the CPA machine. Any data received on this port on the CPA machine is forwarded to the PDBA machine's IP address and the port number, 5873, through the secured SSH tunnel.

NOTE: To implement Remote Port Forwarding to work, the CPA machine must have the OpenSSH suite installed and the SSH daemon must be running.

Request/Response Cycle in SSH Tunnel

When an SSH tunnel is in use, a complete request and response cycle takes place as follows:

1. When an SSH tunnel is in use, a complete request and response cycle takes place as follows:
2. The CPA sends a connect request to its local port number used for creating the tunnel.
3. The SSH encrypts the request message and sends it to the PDBA machine's SSH client port.
4. On the PDBA machine, the SSH client decrypts the message and forwards it to the PDBA port.
5. The SSH client encrypts the response message and sends it to the SSH port on the CPA machine.
6. On the CPA machine, the SSH daemon decrypts the message and forwards it to the CPA. The CPA receives the message unencrypted.

Hardware Requirements

None.

Limitations

This SSH tunneling feature works only for customer provisioning systems with 'Write' permissions. A system with 'Read' permissions is not allowed to use the SSH tunnel with the PDBA machine.

EPAP Support of EAGLE's ITU Duplicate Point Code (Release 29.0)

Description

The EAGLE's Duplicate Point Code feature allows point codes to be provisioned in the EAGLE using a two character "group code." For example, a point code of 1-1-1 could be provisioned 1-1-1-ab, where 1-1-1 is the true point code and ab is the group code. This allows the EAGLE to route between two nodes that have the same true point code. The EAGLE distinguishes between the two by the group code. The group code is only used internally to the EAGLE, and is assigned to an incoming message based on the linkset on which it was received.

Currently, the PDBI (Provisioning Database Interface) does not support entering point code with a group code. This presents a problem for some customers running the DPC feature and either G-Flex, G-Port, or INP.

The EPAP Support of EAGLE’s ITU Duplicate Point Code feature allows group codes to be entered for Network Entity (i.e. SP or RN) point codes via the PDBI.

The following components are affected by this feature:

1. Provisioning Database Interface. Messages related to Network Entity update, create and retrieve will have new optional name value pair called gc for group code.
2. Provisioning Database. EPAP database schema will change. New element gc for group code will be added
3. Provisioning Database Application. Parsing routines will change to accommodate group code.
4. PDBA-RTDB interface will change to accommodate new group code parameter.
5. Real Time Database. Parsing and storing of new data
6. EPAP User Interface PDB Network Entity screens will add new group code field.
7. EPAP 1.0/2.0 to 3.0 data base migration

Hardware Requirements

No new hardware is needed to support this feature.

Upgrade Considerations

Seamless database upgrade (Versant utility sch2db) path from EPAP 2.0 to 3.0 will be used if possible; otherwise, database migration procedure shall be provided. Migration procedure will not take more than 10 minutes with maximum of 50K entries in Network Entity class.

Limitations

This feature extends, and is dependent upon, EAGLE's ITU DPC feature.

EPAP Update Validation (EPAP 7.0)

Description

The EPAP Update Validation feature provides additional data checks (checksums) before applying updates from the EPAP RTDB to the DSM RTDB.

These additional checks are designed to prevent overwriting of existing data records with new data records when operators are provisioning new subscribers.

When update validation is triggered, the DSM card goes DB-DIFF not incoherent. DB-DIFF requires a reload of the DSM card. However, the DSM card will continue to process traffic until it is reloaded.

A checksum of the data about to be overwritten is compared with the old checksum (new data element) in the update about to be applied as well as the existing memory location check. If the checksums and location do not match, the update will not be applied to the DSM RTDB and the DSM will go incoherent.

To use this feature, the EAGLE 5 ISS will first need to be upgraded to Release 34.0.4. The DSM cards will continue to accept and process update records from the EPAP that do not contain the update validation information. After the EAGLE 5 ISS is upgraded, the respective EPAP is upgraded to provide the update validation information. The

DSM cards will provide information to the EPAP that details whether or not it can accept and process update validation information (based on the EAGLE 5 ISS software level) from the EPAP.

EPAP with TPD 1.1 (Release 31.6)

MPS now uses Tekelec Platform Distribution (TPD) Release 1.1, which offers the following improvements over TPD Release 1.0:

- An additional diagnostic service, **`smartd`**, has been added. The **`smartd`** service reads status information from the disk (produced according to the S.M.A.R.T. standard) and reports that status through the **`syscheck`** utility. The standard S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) technology is implemented into all modern hard disks. According to this standard, a special program inside the disk constantly tracks the condition of a number of the vital parameters, such as driver, disk heads, surface state, electronics, etc. At the present time, S.M.A.R.T. technology is able to predict up to 70% of all hard disk problems.

- Various changes that make the platform easier for the EPAP application to use (these changes do not result in changes that are noticeable by the user).

EPAP/ELAP 2.0 Security and UI Enhancements (Release 28.0)

Description

This feature allows the customer to access ELAP and EPAP functionality from any computer workstation capable of supporting an Intranet connection and Microsoft's Internet Explorer 4 browser. This feature does not change major ELAP/EPAP functionality. It does, however, provide Client/Server architecture and a new menu interface to that functionality.

This feature provides a new user interface and presents no impact to the EAGLE. The old text-based UI is available for provisioning purposes.

For more information on the EPAP/ELAP Security and UI Enhancements, refer to the *EPAP Administration Manual* or the *ELAP Administration Manual*, and the *Maintenance Manual*.

Hardware Requirements

Customers need a PC that can connect to the LAN/WAN.

EPAP Provisioning Performance Enhancements (Release 29.0)

Description

The Enhanced EPAP Provisioning Performance feature replaces FTS with an asynchronous replication scheme. FTS (Fault Tolerant Server) is a protocol used by Versant to achieve data synchronous replication.

EPAP 1.0 and 2.0 provided support for MPS provisioning databases spanning two sites, with each site hosting a database whose data is replicated synchronously to the other via FTS. To ensure synchronous replication of data, this transfer protocol requires that 8 messages be exchanged per update.

Messaging and data exchange must take place over potentially slow customer network. When the customer network is slow (that is, there exists a network latency issue between the two customer sites containing PDBs, such that the round trip delay between sites exceeds 4-5 ms.), the messaging overhead can cause provisioning rates to drop to unacceptable levels.

Asynchronous replication means that the database receiving an update, in this case the Active PDB, can commit and send the client a success or failure code prior to sending the update to the replicated database, in this case the Standby PDB. Note that only successful updates are replicated. Response turnaround on the Active PDB is thus shortened, and the overhead involved in keeping the databases in sync is spared.

With this feature, the round trip time between nodes may be up to 100 ms. without encountering active/standby lag problems.

Single Transaction Mode PDBI Connection

In EPAP 1.0 and 2.0, all PDBI provisioning commands had to be encapsulated in 'begin' and 'end' transaction statements. Many customers, however, wanted only to send one update per transaction. In such a case, the overhead involved in sending transaction boundary tags can become considerable.

In EPAP 3.0, a new PDBI connection type called 'single transaction mode' is provided. When using this connection type, PDBI clients are allowed to send updates outside of 'begin' and 'end' transaction delimiters. The PDB treats each update as being its own transaction. However, transaction delimiters are not ignored in 'single mode'. If the PDBI client issues these delimiters, the series of updates encapsulated by them will be treated as one transaction, as they always have been under the default PDBI connection mode.

Hardware Requirements

No new hardware is required or introduced to support the software.

Enhancements to the User Interface

A new state has been added to the set of PDBA states displayed by the Web UI Banner. This state, entitled "REPLERR," denotes the presence of alarm MAINT_ALARM_ PDBA_REPL_FAILED. REPLERR may also appear on the View PDBA Status page, and the View RTDB Status page.

Upgrade Considerations

During upgrade, the Versant replica file, if present on the MPS, will be moved to a different location so that FTS will not be active in EPAP 3.0. Upon removal of the EPAP 3.0 application package, this file will be set back in its original location, so that the system may resume use of FTS following a backout. If updates have been made

to the PDB following upgrade, however, backout will entail full PDB restoration. Otherwise, this feature will not affect the EAGLE 28.x/EPAP 2.x to EAGLE 30.0/EPAP 3.0 upgrade.

Limitations

These enhancements introduce an important change to the behavior of EPAP. PDBA switchover can no longer be forced while the PDBAs are able to communicate and the Standby is behind. Switchover now entails allowing some definable amount of time for the Standby PDB to be brought up to the level of the Active PDB. If it fails to obtain equal database level in the allotted time, switchover will not occur, and it will return with the number of levels still left to be replicated. This is a safeguard designed to prevent database inconsistency. However, if the Standby PDB cannot reach the Active PDB to determine its level, then the EPAP will allow PDBA switchover to be forced.

Equipment Identity Register (EIR) (Release 31.0)

This feature is intended to reduce the number of GSM mobile handset thefts by providing a mechanism that allows the network operators to prevent stolen or disallowed handsets from accessing the network. This control is done by using the International Mobile Equipment Identity (IMEI) provided during handset registration and comparing it against a set of lists provided by the network operator. There are three lists: Black, Gray and White. Mobile Stations (MS) on the white list are allowed access to the network. MSs on the black list are denied access to the network. MS's on the gray list are allowed on the network, but are logged.

This feature meets the mandate of European countries to provide EIR functionality by providing the network operators the ability to prevent stolen handsets from accessing their networks.

Error Message Reporting Enhancement (Release 21.0)

Before Release 21.0, the global title and gateway screening functions display a single error (unsolicited alarm message - UAM). This does not show all of the global title and gateway screening error messages that occur.

This feature allows more information about global title and gateway screening error messages to be reported to the user.

The number of global title error messages and gateway screening error messages displayed is increased to 5 messages/second/card. Each card can report up to 8 messages per second to the system. Any global title error messages and gateway screening error messages generated beyond the 8 messages/second/card rate are discarded, with the newest messages discarded first. Low priority messages are discarded when the transport buffer is full (8 total messages). High priority messages are discarded when the transport buffer is completely full with high priority messages.

Ethernet B Interface for IPGWx and IPLIMx (Release 28.1, IP^7 Release 6.0)

Description

This feature activates the second Ethernet Interface (the B Interface) on the SSEDCM card types. This allows IP connection-oriented transports, such as TALI sockets and IETF SCTP associations, to utilize either of the card's

Ethernet A or B Interfaces when forming a connection. This feature provides direct access to two separate LANs, effectively doubling the connectivity of each SSEDCM card.

As part of this feature's implementation, multiple static IP routes are permitted for SSEDCM card types. Each unique static route can be configured to use a different gateway router to reach remote destinations. This provides the capability to utilize more network paths for IP connection-oriented transports to access remote IP networks.

The addition of Static IP Routes enables IP connection-oriented transports to be accessible through gateways other than the default router. By providing access to a greater number of IP gateways, more destinations can be reached in a more efficient manner. Also, more time efficient IP connections can be utilized.

Doubling the connectivity to local networks and providing a more diversified access to remote networks greatly increases the flexibility of the IP7 Secure Gateway and EAGLE STP. Enabling each SSEDCM card to directly access two Local Area Networks allows the arrangement of co-located IP7 SG's/EAGLEs in ways to provide a higher level of redundancy.

Allowing the SSEDCM to be used as a multi-homing host also allows the SCTP protocol to utilize the protocol's multi-homing capability and provide support for local association endpoints that are multi-homed. SCTP multi-homed endpoints are endpoints that may use both Ethernet interface A and B for SCTP connectivity. This SCTP protocol capability provides for SCTP connections to be established that are more reliable and robust than TCP socket connections.

Hardware Requirements

This feature is intended for SSEDCM cards. The assignment of IP7 connection-oriented transports to the Ethernet B Interface on DCM cards is not permitted.

Limitations

Limitations for the Ethernet B Interface for IPGWx / IPLIMx feature are listed below.

- Only one default router can be assigned per card.
- SSEDCM cards will act as follows:
  - — uni-homing on the Ethernet A interface,
  - — uni-homing on the Ethernet B interface, and
  - — multi-homing on the Ethernet A and B interfaces.
- A finite number of static IP routes per card exists; the limit is 50 per card per EAGLE.
- There are per card and per system limits on the maximum number of static IP routes supported.
  - — a maximum of 64 static IP routes per IPGWx / IPLIMx card, and
  - — a maximum of 1024 static IP routes per system.
- No additional database validations will be performed on upgrade.

- No increased in load performance is provided.
- Static IP routes can lead to unreachable hosts.

Expanded Terminal Output Groups (Release 31.3)

The output groups currently defined by the EAGLE allow the messages generated by the system to be selectively displayed on the various terminals connected to the EAGLE. The expansion adds 12 new output groups and reassigns messages from existing groups to be used exclusively for controlling the output destination of all UAMs and UIMs. Upgrade automatically assigns messages to the correct groups.

The upgrade will automatically change existing groups to the new groups and additional output may be seen post upgrade depending on which groups are activated.

Extended Bus Interface (Release 20.0)

Every two card locations, except for card locations 9 and 10 in all shelves, and 17 and 18 in the control shelf (1117 and 1118), are connected together through the shelf backplane by an extended bus interface (EBI). The EBI is a local bus and not connected to the IMT bus. This allows every two card locations to communicate with each other without going over the IMT bus. The MCAP card and the TDM are connected to each other through the EBI to form the MASP. This also eliminates the 10 Mb/s ethernet LANs with their outboard MAU units that connected the MCMs and PSMs in the EAGLE STP/1 MAS.

Extension Shelf Backplane (Release 23.0)

A new extension shelf backplane has been introduced in Release 23.0 with these changes:

- The extension shelf backplane now contains four -48VDC power and ground connections (DB-26 connectors). Two of these connectors are labeled A1 and B1 and are connected to the fuse and alarm panel. The other two are labeled A2 and B2 and are connected to another power source, allowing the EAGLE to remain in service when replacing the fuse and alarm panel.
- The shelf address of the extension shelves has been expanded from four bits to six bits, increasing the number of addressable extension shelves from 15 to 64 and increasing the maximum number of addressable card slots from 250, or 500 signaling links, to a theoretical limit of 1018, or 2036 signaling links. The actual number of addressable card slots is limited by the system software and the hardware configuration of the EAGLE. In Release 23.0, the actual number of addressable card slots is 378, or 756 signaling links, but is limited by the system software to 250 cards, or 500 signaling links.
- To enable the cards in the extension shelf to select one of two different types of IPMX cards that could be in the extension shelf, pin D53 of connector P9 transmits signal ABMUXIN- to pin D26 on connectors P1 to P8 and P10 to P17, and pin D53 of connector P26 transmits signal BBMUXIN- to pin D27 on connectors P18 to P25 and P27 to P34.

3

Features F - K

False Link Congestion Management (Release 21.0)

It's possible that a problem on a signaling link can cause that signaling link to go into congestion, even though the traffic on the linkset is not high enough to cause congestion. For example, if a signaling link has a large number of retransmissions, the throughput of the signaling link could drop enough to cause congestion on that signaling link. To help prevent this from happening, the EAGLE starts the level 3 T31 timer whenever a signaling link goes into congestion. If the signaling link remains in the same congestion state until the level 3 T31 timer expires, the signaling link is removed from service. The signaling link becomes unaligned, and the alignment procedure is started.

The congestion level that starts the level 3 T31 timer can be set to either congestion level 1 or congestion level 2 using the **chg-stpopts** command with the **mtpt31ctl** parameter. This congestion level can be verified with the **rtrv-stpopts** command and is shown in the MTPT31CTL field. The level 3 T31 timer is started when the signaling link reaches this congestion level or a higher level. An increase in congestion level or abatement to a lower congestion level restarts the timer. When the congestion level goes below the congestion level configured in the **chg-stpopts** command, the level 3 T31 timer is stopped. If the level 3 T31 timer expires and the signaling link's congestion level has not changed, the signaling link is restarted.

For example, if the level 3 T31 timer is set at 60 seconds and a signaling link goes into congestion level 1, the level 3 T31 timer is started. If, after 45 seconds, the signaling link's congestion increases to level 2, the timer is restarted to 60 seconds. If the signaling link remains at congestion level 2 for 60 seconds, the signaling link is taken out of service and it becomes unaligned. Then the alignment procedure is started, and the EAGLE attempts to realign the signaling link. The level 3 T31 timer can only be assigned to ANSI SS7 linksets and signaling links.

Feature Control Mechanism (IP^7 Release 3.0)

Feature Control provides a mechanism for restricting and monitoring controlled features.

DCM throughput is the only controlled feature for release 3.0. The default rate of transactions per second (TPS) on the system for release 3.0 is 200. As a customer's network needs exceed this threshold, ever higher TPS rates can be purchased and enabled in increments of 200 up to a TPS rate of 6000 (raw capicity).

Note that this feature is available only on DCMs running IPGWx GPLs.

File Transfer Utility (Release 20.0)

This feature provides the capability to upload generic updates and changes to the EAGLE via a data communications link. This is an objective stated in Bellcore's TR-NWT-000082, Issue 4, December 1992 publication.

The data communications link is accessed through a dial up modem using one of the EAGLE's RS-232 serial I/O ports. This data link is a secured link with password protection. The capability is also provided to download data or a generic program loads from the EAGLE to a remote site, allowing operators to gather traffic measurement data in bulk or raw form. Tekelec's Technical Services department may also use this capability when troubleshooting site problems.

Flash Memory Management (Release 23.0)

This feature gives the user the ability to update the image of the PROM on the LIMATM, P/N 870-1293-xx, without physically replacing the PROM. The image of the PROM is shown in the EAGLE as a GPL, the BPHCAP GPL.

The LIMATM contains a PROM that can be written to by the system software. In previous releases, cards had to be removed from the EAGLE and the PROM physically removed from the cards to update the image of the PROM. With this feature, the LIMATM does not have to be removed from the EAGLE to update the image of the PROM. Other cards in the system must still be removed from the EAGLE to update the image of the PROM.

The BPHCAP GPL contains software used by the application processor and the IMT processor of the LIMATM. Because the BPHCAP GPL contains software for the IMT processor, the IMT Software Download feature, introduced in Release 21.1, is prevented from downloading the IMT GPL to the LIMATM. The system software detects the presence of the LIMATM, and the IMT download is prevented.

The process of loading the BPHCAP GPL on the EAGLE is different from the loading of other GPLs.

1. To bring the BPHCAP GPL onto the EAGLE, insert the removable cartridge into the removable cartridge drive on the MDAL then copy the BPHCAP GPL from the removable cartridge to the fixed disk with the **chg-gpl** command.

2. Place the card that the BPHCAP GPL is being loaded onto out of service using the **rmv-card** command.

3. Start the BPHCAP GPL change by entering the **init-flash** command with the **code=trial** parameter. This loads the trial version of the BPHCAP GPL onto the specified card. When this command is successful, the card reboots and two minor alarms are generated. One alarm shows that the card is running an unapproved GPL, UAM 0002, and the other shows that the card is running an unactivated BPHCAP GPL, UAM 0004.

4. Place the card back into service with the **rst-card** command.

5. Activate the BPHCAP GPL on the card with the **act-flash** command. UAM 0004 is cleared. UAM 0002 is not cleared until all LIM-ATMs have been updated with the new BPHCAP GPL.

6. Repeat Steps 2 through 5 for other LIMATMs in the EAGLE.

7. Make the trial version of the BPHCAP GPL the approved version with the **act-gpl** command.

Flexible GTT Load-Sharing (Release 35.0)

Description

The Flexible GTT Load Sharing feature allows a PC or PC/SSN combination to be provisioned in multiple load-sharing relationships for post-GTT load sharing of intermediate and final GTT traffic.

Load sharing for intermediate GTT traffic requires the Intermediate GTT Load Sharing feature, which can run in conjunction with the Flexible GTT Load Sharing feature. Intermediate GTT load sharing is performed through the EAGLE 5 ISS MRN table, and the GTT destination is a PC. If both the Intermediate GTT Load Sharing and the Flexible GTT Load Sharing features are on, different load-sharing relationships can be defined between the same set of PCs, and different sets of destinations can contain the same PCs.

The Flexible GTT Load Sharing feature allows a PC to be part of more than one load-sharing group, with each PC defined by a different MRN set. An MRN set consists of a logical grouping of PCs that has been provisioned in the MRN table. An MRN set either has an ID consisting of a specific number or is used as the default MRN set, which contains multiple logical PC groups.

When the Intermediate GTT Load Sharing feature is enabled, all existing entries in the MRN table and all existing GTA translations in the GTT table with RI=GT are stored in default MRN sets. A user can provision additional MRN sets and associate GTT entries to the MRN sets.

Although the Flexible GTT Load Sharing feature allows a PC to be part of multiple MRN sets, there cannot be multiple instances of a single PC within he same MRN set or within the default MRN set.

Load sharing for final GTT traffic is performed through the EAGLE 5 ISS MAP table, and the GTT destination is a PC/SSN combination. If the Flexible GTT Load Sharing feature is on, different load-sharing relationships can be defined between the same set of PC/SSNs, and different sets of destinations can contain the same PC/SSN combinations.

Although the Flexible GTT Load Sharing feature allows a PC/SSN combination to be part of multiple MAP sets, there cannot be multiple instances of a single combination within the same MAP set or within the default MAP set.

Hardware Requirements

The Flexible GTT Load Sharing feature has the following hardware requirements:

- The SCCP application must run on a DSM card or higher.
- No SCCP application can be provisioned in the system if TSM cards are used.

Limitations

The Flexible GTT Load Sharing feature has the following limitations:

- MPS-based features cannot use the Flexible GTT Load Sharing feature.
- The **ent/chg-gtt/gta** commands do not support auto-creation of MAP entries.
- If the Flexible GTT Load Sharing, Intermediate GTT Load Sharing, and SCCP Service Reroute Capability features are enabled, the number of entries that can be provisioned in the MRN table is reduced by the number of entries in the SCCP-SERV table. If the Flexible GTT Load Sharing and Intermediate GTT Load Sharing features are enabled, the maximum number of entries that can be provisioned in the MRN table is 6000. If

the Service Reroute Capability feature is also enabled, the maximum number of entries that can be provisioned in the MRN table is 6000 - the number of entries in the SCCP-SERV table.

Flexible Intermediate GTT Load-Sharing (Release 34.2)

Description

The Flexible Intermediate Global Title Translation (GTT) Load-Sharing feature enables the user to define multiple relationships among groups of destination point codes in the Mated Relay Node (MRN) table. The relationship that is used in a particular translation is based on the Global Title Address digits used for translation.

When the Flexible Intermediate GTT Load-Sharing feature is turned on, it introduces the MRN Set ID into the MRN table, which localizes the scope of a point code to a group. An MRN Set ID uniquely identifies each such group. A point code can now exist in multiple such groups, but is expected to be unique within a group. The feature also introduces MRN Set ID as a result of a Global Title (GT) translation. Following GT translation, the MRN Set ID and the post-translation point code are used as an entry point into the MRN table. The PC and its group of alternate point codes, all of which have same MRN Set ID, will be accessed together along with their respective relative cost (RC) to identify the most cost effective way of load-sharing.

The MRN table contains point codes that are associated in groups with the same MRN Set ID. The groups provide alternate routing options in the event that the desired point code becomes unavailable.

The Flexible Intermediate GTT Load-Sharing feature provides a more flexible way of assigning Load-Sharing rules amongst Global Title Addresses (GTAs). For example, in the following figure,

GTA=9194605500 could translate to PC=1-1-1 and have a load-sharing relationship with PC=2-2-2.

GTA=9194611000 could also translate to PC=1-1-1, but not have a load-sharing relationship with any other PC.

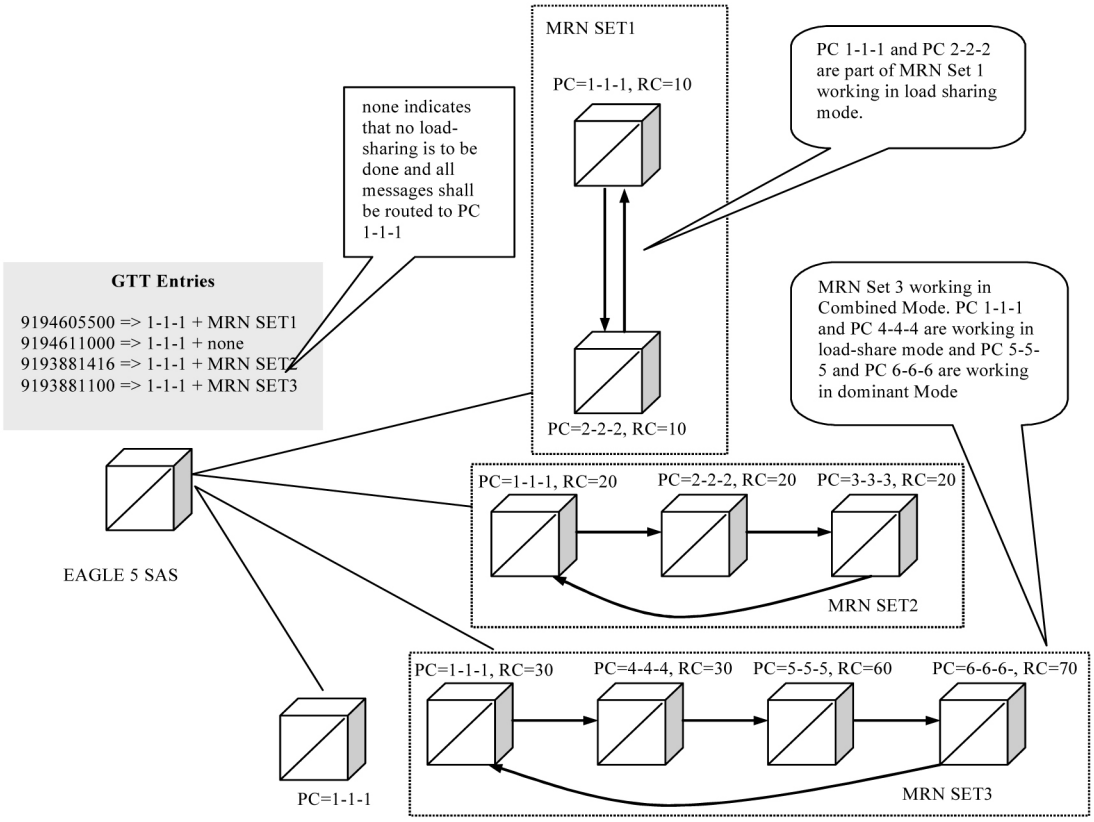
GTA=9193881416 could also translate to PC=1-1-1, and have a load-sharing relationship with PC=2-2-2 and PC=3-3-3.

In the scenario depicted in the following figure, the Flexible Intermediate GTT Load-Sharing feature routes the post-GTT traffic as follows:

- GTA=9194605500 is divided equally between PCs 1-1-1 and 2-2-2,
- GTA=9194611000 is always sent to PC 1-1-1, and
- GTA=9193881416 is divided equally between PCs 1-1-1, 2-2-2, and 3-3-3.

GTA entry 9193881100 would also translate to PC 1-1-1, but PC 1-1-1, PC 4-4-4, PC 5-5-5 and PC 6-6-6 are working in combined mode i.e. PC 1-1-1 and PC 4-4-4 are working in load share mode and PC 5-5-5 and PC 6-6-6 are in dominant mode. Therefore post-GTT traffic for GTA entry 9193881100 is equally divided between PC 1-1-1 and PC 4-4-4.

Figure 3-1. Organization of PCs in Flexible Intermediate GTT Load-Sharing Feature



Flexible Intermediate GTT Load-Sharing provides the ability to load share between multiple nodes after GT translations when the outgoing (post GTT) message is route-on-GT. The resulting PC value of GTT is looked up in the MRN table. If the translated PC is not found in the MRN table, the message is routed as per existing EAGLE 5 SAS functionality.

The destination point code stored in the MSU will be changed when a load-sharing PC is selected.

The Flexible Intermediate GTT Load-Sharing feature provides the ability to define multiple load-sharing groups in the MRN table where a PC can be shared among different load-sharing sets.

Default MRN Set

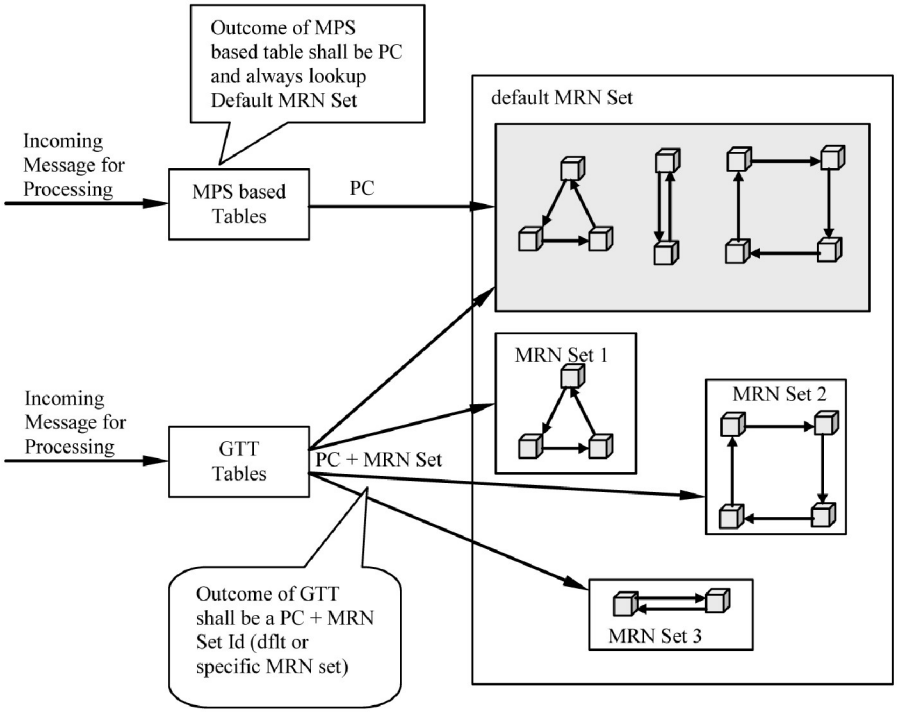
Once the Flexible Intermediate GTT Load-Sharing feature is enabled, any existing entries in the MRN Table become part of a **default MRN Set** . In addition, all existing GTA translations in the GTT Table that have a routing indicator (ri) equal to GT are assigned a default MRN Set.

Flexible Intermediate GTT Load-Sharing provides flexible load-sharing for translations defined in GTT Tables but not MPS-based tables. Since MPS-based features do not support an MRN Set Id, to be able to take advantage of the Flexible GTT Load-Sharing functionality, MPS-based features need to be modified. Until all MPS-based features are converted and able to use Flexible GTT Load-Sharing, a default MRN Set is used to provide the necessary support.

The default MRN Set consists of multiple load sharing groups of PCs that allow both GTT features and MPS-based features to run in parallel. MPS-based features are limited to using ONLY the default MRN Set. GTT features can be provisioned to use the default MRN Set as well. To operate on entries in the default MRN Set, the user must specify default as the value of the MRN Set in the GTA translation.

The default MRN Set consists of multiple load-sharing groups of PCs as shown in the following figure.

Figure 3-2. Concept of Default MRN Set



None MRN Set

As mentioned earlier, once the Flexible Intermediate GTT Load-Sharing feature is enabled, any existing entries in the MRN Table become part of a default MRN Set. All existing GTA translations in the GTT Table that have a routing indicator equal to GT (**ri**= **gt**) are assigned a default MRN Set. This assignment to a default MRN Set in the GTA translation is irrespective to whether the translated PC exists in any MRN Set. If no load sharing is desired, the user must manually change the GTA translation to MRN Set equal to None. (**mrnset=none**).

Load-Sharing Modes

There are three possible load-sharing modes in an MRN Set.

- Dominant
- Load-Share
- Combined Dominant/Load-Share

The mode that gets applied to an MRN Load-Sharing Set is determined by the relative cost of the PCs.

Dominant Mode

An MRN Load-Sharing Set is in Dominant Mode if each PC in the group has a unique relative cost as shown in the following table. The PC selected first (preferred) is the PC with the lowest cost that is available. If the preferred PC is not available, then the PC with the next lowest relative cost that is available is selected

Table 3-1. MRN Table (MRN Set in Dominant Mode)

MRN Set ID	PC	Relative Cost	Next Alternate Point Code
1	1-1-3	15	1-1-1
1	1-1-1	20	1-1-2
1	1-1-2	30	1-1-3

.

Global Title to the Lowest Cost PC

If an MSU comes in with TT =10, GTA= 9194605212, then as shown in the following table:

- If PC 1-1-3 is available, the MSU is routed to 1-1-3, which is the preferred PC.
- If PC 1-1-3 is not available but PC 1-1-1 is available, the MSU is routed to PC 1-1-1, which is the next preferred PC.
- If PC 1-1-3 and PC 1-1-1 are not available but PC 1-1-2 is available, the MSU is routed to PC 1-1-2, which is next preferred PC.
- If all PCs are unavailable in the MRN set, the message are dropped

Table 3-2. GT Translation Table

Translation Type	GTA	PC	MRN Set Id
10	9194605000 to 9194605499	1-1-3	1
10	9194605500 to 9194605599	1-1-1	1
10	9194605600 to 9194605799	1-1-3	2
10	9194605800 to 9194606000	1-1-1	3

.

Global Title to a Higher Cost PC

It is possible that the result of a GT translation is not the same as the lowest cost PC. This PC is still the preferred PC and will be selected if it is available. If the preferred PC is not available then, the available PC in the list of alternate PCs with the next higher relative cost is selected for routing.

If an MSU comes in with TT=10, GTA=9194605555 then as shown in the following table:

- If PC 1-1-1 is available, the MSU is routed to PC 1-1-1, which is the preferred PC for this translation.

- If PC 1-1-1 is unavailable but 1-1-2 is available, the MSU is routed to PC 1-1-2, which is the next preferred PC.
- If PCs 1-1-1 and 1-1-2 are not available but PC 1-1-3 is available, the MSU is routed to PC 1-1-3, which is the next preferred PC.
- If none of the PCs are available, the message is dropped.

Load-Share Mode

An MRN Load-Sharing Set is in Load-Share Mode if each PC in the group has the same relative cost. The EAGLE 5 ISS evenly distributes the translated MSUs to each of the PCs listed in the following table.

- If one or more of the PCs are not available, the EAGLE 5 ISS evenly distributes the MSUs to the remaining PCs in the group that are available.
- If none of the PCs in the group are available, the message is dropped

Table 3-3. MRN Table (MRN Set in Load-Share Mode)

MRN Set ID	PC	Relative Cost	Next Alternate Point Code
2	1-1-3	10	2-2-1
2	2-2-1	10	2-2-2
2	2-2-2	10	1-1-3

Combined Dominant/Load-Share Mode

A group of PCs is in Combined Load-Share/Dominant Mode when

- at least two of the PCs have the same relative cost and,
- another PC, or group of PCs, in the MRN Set has a different relative cost.

Table 3-4. MRN Table (MRN Set in Combined Load-Share/Dominant Mode)

MRN Set	PC	Relative Cost	Next Alternate Point Code
3	1-1-1	10	3-3-1
3	3-3-1	10	3-3-2
3	3-3-2	20	3-3-3
3	3-3-3	20	1-1-1

If an MSU comes in with TT 10, GTA 9194605999 then as shown in the following table:

If both PC 1-1-1 and PC 3-3-1 are available, the EAGLE 5 ISS will evenly distribute MSUs for TT=10 and GTA=9194605999 to PC 1-1-1 and PC 3-3-1.

If PC 1-1-1 is not available, the EAGLE 5 ISS will send all MSUs to PC 3-3-1.

If both PC 1-1-1 and PC 3-3-1 are not available, the EAGLE 5 ISS will evenly distribute the MSUs to PC 3-3-2 and PC 3-3-3.

If all PCs in this MRN Set are unavailable, the message is dropped.

Handling of SCCP Class 1 Messages

If the In-Sequence Class 1 SCCP option is ON, MSUs are routed to the PC that results from the GTT regardless of the mode of the MRN Set, and the sequence of the MSUs is maintained. If that PC is down, then the MSUs are routed to the next preferred node in the MRN Set.

If the In-Sequence Class 1 SCCP option OFF, the EAGLE 5 ISS load-shares the MSUs depending on the mode of the MRN Set, and the sequence of the MSUs is not maintained.

Activation

The Flexible GTT Load-Sharing feature requires activation via a feature access key (FAK). This feature key applies to all flexible GTT loading functionality. However, Flexible Intermediate GTT Load-Sharing is a separate feature within the EAGLE 5 ISS. To access the functionality of this feature, both the Flexible GTT Load-Sharing FAK and the Intermediate GTT Load-Sharing FAK must be on.

NOTE: Currently flexible load-sharing functionality only applies to GTT tables. MPS-based features are NOT be able to take advantage flexible load-sharing.

Hardware Requirements

No new hardware is required for this feature.

The Flexible GTT Load-Sharing Feature requires a DSM card running the VSCCP application.

The Flexible GTT Load-Sharing Feature is not supported on TSM cards running the SCCP application.

Limitations

The MRN table has a maximum of 6000 MRN entries.

The Flexible Intermediate GTT Load-Sharing feature is not supported on TSM cards running the SCCP application.

Flexible GTT Load-Sharing feature does not support SEAS.

Flexible Point Code Formatting (Release 26.0)

Description

The Flexible Point Code Formatting feature provides the customization and flexibility of the EAGLE point code provisioning system to meet the needs of ITU-N customers who required a specific ITU-N point code format. The one commonalty of the all ITU-N point codes is that the point code is stored in a 4-byte field in our database (14 bits used for ITU point codes). This value does not change, no matter how it is displayed or input on the EAGLE.

For example, suppose the EAGLE is deployed to 5 different regions for ITU-N customers in Europe. Each region has its own way of viewing point codes in its private network. One region may wish to distribute its point codes

in a format such as A-B, where A ranges from 1 to 1024, and B ranges from 1 to 16. Other regions may wish to use an A-B-C-D point code format. The following table provides examples of how these point codes might be used in different regions.

Table 3-5. Sample ITU-N Point Codes

Region 1	Region 2	Region 3	Region 4	Region 5
1000-1	5-5-5-1	3-8-3	4000	1000-1-1
1000-5	3-1-1-0	1-7-1	16000	1000-0-1
1000-6	5-2-1-3	1-100-1	12000	800-1-0

Upgrade Considerations

All EAGLEs that are upgraded to software that includes the Flexible ITU-N Point Code Feature must have the NPCFMTI parameter in the STPOPTS table set to a system default of 14-0-0-0.

Limitations

It is important to note that this feature does not provide the ability to support point codes that are not 14 (ITU) or 24 (ANSI) bits in length, and has no impact on EAGLE SS7 message processing. Also, it does not apply to gateway screening commands and output, due to the way that GWS was originally designed to take into account the point code format.

Force Change of an Assigned Password at First Login (Release 21.0)

When a password is assigned to a user by the system administrator with either the **`ent-user`** or **`chg-user`** commands (the **`pid=yes`** parameter must be specified with the **`chg-user`** command to change the user's password), that user is required to change the password when they first login to the EAGLE. If the user does not change the password, the login session is rejected.

As part of the password verification process, a check is performed to make sure that the user has changed the password and did not re-enter the current password as the new password.

FTP Retrieve and Replace (Release 29.0) (IP^7 Release 7.0)

Description

NOTE: The FTP Retrieve and Replace feature provides configuration and data transfer support on the EAGLE for the FTP-based Table Retrieve Application (FTRA), which resides on a customer-provided, Windows-based PC or Unix Workstation. FTRA will be available separately. In order to use FTRA, the IP User Interface: Telnet Support feature (IP UI) must be enabled . When the IP UI feature is enabled in Release 29.0, the functions provided by the FTP Retrieve and Replace feature become available for communication between the EAGLE and FTRA.

The FTP Retrieve and Replace feature adds a new and expanded retrieve and replace capability to the IP User Interface Telnet feature.

This feature utilizes:

1. GPSM-II card as the hardware platform for OAM.

2. IPSM card as the hardware platform for the IPS GPL.

3. FTP-based Table Retrieve Application (FTRA) software running on a Unix or Windows-based PC platform connected to the IPSM card.

The FTP Retrieve and Replace Feature provides the following new capabilities:

- Enhanced retrieve capabilities of EAGLE table data, whereby the application will retrieve table data transparently upon request by the user, and later will convert, on demand, to a comma separated variable (.csv) file.

- Enhanced input capabilities of EAGLE table data, supporting input of script files containing scripts created by the user. The transfer of data to the EAGLE is transparent to the user.

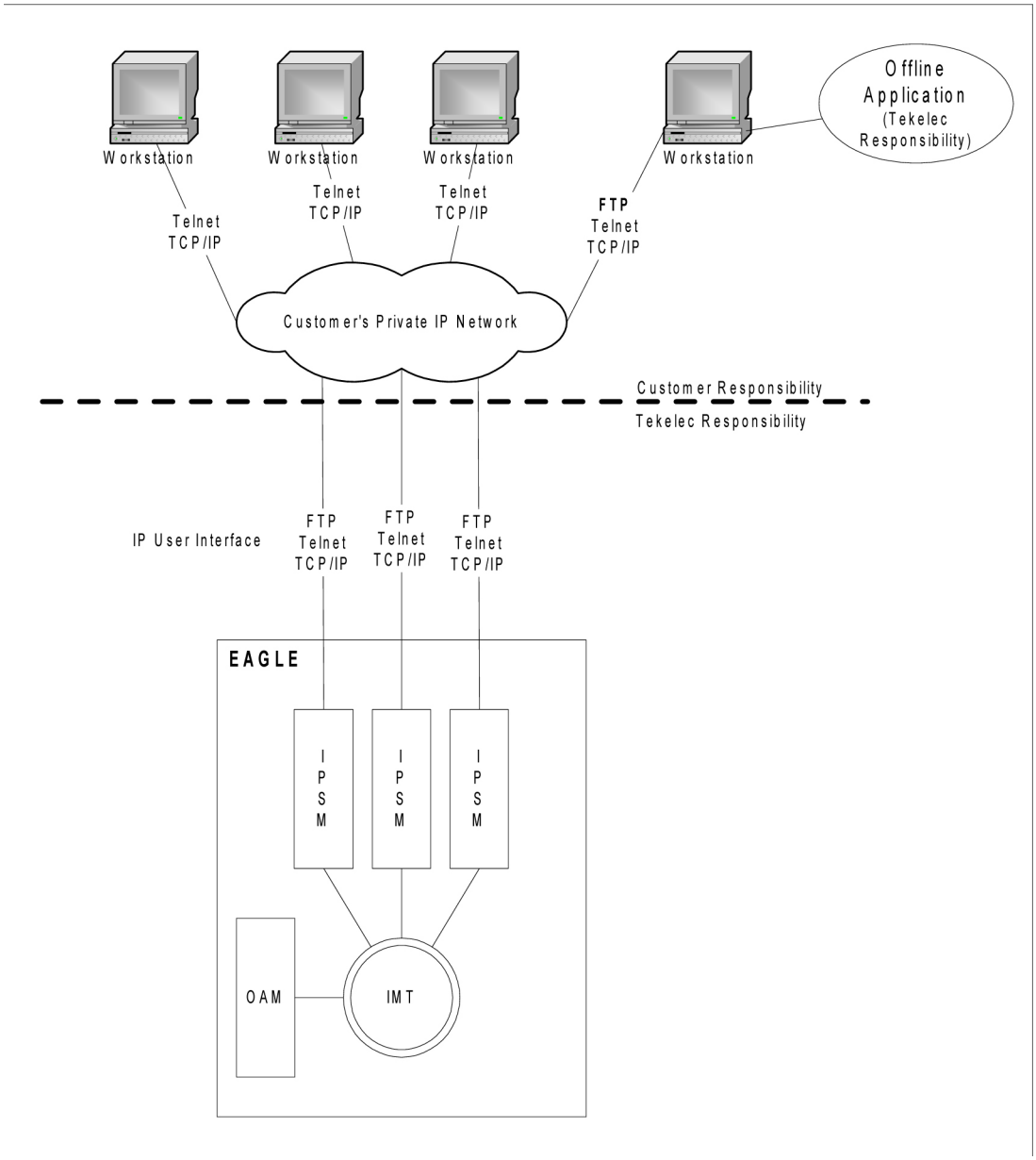
- A much faster and more reliable retrieval and input capability.

- Validating data prior to input and identifying the data at issue.

The FTP Retrieve and Replace feature uses FTP commands to transfer relevant parts of the EAGLE STP OA&M database to a Unix or Windows-based PC, where a new Tekelec-developed Java-based application is running. The application provides features to input changes to table data.

The IPS GPL is memory-mapped such that the FTP area can handle the largest database file on the OA&M. The following figure illustrates the feature in relation to the system and customer's network.

Figure 3-3. FTP Retrieve and Replace



Hardware Requirements

This feature requires IPSM (GPSM-II-based) hardware with at least 1 GB of RAM (i.e., DSM 1GB with the IPS GPL [IPSM].

CAUTION

CAUTION: Never install or initialize MCAP cards in MASP slots 1113 and 1115 after features that require GPSM-II cards are provisioned. Attempting to initialize MCAP cards with GPSM-II features provisioned will cause a system outage. Before replacing an existing GPSM-II card in a MASP slot (1113 and 1115) contact Tekelec Customer Service.

The application requires a UNIX workstation equipped with the following:

- Operating System - Solaris 7
- Processor speed - 500 MHz
- RAM - Minimum 512 MB
- Disk Space - Minimum 10 GB
- CD-ROM drive
- 10/100BaseT Ethernet connection to the LAN
- Static IP addressing
- Java Runtime Environment (JRE) 1.4.0 or later

The application requires a Windows PC workstation equipped with the following:

- Operating System - Windows 98 or later with Win32 API
- Processor speed - Pentium III, 750 MHz or faster
- RAM - Minimum 128 MB
- Disk Space - Minimum 500 MB free + 500 MB free per STP
- CD-ROM drive
- 10/100BaseT Ethernet connection to the LAN
- Static IP addressing
- Java Runtime Environment (JRE) 1.4.0 or later

FTRA 2.1 Compatibility with EAGLE 31.3 (Release 31.3)

The FTRA Release 2.1 provides FTRA compatibility with EAGLE 31.3. There are no new features or functionality in Release 2.1.

FTRA 2.2 Compatibility with EAGLE 31.6 (Release 31.6)

The FTRA Release 2.2 provides FTRA compatibility with EAGLE 31.6. The following changes have been made in FTRA 2.2 to support features new to Release 31.6:

- ASM Obsolescence - Data field of card type "ASM” changed to "TSM” for rtrv-card.
- IPGWx TPS Control and System-wide IPGWx TPSñ New data fields MATELSN, IPTPS, LSUSEALM, SLKUSEALM added in rtrv-ls.

- Support G-Flex at 1700 TPS per DMS ñ New data field ANSIGFLEX added in rtrv-stpopts.
- TDM Global Timing Interface - New data fields HSCLKSRC and HSCLKLL added to support global timing interface in rtrv-stpopts.

Gateway Threshold Exceeded Notification (Release 22.0)

A notification message is produced to alert the user that excessive traffic is occurring on a gateway linkset or an excessive number of MSUs are being discarded on a gateway linkset. When either of these conditions occur, new UIMs are sent to the EAGLE terminals.

UIM 1154 - Gateway Arrival Threshold Exceeded - MSU reception threshold exceeded

```
RLGHNCXA03W 97-06-07 16:28:08 EST Rel 22.0.0
0018.1154    SYSTEM       INFO MSU reception threshold exceeded
             LSN=A1234567 REJ=199     RECV=5200   INTRVL=05
             Report Date: 97-06-07  Time: 16:27:19
```

UIM 1155 - Gateway Discard Threshold Exceeded - MSU discard threshold exceeded

```
RLGHNCXA03W 97-06-07 16:28:08 EST Rel 22.0.0
0018.1155    SYSTEM       INFO MSU discard threshold exceeded
             LSN=A1234567 REJ=199     RECV=5200   INTRVL=05
             Report Date: 97-06-07  Time: 16:27:19
```

The message REPT-GTWYACT is sent to the SEAS interface when these conditions occur.

The term excessive is defined by two values.

- The number of MSUs discarded on the gateway linkset.
- The number of MSUs received on the gateway linkset.

These values measured over a user configurable period of time. If either of these values are exceeded within the specified period of time, then this notification occurs.

The threshold at which these UIMs are generated can be configured by the user on the EAGLE terminal with the **set-gtwy-acthresh** command.

Parameters

The **set-gtwy-acthresh** command uses these parameters.

:lsn = the name of the link set

:rej = the number of MSUs discarded on the gateway linkset threshold. The values for this parameter range from 0 to 999999

:recv = the number of MSUs received on the gateway linkset threshold. The values for this parameter range from 0 to 999999

:intrvl = the time interval, in minutes, during which the counts for the **rej** and **recv** parameters are made. The values for this parameter are 5,10,15, 20, and 30.

The current values for these thresholds can be displayed on the EAGLE terminal with the **rtrv-gtwy-acthresh** command. The following is an example of the **rtrv-gtwy-acthresh** command output.

Output Example

```
RLGHNCXA03W 97-06-07 08:50:12 EST Rel 22.0.0
LSN         REJ        RECV        INTRVL
WY644368    10         1000        10
WY234456    25         2000        20
LN123445    0          0           0
LN123556    25         2500        30
OP239900    0          0           0
```

These thresholds can also be configured on the SEAS interface with the SET-GTWY-ACTHRESH command function and displayed on the SEAS interface with the RTRV-GTWY-ACTHRESH command function.

The counts for the number of MSUs discarded and received on the gateway linkset are collected in the 5 minute measurement collection. These counts do not appear on any measurement reports, but are collected to support this feature. These counts track the two values that need to be monitored.

This feature no longer allows the 5 minute measurement collection to be stopped with the EAGLE's **`chg-meas:collect=off`** command. The 5-minute measurement collection still occurs, but no values are written to disk and no reports are produced.

General Purpose Service Module-II (GPSM-II) for MCAP Slot (Release 28.0)

Description

The Enhanced MCAP, otherwise known as the GPSM-II (General Purpose Service Module, P/N 850-0622-01) for MCAP Slot, is designed to provide better OAM task performance.

Future applications and table expansions will require increased performance across the IMT bus interface, both to and from the Maintenance and Administration Subsystem (MAS). To help meet this need, the GPSM-II card incorporates a DCM design for the OAM functionality on the EAGLE.

GPSM-II is required for supporting the EAGLE Support for Integrated Sentinel feature via the Time Slot Counter (TSC) Synchronization feature.

Refer to the *NSD Hardware Manual* for the current hardware description.

New Hardware Required

The GPSM-II feature requires the new GPSM-II (OAM) card described above); no additional hardware is required.

CAUTION

CAUTION: Never install or initialize MCAP cards in MASP slots 1113 and 1115 after features that require GPSM-II cards are provisioned. Attempting to initialize MCAP cards with GPSM-II features provisioned will cause a system outage. Before replacing an existing GPSM-II card in a MASP slot (1113 and 1115) contact Tekelec Customer Service.

The TSC Synchronization feature requires the new GPSM-II EAGLE® hardware equipped with the new TSC Synchronization hardware to support it. Time Slot Synchronization is an existing option for the EAGLE that allows all cards in the system containing a Time Slot Counter to synchronize with each another. The ability to have synchronized timing between cards is useful in applications such as system-wide message time stamping.

Upgrade Considerations

The GPSM-II feature allows the existing OAM functionality to operate on a GPSM card or MCAP card. In addition, the EAGLE will also support inserting an MCAP or GPSM card in the control shelf as an OAM card, even if the

OAM card that is already inserted does not match the OAM card that is being inserted. This functionality is needed to support upgrade where the hardware is in transition. It is assumed that an EAGLE with an MCAP and a GPSM in OAM card slots 1113 and 1115 is a transitional state.

Consequently, software modification of the one-command upgrade function is necessary to support some requirements. Upgrade command support for the inhibiting of the standby OAM and upgrade of the board Flash memory is required.

G-Flex C7 Relay (Release 26.2)

Description

G-Flex optimizes the use of subscriber numbers and number ranges by providing a logical link between any MSISDN/MIN/MDN and any IMSI, as well as between any subscriber number and any HLR. This feature allows subscribers to easily be moved from one HLR to another.

NOTE: This feature applies to any GSM or IS-41, ITU, or ANSI mobile network. In the following text, the term DN is used to indicate MSISDN numbers, MINs, or MDNs. Also, the term subscriber number is used to indicate DN and/or IMSI.

It also allows each HLR to be filled to 100% of its capacity by allowing subscriber number ranges to be split over different HLRs, and individual DNs/IMSIs to be assigned to any HLR. Another benefit is that subscriber number routing data is not required to be maintained in all MSCs in the network.

The initial version of G-Flex, as defined in this document, applies to routing to HLRs only. In the future, G-Flex may be expanded to include routing to other intelligent devices, such as SCPs (Service Control Points) and VMSCs (Voice Mail Service Centers), depending upon market needs.

G-Flex is optional on the EAGLE STP, and can be turned on (but not turned off) via a feature bit. G-Flex and North American LNP are mutually exclusive on an EAGLE node.

Refer to the Features Manual - G-Flex for the current information on this feature.

Upgrade Considerations

EAGLE Database

The EAGLE upgrade process is responsible for copying new TDM resident G-Flex tables from the upgrade removable cartridge to the newly formatted fixed disks. The G-Flex feature bit should not be turned on prior to or during an upgrade of an existing EAGLE STP.

EAGLE STP Audit

The EAGLE STP audit is designed to recognize when it is in upgrade mode, and will not attempt to do any activity that requires access to new G-Flex tables, since they will not be present until the upgrade has completed.

In order to convey G-Flex audit-detected errors to the active OAM, space in the common maintenance block header must be identified. In order to prevent false alarms during the upgrade, the revision level of the maintenance block has been redefined. Existing code that examines maintenance blocks will not interpret them if the system is in upgrade mode and the revision level in the received maintenance block is not at the expected value.

EAGLE Maintenance

During upgrade, the **`rept-stat-epap`** command output may not reflect the current state of the GSM system.

Hardware Requirements

This feature requires the MPS Hardware System.

Limitations

1. An E.214 number received by the G-Flex™ C7 Relay must first be converted to an E.212 number before searching the G-Flex database. If the original E.212 number was truncated to form the E.214 number, the full original E.212 number cannot be recovered, and G-Flex™ will not work properly.

2. No overload controls are required above and beyond existing EAGLE lower level mechanisms (e.g. for MTP congestion, etc.).

3. This initial version of the G-Flex™ C7 Relay only supports routing of messages to a single network node for a particular subscriber. For example, an individual subscriber cannot have some messages routed to his HLR, and other messages routed to a separate Authentication Center (AuC). In this example, if the AuC is co-located with the HLR, then this version of G-Flex™ will work. The G-Flex™ design allows for expansion to include routing to multiple network elements (corresponding to multiple services) for the same subscriber.

4. Messages routed by G-Flex™ cannot undergo ANSI-ITU conversion.

G-Port MNP (Release 26.2)

GSM Mobile Number Portability (G-Port) provides mobile subscribers the ability to change the GSM subscription network within a portability cluster, while retaining their original MSISDN(s).

Throughout the world, an increasing number of governments are mandating that telecommunications network operators support service provider number portability. Service provider portability allows a consumer to change service providers while retaining his phone number. Service provider portability is intended primarily to promote competition among service providers. It applies to both wireline and mobile phone networks. In particular, this feature is focused on service provider portability in GSM (Global System for Mobile communications) networks.

While the advent of number portability is good news for consumers, it presents many challenges for network operators. G-Port MNP (Mobile Number Portability) minimizes those challenges for GSM network operators, while enabling them to efficiently meet their regulatory obligations.

For current details of this feature, refer to the *Features Manual - G-Port* .

G-Port MNP Circular Route Prevention (Release 28.1)

Description

In some cases, networks may have incorrect number portability data for a subscriber. For example, a subscriber may have ported from network A to network B. Network A has the correct routing information, indicating the subscriber now belongs to network B. However, network B may have incorrect routing information indicating that the subscriber still belongs to network A. In this case, network A routes the call to network B, based on its portability data, but network B routes the call back to network A, based on its incorrect data. This behavior results in a circular route.

This feature provides an option to prevent this from happening.

For current detail on this feature, refer to the *Features Manual - G-Port* .

Hardware Requirements

No new hardware is needed to support this feature.

Upgrade Considerations

The EAGLE upgrade process is only responsible for copying new GSM tables from removable cartridge to the newly formatted fixed disks.

G-PORT SRI Query for Prepaid (Release 35.2)

G-Port SRI Query for Prepaid Detailed Description

The G-Port SRI Query for Prepaid feature enables the EAGLE 5 ISS to provide portability information to a Service Control Point (SCP) database. This information enables the database to determine the network used by a called subscriber.

The G-Port SRI Query for Prepaid feature enables a user to provision the following Message Signal Unit (MSU) values in the EAGLE 5 ISS GSERV table:

- translation type (TT)—The TT of the called party (CdPA)
- originating point code (OPC)—The OPC from the message transfer part (MTP) layer
- global title address (GTA)—The GTA of the calling party (CgPA)

These values are used to determine whether an SRI should receive G-Port SRI Query for Prepaid service or normal G-Port SRI service.

If the G-Port SRI Query for Prepaid feature is enabled and turned on, an incoming SRI's TT, OPC, and GTA values are compared against the values in the GSERV table. If no match is found, or if no values are provisioned in the GSERV table, normal G-Port SRI processing is performed on the message. If a match is found for one or more of the values, the message is treated as a Prepaid Query.

The G-Port SRI Query for Prepaid feature affects only SRI messages. All other messages, including SRI-SM and SRI-GPRS messages, are processed by normal G-Port service, even if the values in those messages match values in the GSERV table.

After an SRI message is identified as requiring G-Port SRI Query for Prepaid service, the EAGLE 5 ISS performs a Mobile Number Portability (MNP) database lookup on the Mobile Station Integrated Services Digital Number (MSISDN). The results of the lookup are returned to the SCP that originated the query.

A TCAP/MAP error specifically related to a decoding error in the SRI MSISDN parameter causes an "Unsupported/ Unexpected Data Value" MAP error. All other TCAP/MAP errors cause the message to be relayed to a Home Location Register (HLR), which then returns the appropriate MAP error based on the status of the subscriber (e.g. Unknown, Barred, etc.)

The message relay is based on information in the G-Port MNP database. SCCP level errors cause the return on a UDTS message to the Prepaid SCP.

This feature requires a Feature Access Key and cannot be turned off once it is turned on.

Hardware Requirements

The G-Port SRI Query for Prepaid feature has the same requirements as those required for the G-Port feature.

GR-376 Interface (Release 26.0)

Description

The GR-376 Support feature provides an optional method of data collection from the EAGLE STP. Measurement and reference data is collected with the EAGLE and passed to a supplemental Network Data Collection (NDC) Q adapter function (QAF).

Refer to the *Feature Manual - GR-376* for current information on this feature.

Limitations

The following limitations apply to the initial release of the GR-376 Support feature:

1. Explicit retrieval of current data objects is not supported.
2. NDC data recovery is provided only when at least one EMAP originally received the data from an EMDC DCM card. No provision is made in the initial release to recover lost data spanning multiple periods.
3. Other than reference data, no GR-495-specified data storage objects are supported for this release.
4. No notifications are supported in the initial release.

Global Option for Connect on INP Query Response (Release 35.0)

Description

The Global Option for Connect on INP Query Response feature adds a global INP option that indicates whether the EAGLE 5 ISS is to send “Connect” or “Continue” messages when an IDP message is received for INP service, the DN digits match, and the HLR ID is present.

NOTE: The Connect INP option does not affect the INP Message Relay service.

Hardware Requirements

The Global Option for Connect on INP Query Response feature has no hardware requirements.

Limitations

The Global Option for Connect on INP Query Response feature has no limitations.

Global Title Modification (Release 28.1) (IP^7 Release 6.0)

Description

This feature allows the user to modify any part of the Global Title in the outgoing message, other than Encoding Scheme, after GTT has been performed. A new Translation Type (TT), Numbering Plan (NP), and/or Network Address Indicator (NAI) value can be specified. Also, a specified number of leading digits of the GT address can be deleted, and/or a set of specified digits can be added to the beginning of the GTA. This is all defined on a per-entry (i.e. GTA) basis.

Refer to the *Database Administration Manual - Features* for current details of this feature.

Hardware Requirements

No new hardware is needed to support this feature.

Upgrade Considerations

The EAGLE provides an upgrade conversion for customers using the Interim GT Modification feature supplied in Release 26.0. Database conversions are handled during upgrade.

Global Title Translation (GTT) (Release 20.0)

The global title translation (GTT) subsystem of the EAGLE can support the following level of activity.

- 850 messages per second
- 21,000 global title translations per second per system

The maximum number of entries in the global title translation table is 270,000 entries. It is possible to enter all 270,000 entries under one translation type. However, the system works most efficiently when there are 65,536 or fewer GTT entries per translation type. While there is no mechanism to limit the number of GTT entries to fewer than 65,537 per translation type, the performance of the GTT subsystem is not guaranteed when more than 65,536 translations are entered for a single translation type.

Group Ticket Voucher (Release 23.0)

Description

This feature is used to control the traffic from the high-speed ATM signaling links to the ASM-SCCP cards and ACMs. The ASM-SCCP cards are used to process messages requiring global title translation. The ACMs are used

by the STPLAN feature to send messages selected by the gateway screening feature to a remote host for further processing. The message rate from a single high-speed ATM signaling link can exceed the capacity of a single ASM-SCCP card or a single ACM, so the message traffic is split between multiple ASM-SCCP cards or ACMs.

To determine which card can process the message, each type of message is assigned a group number by the system software.

- SNM messages - group 1
- STPLAN messages - group 2
- SCCP messages - group 3

NOTE: Only SCCP messages containing a destination point code that is the EAGLE's true point code or one of its capability point codes are affected by this feature.

Each card of each card type is assigned a member number by the system software when the card is entered into the database with the **ent-card** command. This number is not configurable by the user and cannot be displayed with the **rtrv-card** command. This number is used only internally by the software to identify the cards to the group ticket voucher feature. The member number can range from 0 to 31. The number assigned to the card is the smallest number in the range from 0 to 31 that is not already in use. The STPLAN and SCCP member numbers are assigned independently of each other. The system software does not check the number of ASM-SCCP cards entered into the database, but the system software supports a maximum of 25 ASM-SCCP cards, and a maximum of 30 ACMs. If more than 25 ASM-SCCP cards or 30 ACMs are entered into the database, the member number of the newly entered card is set to 31.

When a signaling link receives an SCCP message or wants to send an STPLAN message to a remote host, it sends a request on the IMT bus to find either an ASM-SCCP card or an ACM (depending on the type of message) that has capacity to handle the message. When a card is found that can handle the message, that card answers the request, informs the requesting signaling link that it can handle the message, and sends in its answer the card's group number and member number. When the requesting signaling link receives the answer, it translates the card's group number and member number into the card's IMT address, then sends the SCCP message or STPLAN message to that IMT address. The request to find the ASM-SCCP card or ACM is referred to as a voucher. The answer to the request is referred to as a ticket. The card that is able to handle the message is referred to as the granter.

Sequenced GTT class 1 traffic on the high-speed ATM signaling links is discarded. The current method for ensuring sequencing in the EAGLE is to use only one ASM-SCCP card at a time for any one signaling link's stream of sequenced traffic. This imposes a limit on the rate of traffic from any one stream, the speed of an ASM-SCCP card, 850 messages per second. Since the message rate of a high-speed ATM signaling links far exceeds 850, an ASM-SCCP card cannot handle sequenced traffic from a high-speed ATM signaling link.

The following figure shows an example of the operation of the group ticket voucher on the IMT bus. This example is for an SCCP message. The action would be the same for an STPLAN message, but the group number would be different.

1. The ASM-SCCP cards periodically refresh the hardware grant counters (one for each bus) dynamically based on their individual available capacities.

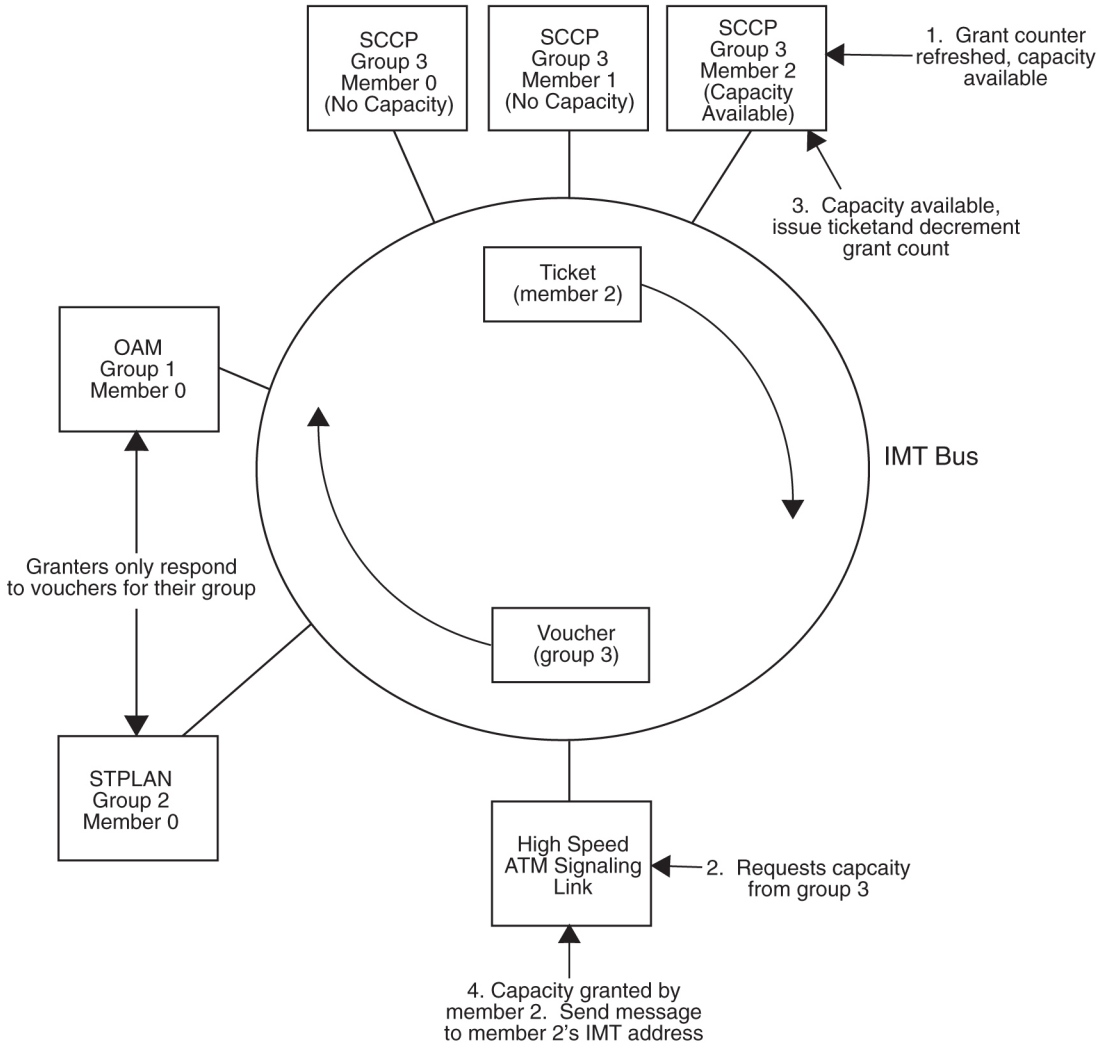
2. When a high-speed ATM signaling link receives an SCCP message, the high-speed ATM signaling link sends a TVG (group ticket voucher) request containing the SCCP message group number (group number 3) to find an ASM-SCCP card that can handle the SCCP message.

3. The request is sent around the IMT bus until it finds an ASM-SCCP card that can handle the message. In this example, members 0 and 1 have no capacity, but member 2 does. Member 2 changes the TVG (group ticket voucher) request, a voucher packet, to a ticket packet, changes the group number of the packet to the

ASM-SCCP card's member number, member 2, and decrements the card's grant counters for each IMT bus. When member 2's grant counter reaches zero, that ASM-SCCP card has no more capacity for handling messages and the next available member with capacity begins granting tickets.

4. The ticket packet returns to the high-speed ATM signaling link requesting the service. The high-speed ATM signaling link translates member 2's group number to the card's IMT address and sends the SCCP message to that card.

Figure 3-4. Group Ticket Voucher Example



Measurements

MSULOST3

The MSULOST3 measurement is currently used to count the number of MSUs discarded when a card does not have an SCCP assignment or when the linkset-on-hold buffer is full. In Release 23.0, this measurement also counts the number of SCCP MSUs that are discarded by the group ticket voucher feature on the high-speed ATM signaling links. The SCCP MSUs are discarded under these conditions:

- All Class 1 (sequenced) SCCP traffic sent to the EAGLE.
- A Class 0 SCCP message for EAGLE arrives when the SCCP group ticket voucher queue is full.
- A SCCP message in the SCCP group ticket voucher queue is more than 2 seconds old.

The MSULOST3 measurement is displayed in these measurement reports:

SYSTOT-STP - STP system total measurement report

MTCD-STP - STP daily maintenance measurement report

MTCDTH-STP - STP day-to-hour maintenance measurement report

NM-STP - STP network management measurement report

SLANDISC1

The SLANDISC1 measurement is currently used to count the number of MSUs that have not been copied to a remote host because the STPLAN feature is disabled. In Release 23.0, this measurement also counts the number of STPLAN MSUs discarded by the group ticket voucher feature on the high-speed ATM signaling links. The STPLAN MSUs are discarded under these conditions:

- An STPLAN MSU arrives when the STPLAN group ticket voucher queue is full.
- An STPLAN MSU in the STPLAN group ticket voucher queue is more than 2 seconds old.

The SLANDISC1 measurement is displayed in these measurement reports:

SYSTOT-STPLAN - STPLAN system total measurement report

MTCD-STPLAN - STPLAN daily maintenance measurement report

MTCDTH-STPLAN - STPLAN day-to-hour maintenance measurement report

AVL-STPLAN - STPLAN availability measurement report

Group Ticket Voucher for SCCP Cards (Release 27.0)

Description

Group Ticket Voucher replaces SCCP Load Balancing as a method of providing SCCP service to LIM cards.

In the current EAGLE implementation, an EAGLE Low Speed LIM (LSL) card is assigned to one SCCP card based on the 16:1 LIM - SCCP Engineering rule via load balancing (LB). The LSL-SCCP assignment may change from time to time, but the engineering rules are maintained at all times. This poses a problem to customers, forcing them to purchase unnecessary hardware (SCCP) so they can meet the engineering rules for LB. The Group Ticket Voucher (TVG) solution currently implemented with HSL/SCCP and HSL/SLAN card assignments alleviates this problem.

The Release 27.0 TVG solution is an extension of the Ticket/Voucher solution to the SNM multicast problem. The Ticket/Voucher concept uses an IMT hardware-based request/grant scheme to provide a flow control solution, which allocates message capacity at hardware speeds. Each grant allows a single message to be sent to the granter. The "group" concept is added to provide for multiple groups of granters, each supporting one particular message type.

Each granter has a group ID that is based on the message type it supports, and will only grant capacity to TVG requests which match its group number. Since the TVG mechanism is designed to provide a one-to-many assignment, there will typically be more than one granter for a group. SNM, by its nature, is the only message type, which will have a single granter (OAM).

Each message type supported by TVG will be assigned to a particular group. A card requesting capacity from a particular group will build a TVG request, and set the group number in the request based on the message type. The group numbers are defined as follows:

- SNM group 1
- SLAN group 2
- SCCP(GTT) group 3
- REROUTE group 31

In addition to the group number, each granter is assigned a member number, which identifies the granter. The member number is unique within a group, but may be repeated within other groups in the EAGLE. When a granter card grants capacity, it changes the voucher packet into a ticket. It also changes the group number in the packet to its member number. When the TVG request returns to the requester as a ticket, the requester uses the member number along with the group number it saved to look up the IMT address of the granter. The IMT address provides the assignment, which allows the requester to forward the message to the granter.

Upgrade Considerations

LB is supported during upgrade to Release 27.0 only.

Limitations

1. Class-1 GTT traffic on will be allowed, but sequencing will not be guaranteed.
2. The number of TVG requests that can be made per card is a function of the number of cards in the system, and decreases as the number of active cards increase. It is approximately 1/(Nx10-6) for N cards. For a system with 250 IMT addresses it is limited to about 3300 requests/second. This limitation could become a bottleneck if the number of cards on the IMT bus were increased.

GSM MAP Screening (Release 26.1)

Description

Traditionally, STP message screening has been limited to the MTP and SCCP levels; this has been sufficient to meet operators' needs. However, GSM mobile operators have an increasing need for screening at the Mobile Application Part (MAP) level. This need is driven by advanced network capabilities and proliferating roaming agreements.

New features that require this enhanced screening capability are Inter-operator Short Message Service (SMS) and Any Time Interrogation (ATI). The GSM MAP Screening feature focuses on solving the screening needs associated with ATI, which is defined in MAP version 3. An ATI message allows an external server to interrogate an HLR

and obtain information about the location and/or state of a GSM subscriber. It may be desirable to control which external entities can request this information, and what information they can request before allowing the message to pass through to the HLR.

The EAGLE-based solution to this problem is designed to allow the user to provision which MAP SSNs are affected, which MAP op codes to screen, which origination points are allowed, and which error messages to use.

NOTE: This feature is only applicable for ITU implementations.

Refer to the *Database Administration Manual - Features* for current information on this feature.

Hardware Requirements

To meet optimum performance in "worst case" scenarios under heavy traffic conditions, it is recommended that GSM MAP Screening be used in conjunction with high performance SCCP hardware (DSMs). There is, however, no specific requirement restricting GSM MAP Screening to DSM hardware, since a throttling mechanism protects system integrity.

Upgrade Considerations

- New tables relating to GSM MAP Screening must be created on the upgraded disk.
- the GSM MAP Screening feature bit should be defaulted to OFF on new upgraded disks.
- The **STPOPTS** value of **GSMSDECERR** shall be **PASS** after upgrade.
- The **STPOPTS** value of **GSMDFLT** shall be **PASS** after upgrade.

Limitations

1. Overlapping range entries cannot be provisioned.
2. There is no cross-checking between the individual entry table and the range table when numbers are provisioned. The individual table entries are exceptions to the range table. Thus, if an individual number is provisioned that is already part of a range, automatic splitting of the range entry will not occur. (This is not necessarily a limitation.)
3. Per-server measurements are not provided for range table entries, and no per- server measurement will be pegged when a match occurs in the range table.
4. This feature is applicable only for ITU implementations.
5. A given GTA may be entered in the MAP Screening table only once.

GSM MAP Screening Duplicate/Forward (Release 29.0)

Description

The GSM MAP Message Duplicate/Forward feature extends the capabilities of GSM MAP Screening by allowing MAP messages to be routed, discarded, duplicated, or forwarded based on the provisioned screening criteria. This gives the EAGLE the ability to offload or copy certain types of MAP messages to an attached processor (such as a SCP) based on the MAP Opcode and/or Calling Party Address.

For these advanced services on MAP messages, targeting messages based only on MTP level screening could lead to many messages being sent to the external platform unnecessarily, possibly impacting the performance of the STP or the external platform. In order to allow a finer granularity in message selection, a method is needed to target only specific MAP messages. Furthermore, it is desirable to achieve this using standard message structures (i.e. SS7).

Refer to the *Database Administration Manual - Features* for current information on this feature.

NOTE: It should be noted that the GSM MAP Message Duplicate/Forward feature is independent of the EAGLE's STPLAN and DTA features. It operates and is provisioned in an entirely different manner than either of these existing features.

Hardware Requirements

No new hardware is needed to support this feature.

Upgrade Considerations

MAP screening tables that were built under the Release 26.1 version of MAP Screening and used the previous default value of NONE for the FORBID parameter will not have that value changed to ALL as a result of an upgrade to this version of MAP Screening. (Those original entries will still have FORBID = NONE, even though new entries after the upgrade will default to FORBID=ALL.)

Limitations

The first implementation of this feature is limited in the following ways:

1. Only works for ITU messages.
2. State and Location are the only GSM Map parameters that screening may forbid.
3. ATI Error responses are the only type of messages that may be sent as a screening rejection response.
4. We do not screen on NP and NAI on a per origination basis, but rather on a per Map Op-Code basis.
5. Measurements are taken on an existing 30-minute schedule and are not reported real-time.
6. During extremely high traffic conditions where 850 messages per second require GSM Map screening on 1 SCCP card, and other SCCP processor intensive features are also in very rare worst case conditions, GSM

Map Screening may be throttled to keep SCCP processor utilization below 70%. There will be no alarm or warning when this condition occurs.

GSM MAP SRI Redirect to Serving HLR (Releases 31.11, 34.0)

Description

This feature provides the capability to resolve the incompatibility introduced by the proprietary implementation of the GSM MAP SRI message. This feature is an extension to the G-Port Mobile Number Portability (G-Port MNP) Protocol. Therefore, the feature is compatible with other MNP enhancement features provided to date, including the "G-Port MNP Circular Route Prevention," "Portability Check for Mobile Originated SMS" and "Pre-paid SMS Intercept" features.

Hardware Requirements

Refer to the hardware baseline.

Limitations

Because this is an ON-only feature, to remove the affect of the feature from call processing, all the VendorID List entries must be deleted.

NOTE: This is similar to the behavior of several other protocol features.

GTT by TT Measurements and GR-376 Enhancements (Release 26.0)

Description

This section combines discussion of *two* Release 26.0 features:

- GTT by TT Measurements
- GR-376 Enhancements

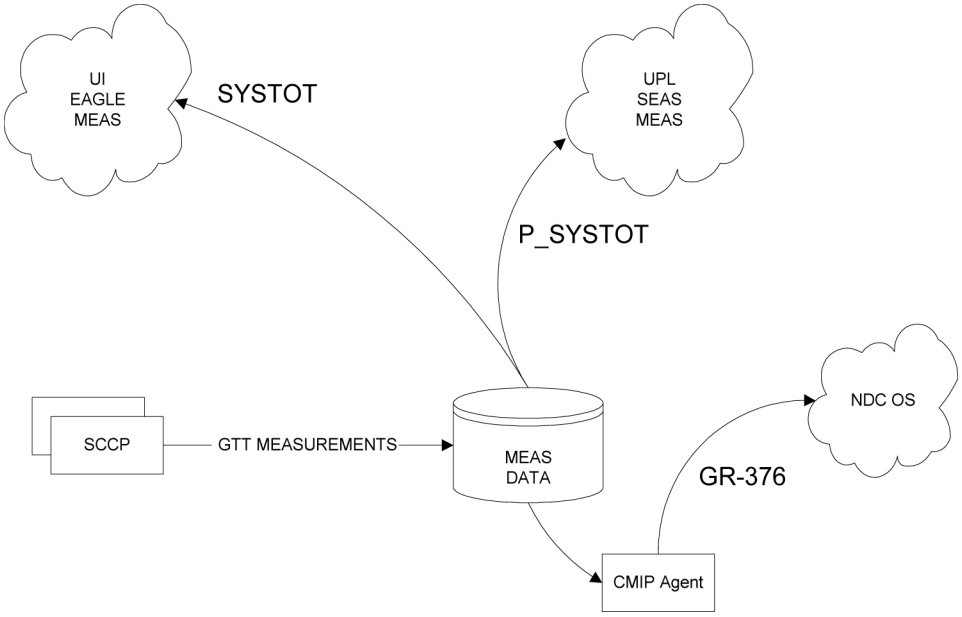
The GTT by TT Measurements feature allows EAGLE customers to collect measurements and generate reports of GTT activity by Translation Type (TT). GTTs-per-TT reports are available from the EAGLE terminal, and via the SEAS interface and the GR-376 interface. GTTs-per-TT reports are available for all provisioned translation types.

The GTT by TT Measurements feature provides EAGLE/SEAS support for the GTT-by-TT capability.

The GR-376 Enhancements feature provides the GR-376 support for GTT-by-TT.

The following figure provides a high-level diagram of the capabilities implemented by GTT by TT Measurements feature and the GR-376 Enhancements feature:

Figure 3-5. Concept Diagram



GTTs are pegged in the SCCP card for each TT and are stored on the fixed disk in 30-minutes intervals and retained for a 24-hour period. The SYSTOT report and the P_SYSTOT schedule are existing capabilities for reporting STP-wide measurement data.

The TT entity type has been expanded to report GTTs performed/not translated per TT for 256 known translation types. This feature provides the customer with information that can be used for service growth trends and potential revenue collection.

A new parameter (**:TT=x**) has been added to the **rept-meas** command to enable the user to specify a translation type to be reported. The demand report requires that a TT be specified, while scheduled reports will provide GTTs per TT for all TTs. This feature provides scheduled and demand reports of GTTs-per-TT to the EAGLE UI for half-hourly measurements. Half-hourly GTTs-per-TT measurements are provided to the SEAS interface.

The following table specifies the EAGLE interpretation of SYSTOT-TT registers that are reported per TT by the GTT by TT Measurements feature and the GR-376 Enhancements feature.

Table 3-6. SYSTOT-TT Register Definition

Register	Description	EAGLE Interpretation
GTTPERFD	GTTs Performed	The total number of MSUs that successfully completed global title translation
GTTUN0NS	GTTs Unable to Perform – Diagnostic 0: No Translation for Address of Such Nature	Total number of times that the specified translation type in an MSU was not supported by the STP or the form of the GTT was incorrect for the given translation type.
GTTUTTNF	GTTs Unable to Perform – TT not found	Not supported
GTTUINVF	GTTs Unable to Perform – Invalid GT format	Not supported
GTTUN1NT	GTTs Unable to Perform – Diagnostic 1: No Translation for This Address	The number of times that a match for the global title could not be found in the translation table.

Register	Description	EAGLE Interpretation
GTTUGTAR	GTTs Unable to Perform – Incorrect GTA Reference	Not supported
GTTUDPCR	GTTs Unable to Perform – Incorrect Ordered DPC Reference	Not supported
GTTUNABL	GTTs Unable to Perform – All Diagnostics	Not supported

Upgrade Considerations

During upgrade, measurement collection is inhibited (except for GR-376) and any measurement data collected prior to the upgrade is lost. This is the historical method of handling measurement tables during upgrade. No change in this processing is anticipated for this feature or release. In addition, all obsolete measurement tables are removed from the fixed disk by the upgrade process.

Implementation of the GTT by TT measurements feature in the EAGLE includes the creation of a new table to store the 30-minute GTTs per TT measurement data. The new table (M30_TT.MEA) resides on the fixed disk and on the measurements removable. The measurement data captured in the table currently requires 16 bytes of storage per entry. The remaining 48 bytes are reserved for future use.

During upgrade, the table will not be present on the previous revision TDM, but is created on the standby TDM during the format disk process. No additional processing is required during the upgrade for this table.

GTT Error Reporting Enhancements (Release 21.0)

The UIM message formats for global title translation (GTT) error messages have been updated to include more useful information for diagnosing problems in the network. The affected messages include:

- SCCP UDT
- SCCP Message
- SCCP Class
- SCCP CDPA
- SCCP Routing
- SCMG - SCCP Management

GTT Loadsharing to 32 Destinations (Release 36.0)

Description

The GTT Loadsharing to 32 Destinations feature increases loadsharing destinations for intermediate and final GTT from 8 to 32 destinations.

The feature allows each Mated Application Table (MAP) set or Mated Relay Node (MRN) set that is used for loadsharing to be associated with up to 32 destination point codes in the EAGLE 5 ISS Destination table.

The support of 32 destination point codes does not increase the maximum number of supported entries in the MAP table or MRN table.

Hardware Requirements

The GTT Loadsharing to 32 Destinations feature requires DSM cards.

Limitations

None

GTT Table Increase (Release 29.0)

Description

This feature increases the number of Global Title Table entries. The EAGLE GTT capacity can be increased from 270,000 to a maximum of 400,000 Global Title Table entries on TSMs (or a combination of TSMs and DSMs), and from 270,000 to a maximum of 1,000,000 Global Title Table entries on DSMs. The GTT Table Increase Feature is also referred to as the XGTT Feature (Expanded GTT).

XGTT is a controlled feature associated with quantity. XGTT must be initialized to default quantity level 270,000 GTT table entries. One of two Part Numbers is required to enable XGTT. If the system meets minimum hardware requirements, the XGTT feature can be enabled at different quantity levels. One Part Number increases the GTT table size from 270,000 entries to 400,000 entries (893-0061-01); the other increases the GTT table size from 270,000 or 400,000 entries to 1,000,000 entries (893-0061-10).

Hardware Requirements

All existing SCCP ASM cards must be replaced with SCCP TSM or better (DSM) equipment when activating XGTT. The 400,000 feature key allows TSMs and/or DSMs; the 1,000,000 GTT feature key allows DSMs only.

All existing SCCP ASM cards must be replaced with SCCP TSM or better (DSM) equipment when activating XMAP.

NOTE 1: The EAGLE will not allow the feature access key to be activated unless the required SCCP hardware is present in the system. Also, the EAGLE does not allow the feature access key to be activated unless both the active and standby OAM is a GPSM-II.

CAUTION: Never install or initialize MCAP cards in MASP slots 1113 and 1115 after features that require GPSM-II cards are provisioned. Attempting to initialize MCAP cards with GPSM-II features provisioned will cause a system outage. Before replacing an existing GPSM-II card in a MASP slot (1113 and 1115) contact Tekelec Customer Service.

The EAGLE will auto-inhibit an SCCP card that does not meet the hardware requirements for the respective GTT Table size. This requirement is only applicable after at least one of the two feature access keys is enabled.

enabled for 400,000 or 1,000,000 GTT entries.

GTT UIM 21 Digit Length Enhancement (Release 29.0)

Description

This enhancement increases the length of GTT UIMs from 10 digits to 21 digits, providing more space for the SCCP called or calling party address to be displayed.

Hardware Requirements

No new hardware is needed to support this feature.

GWS Error Reporting Enhancement (Release 21.0)

The UIM message format for gateway screening messages is expanded to provide the user with more information. UIMs resulting from gateway screening failures include:

- Link Set Name
- Originating Point Code (OPC)
- Destination Point Code (DPC)
- Service Information Octet (SIO)
- Gateway Screening Reference

The following rules apply to the SIO information:

Table 3-7. SIO Information

SIO	SSN	Additional Information Included in UIM
0,1,2	N/A	The H0 and H1 heading codes, and the concerned point code
3	1	The SCCP management (SCMG) message type, message length, multiplicity, concerned point code (CPC) and subsystem
3	|1	The message type, called party address (CDPA) and all sub-fields, calling party address (CGPA) and all sub-fields
> 3	N/A	The first 24 bytes of the MTP user data (the data following the SLS)

Hex Digit Support for GTT (Release 35.3)

Description

The Hex Digit Support for GTT feature enables the EAGLE® 5 ISS to process both ANSI and ITU Message Signaling Units (MSUs) that contain either decimal or hexadecimal Global Title digits (0-9, a-f, A-F) in the Called Party Address (CdPA) field.

When the Hex Digit Support for GTT feature is enabled and turned on, any of the following three scenarios are possible:

- Incoming MSUs whose digits equal 10 are matched to a global title translation that contains a single GTT table entry of GTA=10.
- Incoming MSUs whose digits equal 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30 are matched to GTT table entries with a range of GTA=20 and EGTA=30.
- Incoming MSUs whose **hexadecimal** digits equal **2A**, **2B**, **2C**, **2D**, **2E**, **2F** are matched to GTT table entries with a hexadecimal range of GTA=20 and EGTA=30.

If desired, the user can then split the hexadecimal range into three separate GTT table entries and specify translation data for hexadecimal digits as follows:

GTA=20	EGTA=29	with existing translation data
GTA=2A	**EGTA=F**	**with user specified translation data**
GTA=30		with existing translation data

Before the Hex Digit Support for GTT can be enabled and turned on, the GTT feature must be turned on, and all Translation Services Module (TSM) cards in the system, if installed, must be replaced with Database Services Module (DSM) cards.

When enabled and turned on, the Hex Digit Support for GTT feature enhances the functionality of the following features:

- ANSI-ITU-China SCCP Conversion
  When the Hex Digit Support for GTT and the ANSI-ITU-China SCCP Conversion features are enabled and turned ON, the values specified for the**npds** and **nsds** parameters can be either decimal digits (**0-9**) or hexadecimal digits (**0-9**, **a-f**, **A-F**).

- Enhanced Global Title Translation (EGTT)
  When the Hex Digit Support for GTT and the EGTT features are enabled and turned ON, the values specified for the **gta**, **egta** parameters in the **`gta`** command, can be either decimal digits (**0-9**) or hexadecimal digits (**0-9**, **a-f**,**A-F**).

- Global Title Translation (GTT)
  When the Hex Digit Support for GTT and the GTT features are enabled and turned ON, the values specified for the **gta** and **egta** parameters in the **`gtt`** commands, can be either decimal digits (**0-9**) or hexadecimal digits (**0-9**, **a-f**,**A-F**).

- Modified Global Title Translation (MGTT)
  When the Hex Digit Support for GTT and the MGTT features are enabled and turned ON, the values specified for the **npds**, and **nsds** parameters in the **`gta/gtt`** commands, can be either decimal digits (**0-9**) or hexadecimal digits (**0-9**, **a-f**, **A-F**).

- Origin-based SCCP Routing (OBSR)
  When the Hex Digit Support for GTT feature and the OBSR features are enabled and turned ON, the values specified for the **cdpa gta/egta** and **cgpa gta/egta** parameters can be either decimal digits (**0-9**) or hexadecimal digits (**0-9**, **a-f**, **A-F**).

For more information about how to configure the EAGLE 5 ISS and its database to implement the above listed features, refer to the *Database Administration Manual – Global Title Translation* for this release.

Hardware Requirements

No new hardware is required to support this feature. However, before the Hex Digit Support for GTT feature can be enabled and turned on, all Translation Services Module (TSM) cards in the system, if installed, must be replaced with Database Services Module (DSM) or later revision card running the VSCCP GPL.

NOTE: This feature is supported on both 1 GB and 4 GB DSM/VSCCP cards.

See "Appendix B. Hardware Baseline" for the hardware baseline of this release.

Limitations

- Command length:
  A limitation of the EAGLE 5 ISS is a command length of 150 characters per entry. In some cases, a single **ent/chg-gta/gtt** command entry may not fit on a single line, especially for range entries with MGTT parameters. If an **ent-gta/gtt** command entry does not fit on one line, try running the command specifying less parameters, and then run **chg-gta/gtt** command(s) to modify the translation with the desired parameters. If the **chg-gta/gtt** command entry does not fit on one line, break the command into multiple commands.

CAUTION: Breaking lengthy commands must be done with care to ensure that the commands remain syntactically and semantically correct.

- **chg-gws-redirect/ent-gws-redirect/rtrv-gws-redirect**

  Hexadecimal digits cannot be specified for the global title address (**gta**) parameter for the **chg-gws-redirect** and **ent-gws-redirect** commands.

  Gateway Screening Redirect Commands

- When the Hex Digit Support for GTT and GMS features are enabled and turne ON, the GMS feature **cannot** process incoming MSUs that contain hexadecimal digits. The GMS feature currently supports **only decimal digits** for CGPA.

NOTE: The Enhanced GSM Map Screening (EGMS) feature can process incoming MSUs that contain either decimal or hexadecimal digits regardless of whether the Hex Digit Support for GTT feature is enabled and on or not.

GSM Map Screening (GMS) and Enhanced GSM Map Screening (EGMS)

- Hexadecimal digits are **not supported** by SEAS as values for the global title address (**gta**) parameter.

  Signaling Engineering and Administration System (SEAS) Commands

High Capacity Multi-Channel Interface Module (HC MIM) (Releases 33.0 34.0)

Description

The High Capacity Multi-Channel Interface Module (HC-MIM) provides access to 8 E1 or T1 ports residing on backplane connectors A and B. Each port or data stream consists of 24 T1 DS0 channels or 31 E1 channels assigned

in a time-division multiplex (TDM) manner. Each channel occupies a unique timeslot in the data stream. Up to 64 signaling links can be assigned to an HC-MIM card.

The HC-MIM card increases the signaling link density in the EAGLE 5 ISS. Because the EAGLE 5 ISS supports a finite number of link interface cards, increasing system capacity or reducing system footprint requires increasing the link density per card. Using fewer cards for a given system capacity yields lower per-link cost.

Configurable temperature alarm thresholds indicate when HC-MIM cards are approaching a temperature that could damage the cards.

64 Link HC-MIM Support

The HC-MIM card operates 8 E1 or 8 T1 port interfaces, with a maximum of 64 signaling links provisioned among the 8 E1 or 8 T1 ports. The HC-MIM card is compatible with existing 2-port E1 cards and E1/T1 MIM cards in the EAGLE 5 ISS shelf for ease in upgrading a live system.

EAGLE 5 ISS software has been modified as follows to support the HC-MIM card:

- All Card, Diagnostic, and Link/Route commands support 8 E1 or 8 T1 ports and up to 64 signaling links per HC-MIM card.
- All Card, Diagnostic, and Link/Route commands support 8 E1 or 8 T1 ports and up to 64 signaling links per HC-MIM card.
- New commands **`rept-stat-e1`** and **`rept-stat-t1`** report the status of all E1/T1 links.
- The E1 and T1 commands support the new channel bridging function. On a HC-MIM card, E1 or T1 ports 1, 3, 5, and 7 (master ports) can be independently channel bridged with their adjacent even-numbered (slave) E1 or T1 ports 2, 4, 6, and 8 to allow non-signaling data pass-through.
- The standard alarms have been extended for the additional E1/T1 ports.
- Alarms for the additional E1/T1 ports can be inhibited.
- For links that are assigned HC-MIM cards and E1/T1 MIM cards that are used as T1 cards, the transmission rate can be either 56 Kbps or 64 Kbps.

Multiple LFS

Multiple LFS tests are supported for HC-MIM cards that are used as T1 cards.

LFS (Link Fault Sectionalization) tests are initiated by the EAGLE 5 ISS or other remote network elements. LFS manual, latching or non-latching tests are used to test the functionality of the link from the EAGLE 5 ISS through multiple channel banks to a remote Network Element. LFS can be run on either SS7ANSI and CCS7ITU Application Class (**`appl=`**) cards. LFS is not supported on E1 cards.

“Manual LFS test” refers to the process of creating a loopback on a signaling link activated by manually enabling the far end for reception and transmission of LFS loopback data. Once the loopback is established, it must be removed by manually disabling LFS on the far end of the signaling link.

“Latching LFS test” and “non-latching LFS test” refers to the process of creating a loopback on a signaling link activated by the transmission of a sequence of pre-defined control codes. Once the loopback is established, it can be removed only by another set of pre-defined control codes.

Latching loopback is activated by the following method:

1. The transmission of a predefined set of Loopback commands. The signaling link test proceeds to step 2 after receiving the command from software to begin sending loopback data.

2. Test data transmitted continuously until a pre-defined loopback code is received to halt transmission.
   The latching loopback on the far end will stop only if the correct command is received from the initiator.Test data transmitted continuously until a pre-defined loopback code is received to halt transmission.

Non-latching loopback is activated by the following method:

1. The transmission of a minimum of 40 bytes of loopback code in multiples of 40 bytes, transmitted continuously. The signaling link test proceeds to step 2 after receiving the command from software to begin sending loopback data.
2. Alternating loopback code and test data is transmitted continuously until a message is received to halt transmission.
   The non-latching loopback test is dropped if every other byte transmitted is not a loopback code.

The EAGLE 5 ISS supports 1024 simultaneously-running system tests.

The EAGLE 5 ISS supports a maximum of 32 remote link elements per SS7 link.

An HC-MIM card that is used as a T1 card supports as many simulataneous tests as there are provisioned links on that card.

Hardware Requirements

The hardware requirements are as follows:

- HC-MIM card
- HIPR cards in each shelf that contains one or more HC-MIM cards
- Fan Assembly for each shelf that contains HC-MIM cards
- Air Management card in each empty slot in a shelf that contains HC-MIM cards
- Fuse and Alarm panel (requires 60 Amp feed)

The HC-MIM card is a dual-slot card that is inserted into an odd-even pair of slots. An HC-MIM card will not go onto the IMT bus if it is inserted into an even-odd pair of slots.

Any shelf that contains one or more HC-MIM cards must include HIPR on both the A and B IMT buses. The shelf must have a fan assembly, and the fan feature bit must be turned on (see the **chg-feat:fan=on** command). If these conditions are not met, any HC-MIM cards installed in the shelf will not go onto the IMT bus.

Limitations

The limitations of the HC-MIM card in the system are as follows:

- The HC-MIM will not support channel cards because it uses all connections on the backplane.
- The HC-MIM does not support CAS on an E1 interface.
- The HC-MIM card is a dual-slot card that is inserted into an odd-even pair of slots. An HC-MIM card will not go onto the IMT bus if it is inserted into an even-odd pair of slots.
- The HC-MIM card can be provisioned as either an LIME1 card type or an LIMT1 card type. An HC-MIM card cannot go onto the IMT bus if HIPR cards are not equipped in the shelf where the HC-MIM card resides.

- The HC-MIM card used as a T1 card supports manually initiated Link Fault Sectionalization (LFS) tests, requiring a craftsperson.
- The final LFS test results are displayed only once, upon test completion.
- There is no notification to the remote network element of Link Fault Sectionalization test initiation or test results.
- LFS test duration is specified in terms of hours, minutes and seconds (hh:mm:ss), and at most 24 hours can be specified.
- The Fuse and Alarm panel requires a 60 Amp feed.

High Speed IMT Packet Router (HIPR) (Releases 33.0 34.0)

Description

The High Speed IMT Packet Router (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. The inter-shelf ring is used to connect the shelves together in the EAGLE 5 ISS. A HIPR card installs into the slot that was used by the HMUX card. HIPR cards must replace HMUX cards in shelves that contain HC-MIM cards.

Hourly Report

A HIPR card reports statistics on each of its 16 ports (one port per card slot in the shelf), the high-speed inter-shelf ring, and the UART. For the hourly report, the HIPR card reports the low speed statistics as an aggregate number. The HIPR statistics and the HMUX statistics are different. The rept-imt-info command displays HIPR and HMUX statistics.

Hardware Requirements

HIPR cards can replace HMUX cards in EAGLE 5 ISS shelves. HIPR cards are required in each shelf that contains one or more HC-MIM cards.

Limitations

The accuracy of statistics collected, maintained, and reported by HIPR in the HEM task are limited by the sample rate of the statistics. There are no count values associated with the sampling of the number of times a particular (recoverable) error has occurred since the last (500mS) sampling period, but simply that one or more of a particular error condition has been detected. Subsequently, a count value is incremented by one. This affects the granularity of the error counts, but not their usefulness in diagnosing IMT problems. An initial sample rate of 500mS has been chosen to minimize the number of accesses by the StrongARM processor to the FPGA via the SlowPort Bus. This is because each access via the SlowPort bus to the FPGA blocks the microengines' access to SRAM, because the SRAM and SlowPort are shared buses.

High Speed Master Timing (Release 26.0)

Overview

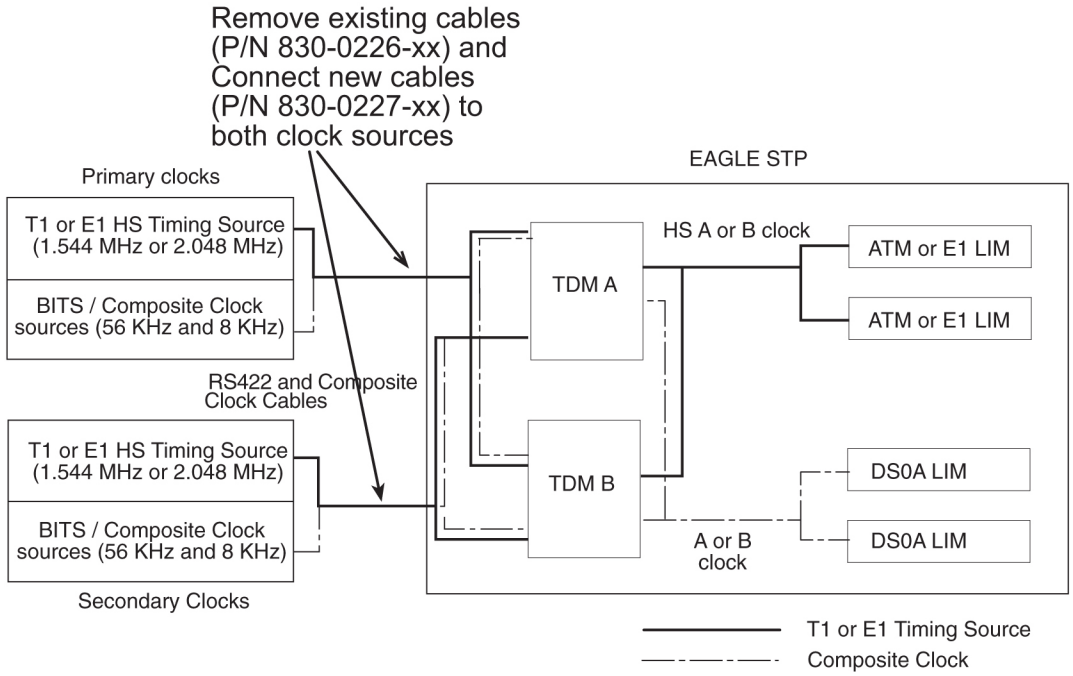
The High-Speed (HS) Master Timing feature offers a new mode of operation that allows a high-speed capable (T1 or E1 rate) Link Interface Module (LIM) installed in an EAGLE STP to receive its transit timing reference directly from an external high-speed master clock source, instead of slaving to the timing information contained in the received data. The timing information is encoded into the T1 or E1 transmitted data stream to synchronize downstream equipment.

NOTE: The EAGLE terminal output screens refer to the composite clocks as Building Integrated Timing Source (BITS) clocks. In this document references to BITS and composite clocks are used interchangeably.

The HS master clock signals are encoded with the data stream originated or received by the EAGLE STP, thus assuring synchronized data transmission. The HS Master Timing feature is integrated into the programmable logic contents on the Terminal Disk Module (TDM) card and the PROM of the MAS communications application processor (MCAP) card. The HS Master Timing feature requires updating these cards and the redundant TDM/MCAP card pair to specified release levels. Since a TDM/MCAP card pair makes up the Maintenance and Administration Subsystem Processor (MASP), this card pair is also referred to as MASP in this manual.

The composite clock cables connect the site's composite (BITS) clocks with the EAGLE STP control shelf. Implementation of the HS Master Timing feature requires the replacement of both composite clock cables with two new HS master clock cables (RS422 compatible) on control shelf backplane (P/N 850-0330-05/06 and later). The following figure illustrates HS master and composite clock cabling with control shelf backplane (P/N 850-0330-05/06 or later).

Figure 3-6. HS Master Timing Concept Control Shelf Backplane (P/N 850-0330-05/06 or later)



Implementation of the HS Master Timing feature requires the addition of two HS master clock cables on control shelf backplane (P/N 850-0330-03/04). The following figure illustrates the HS master timing concept for control shelves with backplane (P/N 850-0330-03/04).

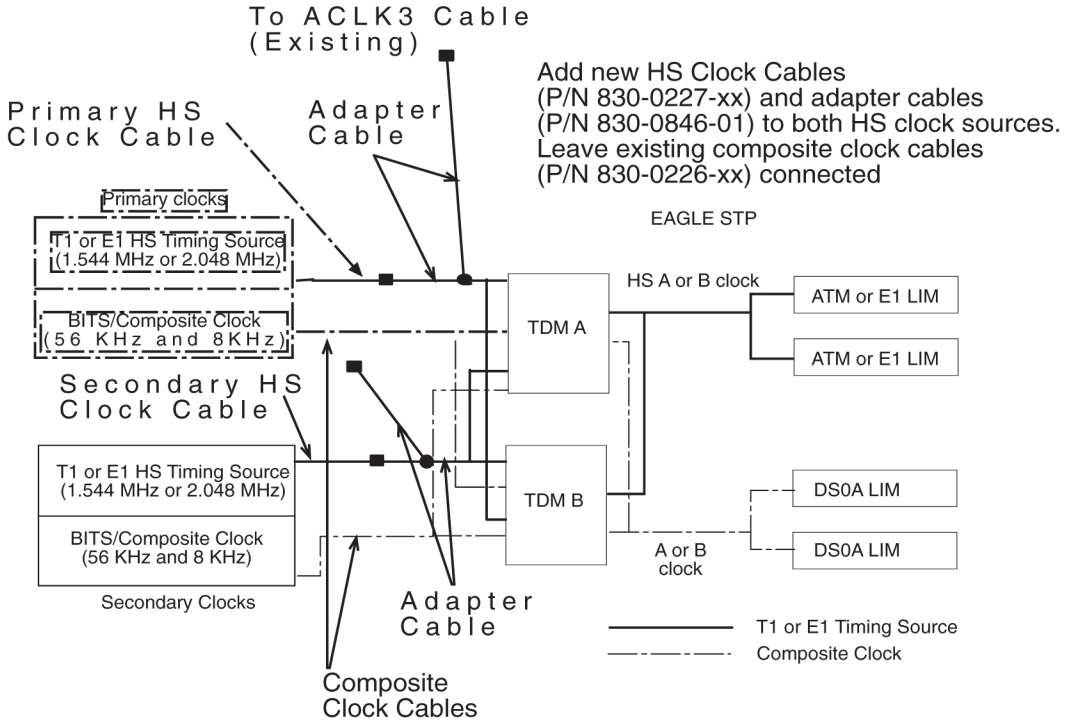
Only ATM LIM cards or E1 LIM cards can be configured or reconfigured for the HS Master Timing feature. Once the baseline hardware requirements for the HS Master Timing feature have been met:

- physically install an ATM card, add the card to the system database, and enable it for the HS Master Timing feature (ent-slk:atmtsel=external); or

- physically install an E1 LIM card, add the card to the system database, and enable it for the HS Master Timing feature (ent-e1:e1tsel=internal).

Reconfigure any existing ATM LIM card or E1 LIM cards to use the HS Master Timing feature. LIM cards that will continue using the composite clock will not require any changes to the card provisioning.

Figure 3-7. HS Master Timing Concept using Control Shelf Backplane (P/N 850-0330-03/04)



Feature Concept

Digital networks require accurate timing sources to maintain the integrity of data transmission. Utilizing high-speed clocking provides improved data synchronization capabilities.

Master Clock

The master clock is the source of timing signals and uses these signals for network synchronization. For the HS Master Timing feature, the site's master clock can be a T1 (1.544 MHz) or E1 (2.048 MHz) rate clock source on RS422 compatible cable.

System Clocks

The EAGLE STP system clock is derived from the site's master clock source, which is often the site's holdover clock. The EAGLE STP typically connects to the site's composite clocks signals, a primary and secondary clock signal for redundancy. The EAGLE STP's internal composite clock distributes the signals to all cards at a combined rate of 56 KHz and 8 KHz.

By enabling the HS Master Timing feature on high-speed capable ATM LIM cards or E1 LIM cards, the cards can take their high-speed clock reference directly from the external HS master clock source, such as the master clock source available at the site.

The external HS clock source provides the EAGLE STP with a second system clock. The EAGLE STP can now connect to

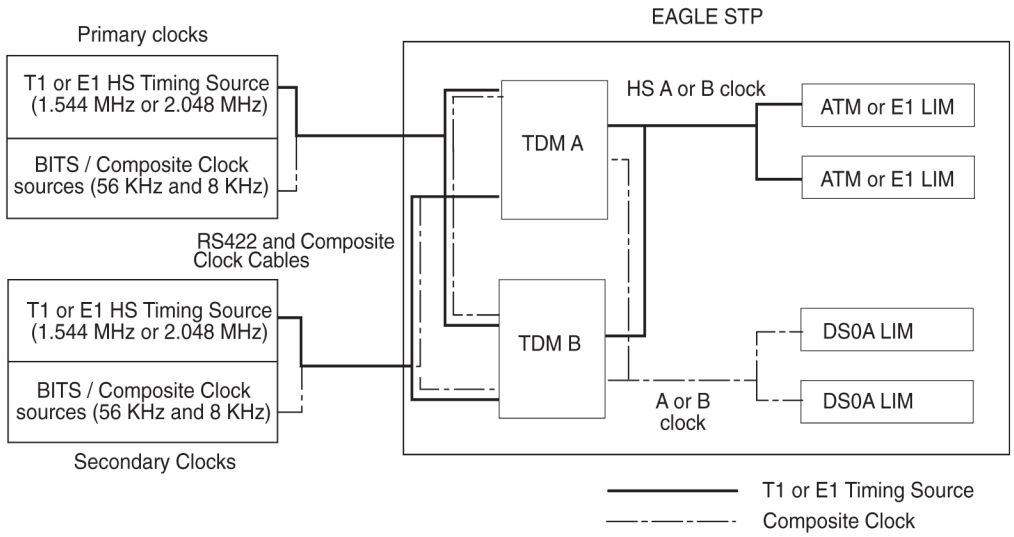
- two 64 KHz composite clocks (primary and secondary clocks) and
- two T1 (1.544 MHz) or E1 (2.048 MHz) rate clock sources (primary and secondary clocks).

With both system clocks, the EAGLE STP will distribute the HS clock signals with the composite clock signals. The EAGLE STP distributes the clock signals to each frame. All shelves, both extension shelves and control shelves, provide *clock in* and *clock out* connections.

The EAGLE STP connects to its primary and secondary system clocks through connectors on the backplane of the control shelf. The backplane connectors are labeled *Primary BITS* and *Secondary BITS* . Both primary and secondary clock signals are sent to each TDM card. The TDM cards selects between the primary and secondary signals to provide system clocks (A clocks and B clocks) to the rest of the EAGLE. ATM LIM cards use a T1 HS master clock source, E1 LIM cards use a E1 HS master clock source, and DS0A LIMs use the internal composite clock sources. Each ATM or E1 LIM card selects between the HS master A or B clock source. Each DS0A LIM selects between the A or B composite clock source. The following figure shows system clock use by LIM cards.

NOTE: An STP can be configured for either a T1 (1.544 MHz) or E1 (2.048 MHz) HS master clock source, but not both.

Figure 3-8. System Clocks



TDM Card

EAGLE operation is controlled by Maintenance and Administration Subsystem (MAS) cards. MAS cards consist of two MAS communications application processor (MCAP) cards, two Terminal Disk Module (TDM) cards, and one Maintenance Disk and Alarm (MDAL) card. The TDM card contains the fixed disk drive, the terminal processor for 16 serial I/O ports, and an interface to the MDAL card. The MDAL card contains the removable cartridge drive and alarm logic. Prior to the implementation of the HS Master Timing feature, the TDM card directly supported all of the EAGLE timing functions by distributing composite clock signals to the system.

Internal Clock Defaults

The TDM card generates an internal composite clock when no external composite clock is present on the primary or secondary inputs. If no T1 or E1 high speed clock, is provided, the high-speed system clocks to the LIM cards become inactive.

The TDM card can independently select between primary and secondary high-speed (HS) master clock and primary and secondary composite clock (BITS clock), and switches automatically to the idle clock when one of the active clocks fail.

The following table lists the various clocking modes resulting from the clock inputs received by the TDM card and the resulting clock output to the LIM card.

Table 3-8. Clock Signal Modes

Site Clock Availability (Input to TDM cards)	Clock Distribution to EAGLE (Possible TDM Card Outputs)	Clock Selection by LIM
Primary **and/or** Secondary HS Master Clock Available	TDM A and B HS CLK available	Software selects A or B HS clock
	TDM A HS CLK unavailable	HW selects B HS clock
	TDM B HS CLK unavailable	HW selects A HS clock
	TDM A and B HS CLK unavailable	No HS clocks available
Primary **and** Secondary HS Master Clock Unavailable	TDM A and B HS CLK unavailable	No HS clocks available
Primary **and/or** Secondary BITS Clock Available	TDM A and B BITS CLK available	Software selects A or B composite clock
	TDM A BITS CLK unavailable	HW selects B composite clock
	TDM B BITS CLK unavailable	HW selects A composite clock
	TDM A and B BITS CLK unavailable	No clocks available (runs on internal)
Primary **and** Secondary BITS Clock Unavailable	TDM A and B BITS CLK unavailable	No clocks available (runs on internal)
Note: “Unavailable” means the clock is not valid or not present.		

For a timing source, ATM LIM cards or E1 LIM cards use the system clock required by their card type and the Generic Program Load (GPL) installed on the card. For detailed information on configuring ATM or E1 cards, refer to the *Database Administration Manual - SS7* of your current documentation suite.

MCAP Card

To support the HS Master Timing feature, a new Programmable Read-Only Memory (PROM) is required for the MCAP card (containing a new Clock LCA bit file in the IMT quadrant of the PROM), new interprocessor message transport (IMT) GPL for LIM cards (SS7ANSI, CCS7ITU, SS7GX25, STPLAN, GLS, SCCP), BPHCAP GPL for High Capacity Application Processor (HCAP) (ATMANSI) cards, BPDCM GPL for DCM cards, and a new OAM GPL.

Administration

The HS Master Timing feature allows a high-speed capable (T1 or E1 rate) Link Interface Module (LIM) installed in an EAGLE STP to receive its transit timing reference directly from an external high-speed master clock source, instead of slaving to the timing information contained in the received data. The high-speed master timing feature is enabled through the provisioning of at least one high speed link (ATM or E1 LIM card). At that time, the GPL required for the feature is downloaded from the MCAP card to the TDM card. For provisioning high speed links, the following commands have been changed to support master timing:

- **REPT-STAT-CARD:MODE=FULL**
- **REPT-STAT-CLK**
- **ENT-SLK**
- **RTRV-SLK**
- **ENT-E1**
- **CHG-E1**

Refer to the *Commands Manual* for current usage information.

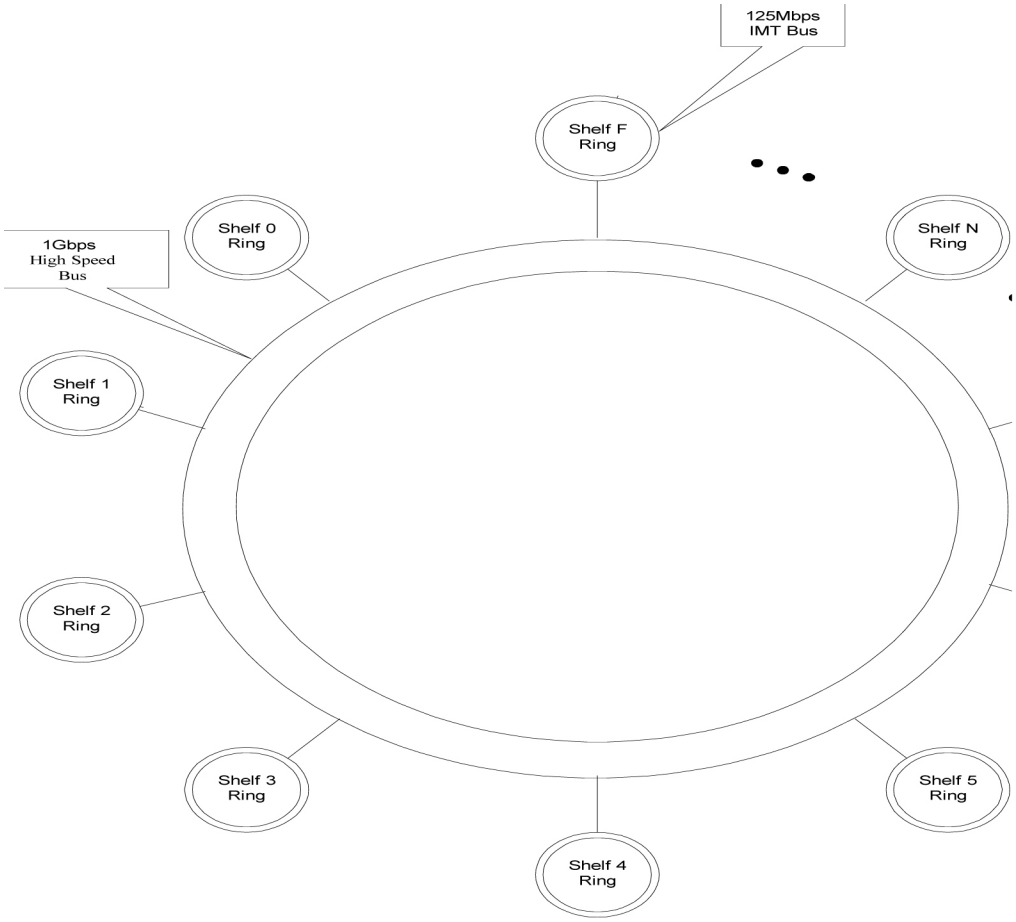
High-Speed Multiplexer (HMUX) (Release 27.2)

The High-Speed Multiplexer (HMUX) supports the EAGLE Large System feature, which expands the number of links supported by the EAGLE STP. The HMUX enhances the IMT bus by introducing a new 1Gb/sec inter-shelf bus bandwidth. The intra-shelf bus data rate will remain the same at 125Mb/sec.

The HMUX feature also enhances IMT performance by transmitting data between shelves only when it is necessary. Traffic between EAGLE cards on the same shelf will be allowed to remain on the shelf IMT, and will not be required to transmit between shelves. Traffic between shelves will not be required to pass onto an intra-shelf IMT bus if it is not necessary.

Introduction of the HMUX transforms each EAGLE IMT bus from a single ring topology running at 125Mbps, to a central primary ring operating at 1Gb/sec, with a maximum of sixteen secondary rings running at 125Mbps. Refer to **Figure 3-9** .

Figure 3-9. HMUX Ring Topology



Hardware Requirements

Support of this feature requires the following hardware:

Hardware	Assembly Part Number
HMUX	870-1965-01 or later
TDM	870-0774-10 or later
Control Shelf *and*	870-2321-01 or later
Adapter cable	830-0857-01
MCAP-256 w/ special PROM with FPGA logic files for new ECAM CLOCK LCA	870-1307-07

Upgrade Considerations

The following EAGLE tables will be modified/converted/created as part of the upgrade for this feature:

- STPOPTS.TBL/BKP
- (T)BPHMUX.ELF

Holdover BITS Clock Support (Release 21.0)

The holdover BITS clock is an optional external device that provides clock input to the EAGLE for a specified period of time when the BITS clock fails. The holdover BITS clock resides in the OAP frame of the EAGLE. This feature adds additional outputs on the control shelf to control the holdover BITS clock. The holdover BITS clock is a Telecom Solutions Digital Clock Distributor, DCD-523. The holdover BITS clock maintains clock synchronization for 15 seconds. This meets the Bellcore requirement as specified in TR-NWT-001244. When used with the EAGLE, the holdover BITS clock contains the following cards:

- 2 CI cards - clock inputs A and B
- 2 ST3E cards - clocks A and B
- 2 TOCA cards in card locations TO1 and TO2 - outputs to the EAGLE

The outputs of the TOCA cards are connected to a wire wrap panel mounted on top of the holdover BITS clock. The clock inputs on the EAGLE control shelf are connected to the wire wrap panel.

Idle Terminal Port Logout (Release 21.0)

The EAGLE keeps track of how long a login session has remained idle. Every minute, the EAGLE examines all of the login sessions currently active. Whenever a login session has been idle (idle is defined as no input from the user) for more than the maximum allowable time (provisionable on a per-port basis), the session is ended by forcing an automatic logout.

The EAGLE issues a message to the scroll area of all system administrator terminals whenever a logout occurs. A slightly different message is issued when an idle time logout occurs:

```
User xxxxxxxx auto logged out (idle time exceeded) on port yy.
```

where xxxxxxxx is the user ID that was logged off and yy is the port that the user ID was using before the logoff. In addition to being issued to all system administrator terminals, this same message is sent to the scroll area of the idle terminal that is being logged out.

The idle time logout is designed so that it will not interfere with existing or planned EAGLE features that might falsely or undersirably trigger the idle time logout:

- The idle time logout feature is suspended for a port while that port is in the process of transferring a file.
- SEAS ports are not affected by idle port logout. SEAS ports are unique in that no login is required in order to access the EAGLE with a SEAS port, and thus there is no login session whose idle time can be monitored.

The maximum idle time value can be configured on a per-port basis; different maximum idle times can be established for each port, using the **tmout** parameter of the **chg-trm** command.

The system administrator is allowed to set a port's idle timeout value to 0. This indicates that a user ID may remain idle on the port indefinitely without being automatically logged off due to idle time expiration.

The system default value for the **tmout** parameter is 30 minutes.

The monitoring of a terminal's idle time (**tmout**) and the automatic logout function only applies to terminal types VT320 (**type=vt320**), KSR, (**type=ksr**), and SCCS (**type=sccs**). The **tmout** parameter can be specified with other terminal types, but it will have no effect.

During a Kermit file transfer, the idle time monitoring is temporarily suspended and the port's idle time is reset to 0 and does not resume until after the file transfer completes, even though there is no user input from the terminal during the file transfer operation. This prevents a terminal from being automatically logged off immediately after a file transfer completes. For example, if the value of the **tmout** parameter for a terminal is 1 minute and a file transfer is performed that takes 5 minutes. The terminal idle monitor is suspended during the file transfer and does not resume until the file transfer operation completes. Therefore, the terminal is logged off 1 minute after the file transfer completes unless there is additional user input.

The idle port logout occurs even if a port is in the process of executing a command when the idle threshold is exceeded. For example, if the **chg-pid** command is executed and the user never supplies any input to the **Enter Old Password :** prompt, when the terminal's idle time threshold is exceeded, the terminal is logged off and the command that was in progress is aborted.

IDP Screening for PrePaid (Release 34.3)

Description

The IDP Screening for Prepaid feature screens GT-routed messages resulting from voice and text calls from a prepaid subscriber to determine whether the subscriber has a "24/7 Call and Text Unlimited" or a "24/7 Text Unlimited" calling plan and then routes the call accordingly.

For a voice or text (short message) call originated by a prepaid subscriber, the serving MSC formulates an INAP IDP message which is destined for a prepaid engine that checks the subscriber's credit status. The IDP Screening for PrePaid feature causes EAGLE 5 SAS to intercept the IDP message and determine whether the subscriber has one of the calling plans referenced above.

Voice and text calls are identified by a predefined Service Key. The value assigned to the Service Key is set by an originating MSC when the call reaches an Intelligent Network (IN) trigger. These values indicate whether the subscriber has the "24/7 Call and Text Unlimited" or "24/7 Text Unlimited" calling plan.

If the subscriber has one of the calling plans, the EAGLE 5 SAS determines whether the call is an in-network call (a call from one subscriber to another belonging to the same network). For an in-network call, the EAGLE 5 SAS returns an INAP Continue message to instruct the MSC to bypass the credit check and continue the call. If the call is not an in-network call, EAGLE 5 SAS routes the calls to the prepaid engine to have the credit check performed.

If the call originates from a non "24/7 Call and Text Unlimited" or non "24/7 Text Unlimited" prepaid subscriber, the EAGLE 5 SAS routes the IDP message to its intended destination.

This feature requires a feature access key.

Hardware Requirements

- After the IDP Screening for Prepaid feature is turned on, no TSM SCCP cards can be provisioned.

- Only DSM cards are used with the IDP Screening for Prepaid feature.

IETF M3UA for "A" Link Connectivity (Release 28.1)

Description

To connect to a variety of IP enabled SCP's, the VXi Softswitch, or other IP enabled network elements, the EAGLE STP and IP ^{7} Secure Gateway must use industry standard protocols. In the IETF Signaling Transport (SIGTRAN) model, SS7 MTP3-User Adaptation Layer (M3UA) is a User Adapter layer which resides on top of SCTP, necessary for connection to IP enabled network elements.

Hardware Requirements

This feature requires a SSEDCM (Single Slot Enhanced DCM).

IETF M3UA Support including IETF SUA (IP^{7} Release 5.0)

Description

Although widely accepted throughout the industry, the TALI protocol is not a standard adapter layer protocol at this time. To interoperate with various vendors, the adapter layer protocols produced by the IETF must be implemented on the Secure Gateway. The concepts defined in the IETF drafts will provide a building block for better support of fail-over scenarios that can be implemented in TALI.

The M3UA Layer is designed to fit the need for signaling protocol delivery from an SS7 Signaling Gateway (SG) to a Media Gateway Controller (MGC) or IP-resident Database. The layer is expected to meet the following criteria:

- Support for the transfer of all SS7 MTP3-User Part messages (for example, ISUP, SCCP, TUP, and so forth)
- Support for the seamless operation of MTP3-User protocol peers
- Support for the management of SCTP transport associations and traffic between a SG and one or more MGCs or IP-resident Databases
- Support for MGC or IP-resident Database process fail-over and load-sharing
- Support for the asynchronous reporting of status changes to management.

The SUA Layer is designed to fit the need for the delivery of SCCP-user messages (MAP and CAP over TCAP, RANAP, and so forth) and new third generation network protocol messages over IP between two signaling endpoints. Consideration is given for the transport from an SS7 Signaling Gateway (SG) to an IP signaling node (such as an IP-resident Database). This protocol can also support transport of SCCP-user messages between two endpoints wholly contained within an IP network.

Refer to the *Database Administration Manual Features* for current information on this feature.

New Hardware

Same as IETF SCTP.

Upgrade Considerations

Same as IETF SCTP.

Limitations

Same as IETF SCTP.

IETF Protocol Update (Release 28.1) (IP^7 Release 6.0)

Description

Since the introduction of the IETF Sigtran protocols in IP ^{7} Secure Gateway Release 5.0, the IETF has created newer versions of these protocols. This feature updates the IP ^{7} Secure Gateway and EAGLE IPLIMx implementation of these protocols to the current revisions.

NOTE: This is a non-orderable feature required for the three IETF Connectivity features and the IPLIM Protocol Support Enhancement feature.

Hardware Requirements

This feature requires a SSEDCM (Single Slot Enhanced DCM).

IETF SCTP for "A" Link Connectivity (Release 28.1)

Description

To connect to a variety of IP enabled SCP's, the VXi Softswitch, or other IP enabled network elements, the EAGLE STP and IP ^{7} Secure Gateway must use industry standard protocols. In the IETF Signaling Transport (SIGTRAN) model, SCTP is the transport layer for all the User Adapter layers.

SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP. It offers the following services to its users:

- acknowledged error-free non-duplicated transfer of user data,
- data fragmentation to conform to discovered path MTU size,
- sequenced delivery of user messages within multiple streams, with an option for unorder delivery of individual user messages,

- optional bundling of multiple user messages into a single SCTP packet, and
- network-level fault tolerance through supporting of multi-homing at either or both ends of an association.

The development of SCTP was necessitated by limitations within TCP. TCP has performed immense service as the primary means of reliable data transfer in IP networks. However, an increasing number of recent applications have found TCP too limiting, and have incorporated their own reliable data transfer protocol on top of UDP. The limitations which users have wished to bypass include the following:

- TCP provides both reliable data transfer and strict order-of-transmission delivery of data. Some applications need reliable transfer without sequence maintenance, while others would be satisfied with partial ordering of the data. In both of these cases the head-of-line blocking offered by TCP causes unnecessary delay.
- The stream-oriented nature of TCP is often an inconvenience. Applications must add their own record marking to delineate their messages, and must make explicit use of the push facility to ensure that a complete message is transferred in a reasonable time.
- The limited scope of TCP sockets complicates the task of providing highly available data transfer capability using multi-homed hosts.
- TCP is relatively vulnerable to denial of service attacks, such as SYN attacks.

The transport of PSTN signaling across the IP network is an application for which all of these limitations of TCP are relevant.

This feature is available on the IPGWx GPL and IPLIMx GPL in both the EAGLE STP and IP ^{7} Secure Gateway products in Release 28.1 of the EAGLE STP, and IP ^{7} Secure Gateway Release 5.0.

SCTP is a protocol designed to operate on top of a non-reliable protocol such as IP, but yet provide a reliable data delivery to the SCTP user.

Hardware Requirements

This feature requires a SSEDCM (Single Slot Enhanced DCM).

IETF SCTP Support (IP^{7} Release 5.0)

Description

SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP. It offers the following services to its users:

- Acknowledged error-free non-duplicated transfer of user data
- Data fragmentation to conform to discovered path MTU size
- Sequenced delivery of user messages within multiple streams, with an option for out-of-order-of-arrival delivery of individual user messages

- Optional bundling of multiple user messages into a single SCTP packet
- Network-level fault tolerance through supporting of multi-homing at either or both ends of an association

The development of SCTP was necessitated by limitations within TCP. TCP has performed immense service as the primary means of reliable data transfer in IP networks. However, an increasing number of recent applications have found TCP too limiting, and have incorporated their own reliable data transfer protocol on top of UDP. The limitations which users have wished to bypass include the following:

TCP provides both reliable data transfer and strict order-of-transmission delivery of data. Some applications need reliable transfer without sequence maintenance, while others would be satisfied with partial ordering of the data. In both of these cases the head-of-line blocking offered by TCP causes unnecessary delay.

The stream-oriented nature of TCP is often an inconvenience. Applications must add their own record marking to delineate their messages, and must make explicit use of the push facility to ensure that a complete message is transferred in a reasonable time.

The limited scope of TCP sockets complicates the task of providing highly available data transfer capability using multi-homed hosts.

TCP is relatively vulnerable to denial of service attacks, such as SYN attacks.

The transport of PSTN signaling across the IP network is an application for which all of these limitations of TCP are relevant.

Refer to the *Database Administration Manual - Features* for the current implementation of this feature.

New Hardware

Hardware support is required for implementation of the IETF Adapter Layer Support feature. Starting with this feature, the new EDCM card is introduced. Refer to the *NSD Hardware Manual* for current information on this card.

These differences in memory are the main reasons for hardware support. We are required to make both socket/association provisioning and card loading decisions differently based on the card type.

Upgrade Considerations

This feature has a unique upgrade consideration than other features in that the specification for which the feature is being developed is not "frozen" until after the feature is complete. This raises the issue of incompatibility between the final specification and this feature. Since the specification is the initial version for the adapter layer, the protocol has defined the version number to be fixed to 1. Therefore, it is not possible to modify the version number from this feature perspective. Another issue is that the impact of any specification changes after this feature is completed is not necessarily impacting the compatibility of the protocol. It is expected that the approved version of revision 1 of the adapter layers is supported at some period in time and that by upgrading the software solves compatibility issues. Another solution is to use a new adapter layer index for the pre-official version of the protocol and convert and fielded releases to the new adapter layer index. The ASPLOG PASS command shows the version of the UA adapter supported. The problem with supporting a revision of a draft is a later revision may be incompatible. The drafts make no provision for support between revisions so a revision 3 of version 1 SUA can't be differentiated between revision 6 of version 1 SUA.

Limitations

The memory requirements for an association are greater than for a socket. Because of this, more associations may be provisioned on the EDCM card.

Not only are socket/association limits based on memory, so is the ratio of associations to sockets. This ratio known as the "trade ratio" defines the number of sockets, which are equivalent to one association with respect to memory consumption.

IETF SUA for “A” Link Connectivity (Release 28.1)

To connect to a variety of IP enabled SCP's, the VXi Softswitch, or other IP enabled network elements, the EAGLE STP and IP ^{7} Secure Gateway must use industry standard protocols. This feature implements the SCCP User Adaptation Layer (SUA). SUA is an adaptation layer protocol, similar to TALI, which transports SCCP User level protocols.

The SUA Layer was designed to fit the need for the delivery of SCCP-user messages (MAP & CAP over TCAP, RANAP, etc.) and new third generation network protocol messages over IP between two signaling endpoints. Consideration is given for the transport from an SS7 Signaling Gateway (SG) to an IP signaling node (such as an IP-resident Database). This protocol can also support transport of SCCP-user messages between two endpoints wholly contained within an IP network. The layer is expected to meet the following criteria:

- Support for transfer of SS7 SCCP-User Part messages (e.g., TCAP, RANAP, etc.).
- Support for SCCP connectionless service.
- Support for SCCP connection oriented service.
- Support for the seamless operation of SCCP-User protocol peers
- Support for the management of SCTP transport associations between a SG and one or more IP-based signaling nodes).
- Support for distributed IP-based signaling nodes.
- Support for the asynchronous reporting of status changes to management.

Hardware Requirements

This feature requires a SSEDCM (Single Slot Enhanced DCM).

IETF SUA Support (Release 34.0)

Description

The IETF SCCP-User Adaptation (SUA) Layer Request for Comment (RFC) feature enhances IPGWx GPL software to support RFC with the following feature highlights:

- Replaces Draft Version 3 support on the IPGWx GPL with SUA RFC.
- Provides support for SCCP Connectionless messages via SUA CLDT and CLDR. Connection oriented messages are not supported.
- Provides support for SUA Signaling Network Management Messages.

Hardware Requirements

An EDCM (single-slot) P/N 870-2372-01 Rev E is required for SUA RFC.

Refer to the hardware baseline of this release.

Limitations

- The version of SUA implemented in this release is NOT backward compatible with the SUA version currently available on EAGLE 5 SAS releases.
- Only the Connections Message transfer part of the SUA protocol is supported for class 0 and class 1 SCCP messages.
- To remove a routing context from a routing key, the routing key must be deleted and re-entered.

Implementation of SNMP Agent (IP^7 Release 2.0)

Overview

This feature implements a Simple Network Management Protocol (SNMP) agent on each DCM that runs an **`ss7ipgw`** or **`iplim`** general program load (GPL). SNMP is an industry-wide standard protocol used for network management. SNMP agents interact with network management applications called Network Management Systems (NMSs).

Supported Managed Object Groups

The SNMP agent maintains data variables that represent aspects of the DCM card. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups. The following table shows the groups that IP ^{7} release 2.0 supports.

Table 3-9. SNMP Object Groups Supported by IP^7 Release 2.0

Group Name	Description	Contents
system	Text description of agent in printable ASCII characters	System description, object identifier, length of time since reinitialization of agent, other administrative details
interfaces	Information about hardware interfaces on the DCM	Table that contains for each interface, speed, physical address, current operational status, and packet statistics

Group Name	Description	Contents
ip	Information about host and router use of the IP	Scalar objects that provide IP-related datagram statistics, and 3 tables: address table, IP-to-physical address translation table, and IP-forwarding table
icmp	Intranetwork control messages, representing various ICMP operations within the DCM	26 scalar objects that maintain statistics for various Internet Control Message Protocol (ICMP) messages
tcp	Information about TCP operation and connections	14 scalar objects that record TCP parameters and statistics, such as the number of TCP connections supported and the total number of TCP segments transmitted, and a table that contains information about individual TCP connections
udp	Information about UDP operation	4 scalar objects that maintain UDP-related datagram statistics, and a table that contains address and port information
snmp	Details about SNMP objects	30 scalar objects, including SNMP message statistics, number of MIB objects retrieved, and number of SNMP traps sent

Supported SNMP Messages

The SNMP agent interacts with up to two NMSs by:

- Responding to *Get* and *GetNext* commands sent from an NMS for monitoring the DCM.
- Responding to *Set* commands sent from an NMS for maintaining the DCM and changing managed objects as specified.
- Sending *Trap* messages to asynchronously notify an NMS of conditions such as a link going up or down. *Trap*s provide a way to alert the NMS in a more timely fashion than waiting to for a *Get* or *GetNext* from the NMS. In this release, only the following traps are supported:
  - *linkUp*, sent when one of the ports on the DCM initially comes up or recovers from a previous failure
  - *linkDown*, sent when one of the ports on the DCM fails

Deviations from SNMP Protocol

The following table shows how IP ^{7} release 2.0 deviates from the standard SNMP protocol definition.

Table 3-10. Deviations from SNMP Protocols

Group	Variable Name	Usage	Deviation
system	sysContact	Text identification of contact information for agent	Cannot be set by *Set* command; may be set only by **`chg-sg-opts`** command.
	sysLocation	Physical location of agent	Cannot be set by *Set* command; internally set using configuration data already available; set to

Group	Variable Name	Usage	Deviation
			<CLLI>-<slot of DCM>
	sysName	Administratively assigned name for agent	Cannot be set by *Set* command; internally set using configuration data already available; set to <CLLI>-<slot of DCM>
interface	ifAdminStatus	Desired state of the interface	Cannot be set by *Set* command (to ensure that an NMS does not disrupt SS7 traffic by placing an IP interface in a nonoperable state)
ip	ipForwarding ipDefaultTTL ipRoute Dest ipRouteIfIndex ipRouteMetric1-5 ipRouteNextHop ipRouteType iprouteAge ipRouteMask	IP route-specific values	Cannot be set by *Set* command
	ipNetToMediaIfIndex ipNetToMediaPhysAdress ipNetToMediaNetAddress ipNetToMediaType	IP-address specific information	Can be set by *Set* command, but not saved across DCM reloads
tcp	tcpConnState	State of a TCP connection	Cannot be set by *Set* command
snmp	snmpEnableAuthenTraps	Indicate whether agent is permitted to generate authentication failure traps	Cannot be set by *Set* command

Improved Routing Management (Release 20.0)

This feature allows the EAGLE to use E-links, allows the user to make link type assignment for display purposes, and provides two new procedures for handling transfer-prohibited (TFP) network management messages.

Before beginning to route traffic on a non-normal route, the EAGLE sends a TFP network management message toward the affected destination. When an STP begins using a lower priority route through another STP to its final destination, a TFP network management message is sent to all accessible adjacent STPs that provide a route to a higher priority. These two handling procedures prevent circular routing.

This feature also uses the ability to enable or disable the broadcast of TFP network management messages. This capability can be administered per linkset or per destination, and has no effect on the EAGLE's method of responding to TFP network management messages.

IMT Fault Isolation (Release 22.0)

IMT fault isolation increases the EAGLE's ability to diagnose problems on the IMT bus with:

- Improvements to the EAGLE's existing diagnostic and reporting mechanisms.
- Additional diagnostics and reports to enable the user to detect IMT faults and to isolate the cause of those faults to the card or bus level.

IMT fault isolation procedures are designed to be used after a problem has been detected. They can be used to solve these problems:

- Isolate IMT bus failures to the bus segment or individual card.
- Identify intermittent failures and the responsible cards.

There are two types of IMT bus errors, transient and nontransient. Transient errors cause packet loss or data corruption, but the cards are still connected to the IMT bus. Nontransient errors cause the cards to be disconnected from the IMT bus. The IMT fault isolation procedures detect nontransient errors.

Nontransient errors fall into two categories:

1. Errors that cause all cards to be isolated from one of the IMT buses (the IMT bus is out of service)
2. Errors that cause a subset of the cards (typically a single card) to be isolated from one of the IMT buses (the IMT bus remains in service).

When an IMT bus is out of service, this feature determines the location and probable cause of the failure. Those faults that are card-specific are isolated to the card. Faults that cannot be isolated to a specific card are isolated to the segment of the IMT bus on which they occur. A segment is identified by the two cards that are its endpoints. No attempt is made to isolate a particular component below the card level. The card is a field replaceable unit.

IMT Subsystem Alarms (Release 20.0)

With this feature, the EAGLE displays minor, major, or critical alarms should one or more of the buses in the Interprocessor Message Transport (IMT) subsystem fail. The alarm levels in the individual buses determine the overall alarm for the IMT subsystem.

INAP-based Number Portability (INP) (Release 26.05)

Description

Throughout the world, wireline and wireless operators are receiving directives from national regulators to support service provider number portability in their networks. This allows for subscribers to change to a new service provider while retaining their phone number. In Europe and other parts of the world, with the exception of North America, wireline providers are planning to implement this via the use of an IN (Intelligent Network)-based solution using the INAP (IN Application Part) protocol. This is in line with developed ITU Number Portability supplements. ETSI standards for Mobile Number Portability also define an IN-based solution to be used at the operator's discretion.

While the advent of number portability is good news for consumers, it presents many challenges for network operators. Tekelec's INAP-based Number Portability (INP) feature is intended to minimize those challenges for network operators, while enabling them to efficiently meet their regulatory obligations.

Refer to the *Feature Manual - INP* for the current details on this feature.

Hardware Requirements

INP requires the use of the Multi-Purpose Server (MPS) hardware to host the EAGLE Provisioning Application Processor (EPAP) software. Refer to the *NSD Hardware Manual* for the current hardware information.

Increase Gateway Screening Screen Sets to 255 (Release 22.0)

In Release 22.0, the total number of gateway screening screen sets that can be configured in the database has been increased from 64 to 255. When a screening table is changed, this feature displays the following scroll area message showing the number of screen sets affected by changing a screening table. There is no limit to the number of screensets a screening table can be a member of.

```
Notice: The number of screensets affected is N.
```

Where **n** is the number of affected screen sets.

Increase GTT Entries per TT to 200,000 (Release 29.0)

Description

This feature increases the number of Global Title Table entries per Translation Type or GTT Set up to 200,000. The GTT Entries Increase per TT to 200,000 Feature does not have any software controls, and therefore no feature keys. The feature is automatically included as part of EAGLE 29.0/IP ^{7} Secure Gateway 7.0, provided that all SCCP cards are TSMs or DSMs.

Hardware Requirements

To support this feature, all SCCP cards in the system must be TSMs or DSMs.

Increase in Time Zones (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)

Description

The Increase in Time Zones feature increases the number of time zones available for EAGLE administration; see the following table.

Table 3-11. New Supported Time Zones

Time Zone	Abbrev.	Offset from GMT (hrs.)
Newfoundland Daylight Time	NDT	- 2.5
Newfoundland Standard Time	NST	- 3.5
Brazil Standard Time	BRA	- 3
Alaska Daylight Time	AKDT	- 8
Alaska Standard Time	AKST	- 9
Universal Time Coordinated	UTC	0
British Summer Time	BST	+ 1
Western European Summer Time	WEST	+ 1
Central European Time	CET	+ 1
Central European Summer Time	CEST	+ 2
French Winter Time	FWT	+ 1
French Summer Time	FST	+ 2
Middle European Time	MET	+ 1
Middle European Summer Time	MEST	+ 2
Eastern European Time	EET	+ 2
Eastern European Summer Time	EEST	+ 3
South African Standard Time	SAST	+ 2
Moscow Time	MSK	+ 3
Moscow Summer Time	MSD	+ 4
India Standard Time	IST	+ 5.5
India Daylight Time	IDT	+ 6.5
China Coast Time	CCT	+ 8
Republic of Korea	ROK	+ 9
Australian Western Standard Time	AWST	+ 8
Australian Western Daylight Time	AWDT	+ 9
Australian Central Standard Time	ACST	+ 9.5
Australian Central Daylight Time	ACDT	+ 10.5
Australian Eastern Standard Time	AEST	+ 10
Australian Eastern Daylight Time	AEDT	+ 11

Time Zone	Abbrev.	Offset from GMT (hrs.)
New Zealand Standard Time	NZST	+ 12
New Zealand Daylight Time	NZDT	+ 13

Prior to this feature, the EAGLE administration supported the time zones shown in the following table.

Table 3-12. Currently Supported Time Zones

Time Zone	Abbreviation	Offset from GMT (hours)
Greenwich Mean Time	GMT	0
US Eastern Daylight Time	EDT	- 4
US Eastern Standard Time	EST	- 5
Pacific Daylight Time	PDT	- 7
Pacific Standard Time	PST	- 8
Mountain Daylight Time	MDT	- 6
Mountain Standard Time	MST	- 7
US Central Daylight Time	CDT	- 5
US Central Standard Time	CST	- 6
Hawaiian Daylight Time	HDT	- 9
Hawaiian Standard Time	HST	- 10
Atlantic Daylight Time	ADT	- 3
Atlantic Standard Time	AST	- 4
Western European Time	WET	0

As a result of this feature, all output banners and display of time zones in output content now allow 4 spaces for the time zone.

NOTE: This does not include SEAS output headers, which will remain at 3 characters. All 4-character time zones will be truncated to 3 characters in SEAS output.

Hardware Requirements

No new hardware is needed to support this feature.

Increase System-Wide IP Signaling Connections (Release 31.6)

This feature increases the system-wide number of IP signaling connections from 250 to 4000.

Table 3-13. Total IP Signaling Connections Supported

Type	Cards Per System	Links Per Card	IP Connections Per Link	Total Connections
IPLIMx	100	8	1	800
IPGWx	64	1	50	3200
System				4000

Because M3UA and SUA protocols require an ASP to be assigned to each association (connection), the number of supported ASPs is increased by the equivalent number.

This feature combines the ASP table with the IPAPSOCK table, but still refers to the ASP table in MTT errors and command output. The IPAPSOCK table has been expanded to contain a maximum of 4000 entries.

The system-wide number of ASPs has been increased from 250 to 4000.

This feature increases the number of system-wide IP signaling connections to 4000.

Increase System-Wide IPGWx TPS (Release 31.6)

This feature increases the limit on the number of SS7IPGW and IPGWI cards from 2 each (4 total) to a total of 64 cards system wide. Each IPGWx card will continue to host one and only one signaling link. This feature implements a new maximum limit of 8 IPGWx links per linkset, if the linkset does not have a mate linkset (mate-set).

Each IPGWx card is now rated at 2000 TPS.

An IPGWx mate-set can now be defined in terms of linkset configuration, rather than simply in terms of application type. An IPGWx mate-set is comprised of IPGWx cards hosting links in the same linkset or in the same combined-linkset with mated linksets.

An IPGWx mate-set is a group of IPGWx cards that act together to carry traffic between the SS7 network and a set of IP-based MTP user-part applications. As an example, the M3UA/SUA Application Server state needs to be maintained throughout an IPGWx mate-set, but is not maintained across multiple IPGWx mate-sets.

Prior to this feature, the IPGWx application simple definition of mate-set was that the cards running the same IPGWx application are considered mates. An IPGWx mate-set can now be defined in terms of linkset configuration, rather than simply in terms of application type. An IPGWx mate-set is comprised of IPGWx cards hosting links in the same linkset or in the same combined-linkset with mated linksets. This feature adds **`matelsn`** as a new parameter to the Change Linkset (**`chg-ls`**) command, thereby providing for the assignment of an IPGWx mate linkset. In addition, the **`CHG-LS`** command now uses the '**action=delete**' parameter to delete a configured **`matelsn`**. The **`matelsn`** linkset parameter provides backward compatibility with the current combined-linkset IPGWx mate-set deployments.

While deployment of IPGWx using combined linksets remains supported, the recommendation is that each IPGWx mate-set be deployed with a single linkset. Any N+K redundant configuration of IPGWx can be deployed, as long as the number of cards in the mate-set is 8 or less and the system-wide limit is not exceeded. Because each IPGWx card is now rated at 2000 TPS, the maximum transaction rate to/from a single IP-based point code for the IPGWx will be 14000 TPS (7+1 redundancy). If the maximum number of IPGWx cards is deployed (64 cards) using 8 mate-sets (linksets), then the total system-wide IPGWx transaction rate will be 112,000 TPS (7+1 redundancy).

Hardware Required

This feature requires SSEDCM cards running the IPGWx applications.

Increase the Number of Mated Application Entries (Release 22.0)

Release 22.0 increases the number of entries that the mated applications table can contain from 256 to 1024.

Increased GTT Transactions (Release 21.0)

This feature increases the performance of the global title translation (GTT) feature from 9300 MSUs per second to 21,000 MSUs per second when the GTT table is at its full capacity.

Increased Linkset Capacity (Release 28.0)

Description

This feature increases linkset capacity to support a *maximum* of 1024 linksets.

NOTE: For Release 28.0, only 255 of the linksets can be *gateway linksets*. A gateway linkset is a linkset that contains routes to a different network indicator (NI) than the network indicator of the EAGLE, or that has Gateway Screening (GWS) on the linkset.

New Hardware Required

There are no additional hardware requirements for the Increased Linkset Capacity feature.

Increasing the Size of the Service Provider ID Table (Release 23.2)

In Release 23.2, the number of service providers that can be configured in the EAGLE database for the Local Number Portability feature with the **ent-lnp-sp**, **ent-lnp-lrn**, and **ent-lnp-sub** commands has been increased 100 to 250. If the service provider ID table is full when either of these commands are executed, the command is rejected with this message.

Error Messages

```
E3133 Cmd Rej: LNP Service Provider table is full
```

The output of the **rtrv-lnp-sp** command has been changed to show that the total number of entries in the service provider ID table is now 250. The percentage of the maximum number of entries that the service provider ID table contains is based on the 250 entries that the service provider ID table can contain.

INP Number Normalization (Release 26.3)

Description

The INP Number Normalization feature allows the INP feature to accept queries either with or without special prefixes on the DN. Upon receipt, INP will strip off the prefix (if specified by the **chg-inpopts** command), convert the DN to international, perform the database query, and return a response to the switch. The CalledPartyNumber in the response may include the special prefix or not, depending on operator configuration of the feature. INP Number Normalization also allows the NAI in an incoming query to be mapped to an internal service NAI.

Hardware Requirements

The INP Number Normalization feature requires the Multi-Platform Server (MPS) system and the EAGLE STP Database Services Module (DSM) subsystem. This hardware was first introduced in EAGLE Release 26.1.

Integrated Monitoring for E5-E1T1 (Release 35.1)

Description

The Integrated Monitoring for E5-E1T1 feature enhances the E1/T1 MIM on EPM (E5-E1T1) feature by adding EAGLE 5 ISS support for use of the Integrated Message Feeder (IMF) platform to monitor link status, link states, and MSU traffic on low-speed links for the E5-E1T1 card.

See also E1/T1 MIM on EPM feature and E1/T1 MIM on EPM" for a discussion of support for E1 functionality and SE-HSL links.

NOTE: The Integrated Monitoring for E5-E1T1 feature is supported only for channelized links on E5-E1T1 cards.

Hardware Requirements

The E1/T1 MIM on EPM feature requires HIPR cards on each shelf that contains E5-E1T1 cards.

Limitations

EAGLE 5 ISS provides IMF support for only low-speed and channelized links. SE-HSL links and non-channelized links do not have IMF support.

Interim Global Title Modification (IP^7 Release 2.2)

The feature is also known as Prefix Deletion of Global Title. The IP ^{7} Secure Gateway changes the SCCP called party address for certain TTs before routing the message, but after GTT is performed, in one of the following ways:

When the IP ^{7} Secure Gateway receives a message that requires global title translation and contains one of the following TT values:

- 180–190
- 202
- 203
- 210–215

it does the following:

1. Performs the global title translation
2. Deletes the first three digits
3. Forwards the message

When the IP ^{7} Secure Gateway receives a message that requires global title translation and contains a TT value of zero, it does the following:

1. Performs the global title translation
2. Deletes the first three digits if they are 050 or 051
3. Forwards the message

These TT values cannot be provisioned or otherwise changed by the user.

Intermediate GTT Loadsharing (Release 28.1)

Description

This feature provides EAGLE the ability to load share between multiple nodes after global title translation, when the post-GTT message is Route-on GT (intermediate GTT).

Previously, the EAGLE only allowed load sharing between multiple nodes when the EAGLE was performing final GTT. Final GTT means the result of the EAGLE's translation is a point code (PC) and subsystem number (SSN), and the routing indicator in the outgoing message is set to Route-on-SSN. The load sharing is accomplished by accessing a mated application (MAP) table, which specifies the PC, SSN and relationship of a mated node. This load sharing mechanism was not allowed if the EAGLE was performing intermediate GTT, where the routing indicator in the outgoing message was set to Route-on-GT.

Some customers have a need to load share between nodes even when the STP is performing intermediate GTT. This may occur in a network that does not use capability point codes (CPC). This generally occurs in a quad-STP configuration where the first STP pair performs an intermediate GTT, and then must load share to the second STP pair, which will then perform the final GTT. If a CPC is not available for routing to the second STP pair, up to now there has been no way for the EAGLE to perform load sharing.

This feature supports a minimum of 1700 GTT transactions per second per DSM card, or 850 GTT transactions per second per TSM card while running GTT, VGTT, EGTT, and Global Title Modification.

Hardware Requirements

No new hardware is needed to support this feature.

Limitations

Any given PC can be part of only one PC group, i.e., any PC entered as part of a PC group cannot later be made part of a different PC group, unless it is first deleted from the initial group.

Intrusion Alert (Release 21.0)

To alert the EAGLE system administrator to a possible attempt by an unauthorized person trying to login to the EAGLE, the EAGLE issues a scroll area message. When 5 or more consecutive attempts to login to the EAGLE have failed, the following scroll area message is sent to all terminal ports that can receive unsolicited Security Administration messages:

```
Info: xxxxxxxxxx successive LOGIN failures on port pp
```

Where:

xxxxxxxxxx is the number of consecutive login failures on the port (1 - 4, 294, 967, 295)

pp is the terminal port (1 - 16) that the login attempts were made on.

When the attempt to login to the EAGLE is successful after a series of failed consecutive login attempts, or if the active MASP reboots, the count of failed consecutive login attempts for that port is reset to 0.

Attempts to login to the EAGLE, which are not completed normally, are not considered login attempts and are not included in the count of failed consecutive attempts. For example, while prompting for a password, you might use the F9 key is used to abort the command, or errors might occur when the EAGLE is looking up a user ID or password.

IP Signaling Serviceability (Release 35.0)

Description

The IP Signaling Serviceability feature enhances the IPLIMx and IPGWx applications to improve serviceability in the following areas:

- New UIMs/UAMs for IPGWx and IPLIMx applications
- Enhancements to routing key commands
- Prevent alternative routes to APCs or SAPCs for IPGWx linksets
- Improvements to PASS commands
- Allows enabling and configuring UA Heartbeat messages, which ensure that UA peers are available to each other for M3UA and SUA associations
- Enhance **`rept-stat-card`** command

- Enhancements to association commands

NOTE: Release 35.0 introduced E5-ENET cards, which provide a higher capacity for IPGWx and IPLIMx applications. However, the IP Signaling Serviceability feature runs on SSEDCM and DCM cards as well as cards.

Hardware Requirements

The IP Signaling Serviceability feature has the following hardware requirements:

- HIPR cards must be installed in any shelf that contains E5-ENET cards.
- An adapter cable per Ethernet port

Limitations

The IP Signaling Serviceability feature has the following limitations:

- If multiple remote IP destinations are advertised and are using only one local interface (no alhost is provisioned) and the Ethernet interface goes down for the unused local network, then the “IP Connection Restricted” alarm does not appear because it is not being used to reach the remote IP destination.
- UIMs are issued when an M3UA/SUA message is received from the far end and results in the SG discarding the message. The generation of these UIMs is paced to occur every 30 seconds: therefore, if multiple messages result in a discard within that 30 seconds, a UIM is only generated for the first message that is discarded.

IP User Interface: Telnet Support (Release 29.0) (IP^7 Release 7.0)

Description

This feature supports IP-based connections to the EAGLE UI via a telnet client. The Telnet feature adds up to 8 connections via a single IPSM card, up to 3 cards per system (total 24 telnet access ports), in addition to the existing 16 RS232 terminal ports.

NOTE: This feature is for use within a customer's private network ONLY. Connectivity to the Internet is NOT recommended, since no encryption scheme has been implemented to protect passwords transmitted across the network to the EAGLE.

Key benefits of this feature are:

- Access speed is improved;
- Remote access is enabled;
- Dial-up will not be required;
- Additional EAGLE UI access points;

- Access to the EAGLE UI from a network;
- Improved UI speed and data throughput;
- Provide a robust platform for future IPUI development.

The additional ports are accessible from any existing LAN or WAN connection along a customer's IP-based network. Craftspersons only need access to a standard **telnet** client in order to connect to and work on the EAGLE.

This feature targets the customer's demand for improvements to the EAGLE UI in the areas of network management, provisioning and maintenance tools, for which this feature provides a foundation.

As the first step in developing user interface improvements, this feature moves away from dedicated, hard-wired RS232 ports, and adds IP-based UI connections to the EAGLE.

With this feature, IP-based access provides a standard interface via which EAGLE commands are entered from a telnet session to the EAGLE. The EAGLE then provides command responses back to the remote telnet terminal. The EAGLE can, in this case, provide responses without pacing (slowing down) the output.

Initially, EAGLE telnet sessions resemble EAGLE user interface in KSR mode. This feature is the first delivery of UI enhancements; additional features will build on the Telnet UI foundation.

The IPUI solution consists of adding 1 to 3 IPSM cards, with IP connectivity, to the EAGLE. This enables telnet clients to connect from anywhere on the customers' IP LAN.

Refer to the *Database Administration Manual - System Management* for current information on this feature.

Hardware Requirements

This feature requires a IPSMI card for every 8 terminal ports, to a maximum of 24 IP terminal ports per system.

Limitations

- This feature does not provide the client telnet application.
- Some function keys are not supported, but alternative keystrokes are identified.
- The ECHO command between TELNET devices and serial terminals is not supported.
- LOCK command not supported from TELNET terminals.
- EAGLE commands **chg-secu-trm** and **rtrv-secu-trm** are not supported for telnet terminals.
- Persistent-device-states feature must be ON, for telnet terminals to default to Inhibited state, through initializations and reboots.
- Entering new passwords, or changing existing passwords is not supported from telnet terminals. This covers the commands **chg-user**, **ent-user**, **dlt-user**, and **chg-pid**. Security-related activity must be performed through a serial terminal (Terminals 1-16). Also, new users logging in for the first time, or users updating expired passwords, or any other activity where the EAGLE prompts for a new password, must be performed from a serial terminal.

IP^7 Transport Feature (Release 26.1)

Description

To address the technological needs of the convergence of voice and data networks, Tekelec introduces the IP ^{7} line of products. This product line addresses the needs of SS7 and IP converged networks, assuring the seamless and secure transfer of voice and data signaling traffic and providing carriers with a full portfolio of applications, including an SS7/IP gateway, internetwork routing, and SS7/IP internetwork services.

New Features

The initial release of the IP ^{7} Transport feature supports the following functions related to SS7/IP convergence.

- The **iplim** application provides point-to-point connectivity (a single TCP/IP connection from a DCM card to another device) within an ANSI network, specifically, SS7-over-IP for point-to-point signaling links (B/C/D links) between STPs.
- The **iplimi** application provides the same connectivity for International Telecommunications Union (ITU) point codes that the **iplim** application provides for American National Standards Institute (ANSI) point codes.
- Two-point IPLIMx allows a single DCM card loaded with the **iplim** application or the **iplimi** application to support two point-to-point links. In previous releases, each point-to-point link required a separate DCM card.
- Support for up-to-41 DCMs that run the **iplim** or **iplimi** application.
- A new DCM card, capable of supporting up-to-2000 MSUs per second, can be loaded with the **iplim** or **iplimi** application; customers can use any combination of the original and new DCM cards.

This section refers to the **iplim** and **iplimi** applications by the term ‘IPLIMx’ when discussing their common functions.

Refer to the *Database Administration Manual - SS7* for current information on this feature.

IP^7 Internationalization (IP^7 Release 4.0)

This Feature the following topics:

- Multiple Point Code Support
- Replacing Two EThis fetxisting STP Pairs with One SG Pair
- Multiple Linksets Between Two Nodes

Refer to the *Database Administration Manual - SS7* for the current details of the feature.

Impact on Other Features - Local Subsystems

The SG allows only the True Point Code to be entered into the MAP table. Also, the SG continues to allow the user to enter translations to the True Point Code, but the SG does not allow the user to enter translation to a Secondary Point Code.

If a node sends a rt-on-gt query, the node should set the query's DPC to be the SG's Capability Point Code. If a node sends a rt-on-ssn query, the node should **Summary of Modifications**

IPGWx Congestion Enhancement (Release 35.1)

Description

The IPGWx Congestion Enhancement feature changes the origination point of a Route Congestion Test (RCT) message to enable the Transfer Congested (TFC) message that is sent in response to reach its destination.

When an abatement procedure for a congested SS7 destination for a IPGWx-connected endpoint begins, a message exchange, consisting of an RCT message sent from the EAGLE 5 ISS node and a TFC message returned from the point of congestion, is supposed to occur if the congestion does not abate. However, if the EAGLE 5 ISS node can not be reached from the point of congestion, the TFC response may not reach its destination.

The IPGWx Congestion Enhancement feature replaces the point code of the EAGLE 5 ISS with the point code of the IPGWx-connected endpoint in the originating point code subfield of the RCT. This replacement causes the IPGWx-connected endpoint to appear to be the originator of the RCT: therefore, the TFC can be routed to the IPGWx-connected endpoint instead of to the EAGLE 5 ISS since the EAGLE 5 ISS may not be reachable from the congested node.

Hardware Requirements

The IPGWx Congestion Enhancement feature has no hardware requirements.

Limitations

The IPGWx Congestion Enhancement feature has no limitations.

IPGWx Data Feed (Release 35.0)

Description

The IPGWx Data Feed feature provides EAGLE 5 ISS support for use of the Integrated Message Feeder (IMF) platform to monitor link status, link states, and MSU traffic on high-speed IPGWx links for the M3UA protocol.

NOTE: Release 35.0 supports the IPGWx Data Feed feature only on SSEDCM cards. Release 35.1 will include support for the IPGWx Data Feed feature on E5-ENET cards.

EAGLE 5 ISS supports sending the following data to the IMF for the IPGWx cards:

- Association configuration/status/alarms
- Link configuration/status/alarms

- Card configuration/status/alarms

Ethernet traffic originating from IPGWx cards is routed through the STC cards, which provide IP connectivity to the IMF platform. Broadcasts sent out by the LIM card are forwarded to both networks through a task on the STC card.

TCP/IP traffic originating from the IPGWx cards is routed to the correct IMF based on the routing table setup. Alarms needed by the IMF that cannot be provided by the LIM cards are sent from the OAM to the IMF by an alarm task on the STC cards.

The IPGWx application on the EAGLE 5 ISS sends signaling message content to the IMF. The content of the signaling message includes the entire M3UA packet.

IPGWx cards create one per card and send link status on that card over that EMP session. The IPGWx GPL TVG functionality routes link events to the IMF. EMP functionality transmits link-copied MSU traffic, events and states between the EAGLE 5 ISS and the IMF. Event Time stamping allows the IMF to align link events.

The following link state changes are reported to IMF in real time by M3UA/SCTP based IPGWx links:

- OOS (Out Of Service)
- IS-NR (In Service Normal)
- Deactivating

A DPL software module provides IP connectively over IMT. IPGWx cards send link events and copied MSU traffic to the IMFs via a TCP/IP connection over the IMT bus through the STC IP router cards.

The IPGWx Data Feed feature requires the EAGLE 5 Integrated Monitoring (E5IS) and the Time Slot Counter Synchronization (TSCSYNC) feature bits to be turned on.

Hardware Requirements

The IPGWx Data Feed feature has the following hardware requirements:

- HIPR cards must be installed in the same shelf as the IPGWx card.
- STC cards must be installed in the same shelf as each IPGWx card being monitored. A minimum of two STC cards is required per system.

  NOTE: A sufficient number of STC cards to accommodate the number of IP links with data feed is required for your system. Contact your Sales Representative to determine the number of cards you will need.

- The K6-III version of SSEDCM (870-2372-01) cards or higher performance hardware is required for the IPGWx cards.

Limitations

The IPGWx Data Feed feature has the following limitations:

- EAGLE 5 ISS does not allow integrated monitoring of traffic on the TALI connections. It sends all configuration/status/alarms data and signaling traffic for all monitored SIGTRAN connections. The presence of TALI connections does not prevent the SIGTRAN connections from being monitored.
- Dual slot DCM (870-1945-xx) and the K6-II variant of SSEDCM cards (870-2508-01) are not supported.

- The number of IPGWx cards supported in an EIS environment depends on the limitation factor driven by platform and IMF subsystem.
- In the following situations, event or alarm data is lost between the EAGLE 5 ISS and the IMF:
  - If the TCP connection between an IPGWx card and the IMF subsystem becomes inoperable, data is lost until another TCP session can be established.
  - Temporary loss of data sent to the IMF can occur when an IPGW becomes congested. If the IPGWx card becomes congested to the point that signaling traffic loss is likely, the IMF application is deactivated and MSUs are not copied to the IMF. When congestion has abated, the IMF application is resumed.
  - During LIM card initialization, links are brought up and transmission of EAGLE 5 ISS traffic begins. Subsequently, a TCP session is established with the IMF subsystem. Between the start of EAGLE 5 ISS traffic and the establishment of a TCP session, link events and states are not sent to the IMF.

IPGWx Data Feed (Release 35.1)

Description

The IPGWx Data Feed feature enhances the IPGWX Data Feed feature from Release 35.0 by adding EAGLE 5 ISS support for use of the Integrated Message Feeder (IMF) platform to monitor link status, link states, and MSU traffic on high-speed IPGWx links for the M3UA and SUA protocols on E5-ENET cards.

Other than support for the E5-ENET card and the hardware requirement shown below, the IPGWx Data Feed feature is not changed from Release 35.0. For a detailed discussion of the IPGWx Data Feed feature, refer to the EAGLE 5 ISS Release 35.0 Feature Notice.

Hardware Requirements

The IPGWx Data Feed feature has the following hardware requirements:

- IMF 2.1 platform
- When monitoring IP links on IPGW cards, all STC cards must be SSEDCM cards. Dual-slot cards are not supported.

IPGWx TPS Control (Release 31.6)

Beginning with this feature, the IPGWx IP Signaling TPS is a true system key, and can be enabled for a quantity up to 112,000 TPS. A portion of the system IPGWx IP Signaling TPS can be assigned to each linkset in the system; the total IP TPS sum across all linksets cannot exceed the enabled system IPGWx IP Signaling TPS.

Temporary keys will no longer be supported for IPGWx IP TPS. Instead, appropriate alarms are generated when system IP TPS exceeds a configurable threshold.

A true system IPGWx IP Signaling TPS maximum quantity is implemented in the system. A default of 200 TPS is provided with no IP Signaling TPS quantity feature access key enabled. IP Signaling TPS up to 112,000 can be enabled with a quantity Feature Access Key.

A portion of the system maximum IP TPS can be assigned to each linkset in the system. The total IP TPS assigned to all linksets cannot exceed the enabled system maximum quantity.

Alarm thresholds can be defined to display a warning when the system IP TPS approaches the enabled maximum, when a linkset approaches its assigned maximum, and when a link approaches its “fair share” of the TPS assigned to its linkset.

IPLIM Protocol Support Enhancement (Release 28.1) (IP^7 Release 6.0)

Description

Customers require IETF protocol-based A-Link capacity up to 30,000 TPS between PSTN network elements and IP network elements. In addition, the customer requires that the data link layer protocols used to communicate with the IP network element be M3UA/SCTP/IP. Current releases of Tekelec IP ^{7} Secure Gateway applications do not provide features supporting these requirements.

In this feature, the IPLIMx GPLs have been enhanced to provide for M3UA/SCTP/IP connections, in addition to the present MTP3/SAAL/TALI/TCP/IP connections. Its rated capacity has been increased from 2000 TPS to 3000 TPS.

Each IPLIMx IP network connection is an SS7 signaling link. Sixteen of these links can be assigned to a linkset, yielding a theoretical total TPS of 48K. Currently, the maximum TPS limit is 30,000. The link can also be made a part of a combined linkset. With this feature, full support is provided for M3UA encodings and decodings; only a subset of the M3UA procedures, however, is supported. M3UA Internet draft v12 is implemented.

Due to the nature of the M3UA/SCTP protocols, links using this type of connection have fewer MTP2 features than those using SAAL/TALI/TCP. The resulting IPLIMx GPL supports DPC-SLS routing, but not SI or CIC routing.

Hardware Requirements

This feature requires a SSEDCM (Single Slot Enhanced DCM).

Limitations

This feature reflects a partial implementation of the M3UA draft specification. All M3UA Internet draft v12 encodings and decodings are supported. A subset of the M3UA Internet draft v12 procedures is supported.

IPLIMx Data Feed (Release 35.0)

Description

The IPLIMx Data Feed feature provides EAGLE 5 ISS support for use of the Integrated Message Feeder (IMF) platform to monitor link status, link states, and MSU traffic on high-speed IPLIMx links for the M2PA protocol.

NOTE: Release 35.0 supports the IPLIMx Data Feed feature only on SSEDCM cards. Release 35.1 will include support for the IPLIMx Data Feed feature on E5-ENET cards.

EAGLE 5 ISS supports sending the following data to the IMF for the IPLIMx cards:

- Association configuration/status/alarms
- Link configuration/status/alarms
- Card configuration/status/alarms

Ethernet traffic originating from IPLIMx cards is routed through the STC cards, which provide IP connectivity to the IMF platform. Broadcasts sent out by the IPLIMx card are forwarded to both networks through a task on the STC card.

TCP/IP traffic originating from the IPLIMx cards is routed to the correct IMF based on the routing table setup. Alarms needed by the IMF that cannot be provided by the LIM cards are sent from the OAM to the IMF by an alarm task on the STCs cards.

The IPLIMx application on the EAGLE 5 ISS sends signaling message content to the IMF. The content of the signaling message includes the entire M2PA packet. EAGLE 5 ISS forwards an indicator to the IMF every time the M2PA proving process takes place on each association. The indicator can be a message exchanged during the proving process or an event message.

IPLIMx cards create an EAGLE Monitoring Protocol (EMP) session per associated link and send copied MSU traffic, link status, and events on each session that pertains to the associated link.

The following M2PA/SCTP Link Status Messages are reported to the IMF in real time for each direction of each IPLIMx high speed link:

- Link Status Alignment (LSA) Rx/Tx
- Link Status Proving Normal (LSPN) Rx/Tx
- Link Status Proving Emergency (LSPE) – Rx/Tx
- Link Status Ready (LSR) – Rx/Tx
- Link Processor Outage (LPO)- Rx/Tx
- Link Processor Outage Ended (LPOE) Rx/Tx
- Link Status Busy (LSB) Rx/Tx
- Link Status Busy Ended (LSBE)- Rx/Tx
- Link Status out of Service (LSO) – Rx/Tx

A DPL software module provides IP connectively over IMT. The IPLIMx cards send link events and copied MSU traffic to the IMFs via a TCP/IP connection over the IMT bus through the STC IP cards.

The IPGWx GPL TVG function routes link events to the IMF.

The EMP function transmits link-copied MSU traffic, events, and states between the EAGLE 5 ISS and the IMF.

Event Time stamping allows the IMF to align link events.

The IPLIMx Data Feed feature requires the EAGLE Integrated Monitoring (ESIS) and the Time Slot Counter Synchronization (TSCSYNC) feature bits to be turned on.

Hardware Requirements

The IPLIMx Data Feed feature has the following hardware requirements:

- HIPR cards must be installed in the same shelf as the IPLIMx card.
- STC cards must be installed in the same shelf as the IPLIMx cards being monitored. A minimum of two STC cards is required per system.

  NOTE: A sufficient number of STC cards to accommodate the number of IP links with data feed is required for your system. Contact your Sales Representative to determine the number of cards you will need.
- The K6-III version of SSEDCM (870-2372-01) cards or higher performance hardware is required for the IPLIMx cards.

Limitations

The IPLIMx Data Feed feature has the following limitations:

- EAGLE 5 ISS does not allow integrated monitoring of traffic on the TALI connections. It sends all configuration/status/alarms data and signaling traffic for all monitored SIGTRAN connections. The presence of TALI connections does not prevent the SIGTRAN connections from being monitored.
- Dual slot DCM (870-1945-xx) and K6-II variant of SSEDCM cards (870-2508-01) are not supported.
- The number of IPLIMx cards supported in an EIS environment depends on the limitation factor driven by platform and IMF subsystem.
- In the following situations, event or alarm data is lost between the EAGLE 5 ISS and the IMF:
  - If the TCP connection between an IPLIMx card and the IMF subsystem becomes inoperable, data is lost until another TCP session can be established.
  - Temporary loss of data sent to the IMF can occur when an IPLIMx card becomes congested. If the IPLIMx card becomes congested to the point that signaling traffic loss is likely, the EAGLE 5 ISS/IMF application is deactivated and MSUs are not copied to the IMF. When congestion has abated, the EAGLE/IMF application is resumed.
  - During LIM card initialization, the links are brought up, and transmission of EAGLE 5 ISS traffic begins. Subsequently, a TCP session is established with the IMF subsystem. During the time from the start of EAGLE 5 ISS traffic to the establishment of a TCP session, link events and states are not sent to the IMF.

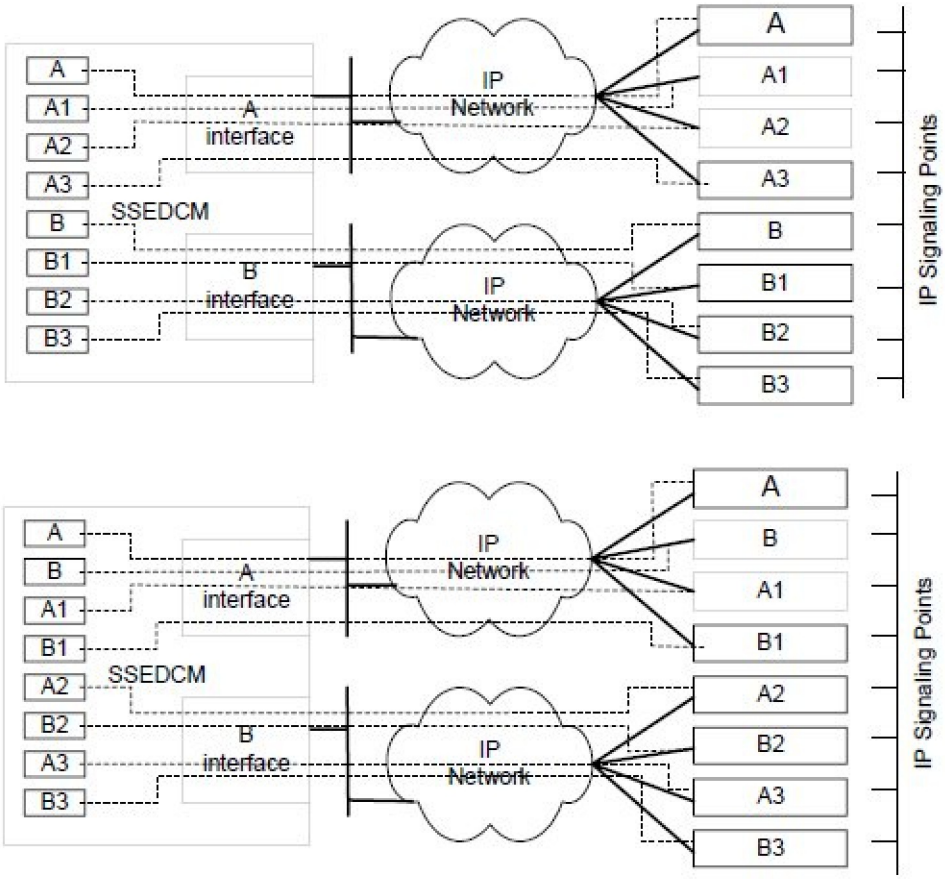
IPLIMx to 8 Points (Release 29.1) (IP7 Release 7.1)

Description

The IPLIMx to 8 Point feature expands the capability of the Multipoint IPLIMx feature to support not just two, but eight IPLIMx signaling links on a SSEDCM. This feature reduces the number of SSEDCM cards required to provide a given number of IPLIMx signaling links. ANSI and ITU are supported by this feature.

The following figure illustrates the configuration supported by the IPLIMx to 8 Point feature. With this configuration 8 IP connections use the "A" and "B" interface. The socket/port identifier names are consistent with the naming convention used for Multi Port LIM. Any signaling link can use either Ethernet interface A or interface B.

Figure 3-10. IPLIMx to 8 Point Connectivity (8 Signaling Links)



Hardware Requirements

This feature requires the Single Slot EDCM (870-2372-01).

IPLIMx/IPGWx on EPM (E5-ENET Card) (Release 35.0)

Description

The IPLIMx/IPGWx on EPM feature provides a single-slot E5-ENET card with increased TPS capacity relative to existing SSEDCM cards.

NOTE: IP links can be assigned to cards in Release 35.0. However, Release 35.0 does not support data feed to the IMF on the E5-ENET card. Data feed to the IMF for IP links is supported on the SSEDCM cards for Release 35.0. Release 35.1 will provide support for data feed to the IMF on both SSEDCM and E5-ENET cards.

The E5-ENET card allows 16 links for IPLIMx. For IPGWx, the E5-ENET card allows 50 connections and 1 signaling link.

Table 3-14. IPLIMx/IPGWx on EPM

Card	IPLIMx		IPGWx	
	Max No. of Signaling Links	Link designations	Max No. of Signaling Links	Max No. of IP Connections
E5-ENET	16	a..a7, b..b7	1	50
DCM	2	a, b	1	50
SSEDCM	8	a..a3, b..b3	1	50

The E5-ENET card supports the SCTP and M2PA protocols for IPLIMx and the SCTP and M3UA protocols for IPGWx.

The E5-ENET card uses a Celeron-M processor and does not require a fan tray or any additional power requirements; however, it does require thermal monitoring, which is provided.

The maximum number of cards per system is 100 for IPLIMx and 64 for IPGWx.

Two new GPLs support the IPLIMx/IPGWx applications: IPLHC for IPLIMx applications and IPGHC for IPGWx applications.

New Concepts

The IPLIMx/IPGWx on EPM feature introduces or enhances the following concepts:

- Configurable SCTP Buffers
- Increased TPS
- Ethernet Interfaces
- Thermal Monitoring

Configurable SCTP Buffers

The IPLIMx/IPGWx on EPM feature allows SCTP buffers to be configured for a connection. These buffers allow users to maximize memory used based on traffic rate. Hardcoded minimum and maximum values are used for range checking. If a value outside this range is configured, the command is rejected.

Auto-inhibit is invoked if more SCTP buffers are configured than the card can handle. Because there is a finite amount of memory available, SCTP buffering is a function of TPS, network round trip time (RTT), and number of connections or links.

Increased TPS

The E5-ENET card capacity is increased. For the IPHLC and IPGHC GPLs, each link can carry up to card capacity. Thus, buffer sizing and congestion thresholds are adjusted for the card maximum and link maximum.

For both IPGHC and IPLHC, the increase in traffic impacts system and network design. There can be 100 IPLIMx and 64 IPGWx cards in a system.

Ethernet Interfaces

Each interface is independent of the other and supports 10/100 Mbps data rates, full/half duplex, fixed/auto-negotiate, DIX/802.3 MAC header modes. Although each Ethernet PMC card has two Ethernet interfaces, for this

feature, only one on each card is used. With the current hardware configuration two PMC cards are required to allow port A and port B interface operation.

The E5-ENET card requires adapters for connection to either dual RJ-45 jacks or DB26 (female connector).

Thermal Monitoring

The E5-ENET card requires thermal monitoring. The card processor can overheat from high ambient temperature or air flow blockage. If the junction temperature goes above operating limits (approximately 125ºC), the CPU halts and the card shuts itself down to prevent permanent, catastrophic damage. If thermal shutdown occurs, all processor activity ceases.

To prevent thermal shutdown from occurring, a series of alarms are used to detect and notify users of increasing thermal conditions.

When the CPU temperature exceeds a configurable thermal threshold (Temperature Level 1, 56ºC - 92ºC [133ºF - 198ºF]), a major alarm is raised against the card. If the temperature exceeds a second thermal threshold (Temperature Level 2, 60ºC - 99ºC [140ºF - 210ºF]), a critical alarm is raised against the card.

When the second thermal event occurs, the application receives a notification from the OS and begins redirecting traffic to other cards if possible. For IPLIMx all links on the card go out of service. For IPGWx, the link is taken out of service and the far end is notified that the connections no longer accept traffic.

Once the temperature returns to below the Temperature Level 2 threshold, the LPO condition is cleared and links can begin operation again. When the temperature returns to below Temperature Level 1, a clearing alarm is raised for the card.

Hardware Requirements

The IPLIMx/IPGWx on EPM feature has the following hardware requirements:

- A HIPR card must be installed on each shelf that contains E5-ENET cards.
- An adapter per Ethernet port

Limitations

The IPLIMx/IPGWx on EPM feature has the following limitations:

- An E5-ENET card cannot support the IPLIMX and IPGWx functions simultaneously
- The number of IPLIMx cards supported in an EIS environment depends on the limitation factor driven by platform and IMF subsystem.
- There is a minimum and maximum SCTP buffer configuration per connection (8192 bytes and 3.125 Mbytes, respectively). The card maximum is 3.125 Mbytes: therefore, if a connection has the maximum buffer configuration, there can be only 1 connection on the card.

IPLIMx/IPGWx on EPM (Release 35.1)

Description

The IPLIMx/IPGWx on EPM feature enhances the IPLIM/IPGWx on EPM feature from Release 35.0 by adding EAGLE 5 ISS support for the SUA protocol on E5-ENET cards.

Other than the added support and the limitations shown below, the IPLIMx/IPGWx on EPM feature is not changed from Release 35.0 Refer to the EAGLE 5 ISS 35.0 Feature Notice for a detailed discussion of the IPLIMx/IPGWx on EPM feature.

Limitations

The IPLIMx/IPGWx on EPM feature has the following limitations:

- E5-ENET cards cannot be deployed in a mixed linkset with DCM cards.
- The maximum number of E5-ENET, DCM, and/or SSEDCM IPLIMx and IPGWx cards in a system is 164. The mixture of these cards is a maximum of 100 cards for IPLIMx and 64 cards for IPGWx in any combination. However, due to the increased throughput of the E5-ENET card, the IMT system capacity has a limit of 100 E5-ENET IPLIMx and IPGWx cards in any combination.

IPMX/MCAP/TDM Replacement (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)

Overview

Beginning in EAGLE Release 30.0, the IPMX, MCAP-256 and TDM* (*all versions earlier than -10) cards are obsolete. Any EAGLE or EAGLE 5 customer upgrading to Release 30.0 must replace all IPMX cards with HMUX cards (870-1965-01), all MCAP-256 cards in slots 1113 and 1115 (the former MCAP slots) with GPSM-II cards (870-2360-01), and any TDM card of a version earlier than -10 with TDM-10 (or later) cards (870-0774-10).

Replacement of the -05 backplane also is required, as this backplane does not support HMUX.

NOTE: These hardware upgrades must be performed prior to the software upgrade. After the upgrade to Release 30.0 has been completed, an MCAP card will not be allowed to boot in the system. Only a GPSM-II card will be allowed in the former MCAP slots.

HMUX

The High-Speed Multiplexer (HMUX) is baseline hardware for IP7 Secure Gateway Release 8.0. It replaces the obsolete IPMX card, and increases the number of links supported by the IP7 Secure Gateway in a future release. The HMUX enhances the IMT bus by introducing a new 1Gb/sec inter-shelf bus bandwidth. (The intra-shelf bus data rate remains the same at 125Mb/sec.)

HMUX also enhances IMT performance by transmitting data between shelves only when it is necessary. Traffic between IP7SG cards on the same shelf is allowed to stay on the shelf IMT, and is not required to transit between shelves. Traffic between shelves is not required to pass onto an intra-shelf IMT bus, if this is not necessary.

GPSM-II for MCAP Slots

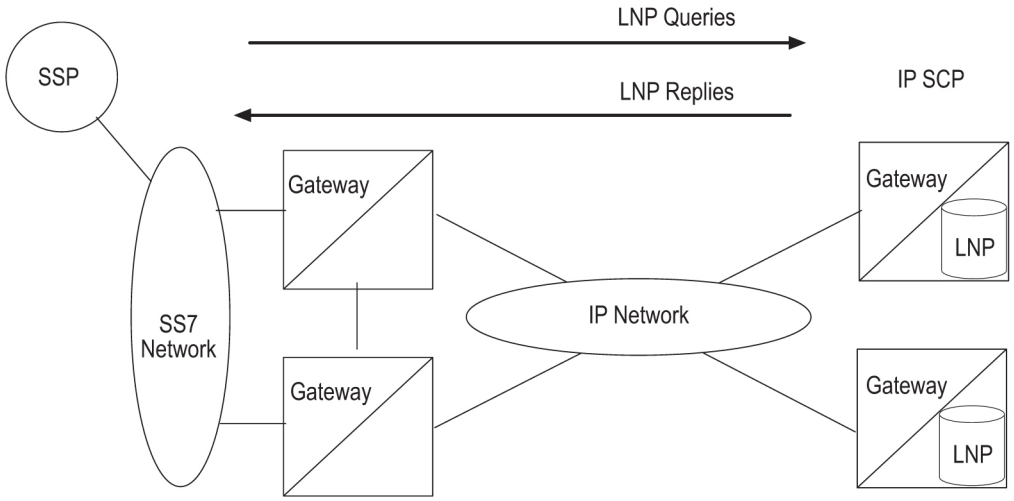
Future applications and table expansions will require increased performance across the IMT bus interface both to and from the Maintenance and Administration Subsystem. To meet this need, the GPSM-II incorporates an EDCM-based design for the OAM functionality on the IP7 Secure Gateway. There is also a need to increase available memory and performance on the OAM for these applications and for future use.

The GPSM-II utilizes a 1GB memory daughterboard.

IP-SCP with LNP Capability (IP^{7}Releases 1.0, 2.0)

This feature, which was available only in a laboratory environment in release 1.0, allows the IP ^{7} Secure Gateway to act as an IP-SCP. The SCCP/TCAP queries are received and responses returned over an IP interface.

Figure 3-11. IP Connected LNP Application (Lab Only)



IS41 GSM Migration (Release 36.0)

Description

The IS41 GSM Migration (IGSM) feature is an enhancement to the original IS-41 to GSM Migration feature, to add GSM to IS-41 migration functions to the existing IS-41 to GSM migration support of call termination for customers in migration from IS-41 to GSM wireless technology. This enhancement adds flexibility in LOCREQ message decoding and encoding for number migration from one mobile protocol to another to the existing support of Loc_Req, MSRCV GSM SRI, and SRI_SM operation code processing.

The original IS-41 to GSM Migration feature functions support call termination for customers in migration from IS-41 to GSM wireless technology. The feature gives the wireless service provider a way to begin the migration of mobile subscribers from IS-41 to GSM, while allowing each subscriber to retain his or her existing phone

number. The feature allows termination of calls to either an IS-41 handset or a GSM handset, based on the provisioned migration status of the subscriber.

The enhancement separates the IS41 GSM Migration feature from the G-Port feature. The IS41 GSM Migration feature can exist as a standalone feature without depending on the G-Port feature. When the IS41 GSM Migration feature is on, the MNP service selector is used instead of the GPORT service selector.

The IS41 GSM Migration feature uses the EPAP (EAGLE Provisioning Application Processor) RTDB to retrieve the subscriber portability status and provision directory numbers for exported and imported IS-41 subscribers. This database maintains information related to subscriber portability in the international E.164 format.

The IS41 GSM Migration feature supports both GT- and MTP-routed messages.

- GT-routed messages support UDT and non-segmented XUDT message types and perform service selector lookup after SCCP verification.

- A-Port processes MTP-routed messages if the MTP Messages for SCCP Applications (MTP Msgs for SCCP Apps) feature is turned on (see "IS41 GSM Migration" for details of MTP-routed message processing).

The IS41 GSM Migration feature adds processing of LOCREQ and SMSREQ messages to the SRI and SRI_SM message processing provided by the original IS-41 to GSM Migration feature.

- An ANSI-41 LOCREQ message is initiated by a TDMA/CDMA MSC that queries the HLR for information regarding user subscription/location before terminating a voice call.

- An ANSI-41 SMSREQ message is initiated by a TDMA/CDMA SMSC that queries the HLR for information regarding user subscription/current location before delivering a short message.

If a data entry matching the conditioned Called Party is found and an NE (either RN or SP) is assigned to the entry, the EAGLE 5 ISS processes the SRI, SRI_SM, LOCREQ, and SMSREQ message based on the NE/PT value assigned.

If a HomeRN is detected in the Called Party and a matching DN with RN is found in the database, the EAGLE 5 ISS generates UIM 1256, indicating detection of circular routing, and routes the message using normal routing if both the MNP Circular Route Prevention feature and the IS41 GSM Migration featureare turned on.

If an undefined TCAP portion (not ITU or ANSI) is received by the IS41 GSM Migration feature, the message falls through to GTT.

New GSM2IS41 Prefix

The EAGLE 5 ISS populates a new following the same mechanism that is used for the existing IS412GSM prefix. The EAGLE 5 ISS returns a GSM2IS41 prefix in the SRI_ACK message if a received SRI message is destined for a non-migrated IS41 or GSM migrated IS41 subscriber (a data entry is found with RN and PT=0).

The MIGRPFX Option

The MIGRPFX field in the **`rtrv-gsmopts`** command output is shown as MULTIPLE (for ON) or SINGLE (for OFF or disabled). If MIGRPFX = MULTPLE, the RN from the RTDB is used as the prefix in the SRI_ ACK message. If MIGRPFX=SINGLE (disabled) and the GSM2IS41 prefix is NONE, the SRI message issues UIM 1341 "SRI rcvd GSM2is41 prefix not provisioned" and the message falls through to GTT.

For systems that are upgraded to the IS41 GSM Migration feature, the upgrade process sets the MIGRPFX option to ON if the G-Port feature is turned on and the IS412GSM prefix is defined. If the G-Port feature is turned on and the IS412GSM prefix is not defined, the upgrade process sets the the to OFF. The default setting for new systems is OFF (disabled).

Service State and Re-Route

The IS41 GSM Migration feature shares the service state and re-route with the A-Port and G-Port features, under one service called the MNP Service state. (The G-Port service state is used if only the G-Port feature is on.) The IS41 GSM Migration feature supports re-route functions as part of MNP service re-route. Alternate PCs are shared by all three features.

Alarms and the **rept-stat-sccp** command output show MNP Service information if the the IS41 GSM Migration feature is enabled.

Database Lookup and Routing

The MSISDN is used for RTDB database lookup.

- The IS41 GSM Migration feature performs RTDB lookup on the conditioned number, and routes or relays the message based on the lookup result.
- The individual number database is searched first.
- If the number is not found, the number range database is searched.
- If a match is not found in the individual and range based databases, GTT is performed on the message.
- When MSISDN numbers in the RTDB database are odd, the CDPA GTI of the incoming message is 2, and the last digit of the number is ‘zero’, database lookup is performed once using the even number. If no match is found, database lookup is performed using the odd number (without the last digit).
- For LOCREQ messages, the DN is derived based on the setting of the LOCREQDN option (see the new **chg-is41opts** command).
- For non-LOCREQ messages, the DN is derived from the SCCP portion of the message.
- Upon successful decode and verification of the message, number conditioning is performed. The DN or SCCP CDPA digits might need to be conditioned to international number format based on the service nature of address (SNAI or TCAPSNAI or MTPLOCREQNAI). HomeRN and IEC or NEC prefixes are removed. The IS41 GSM Migration feature performs RTDB lookup on the conditioned number, and routes or relays the message based on the lookup result.
- An SMSREQ message is relayed like any other non-LOCREQ message. No changes are performed to the TCAP/MAP portion of the message. If the general TCAP/MAP verification is successful, the TCAP opcode is SMSREQ, and the IS412GSM option SMSREQBYPASS is YES (see the **-is412gsm** commands), the message is processed as an SMSREQ message. Otherwise, message relay is performed using SCCP CDPA information.
- The IS41 GSM Migration feature modifies the TCAP information for LOCREQ messages only when a HomeRN was deleted from the TCAP DN and LOCREQRMHRN = YES. Any gaps in the data caused by a change in field length will be resolved by shifting the remaining information up. Any IEC or NEC code is left.
- The IS41 GSM Migration feature falls through to GTT if number conditioning fails or does not find the DN in the RTDB database, or the DN is found with non-A-Port data.
- If a HomeRN is detected in the Called Party and a matching DN with RN is found in the database, the EAGLE 5 ISS generates UIM 1256, indicating detection of circular routing, and routes the message using normal routing if both the MNP Circular Route Prevention feature and the IS41 GSM Migration featureare turned on.

NOTE: Normal routing is performing GTT if the incoming message is sent to the EAGLE 5 ISS Self Point Code. Normal routing is routing the message to the MTP DPC if the incoming message is MTP-routed (the MTP DPC of the message is not the EAGLE 5 ISS Self Point Code).

- If the IS-41 message is LOC_REQ and the MIN parameter has unsupported values (MIN digits < 5 or >15), a LOC_REQ Return Error response message with error code information element as 'unexpected data value' is returned.

- If the IS-41 message is SMS_Request and the CDPA digits in the RTDB are associated with a portability type of 5 (Migrated), an SMS_Request Response with SMS Access Denied Reason = 5 is returned.

- If the GSM message is SRI-SM, the CDPA digits in the RTDB are associated with "RN" Entity type, and the portability type is "not known to be ported", an SRI-SM RETURN ERROR message with Error Code "Unknown Subscriber" is returned.

Measurements

The following enhancements support the collection and retrieval of measurements related to the IS41 GSM Migration feature. These new measurement registers are supported with and without the Measurements Platform feature enabled.

- New registers are added to the NP SYS reports: Hourly Maintenance Measurements on NP System (MTCH-NP) and Daily Maintenance Measurements on NP System (MTCD-NP).

  — APSMSRCV—Number of SMS Request messages received

  — APSMSREL—Number of SMS Request messages relayed

- New registers are added to the NP SSP reports: Hourly Maintenance Measurements on NP SSP (MTCH-SSP) and Daily Maintenance Measurements on NP SSP (MTCD-SSP).

  — APLRACK—Number of call related LOCREQ messages acknowledged.

  — APLRRLY—Number of call related LOCREQ messages relayed.

  — APNOCL—Number of non-call non-LOCREQ related messages relayed.

  — APNOCLGT—Number of non-call Non-LOCREQ related messages that fell through to GTT.

Feature Access Key

A feature access key (FAK) for part number 893017301 is required to enable the IS41 GSM Migration feature.

- The GTT feature must be on before the IS41 GSM Migration feature can be enabled.

- After the feature is enabled and turned on, it cannot be turned off.

- No temporary FAK is allowed for the feature.

- An LNP quantity feature and the IS41 GSM Migration feature cannot be enabled in the system at the same time.

Hardware Requirements

The IS41 GSM Migration feature has the following hardware requirements:

- DSM cards with at least 4G of memory
- The IS41 GSM Migration feature cannot be enabled if any DSM cards with less than 4G of memory or any TSM cards for SCCP are present in the system. When IS41 GSM Migration is enabled, no DSM cards with less than 4G of memory and no TSM cards for SCCP can be provisioned.

Limitations

None

IS-41 to GSM Migration (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)

The IS-41 to GSM Migration Feature is planned for Release 30.1. The overall purpose of this feature is to support call termination for customers in migration from IS-41 to GSM wireless technology. The major functional areas of the EAGLE that support IS-41 to GSM Migration are Database Administration, Protocol, and Measurements. This feature gives the wireless service provider a way to begin the migration of mobile subscribers from IS-41 to GSM while allowing those subscribers to retain their existing phone number. Once the subscriber is marked as migrated, the GSM handset is fully functional. This feature allows termination of calls to either an IS-41 or GSM handset based on the provisioned migration status of the subscriber. The IS-41 to GSM Migration feature is based on the same technology as the EAGLE's G-Port feature. Therefore, this document refers to G-Port in several areas. The IS-41 to GSM Migration feature is implemented as an enhancement to the existing G-Port feature. Therefore, IS-41 to GSM Migration is considered and referred to as a G-Port feature in the current document.

ISCC Interface Loopback Test (Release 22.0)

The ISCC Interface Loopback Test tests the interface to ISCC chip. The ISCC chip has a local loopback mode in which the internal transmit data is tied to the internal receive data such that the data to be transmitted is actually looped back as data just received. If the test is successful, the hardware and software up to the ISCC chip is not the cause of the failure.

The loopback test is similar to looping back the transmit and receive interfaces by using a loopback plug on the backplane. However, the advantages of using the ISCC loopback test over a loopback cable are:

- loopback test is interface independent
- loopback plug will not work for V.35 interfaces
- all hardware baselines supported
- can be done remotely
- no intrusive mechanical action on the part of the user

The disadvantages of the ISCC loopback test are:

- doesn't validate the other hardware components on the SS7 LIM card
- doesn't validate the EAGLE backplane

When the ISCC loopback test is started, the ISCC chip is put into the local loopback mode. The SS7 LIM goes through the alignment process. If the signaling link aligns, the ISCC chip has passed the test. The ISCC chip is put back to normal operation and the results are displayed to the user.

Throughout this test, the link is deactivated and not available for traffic. When the ISCC loopback test is running, the SST state of the signaling link displays the entry LPBK and the AST of the signaling link displays the entry ISCC. These states of the signaling link are displayed with the **rept-stat-slk** command.

Parameters

To run the ISCC loopback test, the **loopback** parameter has been added to the **tst-slk** command. The values of the **loopback** parameter are either **yes** or **no**.

yes = perform the ISCC loopback test

no = do not perform the ISCC loopback test (the default value)

Input/ Output Example

tst-slk:loc=1201:port=a:loopback=yes

```
RLGHNCXA03W 97-06-07 15:55:57 EST Rel 22.0.0
2408.1078    CARD 1203,A  INFO  ISCC Loopback test PASSED

Report Date: 97-06-07  Time: 15:55:57
```

The ISCC loopback test can only test one signaling link at a time. The signaling link to be tested must be in the OOS-MT-DSBLD state or the test cannot be executed. If the link is still active (in the IS-NR state) and an attempt is made to execute the ISCC loopback test, the command is rejected and this message is displayed.

Error Messages

```
E2916 Cmd Rej: Link must not be active to execute loopback
```

The ISCC loopback test cannot be executed if the link fault sectionalization feature is running. If the link fault sectionalization feature is running and an attempt is made to execute the ISCC loopback test, the command is rejected and this message is displayed.

```
E2921 Cmd Rej: LFS must not be running on requested link
```

The ISCC loopback test only works for SS7 LIMs. If the signaling link selected to test is not an SS7 LIM and an attempt is made to execute the ISCC loopback test, the command is rejected and this message is displayed.

```
E2292 Cmd Rej: Card does not exist or is not a LIM (LOC)
```

No command such as **act-slk**, that would change the state of the signaling link from OOS-MT-DSBLD, can be executed while the ISCC loopback test is running.

During the ISCC loopback test, no level 1 information about the link is available.

The ISCC loopback test cannot run if the specified card is unplugged.

ISUP Message Type Screening (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)

Description

The ISUP Message Type Screening feature provides the EAGLE with the capability to screen on ISUP message type. This feature augments the Gateway Screening functionality currently provided by the EAGLE. The feature is based on the previous release of major enhancements to the Gateway Screening feature. (At that time, ISUP message type screening was not implemented.) The enhanced functionality of Gateway Screening results in a more secure, easily administered network.

NOTE: The functionality provided by this feature is not controlled by feature key or STP option. As part of core GWS capability, it becomes a core component the EAGLE STP.

Hardware Requirements

This feature requires the hardware baseline for Release 30.0. This includes the GPSM-II and TDM-10 (or later) configuration of the MASP (for the EOAM GPL), along with ASM cards (for the GLS GPL) and LIM, MPLIM, and ASM (SCCP GPL) cards to support screening of network protocol traffic.

GTWY Measurements

For Release 30.0, the new measurements report type GTWY-LSONISMT has been added. The measurements for this new report are kept on a per-link set, per- originating NI (ANSI), per-ISUP message type basis. These measurements will be reported in the **`gtwy-lsonismt_yyyymmdd_hhmm.csv`** FTP report files (mm is a half-hour boundary).

ISUP Normalization in the IP^7 SG (IP^7 Release 4.0)

This feature allows an IP ^{7} SG to deliver ISUP messages that arrive at the SG from the PSTN in a country specific ISUP variant format, to an IP device in a normalized ISUP format. Likewise, it enables traffic received from an IP device in a normalized ISUP format to be delivered to a PSTN link in the appropriate country variant format. The normalized ISUP messages are carried in TALI packets. Data is contained in the TALI packet itself to specify what National network (i.e., what country) the ISUP message originated from or is destined to and what ISUP variant the original PSTN message was formatted in.

This feature allows an IP device (e.g., a MGC providing Class 4 Tandem functionality) connected to an IP ^{7} SG to perform call setup for multiple countries without knowledge of the various countries' ISUP message formats. The MGC needs only to support encode/decode functionality for the normalized format and does not have to support encode/decode functionality for each ISUP variant.

Refer to the *Database Adminisration Manual - Features* for current information on this feature.

ISUP NP with EPAP (Releases 31.11, 34.0)

Description

The purpose of the Integrated Services Digital Network User Part Numbering Plan with EAGLE 5 SAS Provisioning Application Processor (ISUP NP with EPAP) feature is to prepend a prefix (a SubNet prefix or RN) to the CdPN of an IAM message if the CdPN is a ported in (including never been ported) or a ported out DN before relaying the message to its destination. The prefix provides the recipient switch a means to differentiate a call so that different billing rates or routing can be applied to the call.

The title is selected to distinguish a similar feature developed for support of ELAP database lookup based on the ANSI ISUP Initial Address Message (IAM). This feature presents no impact on the EPAP.

The EAGLE 5 SAS provides the "ISUP NP with EPAP" treatments to the ISUP IAMs that meet certain gateway screening criteria using the existing Gateway Screening feature. The Gateway Screening feature will allow SS7 messages to be selected for the "ISUP NP with EPAP" treatments, minimally, based on:

- OPC
- DPC
- SIO
- ISUP message type (IAM and SAM)

For the selected ISUP messages, the EAGLE 5 SAS performs NPDB lookup based on ISUP IAM CdPN (the B-number). If the CdPN is a ported out number, the EAGLE 5 SAS relays the IAM with CdPN=RN + Initial CdPN. If the CdPN is a ported-in or never been ported subscriber, the EAGLE 5 SAS prepends a SubNet prefix, that identifies the SubNet to which the CdPN belongs within the operator network, to the CdPN of the IAM message before relaying the message to its destination. For any other types of CdPN, the EAGLE 5 SAS relays the IAM without modifications. If SAM are used in the network, then SAM should be entered in the Gateway Screening rules.

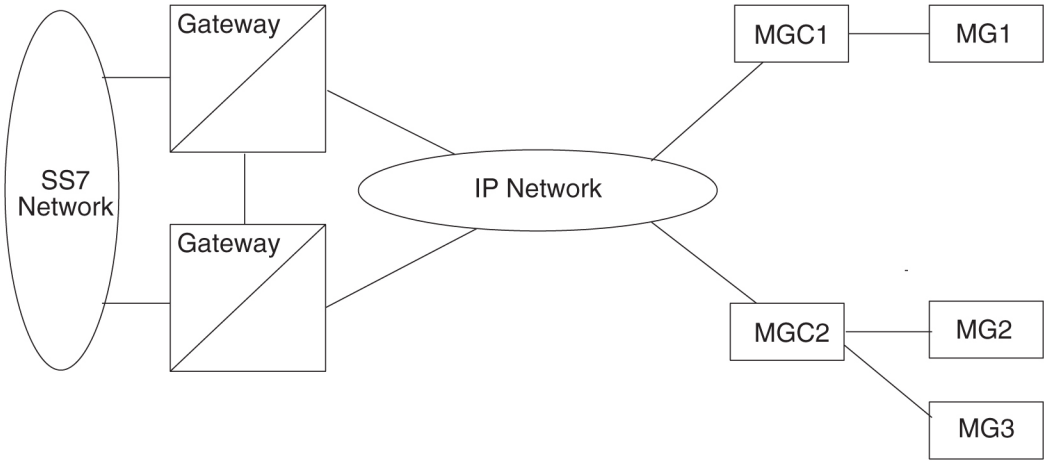
Hardware Requirements

The ISUP NP with EPAP feature does not require any new hardware.

ISUP-Over-IP Gateway for Connectivity to IP-SEPs (IP^7 Release 1.0)

This functionality allows SS7 nodes to exchange ISUP protocol messages with one or more signaling end points (class 4 switches, class 5 switches, VoIP gateways, media gateway controllers (MGCs), or remote access servers) residing on an IP network. The IP ^{7} 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.

Figure 3-12. SEP Connectivity via ISUP over IP



This feature provides TCP/IP point-to-multipoint connectivity by way of a new GPL, SS7IPGW, running on the DCM which, together with the hardware, provides connectivity to databases (or other switching equipment) for SS7 devices that reside on ethernet TCP/IP networks.

A single DCM card running the **SS7IPGW application** provides connections to multiple IP devices (IP-SCPs, class 4 switches, class 5 switches, VoIP gateways, media gateway controllers, or remote access servers.) Multiple DCM cards running the **`SS7IPGW`** application are required, with similar configuration, to provide redundancy. The following is a common sequence of events that illustrates the use of point-to-multipoint connectivity:

1. Traditional SS7 devices route MSUs (such as ISUP Queries) to the gateway.

2. The gateway forwards the translated MSU to the correct TCP/IP device based on point code and filter information in the MSU.

3. The ISUP query is processed at the IP-SEP, and the IP-SEP sends an ISUP reply back to the gateway.

4. The gateway forwards the ISUP reply back to the sender of the original query.

To provide point-to-multipoint connections for SEP connectivity via ISUP over IP, a number of administration steps must first be performed, as follows:

- Set the ISUP over IP feature bit (**`ipisup`**). This is done with the **`chg-feat`** command.

- Links, link sets, destinations and routes to the destinations must be configured.

- The socket connections at each DCM card running the **`SS7IPGW`** application must be configured.

- The SS7 routing keys that are transported over each defined socket at each card must be configured. SS7 routing keys are filters consisting of values representing the DPC, SI, OPC and CIC fields from a incoming MSU message. All MSUs that match the filter are sent to the corresponding socket. The sockets represent TCP sessions. These keys allow for distribution of MSUs on the IP network.

ITU DTA (a.k.a. ITU Triggerless Message Screening) (Release 31.6)

Description

ITU Database Transport Access (DTA) is used to divert SS7 traffic to an internal or external SCP process (via SS7, X.25 or IP) for application handling.

DTA intercepts MSUs that need further application processing and delivers the MSUs to the SCP for modification. The SCP sends the processed MSU to the EAGLE to be routed to its final destination.

The redirect function allows the EAGLE to trap MSUs, modify them, and process the new MSUs as ordinary messages. The redirect function essentially diverts an MSU from the original DPC to the DPC specified by the user.

The original implementation of DTA supported ANSI only. ITU DTA alows transmission to any PC type. However, the EAGLE currently allows only a single DTA DPC to be provisioned. If the incoming message type is not the same as the DTA DPC, the message will be “tunneled” to the DPC. The redirect function encapsulates the original MSU in the SCCP data part of a new MSU. The CgPA SSN is designated as the information element to identify the payload type. Payload types are identified in the following table. Tunneling allows multiple payload types to be carried in the SCCP data. The original DTA implementation for ANSI used SSN=0 for all MSUs; there is no change for ANSI payloads. If the EAGLE ANSI True PC is used, it may be converted to a Secondary Point Code during routing.

Table 3-15. Payload Type MSU encoding information

Payload Type	CgPA SSN	Redirected MSU OPC
ANSI	0	Original OPC
ITU-I/ITU-N	259	EAGLE ANSI True PC
ITU-N24	251	EAGLE ANSI True PC

Tunneling uses a MTP2/MTP3/SCCP header based on the DTA DPC point code type to allow any incoming message to be routed to the DTA DPC. For example, ITU tunneling involves placing an ANSI wrapper around an ITU message and sending it to an ANSI destination. The destination then removes the ANSI wrapper and processes the original ITU information. Tunneling works in the same way for an ANSI MSU encapsulated for an ITU destination.

The original implementation of DTA supported ANSI only. ITU DTA allows transmission to any PC type.

Limitations

- The redirect function must be performed on the receiving LIM.
- Only MTP screening can select MSUs to be redirected. the SCCP screening functions (CGPA, TT, CDPA, and AFTPC) cannot select MSUs to be redirected.
- MSUs may be too large to be encapsulated by the redirect function.
- SLTA (Signal Link Test Acknowledgement) messages should not be redirected. Do not apply a Redirect Stop Action on the Adjacent Node point code for any of the screening functions: **BLKOPC** or **OPC** ..

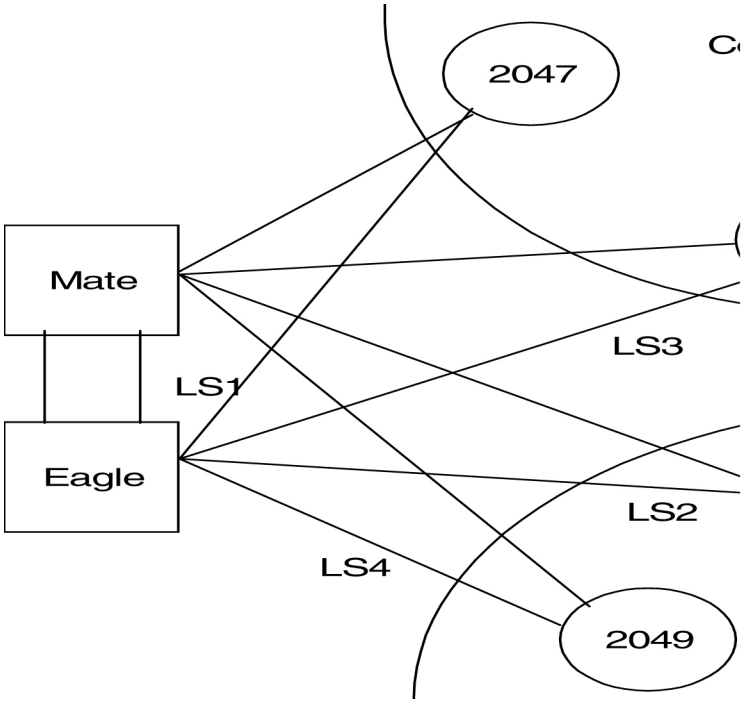
When a Redirect Stop Action is applied to an OPC or BLKOPC screen rule, inbound SLTAs from an adjacent node are not processed by the EAGLE.

- MSUs can be directed only to a single ANSI/ITU-I/ITU-N/ITU-N24 point code.
- Do not apply a Redirect Stop Action for an allowed DPC screen rule if the rule contains the point code of EAGLE where the screening rule is applied. This is because the redirection of SLTA / SLTM's (Signal Link test Messages) will not return to the originating EAGLE and will cause the link to fail.
- If the DTA DPC is the EAGLE, the local SCCP subsystem is active, and TVG is unable to obtain an SCCP granter for the redirected message, the message is discarded without UDTS generation. This could occur if SCCP is overloaded/congested. Discard is the normal operation upon TVG grant failure.
- Do not apply a Redirect Stop Action after any SIO screening rule whereSI=1 or SI=2.

ITU Duplicate Point Code Routing (Release 26.05)

This feature allows an EAGLE STP mated pair to route traffic for two or more countries that may have overlapping point code values. For example, in the network shown in the following figure, both Country 1 and Country 2 have SSPs with a PC value of 2047.

Figure 3-13. Network Example #1



Users must divide their ITU-National destinations into groups. These groups will likely be based on Country. However, one group could have multiple countries within it, or a single country could be divided into multiple groups. The requirements for these groups are:

- No duplicate point codes are allowed within a group.

- ITU-National traffic from a group must be destined for a PC within the same group.
- The user must assign a unique two-letter group code to each group.

For example, in the network shown in the figure, Country 1 can only have 1 point code with a value of 2047. Traffic coming from SSP 2047 in Country 1 can only be destined to other nodes within Country 1. In this example, the user assigns a group code of 1 to Country 1, and a group code of 2 to Country 2.

When the user enters an ITU-National point code, he or she must also enter the group code, using the format "point code - group code". This group code must be used for any command that uses an ITU-N point code.

For current details on this feature, refer to the *Database Administration Manual - SS7* .

ITU Gateway Measurements Enhancements (PR19536) (Release 26.05)

Description

The ITU GTWY measurements schedule allows for the collection and reporting of ITU gateway-related data from the STP. The EAGLE already has ANSI GTWY measurements collection and reporting facility in place, but the LIM & SCCP cards do not currently measure the ITU data required to be reported in the GTWY measurements schedule.

To address this situation, the LIM & SCCP cards have been modified to measure this data, and the OAM has been modified to collect it from the MTP (LIM) and SCCP cards, store it, and report it when requested.

The OAM currently polls MTP and SCCP cards every 30 minutes for GTWY measurements data. The responses the MTP/SCCP cards send back in response to these polls has been extended to include the ITU gateway-related data required by the ITU GTWY measurements. The OAM now stores this data in the measurements database, and retains it for a 25-hour period (same as for ANSI measurements).

New Measurements Reports Implemented for this Feature

The following ITU GTWY measurements have been implemented for this feature.

- The ITU GTWY measurements for the STP, LNKSET, LSDESTNI and LSORIGNI entity types have been implemented. The implementation is based on the existing ANSI GTWY measurement processing, with the exception that the ITU GTWY measurements are done per Linkset basis, whereas ANSI measurements are done per Linkset per NI basis.
- The measurements for entity type LNKSET provide the counts for various types of MSUs (for example, TFP/TCP, TFR/TCR, TFA/TCA, SLTA/SLTM, sub-system messages, and so on) received and transmitted per ITU GTWY Linkset.
- The measurements for entity type LSDESTNI provide the counts for inter-network messages received and transmitted per ITU GTWY Linkset.
- The measurements for LSORIGNI provide the counts for the various types of MSUs rejected, as a result of Gateway Screening failure due to one or more factors. The measurements are done per linkset basis.

- The STP-GTWY measurements provide the aggregate of other GTWY types measurements on a system total basis.

The diagrams below illustrate various GTWY configurations (OPC/ DPC in networks other than EAGLE's Adj Point Code).

Figure 3-14. ANSI Gateway Configuration - (Linksets LSA1 & LSA2 are ANSI Gateway Linksets)

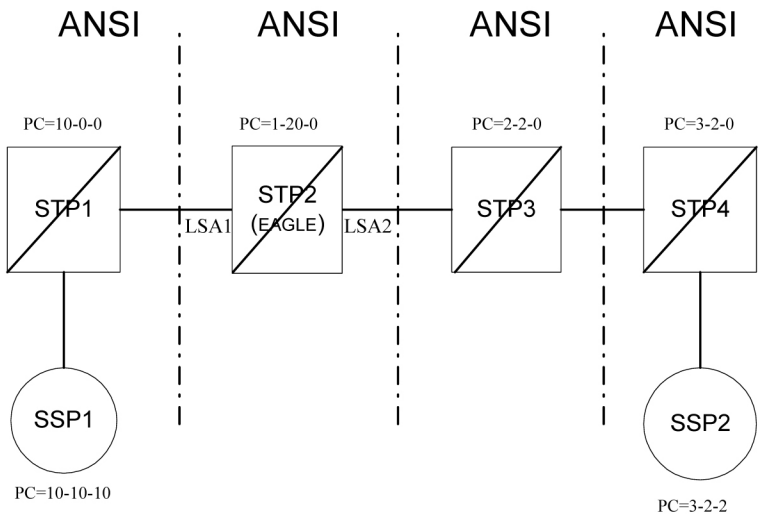


Figure 3-15. ITU Gateway Configuration (Linksets LSI1 & LSI2 are ITU Gateway Linksets)

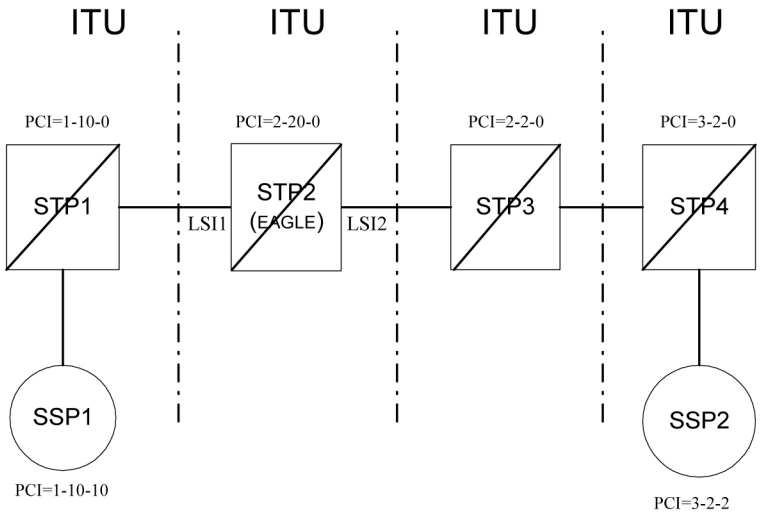
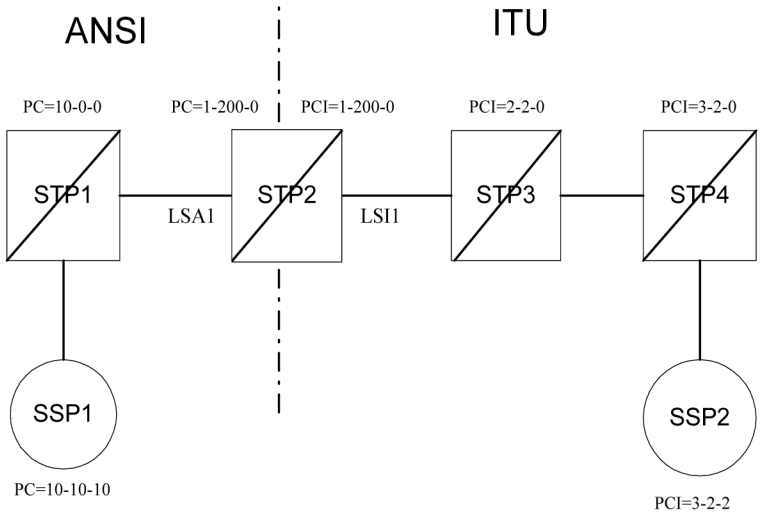


Figure 3-16. ANSI-ITU Gateway Configuration



To obtain these measurement reports via the EAGLE interface, the value "**gtwy**" must be specified for the **type** parameter for the **rept-meas** command. For the **rept-meas:type=gtwy** command, support for STP, LNKSET, LSDESTNI and LSORIGNI as valid values for the **type** parameter is continued.

ITU International and National Spare Point Code (Release 34.0)

Description

The EAGLE allows a network operator to use the same Point Codes across two networks (either ITU-I or ITU-N). The feature also enables both ITU spare and non-spare traffic to be routed over the same linkset. The EAGLE uses the MSU Network Indicator (NI) to differentiate the same point code of one network from the other. In accordance with the SS7 standard, unique Network Indicator values are defined for ITU-I, ITU-N, ITU-I Spare, and ITU-N Spare Point Code types.

The EAGLE currently provides full support for four types of point codes:

- ANSI, ITU-National (NI=10binary)
- ITU-National 24-bit
- ITU-International (NI=00 binary)
- ITU National Spare PCs (NI=11 binary) can be primarily supported via a combination of the following two items:

    1. Support for ITU-National Spare can be set on a per linkset basis using the linkset NIS parameter. If set, the EAGLE will allow receipt of messages with NI=11binary on the designated linkset and will force all outgoing messages on that linkset to have NI=11binary.
    2. The Duplicate Point Code routing feature, combined with the Multiple Point Code Support feature, can be used to create a separate routing group for a National Spare Point Code network.

    While these two functions can be combined to support ITU National Spare Point Code routing, there are limitations described as follows:

— The EAGLE cannot distinguish between messages with different network indicators received over the same linkset. For example, the EAGLE will route a message with DPC = 1-1-1 (NI=10binary) the same way as a message with DPC = 1-1-1 (NI=11binary).

— Forcing the user to use the Duplicate PC Routing feature requires that all linksets in the system be placed in one of the defined groups.

The Spare Point Code Support feature addresses the above limitations and provides a new PC sub type named Spare that supports both the ITU-N Spare and ITU-I Spare Point Code feature.

Additionally, this feature requires a single linkset to support multiple outgoing network indicators (e.g. 11 binary, 00 binary). In turn, messages are routed according to the Point Code on the outgoing node that corresponds to the associated network indicator.

Hardware Requirements

There is no new hardware for this release.

Limitations

1. This feature does not allow the EAGLE to MTP convert between National and National Spare Point Codes. Likewise, this feature does not allow the EAGLE to MTP convert between International and International Spare Point Codes.
2. In the destination table, an ITU-I alias and an ITU-I Spare alias cannot be defined for the same Point Code, likewise an ITU-N alias and an ITU-N Spare alias cannot be defined for the same point code.
3. The feature is not supported on the SEAS interface. Spare point codes are only supported for ITU point codes, and SEAS only supports ANSI point codes. Any Private ANSI point code provisioned using the standard EAGLE 5 SAS command line interface is not displayed by the SEAS VFY- command.
4. ITU National and ITU National Spare Point Code are implemented as separate network domains that can co-exist within the same STP.
5. Spare point codes are not supported for IPGWI sockets using TALI protocols. The spare point code feature may not be enabled if any application sockets have been provisioned on IPGWI cards.
6. The existing implementation of Gateway Screening does not support Group Code (Duplicate Point Codes). Gateway Screening will also not support PPCs.
7. The Spare Point Code and PPC prefix value, s- and p- do not apply to domain type point codes for ANSI and ITU-N24.
8. ITU-N and ITU-N24 Point Codes cannot co-exist as SID Destination True Point Codes and therefore ITU-N Spare and ITU-N24 Point Codes cannot coexist as SID Destination True Point Codes.
9. A single STPOPTS value (cnvcgdi) will be used to control message handling for ITU-I and ITU-I Spare messages when the CgPA PC does not have a required alias.
10. A single STPOPTS value (cnvcgdn) will be used to control message handling for ITU-N and ITU-N Spare messages when the CgPA PC does not have a required alias.
11. The existing implementation of the SRVSEL command interface to the SRVSEL table does not provide a way to separate MSU traffic for different ITU National Group Code networks. Therefore no provision is made for the SRVSEL command to control the separation of ITU spare and non-spare traffic. The SRVSEL table applies to the EPAP based features G-FLEX, INP, G-PORT, SMS Prepaid, and IS-41 to GSM

Migration. Likewise, no provision is made for the GTTSEL command interface to the GTTSEL table to allow separation of ITU spare and non-spare traffic for EGTT, VGTT and MGTT.

ITU MTP Restart (Release 26.0)

Description

ITU MTP restart is a network management feature. It enables a restarting signaling point to bring a sufficient number of signaling links into the available state, and to update its routing tables before user traffic is restarted to the newly available signaling point.

This feature enables operators to implement ITU MTP Restart throughout their networks.

A central part of the restart procedure is the exchange of network status information between the restarting MTP and the adjacent nodes. In order for the procedure to make sense, the network status should not change significantly during this information exchange. As a consequence, there is an overall restart time defined for the node whose MTP is restarting as well as for the adjacent nodes. During this time, all activities within the node whose MTP is restarting as well as the adjacent nodes should be completed. This requires that the time available is used in an efficient way.

As a basis of the restart procedure, it is assumed that most of the signaling points within the network are accessible. Thus at the beginning of the restart procedure, all concerned routes are considered to be allowed, and the update of the network status is performed by the exchange of transfer-prohibited (TFP) and/or transfer-restricted (TFR) messages. The MTP restart procedure uses the Traffic Restart Allowed (TRA) message that is defined in section 15 of Q.704.

When an adjacent node has finished sending all relevant TFP and/or TFR messages to the node with the restarting MTP, it finally sends a TRA message that indicates that all relevant routing information has been transferred. Thus, at the node with the restarting MTP, the number of received TRA messages is an indication of the completeness of the routing data.

When the restarting MTP has completed all actions or when the overall restart time is over, it sends TRA messages directly to all of its adjacent nodes accessible via a direct link set. These messages indicate that the restart procedure is terminated and User traffic should be started.

Refer to the *Database Administration Manual - SS7* for current information on this feature.

Upgrade Considerations

ITU MTP Restart introduces four new timers into the EAGLE's Level 3 Timer Table (IT18, IT19, IT20, IT21). There now resides 24 extra bytes of padding in the Level 3 Timer structure. With each timer taking 4 bytes, the total number of bytes needed for the new timers is 16 bytes.

The Level 3 Timer provides plenty of space to house the four new timers. Therefore during upgrade, only a conversion function will be required to handle the new table. This will convert the old structures without the timers to the new structures with the new timers, and set the new timers to their default values.

Measurements

The measurement MTPRESTS will be pegged when EAGLE restarts. This is an existing peg count that was previously used by ANSI restart, and will now be used for ANSI Only Restarts, ITU Only Restarts, and Mixed ITU/ANSI Restarts.

Limitations

1. The EAGLE will delay bringing into service Linksets that are not Restart Capable (**`mtprse=no`**) until after Restart is Complete.

2. While it is desirable to bring one link per linkset into service first when performing a Full Restart, because of the EAGLE's distributed architecture there is no advantage to this. Thus the EAGLE tries to align all links.

3. The restarting node should stop T18 when sufficient links are available, and enough TRA messages have been received. The EAGLE will stop T18 when all activated restart capable links are available, and it has received TRAs on all restart-capable linksets.

4. If all ITU links fail, but the EAGLE still has ANSI links available, the EAGLE will not perform a Full MTP Restart. In a Mixed ANSI/ITU network, the EAGLE will only perform a Full restart if all links, both ITU and ANSI, fail.

5. TFPs received on a link before the link is available at Level 3 will not be processed.

ITU SLS Enhancements (Release 26.0)

Description

The ITU SLS Enhancements feature gives EAGLE customers the ability to modify the method the EAGLE distributes traffic across ITU SS7 links.

EAGLE uses the LSB of SLS to load share between linksets of a combined linkset. ITU-T ISUP messages use a SLS that is obtained from the lower 4 bits of the CIC field representing the circuit being used.

CIC selection can be determined based on an odd/even method where a SSP uses either all odd CICs, or all even CICs, to help prevent “glaring” (i.e., 2 SSP attempting to seize the same trunk at the same time). This causes the LSB of the SLS to be fixed; if the LSB is fixed, inadequate load sharing occurs for the SS7 network. This situation can also occur within a single linkset (international), since EAGLE also uses the SLS (containing a fixed LSB) to select a link within a linkset.

Refer to the *Database Administration Manual - SS7* for current information on this feature.

Restrictions

When two linksets are used as a combined linkset, they should have the same *Other CIC Bit* and *Rotated SLS Bit* settings. This is not enforced in the EAGLE, and there is no warning mechanism for incorrectly provisioned linksets and routes

Upgrade Considerations

- Default values “Bit Rotation” and “Other Bit” must be set in LS tables during upgrade from Release 25 to 26.

- The *Use Other CIC Bit* feature bit must be set to disabled during the upgrade.

ITUN-ANSI SMS Conversion (Release 37.0)

Description

The ITUN-ANSI SMS Conversion feature performs SMS address conversion for Registration Notification, SMS Request Return Result, and SMS Notification messages crossing the ITUN-ANSI network boundary to determine the destination point code in the destination network.

A FAK is required to enable the ITUN-ANSI SMS Conversion feature.

The ITUN-ANSI SMS Conversion feature modifies the SMS Address parameter in the TCAP/IS41 layer of the Registration Notification, SMS Request Return Result, and SMS Notification messages that cross the ITUN-ANSI network boundary. These messages are called identified messages and are modified per the destination network type. The SMS Address parameter in the identified messages must contain an ANSI or ITU-N point code value to enable the ITUN-ANSI SMS Conversion feature to process the messages.

Feature Control Requirements

The ITUN-ANSI SMS Conversion feature has the following feature control requirements:

- A FAK for part number 893-0153-01
- A temporary key cannot be used to enable the feature.
- After the feature has been turned on, it cannot be turned off.

Hardware Requirements

The ITUN-ANSI SMS Conversion feature requires DSM or TSM cards running the SCCP application

Limitations

The ITUN-ANSI SMS Conversion feature has the following limitations:

- ITU-I and ITUN-24 point codes are not supported.
- If DSM and TSM cards are down, the ITUN-ANSI SMS Conversion is not performed.

ITU-TFR Procedure (Release 26.1)

Currently, the EAGLE implements most, but not all, of the signaling route management capabilities defined in ITU-T recommendation Q.704, section 13. In particular, those capabilities defined as national options are not yet implemented.

The ITU TFR (International Telecommunication Union - Transfer Restricted) feature implements the transfer-restricted procedures defined in section 13.4 of Q.704 [1]. The TFR procedure is used to redirect traffic away

from a STP that is having problems routing traffic to a destination. When a STP determines that a destination is restricted, the STP will send, to its adjacent SPs, a TFR message containing an affected destination.

When a destination is restricted, the STP should not be used to route messages to the destination, even though it still has limited capability to do so. The TFR message is sent to the adjacent STPs to inform them of this condition.

The ITU TFR procedure can be enabled or disabled on a per ITU-N linkset basis (see "ITU Gateway Measurements Enhancements (PR19536) (Release 26.05)"). When the TFR procedure is enabled on a given linkset, TFR messages can be sent to the adjacent PC for the affected destinations.

NOTE: The procedure does not apply to ITU-I linksets. The ANSI network employs its own similar version of the TFR procedure for ANSI linksets.

Upgrade Considerations

Default values for "ITU TFR Procedure" must be set in LS tables during upgrade to Release 26.1. **Table 3-16** shows the tables requiring modifications during the upgrade process.

Table 3-16. Tables and Fields Affected by Upgrade

Modified Tables	New Fields	Size	Value
Linkset	ITUTFR	1 byte	0 (off)

New UIMs

This feature introduces a new UIM that is output in the event a TFR message is received on a ITU-N linkset that does not support the ITU TFR Procedure (parameter is OFF).

```
1233 MTP Invalid ITU TFR RCVD
```

When this occurs, the craftsperson should check if the **itutfr** parameter needs to be enabled for the linkset, or if the problem exists on an adjacent STP.

KSR Terminal Feature (Release 20.0)

The Keyboard Send Receive (KSR) feature enhances the EAGLE's dial-up administration functions by allowing faster throughput, since the control characters associated with the VT320 mode of terminal operation need not be transmitted.

The command used to modify the terminal configurations has a new parameter added to enable the KSR feature.

[1] *ITU-T Recommendation Q.704, SS7 - Signalling network functions and messages*, ITU-T, July 1996.

4

Features L - O

Large BICC MSU Support for IP Signaling (Release 37.0)

Description

The Large BICC MSU Support for IP Signaling enhances the EAGLE 5 ISS by increasing the SIF size of the BICC MSUs that the system can send and receive from 272 bytes to 4095 bytes over the M2PA and M3UA protocols.

A FAK is required to enable the Large BICC MSU Support for IP Signaling feature.

The Large BICC MSU Support for IP Signaling feature increases the SIF size of the Bearer Independent Call Control (BICC) MSUs that the EAGLE 5 ISS can send and receive over the M2PA and M3UA protocols from 272 bytes to 4095 bytes.

The Large BICC MSU Support for IP Signaling feature allows large BICC MSU traffic on IP7 signaling-links/ connections cards. The cards that support the feature include the SSEDCM cards (SS7IPGW, IPGWI, IPLIM, and IPLIMI GPLs) and the E5-ENET cards (IPGHC and IPLHC GPLs).

The feature also prevents routing of large BICC MSU traffic on non-IP7 GPLs. The IPGWx software rejects a large BICC MSU if it arrives on a double-slot DCM card. If a large BICC MSU is rejected, then the MSU is discarded, a discard measurement is updated, and a UIM is issued.

The feature supports ANSI, ITU-N, ITU-I and ITU-N24 networks.

If the feature is enabled and turned on, then BICC MSUs with a SIF size greater 272 bytes can be routed. MSUs with a SIF size that is equal to or less than 272 bytes can be routed when the feature is not enabled.

NOTE: Data feed to the Sentinel and IMF systems is not supported for BICC MSU messages with a SIF size greater than 272 bytes. DTA and STP LAN do not support large BICC MSUs. If a large BICC MSU initiates DTA or STPLAN processing, then the MSU is routed without copying and the appropriate UIM will be issued. See Table FN-3 on page FN-94 for more information for the UIMs generated for the Large BICC MSU Support for IP Signaling feature.

Measurements

The following LINK-COMP measurements are added for the Large BICC MSU Support for IP Signaling feature:

- LMSURCV: Number of large MSUs received
- LMSUTRN: Number of large MSUs transmitted
- LMSUOCTRCV: Number of octets received in large MSUs
- LMSUOCTTRN: Number of octets transmitted in large MSUs
- LMSURCVDSC: Number of large MSUs discarded in the receive path
- LMSUTRNDSC: Number of large MSUs discarded in the transmit path

Feature Control Requirements

The Large BICC MSU Support for IP Signaling feature has the following feature control requirements:

- A FAK for part number 893-0184-01
- A temporary key cannot be used to enable the feature.

- The feature can be turned off after it is turned on.

Hardware Requirements

None.

Limitations

None.

Large System (Phase 3)—1500 Links (Release 29.0)

Description

The Large System (Phase 3)—1500 Links feature is the EAGLE with 1,500 links.

Customers continue to rapidly expand their link capacities beyond the configuration supported in previous releases. The Large System—Phase 2 feature with 1200 links, 115 ATM cards and 100 IPLIMs, implemented in Release 28.0, has been expanded to include additional links, as well as Sigtran-based associations.

With the increased number of links (and with the introduction of the 6,000 Routesets feature) the Multicast traffic will grow significantly.

With this feature, the total number of signal links supported by EAGLE is 1500 total links per system. The EAGLE also enforces the following link/card counts:

- Maximum of 1500 links is the total number of links supported per system:
  - Default of 1200 links are allowed
  - Allow maximum 1500 links by Feature Key
- Within the total number of links allowed, the user may provision:
  - Maximum 115 ATM cards
  - Maximum 100 IPLIM cards
  - Maximum 2 SS7IPGW (ANSI) application DCM cards
  - Maximum 2 IPGWI (ITU) application DCM cards

The EAGLE enforces a maximum link count of 1500 total links per system, as well as the following link/card counts:

- Maximum 1500 links
- Maximum 115 ATM cards

- Maximum 100 IPLIM cards
- Maximum 2 IPGTWY cards

For this feature, the EAGLE provides feature access keys to exceed 1200 links. The default for these feature access key is OFF.

Hardware Requirements

No new hardware required or introduced to support the software. However, in order to provision more than 1,200 links, the EAGLE must be equipped with the HMUX and TDMs (870-0774-10) or later, and GPSM-II must be the active and standby EOAM.

CAUTION: Never install or initialize MCAP cards in MASP slots 1113 and 1115 after features that require GPSM-II cards are provisioned. Attempting to initialize MCAP cards with GPSM-II features provisioned will cause a system outage. Before replacing an existing GPSM-II card in a MASP slot (1113 and 1115) contact Tekelec Customer Service.

Large System (Release 27.2)

Description

EAGLE 27.2 introduces the Large System Feature, which increases the number of SS7 high- and low-speed links supported by the EAGLE, currently limited to 500 links per system, to 700 links.

The EAGLE Large System supports, with the existing 250 available card slots, the simultaneous operation of the following combinations of links:

Table 4-1. Large System Configurations

Configuration	ATM Links	Low Speed Links
Configuration #1	100	600
Configuration #2	0	700

- Low speed links are defined as 56kb/sec or 64kb/sec links achieved through multi-port LIMs or any combination of the multi-port LIMs and 2-port LIMs.
- ATM links are defined by the existing EAGLE High Speed Link feature provided via the LIM-ATM board. Up to 100 of the 700 links can be LIM ATM links.

Large System—Phase 2 (Release 28.0)

Description

This feature builds upon the Large System foundation, and increases the number of SS7 high- and low-speed links supported by the EAGLE to 1200 links.

Refer to the *Database Administration Manual - SS7* for more information.

Hardware Required

To provision up to 1200 signaling links in the database, the following hardware must be installed:

- HMUX cards, P/N 870-1965-XX, replacing all the IPMX cards.
- GPSM-II, P/N 870-2360-XX or later, installed in card locations 1113 and 1115.

CAUTION: Never install or initialize MCAP cards in MASP slots 1113 and 1115 after features that require GPSM-II cards are provisioned.

Attempting to initialize MCAP cards with GPSM-II features provisioned will cause a system outage. Before replacing an existing GPSM-II card in a MASP slot (1113 and 1115) contact Tekelec Customer Service.

- TDM, P/N 870-0774-10 or later, installed in card locations 1114 and 1116.
- Control Shelf Backplane, P/N 850-0330-06
- The Measurements Platform feature must be enabled.
- Enough Multiport LIMs (MPL), P/N 870-1826-XX, or E1/T1 MIMs, P/N 870-2198-XX to bring the number of signaling links from 701 to 1200, installed according to the provisioning rules for a 1200 signaling link system; see the following section. The system can contain a mix of 2-port LIMs, Multiport LIMs, and E1/T1 MIMs.

For detailed hardware information, refer to the *NSD Hardware Manual*.

Last 10 Command Retrieval (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)

Description

Currently the EAGLE supports retrieving the last command entered from the terminal only. Customers use this feature when making multiple entries that require only minor changes to the previous command. They want the ability to display the last 10 commands entered, in a manner similar to the DOSKEY function.

The Last 10 Command Retrieval feature supports command retrieval of at least the last 10 commands entered at KSR, VT 320, and SCCS type terminal (up to 20 commands for IP User Interface terminals). This capability is supported at the EAGLE MMI terminals, as well as at terminals connected via the IP user interface.

NOTE: This feature is supported only on KSR, VT 320, and SCCS type terminals. Terminals configured as SEAS or OAP terminals are not supported for this feature.

Hardware Requirements

No new hardware is needed to support this feature.

Limitations

Resetting the COM parameters on terminal clears the history queue. This is only done internally by software. This occurs when a terminal is inhibited and allowed (i.e. **`inh-trm:trm=xx`** and **`alw-trm:trm=xx`**) or Kermit transfer is initialized (i.e. with command **`act-file-trns`**).

Link Failure Status Information (Release 22.0)

The level 2 SS7 data is divided into 2 groups, service data and alignment data.

Service data is a running history of when the link comes in service and goes out of service. The history contains the reason the link fails from the perspective of Level 2 along with the timestamp. This information can be used to help solve whether the near end or far end node is responsible for causing the link to fail. This is a list of all the possible level 2 link failure reasons.

- RC/BSNR link failure — Received two out of three invalid backward sequence numbers from the far end. The far end office should be contacted to determine why invalid BSNs are being sent.
- RC/FIBR link failure — Received two out of three invalid forward indicator bits from the far end. The far end office should be contacted to determine why invalid FIBs are being sent.
- SIE received — Received status indication of Emergency from the far end. An SIE indicates the far end is now being aligned. The far end office should be contacted to determine why an SIE was sent.
- SIN received — Received status indication of Normal from the far end. An SIN indicates the far end is now being aligned. The far end office should be contacted to determine why an SIN was sent.
- SIO received — Received status indication of Out of Alignment from the far end. An SIO is sent when the node begins initial alignment. The far end office should be contacted to determine why an SIO was sent.
- SIOS received — Received status indication of Out of Service from the far end. An SIOS is sent upon completion power up until initial alignment is started. An SIOS is also sent when the far end cannot transmit or receive message signal units for reasons other than processor outage. The far end office should be contacted to determine why an SIOS was sent.
- Stop commanded — Level 3 commanded Level 2 to stop.
- Stopped receiving data — No data is being received on the signaling link. Check the physical connections of the signaling link. Using an analyzer, test for level 1 and level 2 functions.
- SUERM link failure — Signal Unit Error Rate Monitor (SUERM) counter exceeded threshold. The SUERM maintains a counter to estimate the signal unit error rate. The far end office should be contacted to determine why the error rate is high.
- Too many ISCC interrupts — Too many interrupts received over the link.
- TXC/T6 expired — Remote congestion timer expired. The far end is in congestion too long. The far end office should be contacted to determine why BSN and BIB are not being sent.

- TXC/T7 expired — Excessive delay of acknowledgment timer expired. Far end taking too long to acknowledge the messages sent to it by the near end. The far end office should be contacted to determine why the delay in acknowledging MSUs.

The level 2 link failure reason shows which node on the link caused the fault and why. If the history shows the link did not realign after the failure, the alignment data buffer shows the reason the link was unable to be realigned.

Alignment data is a running history of Level 2 alignment events with timestamps. This information can be used to help solve why the link does not realign.

Alignment events are buffered during the out of service, initial alignment, aligned/ready and aligned/not ready states. Only the first unique occurrence of an event and its timestamp is buffered. Alignment events are transmitted signal units, received signal units, level 3 commands, level 2 status and state transitions. The following table lists all the possible alignment events sorted by event type. Realignment may fail for reasons other that the events listed in the table. For example, realignment fails if an SIO is received when the link is in the aligned/ready state. Therefore, the failure reason is displayed as an abnormal link state control state transition.

Table 4-2. Signaling Link Alignment Events

Transmitted	Received	State	Event
FISU	FISU/MSU	IAC Idle	AERM/Abort proving
SIO	SIO	IAC Not aligned	T2 expired
SIE	SIE	IAC Aligned	T3 expired
SIN	SIN	IAC Proving	Exceeded proving period count
SIB	SIB	Out of Service	Stop commanded
SIOS	SIOS	Initial Align	SUERM link failure
SIPO	SIPO	Align/Ready	RC/BSNR link failure
		Align/Not Ready	RC/FIBR link failure
		In Service	Stopped receiving data
		Processor Outage	Too many ISCC interrupts
			T1 expired

These are definitions of the alignment failure reasons.

- AERM/Abort proving - Alignment Error Rate Monitor (AERM) counter exceeded threshold. AERM increments a counter if it detects an error in the signal unit. Aborting the proving period causes the proving period count to be incremented. If the proving period count exceeds its threshold, the link will fail with the Level 2 Exceeded proving period count failure reason. The far end office should be contacted to determine the cause for the high error rate.

- Exceeded proving period count - The proving period was aborted five times by the AERM before the proving period timer expired. The far end office should be contacted to determine the cause for the high error rate.

- RC/BSNR link failure — Received two out of three invalid backward sequence numbers from the far end. The far end office should be contacted to determine why invalid BSNs are being sent.

- RC/FIBR link failure — Received two out of three invalid forward indicator bits from the far end. The far end office should be contacted to determine why invalid FIBs are being sent.
- Stop commanded — Level 3 commanded Level 2 to stop.
- Stopped receiving data — No data is being received on the signaling link. Check the physical connections of the signaling link. Using an analyzer, test for level 1 and level 2 functions.
- SUERM link failure — Signal Unit Error Rate Monitor (SUERM) counter exceeded threshold. The SUERM maintains a counter to estimate the signal unit error rate. The far end office should be contacted to determine why the error rate is high.
- T1 expired - Align/Ready timer expired. Far end is not responding during Aligned/Ready or Aligned/Not Ready states before timer expires. The far end office should be contacted to determine why the far is not responding.
- T2 expired - Not aligned timer expired. Far end is not responding during Not Aligned Initial Alignment Control state before timer expires. The far end office should be contacted to determine why the far end is not responding.
- T3 expired - Aligned timer expired. Far end is not responding during Aligned Initial Alignment Control state before timer expires. The far end office should be contacted to determine why the far end is not responding.
- Too many ISCC interrupts — Too many interrupts received over the link.

The service data and alignment data is displayed with the **`L2stats`** parameter of the **`rept-stat-slk`** command. The **`L2stats`** parameter has the following values:

`no` = don't display Level 2 status information (the default value)

`align` = display alignment data only

`service` = display service data only

`both` = display both alignment and service data

`brief` = display at most last 10 alignment data events only

The alignment data is displayed in a three column format. Column 1 is the type of event that was buffered. Column 2 is the event. Column 3 is the timestamp for the event.

The service data is displayed in a two column format. Column 1 contains the event. Column 2 has the corresponding timestamp.

The following is an example of how the service data and alignment data is displayed.

Input/Output Examples

`rept-stat-slk:loc=1203:port=b:L2stats=both`

```
SLK    LSN       CLLI        PST            SST       AST
1203,B lsnsspn2  ----------- OOS-MT-DSBLD   LPBK     ISCC

Event Type Event               Timestamp
Transmit   SIOS                97-06-07 10:04:23.000
State      Out of Service      97-06-07 10:04:23.000
State      Initial Align       97-06-07 10:05:31.100
State      Idle                97-06-07 10:05:31.100
Transmit   SIO                 97-06-07 10:05:31.105
```

```
State      Not Aligned          97-06-07 10:05:31.105
Receive    SIO                  97-06-07 10:05:46.425
Transmit   SIN                  97-06-07 10:05:46.430
State      Aligned              97-06-07 10:05:46.430
Receive    SIN                  97-06-07 10:06:02.110
State      Proving              97-06-07 10:06:02.120
Receive    SIN                  97-06-07 10:06:02.885
State      Idle                 97-06-07 10:06:53.625
Transmit   FISU                 97-06-07 10:07:14.000
State      Align/Ready          97-06-07 10:07:14.000
Receive    FISU                 97-06-07 10:08:01.760
State      In Service           97-06-07 10:08:01.760

Service Event       Timestamp
In Service          97-06-07 02:11:54.875
SIOS received       97-06-07 05:40:10.160
In Service          97-06-07 05:42:12.235
SIOS received       97-06-07 09:37:02.100
In Service          97-06-07 09:38:55.995
SUERM link failure  97-06-07 10:02:02.125
In Service          97-06-07 10:08:01.760
```

rept-stat-slk:loc=1203:port=b:L2stats=brief

```
SLK    LSN       CLLI        PST            SST       AST
1203,B lsnsspn2  ----------- OOS-MT-DSBLD   LPBK     ISCC

Event Type Event               Timestamp
Transmit   SIOS                97-06-07 02:44:23.000
State      Out of Service      97-06-07 02:44:23.000
State      Initial Align       97-06-07 02:45:31.100
State      Idle                97-06-07 02:45:31.100
Transmit   SIO                 97-06-07 02:45:31.105
State      Not Aligned         97-06-07 02:45:31.105
State      T2 Expired          97-06-07 02:45:46.425
```

If a card is unplugged, the link status information is lost.

The alignment data buffer and service data buffers are circular buffers that can hold 69 events.

The level 2 statistics can only be displayed for SS7 LIMs. If the specified signaling link is not an SS7 LIM, the command is rejected and this message is displayed.

Error Message

```
E2918 Cmd Rej: Link must be SS7 to display Level 2 stats
```

Link Fault Sectionalization (Release 21.0)

Overview

The EAGLE STP supports up to 16 Link Fault Sectionalization (LFS) tests at one time and a maximum of 32 remote link elements for each LFS Test while being able to display real time results of the tests in progress.

Link fault sectionalization allows maintenance personnel, using industry standard error patterns, to perform DSOA fault sectionalization tests, a series of far-end loopback tests from the local EAGLE STP or to a remote EAGLE STP, and to identify faulty segments of an SS7 transmission path up to and including the remote network element. Refer to the following two figures.

The SS7 LIM must be powered up and provisioned with the signaling link deactivated before starting the link fault sectionalization tests. No messages are transferred to or from the signaling link by the SS7 LIM while the link is performing a link fault sectionalization test.

Figure 4-1. DS0 Link LBPs for Latching Test

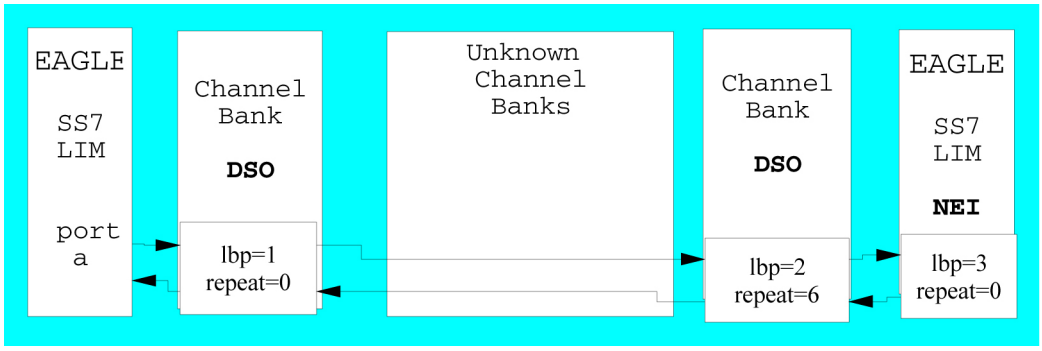
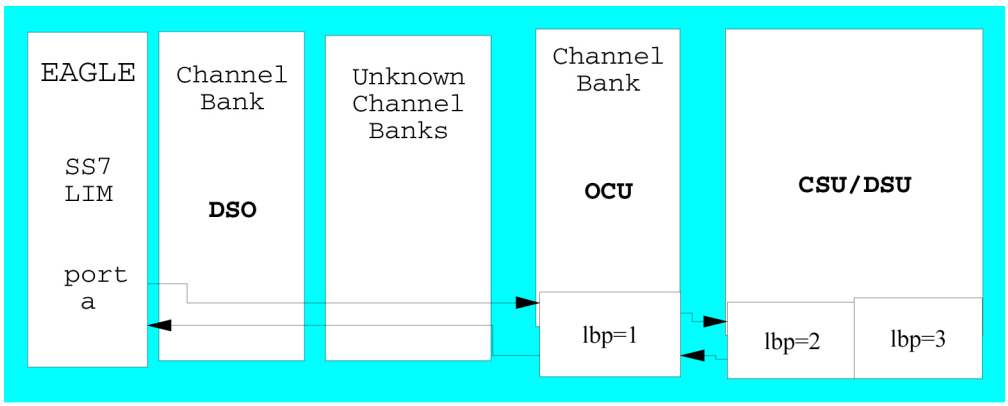


Figure 4-2. OCU/DCU Link LBPs for Non-Latching Test



The point on the signaling link at which each loopback test ends is called the far-end loopback point. A far-end loopback point (LBP) is achieved when the remote link element (RLE) sends the received data back to the transmitter, allowing the transmitter to verify the received data.

The remote link elements are shown in the following table.

Table 4-3. Link Fault Sectionalization Tests Remote Link Element (RLE) Types

Element	RLE Description	Latching	Nonlatching
DSO	DSO Dataport	Yes	No
OCU	OCU Dataport	Yes*	Yes
CSU	CSU Dataport	Yes*	Yes
DSU	DSU Dataport	Yes*	Yes
NEI	Network Element Interface	Yes	No
* The OCU, CSU and DSU must be strapped or optioned to support latching link fault sectionalization loopback.			

The LBP is moved along the signaling link path until the LBP is in the far-end network element. Therefore, each LBP along the link requires the initiation of one link fault sectionalization test on the SS7 LIM.

The link fault sectionalization test types for loopback tests are shown in the following table.

Table 4-4. Link Fault Sectionalization Test Types

Link Fault Sectionalization Test Types	Description
Latching link fault sectionalization test (LLT-auto)	A loopback point is established using signaling commands and remains until it is removed by signaling commands.
Latching link fault sectionalization test (LLT-man)	A loopback point is established by manual means and remains until it is removed by manual means.
Nonlatching link fault sectionalization test (NLT)	A loopback command is interleaved with the test data.

Remote Loopback Testing for DS0A

This capability allows a LIM card at a remote location running the *ss7ansi* application to be placed in loopback automatically when it receives a valid latching loopback code sequence from the network (when a test pattern is detected). This allows the signaling link connected to that card to be tested from another far-end network element or maintenance test unit. While in loopback mode, the signaling link assigned to the LIM card that is in loopback mode is out of service.

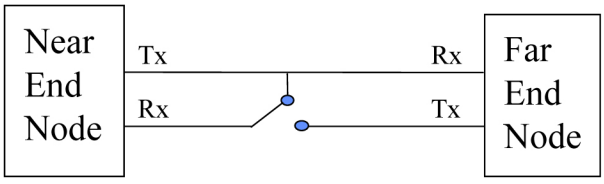
Remote Loopback Testing for OCU

This feature allows a LIM card (configured as a LIMOCU) running the *ss7ansi* application to be placed in loopback automatically when it receives a valid latching loopback code sequence from the network (when a test pattern is detected). Both latching and nonlatching loopback are supported. Because latching and nonlatching loopback cannot be mixed in a network, the loopback testing mode selected depends on the network configuration and configuration of OCU channel bank. The OCU channel back recognizes the loopback control codes and does a current reversal. The LIMOCU only sees a current reversal and acts on that without knowing whether it is latching or nonlatching. While in loopback mode, the signaling link assigned to the LIM card that is in loopback mode is out of service.

Link Diagnostics

Link Diagnostics provides detailed status information of link failures. This capability either confirms or eliminates a portion of the near-end node as the reason for the link failure.

Figure 4-3. Link Diagnostic Diagram



SS7 Level 2 status information is buffered before and after a link failure has occurred. This feature provides the capability to loop the internal transmit and receive data on the LIM card. Link failures can occur on the near end node, far end node, or the cable connecting the two nodes.

Link Failure Status Information

The Level 2 SS7 data is divided into two groups: service data and alignment data.

Service data is a running history of when the link comes in service and goes out of service. The history contains the reason the link fails from the perspective of Level 2 along with the timestamp. This information can be used to help solve whether the near end or far end node is responsible for causing the link to fail.

Alignment data is a running history of Level 2 alignment events with timestamps. This information can be used to help determine why the link does not realign.

The service and alignment data buffer and service data buffers can each hold 69 events.

Hardware Configuration

The link fault sectionalization feature requires a LIM running the SS7ANSI application with the AINF interface. With this interface, the test data is guaranteed to be a continuous data stream, and the commands provide the ability to put any element in the link into latched loopback.

The test data is provided by the AINF interface and is shown in the following table. The data stream sent is verified against the data stream received and a bit error count is updated. When the bit error count exceeds 255, the value of the bit error count remains at 255 and does not overflow.

Table 4-5. Link Fault Sectionalization Test Patterns

Test Pattern	Data	Description
B2047	N/A	2047-bit Bert pattern sent until it is terminated by software.
B2047 Non Latching	N/A	2047-bit Bert pattern sent interleaved with loopback command until it is terminated by software.
B511	N/A	511-bit Bert pattern sent until it is terminated by software.
B511 Non latching	N/A	511-bit Bert pattern sent interleaved with loopback command until it is terminated by software.
OCTET	default =h'32	A continuous series of the specified octet data is sent until it is terminated by software. (Latching only)
ALTERNATE	default = h'FF	A count of 100 octets of the specified data followed by 100 octets of 0 is sent alternating until it is terminated by software. (Latching only)

Link Fault Sectionalization Test Indicators

Two indicators have been added to the **`rept-stat-slk`** and **`rept-stat-ls`** commands to show whether the signaling link has a far end loopback condition and if a link fault sectionalization test is in progress.

When the signaling link is in a far end loopback condition:

- The primary state (PST) is OOS-MT-DSBLD.
- The secondary state (SST) is LPBK.
- The associate state (AST) is FE.

When a link fault sectionalization test is in progress:

- The primary state (PST) is OOS-MT-DSBLD.
- The secondary state (SST) is LPBK.
- The associate state (AST) is LFS.

When both the signaling link is in a far end loopback condition and a link fault sectionalization test is in progress:

- The primary state (PST) is OOS-MT-DSBLD.
- The secondary state (SST) is LPBK.
- The associate state (AST) is FE-LFS.

Link Fault Sectionalization Test Report

Test results are displayed to the terminal when the link fault sectionalization tests have completed. The following is an example of a link fault sectionalization test report.

Output Example

```
RLGHNCXA03W 96-04-16 16:02:05 EST  Rel 21.0.0
LOC = 1205  Port = B  LSN = --------  Start time = 11:10:34

PATTERN = ALTERNATE  DATA= FF  MAXERR = 10  TIME = 00:02:00

TEST STATUS = ERROR, bit error exceeded threshold.

LBP  CLLI         RLE  REP  LFST  BIT_ERROR  ERRORED_SEC   DURATION
2    rlghncxa05w  DSO  0    LLT   0          0             00:02:00
3    ------------ OCU  0    NLT   8          2             00:02:00
5    ------------ NEI  0    LLT   15         1             00:01:20
```

Link Maintenance Enhancements/LFS Increase for MPL-T and MIM (Release 31.3)

Proper functionality of a signaling link (SLK), from an EAGLE MTP card to a remote Network Element, is determined through a variety of mechanisms provided by EAGLE. This feature covers two main areas of improvement to these mechanisms. These improvements are the introduction of an operator command to force a signaling link into local line-oriented loopback and the enhancement of the TST-SLK command to allow for duration tests up to 24 hours.

The LFS Increase for MPL-T and MIM feature increases the number of simultaneously initiated Link Fault Sectionalization (LFS) tests on the MPL-T, T1 MIM and CR-T1 MIM from 1 to at least 4.

Link Status Reporting (Release 21.0)

The current method for reporting link unavailability requires the user to decipher several print outs. The first report informs the user of the link status, while subsequent reports detail the reasons for the status change. This feature provides a single report informing the user of the link unavailability with the corresponding reason. This report is

generated by the **`rept-stat-slk`** command. If there are multiple reasons for the link becoming unavailable, the user is informed of the highest priority cause.

The **`rept-stat-slk`** command output is expanded to display new error codes in the Unvail Cause field for each of the link unavailability causes detailed in the following table. Two lines of information for the Unavail Cause field are displayed if conditions require it.

When an unavailability cause clears, the alarm text is displayed for the next highest priority cause.

When the last unavailability cause clears, a link available message (UAM 200) is displayed.

Table 4-6. 21.0 Link and Link Set UAMs

UAM	Alarm	MRN in Release 21.0	Signaling Link Unavailability Priority	Abbreviation for the `rept-stat-slk` *Unavail Cause* field
0200	None	RCVRY-LKF: link available		
0201	Minor	REPT-LKF: remote NE loopback	1	NE
0202	Minor	REPT-LKF: HWP - too many link interrupts	3	INTR
0203	Minor	REPT-LKF: lost data	4	LD
0204	Minor	REPT-LKF: XER - SUERM threshold exceeded	5	XER
0205	Minor	REPT-LKF: APF - lvl-2 T1 expd (ready)	6	T1R
0206	Minor	REPT-LKF: APF - lvl-2 T1 expd(not ready)	7	T1NR
0207	Minor	REPT-LKF: APF - lvl-2 T3 expired	8	T3
0208	Minor	REPT-LKF: APF - lvl-2 T2 expired	9	T2
0209	Minor	REPT-LKF: APF - failed proving period	10	PF
0210	Minor	REPT-LKF: OSA - received SIO	11	SIO
0211	Minor	REPT-LKF: OSA - received SIN	12	SIN
0212	Minor	REPT-LKF: OSA - received SIE	13	SIE
0213	Minor	REPT-LKF: OSA - received SIOS	14	SIOS
0214	Minor	REPT-LKF: ABN - rcvd 2 of 3 invalid BSN	15	BSN
0215	Minor	REPT-LKF: ABN - rcvd 2 of 3 invalid FIB	16	FIB
0216	Minor	REPT-LKF: remote congestion timeout	17	CNGT
0217	Minor	REPT-LKF: excess acknowledge delay	18	XDA

UAM	Alarm	MRN in Release 21.0	Signaling Link Unavailability Priority	Abbreviation for the `rept-stat-slk` *Unavail Cause* field
0218	Minor	REPT-LKF: COO - rcvd changeover order	19	COO
0219	Minor	REPT-LKF: false congestion restart	20	FC
0220	Minor	REPT-LKF: MTP link restart delayed	21	RD
0221	Minor	REPT-LKF: X25 link unavailable	22	X25FL
0222	Minor	REPT-LKF: remote FE loopback	2	FE
0232	Minor	REPT-LKF: remote blocked	24	RB
0233	Minor	REPT-LNK-MANUAV: local blocked	25	LB
0234	Minor	REPT-LKF: RMI - remote inhibited	26	RMI
0235	Minor	REPT-LNK-MGTINH: local inhibited	27	LI
0236	Minor	REPT-LKF: not aligned	23	NA
0264	None	REPT-LINK-CGST: congestion level 0 to 1		
0265	None	REPT-LINK-CGST: congestion level 1 to 2		
0266	None	REPT-LINK-CGST: congestion level 2 to 3		
0267	None	REPT-LINK-CGST: congestion level 3 to 2		
0268	None	RCVRY-LINK-CGST: congestion level 2 to 1		
0269	None	RCVRY-LINK-CGST: congestion has cleared		
0270	None	REPT-LINK-CGST: discard level 0 to 1		
0271	None	REPT-LINK-CGST: discard level 1 to 2		
0272	None	REPT-LINK-CGST: discard level 2 to 3		
0273	None	RCVRY-LINK-CGST: discard level 3 to 2		
0274	None	RCVRY-LINK-CGST: discard level 2 to 1		
0275	None	RCVRY-LINK-CGST: discard has cleared		

UAM	Alarm	MRN in Release 21.0	Signaling Link Unavailability Priority	Abbreviation for the `rept-stat-slk` *Unavail Cause* field
0317	None	RCVRY-LKSTO: link set allowed		
0318	Minor	REPT-LKSTO: link set prohibited		

The signaling link unavailability messages use Bellcore recommended keywords in the output message. The following table shows the keywords that are supported in Release 21.0.

The signaling link unavailability messages also support Bellcore signaling link related keywords, link unavailability messages have been updated to support SEAS link failure cause codes shown in Section 8 of the *SEAS-STP Interface Specification, GR-310-CORE* , Issue 1, November 1994. These standard three letter codes denote the reason for link failure.

Table 4-7. Bellcore Message Keywords

Keyword	Event
REPT-XLST-TIMO	Removal of Member from X-list Due to Timeout
REPT-MTPLP-DET	MTP Loop detected: Prohibited Destination
REPT-MTPLP-SUST	Sustained Prohibited Destination Due to MTP Loop
RCVRY-MTPLP-RST	Resumption of Traffic to Loop Prohibited Destination
REPT-LKSTO	Link Set Failure
RCVRY-LKSTO	Recovery From Link Set Failure
REPT-MTP-RSTRT	Commencement of MTP Restart
REPT-STATUS-RSTRT	Progress of MTP Restart
RCVRY-MTP-RSTRT	Completion of MTP Restart
REPT-LINK-CGST	Link Congestion Level Increase
RCVRY-LINK-CGST	Link Congestion Level Decrease
REPT-LNK-MGTINH	Near End Link Management Inhibit
RCVRY-LNK-MGTINH	Near End Link Management Uninhibit
REPT-LKF	Link Failure
RCVRY-LKF	Recovery From Link Failure
REPT-LNK-MANUAV	Near End Manually Made Link Unavailable
RCVRY-LNK-MANUAV	Near End Manually Made Link Available

Linkset ID to Measurements Report (EAGLE Release 30.0/ IP7 Secure Gateway Release 8.0)

Description

Currently, the EAGLE On-Demand Component Measurement report for the command **rept-meas:enttype=link** provides the linkset ID (name) for the linkset to which the link in question belongs. However, unsolicited scheduled reports of this type do not provide the linkset ID in the report, which can make link monitoring difficult for some customers.

The Linkset ID to Measurements Report feature adds the field "Linkset ID" to the unsolicited Component Measurement reports created with **rept-meas:enttype=link**.

Hardware Requirements

There are no hardware requirements for this feature.

Linkset Name Increase—ANSI/ITU (EAGLE Release 30.0/ IP7 Secure Gateway Release 8.0)

Description

Customers may need more than 8 characters that the EAGLE currently allows for the linkset name. The linkset name may be used to identify the EAGLE and the adjacent point code and have other codes associated with it such as link speed and linkset size codes. All these attributes added up can exceed 8 characters.

The Linkset Name Increase—ANSI/ITU feature increases the maximum linkset name from 8 characters to 10 characters.

NOTE: For SEAS-provisioned linksets, SEAS still supports a maximum of 8 characters.

Hardware Requirements

No new hardware is needed to support this feature.

Limitations

For SEAS verify commands that allow a wildcard for the linkset name parameter, the EAGLE will display all linkset names, including the ones that were entered via EAGLE commands and contain more than 8 characters. However, the names will be truncated to 8 characters. Therefore it may appear that there are duplicate linkset names, when each actually is unique.

Furthermore, in SEAS, the user cannot specify a particular linkset name that is greater than 8 characters, either for ENT-, CHG-, or VFY- commands. If the user tries to retrieve information about a specific linkset that appears to have duplicates, it will not be clear which is the desired linkset name from the results of a wildcard display of VFY-LS. The best thing for a user to do is to enter all linkset names via SEAS, or, if also entering them via

EAGLE commands, structure the names with >8 characters so as not to cause duplicates if they are truncated to 8 characters.

Linkset Restricted Support (Release 31.9)

This feature provides an optional alternate routing determination algorithm that is more tolerant during linkset transitions and reduces the likelihood of experiencing congestion on linksets that do not have a sufficient quantity of available links to carry normal traffic loads.

This feature prevents congestion on newly available linksets for GT routed traffic in addition to MTP routed traffic.

This feature supports ITU linksets and ANSI linksets.

Transfer Restricted (TFR) procedures support ITU-N linksets only if the ITU TFR option is turned on for the linkset. ITU-I linksets do not support TFR procedures. However, the restricted status for a route internal in the EAGLE still applies for ITU linksets when the **lsrestrict** option is on. The user can set the number of links required to a higher number just like ANSI linksets.

The restricted status for a route internal in the EAGLE still applies for ITU linksets when the **lsrestrict** option is on.

For routing path decisions, two factors determine what route (linkset) a message should take:

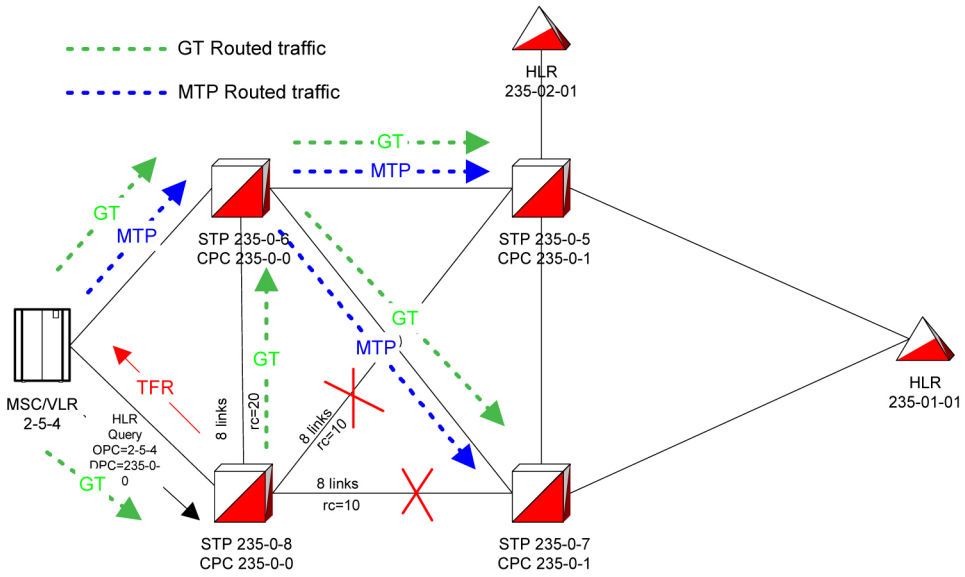
1. Route Status. Restricted and Allowed are both considered available from a routing path perspective.

2. Routing cost (ent-rte:rc=)

Currently, once the lowest cost available route is determined, it is always used. This can lead to congestion issues when the least cost Available route has a linkset status of Restricted (too few links available to handle the expected load). A higher cost Available route that is Allowed will receive no traffic, even though it may have more links available than the lowest cost Available route and would be able to handle the load without causing congestion.

The current routing determination algorithm does not use Restricted status when determining the preferred route. Use of the current algorithm is normally not an issue for messages not destined to the EAGLE (e.g., ISUP) but can have detrimental effects on messages destined to the EAGLE's point code (e.g., GTT traffic). The EAGLE can issue TFRs for MTP-routed traffic and expect the upstream nodes to find alternate routes. However, when GTT traffic arrives destined for the EAGLE's point code during a linkset failure, the originating node does not receive a TFR concerning the EAGLE's point code. Therefore, GTT traffic will not be diverted; and when the first link in the failed linkset becomes allowed, the EAGLE will try to route all traffic over the newly available link. Congestion can occur due to the potentially large amounts of GTT traffic. This behavior is shown in the following figure.

Figure 4-4. Example of SCCP Traffic During Linkset Failures



The B-linkset from STP 235-0-8 to STP 235-0-7 and the D-Linkset from STP 235-0-8 to STP 235-0-5 fail. Normally, a TFR would be sent to the MSC/VLR concerning destinations such as HLR 235-1-1. MTP traffic would be diverted from STP 235-0-8 to STP 235-0-6 and STP 235-0-8 would not receive any traffic. As links become available again on the B- or D-linksets, when the threshold is specified by the **tfatcabmlq** parameter, a TFA/TCA is broadcast to the MSC/VLR and thus allow MTP-routed traffic to flow again through STP 235-0-8.

However, GT-routed traffic to the true point code or CPC of STP 235-0-8 continues to arrive at STP 235-0-8 and be sent over the C-linkset when the B- and D-linksets fail. The failure is caused by an affected destination of the TFx message. The destination tells the receiving node the point code that is allowed, restricted, or prohibited. The affected destination would not be the EAGLE's point code.

When links start to become available on the B-linkset again, GT-routed traffic immediately starts to undergo changeback procedures, and these procedures can congest the newly available links if there are not enough links within the B-linkset to carry the normal traffic load. Again, MTP-routed traffic is still be diverted to the mate STP 235-0-6 by the MSC/VLR until the setting in the **tfatcabmlq** parameter is met and a TFA/TCA is issued.

The Linkset Restricted Support feature changes the routing path decision process. The routing path decision process chooses a higher-cost Allowed route over a lower-cost Restricted route based on available link count.

NOTE: NonAdjacent Restricted status is not used to determine when to use higher-cost routes. A route that has a linkset status of Allowed and a NonAdjacent status of Restricted is considered the lowest-cost available route and is used. NonAdjacent Prohibited status is still used to determine routing path decisions.

Linkset Restricted Support (Release 34.0)

The Linkset Restricted Support feature provides an optional alternate routing determination algorithm that is more tolerant during linkset transitions and reduces the likelihood of experiencing congestion on linksets that do not have a sufficient quantity of available links to carry normal traffic loads.

This feature prevents congestion on newly available linksets for GT-routed traffic in addition to MTP-routed traffic.

The route (linkset) that a message takes is determined using one of two factors:

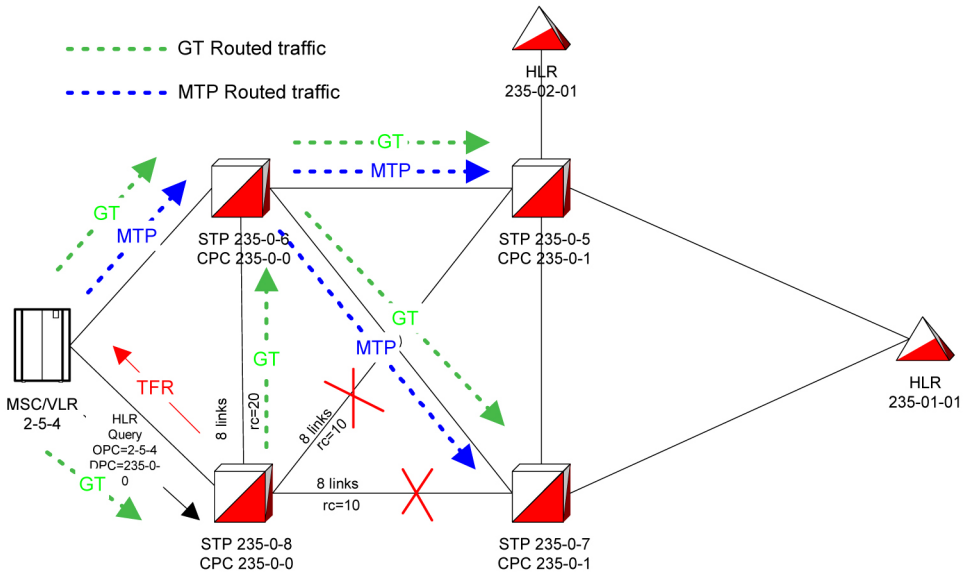
1. Route Status. Restricted and Allowed are both considered available from a routing path perspective.

2. Routing cost (ent-rte:rc=)

Current routing procedures determine and use the least cost available route, regardless of whether the route is Allowed or Restricted. However, congestion can occur if too few Allowed links are available to handle an unexpected spike in the traffic load. While at the same time, a higher cost available route may exist that is Allowed and with more links available to handle the congestion, receives no traffic.

The current routing determination algorithm does not use Restricted status when determining the preferred route. Use of the current algorithm is normally not an issue for messages not destined to the EAGLE 5 SAS (e.g., ISUP) but can have detrimental effects on messages destined to the EAGLE 5 SAS's point code (e.g., GTT traffic). The EAGLE 5 SAS can issue TFRs for MTP-routed traffic and expect the upstream nodes to find alternate routes. However, when GTT traffic arrives destined for the EAGLE 5 SAS's point code during a linkset failure, the originating node does not receive a TFR concerning the EAGLE 5 SAS's point code. Therefore, GTT traffic will not be diverted; and when the first link in the failed linkset becomes allowed, the EAGLE 5 SAS will try to route all traffic over the newly available link. Congestion can occur due to the potentially large amounts of GTT traffic. This behavior is shown in the following figure.

Figure 4-5. Example of SCCP Traffic During Linkset Failures



The B-linkset from STP 235-0-8 to STP 235-0-7 and the D-Linkset from STP 235-0-8 to STP 235-0-5 fail. Normally, a TFR would be sent to the MSC/VLR concerning destinations such as HLR 235-1-1. MTP traffic would be diverted from STP 235-0-8 to STP 235-0-6 and STP 235-0-8 would not receive any traffic. As links become available again on the B- or D-linksets, when the threshold is specified by the **tfatcabmlq** parameter, a TFA/TCA is broadcast to the MSC/VLR and thus allow MTP-routed traffic to flow again through STP 235-0-8.

However, GT-routed traffic to the true point code or CPC of STP 235-0-8 continues to arrive at STP 235-0-8 and be sent over the C-linkset when the B- and D-linksets failed. STP 235-0-8 knows that HLR 235-1-1 is restricted, but has no method of notifying MSC 2-5-4 to attemp to find an alternate path. Since the destination of the GT-routed traffic is STP 235-0-8, a TFR to MSC 254 concerning HLR 235-1-1 is ignored.

As links become available on the B-linkset again, GT-routed traffic immediately starts to undergo changeback procedures. This can congest the newly available links, if there are not enough, within the B-linkset to carry the normal traffic load. Again, MTP-routed traffic is still being diverted to the mate STP 235-0-6 by the MSC/VLR until the setting in the tfatcabmlq parameter (broadcast minimum link quanity) is met and a TFA/TCA is issued.

The Linkset Restricted Support feature compares a linkset's available links against its provisioned links to determine if it is capable of carrying its normal load. If all or most links are available, the linkset is considered Allowed. If fewer than a specified number of links are available, the linkset may experience congestion and is considered Restricted.

Based on available link count, the Linkset Restricted Support feature alters the routing path decision process and chooses the higher-cost Allowed route instead of the lower-cost Restricted route.

For Linkset Restriced Support, while the B-Linkset is Restricted, it gets bypassed and GT-routed traffic is sent on the C-Linkset. When enough links become available for the B-Linkset to be Allowed, then B-Linkset will again be used for routing. This helps prevent congestion by ensuring that traffic gets routed on the linkset with the most available capacity.

NOTE: NonAdjacent Restricted status is not used to determine when to use higher-cost routes. A route that has a linkset status of Allowed and a NonAdjacent status of Restricted is considered the lowest-cost available route and is used. NonAdjacent Prohibited status is still used to determine routing path decisions.

LNP 96 Million TNs—EAGLE 5 (EAGLE Release 30.0, IP7 Secure Gateway Release 8.0)

The concepts and facilities in this section apply to the LNP 96 Million TNs feature, the Increase LNP LRN and Default NPA-NXX Table Capacities feature, and the Mass Update of SPIDs feature. For convenience of discussion, these three features are presented here.

NOTE: The LNP 96 Million TNs feature, the Default NPA-NXX Table Capacities feature, and the Mass Update of SPIDs feature are EAGLE 5 features.

Overview

LNP 96 Million TNs Feature—EAGLE 5

Customers would like to increase the database capacity of the existing 48 Million number EAGLE LNP solution. Increasing the database capacity on a single node solves several architectural issues some customers face in regionalizing their LNP solutions.

This feature increases an EAGLE single node LNP number capacity from 48 Million to 60, 72, 84, or 96 Million LNP Numbers.

NOTE: The existing 4G DSM cards will support this feature. Other variants of DSM cards (i.e. 1G, 2G, and 3G), however, are not supported.

Increase LNP LRN and Default NPA-NXX Table Capacities Feature

Currently, major hub customers, whether regionalized or centralized, potentially can run out of LRN table capacity and, more critically, default NPA-NXX table capacity. There is an anticipated need to increase these tables in all supported ELAP-DSM LNP configurations, except the 1GB (12 Million) configuration.

This feature increases an EAGLE single node LNP LRN table to a maximum of 150,000, and the default NPA-NXX table to a maximum of 300,000 entries for all configurations of the ELAP-DSM LNP solution, excluding 1 GB DSM and all TSM variants.

Mass Update of SPIDs

NOTE: The Mass Update of SPIDs function is not operational unless LSMS 6.1 is used.

This feature supports the ability to update a set of subscription and network data from one Service Provider ID to another. The NPAC (Number Portability Administration Center) provides an offline file with selection criteria for the data to be modified. The data is independently updated at the LSMS (Local Service Management System); update information is not received over the NPAC/LSMS interface. The LSMS then creates the necessary file to transmit to the EAGLE to effect the same changes. This must be done for systems having TSMs or DSMs.

Although this feature is optional, no feature controls are required at the EAGLE; these controls are present at the LSMS.

NOTE: The Mass Update of SPIDs feature is supported only on the MPS-LSMS interface.

Description

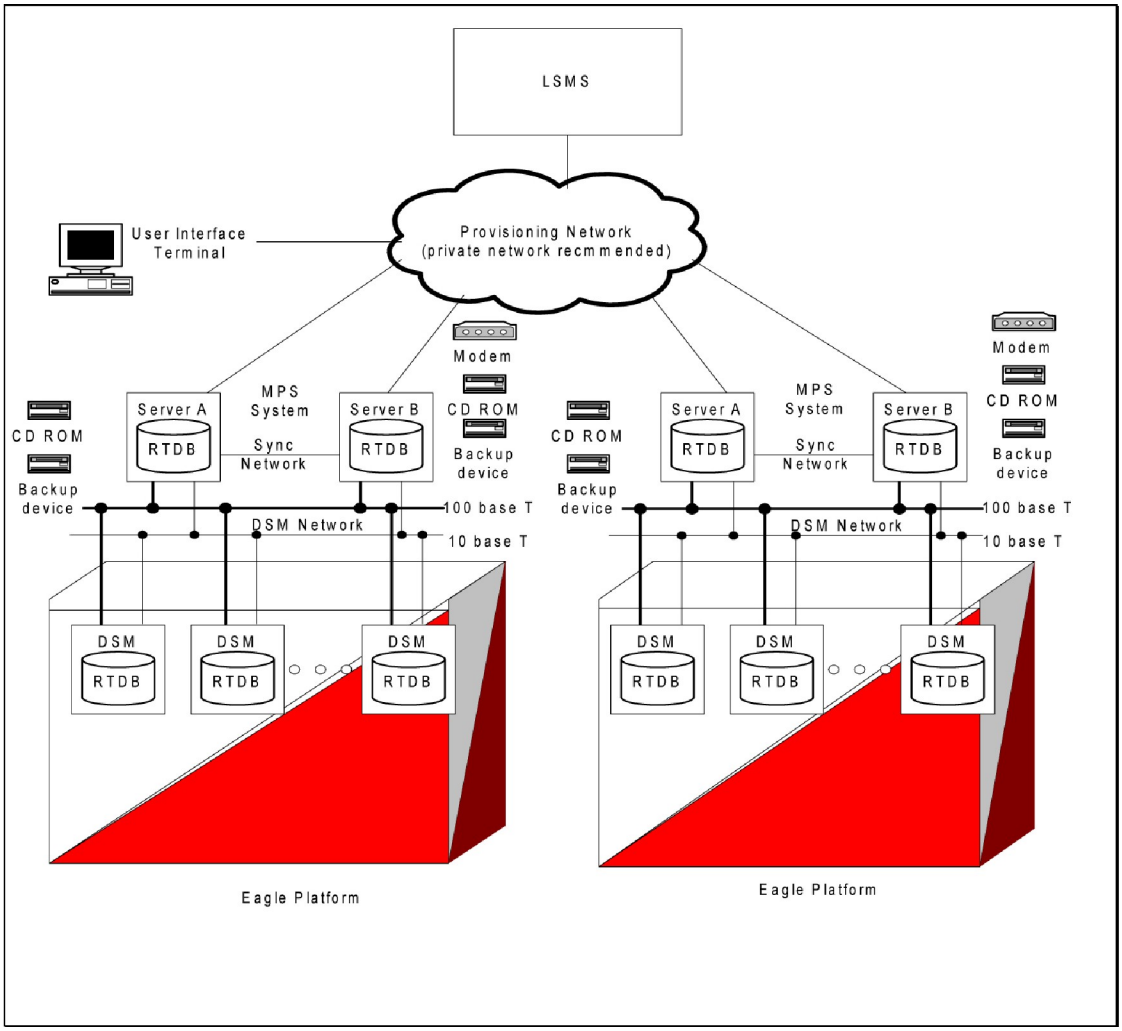
The Local Number Portability (LNP) implementation for the ELAP Application on the MPS platform consists of a Real-Time-Database (RTDB) component, which performs the following tasks.

- Accepts provisional transactional updates from a Local Service Management System (LSMS).
- Processes Auditing requests.
- Processes Bulk re-load request of the entire Database (DB).
- Handles Provisioning & Reload sessions to the PROV task.
- Services UI requests for Data Retrieval.

Ownership of the "golden database" resides on the LSMS, and maintains the integrity of the RTDB. All provisioning occurs on the LSMS. Additionally, the ELAP provides the ability to locally provision LNP data through the ELAP User Interface.

The following figure provides an architectural overview an LNP 48/96 Million System.

Figure 4-6. LNP 48/96 Million System Architectural Overview



Feature Control Mechanism

This feature requires that the LNP feature be on. Previously, the mechanism for identifying this condition was to perform the EAGLE UI command **rtrv-feat** and to view the LNP component in the "ON" state. This feature employs the Feature Control Mechanism. With feature keys, the verification method for identifying the LNP feature condition is to perform the EAGLE UI command **rtrv-ctrl-feat**. If the "LNP portedTN" entry is displayed, the LNP feature is considered to be ON.

The feature key mechanism provides some additional security against mistakes and/or fraud, thereby protecting the feature assets. There is a single feature key to indicate the existence of the ELAP device. This feature key behaves similarly to the previous LNP48MIL feature bit.

The LNP ELAP Configuration feature key indicates that the VSCCP applications should look to the TCP/IP connection for the source of the LNP DB. Three additional feature keys (LNP ported TN QTY, LNP ported NPANXXs QTY, and LNP ported LRNs QTY) regulate the maximum capacity allowed within the LNP DB System.

Under the current system, neither the feature bits nor the feature keys are conveyed to the ELAP. The ELAP currently performs no regulation of the capacities within the LNP System, other than the global capacity that it can perform. The LNP 96 Million TNs Feature enforces LNP quantities on the ELAP by way of the feature keys.

Loading and maintaining the feature key table on the ELAP via the OAM accomplishes this enforcement. Therefore, the feature keys are to be provisioned solely on the OAM, and the associated keys are to be distributed to the ELAP. Synchronization occurs on the ELAP in a similar manner to that of the EAGLE LIM cards.

Upgrade routines convert feature bits to feature keys by examining the existing feature bits and SCCP hardware to determine the LNP ELAP Configuration feature key and LNP QTY levels.

Object Capacity

The maximum capacity of the objects for persistent storage is increasing; see the following table.

Table 4-8. Maximum Object Capacity

Object	LNP 12 Million	LNP 48 Million	LNP 96 Million
Telephone Number (TN)	12 Million	48 Million	96 Million.
NPANXX	150,000	150,000	300,000
Local Routing Number (LRN)	100,000	100,000	150,000

Measurements Collection

The measurements requirements remain the same as the existing LNP 12 Million and LNP 48 Million architectures, with the exception of the expanded NPANXX and LRN listed in the previous table. Measurement objects are capped at 150,000 NPANXXs and 100,000 LRNs when collection is performed via the OAM. When measurements are being collected by the Measurement Platform, the objects are capped at 300,000 NPANXXs and 150,000 LRNs.

SCCP Application Storage and Provisioning

The new LNP 96 Million TNs architecture utilizes DSM cards ranging from 1 GB to 4 GB of expanded memory. Like the existing LNP systems, the LNP 96 Million TNs feature auto-inhibits any SCCP application card that does not meet the minimum hardware requirements, based upon feature key capacities and the LNP ELAP Configuration feature keys.

Hardware Requirements

The MPS 3.0 platform is required for this feature.

DSMs

The following DSM configurations are supported:

Table 4-9. DSM Configuration Table for Release 30

Name	Description	Maximum Number of Ported/pooled numbers supported
DSM 1GB	DSM with 1GB populated memory and 12 Million feature access keys activated	12,000,000
DSM 2GB	DSM with 2GB populated memory and 24 Million feature access keys activated	24,000,000

Name	Description	Maximum Number of Ported/pooled numbers supported
DSM 3GB	DSM with 3GB populated memory and 36 Million feature access keys activated	36,000,000
DSM 4GB	DSM with 4GB populated memory and 48, 60, 72, 84, or 96 Million feature access keys activated	96,000,000

MPS

The Multi-Purpose Server (MPS) does not require additional processors, memory, and/or additional disk capacity to accommodate the requirements for the 96 Million number feature.

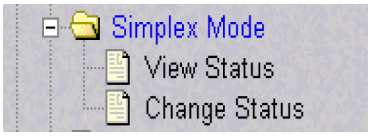
Enhancements to ELAP Graphical User Interface

The ELAP Graphic User Interface has been enhanced to support this feature. For more information, see the *ELAP Administration Manual*.

Simplex Mode Menu Option

The new Simplex Mode menu option provides the functionality to view as well as change (i.e toggle) whether or not the ExAP is in simplex mode; see the following figure.

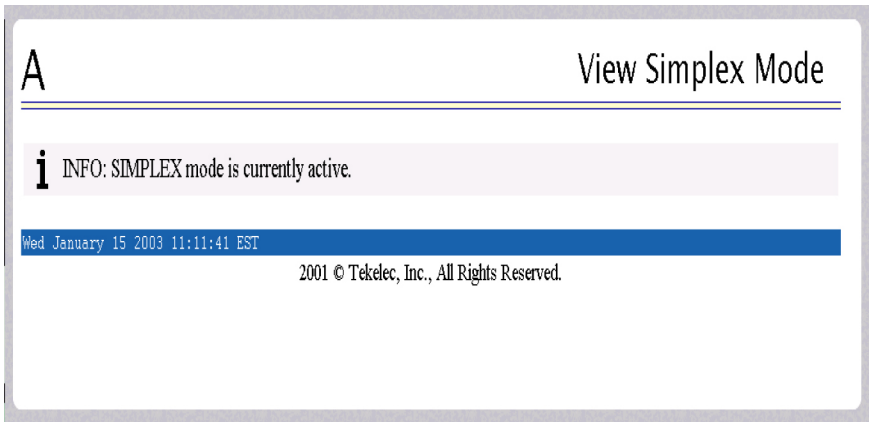
Figure 4-7. Maintenance>Simplex Mode Submenu



View Simplex Mode

This menu selection displays whether or not the ExAP is in simplex mode state. The user requires "View Simplex Mode" action privilege to view this menu selection.

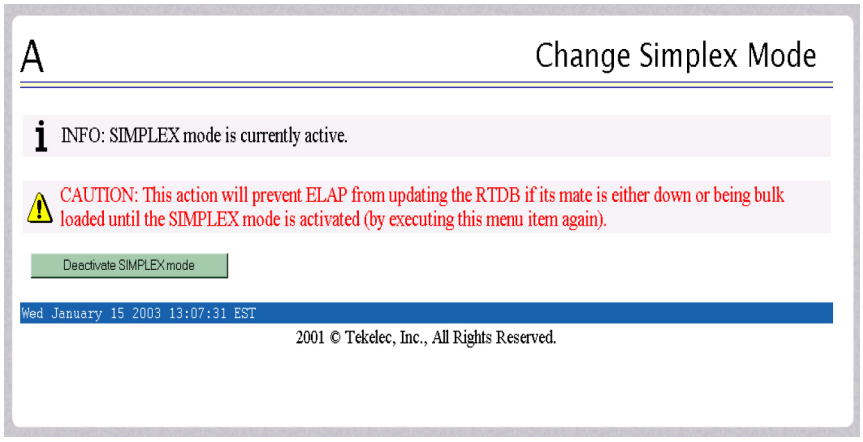
Figure 4-8. View Simplex Mode Screen



Change Simplex Mode

This menu selection toggles simplex mode on the selected ExAP.

Figure 4-9. Change Simplex Mode Screen



The current state of the selected ExAP is determined prior to the output of this screen. If the ExAP is not currently in simplex mode, this screen will enable the user to force it into simplex mode. If the contrary is true, the user will be enabled to remove the simplex mode condition on the selected ExAP. User requires "Change Simplex Mode" action privilege to view this menu selection.

View LNP Qty Features

This new ELAP version-only menu item selection displays the enabled LNP quantity features as provisioned on the EAGLE . The user requires "View LNP Qty Features" action privilege to view this menu selection.

Figure 4-10. View LNP Qty Features Screen

A View LNP Qty Features

LNP Quantity Feature	Quantity Enabled
LNP ported TNs	96000000
LNP ported NPANXXs	300000
LNP ported LRNs	150000

Thu October 24 2002 17:16:50 EDT

2001 © Tekelec, Inc., All Rights Reserved.

Subscriptions

This menu option allows the user to retrieve a single subscription record using a single 10-digit subscription or an optional 10-digit subscription range as a key. If a single 10 digit subscription is used the exact value is displayed if present, otherwise, a "not found" message is displayed.

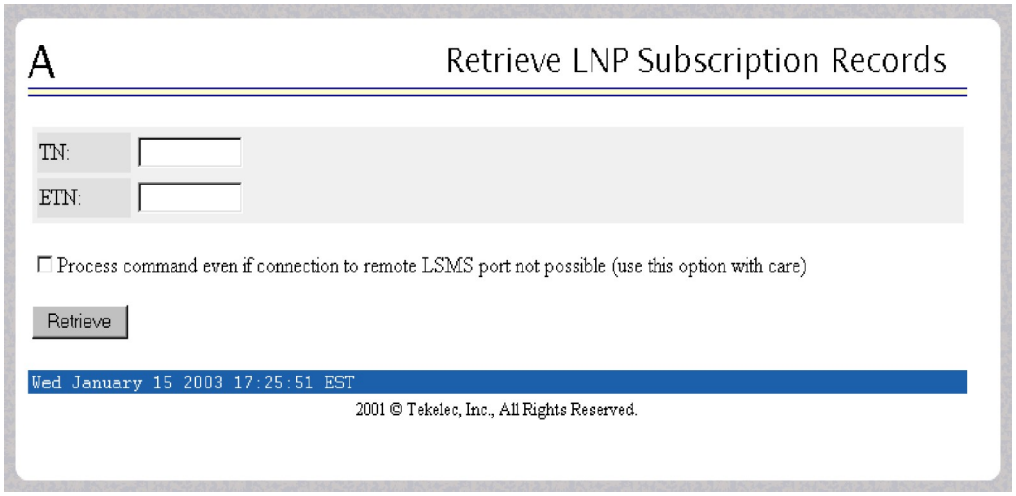
If a 10-digit subscription range is used a start value (TN:) and end value (ETN:) must be specified and the first subscription found in the specified range is displayed if present, otherwise, a "not found" message is displayed.

Figure 4-11. Retrieve Subscription Screen

Retrieve

This menu option allows the user to retrieve a single subscription record using a single 10 digit subscription or an optional 10 digit subscription range as a key.

Figure 4-12. Retrieve Subscription Screen



If a single 10-digit subscription is used, the exact value is displayed if present; otherwise, a "not found" message is displayed. If a 10-digit subscription range is used, a start value (TN:) and end value (ETN:) must be specified. The first subscription found in the specified range is displayed, if present; otherwise, a "not found" message is displayed.

Upgrade Considerations

EAGLE

The EAGLE upgrade must occur prior to the ELAP v3.0 upgrade. This allows for a stepwise upgrade process that will ensure “loss-less” traffic and continued service through the upgrade process. The EAGLE VSCCP-DSM application will support the legacy ELAP up to the LNP 48 Million architecture, including Warm-Restart.

The EAGLE will convert the existing LNP feature bits to feature keys as part of the upgrade conversion process. In all cases, the Feature Keys 893-0094-01 representing 150,000 NPANXXs and 893-0105-05 representing 100,000 LRN capacities will be set, except for those specifically indicated.

The next two tables show how the LNP Subscription quantities and LNP ELAP Configuration key are to be set through examining existing feature bits and IS-NR SCCP hardware. If conflicting feature bits and SCCP hardware are encountered during the upgrade process, the upgrade will fail during the table conversion.

Table 4-10. TSM Feature Key Upgrade Matrix

Feature Bit On	SCCP Hardware IS-NR			
	TSM-256 MB	TSM-512 MB	TSM-768 MB	TSM-1024 MB
LNP	**893-0110-01 (2M TNs)**	**893-0110-02 (4M TNs)**	**893-0110-03 (6M TNs)**	**893-0110-04 (8M TNs)**
LNP12MIL	[2] N/A	N/A[a]	N/A[a]	**893-0110-05 (12M TNs)**
[3] LNP18MIL	*N/A* [a]	*N/A* [a]	*N/A* [a]	*N/A* [a]
LNP48MIL	*N/A* [a]	*N/A* [a]	*N/A* [a]	*N/A* [a]

Table 4-11. DSM Feature Key Upgrade Matrix

Feature Bit On	SCCP Hardware IS-NR			
	DSM-1 GB	DSM-2 GB	DSM-3 GB	DSM-4 GB
LNP	**893-0110-04 (8M TNs)**	**893-0110-04 (8M TNs)**	**893-0110-04 (8M TNs)**	**893-0110-04 (8M TNs)**
LNP12MIL	**893-0110-05 (12M TNs)**	**893-0110-05 (12M TNs)**	**893-0110-05 (12M TNs)**	**893-0110-05 (12M TNs)**
LNP18MIL [b]	*N/A*[b]	*N/A*[b]	*N/A*[b]	*N/A*[b]
LNP48MIL	**893-0109-01 (ELAP)** **893-0110-05 (12M TNs)** **893-0105-05 (100k LRNs)** **893-0094-01 (150k NPAs)**	**893-0109-01 (ELAP)** **893-0110-06 (24M TNs)** **893-0105-01 (150k LRNs)** **893-0094-02 (300k NPAs)**	**893-0109-01 (ELAP)** **893-0110-07 (36M TNs)** **893-0105-01 (150k LRNs)** **893-0094-02 (300k NPAs)**	**893-0109-01 (ELAP)** **893-0110-08 (48M TNs)** **893-0105-01 (150k LRNs)** **893-0094-02 (300k NPAs)**

ELAP

The ELAP v3.0 upgrade must occur after the EAGLE v30.0 upgrade has occurred. This is to allow the EAGLE v30.0 time to soak with upgraded hardware such as GPSM-II and HMUX. During the ELAP upgrade process the RTDB database will be moved from its current location **/usr/rt** to the **/usr/db** location in preparation for the upgrade process and allows for back-out capabilities.

Once the LNP 48 Million tables are located in the **/usr/db** directory, new LNP 96 Million TNs architecture tables are created and populated through conversion of the old data. This avoids the Bulk Download procedures from the LSMS in order to populate the new architecture. Once conversion has occurred on one ELAP, it can then be loaded from the mate as part of the mate upgrade.

When upgrade of the ELAPs are complete, the DSM connection will be re-established. Once the ELAP-DSM connection is re-established, the VSCCP-DSM application will recognize the architectural change and set all connected DSM cards to INCONSISTENT. This will allow for continuation of LNP queries from the protocol,

[2] These cards will be auto-inhibited and not detected during the upgrade process.

[3] LNP18MIL is an Obsolete Feature Configuration and should not be present in the field.

yet prevents any further DB updates. By re-booting the SCCP application, the reloading of data will take on the new architecture.

NOTE 1: This specifically entails that a COLD re-start will occur on each DSM card being reloaded with the new 96 Million architecture, regardless of the LNP quantity setting in the feature key.

NOTE: An ELAP v3.0 is not structurally compatible with and EAGLE Release v27, 28 and 29 (pre release 30.0); therefore it must not be connected in that configuration.

The steps involved in performing the upgrade are specific to maintaining provisioning capability to the EAGLE DSM cards at all times, starting with ELAP v1.0 or v2.0 units operating in duplex mode.

- Maximum NPANXX Objects

  The maximum NPANXX objects is capped at 300,000 NPANXXs. Although feature keys have been allocated for further expansion in the future, they will not be permitted to be provisioned.

- Maximum NPANXX Objects

  The maximum LRN objects is capped at 150,000 LRNs. Although feature keys have been allocated for further expansion in the future, they will not be permitted to be provisioned.

- OAM-based Measurements Subsystem

  The OAM-based Measurements Subsystem will not support the LRN and NPANXX increase to 150,000 and 300,000 entries, respectively. The OAM will collect and report 100,000 LRNs and 150,000 NPANXXs only.

  The NPANXXs reported will be the first 150,000 provisioned NPANXXs. Collection data for the remaining 150,000 NPANXXs will be discarded.

  The LRNs reported will be the first 100,000 provisioned LRNs. Collection data for the remaining 50,000 LRNs will be discarded. Note that this could result in a significant change in the reported data set, if provisioning occurs during upgrade.

- OAM Upgrade

The OAM Upgrade will not execute if LNP18MIL = ON and LNP48MIL = OFF. Although this is a condition carried over from the LNP 18 Million TN feature (which became obsolete in EAGLE Release 27.0), it still may be encountered. In this event, the upgrade will return a failure, and will not continue until the LNP48MIL feature bit is turned ON.

LNP AIN Query Enhancement (PR28376) (Release 26.0)

Currently, the LNP AIN solution does not preserve the Charge Number and Charge Party Station type in the LNP AIN query and response. Without these parameters, SSP’s cannot set up calls to IC type trunk groups.

With this enhancement, the EAGLE STP’s LNP solution provides the ability to copy Charge Number and Charge Party Station type parameters from the LNP AIN query to the LNP AIN response. This capability is accessed on a per-STP basis via the LNPOPTS.

LNP Measurements Enhancements (Release 25.0)

Overview

This feature adds additional per SSP measurements for LNP Queries and for LNP Message Relay. It splits existing per SSP measurments into ported and non-ported measurements, and it adds Message Relay measurements for CNAM and ISVM messages to the existing LIDB and CLASS Message Relay measurements.

Message Relay Measurements per SSP

The following message relay measurements are pegged per SSP:

1. LIDBGTP - Ported LIDB transactions, per originating SSP
2. LIDBGTNP - Non-Ported LIDB transactions, per originating SSP
3. CLASSGTP - Ported Class transactions, per originating SSP
4. CLASSGTNP - Non-Ported Class transactions, per originating SSP
5. CNAMGTP - Ported CNAM transactions, per originating SSP
6. CNAMGTNP - Non-Ported CNAM transactions, per originating SSP
7. ISVMGTP - Ported ISVM transactions, per originating SSP
8. ISVMGTNP - Non-Ported ISVM transactions, per originating SSP

For the above counts, Ported means Successful 10 digit translations; non-Ported means an aggregate of the following:

- Successful 6 digit translations (non-ported numbers in portable NPA-NXX) either default GTT or normal GTT
- Successful 6 digit translations (non portable numbers) normal GTT
- Failed 6 digit translations (no GTT entry matched)

NOTE: Only MSUs with valid and supported parameters are pegged.

The originating SSP is derived from:

1. Calling Party address in the SCCP header. The point code must exist and the RI must NOT = GT.
2. OR the OPC of the MTP routing label.

This implementation will peg measurements under the above circumstances for any ANSI UDT or UDTS MSU requiring global title.

For backwards compatibility, the following counts also are maintained on disk. These counts are the sum of the ported and non-ported measurements for that service:

1. LIDBGTRQ - Total LIDB transactions, per originating SSP

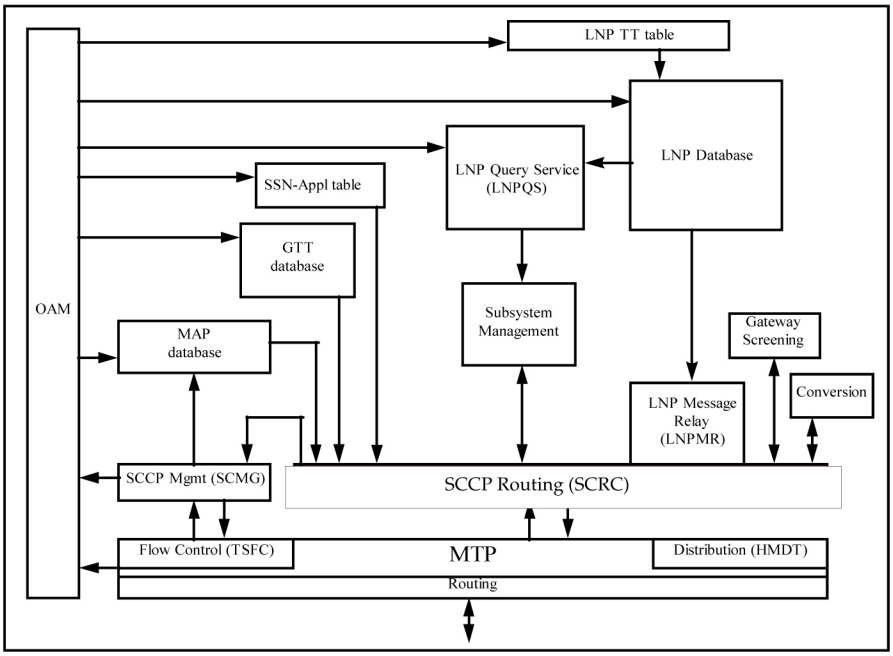
2. CLASSGTRQ - Total Class transactions, per originating SSP

   LIDBGTRQ = LIDBGTP + LIDBGTNP CLASSGTRQ = CLASSGTP + CLASSGTNP

The following figure illustrates the various subsystems involved in the EAGLE/LNP. The shaded boxes represent the subsystems affected by these new measurements. For measurements purposes all GTT measurements occur with the SCRC application, regardless of whether the MSU is a routine GTT or MR GTT. The transactions are recorded for LNP MR service and regular GTT entries.

NOTE: Only MSUs with valid GTT parameters and format are pegged.

Figure 4-13. LNP Block Diagram



Message Relay Measurements per SSP

Limitations for Message Relay Measurements

1. Only valid GTT MSUs are pegged. The following conditions are considered invalid MSUs:

   a. SCCP called SSN not included in MSU,

   b. Called party GT indicator not equal to 0010 (TT only)

2. ITU MSUs are not pegged.

3. CLASS, LIDB, CNAM, and ISVM translations are recorded *only* if the TT-SERV table is provisioned with CLASS, LIDB, CNAM, and ISVM TT values

4. These measurements are recorded per originating SSP only so far as the point code exists in the provisioned routing table data base.

5. If the originating SSP does not have a full PC entry in the routing table, but does have a cluster entry, the measurement will be pegged for the cluster entry.

LNP Query Measurements per SSP

Before Release 25.0, the number of LNP Queries processed per SSP were pegged. Beginning with Release 25.0, this count is broken into two separate counts:

1. SSPQRCVP - Ported LNP Queries processed, per originating SSP

2. SSPQRCVNP - Non-Ported LNP Queries processed, per originating SSP

These measurements are pegged only if the message goes to EAGLE's LNP subsystem. The message must also be formatted correctly.

The following types of LNP Queries are pegged:

- AIN Queries
- IN Queries
- Wireless LNP Queries
- Triggerless LNP Messages (ISUP IAM messages intercepted by TLNP)

The originating SSP is derived from:

1. Calling Party Point Code in the SCCP header (AIN, IN, and WLNP Only). The point code must exist and the RI must NOT = GT.

2. OR the OPC of the MTP routing label.

The originating SSP must be in the routing table, or the measurement will not be pegged. If the originating SSP does not have a full PC entry in the routing table, but does have a cluster entry, the measurement will be pegged for the cluster entry.

For backwards compatibility, SSPQRCV - the count of Total Queries processed, per originating SSP, will also be maintained on disk. This count is the sum of the ported and non-ported LNP Queries processed.

SSPQRCV = SSPQRCVP + SSPQRCVNP

Collection

These new measurements are added to the existing per SSP LNP measurements data maintained hourly and daily. The data is collected along with the existing per SSP data from all SCCP cards.

Storage

The per SSP measurements tables on disk are replaced with enhanced tables to store the additional registers.

Upgrade Considerattions

The new software accommodates the old database during the upgrade. The new fields for the existing tables, such as the NCR bit in the feature table, defaults to 0 (OFF), and the **NCAI** parameter in the destination table defaults to 0 (NO).

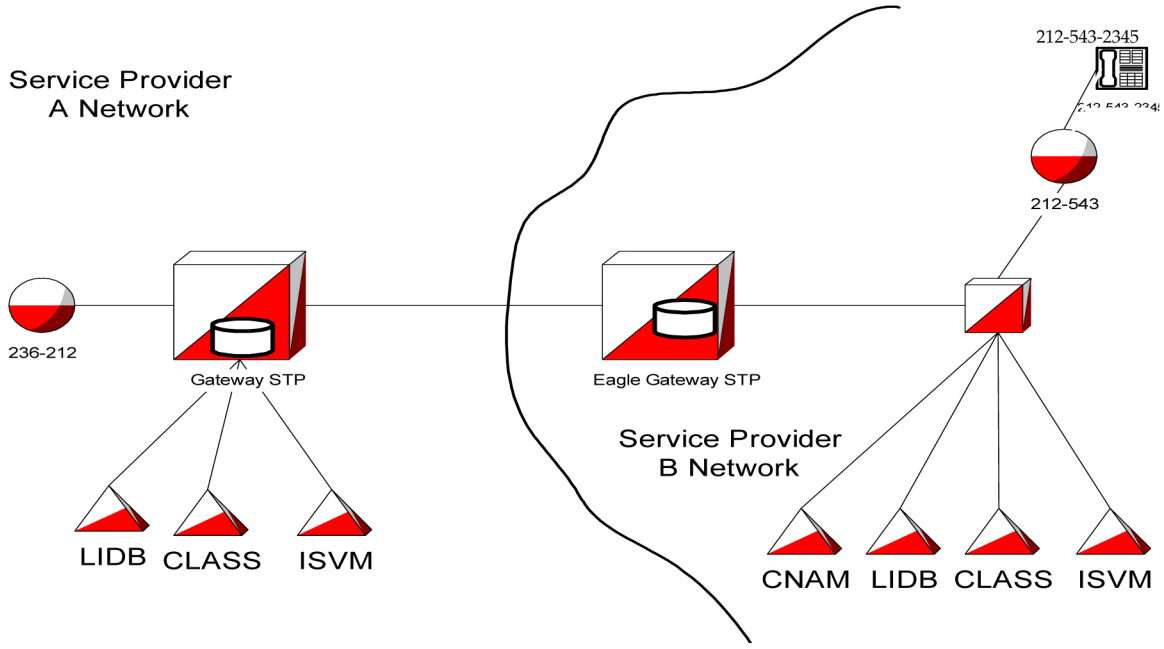
Use the **rtrv-dstn** command to verify the status of the **NCAI** parameter (it should display **ncai = no** for existing cluster destinations). To activate the Nested Cluster Feature, the software release must contain the CRMD feature (non-nested cluster management).

LNP Message Relay Enhancement (PR28810) (Release 26.0)

In Release 24.0, a change was implemented to address a non-conformance to the LNP message relay function. This change involved discarding a message if it was related to a ported TN, with LRN override data provisioned, but not for the specific service. This change has resulted in these customers provisioning default service data into the override tables to continue this type of LNP message relay service portability functionality.

In order to address the needs of these customers while continuing to provide the enhanced solution, in Release 26.0 the EAGLE will allow for either method of operation for LNP message relay on a per STP basis.

Figure 4-14. Example Network



Consider the network depicted in the figure. If customer 212-543-2345 ports from Service Provider B to A, Service Provider A needs to provide CNAM functionality, as it does not provide CNAM service within its network. However, Service Provider B can potentially "resell" CNAM service to Service provider A. The EAGLE LNP subsystem for Service Provider B would require that only the override GTT for the CNAM service be provisioned at the STP. Calls from the customer requiring LIDB service that originate in Service Provider's B network would arrive at Service Provider's B EAGLE Gateway STP.

Since 212-543-2345 is ported out, the override GTT data is first used. If the override data contains only data for CNAM service, the EAGLE formerly used the default data in the NPAC subscription information for LIDB and route the query to Service Provider A's Gateway STP.

This functionality was changed so that individual services would not default to the NPAC subscription data if the override GTT data was provisioned for one service, but was missing for another service. Due to this change, if Service Provider B wanted to route the LIDB query to Service Provider A's gateway STP, Service Provider B would have to provision the NPAC default data into the override table in order not to reject the LIDB query. This could cause unacceptable provisioning requirements for Service Provider B.

LNP Response to STPLAN (PR28660) (Release 26.0)

Currently, STPLAN functionality does not include LNP responses generated from the EAGLE LNP Database. This is due to the fact that the response is an EAGLE-generated MSU that does not have the STPLAN copy flag set.

With this feature, the LNP Query Service application now supports the copying of LNP response messages to the STP/LAN application. All LNP response messages will have the GWS Action Set ID set to the value of the corresponding LNP query message. This ensures that all LNP query messages that passed gateway screening with the STOP&COPY action set will have their responses copied to STPLAN.

The LNP response messages that are copied to STP/LAN are:

- AIN
- IN
- TCAP Error Response
- Wireless LNP
- PCS 1900

LNP Short Message Service (Release 28.2)

Description

EAGLE LNP currently supports the message relay function. LNP Short Message Service is an additional service offered in the message relay function. The DPC/SSN for the WSMSC is provisioned in the subscription versions received from the NPAC via the LSMS. This feature incorporates interface, administration, and protocol changes. All functions of the core LNP message relay feature are supported for the new LNP Short Message service. The LNP Short Message Service is unique, in that the service is supported for two protocols, ANSI-41 and PCS1900.

All EAGLEs must be upgraded to the LNP SMS capable release prior to configuring the LSMS to send WSMSC data in the subscription version. The LNP SMS capable EAGLE release will be capable of receiving subscription versions with and without WSMSC data. This allows the EAGLEs to operate without receiving WSMSC data, until all EAGLEs are upgraded and the LSMS configuration change is made.

Protocol

Message relay operates on GTT messages with translation types administered as "LNP Services." The 10-digit ported number is extracted from the message, and used to perform a lookup in the LNP database. If the ported number is found, the appropriate ported number or LRN override routing information is used to route the message. If the number is not found, default GTT data is used, if provisioned. Otherwise, the traditional (non-LNP) global title function is performed, using all the digits present in the SCCP layer.

To perform the lookup, the 10-digit dialed number (NPA-NXX-XXXX) is required as the key. Two protocols are supported for the WSMSC support, ANSI-41 and PCS1900. For ANSI-41, the WSMSC DPC/SSN in the subscription version locates the Message Center. For PCS 1900, the WSMSC DPC/SSN locates the HLR. The

subscription version contains one set of WSMSC DPC/SSN data. Therefore, incoming messages with different TTs may resolve to the same information in the TN record, using TT aliasing.

Hardware Requirements

No new hardware is needed to support this feature.

NOTE: This feature requires the MPS and DSMs on the EAGLE (i.e. 48 Million Number Architecture). This feature also requires the corresponding feature on the LSMS.

Measurements

Two new Measurements Registers have been added to the LNP SSP report.

Table 4-12. LNP Short Message Service Measurements Registers

Name	Description
WSMSCGTP	Number of WSMSC Global Title Translations for ported TNs received per originating SSP.
WSMSCGTNP	Number of WSMSC Global Title Translations for non-ported TNs received per originating SSP.

These new LNP SMS Measurements Registers are supported for two protocols: ANSI-41 and PCS 1900. Also, they are supported with and without the Measurements Platform feature enabled. If the Measurements Platform feature is not enabled, the LNP SSP report is generated to the FTA area from which it can be downloaded via Kermit. If the Measurements Platform feature is enabled, the LNP SSP report is transferred to an FTP server.

LNP—10 Digit Telephone Number Subscription Commands (Release 22.0)

Refer to the *Commands Manual* for current usage information.

ent-lnp-sub

The **ent-lnp-sub** command is used to add an LNP 10 digit ported telephone number and its LNP query LRN or message relay global title information to the database.

dlt-lnp-sub

The **dlt-lnp-sub** command is used to remove an LNP 10 digit ported telephone number message relay service, LRN, or the entire telephone number subscription from the database.

chg-lnp-sub

The **chg-lnp-sub** command is used to change the attributes of an existing 10 digit telephone number subscription. The **chg-lnp-sub** command uses these parameters.

rtrv-lnp-sub

The **rtrv-lnp-sub** command displays all the LNP 10 digit ported TNs and their assigned services in the database.

dlt-lnp-serv

The **dlt-lnp-serv** command is used to remove an LNP service from the database.

chg-lnp-serv

This **chg-lnp-serv** command is used to change the attributes of an existing LNP service using the **chg-lnp-serv** command.

LNP—Allow Subsystem Command (Release 22.0)

The **alw-ss** command is used to bring a mated application subsystem back into service. This command uses only one parameter, **ssn**, the mated application subsystem number. This command can only be executed when the current state of the mated application subsystem is OOS-MT-DSBLD and the subsystem is online. When the subsystem has been successfully placed back into service, the primary maintenance state of the specified mated application subsystem is set to IS-NR (in service normal).

LNP—Automatic Call Gapping (Release 22.0)

Automatic call gapping controls the rate that location routing number (LRN) queries for a particular telephone number or a portion of a telephone number are received by the EAGLE LNP when a particular threshold is reached. ACG controls are used under two conditions:

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

2. If no overload control is sent, the EAGLE LNP sends an ACG for a manually initiated control to control the rate of queries for a particular area code (3 digits), area code and prefix (6 digits), 10 digit telephone number, or part of a 10 digit telephone number (6 to 10 digits) are processed. The database can contain a maximum of 256 manually initiated ACG controls.

3. Refer to the *Database Administration Manual - LNP* for the current details of this feature.

LNP—Automatic Call Gapping Commands (Release 22.0)

Refer to the *Commands Manual* for current usage information.

ent-acg-nog The **ent-acg-noc** command is used to add an ACG node overload control level to the database.

dlt-acg-noc The **dlt-acg-noc** command is used to remove an ACG node overload control level from the database. The **dlt-acg-noc** command uses only one parameter, **lvl** - the overload levels 1 though 9. The database contains 10 ACG node overload levels, but only nine are configurable.

chg-acg-noc The **chg-acg-noc** command is used to change the values of an existing ACG node overload control level in the database.

rtrv-acg-noc The **rtrv-acg-noc** command displays the definitions of the node overload levels in the database. The definition is comprised of the threshold LNP query rates for node overload levels and the values for the ACGs to be sent when at the level. The **rtrv-acg-noc** command uses one parameter, **lvl**, to display a specific node overload level.

ent-acg-mic The **ent-acg-mic** command is used to assign ACG controls to all LNP queries or to specific LNP query services and called party digits. If the EAGLE LNP query service receives a query to which a control applies, then the EAGLE LNP sends an ACG, encoded as configured, with the response.

dlt-acg-mic The **dlt-acg-mic** command is used to remove an ACG manually initiated control.

chg-acg-mic The **chg-acg-mic** command is used to change an existing ACG manually initiated controls .

rtrv-acg-mic The **rtrv-acg-mic** command displays the values of ACG controls assigned to certain queries. The control can apply to all queries or to specific query services and called party digits. A set of controls is selected to be displayed by specifying the **type** of control(s), the service (**serv**), and/or the digits (**dgts**).

LNP—Call Completion to Ported Number (CCPN) (Release 22.0)

This capability allows the call to be completed to a telephone number that has been moved from one switch to another, a ported number. When a call is placed to a ported telephone number, the switch where the number used to reside sends a query to the LNP database to obtain the location routing number (LRN). The LRN gives the location of the new switch that the telephone number resides on. When a response to the query is returned to the old switch, the call is completed using the LRN to route the call to the new switch. To implement this capability, these features are required.

- LRN query processing - services LRN queries in real time and generates the appropriate LRN response. Multiple query types are supported.
- SMS interface - the SMS interface is required for LNP database management from an SMS system.
- ACG control - Automatic call gapping is required for overload control when an excessive number of LRN queries are received for a number.
- Local subsystem management - The LNP query processing application is implemented as a local SCCP subsystem and local subsystem management functions are performed in the EAGLE LNP.

LNP—Change Database Command (Release 22.0)

A new action, **import**, has been added to the **action** parameter of the **chg-db** command. The **action=import** parameter restores selected portions of the current LNP database from a removable cartridge created by the LSMS. If the EAGLE LNP's database becomes severely out of sync with the LSMS's LNP database, the **chg-db:action=import** command can be used to resynchronize the LNP portion of the database with the LSMS.

The removable cartridge containing a copy of the LSMS's LNP database, formatted in EAGLE database format, is created at the LSMS. The action of the **chg-db:action=import** command is similar to the action of the **chg-db:action=restore:src=remove** command, except that only these tables in the LNP portion of the database are replaced.

- servprov.tbl
- lnp_stat.tbl (only a portion of this table is imported)

- lnp_lrn.tbl
- lnp_mr.tbl
- lnp_npa.tbl
- lnp_4dig.tbl
- lnp_dbmm.tbl

After the **chg-db:action=import** command has completed, this minor alarm is raised for all operational TSMs showing that the TSMs must be reinitialized to use the newly imported LNP data.

```
 *   5022.0429 *  CARD xxxx SCCP       LNP database is inconsistent
```

When the **chg-db:action=import** command has completed successfully, both the active and standby MASPs are reinitialized.

LNP—Changes to Existing Commands (Release 22.0)

LNP—Self ID Commands

The **cpctype** parameter has been added to the **chg-sid** command to define the type of capability point code being added to the self ID of the EAGLE LNP. The EAGLE LNP can contain two types of capability point codes, LNP and STP. If the **cpctype=lnp** parameter is specified, the capability point code must be an ANSI point code. The LNP capability point codes are used to associate a specific LNP service or capability (for example, Local Number Portability Query Response and Message Relay service) with one or more of the capability point codes in the self ID of the EAGLE LNP. If the **cpctype=stp** parameter is specified, the capability point codes can be an ANSI, ITU international, or ITU national point code. The self ID of the EAGLE LNP can contain a maximum of 96 capability point codes.

The CPCA (LNP) field has been added to the output of the **rtrv-sid** command to display the LNP capability point codes contained in the self ID of the EAGLE LNP. The **cpctype** parameter has been added to the **rtrv-sid** command to display either the LNP capability point codes (**cpctype=lnp**) or the STP point codes (**cpctype=stp**).

LNP—Mated Application Commands

The **ent-map** and **chg-map** commands have been changed to allow the EAGLE's true point code and the LNP subsystem number to be entered into the mated application table, if the LNP feature is turned on. When the LNP subsystem number is specified, the multiplicity indicator can be either solitary (**mult=sol**) or dominant (**mult=dom**). If the LNP feature is not on, the point code specified in these commands must be in the routing table.

LNP—chg-feat and rtrv-feat Commands

The **lnp=on** parameter has been added to the **chg-feat** command to turn the LNP feature on. To show whether the LNP feature is on, the LNP field has been added to the **rtrv-feat** command output.

Before the LNP feature can be turned on, the global title translation feature must be on and the EAGLE LNP must be configured with this hardware.

- TSM - P/Ns 870-1289-xx, 870-1290-xx, 870-1291-xx, 870-1292-xx
- MCAP card - P/N 870-1307-xx

NOTE: Once any feature is turned on with the `chg-feat` command, they cannot be turned off.

LNP—clr-disk-stats Command (Release 22.0)

The **`clr-disk-stats`** command is a debug command used to clear the disk performance statistics and set all the disk performance statistic fields to 0. This command uses only one parameter, **`loc`** - the card location of the MASPs, either 1113 or 1115.

LNP—Degraded Mode (Release 22.0)

For the LNP application, software loading has been modified to verify the validity of the hardware configuration for both MASP and SCCP cards. The MASP hardware configuration is verified first. Once MASPs configuration is determined to be valid, then the SCCP hardware configuration is verified. The hardware configuration for MASP and SCCP cards is verified only when the LNP feature is turned on. The verification of the hardware includes:

- validity of the main assembly
- verification of applique's memory size

When the hardware configuration for the MASP is determined to be invalid for the LNP feature, the MASP enters a degraded mode. Degraded mode inhibits some MASP functionality in hopes of preventing more serious system fault conditions.

When the hardware configuration for an SCCP card is determined to be invalid for the LNP application, SCM automatically inhibits loading for that specific SCCP card. A minor alarm is generated indicating that card loading for that SCCP card has failed and has been automatically inhibited (i.e. prevented from reloading again). When card loading has been inhibited, the primary state of the card is set to OOS-MT-DSBLD and the secondary state of the card is set to MEA (Mismatch of Equipment and Attributes).

To activate loading of an SCCP card which has been automatically inhibited, enter the **`alw-card`** command. The **`alw-card`** command is rejected if the LNP is in degraded mode.

Degraded mode is entered under any of these situations:

- Active and standby MASPs do not have an E586 main assembly and an applique with a minimum of 256 Mbytes of memory.
- Any IS-NR SCCP card does not have an E586 main assembly and an applique with a minimum of 256 Mbytes of memory.

The following actions are taken during degraded mode:

- LNP database commands for configuring LNP data in the database is rejected. Retrieve commands is accepted.
- Loading of SCCP cards is disabled. SCCP cards requesting to be loaded will have loading automatically inhibited. SCCP cards already in service continue to run.
- The LNP subsystem is prevented from going online. (any attempt to execute the **alw-map-ss** is rejected). The LNP subsystem can be taken offline (the **inh-map-ss** is accepted).
- The PST/SST of each MASP with an invalid configuration is set to IS-ANR/MEA.
- The **rept-stat-sys** command output shows that the EAGLE is in degraded mode.

The method to recover from degraded mode is dependent upon the reason degraded mode was entered. The list below defines method(s) to recover from degraded mode for each possible reason the mode can be entered.

- The active and standby OAMs do not have the correct main assembly/applique combination.

  Change the MASP hardware configuration to an E586 main assembly with a minimum of 256 Mbytes of memory on the applique.

- An SCCP card does not have the correct main assembly/applique combination.

  Change the SCCP hardware configuration to an E586 main assembly with a minimum of 256 Mbytes of memory on the applique.

LNP—Destination Point Code Exception Report (Release 23.1)

The EAGLE requires that the destination point code contained in the global title translation data in the database has a route assigned to it so the MSU can be routed to the destination point code. The LNP subscription data the EAGLE receives from the LSMS can contain global title translation data with destination point codes that do not have routes assigned to them in the EAGLE database. Normally this type of data would be rejected since the EAGLE does not know how to route to the destination point code. However, since this data is coming from the LSMS for LNP updates, the EAGLE must accept it.

This feature generates a report of LNP subscriptions in the database whose destination point codes have not been assigned to a route. Two types of reports are generated:

- All destination point codes in the LNP database that are not assigned to a route.
- For each telephone number, all destination point codes in the LNP database that are not assigned to a route.

LNP—disp-disk-stats Command (Release 22.0)

The **disp-disk-stats** command is a debug command that displays the disk performance statistics. The MASPs maintain disk read/write access times as well as statistics for each table and application showing the number of disk accesses and cache accesses. The application and table statistics that have zero values will not be output if an application ID or table ID is not specified; only non-zero statistics are displayed in the default report.

Refer to the *Commands Manual* for current usage information.

LNP—EAGLE LNP Configuration (Release 22.0)

The EAGLE LNP uses the same platform as the EAGLE STP, but with these changes.

The LNP data is stored on the fixed disk drive on the TDM. The fixed disk is partitioned to store both the LNP data and the STP data to prevent a failure of either database from affecting the other. The LNP data is downloaded from the fixed disk drive to the TSM, an ASM containing 1 Gbyte of memory. The TSM is made up of an E586 main assembly and 4 M256 appliques. Each M256 applique contains 256 Mbytes of memory.

To configure an EAGLE LNP for the LNP feature, these software changes have been made.

- The LNP feature must be turned on with the **chg-feat** command. No LNP commands can be executed if the LNP feature is not turned on. The LNP feature cannot be turned on if the SCCP memory (ASM or TSM) is not large enough to hold the LNP data.
- If a TSM card is loading data, LNP data cannot be configured until the loading process has completed.
- The LNP database is audited every 24 hours.

The LNP database contains this data.

- Six global title translation services requiring message relay service. This data is received from the LSMS.
- Default global title translation for each ported NPANXX. This data is received from the LSMS.
- A list of ported NPANXX requiring SCCP message relay service at the EAGLE LNP. This data is received from the LSMS.
- An indication for each translation type (applicable for only ported NPANXXs requiring LIDB, CLASS, ISVM, and CNAM message relay service) indicating if SCCP CDPA includes 10 digits. The default is “Yes.” This indicator is used only when the length of the SCCP CDPA is 10 digits, but only 6 digits are included. If the length of the CDPA is 6 digits, this indicator is ignored. This data is received from the LSMS.
- Six digit global title translation for LNP query messages. This data is not required if this global title translation is performed in a preceding STP. The results of the global title translation is an alias point code (or true point code of the EAGLE LNP) and SSN of the LNP query function. The alias point code represents the LNP query function. Using the alias point code instead of true point code allows using same global title translation record in both mated STPs. This global title translation data can be configured from SEAS or EAGLE LNP terminals.
- LNP information for each 10 digit ported telephone number. This data is received from the LSMS.
  - — Directory number (DN) or range of directory numbers
  - — Location routing number (LRN)
  - — Current facilities based service provider ID
  - — Service 1 global title translation data through Service 6 global title translation data (DPC/SSN, routing indicator, etc.)

— Billing Service Provider ID

— If the global title translation is a final global title translation, then the mated application and related data (loadshare mode, concerned point code list, etc.) corresponding to the global title translation data.

- Parameters required to customize LNP query and response processing. These are configured on each EAGLE LNP.

  — AMAslpID value

  — Indicator to include or exclude AMAslpID parameter in the AIN response

  — Billing indicators (call type and feature ID) for the IN connection control response

  — 3 or 4 digit CIC for IN connection-control response

Parameters for treatment of outgoing global title translation messages. The new translation type and global title address indicator can be configured for each DPC, as long as the DPC is used in an existing non-final global title translation. The global title address indicator shows the outgoing global title address treatment, either the telephone number or LRN.

LNP—Element Manager System (EMS) (Release 22.0)

The EMS is an interface between the EAGLE LNP and the LSMS and converts the LSMS protocol (CMIP) to an asynchronous serial format. Two terminal disk module (TDM) ports (RS-232) running at 19,200 bps connect the EMS to the EAGLE. The EMS is connected to the LSMS using the Q.3 interface. The EMS is mounted in the OAPF frame.

The EMS performs these functions.

- Receiving LNP data and requests from the LSMS and converting the LNP data to EAGLE LNP commands
- Connection management to the LSMS
- Support data audit function between EAGLE LNP and the LSMS

The data downloaded to the EAGLE through the EMS is stored in the fixed disks on the TDMs.

The EMS is a TEXAS MICRO™ Intelligent Processor Unit Telecommunications Server, model 9605 (Sparc 05, 85 MHz processor) and contains:

- 32 megabytes of RAM
- a 1.02 gigabyte hard drive using a SCSI interface
- a 1.44 megabyte floppy disk drive, a high-speed serial interface (HSI) SBUS card (with 4 synchronous ports)
- RS-232C-extender SBUS communications board (with 4 asynchronous ports).

The EMS is powered from the OAP frame's fuse and alarm panel with -48 VDC.

The EMS uses this software to allow the EAGLE to communicate with the LSMS.

- SUN™ Solaris version 2.4 operating system
- SunLink Solaris version 9 for X.25
- The EMS application software.

The EMS is deployed in pairs at each EAGLE LNP for redundancy.

LNP—Enhanced Global Title Translation Routing Services (Release 22.0)

This capability locates the LNP database using 10 digit global title translation. To implement this capability, these features are required.

- Ported NPANXX detection - the EAGLE LNP maintains a list of all ported NPANXXs for each translation type that the node must perform 10 digit global title translation for. The first pass search shows if the number belongs to a ported NPANXX.

  If the number does not belong to a ported NPANXX, normal global title translation is performed on the number.

  If the number belongs to a ported NPANXX, two options are available for performing LNP global title translation.

  — The EAGLE LNP is not responsible for performing 10 digit LNP global title translation. The EAGLE LNP performs normal global title translation which results in routing the MSU to an external LNP database (for example, an LNP SCP) or another STP.

  — The EAGLE LNP is responsible for performing 10 digit LNP global title translation. This routes the MSU to an internal LNP subsystem for performing 10 digit LNP global title translation.

- Message Relay - This function is required to perform 10 digit LNP global title translation while maintaining backward compatibility with existing non-LNP OSSs. Currently, OSSs (and some switches) use 6 digit global title translation for certain services. To minimize the impact of LNP on these systems, they will continue to route using 6 digit global title translation. If the called party address does not include 10 digits, the 10 digits are extracted from the TCAP portion of the message and are used as a global title address (GTA).

- Prevention of SCCP looping - The complexity of LNP data administration across multiple carrier networks increases the chances of data inconsistencies and may result in SCCP circular looping. The global title translation feature has been enhanced to modify the translation type (TT) and global title address (GTA) as result of translation. The GTA is replaced by the location routing number. This function is optional and can be configured by the user.

- SMS interface - the SMS interface is required for loading LNP global title translation data from an SMS system.

- 10 digit final LNP global title translation - The EAGLE LNP requires that final global title translation is performed on 10 digits. When the STP performs 10 digit final global title translation, it will be capable of supporting routing and management of mated databases. All existing functions (load sharing between

databases, primary/backup relationship between databases, remote subsystem management, translation type mapping, translation aliasing, etc.) are performed with the 10 digit final LNP global title translation.

- 6 digit default LNP global title translation - If the 10 digit global title translation does not find a match (for example, when a number is not ported but belongs to a ported NPANXX), the EAGLE LNP performs a 6 digit default global title translation.

LNP—Inhibit Subsystem Command (Release 22.0)

The **inh-ss** command is used to place a mated application subsystem out of service. This command uses two parameters, **ssn** and **force**. The **ssn** parameter specifies the subsystem number of the mated application subsystem to be taken out of service. If the **inh-ss** command is entered with the **force** parameter set to **yes**, the mated application subsystem is forced out of service. When the subsystem has been successfully taken out of service, the primary maintenance state of the specified mated application subsystem is set to OOS-MT-DSBLD (out of service maintenance disabled).

LNP—Impact of LNP on Other Features (Release 22.0)

Gateway Screening

Gateway screening has been modified to help prevent the looping of SCCP messages. When LNP global title translation is performed at SCCP level, SCCP Called Party Address screening is performed after the 6 digit default global title translation, if required, or after 10 digit LNP global title translation.

Translation Type Mapping

Translation type mapping is used on internetwork linksets to prevent the looping of SCCP messages between networks. For example, an originating network maps the translation type **x** to the new value **y** before transmitting it to the destination network. The new translation type value **y** is used in the destination network for translating and routing the MSU to a node inside the destination network. The MSU stays inside the destination network and message looping is prevented.

STPLAN

Gateway screening is used for STPLAN feature to selectively copy MSUs. This has the same impact as gateway screening.

Database Transport Access (DTA)

LNP has no impact on the DTA feature because MSUs are only redirected by the DTA feature before any global title translation takes place.

Other Features

Because LNP applies only to ANSI SS7 networks, the LNP feature has no impact on these features.

- ITU/ANSI Interworking
- X25/SS7 Interworking

LNP—Location Routing Number Commands (Release 22.0)

Refer to the *Commands Manual* for current usage information.

ent-lnp-lrn

The **ent-lnp-lrn** command is used to add an LNP location routing number (**lrn**) and its corresponding overriding message relay global title translations (**mrgt**) to the database.

dlt-lnp-lrn

The **dlt-lnp-lrn** command is used to remove a location routing number or its corresponding overriding message relay global title translations from the database.

chg-lnp-lrn

The **chg-lnp-lrn** command is used to change the attributes of an existing LRN and its corresponding overriding message relay global title translations in the database.

rtrv-lnp-lrn

The **rtrv-lnp-lrn** command displays all the LRNs and their associated final overriding message relay global title translations in the database.

LNP—Mapping LNP Translation Type Commands (Release 22.0)

Refer to the *Commands Manual* for current usage information.

chg-lnp-ttmap

The **chg-lnp-ttmap** command is used to change globally administered NGT and RGTA indications for each point code and translation type combinations for a group of existing telephone numbers in the database.

rtrv-lnp-ttmap

The **rtrv-lnp-ttmap** command displays all globally administered NGT and RGTA indications for each point code and translation type combinations for a group of existing telephone numbers in the database.

LNP—Measurements (Release 22.0)

Overview

LNP measurements are obtained using the **rept-meas** command and specifying the report types MTCH (**:type=mtch**, an hourly maintenance report) or MTCD (**:type=mtcd**, a daily maintenance report) and the entity type LNP (**:enttype=lnp**). When a report of LNP measurements is requested with the **rept-meas**

command, four comma delimited text files containing the LNP measurement information are created in the file transfer area on the active fixed disk. For a daily maintenance report, these files are created.

- MDAY_ LNP.CSV - Daily LNP System Wide Measurements
- MDAY_ SSP.CSV - Daily LNP Measurements per SSP
- MDAY_ LRN.CSV - Daily LNP Measurements per LRN
- MDAY_ NPA.CSV - Daily LNP Measurements per NPA

For an hourly maintenance report, these files are created.

- M60_LNP.CSV - Hourly LNP System Wide Measurements
- M60_SSP.CSV - Hourly LNP Measurements per SSP
- M60_LRN.CSV - Hourly LNP Measurements per LRN
- M60_NPA.CSV - Hourly LNP Measurements per NPA

LNP—System Wide Measurements

Table 4-13. MTCD - LNP and MTCH-LNP System Wide Measurement Report

Event Name	Description	Unit
LNPQRCV	The number of total queries received by LNPQS.	peg count
LNPQDSC	The number of invalid queries that are discarded as no reply can be generated.	peg count
LNPQTCPE	The number of error replies with TCAP error code.	peg count
LNPSREP	The number of successful replies.	peg count
LNPQUNPA	The number of correct queries received for non-ported DN when NPANXX is not provisioned.	peg count

This is an example of the text file created when a system wide LNP measurement report is requested.

```
"rlghncxa03w 97-06-30 15:51:37 EST Rel 22.0.0 "<cr><lf>
"TYPE OF REPORT: DAILY MAINTENANCE MEASUREMENTS ON LNP SYSTEM"<cr><lf>
"REPORT PERIOD: LAST"<cr><lf>
"REPORT INTERVAL:  97-06-29,  00:00:00 THROUGH 23:59:59 "<cr><lf>
<cr><lf>
"LNPQRCV","LNPQDSC","LNPQTCPE","LNPSREP","LNPQUNPA"<cr><lf>
4294967295,4294967295,4294967295,4294967295,4294967295<cr><lf>
```

SSP Measurements

Table 4-14. MTCD - LNP and MTCH-LNP SSP Measurement Report

Event Name	Description	Unit
SSPQRCV	The number of correct queries received per originating SSP.	peg count

This is an example of the text file created when an SSP LNP measurement report is requested.

```
"rlghncxa03w 97-06-30 15:51:37 EST Rel 22.0.0 "<cr><lf>
"TYPE OF REPORT: DAILY MAINTENANCE MEASUREMENTS ON LNP SSP"<cr><lf>
"REPORT PERIOD: LAST"<cr><lf>
"REPORT INTERVAL:  97-06-29,  00:00:00 THROUGH 23:59:59 "<cr><lf>
<cr><lf>
"SSP","SSPQRCV"<cr><lf>
"002-002-100",123456789<cr><lf>
"004-052-033",23456789<cr><lf>
"001-023-073",456789<cr><lf>
"240-098-019",345<cr><lf>
"123-043-099",99999<cr><lf>
"123-048-059",4294967295<cr><lf>
```

LNP—LRN Measurements

Table 4-15. MTCD - LNP and MTCH-LNP LRN Measurement Report

Event Name	Description	Unit
LRNQRCV	The number of correct queries received per LRN.	peg count

This is an example of the text file created when an SSP LNP measurement report is requested.

```
"rlghncxa03w 97-06-30 15:51:37 EST Rel 22.0.0 "<cr><lf>
"TYPE OF REPORT: DAILY MAINTENANCE MEASUREMENTS ON LNP LRN"<cr><lf>
"REPORT PERIOD: LAST"<cr><lf>
"REPORT INTERVAL:  97-06-29,  00:00:00 THROUGH 23:59:59 "<cr><lf>
<cr><lf>
"LRN","LRNQRCV"<cr><lf>
9194560000,123456789<cr><lf>
4087550001,23456789<cr><lf>
5155550000,456789<cr><lf>
3022330001,345<cr><lf>
7032110002,99999<cr><lf>
8123048059,4294967295<cr><lf>
```

NPANXX Measurements

Table 4-16. MTCD - LNP and MTCH-LNP NPANXX Measurement Report

Event Name	Description	Unit
NPAQRCV	The number of correct queries received per NPANXX for non-ported DN.	peg count

This is an example of the text file created when an NPANXX LNP measurement report is requested.

```
"rlghncxa03w 97-06-30 15:51:37 EST Rel 22.0.0 "<cr><lf>
```

```
"TYPE OF REPORT: DAILY MAINTENANCE MEASUREMENTS ON LNP NPXNXX"<cr><lf>
"REPORT PERIOD: LAST"<cr><lf>
"REPORT INTERVAL:  97-06-29,  00:00:00 THROUGH 23:59:59 "<cr><lf>
<cr><lf>
"NPANXX","NPAQRCV"<cr><lf>
919456,123456789<cr><lf>
408755,23456789<cr><lf>
515555,456789<cr><lf>
302233,345<cr><lf>
703211,99999<cr><lf>
812304,4294967295<cr><lf>
```

Once the LNP measurement files have been created in the file transfer area on the active fixed disk, these files can be transferred to another computer using the **act-file-trns** command for further processing. To make the file transfer, the computer that the files are transferred to must have these items.

- a VT320 or KSR connection to the EAGLE LNP
- a communication program that emulates VT terminals and supports Kermit file transfer, for example, ProComm© for Windows
- a spreadsheet software program that interprets comma separated value text files, for example, Microsoft Excel©

Once the measurement text files have been created, they must be transferred to another computer. When the files have been transferred, they must be removed from the file transfer area with the **dlt-fta** command. If these files are not removed, no other LNP measurement reports of that report type can be created.

LNP—Message Relay (Release 22.0)

Message Relay (MR) contains these enhancements to existing global title translation functions.

- Extraction of 10 digit dialed number from the TCAP portion of the message: If the MSU contains a 6 digit called party address, the 10 digit dialed number is extracted from the TCAP portion of the MSU.
- Increased number of translations: For each 10 digit dialed number, up to 6 translations are available. The previous limit was 270,000 total translations. The number of dialed numbers that can be entered depends on the hardware, but the minimum hardware configuration supports 500,000 dialed numbers, so 3 million translations can be entered on the minimum hardware configuration. The maximum hardware configuration supports 2 million dialed numbers, so 12 million message relay translations can be entered on the maximum hardware configuration.
- Replacing the global title address: The global title address in the called party address can be replaced 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 LNP performs 6 digit (NPANXX) translation. The result of this translation indicates if message relay is required. If it is required, the result of this translation also gives the default data that may be used in stage 3.
2. If the results of stage 1 indicates message relay is required, the EAGLE LNP 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.

LNP—MSU Trap and Trace Command (Release 22.0)

Refer to the *Commands Manual* for current usage information.

The **ent-trace** command is a debug command used to trace MSUs sent to SCCP cards.

LNP—MTP and SCCP Management to Support LNP (Release 22.0)

When the LNP subsystem goes offline, the EAGLE sends SSPs that cause messages with the routing indicator set to SSN to be diverted to the mate subsystem. But these will not cause messages with the routing indicator set to GT to be diverted. In order to make other nodes divert the messages with the routing indicator set to GT to the mate, the EAGLE sends response method TFPs for these messages that require either message relay or LNP query.

There are two reasons the EAGLE generates a response method TFP.

While the LNP subsystem is offline, a message arrives with the routing indicator set to GT for one of EAGLE's capability point codes. The result of the global title translation is the EAGLE's LNP subsystem or that message relay is required on EAGLE.

In both of these cases, the EAGLE generates a TFP concerning the capability point code and sends the TFP to the OPC in the message. This TFP should cause the OPC to divert traffic to the mate. If a message arrives with the routing indicator set to GT for EAGLE's true point code, EAGLE does not generate a TFP. Nodes that send traffic to EAGLE with the routing indicator set to GT should use one of EAGLE's capability point codes, not EAGLE's true point code.

If the EAGLE receives an RSP (Route Set Test Message - Prohibited) for a capability point code that is used for LNP, and the LNP subsystem is offline, the EAGLE does not reply. If the EAGLE receives an RSR (Route Set Test Message - Restricted) for a capability point code for LNP, and the LNP subsystem is offline, the EAGLE replies with a TFP concerning the capability point code. When LNP subsystem is online, the RSRT replies to both RSRs and RSPs for a capability point code that is used for LNP with a TFA.

LNP—New LNP Input and Output Groups (Release 22.0)

The LNP commands described in the New Commands section are assigned to three new command classes: LNP Basic, LNP Database Administration, and LNP Subscription. To allow users to execute these commands, three new parameters have been added to the **ent-user**, **chg-user**, and **chg-secu-trm** commands: **lnpbas**, **lnpdb**, and **lnpsub**. To show the values assigned to these parameters, the **lnpbas**, **lnpdb**, and **lnpsub** fields have been added to the **rtrv-secu-user**, **rtrv-user**, and **rtrv-secu-trm** command outputs.

Two new unsolicited output message groups have been added to support the LNP feature: LNP Database Administration and LNP Subscription. To allow these types of messages to be output on a specific terminal, the **lnpdb** and **lnpsub** parameters have been added to the **chg-trm** command. To show the values assigned to these parameter, the LNPDB and LNPSUB fields have been added to the **rtrv-trm** command output.

LNP—New Unsolicited Alarm Messages (UAMs) (Release 22.0)

LNP Degraded Mode Alarm

This critical alarm is displayed when the system automatically puts itself in a degraded mode because of invalid OAM hardware configuration for the LNP feature.

UAMs

```
*C  0012.0419 *C SYSTEM                Entering LNP Degraded Mode
```

When the reason the system has entered degraded mode is resolved, this message is displayed showing that system has returned to normal operation.

```
    0012.0420    SYSTEM                Exiting LNP Degraded Mode
```

LNP—Auto Inhibit/Uninhibit Alarms

This minor alarm is displayed when an SCCP card does not have the hardware configuration required for the LNP application. Loading of the SCCP card is automatically inhibited.

```
*  0012.0421 *  CARD 1108 SCCP           CARD REPAIR:  Incorrect HW configuration
```

This minor alarm is displayed when an SCCP card hardware configuration does not have enough memory for the LNP data. Loading of the SCCP card is automatically inhibited.

```
*   0012.0422 *  CARD 1108 SCCP         CARD REPAIR: Insufficient memory for LNP
```

When the **alw-card** command is executed, loading of the SCCP card is attempted. This message is displayed indicating that card loading is no longer inhibited.

```
    0012.0423    CARD 1108 SCCP         CARD REPAIR:  Card reload attempted
```

LNP Subsystem Alarms

This critical alarm is displayed when the LNP subsystem is unavailable.

UAMs

```
*C  0012.0424 *C LNP SYSTEM            LNP Subsystem is not available
```

This minor alarm is displayed when the LNP subsystem is available, but the LNP Status of all of the SCCP cards is not ACTIVE.

```
*   0013.0425 *  LNP SYSTEM            LNP normal, card(s) abnormal
```

This message is displayed when the LNP subsystem becomes available.

```
    0014.0426    LNP SYSTEM              LNP subsystem is available
```

LNP—New Unsolicited Information Messages (UIMs) (Release 22.0)

LNP—Subsystem State Change Failures

When the **inh-ss** command is entered and the subsystem is not inhibited, but an inhibit request is already outstanding, this message is displayed.

UAMs

```
    RLGHNCXA03W 97-06-30 16:28:08 EST Rel 22.0.0
    0002.1164    SYSTEM       INFO      Inh LNP SS request already
 outstanding
                 Report Date: 94-03-30  Time: 16:27:19
```

The failure of a coordinated state change of the LNP subsystem resulting from the **inh-ss** command will be reported with this message.

```
    RLGHNCXA03W 97-06-30 16:28:08 EST Rel 22.0.0
    0002.1165    SYSTEM       INFO      Failure Inhibiting LNP SS
                 Report Date: 94-03-30  Time: 16:27:19
```

LNP—ACG Overload Level Change

When the overall ACG overload level of the system has changed, UIM 1166 is displayed.

UAM

```
    RLGHNCXA03W 97-06-30 16:28:08 EST Rel 22.0.0
    0003.1166    SYSTEM       INFO      ACG Node Overload Level Change
                 OLD ACG LEVEL= 4   NEW ACG LEVEL= 5
                 Report Date: 94-03-30  Time: 16:27:19
```

LNP—NPANXX Commands (Release 22.0)

Refer to the *Commands Manual* for current usage information.

ent-lnp-npanxx

The **ent-lnp-npanxx** command is used to add an LNP NPANXX (area code and office prefix) and its associated default global title translations to the database.

pdlt-lnp-npanxx

The **dlt-lnp-npanxx** command is used to remove an LNP NPANXX or its associated default global title translations from the database.

chg-lnp-npanxx

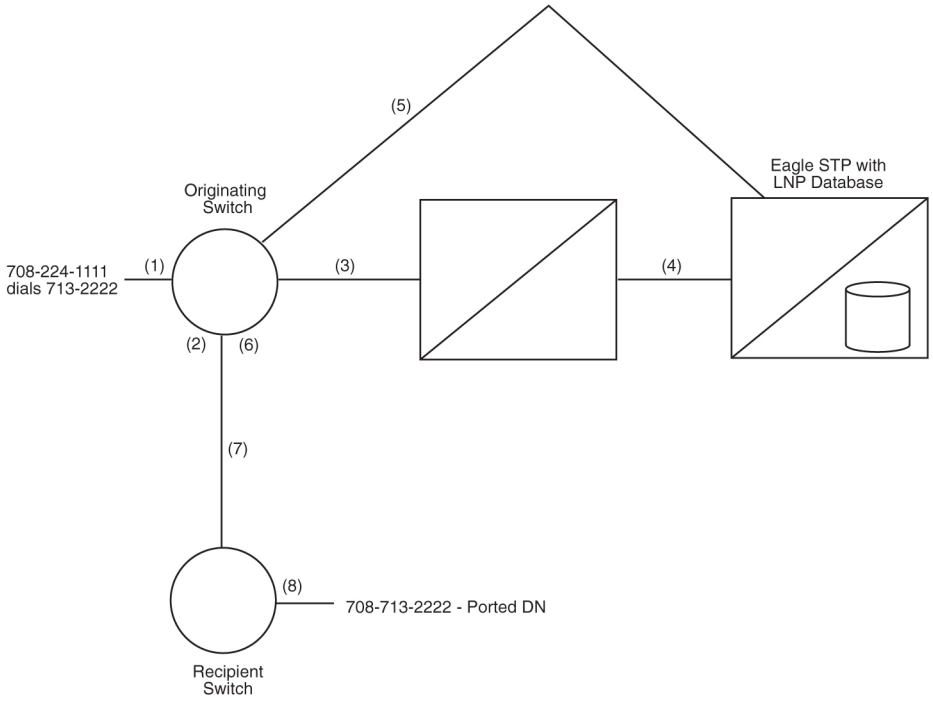
The **chg-lnp-npanxx** command is used to change the attributes of an existing LNP NPANXX and its associated default global title translations in the database.

LNP—Query Routed as Final Global Title Translation (Release 22.0)

Description

This is a case where the final global title translation is performed by a different STP before routing the LNP query to the EAGLE LNP. The first STP performs the 6 digit final global title translation and routes the message using EAGLE LNP's true point code and subsystem number of LNP query application. The EAGLE LNP processes LNP query and sends an LNP response. The following figure illustrates this action.

Figure 4-15. LNP Query Routed as Final Global Title Translation



1. Line A (708-224-1111) dials Line B (708-713-2222).

2. The originating switch performs digit analysis on the dialed digits to determine how to route the call. The switch determines that B is in a portable NPANXX (708-713) and the line does not reside on the switch.

3. The switch sends an AIN (Info_Analyzed) or IN (InstructionStart) query based on the dialed digits to the capability point code of the first STP.

4. The STP performs final global title translation using 6 digits, determines that the query should be routed to EAGLE LNP. The query is routed to LNP application at EAGLE LNP using it's true point code and subsystem number identifying LNP query application.

5. The LNP application at EAGLE LNP finds the telephone number in its LNP database and sends an AIN (Analyze_Route) or IN (ControlConnect) response containing the LRN of the recipient switch.

6. The originating switch receives the LNP response and analyzes the data. The LRN is translated in the LNP routing tables and an ISUP route out of the switch is determined. The LRN is stored in the called party

number parameter and the dialed digits are stored in the generic address parameter of the ISUP IAM message. The FCI translated called number indicator is set to indicate a query has been done (set to “translated number”).

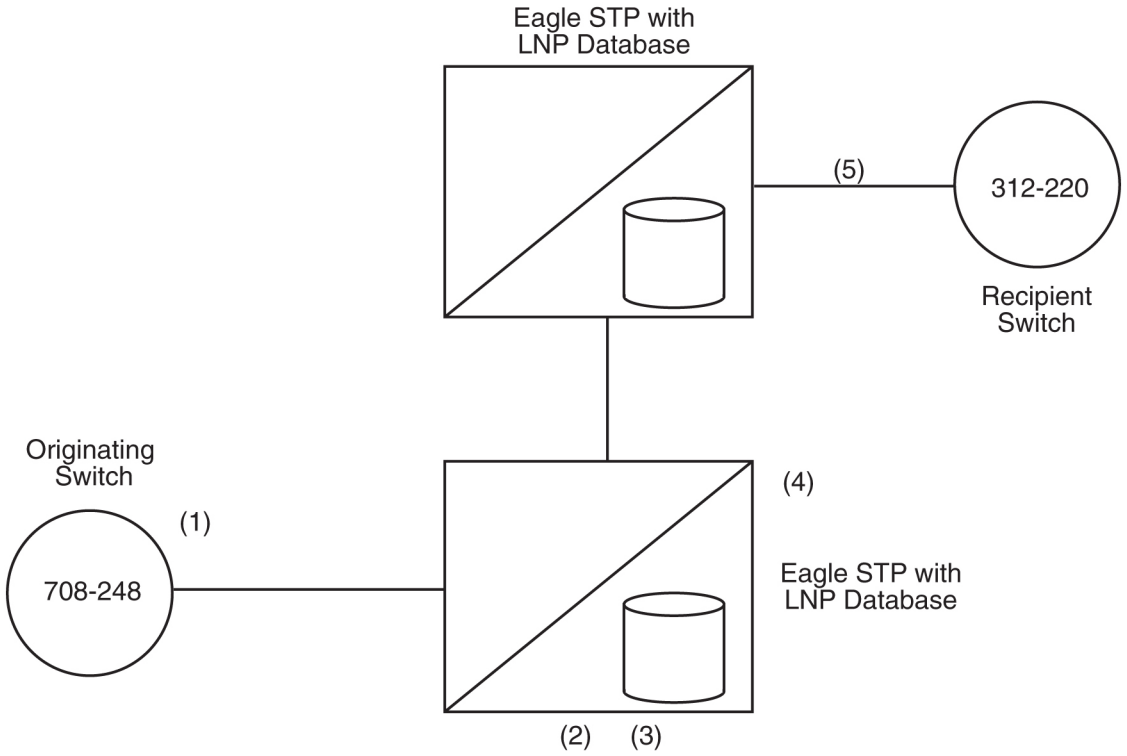
7. The call is routed to the recipient switch based on the LRN.

8. The recipient switch receives and processes the contents of the IAM message. The switch determines that an LRN is received and that it is the switch’s LRN, and the switch replaces the called party number parameter's contents with the dialed digits stored in the generic address parameter. The switch does digit analysis on the dialed digits and finds the subscriber on the switch. The recipient switch completes the call to the subscriber.

Global Title Translation Examples

CLASS TCAP Queries for Portable NPANXX to Another Network

Figure 4-16. Internetwork Class Query



1. The originating switch (708-248) needs to launch a CLASS query for 312-727-1111. The switch formulates the query using the alias point code of the EAGLE STP as the destination, and codes the SCCP global title address as the queried number (312-727-1111). The translation type is coded as appropriate for a CLASS query.

2. The EAGLE STP receives the query and looks up the global title address of 312-727-1111 in the six digit global title translation table identified by the translation type. Since 312-727 has been designated as a portable NPANXX, the six digit global title translation indicates that message requires 10 digit global title translation on EAGLE.

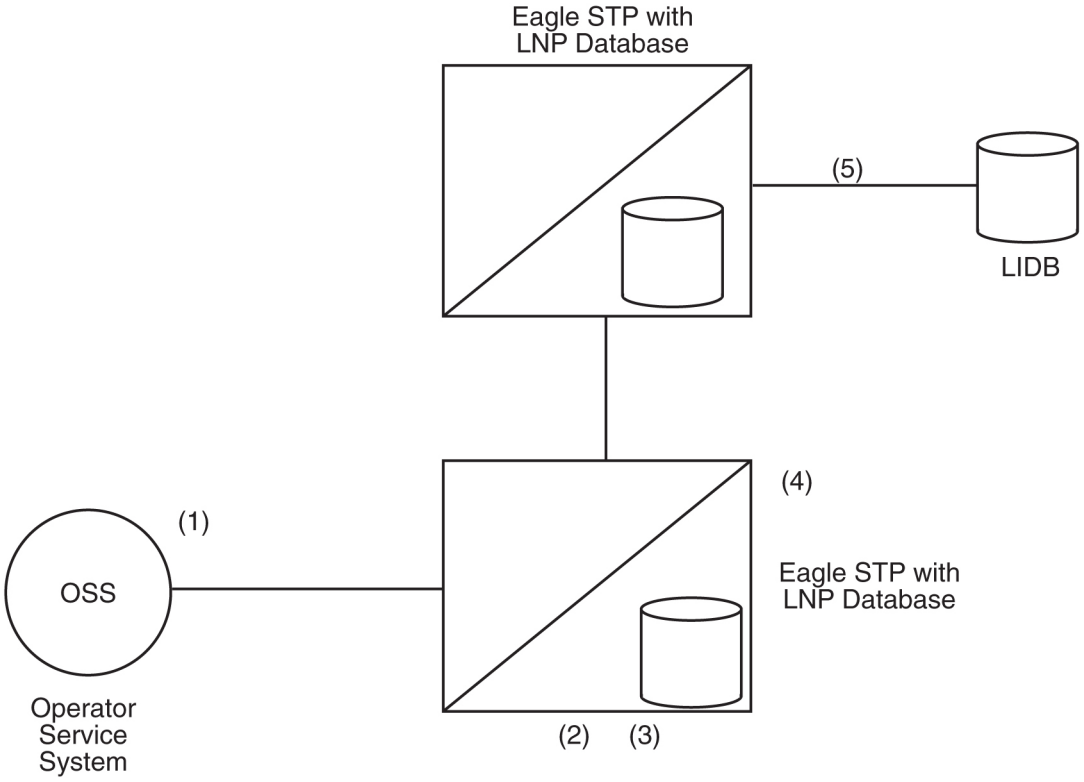
3. The EAGLE message relay function checks to see if there is a ten digit translation for the number in the global title address. If there is, the translation information is used to forward the query to the gateway STP of the switch currently serving that telephone number. If no 10 digit translation is found, then the telephone number is still associated with the donor exchange, and a default six digit translation for the NPANXX value would be performed before forwarding the query.

4. The STP performs MTP routing for the message.

5. The gateway EAGLE STP performs ten digit final global title translation and routes the CLASS query to the recipient switch. Remote subsystem management is performed. The recipient switch processes it as appropriate. The destination SSP can route the response message directly to the originating SSP, since the point code and SSN for the originating SSP would have been carried unchanged in the calling party address of the SCCP.

Internetwork LIDB Query with 6 Digits Included in the Global Title Address

Figure 4-17. Internetwork LIDB Query with 6-Digit GTA



1. The operator service system launches a LIDB query for 312-727-1111. The switch formulates the query using the alias point code of the STP as the destination, and codes the SCCP global title address with the NPANXX of the queried number (312-727). The translation type is for a LIDB query.

2. The STP receives the query and looks up the global title address of 312-727 in the six digit global title translation table identified by the translation type. Since 312-727 has been designated as a portable NPANXX, the EAGLE STP forwards the query to the local LNP global title translation function.

3. The LNP global title translation function recognizes that only 6 digits are present in the global title address. Based on the translation type, the type of query (LIDB) is determined, and the LNP global title translation

function decodes the necessary portion of the LIDB TCAP message to determine the ten digit telephone number for the LIDB query. Once the telephone number has been retrieved from the TCAP portion, the LNP global title translation function checks to see if there is a ten digit translation for the number. If there is a match on the full 10 digits of the telephone number, the translation information is used to route the message. (When no match is found for the 10 digit telephone number in the global title translation translations, the default data would be examined on a six digit basis to determine the translation information.) In this case, the ported number is served by another network, so the ten digit translation indicates a non-final global title translation to route to that network's gateway.

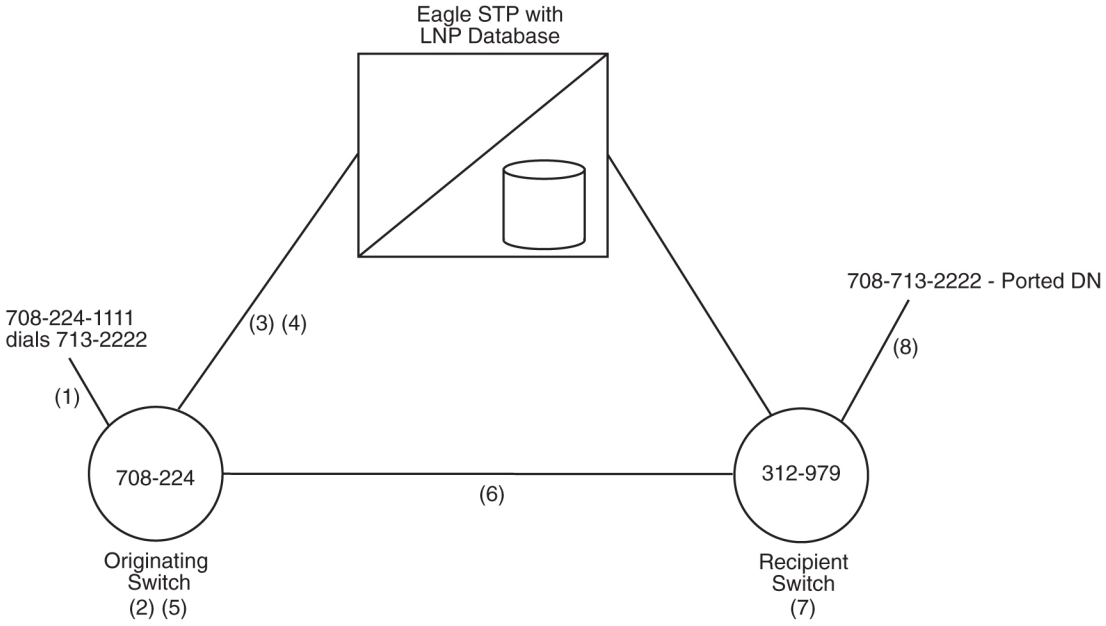
4. The EAGLE STP would perform MTP routing for the message. The message would be routed to the gateway STP in the next network.

5. The gateway STP receives the LIDB query and processes it as appropriate. The gateway STP may be able to perform a final global title translation based on the six digit global title address value, or may need to perform an LNP global title translation to route the message on ten digits. The gateway STP performs remote subsystem management.

LNP—Query Routed as Non-Final Global Title Translation (Release 22.0)

This is a case where the LNP query is routed as a non-final global title translation MSU. The EAGLE STP first performs the regular 6 digit global title translation. If the result of the global title translation is an internal LNP query application, the LNP query is processed and the response is sent to the originating switch. This example illustrates both normal 6 digit global title translation and LNP query processing are done on the same STP. The originating switch uses a separate capability point code (different from capability point code used for non-LNP global title translation) to route LNP global title translation traffic. The advantage of using a separate capability point code is that Level 3 network management can be performed independently for LNP global title translation traffic and non-LNP traffic, such as 800 global title translation traffic. For example, if the LNP application is manually taken out of service, the STP can divert the LNP traffic to the mate by sending a TFR concerning the LNP capability point code. The EAGLE LNP continues to process 800 global title translation traffic.

Figure 4-18. LNP Query Routed as a Non-Final Global Title Translation



1. Line A (708-224-1111) dials Line B (708-713-2222).

2. The originating switch performs digit analysis on the dialed digits to determine how to route the call. The switch determines that B is in a portable NPANXX (708-713) and the line does not reside on the switch.

3. The switch sends an AIN (Info_Analyzed) or IN (InstructionStart) query based on the dialed digits to the capability point code of the EAGLE STP pair. Different capability point codes are used for LNP and non-LNP global title translation.

4. The EAGLE STP performs global title translation on the query and sends the query to a local LNP subsystem. The local LNP subsystem finds the telephone number in its LNP database and sends an AIN (Analyze_Route) or IN (ControlConnect) response containing the location routing number (LRN) (312 979) of the recipient switch.

5. The originating switch receives the LNP response and analyzes the data. The LRN is translated in the LNP routing tables and an ISUP route out of the switch is determined. The LRN is stored in the called party number parameter and the dialed digits are stored in the generic address parameter of the ISUP IAM message. The FCI translated called number indicator is set to indicate a query has been done (set to “translated number”).

6. The call is routed to the recipient switch based on the LRN.

7. The recipient switch receives and processes the contents of the IAM message. The switch determines that an LRN is received and that it is the switch’s LRN, and the switch replaces the called party number parameter's contents with the dialed digits stored in the generic address parameter. The switch does digit analysis on the dialed digits and finds the subscriber on the switch.

8. The recipient switch completes the call to the subscriber.

LNP—Report LNP Status Command (Release 22.0)

The **rept-stat-lnp** command displays the current status of LNP. This command uses the two parameters, **loc** and **card**.

The **loc** parameter is used to display a detailed status of LNP information for the TSM specified by the card location. This detailed report includes information for each of the global title translation (GTT), LNP message relay (LNPMR), LNP query service (LNPQS) and automatic call gapping (ACG) functions.

The **card** parameter has only one value, **sccp-all**. When **card=sccp-all** parameter is specified, a detailed status of LNP information for all SCCP cards is provided.

When the **rept-stat-lnp** command is entered with no parameters, a summary of the LNP status of all equipped TSMs is provided. This summary includes global title translation (GTT) and LNP function status for every TSM as well as LNPQS system information. The possible states of the global title translation status are ACTIVE and SWDL (software loading). The possible states of LNP Status are ACTIVE, OFFLINE and SWDL.

Refer to the *Commands Manual* for current information on this command.

LNP—Rerouting Messages for the Local Subsystem (Release 22.0)

If the local LNP subsystem is unavailable and the mated subsystem is available, EAGLE uses the routing indicator to determine whether to reroute the message.

If the routing indicator of the message is SSN, EAGLE does not reroute the message to the mate. In this case, EAGLE is acting as an end node, and end nodes do not reroute. If the return on error option is set, EAGLE will generate a UDTS, otherwise it discards the message

If the routing indicator of the message is GT, EAGLE reroutes the message to the mated subsystem.

LNP—Retrieve LNP Database Time Stamp Command (Release 22.0)

The **rtrv-lnp-dbts** command displays the LNP database time stamp corresponding to the latest LNP Database update applied by the LSMS.

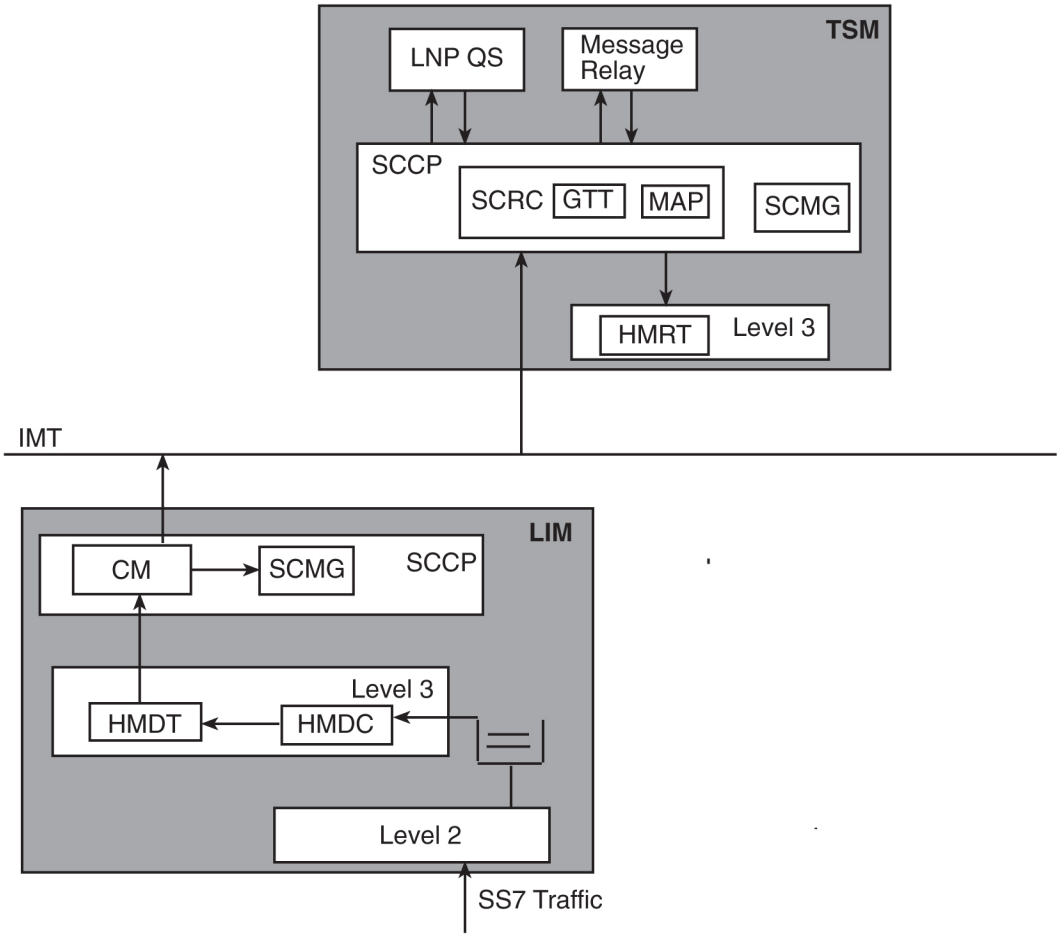
The time stamp displayed by this command is updated when an LNP database is downloaded from the LSMS with the **chg-db:action=import** command or when a command updating a 10 digit telephone number subscription is received from the LSMS.

Refer to the *Commands Manual* for current information on this command.

LNP—SCCP Management on the LIMs (Release 22.0)

SCCP Management (SCMG) on the LIM is used when the LIM does not have an SCCP card assigned to it. The following figure shows the message flow for SCMG. If an SCCP message arrives destined for EAGLE, the cluster manager (CM) attempts to send the message to an SCCP card. If the LIM is not assigned to an SCCP card, the cluster manager sends the message to SCMG on the LIM.

Figure 4-19. SCMG on the LIM



SCMG on the LIM first determines if all SCCP cards have failed. It performs the following functions when all SCCP cards are unavailable:

1. Generate response method SSPs if the routing indicator in the message is SSN for a local subsystem, other than SCMG.

2. Notify MTP to generate response method TFPs if the routing indicator of the message is GT and is destined for an EAGLE capability point code that is used for LNP.

3. Generate UDTS messages if the incoming message is a UDT with the return on error option.

If some SCCP cards are available, SCMG does not send SSPs or TFPs. In this case, the SCCP cards are available, but are overloaded. This is a partial failure: some LIMs have been denied service, but other LIMs have SCCP service. SCMG on the LIM still generates UDTS messages if the incoming message is a UDT with the return on error option.

NOTE: If the UDT message has a calling party address whose routing indicator is set to GT, the LIM does not generate a UDTS, because the LIM cannot perform global title translation.

The following table shows what actions the EAGLE takes when SCCP cards are unavailable and a message arrives requiring LNP.

Table 4-17. Receiving Messages When SCCP is Unavailable

Routing Indicator in Incoming Message	DPC	Full or Partial Failure	LNP Status	Message Handling	Network Management
GT	Capability Point Code	Full	--	Generate UDTS	Send TFP Concerning CPC
GT	True Point Code	Full	--	Generate UDTS	Send UPU
SSN	Capability Point Code	Full	--	Generate UDTS	None
SSN	True Point Code	Full	--	Generate UDTS	Send SSP Concerning True Point Code
GT	LNP Capability Point Code	Partial	Online	Generate UDTS	None
GT	True Point Code	Partial	Online	Generate UDTS	None
SSN	LNP Capability Point Code	Partial	Online	Generate UDTS	None
SSN	True Point Code	Partial	Online	Generate UDTS	None
GT	LNP Capability Point Code	Partial	Offline	Generate UDTS	Send TFP Concerning CPC
GT	True Point Code	Partial	Offline	Generate UDTS	None
SSN	LNP Capability Point Code	Partial	Offline	Generate UDTS	None
SSN	True Point Code	Partial	Offline	Generate UDTS	Send SSP Concerning True Point Code
GT	Non LNP Capability Point Code	Partial	--	Generate UDTS	None
SSN	Non LNP Capability Point Code	Partial	--	Generate UDTS	None

LNP—Service Commands (Release 22.0)

Refer to the *Commands Manual* for current information on the following commands.

`ent-lnp-serv`

The **`ent-lnp-serv`** command is used to assign an LNP translation type to a unique LNP service.

Refer to the *Commands Manual* for current information on this command.

LNP—Service Provider Commands (Release 22.0)

Refer to the *Commands Manual* for current information on the following commands.

ent-lnp-sp

The **ent-lnp-sp** command is used to assign an LNP service provider to the database. The **ent-lnp sp** command uses only one parameter, **sp**—4 alphanumeric characters identifying the service provider.

dlt-lnp-sp

The **dlt-lnp-sp** command is used to remove an LNP service provider from the database. The **dlt-lnp-sp** command uses only one parameter, **sp**—4 alphanumeric characters identifying the service provider.

rtrv-lnp-sp

The **rtrv-lnp-sp** command displays the LNP service provider information in the database.

LNP—Split NPA Commands (Release 22.0)

Refer to the *Commands Manual* for current information on the following commands.

By splitting the NPANXX, the user can force 2 different NPANXXs to reference the same last 4 digits of a 10 digit ported telephone number in the database. When either NPANXX is updated, the 10 digit ported telephone numbers in each NPANXX with the same last 4 digits are updated. When the NPANXX is split, all existing NPANXX data for the NPANXX being split is copied to the new NPANXX.

ent-split-npa

The **ent-split-npa** command is used to add a split NPANXX to the database.

dlt-split-npa

The **dlt-split-npa** command is used to remove a split NPANXX from the database. The **dlt-split-npa** command uses only one parameter, **npanxx** - the split NPANXX, the value in either the NPANXX or NEW NPANXX fields of the **rtrv-split-npa** command output.

rtrv-split-npa

The **rtrv-split-npa** command displays all split NPANXXs in the database. Displaying the split NPANXX is done from the perspective of the old NPANXX, the NPANXX which contains default data.

LNP—Subsystem Application Commands (Release 22.0)

Refer to the *Commands Manual* for current information on the following commands.

ent-ss-appl

The **ent-ss-appl** command is used to reserve a subsystem number for the LNP application and place the LNP application either online or offline using the **ent-ss-appl** command.

dlt-ss-appl

The **dlt-ss-appl** command is used to remove a subsystem application from the database using the **dlt-ss-appl** command. The **dlt-ss-appl** command uses only one parameter, **:appl** = the subsystem application,. The EAGLE LNP contains only one subsystem application, the LNP subsystem application.

chg-ss-appl

The **chg-ss-appl** command is used to set an existing subsystem application either online or offline using the **chg-ss-appl** command.

rtrv-ss-appl

The **rtrv-ss-appl** command is used to display all of the applications from the database. The command displays the application type, subsystem number, and application status.

LNP—System Options Commands (Release 22.0)

Refer to the *Commands Manual* for current information on the following commands.

chg-lnpopts

The **chg-lnpopts** command is used to change the LNP specific options.

rtrv-lnpopts

The **rtrv-lnpopts** command displays the LNP specific system options in the database.

Login Failure Message (Release 21.0)

When a user attempts to log in to the EAGLE and enters either an invalid user ID or password, the EAGLE currently responds with the following message.

Error Messages

```
E2264 Cmd Rej: Password verification failed
```

Error message E2264 is the same message that is issued when the new and verify passwords entered during a password change do not match.

When this message is issued after a failed login attempt, it implies that only password was invalid, when an invalid user ID was entered with a correct password, or both the user ID and password were invalid.

Now, after a failed login attempt, the EAGLE responds with a new message,

```
E2757 Cmd Rej: Invalid userID/password combination.
```

When this message is received, the user should verify both user ID and password.

Error message E2264 is still issued when the new and verify passwords entered during a password change do not match.

Login Success or Failure Tracking (Release 21.0)

When a user has successfully logged on to the EAGLE, a message is displayed followed by 2 lines of login history information. The login history information contains the number of login failures that have occurred since the last time the user successfully logged in to the EAGLE and the date and time of the user's last successful login and the terminal that the user logged in to the EAGLE on. At each successful login, the login history messages are displayed to the user in the scroll area.

```
xxxx LOGIN failures since last successful LOGIN
Last successful LOGIN was on port zz on yy-mm-dd @ hh:mm:ss
```

where:

xxxx—the number of unsuccessful login failures since the last successful login

zz—the number (1 - 16) of the port on which the last successful login occurred.

yy-mm-dd—the date of the last successful login

hh:mm:ss—the time of the last successful login

An unsuccessful login attempt is any use of the **login** command, while not already logged on, that does not result in the user getting logged on to the EAGLE. Some examples of an unsuccessful login in which the failure count maintained for the user ID is incremented are:

- user ID valid, password invalid
- user ID valid, password valid, user ID is already logged on at some other port.
- user ID valid, password valid, user ID has been suspended
- user ID valid, password valid, a password change is required and the new password is not valid
- user ID valid, password valid, the password is older than allowed by the **page** parameter of either the **ent-user**, **chg-user**, or **chg-secu-dflt** commands, the new password is not valid.
- user ID valid, password valid, the user ID has been inactive for a period of time that is greater than the value of the **uout** parameter of either the **ent-user**, **chg-user**, or **chg-secu-dflt** commands.

Login attempts that are rejected while a terminal port is temporarily locked out due to excessive login failures are not counted. While the terminal port is temporarily locked out, the EAGLE immediately rejects all login attempts regardless of the user ID specified on the **login** command and makes no attempt to verify that the specified user ID.

Logout on Communications Failures (Release 22.0)

Whenever communications is lost between the EAGLE and a terminal, the user logged on to that terminal will be automatically logged off. Some examples of communications loss are:

- terminal is powered off
- telephone connection between dial-up terminal and EAGLE is disrupted
- directly-connected terminal is unplugged from the backplane.

When communications between EAGLE and the terminal are re-established, the user must login on the terminal again to access the EAGLE on that terminal.

This does not apply to SEAS terminals. SEAS terminals are considered to be connected to the EAGLE by secure lines and the **login** command cannot be entered on that terminal.

When a user is logged off of a terminal because of a communications loss, the following message is displayed to all terminals that are able to receive unsolicited system administration messages in addition to the affected terminal.

```
User xxxxxxxx auto logged out (communications failure) on port yy.
```

Where:

xxxxxxxx = the user ID that was logged off

yy = the affected terminal port (1 - 16)

If a user is logged off a terminal when the system is in the middle of processing a command that gathers passwords (for example, the **chg-pid**, **chg-user**, or **ent-user** commands), any prompt that is being displayed is removed and the character echo (which was disabled so that the password could be entered) is re-enabled. If the communications loss occurs while the system is in the middle of processing other types of commands (such as a database backup or restore), the user is logged off the terminal, but the command will continue to be executed until it has completed.

If the communications loss occurs while displaying the password prompt while the **login** command is being executed, the command is not interrupted since while the **login** command is in progress, the user is not yet logged in.

If the keyboard is locked when the communications loss occurs, the user is logged off and the keyboard is unlocked.

If a communication failure occurs while a file transfer is in progress, the user is logged off the terminal, but the file transfer continues. The communications failure may or may not affect the successful transfer of the file.

LRN Table Increase (Release 26.1)

This feature increases the size of the LRN table within EAGLE from 30000 LRN entries to 100000 LRN entries. It provides the user the ability to administer up to 100,000 LRN entries at the EAGLE STP. This number was selected because there are possibly 25,000 end offices, with two LRNs per office (2X maximum capacity).

The enlarged number of LRN entries applies to the OAM and SCCPs GPLs.

M2PA on IPLIMx (Release 29.1) (IP7 Release 7.1)

Description

The M2PA on IPLIMx feature provides support for the IETF's SS7 MTP2-User Peer-to-Peer Adaptation Layer (M2PA) protocol to the IPLIMx, prior to RFC status of the protocol.

The SS7 MTP2-User Peer-to-Peer Adaptation Layer (M2PA) protocol supports the transport of SS7 Message Transfer Part (MTP) Layer 3 signaling messages over IP, using the services of SCTP. This protocol would be used between the IPLIMx and an IP Signaling Point employing the MTP Level 3 protocol. M2PA is an IETF-based replacement for the EAGLE STP IP Transport feature.

This protocol is intended for use between:

- a Signaling Gateway (SG) and a Media Gateway Controller (MGC)
- an SG and an IP Signaling Point (IPSP)
- an SG and another SG

where Signaling Gateway (SG) is the IPLIMx-equipped EAGLE STP or IP ^{7} Secure Gateway.

The M2PA on IPLIMx feature enhances IPLIMx in the following ways:

- Adds the M2PA adapter type when provisioning an association for an IPLIMx card.
- Provides an M2PA implementation on IPLIMx that is compliant with v6 of the M2PA internet draft.
- A M2PA link provides for zero message loss on fail-over, while a M3UA link can lose messages.
- A M2PA link provides additional MTP2 features beyond that provided by either SAALTALI or M3UA links.
- A M2PA association acts as both server and client. Both sides of an M2PA link may initiate the association. Two EAGLEs or Secure Gateways can be connected using M2PA links.

The following aspects of IPLIMx remain unchanged by this feature:

- IPLIMx on SSEDCM (870-2372-xx) continues to support both SAALTALI and M3UA links.
- IPLIMx on SSEDCM continues to provide a card capacity of 3000 TPS. Application-rated capacity on other cards is unaffected by this feature.
- IPLIMx on SSEDCM now supports a maximum of eight signaling links. This maximum applies to links of the SAALTALI, M3UA, and M2PA types.
- IPLIMx continues to support only DPC-SLS routing. Routing keys are not supported.
- Multiple ITU-N groups support is provided by SAALTALI and M3UA links. Support of multiple ITU-N groupcodes over M2PA links is provided only for links connecting two Tekelec SGs. Multiple ITU-N groupcode support is not provided by a M2PA link connecting a Tekelec SG to a non-Tekelec IP signaling point.
- IPLIMx does not support ISUP Normalization.

This feature allows for convergence of some signaling and data networks. Switched Circuit Network signaling nodes would have access to databases and other devices in the IP network domain that do not employ SS7 signaling links.

Likewise, IP telephony applications would have access to SS7 services over B, C, and D links. There also may be operational cost and performance advantages when traditional signaling links are replaced by IP network "connections."

Hardware Requirements

This feature requires the Single Slot EDCM (870-2372-01).

Limitations

The M2PA draft v6 protocol provides no facility for specifying network context, such as a group code or network appearance.

IPLIMx supports multiple ITU-N groupcodes over a M2PA link, when the link connects two Tekelec SGs, and each Tekelec SG has the ITUDUPPC feature bit enabled. IPLIMx does not support multiple ITU-N groupcodes

over a M2PAlink, when the link connects a non-Tekelec signaling point, or the Tekelec SG ITUDUPPC feature bit is disabled.

M2PA RFC Support (Release 34.3)

The MTP Level 2 Peer to Peer Adaptation Layer (M2PA) is a protocol used between the SCTP and the MTP Level 3 that enables SS7 links to run over IP.

M2PA provides a mechanism to transport SS7 MTP2 user signaling (e.g., MTP3 messages) over IP using SCTP. M2PA enables seamless operation between MTP2 user peers in the SS7 and IP space.

The M2PA RFC Support feature adds functionality to support the M2PA RFC implementation while continuing to support earlier (Draft 6) implementations.

To aid the transition from Draft 6 to RFC, the following changes are implemented:

1. 20 new M2PA timer sets are created for M2PA RFC associations.

2. Existing associations are changed to have **ver=d6** during upgrade.

3. M2PA Draft 6 timer set values were not changed during upgrade (T16 changed from ms to s, hence table values are multiplied by 1000).

4. M2PA Draft 6 associations use the **d6** timers.

5. M2PA RFC adapters use the **rfc** timers.

NOTE: It is not necessary to change the m2patset value on the association to retrieve the new timer values.

6. The **chg-m2pa-tset** command defaults to the **rfc** values.

7. To change the MP2A Draft 6 timers, a new **ver=d6** parameter is specified.

M3UA Protocol Enhancements (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)

Description

Customers for M3UA have requested the implementation of the enhancements to RFC3332 to ease Application Server development, enhance robustness, and incorporate support for the SG abating congestion and maintaining congestion status of SS7 destinations on behalf of AS's.

Since the introduction of the IETF Sigtran protocols in IP ^{7} Secure Gateway Release 5.0, the IETF has created newer versions of these protocols. This feature updates the IP ^{7} Secure Gateway and EAGLE IPLIMx implementation of these protocols to the current revisions.

The following summarizes the M3UA RFC updates to this feature:

- Tekelec's M3UA implementation adds support for the optional ASP ID parameter.

- Congestion Control
  - — The Secure Gateway prevents a UA (IETF User Adaptation Layers) association from remaining congested forever.
  - — The Secure Gateway maintains congestion status of SS7 destinations on behalf of the Applications Servers, as well as abates congestion.
- This feature complies with RFC3332, and supports additional protocol updates.
- This feature also supports several “custom” extensions to RFC3332, to satisfy customer requests.

Hardware Requirements

The M3UA for IP ^{7} 8.0 feature runs on existing hardware, i.e. the Single Slot Enhanced DCM (P/N 870-2372-01).

Limitations

1. Tekelec's implementation neither supports nor prevents hooking up M3UA to M3UARFC associations, and relies on the M3UA user to configure both ends correctly. A mismatch between versions can transition to the ASP-UP and ASP-Active States, although DATA Messages and others may fail with error messages returned. No adverse affects should occur either.
2. In Tekelec's implementation, since individual queues are not allocated to ASs, any initiation of the AS Recovery Timer T(r) causes the L3_L2 queue for the entire IPGWx card to be placed on hold, queuing messages for all of the AS's ASPs assigned to the card. Because multiple ASs can effectively be assigned to one card, multiple instances of T(r) can be in effect at one time controlling the same L3_L2 queue.

   The net result is that the total time the L3_L2 queue is on hold is longer than the duration of the first timer instance, and is not predictable. Because the delay between multiple instances of the timer can't be predicted, the overlap can't be predicted. If each AS is assigned a different value of T(r), this complicates the problem. Therefore, the total time the queue can be on hold is bounded by either an absolute 200 ms, or by the queue depth exceeding congestion thresholds.

Tekelec's implementation will not account for the ASP ID Race Condition. If two ASPs send ASP-UP messages containing the same ASP ID on two different cards simultaneously, there's the potential that the same ASP ID value will be assigned to both the ASPs.

Management of Unused User IDs (Release 21.0)

In Release 21.0, the EAGLE maintains the date and time that each user ID last successfully logged on to the EAGLE. During the login process, the system computes how many days have elapsed since the last successful login. If the number of elapsed days exceeds the value of the **uout** parameter, used with either the **ent-user**, **chg-user**, or **chg-secu-dflt** commands, access to the EAGLE is denied, and the following message is displayed to the user.

Error Message

```
E2752 Cmd Rej: UserID has become obsolete and cannot be used
```

This test for inactivity is performed after the user ID and password combination has been validated, and before any of the password aging tests.

The **rstlsl=yes** parameter with the **chg-user** command resets the last successful login date associated with the user to the current date. This allows that user to login to the system.

When a user ID is initially created, the last successful login date and time that is entered in the database is set to the date and time that the user ID was created. If a user ID is created and never used, it becomes obsolete when the number of days the user ID was inactive, measured from the creation date, is greater than the value of the **uout** parameter. At that time, the system does not allow a login session to be established with that user ID.

This feature does not apply to all user IDs assigned to the Security Administration command class. If the EAGLE detects that all user IDs have been inactive longer than value of the **uout** parameter (for example, the system administrator mis-typed the date 10 years in the past with the **set-date** command resulting in all user IDs appearing obsolete to the system), no one would have access to the EAGLE and the EAGLE would be un-administrable. Since the EAGLE requires at least one user ID to be assigned to the Security Administration command class, by having this feature not apply to any user IDs assigned to the Security Administration command class ensures that at least one user will always have access to the EAGLE.

Manual Deactivation of SRST Message (Release 21.0)

When a destination for a route becomes restricted or prohibited, the EAGLE starts sending signaling route set test (SRST) messages for that destination. This feature allows a user to manually stop sending signaling route set test messages for a specific destination on a specific route using the **dact-rstst** command. The destination of the route must be either the DPC of the route, a cluster point code of a route, or an entry on the cluster routing exception list. The route's status is changed to allowed.

If the SRST messages for a particular destination have been manually deactivated and that destination becomes restricted or prohibited again, the **dact-rstst** command must be issued again to manually stop sending the SRST messages for that destination.

MAP Table Increase (Release 29.0)

Description

With the MAP Table Increase feature, the number of GTT MAP Table entries can be increased from 1024 to 2000 or 3000, independent of the GTT capacity. The GTT MAP Table is used for final global title applications. This feature is also known as the XMAP feature.

Hardware Requirements

All existing SCCP ASM cards must be replaced with SCCP TSM or better (DSM) equipment when activating XGTT.

All existing SCCP ASM cards must be replaced with SCCP TSM or better (DSM) equipment when activating XMAP.

Measurements Enhancements (Release 22.0)

These new measurements are being added to the EAGLE.

- The GTWY measurement report type.
- The RBASE measurement report type.
- These measurements in the daily reports (MTCD and MTCDTH): OCTRETRN, TLNKACTV and MSURCERR.
- The MTCH measurement report type for the LNP entity. This report contains measurements that apply to the LNP feature. The details of this report are discussed in the LNP Feature Notice.

The GTWY measurement report collects and reports gateway-related data from the STP. The gateway related data collected for this report is the network management and global title translation load on the EAGLE, and the source of this load. The level and source of pass through TCAP traffic is also collected. In previous releases, the MTP cards in the EAGLE did not measure the data required to be reported for the GTWY measurement report. In release 22.0, the MTP cards measure this data which is reported when requested. The MTP cards are polled every 30 minutes for the gateway-related data. The gateway-related data is retained by the EAGLE for 24 hours.

The addition of the GTWY measurements increases the amount of measurements data collected and reported. To make sure that no measurements data is lost when the data is printed on a printer, Release 22.0 requires that the minimum baud rate of the printer is 9600 bps and that the printer must be able to print at a minimum at 1200 characters per second.

The RBASE measurement report reports various data related to the configuration or status of the EAGLE's major configurable components. The data that appears in this report could be obtained in an existing system by issuing a variety of **`rtrv-xxxx`** and **`rept-stat-xxxx`** commands. In release 22.0, this information can be obtained by entering a single command and can be displayed in a single report. The data in this measurement report is obtained from either the database or from maintenance tasks performed on the EAGLE. The data is not periodically collected and stored in same the manner of other measurements data, but it is collected on demand when a RBASE measurement report is requested.

Measurements Platform Filename with CLLI (Release 31.3)

The Measurements Platform Filename with CLLI feature allows Measurement Platform processors on several EAGLEs to send their measurements reports to a single directory on a centralized FTP server without duplicate file name problems or overwritten files caused by multiple EAGLEs writing to the directory.

The Measurements Platform Filename with CLLI function is controlled. Feature ON/OFF status is controlled by a measurements option. when the option is turned ON, the unique CLLI field for each EAGLE is prepended to the beginning of the measurements report file name.

The only other major impact of this feature on the filenames generated to the FTP server is that when the option is ON the year is not included as a part of the name.

Measurements Platform IP Security (Release 31.6)

Description

Secure Shell defines a protocol for secure network services over any non-secure network. The Secure Shell utility SFTP is a file transfer replacement for FTP used for transferring Measurements Platform measurement reports.

SFTP uses the same provisioning information as FTP (IP address, username, password) and transparently replaces FTP. The EAGLE OA&M IP Security Enhancements feature provides the Secure Shell SFTP file transfer program on the EAGLE for the Measurements Platform IP Security feature (and for the IP User Interface telnet sessions).

The EAGLE OA&M IP Security Enhancements Feature provides tools to securely pass data across an otherwise non-secure network. Once the EAGLE OA&M IP Security Enhancements Feature is turned on, the EAGLE provides secure measurements information transfer between the EAGLE and the target server.

In order to use security, the target server needs to support Secure Shell Server with SFTP specified with subsystem option in SSH Server configuration file. When operational, the secure file transfers requires SSHD Server & SFTP server, version 2.0, to be available. (Customer responsibility)

The hardware baseline for EAGLE 31.6 software release only supports EDSM-2G (870-2372-03) for the MCP application. If any DSM-2G card is presently congigured to run the MCP application in an EAGLE 31.6 system, it will be auto-inhibited during it's loading process. The hardware baseline is independent of activated features. Therefore if an MCP is provisioned in any 31.6 system, it must be running on an EDSM-2G.

The swap of hardware from DSM-2G to EDSM-2G for MCPMs must be done prior to the system being upgraded to EAGLE 31.6. The upgrade command will verify that all MCP provisioned in a system are running EDSM-2G prior to executing the upgrade. In event of an MCP running on a DSM-2G, the MO must be removed and the system will need to be booted out of upgrade and the hardware swapped, prior to any re-attempt. This check is to prevent the loss of any MCP service.

If the IP security feature is activated before the software upgrade to Release 31.6, a secure FTP server should be in the Measurements FTP server list before starting the upgrade. The FTP server list can be retrieved via rtrv-ftp-serv. All servers listed with app=meas are Measurements FTP servers. A maximum of two can be Measurements FTP servers. Servers may be provisioned with the ent-ftp-serv command. After the MCP software is upgraded during EAGLE Upgrade to 31.6, it will immediately begin transferring files to the secure FTP server. If no secure FTP server is found, the report transfers will fail. No servers can be provisioned during upgrade, so the servers must be provisioned before upgrade in order to transfer all measurements.

The EAGLE OA&M IP Security Enhancements feature provides the Secure Shell SFTP file transfer program on the EAGLE for the Measurements Platform IP Security feature.

Once the EAGLE OA&M IP Security Enhancements Feature is turned on, the EAGLE provides secure measurements information transfer between the EAGLE and the target server.

Hardware Required

The Measurements Platform feature in Release 31.6, with or without use of the IP Security feature, requires an MCPM card with 32MB FSRAM and 2 GB RAM (EDSM-2G, part number 870-2372-03). This is a hardware baseline change for the MCPM to be upgraded to the EDSM-2G.

NOTE: Release 31.X baseline hardware includes GPSMIIs, HMUXs, -10s TDMs. If these modules are not equipped the act-upgrade command will be rejected.

Limitations

- This feature provides secure access for the EAGLE transfer of data off-board to remote SFTP servers.
- This feature does not provide the remote Secure Shell client or server applications (SSH, SFTP).
- The EAGLE OA&M IP Security Enhancements feature is an On/Off feature. Turning on the EAGLE OA&M IP Security Enhancements disables the unsecure FTP, and telnet functions for all MCPM **and** IPSM cards, and enables secure datat transfer. Turning off the EAGLE OA&M IP Security Enhancements

feature disables the secure data transfer for all MCPM **and** IPSM cards and enables Telnet/FTP functions. Security cannot be enabeld and disabled separately for telnet and Measurements Platform.

- If data transfer is in progress when the EAGLE OA&M IP Security feature is turned on or off, the transfer will be allowed to complete. Subsequent transfers will occur in the mode that is enabled by the change in the feature status (on or off, secure or not secure). The Measurements Platform entries in the FTP Servier table must be defined to allow the switch between secure and unsecure data transfer.

- Multiple SFTP sessions are not allowed on an MCPM card. Each MCPM card in an EAGLE system shall support one SFTP session, but only one session is allowed to be in progress at any given time on the Measurements Platform, regardless of the number of MCPMs installed.

- The Measurements Platform as FTP Client provides no inherent control of access to the FTP session (there is no available way to manually exchange server keys on the EAGLE). Access is controlled at the FTP Server. Thus, references to IP Security on the Measurements Platform essentially describe encryption of the data transmitted during the FTP session.

- There is the potential for the restart data to be over-written on EDSMs. Should a software error occur, the MCPM card will cold-reboot and request reload from mate. Should the fault occur simultaneously on both MCPM cards, Measurement data will be lost.

Measurements Platform—Phase 1 (Release 28.0)

Description

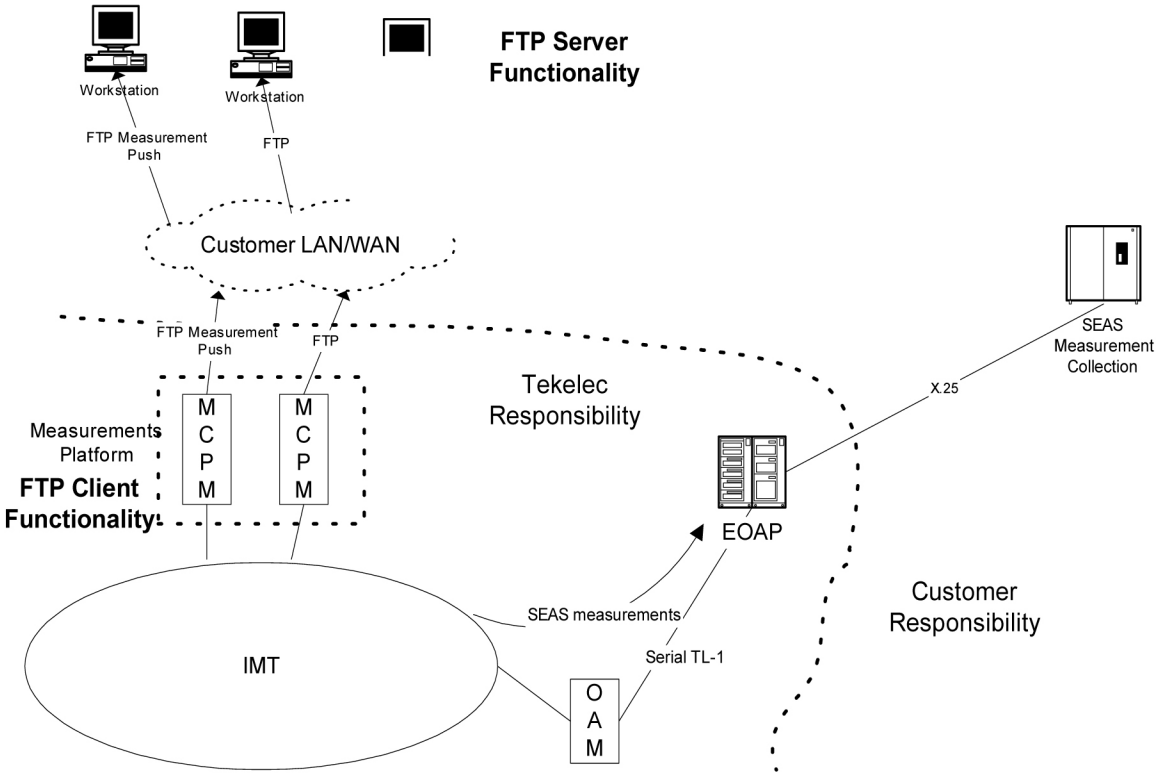
The Measurements Platform supports the growth path of the EAGLE STP beyond 700 links by providing a dedicated processor for collecting and reporting STP, LNP, INP, G-Flex, and G-Port Measurements data. This platform consists of multiple MCPM (Measurement Collection and Polling Module) cards in a primary/secondaries configuration, in which a single primary MCPM performs all collection and reporting functions. The secondary MCPM cards serve as backup for the primary.

NOTE: The measurements platform is required for customers with more than 700 links.

The following figure presents a logical diagram of the Measurements Platform and its interfaces to the customer's network and the existing EAGLE architecture. The EAGLE interface is via the standard IMT bus, and allows communications with the network elements and the OAM. The interface to the customer's network supports the FTP transfer of Measurements reports to an FTP server.

Refer to the *Database Administration Manual - System Management* for configuration information. Refer to the *Maintenance Manual* for detailed measurements information.

Figure 4-20. Measurements Platform Architecture



Hardware Required

The Measurements Platform requires a minimum of 2 MCPM cards with at least 2 GB of memory. For Release 28.0, the Measurement Platform uses GPSM-II based cards (P/N 850-0622-01) as the MCPM cards.

CAUTION

CAUTION: Never install or initialize MCAP cards in MASP slots 1113 and 1115 after features that require GPSM-II cards are provisioned. Attempting to initialize MCAP cards with GPSM-II features provisioned will cause a system outage. Before replacing an existing GPSM-II card in a MASP slot (1113 and 1115) contact Tekelec Customer Service.

During card boot up, the amount of memory in the card is verified; if it is less than 2 GB, the card is inhibited.

For detailed information on hardware, refer to the *NSD Hardware Manual*.

Miscellaneous Command Adjustments (Release 26.0)

Refer to the *Commands Manual* for current command usage information.

Activate Echo to a Terminal

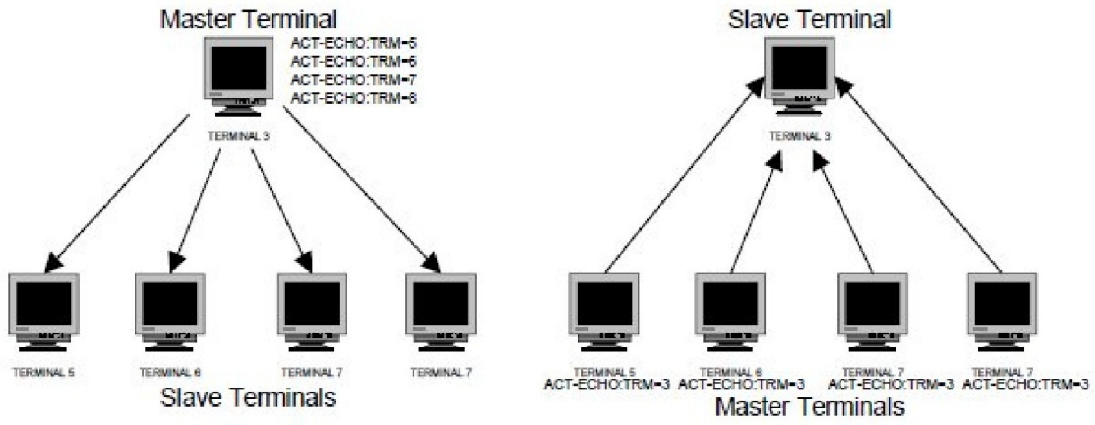
Customers want the ability to echo a terminal to another terminal(s), in addition to a printer. This capability will allow customers to monitor terminal command input and output from another terminal. This will also allow Tekelec's Technical Services group to monitor customer terminal activity while dialed in on a customer's switch.

Also, during upgrades, this feature will allow Technical services to monitor what the customer is entering into the terminal, step-by-step.

Note that unsolicited output (alarm and network messages) still require the **chg-trm** command to be sent to the screen.

The terminal receiving the echo must be logged on.

Figure 4-21. Echoing Remote Terminal Input/Output



Miscellaneous Command Adjustments (Release 26.1)

Customers desire multiple enhancements to the administration functionality for the OAM. The following sections describe the enhancements implemented for Release 26.1.

Different Database Level Alarm Repetition When UAM 34 Has Been Raised (PR28908)

When a card in the system is at a different database level than the active OAM, a UAM 34 is sent to the terminal. Because this occurs only once, operators may not notice the alarm at the card, or might enter a **rtrv-trb**l command to see that the card's database is inconsistent with the OAM. Customers wish to have this alarm added to the list of alarms that are reissued to the terminal at prescribed intervals.

For every card in the EAGLE system that is at a different database level than the active OAM, UAM 34 is logged and issued to the terminal 30 minutes after the database mismatch occurs, and 30 minutes thereafter.

Output Example

```
**     Alarm Summary: Card database is inconsistent   (xxx of yyy shown)
**      ------------------------------------------------------------------------
**      card 1101,  card 1201,  card 1202,  card 1203,  card 3113,  card
1314,
**      card 4101,  card 4102,  card 4103,  card 4104,  card 4105,  card
4106,
```

Ent-/Chg-GTT Failure Message Should Show Overlap (PR28909)

When customers enter or modify GTT's, they are able to do so for a range of Global Title Addresses. If GTT entries already exist within that range, the command is rejected and displayed in the scroll area. Customers want the ability

to see the actual condition that caused the command to fail, instead of having to execute a **rtrv-gtt** or **rtrv-gta** command on that range.

This enhancement affects the **ent-gtt/-gta**, **chg-gtt/-gta**, and **dlt-gtt/-gta** commands.

For **ent-gtt**, the scroll area message shows the first instance of an overlap for an entry/range.

For **chg-gtt**, the scroll area message shows the first instance of the two existing entries/ranges that the user attempted to change.

Examples: VGTT feature is off:

TT	GTA	EGTA	PC	XLAT	RI
253	3037070000	30370799999	1-1-3	DPC	GT
253	3037071000	30370729999	1-1-4	DPC	GT
253	3037073000	30370799999	1-1-1	DPCSSN	SSN

The command **ent-gtt:gta=3037073333** would display an E2401 message, and the scroll area message would be displayed, since there is an overlapping range.

The command **chg-gtt:gta=3037072000:egta=3037074000** would display an E2401 message, and the scroll area message would be displayed, since the change covers two entries. (See the examples below.)

chg-gtt

This example shows what happens when the database contains point codes within the range of 800555000 to 800555999, and the user attempts to change a point code that overlaps that range. In this situation. error message E2401 is generated:

Error Message

```
E2401 Cmd Rej: GTA range overlaps a current range
```

Output Example

```
Enter UI command or 'exit':
chg-gtt:type=2:gta=8005550000:egta=8005555999:pc=5-5-2
chg-gtt:type=2:gta=8005550000:egta=8005555999:pc=5-5-2
Command entered at terminal #4.
    The following GTA ranges overlap the input GTA range
    START GTA             END GTA
    8005550000            8005551999
    8005552000            8005553999
    8005554000            8005555999
E2401 Cmd Rej: GTA range overlaps a current range

        CHG-GTT: MASP A - Command Aborted
```

dlt-gtt

This example shows what happens when the database contains point codes within the range of 800555000 to 800555999, and the user attempts to change a point code that overlaps that range. In this situation. error message E2401 is generated:

```
E2401 Cmd Rej: GTA range overlaps a current range
```

Output Example

```
Enter UI command or 'exit':
dlt-gtt:type=2:gta=8005550020:egta=8005555900
dlt-gtt:type=2:gta=8005550020:egta=8005555900
Command entered at terminal #4.
    The following GTA ranges overlap the input GTA range
    START GTA             END GTA
```

```
    8005550000            8005551999
    8005552000            8005553999
    8005554000            8005555999
E2401 Cmd Rej: GTA range overlaps a current range

        DLT-GTT: MASP A - Command Aborted
```

MSISDN Truncation Support for G-Port (Release 31.6)

In some networks, the SRI-ack response returned by G-Port includes the Routing Number (RN) associated with a ported out number prefixed to the International MSISDN in the MAP MSRN parameter. Depending on the number of digits in the MSISDN and the RN, this prefixing could result in the MSRN parameter exceeding 15 digits. This can cause problems with certain MSCs. Therefore, a new option for G-Port allows a certain specified number of digits to be deleted from the beginning of the National MSISDN (MSISDN without Country Code) prior to formulating the MSRN parameter of the SRI-ack response. (This feature does not affect the encoding of any other parameters or any other messages processed by G-Port.)

A new option for G-Port allows a specified number of digits to be deleted from the beginning of the National MSISDN (MSISDN without Country Code) prior to formulating the MSRN parameter of the SRI-ack response.

MTP and other MRN Message Format Improvements (Release 21.0)

The following table shows the MRNs that have been added to Release 21.0.

Table 4-18. MRNs Added to Release 21.0

MRN	Alarm	Message Text
0010	None	MASP became standby
0061	None	Customer trouble detected
0063	Critical	Critical holdover clock trouble detected
0064	Major	Major holdover clock trouble detected
0065	Minor	Minor holdover clock trouble detected
0066	None	Holdover clock trouble cleared
0204	Minor	REPT-LKF: XER - SUERM threshold exceeded
0206	Minor	REPT-LKF: APF - lvl-2 T1 expd(not ready)
0264	None	REPT-LINK-CGST: congestion level 0 to 1
0265	None	REPT-LINK-CGST: congestion level 1 to 2
0266	None	REPT-LINK-CGST: congestion level 2 to 3
0267	None	REPT-LINK-CGST: congestion level 3 to 2
0268	None	RCVRY-LINK-CGST: congestion level 2 to 1
0269	None	RCVRY-LINK-CGST: congestion has cleared

MRN	Alarm	Message Text
0270	None	REPT-LINK-CGST: discard level 0 to 1
0271	None	REPT-LINK-CGST: discard level 1 to 2
0272	None	REPT-LINK-CGST: discard level 2 to 3
0273	None	RCVRY-LINK-CGST: discard level 3 to 2
0274	None	RCVRY-LINK-CGST: discard level 2 to 1
0275	None	RCVRY-LINK-CGST: discard has cleared
0300	Minor	Active OAM Grant Failure
0301	None	Active OAM Grant Recovery
0302	Minor	CARD REPAIR: Card Auto Inhibited
0303	None	CARD REPAIR: Card Auto Uninhibited
0304	Minor	REPT-NMTSK-DSCD: SNM Discard Onset
0305	None	RECVY-NMTSK-DSCD: SNM Discard Abated
0306	Minor	SNM Overload Onset
0307	None	SNM Overload Abated
0319	Critical	REPT-MTPLP-DET: Circ rte det(cong)
0320	Critical	REPT-MTPLP-SUST:Sustained circ rte(cong)
0321	Minor	X-LIST occupancy threshold exceeded
0322	None	X-LIST occupancy below threshold
0338	Major	X-LIST space full-entry(s) discarded
0339	None	X-LIST space full condition abated
0340	None	RCVRY-MTPLP-RST:Circ rte status cleared
0341	Major	OAP unavailable
0342	Major	SEAS UAL unavailable
0343	Major	SEAS X.25 Link unavailable
0344	Minor	SEAS PVC unavailable
0345	Major	SEAS UAL unavailable
0346	Minor	SEAS PVC session unavailable
0347	None	SEAS X.25 Link is available
0348	Major	SEAS is at min service limit
0349	Critical	SEAS unavailable

MRN	Alarm	Message Text
0350	Critical	SEAS ports inhibited
0351	None	SEAS is available
0352	None	SEAS is removed
0353	None	OAP is available
0354	Major	One SEAS TDM Port unavailable
1083	None	GWS rcvd H0/H1 that is not allowed
1087	None	MTP RSTRT rcvd unexpected user traffic
1088	None	REPT-MTP-RSTRT MTP Restart started
1089	None	RCVRY-MTP-RSTRT MTP Restart completed
1099	None	String Data Dump
1146	None	REPT-XLST-TIMO: X-LIST entry expired
1147	None	MTP Invalid TFA received
1148	None	MTP Invalid TFR received

The following table shows the MRNs that have been changed from Release 20.0 to Release 21.0.

Table 4-19. MRNs Changed from Release 20.0 to Release 21.0

Release 20.0 MRN	Release 20.0 Alarm Level	Release 20.0 Message Text	Release 21.0 MRN	Release 21.0 Alarm Level	Release 21.0 Message Text
0082	Major	Alarm in Fuse Panel	0082	Minor	Alarm in Fuse Panel
0110	Minor	Minor failure detected on both IMTs	0110	Minor	Major failure detected on IMT
0200	None	SLK available: aligned	0200	None	RCVRY-LKF: link available
0201	Minor	SLK unavailable for traffic	0201	Minor	REPT-LKF: remote NE loopback
0202	None	SLK aligned	0202	Minor	REPT-LKF: HWP - too many link interrupts
0203	Minor	SLK unavailable: not aligned	0203	Minor	REPT-LKF: lost data
0205	Minor	SLK unavailable: link failure	0205	Minor	REPT-LKF: APF - lvl-2 T1 expd (ready)
0207	Minor	SLK unavailable: remote blocked	0207	Minor	REPT-LKF: APF - lvl-2 T3 expired
0208	Minor	SLK unavailable: local blocked	0208	Minor	REPT-LKF: APF - lvl-2 T2 expired

Release 20.0 MRN	Release 20.0 Alarm Level	Release 20.0 Message Text	Release 21.0 MRN	Release 21.0 Alarm Level	Release 21.0 Message Text
0209	Minor	SLK unavailable: remote inhibited	0209	Minor	REPT-LKF: APF - failed proving period
0210	Minor	SLK unavailable: local inhibited	0210	Minor	REPT-LKF: OSA - received SIO
0211	None	SLK congestion has cleared	0211	Minor	REPT-LKF: OSA - received SIN
0212	None	SLK congestion onset from level 0 to 1	0212	Minor	REPT-LKF: OSA - received SIE
0213	None	SLK congestion onset from level 1 to 2	0213	Minor	REPT-LKF: OSA - received SIOS
0214	None	SLK congestion onset from level 2 to 3	0214	Minor	REPT-LKF: ABN - rcvd 2 of 3 invalid BSN
0215	None	SLK discard has cleared	0215	Minor	REPT-LKF: ABN - rcvd 2 of 3 invalid FIB
0216	None	SLK discard onset from level 0 to 1	0216	Minor	REPT-LKF: remote congestion timeout
0217	None	SLK discard onset from level 1 to 2	0217	Minor	REPT-LKF: excess acknowledge delay
0218	None	SLK discard onset from level 2 to 3	0218	Minor	REPT-LKF: COO - rcvd changeover order
0219	None	SLK has received SIO	0219	Minor	REPT-LKF: false congestion restart
0220	None	SLK has received SIN	0220	Minor	REPT-LKF: MTP link restart delayed
0221	None	SLK has received SIE	0221	Minor	REPT-LKF: X25 link unavailable
0222	None	SLK has received SIOS	0222	Minor	REPT-LKF: remote FE loopback
0232	None	SLK Level-2 T2 timer expired	0232	Minor	REPT-LKF: remote blocked
0233	None	SLK Level-2 T1 timer exp (not ready)	0233	Minor	REPT-LINK-MANUAV: local blocked
0234	None	SLK Level-2 T1 timer exp (ready)	0234	Minor	REPT-LKF: RMI remote inhibited
0235	None	SLK has lost data	0235	Minor	REPT-LINK-MGTINH: local inhibited
0236	None	SLK is attempting to align	0236	Minor	REPT-LKF: not aligned
0248	None	SLK Level-3 T19 timer expired	1149	None	SLK Level-3 T19 timer expired

Release 20.0 MRN	Release 20.0 Alarm Level	Release 20.0 Message Text	Release 21.0 MRN	Release 21.0 Alarm Level	Release 21.0 Message Text
0253	None	SLK Inhibit denied	1150	None	SLK Inhibit denied
0254	None	SLK Inhibit response timeout	1151	None	SLK Inhibit response timeout
0255	None	SLK Uninhibit denied	1152	None	SLK Uninhibit denied
0256	None	SLK Uninhibit response timeout	1153	None	SLK Uninhibit response timeout
0317	None	Link Set allowed: RCVRY-LKSTO	0317	None	RCVRY-LKSTO: link set allowed
0318	None	Link Set prohibited: REPT-LKSTO	0318	Minor	REPT-LKSTO: link set prohibited

The following table shows the MRNs that have been removed from Release 21.0.

Table 4-20. Release 20.0 MRNs Removed from Release 21.0

MRN	Alarm	Message Text
0006	None	Card connected to IMT
0007	Minor	Card disconnected from IMT
0027	Major	Clock A distribution failed
0028	Major	Clock B distribution failed
0030	None	Clock A distribution normal
0031	None	Clock B distribution normal
0032	None	Clocks A and B distribution normal
0129	Minor	Wrong card type in position
0223	None	SLK has become remotely blocked
0224	None	SLK received 2 out of 3 invalid BSN
0225	None	SLK received 2 out of 3 invalid FIB
0226	None	SLK SUERM threshold exceeded
0227	None	SLK detected remote congestion timeout
0228	None	SLK excessive delay of acknowledgment
0229	None	SLK received an unexpected SIOS
0230	None	SLK has failed proving period
0231	None	SLK Level-2 T2 timer expired
0239	None	Too many link interrupts have occurred

MRN	Alarm	Message Text
0240	None	SLK has received a changeover order
0241	None	SLK has been automatically canceled
0243	None	SLK has returned to service
0244	None	SLK has become locally uninhibited
0245	None	SLK has become remotely uninhibited
0246	None	SLK has become locally unblocked
0247	None	SLK has become remotely unblocked
0249	None	SLTC failure: invalid Point Code
0250	None	SLTC failure: invalid SLC
0251	None	SLTC failure: no response
0252	None	SLTC failure: bad data pattern
0257	None	SLK congestion cleared from level 2 to 1
0258	None	SLK congestion cleared from level 3 to 2
0259	None	SLK discard cleared from level 2 to 1
0260	None	SLK discard cleared from level 3 to 2

MTP Circular Route Detection (Release 21.0)

The EAGLE automatically tests for circular routing when congestion occurs on an ANSI signaling link. If the routing data were provisioned incorrectly, or were corrupted, MSUs could be routed in an endless circular route. The incorrect routing data could be on the EAGLE or at a remote STP. With the addition of cluster routing and E links, the danger of circular routing is greater.

The EAGLE starts the test when a signaling link reaches onset congestion threshold 1. The EAGLE only runs the test for one signaling link per linkset. If a second signaling link in the same linkset goes into congestion, the EAGLE does not start a new test. Each time the signaling link's congestion level increases, the test is restarted. The link interface module (LIM) that terminates to the congested signaling link determines which DPCs have the most MSUs transmitted on the signaling link. The LIM then transmits a circular routing test message to the DPCs that have been sent the most MSUs. The circular route test message can be sent to a maximum of 10 DPCs. This value is configured by the **chg-stpopts** command with the **mtpltctdpcq** parameter. A circular routing test message is a routeset congestion test message with priority of 3.

If any LIM receives one of the test messages before the circular route test timer expires, the EAGLE performs the following actions.

- Marks the destination as prohibited due to circular routing.
- Broadcasts TFPs for the destination.
- Reports that circular routing was detected for the destination.

- Raises a critical alarm.

The circular route test timer can be configured by the user using the **chg-stpopts** command with the **mtpltst** parameter. The **mtpltst** parameter value is between 10 and 20 seconds, with 10 seconds being the default value. The DPC remains prohibited until it is manually allowed using the **rst-dstn** (reset destination) command.

If the destination is a cluster point code entry in the routing table, then an exception list (x-list) entry is created for the destination. If the cluster has the exception list exclusion indicator set to yes (meaning do not create x-lists for that cluster), then an x-list is not created, UAM 319 is generated, and a critical alarm is raised for the cluster. The critical alarm can be cleared by entering the **rst-dstn** command for the cluster. The following is an example of UAM 319.

UAMs

```
    RLGHNCXA03W 96-04-16 16:28:08 EST Rel 21.0.0
*C  0101.0319 *C DPC 011-210-*         REPT-MTPLP-DET: Circ rte det(cong)
                 XMIT LSN=ls01   RC=10
                 RCV LSN=ls14
                 MEMBER=011-210-007
```

If the number of entries in the x-list has exceeded the maximum allowed for the x-list and circular routing is detected, then additional entries to the x-list are not added. In addition to UAM 319 being generated, UAM 321 is also generated. The following is an example of UAM 321.

```
    RLGHNCXA03W 96-04-16 16:21:11 EDT Rel 21.0.0
*   0061.0321  * XLIST                X-LIST occupancy threshold exceeded
```

When a point code is prohibited due to circular routing, the EAGLE ignores TFx/TCx management messages for that point code. The EAGLE does not send routeset test messages for the point code. The EAGLE discards any MSUs received for the point code and sends response method TFPs or TCPs.

When EAGLE detects circular routing for a destination, it sets the circular routing flag for the destination in the routing table. The **rst-dstn** command clears this flag. Once the circular routing flag is cleared, the status of the destination depends on what type of entry is used.

- If the destination is a member of a cluster for which EAGLE performs full point code routing only, all routes to the destination are marked as allowed and the destination's status is allowed. The EAGLE broadcasts TFAs for the destination.

- If the destination has a full point code entry in the routing table, and there is also an entry for the point code's cluster, then each route used by the point code that is also used by the cluster entry assumes the status of the route for the cluster entry. The EAGLE then determines the point codes route set status and broadcasts TFA/TFR if the point code becomes allowed or restricted.

If the **rst-dstn** command is entered for an x-list entry with the circular routing flag set, the x-list entry is deleted. The point code's status becomes the same as the cluster entry's status.

The circular route detection test feature can be turned on or off with the **mtplti** parameter of the **chg-stpopts** command.

The circular route detection test is not performed for ITU or X25 signaling links.

MTP Map Screening (Releases 31.7, 34.0)

Description

MTP MAP Screening is an enhancement to the existing GMS/EGMS features that adds the ability to route MTP traffic whose service indicator (SI) field is SCCP through the MAP Screening subsystem.

If the MTP MAP Screening feature is enabled and turned on and the linkset that an SCCP MSU arrives on has GSMSCRN=ON, the SCCP MSU arrives at the MAP Screening subsystem, even if it does not require GTT, and is MTP-routed. All MAP Screening measurements registers will contain counts for MTP-routed messages in addition to GTT-routed messages.

MTP MAP Screening added the following register to the per-path MTCH and MTCD-MAP hourly and daily MAP Screening reports:

MSCRNPAFP - Total number of messages that contained the forbidden parameter but were not rejected due to Screening action set as PASS

Hardware Required

This feature requires an MCPM EDSM-2G (870-2372-03) card and DSM cards.

MTP Messages for SCCP Applications (Release 36.0)

Description

The MTP Messages for SCCP Applications (MTP Msgs for SCCP Apps feature allows MTP-routed ANSI-41 LOCREQ messages to be subject to the A-Port, IS41 GSM Migration, and G-flex processing. (The GSM messages are still not supported by the IS41 GSM Migration feature.)

The MTP Msgs for SCCP Apps feature can be used only when the A-Port feature or the IS41 GSM Migration feature or the G-Flex feature is on.

NOTE: Use of the MTP Msgs for SCCP Apps feature adversely affects the SCCP capacity, because all of the messages are counted under SCCP capacity.

Service Selection and Routing

All service selector options are not supported by the MTP Msgs for SCCP Apps feature. Only MNP services for the A-Port and IS41 GSM Migration features and GFLEX services for the G-Flex feature are supported by this feature.

Service re-route is not performed on MTP-routed messages.

If the MTP Msgs for SCCP Apps feature is turned on, all SCCP messages are routed to SCCP cards. SCCP cards perform SCCP decode and verification as they do for GTT today.

If the MTP-routed messages have CDPA GTI =0 and the IGM feature is turned on, a message is sent for MNP processing. If MNP service is OFFLINE, MTP routing is performed on messages.

If the MTP-routed messages have CDPA GTI not zero, service selector lookup is performed using the SCCP CDPA information.

- If the result of the lookup is for MNP service, a message shall be sent to MNP handling. MNP shall check if the TCAP portion of the message is ITU or ANSI. If the message has ITU TCAP, the message is forwarded to G-Flex processing. If the message has ANSI TCAP, A-Port general TCAP/MAP verification is performed if A-Port or IGM feature is turned ON.

- If a service selector is not defined or does not match, or if the service is OFFLINE, MTP routing is performed on the messages. Service re-route is not performed on MTP-routed messages.

- Only LOCREQ messages are supported . See the A-Port and IGM feature descriptions for LOCREQ message handling.

G-Flex Feature Processing

If the result of service selector lookup is for G-Flex service, G-Flex message processing is performed. This feature supports GFLEX service for MTP-routed TCAP/MAP messages. If the MTP Map Screening feature is on, MTP Map Screening is performed on post G-Flex messages and fall-through MTP-routed messages.

SMS Address Conversion

SMS Address conversion is not affected by the MTP Msgs for SCCP Apps feature; SMS conversion handles only Registration Notification and SMS Notification messages.

Feature Access Key

A feature access key (FAK) for part number 893017401 is required to enable the MTP Msgs for SCCP Apps feature.

- The A-Port feature or the IS41 GSM Migration feature or the G-Flex feature must be on before the MTP Msgs for SCCP Apps feature can be enabled.

- After the feature is enabled and turned on, it cannot be turned off.

- No temporary FAK is allowed for the feature.

Hardware Requirements

The MTP Msgs for SCCP Apps feature requires DSM cards.

Limitations

None

MTP Restart (Release 21.0)

The MTP restart feature provides an orderly process for bringing signaling links back into service after the EAGLE has been restarted after being isolated. During a node's isolation, its route status information could become incorrect. When the node is restarted, the node starts carrying traffic too soon without updating its routing tables. This results in sending traffic on prohibited and restricted routes which eventually are discarded. This increases loss of traffic and also burdens the network to process this unnecessary traffic.

As routes become available or unavailable during restarting, the node acts on a per event basis and propagates the route status to the rest of the network. The sequence of route status messages broadcast depends on the sequence

in which the routes became available or unavailable. This can result in sending lot of redundant network management messages. Since the route status is propagated from one node to other, this may have a ripple effect and increases the network management load of the network.

When the MTP restart process is used, a restarting node does not start carrying user traffic until a sufficient number of signaling links are available and the routing tables are sufficiently updated with the current status. Also, the restarting STP broadcasts the network management messages only after its routing table are updated. This reduces the number of unnecessary network management messages broadcast to the adjacent nodes and also makes the behavior of restarting STP more predictable.

The MTP restart process is started when the EAGLE detects that it has been isolated under the following conditions.

1. SS7 application subsystem loading (after power on reset, system initialization or SS7 application subsystem initialization). In this case, route status is lost due to memory reset.

2. When the node is totally isolated for a period of time that is equal to the isolation timer (**mtprsit**) due to all signaling link failures (for example, losing both primary and secondary clock). The isolation timer is configurable. In this case, the status of the routes may become inaccurate due to the long amount of time that the node is isolated. The MTP restart procedure is started only if the node is isolated for a period of time that exceeds the value of the isolation timer. The reasons for waiting for the isolation timer to expire before starting the MTP restart process are:

    a. If the amount of time that the node is isolated is less than the isolation timer, the status of the routes is more accurate.

    b. Allows the EAGLE to force uninhibit signaling links and come out of isolation.

The following conditions should also be met for starting a full MTP restart:

- The MTP restart feature is enabled (**chg-stpopts:mtprsi=yes**)

- There is at least one restart-capable adjacent node (linkset parameter **mtprse=yes**)

There are other conditions in which the EAGLE may have inaccurate route status information such as a major but partial failure of the EAGLE. The MTP restart process is not invoked in these cases. However, such failures are likely to cause adjacent nodes to become unavailable. This may result in invoking of the MTP restart process in the role of being adjacent to a restarting node.

The MTP restart process brings the signaling links back into service in four steps.

1. The signaling links are activated and traffic is stopped.

2. The EAGLE receives route status information from all adjacent nodes.

3. The EAGLE broadcasts route status information to all adjacent nodes.

4. Traffic is restarted.

User traffic is not carried on the signaling links during the MTP restart process. Two new protocol messages have been defined to signal the adjacent nodes when traffic may be sent on the linkset connecting the restarting node and the adjacent node.

1. Traffic-restart-waiting (TRW) — an indication to the receiving STP that no user traffic can be sent to the sending signaling point.

2. Traffic-restart-allowed (TRA) — an indication to the receiving STP that user traffic can be sent to the node sending the TRA message.

The route status is exchanged using Transfer (TFx) and Transfer Cluster (TCx) messages.

The MTP restart feature is supported only for ANSI signaling links. This feature is not supported for ITU and X.25 signaling links.

The time it takes to come out of isolation (when the first signaling link is available to carry level 3 traffic) is not increased due to the MTP restart feature.

Message Routing

Route availability has two parts:

- The network route status. This is affected by the TFx/TCx network management messages received from the network. The network route status is in either an Allowed, Restricted, or Prohibited state.

- The local route status. This is affected by changes in the linkset states. Currently, this can be either Allowed or Prohibited.

The MTP restart feature affects the linkset state and thus affects the local route state of all routes using that linkset. Currently a linkset can be in one of the two states, Available or Not Available. With the MTP restart feature, in certain states of the restart procedure, a linkset is available to carry only certain type of messages. During these states, the linkset is available to carry network management messages, signaling test, and maintenance messages that are originated and terminated at the nodes engaged in the MTP restart process. The linkset is not available to carry other types of messages which are commonly referred as user traffic. The user traffic includes ISUP, SCCP and management messages like TFC which are not originated and terminated at the nodes engaged in the MTP restart process. A new state Restart has been added to the local route status during which it is not available to carry user traffic. The local route state of a route can now be in one of three states.

- Prohibit — Linkset failure, same as before

- Restart — Because of the MTP restart process, the linkset cannot carry user traffic

- Allowed — Linkset available to carry all traffic

Aligning Signaling Links in a fully Restarting Node

During the MTP restart process, all adjacent nodes are sending TFx/TCx messages to the restarting node. To handle this burst of traffic and to avoid excessive network management load, the signaling links are activated in the following order:

1. restart-capable signaling links

2. non-restart-capable signaling links

3. X.25 signaling links

If the MTP restart feature is turned on, the alignment of all ANSI signaling links is delayed until all the LIMs containing ANSI signaling links are in service. This allows the EAGLE to be restored to network service in an orderly fashion and allows all the LIMs containing ANSI signaling links to participate in the MTP restart process. The amount of time that the alignment of the signaling links is delayed is dependent on the number of LIMs in the EAGLE and is shown in the following table.

Table 4-21. MTP Restart Signaling Link Alignment Delay

Number of LIMs Containing ANSI Signaling Links	Signaling Link Alignment Delay
1 to 64	62 seconds
64 to 127	97 seconds
128 to 191	132 seconds
192 or more	167 seconds

Measurements

One new measurement has been added to support the MTP restart feature.

Number of MTP Restarts Initiated —The number of times a full MTP restart is initiated by the STP. This measurement count does not include the number of times the MTP restart process was initiated as a result of messages from adjacent nodes.

This measurement is collected for the whole system and is reported every hour in the STP-SYSTOT measurement report.

Event Reporting

Two new UIMs have been added to support the MTP restart feature.

UIMs

1. Commencement of MTP restart process (UIM 1088) — This UIM shows that the EAGLE has started the MTP restart process. The following is an example of UIM 1088.

```
RLGHNCXA03W 96-04-16 16:28:08 EST Rel 21.0.0
0002.1088    SYSTEM       INFO  REPT-MTP-RSTRT MTP Restart started
             Report Date: 96-04-16  Time: 16:27:19
```

2. Completion of MTP Restart (UIM 1089) — This UIM shows that the EAGLE has completed the MTP restart process. The following is an example of UIM 1089.

```
RLGHNCXA03W 96-04-16 16:28:08 EST Rel 21.0.0
0002.1089    SYSTEM       INFO  RCVRY-MTP-RSTRT: MTP Restart Completed
             Report Date: 96-04-16  Time: 16:27:19
```

Alarms

No new alarms are required for this feature. The definition of clearing an existing alarm messages has changed because of the MTP restart feature.

- Critical Alarm 0308—Node Isolated due to SLK failures

  This alarm is cleared when the first signaling link becomes available at level 3 and not when the EAGLE is ready to carry user traffic like ISUP/SCCP. Even though this alarm is cleared, the EAGLE is not available to carry user traffic because the MTP restart process is in progress.

Multiple Capability Point Codes (Release 21.0)

Before Release 21.0, the EAGLE could have only one capability point code of each network type (ANSI, ITU international, and ITU national) defined with the self ID of the EAGLE. With this feature, the EAGLE can have up to 96 capability point codes and these capability point codes can have any mixture of network types. This feature also allows the EAGLE to use capability point codes when performing global title translation. The capability point code identifies a group of functionally related STPs.

Messages requiring global title translation can be sent to other STPs to determine the final destination of the message. Since each STP has its own unique point code, the message must be sent to a specific STP. There can be more than one STP in a network that can perform the global title translation on the message. To make it easier to route these messages to STPs, capability point codes are assigned to the STPs and the global title translation tables are configured with the capability point code instead of the self ID point code of the STPs in the network. The capability point codes can be assigned to more than one STP in the network.

This allows other STPs to handle the required translation if, for example, the desired STP fails and no action would be required at the sending STP or at the other signaling points in the network to route the message to other STPs in the network to get the required translation.

Multiple Country Code Support for G-Port (Release 31.6)

Description

Currently, the EAGLE's G-Port MNP feature allows entry of one Default Country Code (DEFCC) per system. The DEFCC has four main uses in G-Port:

To condition non-International format MSISDNs received by G-Port prior to performing a Mobile Number Portability (MNP) database lookup. (All Mobile Switching Integrated Services Digital Network Numbers (MSISDNs) stored in the MNP database are stored in International format. Therefore, if a MSISDN is received in National format, G-Port converts it to International by appending the DEFCC.)

To formulate the CC+RN+MSISDN response format for the MSRN parameter in SRI-ack responses. (In this case, G-Port compares the DEFCC against the leading digits of the International MSISDN (i.e. CC+MSISDN) to determine where to place the RN returned from the database.)

To formulate the CC+RN+MSISDN format in the outgoing SCCP CdPA GTA parameter in message relay scenarios for non-SRI messages. (As with MSRN formulation, G-Port uses the DEFCC to determine where to place the RN).

To perform HomeRN deletion. Again, G-Port uses the DEFCC to determine which digits are the RN.

Certain operators wish to use a single MNP database to handle portability for different countries, and some areas may have more than one country code defined. In this case, due to condition 1 noted above, G-Port would not be able to correctly condition numbers that are received in non-International format, because it will always append the same DEFCC. However, because numbers must be provisioned in International format in the MNP database, this limitation can be easily overcome by insuring that the Mobile Switching Centers (MSCs) always send the

MSISDN in the SCCP Called Party Address (CdPA) in International format. Therefore, no conditioning needs to be performed.

On the other hand, if these customers also require the use of the CC+RN+MSISDN format in the SRI-ack response or for message relay, G-Port is currently unable to handle this condition. This is because G-Port currently uses the DEFCC to determine which digits of the International number are the CC, and there can be only one DEFCC per system.

Likewise, if the EAGLE is configured to perform non-SRI message relay using the digit action of "Insert", this will cause the SCCP CdPA of outgoing messages to be in the format CC+RN+MSISDN. Using only DEFCC, the same problems would be encountered when constructing the outgoing SCCP CdPA as detailed for the MSRN parameter above.

The Multiple Country Code Support for G-Port MNP feature addresses the problem noted in condition 2 above. The G-Port MNP feature is modified to provide support for up to 10 "Multiple Country Codes" (MultCCs) for use in formulating the MSRN parameter of the SRI-ack response for G-Port Query Response, and for constructing the SCCP CdPA in certain cases of G-Port Message Relay.

The existing **defcc** parameter in the **chg-stpopts** command will continue to be used for conditioning of numbers to International format when necessary, and will also be used for constructing the MSRN and SCCP CdPA parameters in addition to the new MULTCC list.

This feature provides the ability to define multiple country codes in the system (up to 10) for use by the G-Port MNP feature, in addition to the existing default country code (**dsefcc**).

Limitations

- For a network using multiple country codes, it is assumed that all messages needing G-Port service will be sent with MSISDNs in International format. This is true whether the SCCP CdPA digits or the MAP MSISDN digits are used for the database lookup. (This is determined by the message type and the setting of the SRIDN option in G-Port). There continues to be only one default country code (DEFCC) per system for conditioning of non-International MSISDNs. All MSISDNs sent in National format will be conditioned using the same system-wide DEFCC, regardless of the actual country code that may be assigned to the MSISDN.

- This feature changes only the encoding of the MAP MSRN parameter in the SRI-ack response generated by G-Port for a ported out number and the encoding of the SCCP CdPA parameter for G-Port message relay when Digit Action = "Insert". It does not change the encoding of the MAP MSISDN or SCCP CdPA parameters in the SRI-ack, or SCCP parameters when Digit Action is not equal to "Insert".

- The country code search is a longest match search; for example, if MSISDN = 12345, and two country codes are provisioned equal to 1 and 123, G-Port MULTCC will match on 123 for this number and consider this to be the country code. There may be cases of overlap depending upon the country code and the digits allowed by the particular numbering plan. For example, assume 1 and 123 are both valid country codes for the node. Also assume that 2345 is a valid National MSISDN for country code 1. This will cause a problem with G-Port because MULTCC will match on 123 for this number, and consider the National MSISDN to be 45 instead of 2345. Therefore, the number returned will be 123RN45 instead of 1RN2345 as it should be. Using country codes of all one length will reduce the likelihood of a mismatch occurring.

Multiple Flash Download (Release 29.0)

Description

This feature reduces the total time required to update Flash GPLs (i.e. board PROM) by providing the capability to simultaneously update, via commands, the Flash GPL for multiple cards.

Hardware Requirements

No new hardware is needed to support this feature.

Multiple LFS Tests (Release 26.0)

Overview

The Multiple Link Fault Sectionalization (LFS) Feature allows the maintenance craftsperson to perform up to 16 DSOA fault sectionalization tests from the EAGLE. The LFS tests are initiated by the EAGLE, and are used to test the functionality of the link from the EAGLE SS7 LIM through multiple channel banks to a remote Network Element. With this feature, a craftsperson can test up to 16 SS7 links simultaneously. An unlimited number of tests are supported if the EAGLE is not the integrating node for the LFS test.

NOTE: The Multiple LFS is a debug tool provided to the craftsperson. It should be used to help isolate a link failure. Improper use of this feature can result in a link element stuck in a far-end loop-back mode. If an LFS test is aborted by a card reset, it could leave the remote far-end loop-back condition active. Therefore, LFS tests must always be cancelled by the craftsperson if they need to be aborted.

Latching versus Non-latching LFS Tests

The process of activating and maintaining a loop-back is the major difference between latching and non-latching LFS tests.

Non-latching loop-backs are activated by the transmission of the following sequence:

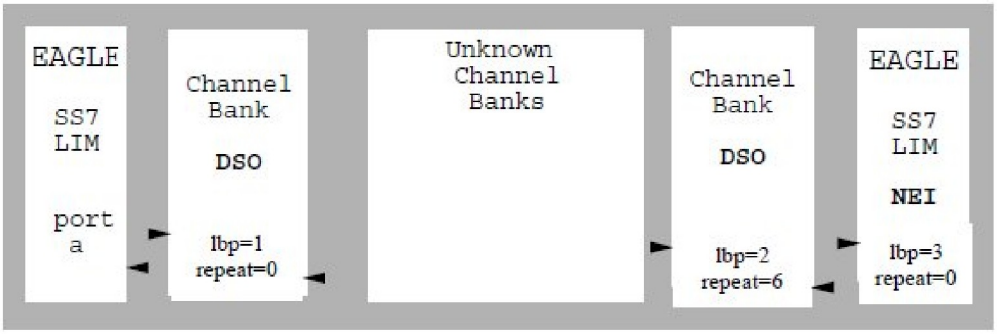
- Minimum of 40 bytes of loop-back code, in multiples of 40 bytes, transmitted continuously until a software command is received to halt transmission or begin test data transmission.
- Alternating loop-back code and test data transmitted continuously until a message is received to halt transmission.

In this case, the loop-back is dropped if every other byte transmitted is not a loop-back code.

Latching loop-backs are activated by the transmission of a sequence of pre-defined control codes. In this case, once the loop-back is established, it can only be removed by another set of pre-defined control codes.

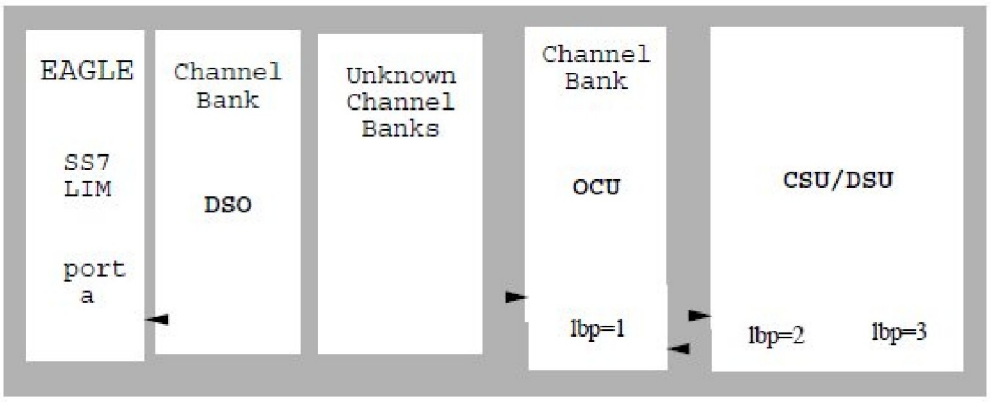
The following figure illustrates a link from an EAGLE to another EAGLE with two DSO Channel banks in the path, allowing for three LBP for Latching LFS Test.

Figure 4-22. DSO Link LBPs for LLT



The following figure illustrates a link from an EAGLE to a CSU/DSU with a DS0 and OCU in the path, allowing for three LBP for Non-Latching LFS Test. A loop back cannot be set in the DS0.

Figure 4-23. OCU/DCU link LBPs for NLT



Administrative commands (**ent-lbp**, **chg-lbp**, **dlt-lbp** and **rtrv-lbp**) are used to store, change, delete and confirm the SS7 link RLEs as LBPs in the EAGLE database, where the RLE nearest the EAGLE is known as LBP one.

The following figure shows the valid RLE types for LLT and NLT.

Table 4-22. Remote Link Element (RLE) Types

Element	RLE Description	Valid RLE for LLT	Valid for RLE for NLT
DSO	DSO Dataport.	Yes	No
OCU	OCU Dataport.	Yes **	Yes
CSU	CSU Dataport.	Yes **	Yes
DSU	DSU Dataport.	Yes **	Yes
NEI	Network Element Interface	Yes	No

UAM

```
** The OCU, CSU and DSU must be strapped/optioned to support Latching
LFS loop back.
```

Maintenance commands (**act-lbp**, **dact-lbp**) should be used to initiate and stop the LFS feature. The SS7 LIM card must be powered up and in service with the link deactivated (OOS_MT_DSBLD) prior to invoking the LFS tests. No SS7 traffic will be transferred to or from the signaling link by the SS7 LIM while the link is performing an LFS test.

Multiple Point Code Support (Release 26.05)

Overview

Currently, the EAGLE supports three true point codes (one each for ANSI, ITU-National, and ITU-International). In addition, the EAGLE supports up to 96 capability point codes, each of which can be designated as either ANSI, ITU-N, or ITU-I. Each capability point code defined on an EAGLE node can be used for routing messages to that node. For various reasons, customers might need the EAGLE to support more than one true point code in a particular domain.

This feature adds the ability to support Secondary Point Codes (SPCs) in addition to the true point codes used by the EAGLE in any of the three domains ANSI, ITU-N and ITUI. Secondary point codes are used by provisioning and routing as if they are the true point code of the EAGLE. SPCs are supported for any type of link (A, B, C, D, etc.). There is no effect on provisioning capability point codes as a result of this feature.

In addition to the one True Point Code (TPC) already supported for each of the ANSI, ITU-N and ITU-I domains, the EAGLE support a pool of 40 Secondary Point Codes (SPC), each of which may be assigned as either ANSI, ITU-N, or ITU-I (not to exceed a total of 40 in one system). SPCs can be used in the same ways that true PCs are used.

There are three main reasons for this feature:

1. Some customers desire to collapse multiple existing STP's into one EAGLE. This can present problems in that end offices and other nodes may not be controlled by the carrier making reprovisioning of these network elements difficult. Multiple Point Code (MPC) support is designed to allow the EAGLE to assume more than one point code for SS7 routing. MPC support is different in concept from capability point codes in that provisioning and routing will use secondary point codes as if they were the actual point code of the EAGLE.

2. Several customers in the international market want to deploy a single STP pair in multiple national (ITU-N) networks. This may not be possible without the MPC feature, as these operators are often forced to use a unique point code assigned by each national regulator of these target countries.

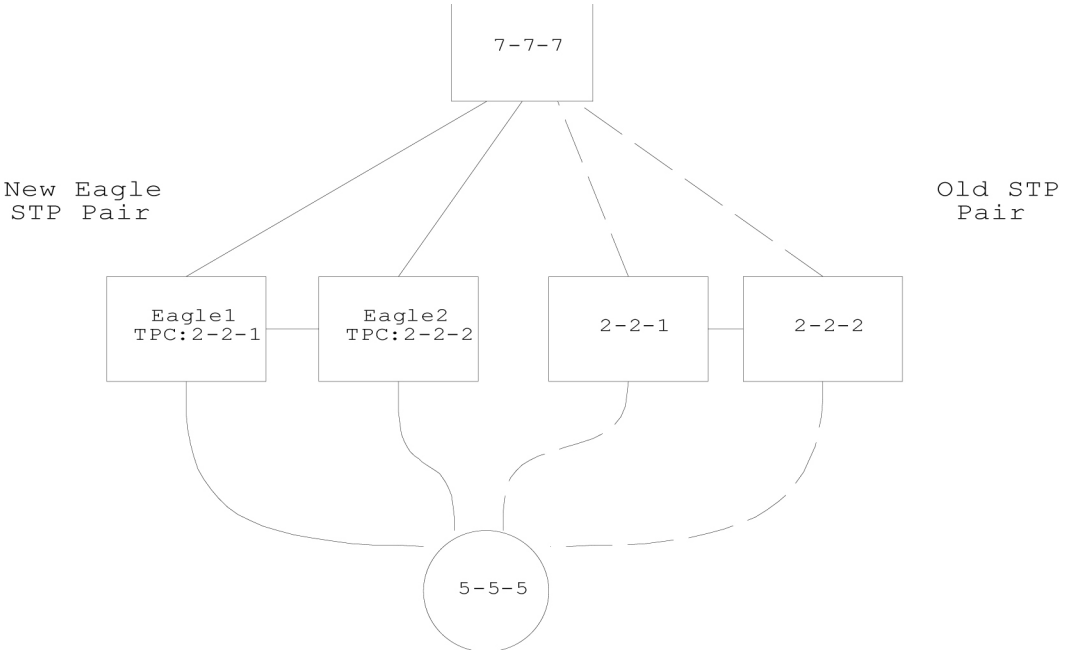
3. Customers may require additional links between two nodes beyond the number of links permitted by the protocol. For example, the maximum number of links between two nodes in an ITU network is 16. The MPC feature can allow for additional linksets between these nodes, increasing the number of links that can be used.

Replacing Two STP Pairs with One EAGLE Pair

The following example shows how an EAGLE pair can replace two existing STP pairs. In this example, each EAGLE in the pair uses one True Point Code and one Secondary Point Code.

As shown in the following figure, a new EAGLE first replaces one existing STP pair. In this case, EAGLE's True Point code is set to the True Point Code of the old STP. The adjacent nodes are cut over to the EAGLE STP pair. The adjacent nodes do not need to be reconfigured.

Figure 4-24. Replacing the First STP Pair



Next, a second STP pair is replaced with the EAGLE pair. As shown in the following figure, an SSP and an STP are being “re-homed” from an old STP pair to a new EAGLE STP pair. In this example, the STP (3-3-3) is reconfigured with new routes to recognize that it is now connected to Eagel1 and EAGLE2 instead of 1-1-1 and 1-1-2. STP 3-3-3, if not an EAGLE STP with Multiple Point Codes, may not be able to support more than one linkset to the same point code. See Multiple Linksets between Two Nodes for a description of this capability. The interconnecting device (STP or SSP) can use either the TPC or SPC as the device requires.

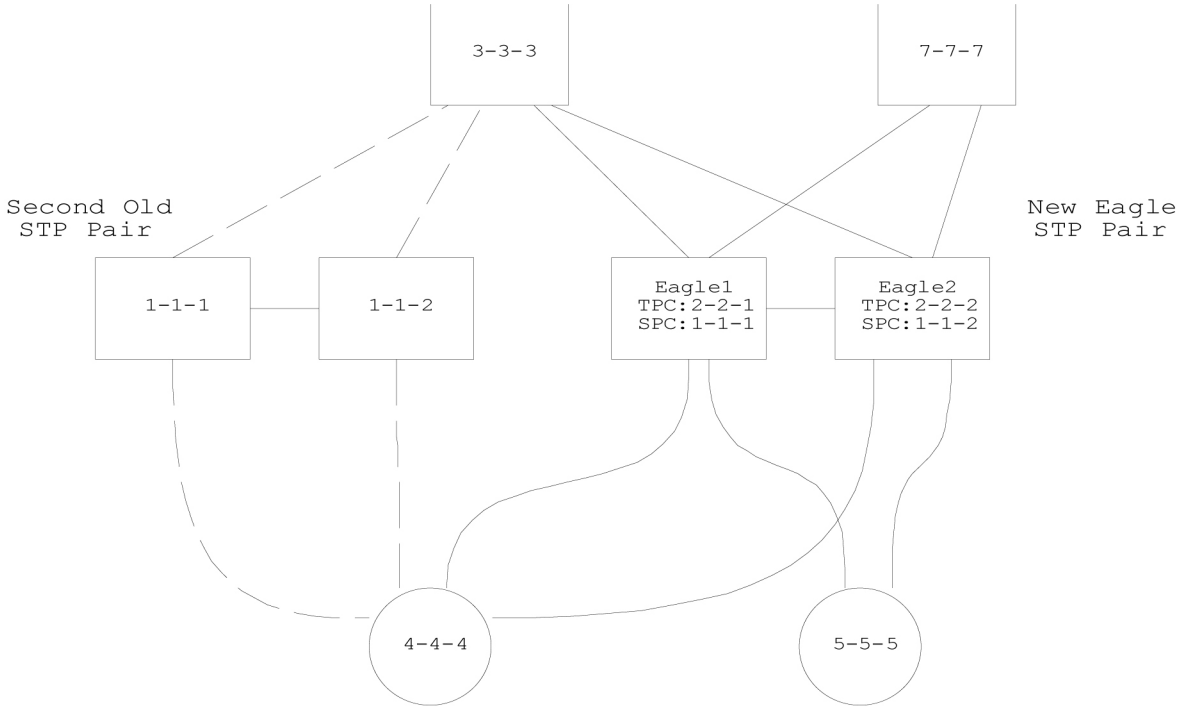
At EAGLE1, the user would configure the secondary point code 1-1-1, using the **ent-spc** command. The user would also configure a route to 1-1-2 over the C-linkset. The user would then configure point code 4-4-4 in the EAGLE's database to indicate that this point code uses the secondary point code 1-1-1, instead of the EAGLE's true point code (**chg-dstn:dpc=4-4-4:spc=1-1-1**. This last step would be repeated for all other adjacent SSPs and SCPs that are re-homed from the old STP Pair to the new EAGLE Pair.

Similarly, at EAGLE2, the user would configure the secondary point code 1-1-2, and configure a route over the C-link to 1-1-1. The user would also configure point code 4-4-4 in EAGLE2's database to indicate that this point code uses the secondary point code 1-1-2, instead of the EAGLE's true point code.

When EAGLE1 receives a message from the SSP destined for 1-1-1, EAGLE processes the message as if the message was sent to EAGLE's True Point Code.

When EAGLE1 generates a message (for example, Network Management, Link Test Messages, or GTT messages) that is destined for 4-4-4, EAGLE1 puts the OPC 1-1-1 in the message. When EAGLE1 generates a message that is destined for 3-3-3 or 5-5-5, it puts the OPC 2-2-1 in the message. When EAGLE1 generates GTT and SCMG messages that are destined for non-adjacent PCs, it includes the OPC 2-2-1 in the message.

Figure 4-25. Replacing a Second STP Pair

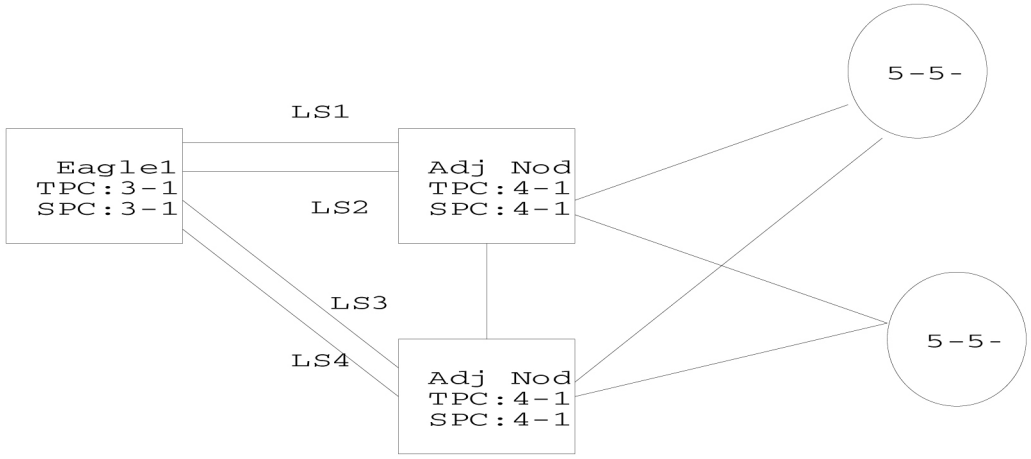


Multiple Linksets between Two Nodes

With this feature, it is possible to configure multiple linksets between two nodes, if the adjacent node also supports Multiple Point Codes. EAGLE continues to enforce the rule that each linkset must have a different adjacent point code.

One reason for provisioning multiple linksets between two nodes is to increase the number of links that can be configured between STP pairs. For example, in **Figure 4-26** , EAGLE is connected to an STP pair that supports multiple point codes. Without this feature, only 16 ITU links can be configured between EAGLE and the STP pair (8 links in LS1 and 8 links in LS2). In this example, two linksets are added, increasing the number of links to 32 (8 links in each of LS1, LS2, LS3, and LS4).

Figure 4-26. Multiple Linkset Example



In this example, the adjacent point code (APC) for LS1 is 4-1-0 and the APC for LS2 is 4-1-1. 4-1-1 is assigned an SPC of 3-1-1. So adjacent, Adj Node1 sees LS1 as having an APC of 3-1-0, and LS2 as having an APC of 3-1-1.

To load balance over these 4 linksets, half the destinations that use the STP pair can be assigned LS1 and LS3 as a combined linkset. The other half of the destinations can be assigned LS2 and LS4 as a combined linkset.

The commands to provision EAGLE1 for the above network are:

Input Examples

```
chg-sid:pc=3-1-0:
ent-spc=3-1-1
ent-dstn:dpc=4-1-0
ent-dstn:dpc=4-1-1:spc=3-1-1
ent-dstn:dpc=4-1-5
ent-dstn:dpc=4-1-6:spc=3-1-1
ent-dstn:dpc=5-5-1
ent-dstn:dpc=5-5-5
ent-ls:lsn=LS1:apc=4-1-0
ent-ls: lsn=LS2:apc=4-1-1
ent-ls: lsn=LS3:apc=4-1-5
ent-ls: lsn=LS4:apc=4-1-6
ent-rte:dpc=4-1-0:lsn=ls1:rc=10
ent-rte:dpc=4-1-1:lsn=ls2:rc=10
ent-rte:dpc=4-1-5:lsn=ls3:rc=10
ent-rte:dpc=4-1-6:lsn=ls4:rc=10
```

ent-rte:dpc=5-5-1:lsn=ls1:rc=10

ent-rte:dpc=5-5-1:lsn=ls3:rc=10

ent-rte:dpc=5-5-5:lsn=ls2:rc=10

ent-rte:dpc=5-5-5:lsn=ls4:rc=10

Impact on Other Features

Local Subsystems (LNP and Toll-Free)

EAGLE allows only the True Point Code to be entered into the MAP table. Also, EAGLE continues to allow the user to enter translations to the True Point Code. However, EAGLE does not allow the user to enter translation to a Secondary Point Code.

If a node sends a **rt-on-gt** query, the node should set the query's DPC to EAGLE's Capability Point Code. If a node sends a **rt-on-ssn** query, the node should set the query's DPC to the TSPC used by that node.

rt-on-gt Queries from a Node That Uses Secondary PC

Nodes that send **rt-on-gt** queries should use the Capability PC, regardless of whether these nodes use a True or a Secondary Point Code.

1. Node sends query with DPC=EAGLE's LSS Capability PC, CDPA is **rt-on-gt**, CGPA PC=node's PC
2. Result of translation on EAGLE is: DPC=TPC, CDPA is **rt-on-ssn**, CDPA SSN = LSS Subsystem number
3. LSS sends reply with DPC=CGPA PC, OPC = SPC, CDPA is **rt-on-ssn**

In this case, if the Local Subsystem on EAGLE fails or is taken offline, EAGLE sends a response method TFP:

TFP with DPC = node's PC, OPC = SPC, Concerned PC = EAGLE's Capability PC

This TFP causes the node to divert traffic to the mate.

If a node sends a **rt-on-gt** query to either EAGLE's True Point Code or a Secondary Point Code, EAGLE cannot divert traffic to the mate. In this case, EAGLE does not send a TFP concerning the Secondary Point Code or the True Point Code, so the node will not divert traffic to the mate.

rt-on-ssn queries from a Node That Uses Secondary PC

It is possible that nodes using a Secondary PC will send **rt-on-ssn** queries. In this case, these nodes should send the queries to the Secondary Point Code. EAGLE will accept **rt-on-ssn** queries from these nodes if the DPC is the TPC or an SPC. However, SCCP Management will not work correctly if the **rt-on-ssn** queries do not use TSPC associated with the sending node.

1. Nodes send query with DPC=SPC, CDPA is **rt-on-ssn**, CDPA SSN = CDPA, SSN = LSS Subsystem number, CGPA PC=node's PC
2. LSS sends reply with DPC=CGPA PC, OPC = SPC, CDPA is **rt-on-ssn**, CGPA PC = SPC

In this case, if the Local Subsystem on EAGLE fails or is taken offline, EAGLE broadcasts an SSP (assuming that the node is in the Concerned Point Code group):

SSP with DPC = node's PC, OPC = SPC, Affected PC = SPC, Affected SSN = LSS Subsystem number

Measurements

EAGLE pegs the following ANSI measurements for messages received from or destined for a different network:

- MSURCVNA
- OCTRCVNA
- ORIGNET_30_ SCCP_GTTUNTT
- ORIGNET_30_ SCCP_GTTUNADDR
- ORIGNET_30_ SCCP_GTTPFDPC
- ORIGNET_30_ SCCP_GTTPFDIC

For this feature it is likely, but not required, that the True ANSI point code and the ANSI Secondary Point codes will be in the same network. If they are in different networks, EAGLE uses only the network of the True ANSI point code to determine EAGLE's network.

For example, assume that EAGLE's True ANSI point code belongs to network A, and a Secondary point code is entered that belongs to network B. If a message arrives destined for point code in Network B (other than EAGLE's SPC), EAGLE treats that message as if it were destined for a different network.

Gateway Screening

The use of the Multiple Point Code feature requires a customer who is also using the gateway screening feature to add provisioning rules to recognize the new site id point code provided by the MPC feature. Failure to add the appropriate rules could result in inappropriately blocked messages.

Provisioning Multiple Point Codes

To use this feature, the user must perform some extra steps when provisioning the EAGLE:

- Provision each Secondary Point Code using the **ent-spc** command.
- Provision a route to each of the mate's Secondary Point Codes.
- For each destination that uses a Secondary Point Code, enter the Secondary Point Code using the **ent-dstn** or **chg-dstn** command.

Upgrade Considerations

The upgrade of fielded EAGLE software takes into account the changes introduced by Multiple Point Codes and no degradation of system capability will occur as a result of performing the system upgrade.

Any Table Creation Utility (TCU) support needed to transfer information from the single Site Id table to the planned use of a combined Site Id Table and Secondary Point Code table form will be provided.

The MPC Feature Bit will be initialized to OFF.

Limitations

1. The same adjacent point code cannot be used for two different links.

2. Local EAGLE subsystems (e.g. LNP) must use the True Point Code.

Multiple Routing Contexts (Release 34.0)

Description

EAGLE 5 ISS RELEASE 34.0 supports Multiple Routing Contexts for M3UA and SUA protocols.

In the M3UA and SUA protocols, there is a Routing Context parameter that can be used by the application to distinguish between traffic associated with different Application Servers (ASs).

In the original EAGLE 5 SAS implementation, an Application Server Process (ASP) could be assigned to only a single AS. A single AS could be associated with any number of routing keys if the routing keys do not contain a Routing Context. A single AS could be associated with up to 4 Routing Keys if the routing keys contain a Routing Context. However, the traffic state (ASP-Active/ASP-Inactive) for the ASPs within an AS could not be independently controlled using the individual Routing Contexts. This effectively restricts the traffic on each SCTP association to 4 Routing Contexts that must all transition their traffic state in unison. If traffic to the same far end has different Routing Context values, the original EAGLE 5 SAS design requires multiple SCTP associations to the far end in order to support independent control of the traffic state using the Routing Context.

This feature enhances the original EAGLE 5 SAS Routing Context implementation to allow more than one Routing Context to be assigned to a single M3UA/SUA SCTP association, while supporting independent control of the traffic state using the Routing Contexts. The traffic state (ASP-Active / ASP-Inactive) can be modified for one Routing Context independently of any other Routing Context.

The following changes to EAGLE 5 SAS IP functions have been made in conjunction with the Multiple Routing Contexts implementation:

- This feature removes the ASP entity from M3UA and SUA configuration. Although the configuration of ASPs is being removed from the EAGLE 5 SAS for this feature, the ASP entity still exists in the M3UA and SUA architecture. The ASP states (ASP-Down, ASP-Inactive, and ASP-Active) are still used in the EAGLE 5 SAS when reporting the management and traffic handling states of each Association/AS combination within the EAGLE 5 SAS.

The **rept-stat-as** command can be used to retrieve association ASP states and ASP-IDs per AS or per association. The **asplog** pass-through command is renamed to **ualog,** and the log entries are enhanced to include a routing context indication for all applicable log entries. The ASPNAME parameter in the **ent-as**, **dlt-as**, **rtrv-as** and **ualog** commands has been changed to the ANAME parameter.

- With the removal of the ASP entity in configuration, the feature allows an M3UA/SUA association to be assigned to more than one Application Server (AS).

  Each time an association is assigned to an AS, it requires that the IPGWx card which hosts the Association maintain a unique adapter state for the association-AS combination. Each time a TALI socket is entered, it requires that the IPGWx card which hosts the socket maintain an adapter state for the TALI socket. This feature requires that the total number of adapter states maintained by a single IPGWx card is less than or equal to 50. On a given IPGWx card, the total number of all association-to-AS assignments and

TALI connections cannot exceed 50. This total number could be reached by assigning a single association to up to 50 Application Servers.

- To ensure that it is not possible for an M3UA or SUA connection to be in the ASP-Active state without a routing key, the last routing key containing a given AS may not be deleted unless all associations in the AS are set to OPEN=NO.

- Prior to this feature, many of the IP database tables reference other IP database tables using name strings. In many cases, the name strings are not resolved to existing IP database entries at the time of provisioning. For example, a routing key can be successfully entered with an Application Server Name that does not exist in the AS table. As another example, it is possible to have a connection with an LHOST that cannot be resolved to a card because the matching IPHOST entry does not have a corresponding IPLNK entry. In this case the card location for the association cannot be determined. This lack of IP database cross-checking at provisioning time provides flexibility in command order and eases re-mapping of IP database entries, but it creates complexity and allows provisioning errors to go unnoticed.

  This feature modifies the IP database provisioning rules to require a strict order of entry and deletion in order to prevent unresolved references. The IP database tables must be provisioned in the following order:

NOTE: In previous releases, the IPHOST table was required to be provisioned before the IPLNK table for a given IP address. This feature reverses the required order.

1. Provision the card (**ent-card** command)

2. Provision the IPLNK entry with the card's IP address(es) (**chg-ip-lnk** command).

3. Provision the IPHOST entry with the card's IP address and host name (**ent-ip-host** command).* IPHOST entries for local hosts (IP cards in this EAGLE 5 SAS) will be designated as "local" in the ent-ip-host command and must exist in the IPLNK table. If the entry is not specifically designated as local or remote, it defaults to "local". Attempts to enter IPHOST entries as "remote" are rejected if the corresponding IP address exists in the IPLNK table.

4. Provision the Association/Socket connections (**ent-assoc** command and **ent-appl-sock** command). The LHOST parameter is now mandatory for these commands. The LHOST and ALHOST of the connection must exist and must be provisioned as "local" in the IPHOST table. The RHOST of the connection is not required to be provisioned in the IPHOST table. If the RHOST of the connection is provisioned in the IPHOST table, it is not required to be provisioned as "remote".

5. Provision the Application Server (**ent-as** command). Each association that is added to the AS must exist.

6. Provision the routing key (**ent-appl-rtkey** command). For M3UA/SUA, the AS being entered into the routing key must exist. For TALI, each socket entered into the routing key must exist.

   Deleting of configuration entities that are referenced by other configuration entities is required before the referencing configuration entities can be modified or deleted (don't break the chain).

- Before the IP address or hostname assigned to an IP card's Ethernet interface can be changed, all connections referencing the hostname must be closed, removed from any Application Servers and/or routing keys that they are assigned to, and deleted or temporarily modified to reference another valid LHOST/ALHOST. This requires entry of more commands than in previous releases, but it does not present any new out-of-service conditions because the card has always been required to be inhibited prior to modifying its IP address(es).

- The AS recovery timer has been relocated from the UAPS Timer 1 in the UAPS table to the AS table. Because with this feature a single association can now exist in more than one AS, the **chg-as** command is now used

to modify the AS recovery timer (instead of the **chg-uaps** command). The timer units are in milliseconds, and the valid range is 10-2000 ms.

- This feature modifies the existing reporting of primary service state (PST) and secondary service state (SST) for all SCTP associations. This change in PST function for SCTP associations results in a change in the meaning of the "IP Connection" alarms for SCTP (M3UA/SUA/M2PA) associations only. TALI socket IP Connection alarms remain unchanged.

- This feature removes support for M3UA/SUA connections on IPLIMx cards. All M3UA deployments must use IPGWx cards only. An EAGLE 5 SAS containing M3UA IPLIMx links cannot be upgraded to this release. The EAGLE 5 SAS Health Check procedure has been updated to detect this condition.

The following changes have also been made for IPGWx functions:

- M3UA/SUA connections must be assigned to an Application Server (AS) and the AS must have at least one routing key assigned to transition to ASP-Active state.

- Validation that the ASP-ID received in an ASP-UP message is unique across connections within the AS will be removed (this removes Strict/Relaxed ASP-ID validation); as a result, the UAPS Parm 3 becomes undefined.

- The **chg-appl-rtkey** command no longer has the capability to override the current AS in a routing key to another AS; or the current set of sockets in a routing key to a single socket. This prevents an M3UA or SUA association from being brought into service (ASP-ACTIVE) without having an assigned AS and routing key. The NSNAME and NASNAME parameters are no longer valid for the **chg-appl-rtkey** command. The equivalent function can be accomplished using the **dlt-appl-rtkey** and **ent-appl-rtkey** commands.

Hardware Requirements

No new hardware is required for this feature.

Limitations

Currently there is no maintenance action at the EAGLE 5 SAS to prohibit or allow an association's traffic state for a specific AS. For this reason, an association that is to be added to or removed from an AS must be set to OPEN=NO, preventing it from carrying traffic in any other AS during these provisioning activities. The OPEN=NO state ensures that there are other associations in the ASs being modified that can carry the traffic during the provisioning activities.

Multi-Port LIM (Release 27.1) (IP^7 Release 6.0)

Description

The Multi-Port LIM feature improves the functionality of SS7 routing within EAGLE by increasing the number of SS7 links the EAGLE handles per LIM card. This will allow the EAGLE to interact in larger SS7 networks, and reduces the footprint of an EAGLE (i.e. previously 250 cards would have been required to support 500 links; now only 63 cards are required).

The Multi-Port LIM feature has been engineered to satisfy the following requirements:

- Increase link capacity while reducing footprint
- Increase the number of ports on a LIM card from the current 2 to 8.
- Support the complement of low speed links with any combination of 2-port and multi-port LIMs.
- Allow easy transition to higher capacity LIM cards.
- Support alarms for higher-capacity LIM cards, and a larger number of links.

No new measurements are defined in this feature.

The Multi-Port LIM card supports all the card functionality and table capacity currently available (as of Release 26.1) for the 2-port LIM DS0-A card.

The Multi-Port LIM card can replace a 2-port LIM DS0-A within the same slot.

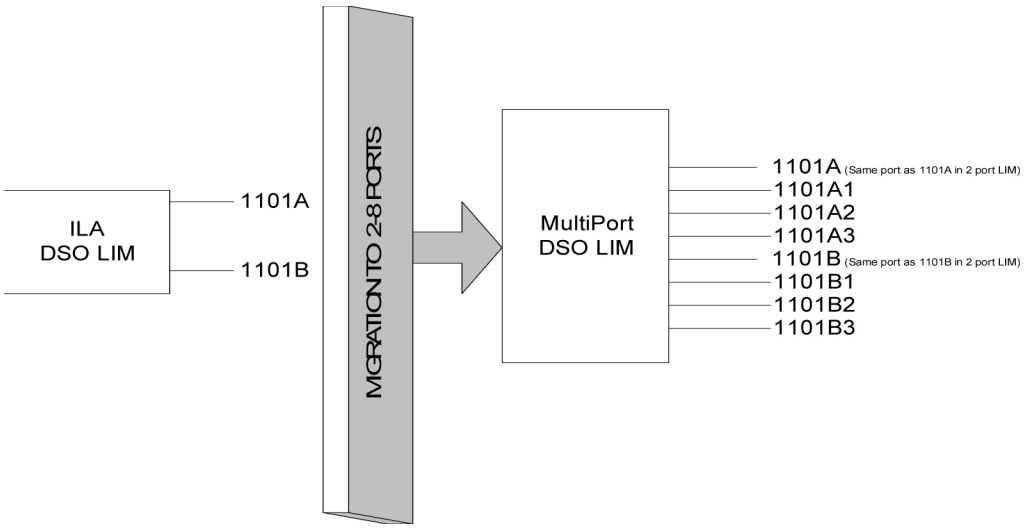
Table 4-23. Multi-Port LIM/2-Port LIM Provisioning Matrix

Provisioned Ports (56 kps)	LIM Type	System Response
A-B	2-port	Accept card
A-B	Multi-port	Accept card
A1-B3	2-port	Reject card
A1-B3	Multi-port	Accept card

A 2-port DS0-A LIM can replace a Multi-Port LIM, depending on the number of ports provisioned.

The Multi-Port LIM provides mapping of ports according to the diagram in the following figure.

Figure 4-27. Multi-Port LIM to 2-Port LIM Relationship



The provisioning of additional ports is not limited to a particular pattern. For example, customers can provision six ports with the following link identifiers:

1st Port-1101A	1st Port-1101A3
2nd Port-1101B	2nd Port-1101B
3rd Port-1101A1	3rd Port-1101A1
4th Port-1101B1	*OR* 4th Port-1101A2
5th Port-1101A2	5th Port-1101B2
6th Port-1101B2	6th Port-1101B3

Hardware Requirements

To support the increased data content in scheduled reports, terminal pacing must be increased, which requires a 19.2K baud terminal dedicated to output class TRAFFIC. For systems exceeding 350 links, a printer is not recommended.

For the Multi-Port LIM card, no new hardware other than the new MPL card (870-2061-01) itself is needed to support more than 8 ports.

Upgrade Considerations

Measurements data are not preserved from a prior release to the upgrade release during an upgrade. If the customer desires to retain a record of pre-upgrade measurements, a hardcopy of the measurements data can be obtained using the documented measurement report procedures. Alternatively, measurements data can be copied to a Measurements removable cartridge, using the **copy-meas** command. The data is then available for offline (non-EAGLE) processing. Measurements data cannot be restored to the upgraded EAGLE, due to potential changes in data formats as a result of the upgrade.

National Spare Network Indicator Support (Release 22.2)

The National Spare Network Indicator feature enables the EAGLE to support the National Spare value for Network Indicator for both ANSI and ITU-National (ITU-N) links. The National Spare Network Indicator feature is either enabled or disabled for each linkset, where the disabled state is the default condition.

Enabled States

When the National Spare Network Indicator feature is enabled for an ANSI linkset, the incoming message, National (10) or National Spare (11), is read and the outgoing message is forced to National Spare (11).

When the National Spare Network Indicator feature is enabled for an ITU-N linkset, the incoming message of International (00), National (10), or National Spare (11) is read, and the outgoing message is forced to National Spare (11).

Disabled States

When the National Spare Network Indicator feature is disabled for an ANSI linkset, the EAGLE can accept only National network indicator (10) and the outgoing message is National (10).

When the National Spare Network Indicator feature is disabled for an ITU-N linkset, the EAGLE can accept International network indicator (00) or National (10), and the outgoing message is National (10).

Gateway STP Impact

The National Spare Network Indicator impacts ANSI to ITU-National and ITU-National to ANSI message conversions when the EAGLE is configured as a Gateway STP. When enabled, the National Spare Network Indicator feature takes priority over those message conversions.

National Spare Network Indicator Support (Release 24.0)

The National Spare Network Indicator feature enables the EAGLE to support the National Spare value for Network Indicator for both ANSI and ITU-National (ITU-N) links. The National Spare Network Indicator feature is either enabled or disabled for each linkset, where the disabled state is the default condition.

Enabled States

When the National Spare Network Indicator feature is enabled for an ANSI linkset, the incoming message, National (10) or National Spare (11), is read and the outgoing message is forced to National Spare (11).

When the National Spare Network Indicator feature is enabled for an ITU-N linkset, the incoming message of International (00), National (10), or National Spare (11) is read, and the outgoing message is forced to National Spare (11).

Disabled States

When the National Spare Network Indicator feature is disabled for an ANSI linkset, the EAGLE can accept only National network indicator (10) and the outgoing message is National (10).

When the National Spare Network Indicator feature is disabled for an ITU-N linkset, the EAGLE can accept International network indicator (00) or National (10), and the outgoing message is National (10).

Gateway STP Impact

The National Spare Network Indicator impacts ANSI to ITU-National and ITU-National to ANSI message conversions when the EAGLE is configured as a Gateway STP. When enabled, the National Spare Network Indicator feature takes priority over those message conversions. The network indicator of the MSU will be the National Spare network indicator, no matter what other network indicator conversion rules are enabled for the EAGLE.

NEBS Compliance (Release 20.0)

The EAGLE will comply with the requirements of Bellcore's TR-NWT-000063, Network Equipment-Building System (NEBS) Generic Equipment Requirements. This document lists the generic requirements for all new telecommunications equipment systems used in central offices and other telephone buildings of a typical Bellcore Compliant Company. These requirements include:

- Spatial Requirements - vertical and horizontal space allocations within central offices for equipment frames, overhead cabling, lights, and air distribution elements.
- Environmental requirements for all new central office equipment systems including the cable distribution systems, distributing and interconnecting frames, power equipment, operations systems, and cable entrance facilities, and the methods for testing the equipment to determine if it meets the environmental requirements.

There have been no electrical or software changes made to the EAGLE for NEBS compliance. The following hardware changes have been made:

- The rear panel support brackets have now been completely welded to the frame instead of tack welded.
- The door closing mechanism is now threaded instead of notched.
- There have been minor changes made to the shelves to strengthen them.
- The end panels are now attached to the bottom of the frames with screws.

Nested Cluster Routing (Release 26.0)

Description

Nested Cluster Routing removes the restriction of having the full point code route on the same route as the cluster route. The EAGLE supports up to 500 nested cluster routes with full Network management functionality. A nested cluster route counts as 1 route entry in the route table, and does not otherwise affect the capacity of the route or xlist table.

Nested Clusters and Cluster Members

The cluster routing and management available in prior release of EAGLE software required cluster and cluster members to have same route set. With the Nested Cluster feature, however, users can have certain members of the provisioned cluster with different FPC route set. This different route set may be totally different, partially different, or exactly the same.

With the Nested Cluster Routing feature, routes to these members can be changed, deleted, or added. Deletion of a FPC route entry within a cluster will result in the member using the cluster entry for routing. Deletion of a cluster route entry will not delete the FPC route entry. This holds true even if the FPC entry and the cluster have the same route.

The EAGLE send cluster network management messages (TCA, TCR, TCP) based on the least restrictive of the cluster's route set status, and the route set status of any FPC entries within the cluster.

The Nested Cluster Routing feature provides a new routing model. (The EAGLE allows several routing models.) The table describes coupling between the cluster and its members. Coupling describes the relationship between the cluster and member route statuses.

Table 4-24. EAGLE Routing Models

EAGLE Routing Model	Characteristics	Issues and Resolution	Release
Full Point Code Routing (FPR) No coupling	EAGLE will behave as a FPC router when CRMD feature bit is OFF. Only FPC destinations are provisioned. EAGLE will never generate TCX messages concerning clusters of provisioned members. Received TCX messages are applied to all members of the concerned cluster.	No issues. There is not coupling between cluster status and member statuses due to the lack of clusters.	Rel 21
Cluster Routing (CR) No coupling NCAI=No	With CRMD feature bit ON, EAGLE will allow provisioning of cluster destinations. For cluster destinations, only cluster entries are provisioned. EAGLE will generate TCX messages only for provisioned cluster destinations. All received TCX messages are applied to concerned cluster entry if it exists. Otherwise it is applied to all individual members.	No issues. There is no coupling between cluster status and member status's due to the lack of members belonging to provisioned cluster.	Rel 21
Cluster Routing and Management Diversity (CRMD) Full coupling NCAI=No	In this mode, EAGLE allows provisioning of clusters as well as members of same clusters. Here cluster and member have the same route set, and they are fully coupled. All TCX messages are applied to members and TCX messages generated by EAGLE reflect member status. In this mode, member status cannot be less restrictive than cluster.	No issues regarding network management message generation and processing. Cluster and members cannot have a different route set, and thus E-links cannot be provisioned for member of a cluster.	Rel 21
Nested Cluster Routing No coupling NCAI=Yes	In this mode, if the **ncai** parameter is **yes** (provided both the feature NCR and the feature CRMD are ON), the user can enter a cluster route set, then enter a different route set for a member of that cluster. In this case, member route set status can be less restricted than cluster route set status.	There is an issue regarding broadcasting network management messages. Because members can be less restricted than the Cluster, broadcast of cluster messages (TCA, TCR, TCP) is based on the least restrictive of the following: The cluster's route set status The route set status of any full point code entries within the cluster	Rel 26

EAGLE Routing Model	Characteristics	Issues and Resolution	Release
		Also, when **ncai=yes**, EAGLE will not generate preventive TCPs.	

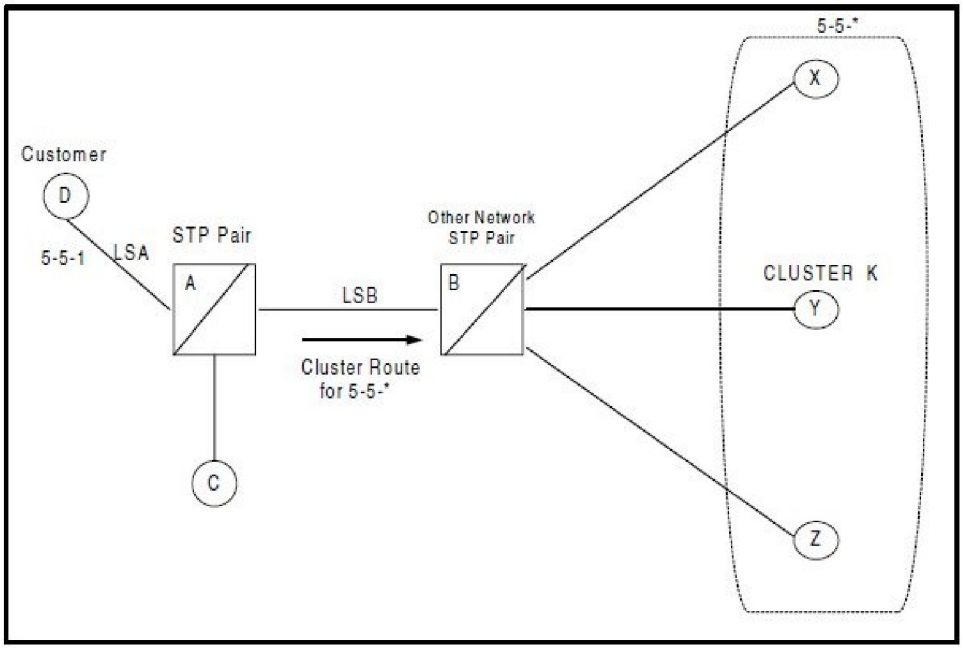
Administration

Nested Cluster Routing (NCR) is administered as a new feature in the EAGLE's database. In order to specify the **ncai** parameter (yes, no), both the CRMD feature and the NCR feature must be ON. If **ncai** is **yes**, EAGLE allows certain members of the provisioned cluster to have different full point code route set.

If the **ncai** parameter is **no**, standard command handler rules apply (any full point code route set within a cluster must have the same route set as the cluster). If **ncai** parameter is specified as **yes**, new command handler rules apply (full point code route set can be different from the cluster route set). Following is an example of provisioning a nested cluster and associated member.

1. Turn CRMD feature on: **chg-feat:CRMD=ON**
2. Turn NCR feature on: **chg-feat:NCR=ON**
3. Enter nested cluster destination: **ent-dstn:dpc=5-5-* NCAI=yes**
4. Enter routes for nested cluster routing: Enter nested cluster's member X destination: **ent-dstn:dpc=5-5-1**
5. Enter route for associated member X: **ent-rte:dpc=5-5-1:lsn=lsA:rc=10**

Figure 4-28. Cluster Network Configuration



In the figure, cluster route 5-5-* exists from STP-A to STP-B. A member in that cluster, SSP-D, is directly connected to STP-A. If SSP-C is signaling to any member other that 5-5-1, it follows the cluster route to STP-B. The nested feature is used in STP-A.

General Requirements

Circular Routing

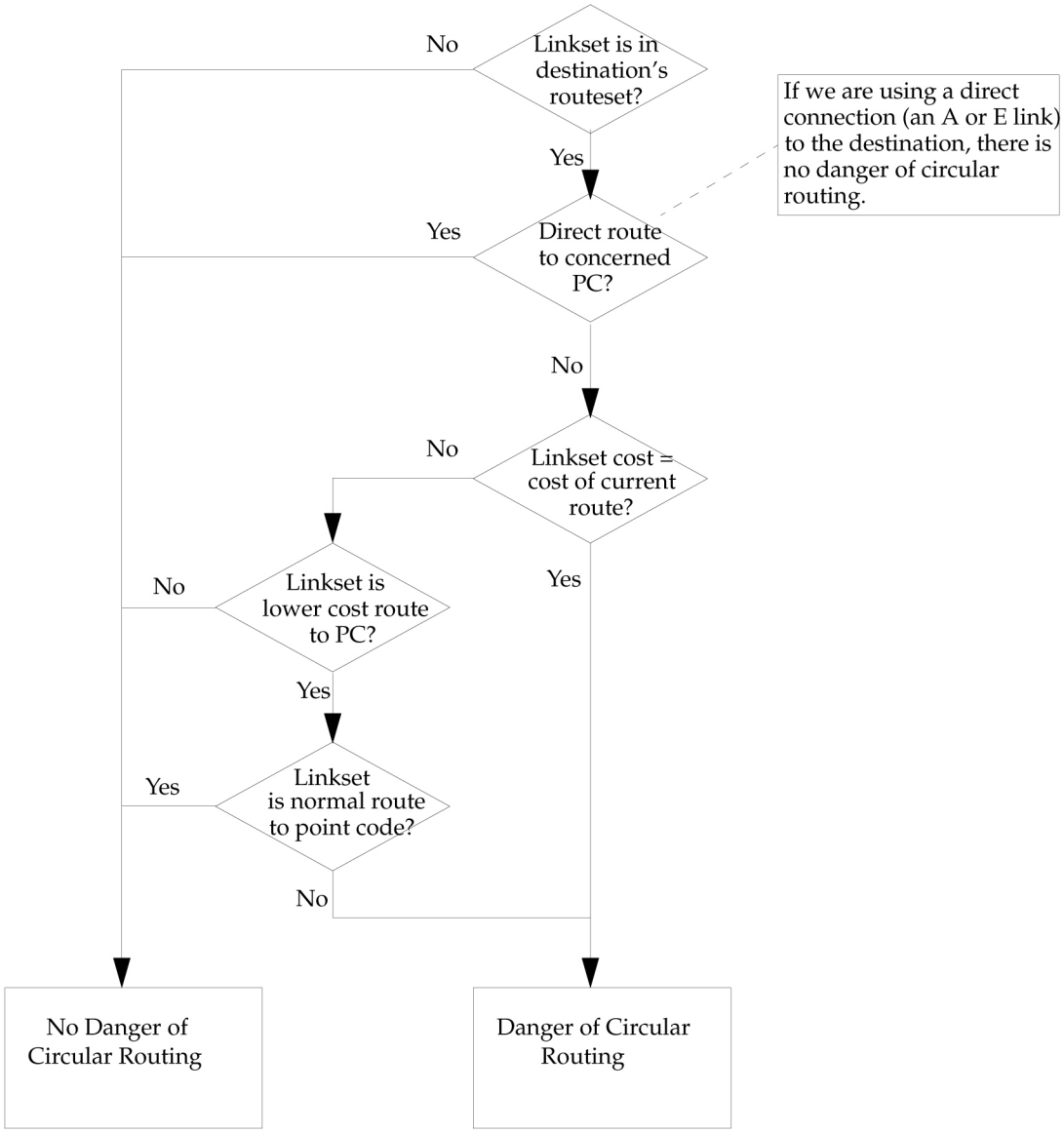
Danger of Circular Routing

Danger of circular routing means that if EAGLE receives an MSU on a linkset and then routes that MSU, circular routing may occur. In these cases, EAGLE normally sends preventive TFPs on these linksets.

This feature does not change the rules for determining if danger of circular routing exists for a destination and linkset. These rules are:

- Danger of Circular Routing only occurs on linksets that are part of the routeset for the destination
- Danger of Circular Routing only occurs if routing over an STP to a destination.
- If the linkset is a Higher cost route than the current route to the destination, there is no danger of circular routing.
- If the linkset is equal cost route as the current route to the destination, there is danger of circular routing.
- If the linkset is lower cost route than the current route to the destination, and the linkset is the least cost route, there is no danger of circular routing.

Figure 4-29. Determining If Danger of Circular Routing Exists



Nested Cluster Routing Rules of Operations

The following rules apply to nested clusters (cluster entries with NCAI set to YES):

1. EAGLE will allow the user to enter a full point code route set entry even if the point code is a member of a cluster that has a different route set.

2. When EAGLE performs broadcast, EAGLE will use the least restricted of the following to determine which cluster message (TCA, TCR, TCP) to send:

    - The Cluster's route set status

- The route set status of any full point code entries within the cluster

3. Response method TFP or TFR will be used when the cluster destination is more restrictive than a FPC member. The modified TFP response method will send no more than one TFP per cluster member per T8 timer. The modified TFR response method sends no more than one response TFR per cluster member.

4. EAGLE will not send preventive TCPs when it begins routing towards a nested cluster. EAGLE will, however, send response method preventive TFPs if it receives an MSU when there is danger of circular routing

   (Note that it will still send preventive TFPs when it starts routing towards a FPC member of a nested cluster.)

5. EAGLE will reply to RCX cluster route set test messages using the less restrictive route set status, as indicated in rule #2.

6. EAGLE will reply to RSX full point code route set messages using the full point code's route set status and danger of circular routing.

Received TFX /TCX Message Processing

For this feature, there is no change to received TCx message processing (although a change is required deciding whether to broadcast TCX messages), and there is only one change to received TFx message processing.

A TFX message received for a FPC member will be applied to the FPC member only. However, receiving a TFX message for a member of a nested cluster may cause EAGLE to broadcast a cluster message. This is a change from the way cluster routing currently works.

If EAGLE then receives a TFP from STP E concerning 5-5-5, EAGLE will apply that TFP to 5-5-5. Because all members of the cluster 5-5-* are at least Restricted, EAGLE will broadcast a TCR concerning 5-5-*. EAGLE will also begin routing traffic to 5-5-5 over LSC.

Broadcasting TCR (for nested cluster) will override the status of previously TFPs sent (for cluster members). However when traffic resumes and the conditions persists (MSU received and there is a danger of circular routing), EAGLE will again send response method TFPs for the affected cluster members.

EAGLE will still perform the following check for invalid TFx messages: If EAGLE receives a TFx message that is less restricted than the status of the route for the cluster, EAGLE will discard the TFx and generate a UIM (UIM #1147 for TFA, and UIM#1148 for TFR).

Generating TFX Messages

In regard to generating TFX messages, FPC members are considered individual full point code. Broadcast TFX messages, Preventive TFPs and back-routing TFRs are generated based on route set status and danger of circular routing. For example, in Figure 4-27 , when LSE is down, EAGLE will broadcast TFR(X) because alternate route LSB is still available. When LSE becomes available, EAGLE will broadcast TFA(X).

If we have already sent a TCP (transfer cluster prohibited), we do not send a TFP (transfer prohibited for cluster members).

For full point code (FPC) members, a TFX condition is first broadcast and then sent in response method. If the FPC member's route set status is restricted, a TFR is broadcast after T11, then a one time response method TFR is sent after T18.

Generating TCX Messages

EAGLE will generate TCX messages based on the least restricted of the following (see rule #2):

- The Cluster route set status
- The route set status of any FPC entries within the cluster

For example, in Figure 4-27 , if the status of the cluster K route set changed from allowed to prohibited and the member D FPC route set status is allowed, STP-A will generate TCA message based on the least restricted route set status.

If all of the members in a nested cluster have the same route set status, then response method TCX messages will be sent after the broadcast.

If a TCX condition does not change but a TFX condition does, the TCX condition is not broadcast again. But if the TCX condition does change, then we do broadcast the new TCX condition.

The EAGLE will only broadcast TCX messages when the nested cluster's route set status changes. TCR broadcast for nested clusters should take place after the expiration of T11.

Generating RSX/RCX Messages

Generating RSX messages

Generating RSX messages will not change for the nested cluster feature.

Responding RSX/RCX Messages

Responding RCX Messages

EAGLE will not reply to RCX message when the status of the RCX message matches the status of the reply. If the RCX message is an RCR and the indicated reply is a TCR, EAGLE will not send a reply. If the RCX message is a RCP and the indicated reply is a TCP, EAGLE will not send a reply. If the **ncai** parameter is **yes**, the response to RCX messages will change.

EAGLE will reply to Route Set Cluster Test messages (RCX) using the least restrictive of the cluster's route set status and the route set status of any of the FPC entries within a cluster. The following table describes the EAGLE reply message upon reception of an RCX message.

Table 4-25. RCX Reply Message

Cluster Status	NCAI	Danger of Circular Routing for Cluster?	Status of Least Restricted member	Reply
A	N	N	A	TCA
A	N	Y	A	TCP
R	N	N	R	TCR
R	N	N	P	TCR

Cluster Status	NCAI	Danger of Circular Routing for Cluster?	Status of Least Restricted member	Reply
R	N	Y	R	TCP
R	N	Y	P	TCP
P	N	NA	P	TCP
A	Y	X	A	TCA
A	Y	X	R	TCA
A	Y	X	P	TCA
R	Y	X	A	TCA
R	Y	X	R	TCR
R	Y	X	P	TCR
P	Y	X	A	TCA
P	Y	X	R	TCR
P	Y	X	P	TCP

Y= Yes, N= No, NA= Not Applicable, X= Don't care, A= Allowed, P= Prohibited, R= Restricted

Responding RSX Messages

Whenever the NCAI parameter is set to YES and a FPC entry exists for the Concerned PC, EAGLE will reply based only on the status of the FPC and the danger of circular routing for the FPC. EAGLE will not reply to RSX message when the status of the message matches the status of the reply. If the RSX message is an RSR and the indicated reply is a TFR, EAGLE will not send a reply. If the RSX message is an RSP and the indicated reply is a TFP, EAGLE will not send a reply. The following table shows how EAGLE will reply when it receives a Route Set Test (RSX) message for a member of a cluster.

Table 4-26. RSX Reply Messages

FPC entry exists?	Cluster Status	Danger of Circular Routing for Cluster?	Status of FPC	Danger of Circular Routing for FPC?	Reply
Y	X	X	A	N	TFA
Y	X	X	A	Y	TFP
Y	X	X	R	N	TFR
Y	X	X	R	Y	TFP
Y	X	X	P	NA	TFP
N	A	N	NA	NA	TFA

FPC entry exists?	Cluster Status	Danger of Circular Routing for Cluster?	Status of FPC	Danger of Circular Routing for FPC?	Reply
N	A	Y	NA	NA	TFP
N	R	N	NA	NA	TFR
N	R	Y	NA	NA	TFP
N	P	NA	NA	NA	TFP

Y= Yes, N= No, NA= Not Applicable, X= Don't care, A= Allowed, P= Prohibited, R= Restricted

Response Method TFX

Broadcasting TFX messages for all members of a cluster that do not have a full point code entry could create a huge amount of network management messages. For example, in a customer site of 200 nested clusters, a condition in which a B-link set fails but the E-links are available could generate 255 TFPs or TFRs per cluster, resulting in over 50,000 TFPs or TFRs. The change is not to broadcast TFX messages, but to send TFX messages by response method, with changes to the way we pace response method messages.

If a cluster destination is more restricted than a full point code member, the STP will send a cluster message (TCA or TCR) for the status of the least restrictive member. The STP will then immediately allow response method transfer messages (TFP or TFR) for individual members of the cluster. The STP will limit response method TFPs to 1 TFP per individual member per T8 timer. The STP will only send 1 TFR per individual member.

Response Method TFP

Once the cluster destination is inaccessible (B-link set fails but E-links are available), EAGLE sends a (TCA or TCR) message (cluster destination is more restricted than a full point code member). The T8 timer is started after sending the first link set response method TFP. EAGLE will send a response method TFP for every member of the cluster (up to 256) that does not have a provisioned FPC route entry.

Response Method TFR

Once the cluster destination is inaccessible (B-link set fails but E-links are available), EAGLE sends a (TCA or TCR) message (cluster destination is more restricted than a full point code member). T8 timer is started after sending first link set response method TFP. EAGLE will send a response method TFP for every member of the cluster (up to 256) that does not have a provisioned FPC route entry.

Preventive TCP/TFP

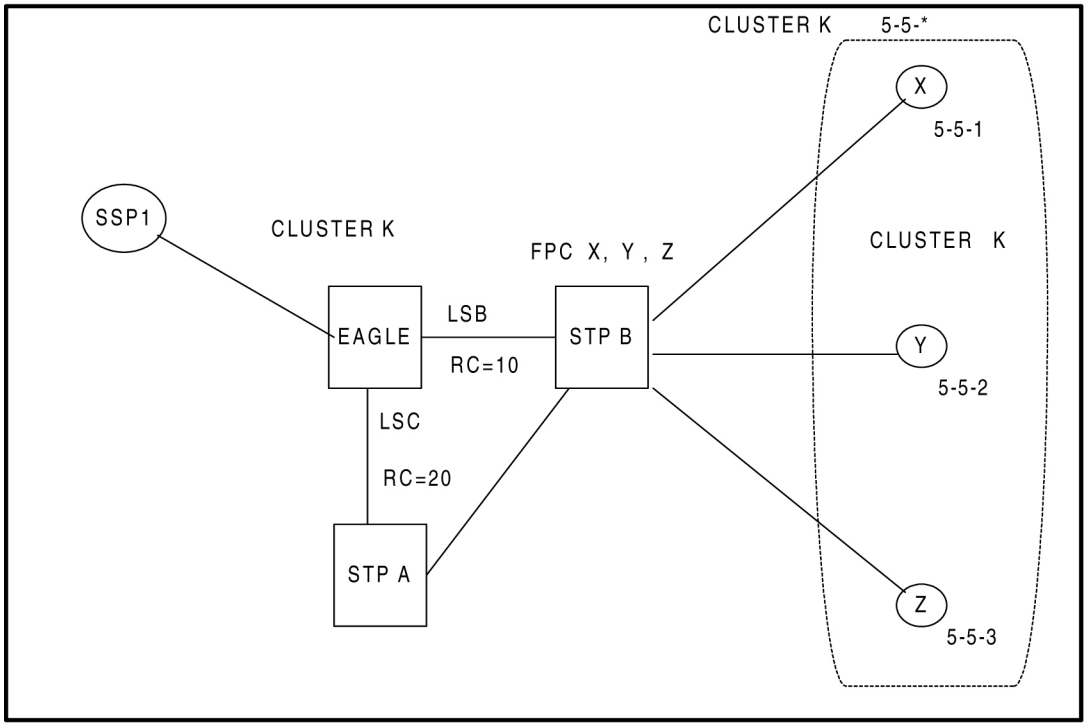
Normally, when EAGLE begins routing through an STP to a remote destination, EAGLE will send a TFP on any linkset where there is danger of circular routing. If the remote destination is a cluster entry with NCAI=NO, EAGLE will send a TCP on the linkset.

For example, in the next figure, when EAGLE begins routing over LSB to cluster K, EAGLE sends a preventive TCP concerning cluster K to STP-B and STP-C.

When **`ncai=yes`** for cluster, EAGLE will not send preventive TCPs. However, if EAGLE receives an MSU for the cluster on a linkset that has danger of circular routing, EAGLE will send a response method TFP and discard the MSU.

For example, in the next figure, when EAGLE begins routing over LSB to Cluster K, EAGLE will not send a TCP to STP-B. However, if STP-B sends EAGLE an MSU destined for 5-5-2, EAGLE will discard the MSU and send a TFP concerning 5-5-2 to STP-B. This will prevent a potential circular routing loop between STP-B, EAGLE, and STP-A.

Figure 4-30. Preventive TCP Example



Route Table for Cluster K (5-5-*) 5-5-* LSB, RC=10 5-5-* LSC, RC=20

In the next figure, if LSB and the linkset between STP-A and STP-B fail, and if **NCAI=NO** for 5-5-*, EAGLE would send a preventive TCP to STP-A before trying to route traffic for 5-5-* over LSC. (Note that with **ncai=no**, LSE cannot be provisioned.) STP-A would also send a preventive TCP to EAGLE concerning 5-5-* before trying to route traffic to 5-5-* over LSC. After receiving the preventive TCP from STP-A, EAGLE would determine that the cluster 5-5-* is prohibited.

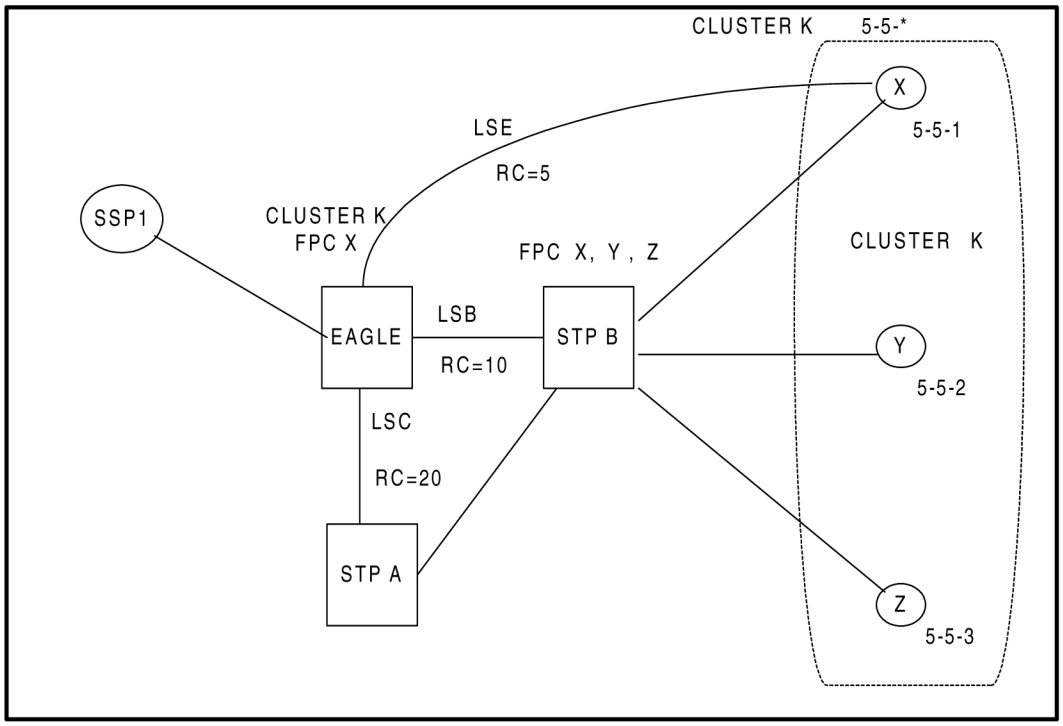
If both EAGLE and STP-A are using nested cluster routing with **ncai=yes** for 5-5-*, they will not send preventive TCPs when they start routing over the LSC. When an MSU destined for 5-5-2 arrives at STP-A, STP-A will route it over LSC.

When EAGLE receives the MSU, it will detect the danger of circular routing, and send a response method TFP. STP-A will then create an x-list for 5-5-2. When an MSU destined for 5-5-2 arrives at EAGLE, EAGLE will route it over LSC. When STP-A receives the MSU, it will detect the danger of circular routing, and send a response method TFP. EAGLE will then create an x-list for 5-5-2. This scenario is repeated for each member of 5-5-* other than 5-5-1.

Nested Cluster Routing Examples

The next figure and table provide an example of nested cluster routing.

Figure 4-31. Nested Cluster Example #1



Route Table for Nested Cluster K (5-5-*)

5-5-* LSB, RC=10

5-5-*LSC, RC=20

Route Table for FPC Member X (5-5-1)

5-5-1 LSE, RC=5

5-5-1 LSB, RC=10

5-5-1 LSC, RC=20

Table 4-27. Nested Cluster Routing Example

No	Event	Action
1	All link sets are up and all routes are available	EAGLE will not send preventive TCP(K) to STP-B because if K is a nested cluster, start routing messages to X using LSE and K using LSB. EAGLE will broadcast TCA(K) to SSP1, SSP-X, STP-B, and STP-B.
2	Link set between STP-B and SSP-Y (5-5-2) fails, STP-B sends a TFP(Y)	EAGLE will create a (5-5-2) x-list entry and mark it to PROHIBITED on LSB. EAGLE will broadcast TFP to SSP1, SSP-X and STP and sends response method TFP concerning 5-5-2 (Rule #3). EAGLE will start RSP for Y on LSB.
3	Link set between STP-B and SSP-X (5-5-1) fails, STP-B sends a TFP(X) to EAGLE.	EAGLE will mark FPC 5-5-1 to PROHIBITED on LSB, EAGLE routes the traffic to X via LSE. EAGLE will start RSP for X on LSB.

No	Event	Action
4	Link set between STP-B and SSP-Y(5-5-2) recovers and STP-B sends a TFA(Y) to EAGLE.	EAGLE will remove (5-5-2) x-list entry prohibited status on LSB, performs rerouting and start routing traffic to SSP-Y via LSB. EAGLE will broadcast TFA(Y) to SSP1, SSP-X and STP-A. EAGLE sends a preventive TFP(Y) to STP-B
5	Link set between STP-B and SSP-X (5-5-1) recovers and STP-B sends a TFA(X) to EAGLE	EAGLE will mark FPC 5-5-1 to allowed status on LSB.
6	LSB fails	EAGLE will stop using LSB to send traffic to cluster K, mark PROHIBITED on LSB, perform forced re-routing, start T11(K), and start using LSC to switch messages to K. EAGLE will mark K RESTRICTED on LSC for all members of K except FPC X. When T11 expires, send TFR response method for all members of K except FPC X.
7	SSP1 sends an MSU with DPC=Y	EAGLE will respond with TFR(Y) to SSP1. MSU will be routed on LSC.
8	SSP1 sends an MSU with DPC=X	EAGLE will route MSU to SSP-X using LSE.
9	LSB recovers	EAGLE will stop using LSC to send traffic to cluster K, performs controlling rerouting on K, and mark cluster K as ALLOWED on LSB, starts routing traffic to cluster K via LSB.
10	SSP sends a route set test (RSR) concerning Y to EAGLE	EAGLE responds with a TFA(Y).
11	LSC fails.	EAGLE will stop using LSC to send traffic to cluster K or FPC X and mark K and FPC X PROHIBITED on LSC.
12	LSC recovers.	EAGLE will mark cluster K and FPC X ALLOWED on LSC.
13	LSE fails.	EAGLE will stop using LSE to send traffic to SSP-X, marks PROHIBITED on LSE, perform forced rerouting, start T11(X), send preventive TFP(X) to STP-B and start using LSB to switch messages to FPC X. EAGLE will mark FPC X RESTRICTED on LSB. When T11 expires and broadcast TFR(X) to SSP1 and STP-A.
14	SSP1 sends an MSU with DPC=SSP-Y	EAGLE will route MSU to SSP-Y using LSB.
15	SSP1 sends an MSU with DPC=SSP-X	EAGLE will respond with a TFR(X) to SSP1. MSU will be routed to SSP-X using LSB.
16	LSE recovers.	EAGLE will stop using LSB to send traffic to SSP-X, perform controlling rerouting on FPC X and mark FPC X as ALLOWED on LSE, start routing traffic to FPC X via LSE. EAGLE broadcast TFA(X) to SSP1, STP-A, and STP-B.

Route Table for Nested Cluster K (5-5-*)

5-5-* LSB, RC=10

5-5-* LSC, RC=20

Route Table for FPC Member P (5-5-1)

5-5-1 LSE, RC=10

5-5-1 LSC, RC=20

Route Table for FPC Member Q (5-5-5)

5-5-5 LSE, RC=10

5-5-5 LSC, RC=20

Upgrade Considerations

The new software accommodates the old database during the upgrade. The new fields for the existing tables, such as the NCR bit in the feature table, defaults to 0 (OFF), and the **NCAI** parameter in the destination table defaults to 0 (NO).

Use the **rtrv-dstn** command to verify the status of the **NCAI** parameter (it should display **ncai = no** for existing cluster destinations). To activate the Nested Cluster Feature, the software release must contain the CRMD feature (non-nested cluster management).

Network Routing (Release 26.0)

Overview

Network routing allows the user to provision a single routeset that will be used for all MSUs destined to members of that network. The advantages of network routing are:

- reduces the number of entries in the route table
- allows routing to members of a network without having to add those members to the route table

An EAGLE user can connect to a remote network by provisioning a single route table element. As the remote network grows, the EAGLE user does not have to add new route table entries for each new point code in the remote network.

Types of Routing Strategies Available

EAGLE currently allows a user to provision two types of routing strategies:

- full point code routing
- network/cluster routing (also called cluster routing)

This feature allows the user to provision a third type of routing strategy:

- network routing

It is possible to provision full point code entries, cluster entries, and network entries for members of the same network. Any overlaps in the routing strategies are handled by a specific searching hierarchy.

Example

All of these route table entries can coexist:

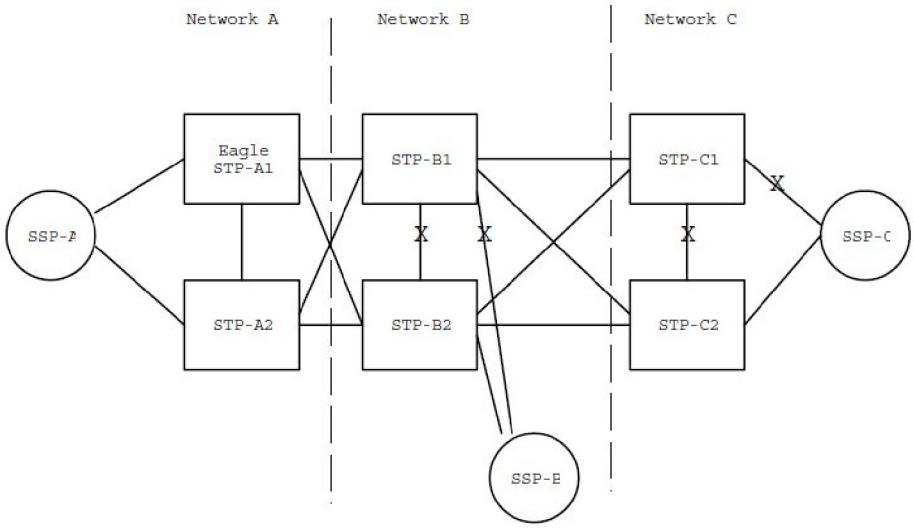
1. 8-1-1 full point code entry
2. 8-1-* cluster entry
3. 8-*-* network entry

The searching hierarchy will try to match against a full point code entry first, followed by a cluster entry, and finally a network entry. In the preceding example, when EAGLE routes an MSU destined for 8-1-1, it uses the full point code entry; when EAGLE routes an MSU destined for 8-1-2 it uses the cluster entry; and when EAGLE routes an MSU destined for 8-2-2, it uses the network entry.

Applications

Network routing is very useful when the destination node is located far from the source node. The reliability of network routing increases when the destination is further away. As shown in the following figure, routing from network A is more reliable to nodes in network C than to nodes in network B.

Figure 4-32. Example of Network Routing Reliability



If the STPs in Network A use network routing for Network C, Network A can still route traffic to SSP-C, even if two linksets fail. In this example, one of the A-linksets to SSP-C and the C-linkset between STP-C1 and STP-C2 fail. In this case, the EAGLE in Network A will continue to route half its traffic to STP-B1, and half to STP-B2. STP-B1 and STP-B2 (which do not use network routing) will route all traffic for SSP-C through STP-C2.

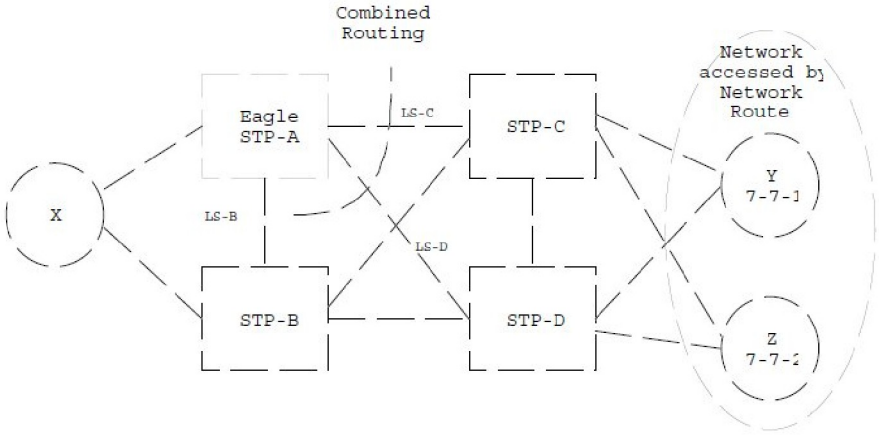
If the STPs in Network A use network routing for Network B, traffic going to SSP-B may be lost if two linksets fail. In this example, one of the A-linksets to SSP-B and the C-linkset between STP-B1 and STP-B2 fail. In this case, the EAGLE in Network A will continue to route half its traffic to STP-B1, and half to STP-B2. Traffic for SSP-B routed through STP-B1 will be discarded, resulting in message loss.

MTP Requirements

Routing

In the following discussion, refer to the following figure:

Figure 4-33. Generic Network



Route Availability

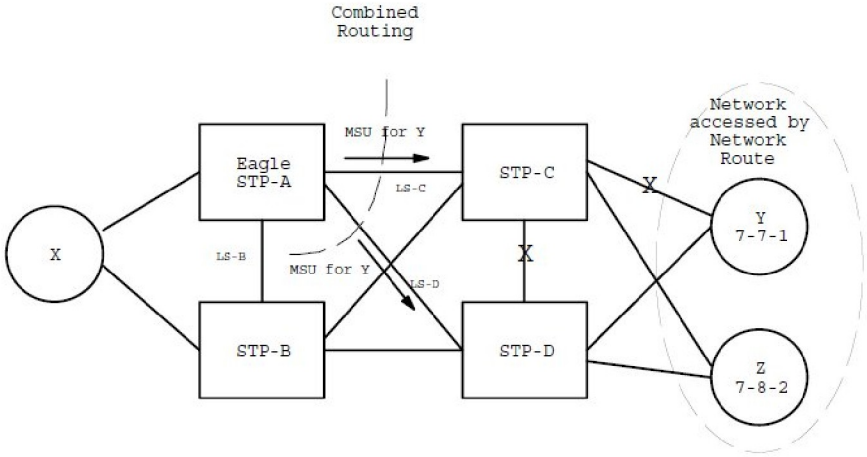
A route is one path to a destination. A routeset is a list of paths to a destination. Route availability consists of two parts:

1. local availability, and

2. remote availability

Remote availability is affected by TFx network management messages. Local availability is affected by linkset failures and recoveries. TFx messages do not affect point codes accessed by network route entries. Therefore, for network route entries, route availability consists of only local availability. The highest priority linkset available for traffic will be used for routing MSUs regardless of the remote availability of that route.

Figure 4-34. Potential Routing Network Failure



In the example in the following figure, linksets LS-C and LS-D form a combined route to network route 7-*-*. Because 7-*-* is a network route, EAGLE will always consider the non-adjacent status of the routes to be allowed. In the example shown, EAGLE routes traffic destined to 7-7-1 over LS-C and LS-D. EAGLE will ignore TFPs concerning 7-7-1 or TCPs concerning 7-7-*.

Point Code Availability

A point code that is accessed by a network route entry is considered available if there is any linkset in the routeset that is available for traffic.

Routing MSUs

MTP message routing will search the routing table up to 3 times to find a routing entry for the received MSU.

The search order is:

1. a full point code match
2. a network/cluster match
3. a network match

Route Management

Congestion

Local Link Congestion

This feature has no impact on the generation of TFC messages. A TFC will be generated concerning point code X-Y-Z, even if X-Y-Z is routed using a network route entry.

Remote Congestion

Because EAGLE has global title capabilities, it is possible that a TFC is received by EAGLE concerning a point code that is accessed by a network route entry. Network route entries will not be affected by TFC messages.

Transfer Messages (TFP, TCP, TFR, TCR, TFA, and TCA)

Broadcast Transfer Messages

EAGLE will not broadcast TFx messages for network route entries.

Response Method Transfer Messages

EAGLE will send response method TFx messages for network routes as follows:

- Prohibited Network Routes

  If EAGLE receives an MSU that is accessed by a network route entry, and that network route is prohibited, EAGLE will send a response method TFP or TCP message, as follows:

  — If there is a full point code defined in the same cluster as the MSU (e.g. 8-*-* and 8-1-1 are defined in EAGLE's routing table, and MSU is destined for 8-1-2), EAGLE will send a TFP with Concerned PC set to the MSU's DPC.

  — Otherwise, EAGLE will send a TCP with Concerned PC set to the cluster of the MSU's DPC.

  EAGLE will pace response method TCPs or TFPs sent to 1 per link per T8 per network route.

  For example, in figure Potential Routing Network Failure , the network route for 7-*-* becomes Prohibited due to the failure of LS-B, LS-C, and LS-D. When EAGLE receives an MSU from X destined for 7-7-1, EAGLE will send a response method TCP concerning 7-7-*. When EAGLE

receives an MSU from X destined for 7-8-2, EAGLE will send a response method TCP concerning 7-8-*.

- Danger of Circular Routing

  If EAGLE receives an MSU that is accessed by a network route entry, and EAGLE detects danger of circular routing (see "Circular Routing" for an explanation of danger of circular routing), EAGLE will send a response method TFP or TCP message, as follows:

  — If there is a full point code defined in the same cluster as the MSU (e.g. 8-*-* and 8-1-1 are defined in EAGLE's routing table, and MSU is destined for 8-1-2), EAGLE will send a TFP with Concerned PC set to the MSU's DPC.

  — Otherwise, EAGLE will send a TCP with Concerned PC set to the cluster of the MSU's DPC.

  EAGLE will pace response method TCPs sent to 1 TCP per link per T8 per network route.

  For example, in figure Generic Network , all linksets are available. If EAGLE receives an MSU from STP-C destined for 7-7-1, EAGLE will detect danger of circular routing, and send a response method TCP concerning 7-7-*. EAGLE will also discard the MSU.

- Restricted Network Routes

  If EAGLE receives an MSU that is accessed by a network route entry, and that network route is Restricted, EAGLE will send a one time response method TFR or TCR message, as follows:

  — If there is a full point code defined in the same cluster as the MSU (e.g. 8-*-* and 8-1-1 are defined in EAGLE's routing table, and MSU is destined for 8-1-2), EAGLE will send a TFR with Concerned PC set to the MSU's DPC.

  — Otherwise, EAGLE will send a TCR with Concerned PC set to the cluster of the MSU's DPC.

  For example, in the following figure, the network route for 7-*-* becomes Restricted due to the failure of LS-C, and LS-D. When EAGLE receives an MSU from X destined for 7-7-1, EAGLE will send a response method TCR concerning 7-7-*, then route the MSU over LS-B. When EAGLE next receives an MSU from X destined for 7-8-2, EAGLE will not respond, and will route the MSU over LS-B.

Reception of Transfer Messages

EAGLE will not apply received Transfer messages to a network route.

For example, in the following figure, if EAGLE receives a TFP concerning 7-7-1, it will have no effect on the routing status of 7-*-*. EAGLE will continue to send MSUs destined to 7-*-*, including MSUs destined to 7-7-1, on LS-C.

As another example, if EAGLE receives a TCP concerning 7-8-*, it will have no effect on the routing status of 7-*-*. EAGLE will continue to send MSUs destined to 7-*-*, including MSUs destined to 7-8-2, on LS-C.

Route Set Test

The MTP routeset test application will be able to handle the reception of full point code RSx and cluster RCx messages that apply to network route entries.

Reception of an RSx Message

If a route set test (RSP or RSR) is received, a full point code reply (TFx) is generated.

The responses to RSP/RSR will be modified according to the following table .

Note that the searching hierarchy applies.

Table 4-28. Reception of an RSx Message

Concerned point code is:	Result
Found by a full point code match	No change to existing rules.
Found by a cluster match	No change to existing rules.
Found by a network match	Send a TFx message based on the current routeset status. • Send a TFP if danger of circular routing. Otherwise: • Send a TFA if network route is Allowed • Send a TFR if network route is Restricted. • Send a TFP if network route is Prohibited.
Not found	No change to existing rules. Send a TFP.

Reception of an RCx Message

If a routeset cluster test (RCP or RCR) is received, a cluster reply (TCx) is generated. The responses to RCP/ RCR will be modified according to the following table. Note that the searching hierarchy applies.

Table 4-29. Reception of an RCx Message

Concerned point code is:	Result
Found by a cluster match	No change to existing rules.
Found by a network match	Send a TCx message based on the current routeset status. • Send a TCP if danger of circular routing. Otherwise: • Send a TCA if network route is Allowed • Send a TCR if network route is Restricted • Send a TCP if network route is Prohibited.
Not found	No change to existing rules. Send a TCP.

Network Security Enhancements (Release 29.0)

Overview

The Network Security Enhancements feature enhances the EAGLE's network security by discarding messages that should not be received by the EAGLE. This feature is designed to allow maximum flexibility to the user, so that different network implementations can still use the applicable functionalities provided by this feature.

This feature is controlled by a centralized feature key and has four different STP command options to control activation of the three major aspects of this feature:

- MTP message SID verification (Enhanced MTP Security)

— *Option #1*: Mate SID verification - SECMTPMATE

— *Option #2*: Self SID verification - SECMTPSID

- *Option #3*: MTP Network management message OPC verification (Enhanced MTP Management Protection) - SECMTPSNM
- *Option #4*: SCMG AFTPC verification (Enhanced SCCP Management Protection) - SECSCCPSCMG

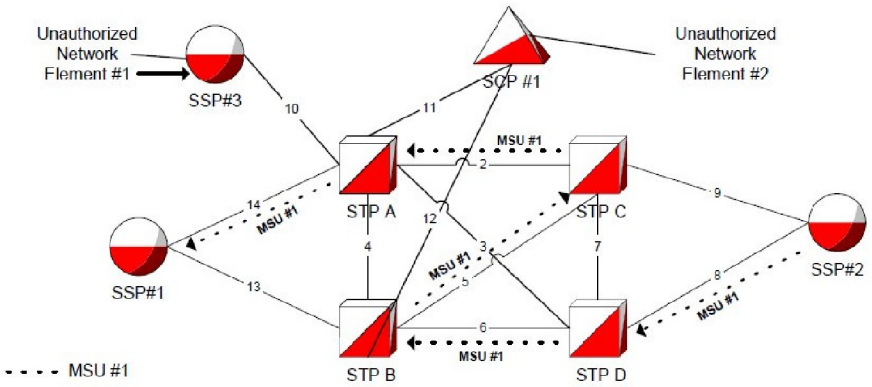
The four STP options can be turned on/off independently (see below).

NOTE: This feature is independent of Gateway Screening and is performed before Gateway Screening occurs on the MSU.

MTP Message OPC Verification (SECMTPSID & SECMTPMATE)

The basic concept behind the SECMTPSID option is that for most cases, the EAGLE should not receive a message where the OPC is equal to the EAGLE's own True, Secondary or Capability Point Code(s). The basic concept behind the SECMTPMATE option is that the EAGLE should not receive a message with the True, Secondary, or Capability Point Code of the Mate STP other than across the C link. See the following figure.

Figure 4-35. SECMTPMATE Option Diagram



SECMTPMATE Option

An example of the SECMTPMATE option is shown by the flow of MSU #1 in the previous figure. In a standard network configuration, in the event LSN13 and LSN 4 are not available, all messages destined for SSP#1 will be routed through STP A.

STP B should have issued a TFP for SSP #1. However, if the customer provisioned a route to SSP#1 as shown by MSU #1, traffic would still be going to SSP #1 through STP B. STP D should be using D link-LSN 3 to route traffic to SSP #1.

It should be noted that messages following MSU #1 call flow could be 2 possible types.

- MTP routed messages- these would NOT be blocked as the OPC in the routing label would be equal to SSP #2

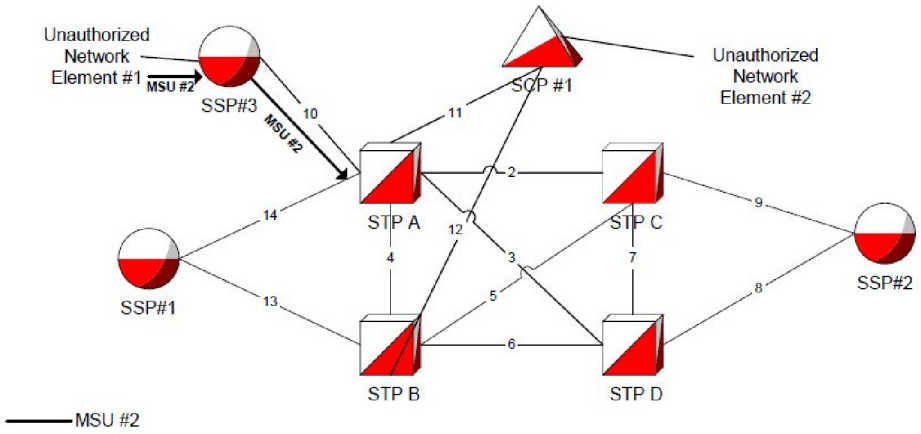
- GTT routed messages/Messages Originated by STP B-these would be blocked as the OPC in the routing label would the OPC of STP B.

Therefore, if STP A has the SECMTPMATE option active, STP A will discard messages received over any link other than LSN 4 whose OPC is equal to the True, Secondary, or Capability point code of STP B. It should again be noted that this option enforces a standard network configuration rule that may not apply to all customers.

SECMTPSID Option

An example of the SECMTPSID option is shown by the flow of MSU #2 in the following figure. Unauthorized Network Element #1potentially can flood and or send harmful bogus SS7 messages over LSN 10 that appear to have been generated by STP A by sending various messages with the OPC =STP A. This is obviously an undesirable situation and should not be allowed. The EAGLE should not receive a message with its own OPC, unless the message is a result of a circular route test or is an SLTM when the far end is in loopback.

Figure 4-36. SECMTPSID Option Diagram



Therefore, assuming STP A has the SECMTPSID option active, it will discard all received messages with an Origination Point Code (OPC) equal to its True, Secondary or Capability Point Code(s), unless all the following criteria are met:

- The EAGLE's MTP Circular Route Detection Mechanism sent the message with an OPC equal to the EAGLE's TPC/SPC (i.e. message is an RCT message with a priority of 3).

OR

- Message is an SLTM and has an OPC equal to the EAGLE's TPC or SPC.

NOTE: SLTMs with an OPC equal to the EAGLE's TPC/SPC can be received when the far end is in a physical loopback, and the EAGLE will transmit an SLTM (e.g. via `TST-SLK`). Instead of receiving an SLTA from the far end with an OPC of the far end, the EAGLE's SLTM message will be returned. Without this check, SLTMs would be discarded.

MTP Network Management Message OPC Verification (SECMTPSNM)

SECMTPSNM option functionality is based upon the assertion that the EAGLE should not receive an MTP network management message unless:

Rule #1 - The OPC is an adjacent point code

Rule #2 - The EAGLE has a route to the OPC of the MTP network management message on the linkset which the message was received.

Rule #3 - The EAGLE has a route to the destination field in the message (if applicable to the concerned message) on the linkset which the message was received.

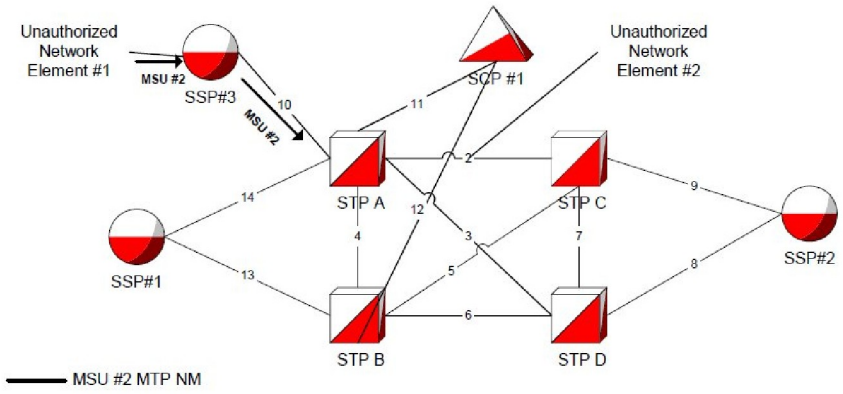
For all link types, the following additions/exceptions apply:

- Rule #3 would not apply to RSM messages.
- Rule #1 would not apply to UPU, TFC and RCT messages.

SECMTPSNM Option for A and E Links

Assuming STP A has the SECMTPSNM option active and an MTP network management message is received over an A link, STP A will only allow the message to itself when all the criteria are met. Refer to the following figure.

Figure 4-37. SECMTPSNM A link Option Diagram

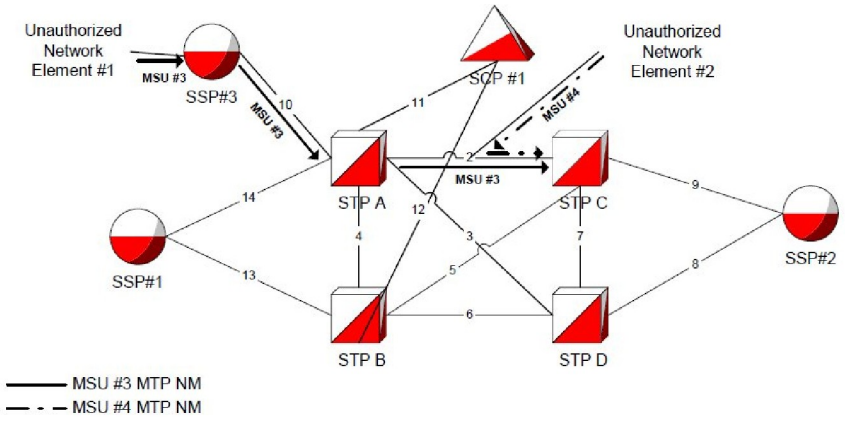


- As shown by MSU #2, Unauthorized Network Element #1 can send a TFP with a destination field = SSP#1,an OPC=SSP #3, and a DPC=STP A to STP A. It would pass Rule #1, pass Rule #2 and fail Rule #3.
- Example of why RSM messages are excluded from Rule #3: If LSN 14 and LSN 13 were to fail, STP A would send a TFP to SSP#3 concerning SSP#1. SSP #3 would subsequently send a RSPs to STP A concerning SSP #1 via LSN 10. If Rule #3 applied to the RSP, it would be discarded, since STP A does not have a route to SSP #1 on LSN 10.

SECMTPSNM Option for B-C-D Links

Assuming the STP C has the SECMTPSNM option active, it will allow all MTP network management messages received over B-C-D links when criteria listed in 2.2 are met. Refer to the following figure.

Figure 4-38. SECMTPSNM B-C-D link Option Diagram



- As shown by MSU #3, Unauthorized Network Element #1 can send a TFP with a destination field = SSP#2, an OPC=SSP #3, and a DPC=STP C. STP A would MTP route this message to STP C over LSN 2. STP C would receive this message and it would fail Rule #1, pass Rule #2 and fail Rule #3.

- Example of why RSM messages are excluded from Rule #3- MSU #4-if Unauthorized Network Element #2 injected RSP messages with an OPC=SSP#1, DPC=STP C and a destination field= SSP#2. STP C would reject the message since SSP#1 is a non-adjacent node and would subsequently fail Rule #1. Furthermore, if Unauthorized Network Element #2 injected RSP messages with an OPC=STP A, DPC=STP C, and a destination field= SSP#2, STP C would NOT reject this message since Rules 1 and 2 would be passed.

SCMG AFTPC Verification (SECSCCPSCMG)

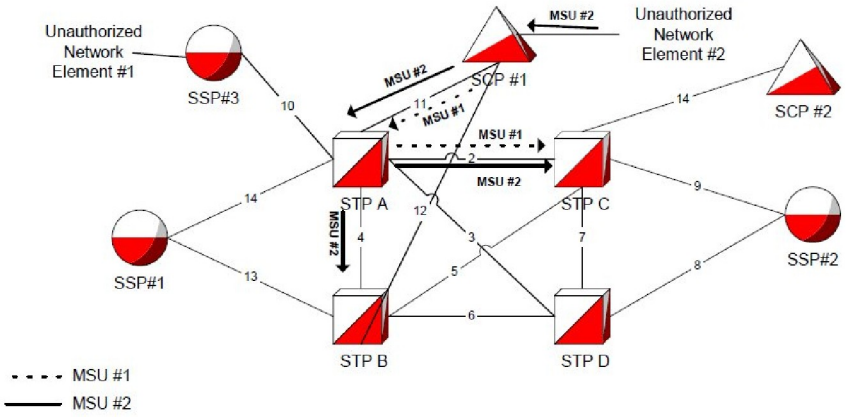
SECMTPSCMG option functionality is based upon the assertion that the EAGLE should not receive a SCCP network management message unless:

1. The EAGLE has a route to the OPC of the SCMG message on the linkset, on which the message was received.

2. The EAGLE has a route to the Affected Point Code in the message on the linkset on which the message was received.

The Affected Point Code (industry term) and the Concerned Point Code (EAGLE term) are synonymous. This option will only apply to SSP and SOR messages. This feature will not affect the following messages: SSA, SST, SOG, SBR, SNR and SRT. Refer to the following figure.

Figure 4-39. SECSCCPSCMG Option Diagram



Normal operation for SCMG messages (e.g. SSP) would be for SCP#1 to send an SSP to STPA. STP A will look in the Concerned Point Code table and broadcast SSPs to point codes listed in that table with an OPC =STPA. The SSPs that are broadcasted will have an OPC= STP A and an AFTPC = SCP#1.

As shown by MSU #1 (normal operation), if SCP #1 sends an SSP to STP A (MSU #1), STPA will look in the Concerned Point Code table to see which point codes should receive a broadcast SSP concerning SCP#1. Assuming STP B and STP C are in the CSPC table, SSPs are broadcast to STP B and STP C (MSU #2).

Assuming STP C has the SECSCCPSCMG option active, it will discard any SSP or SOR message received on a linkset for which the EAGLE does not have a route to the AFTPC on that linkset. This is similar in nature to the SECMTPNM option except the AFTPC field in the SCMG is checked, instead of the destination field in the MTP network management messages, and ensures that an SSP or SOR message is received over a linkset that STP C has a route for.

As shown by MSU #2, if Unauthorized Network Element #2 attempts to send SSPs with an AFTPC of SCP #2 and a DPC of STP C via LSN 11, STP C will receive the SSP MTP routed from STP A over LSN 2 with the OPC=SCP #2, DPC=STP C, and AFTPC=SCP #2. Since STP C does not have a route to SCP#2 over LSN 2, the message will be discarded.

Hardware Requirements

No new hardware is needed to support this feature.

Limitations

This feature will not be implemented on GX25 cards.

It will be assumed that the CPC of the Mate STP will match the CPC of the EAGLE. This feature also assumes that routing is provisioned symmetrically between any two points (i.e., if a valid NM message is received on a link set, there should be a corresponding route provisioned to the OPC and destination over that incoming link set; e.g., if A can route to B through C, B should also be able to route to A through C).

New Control Shelf Backplane (Release 23.0)

A new backplane for the control shelf has been introduced in Release 23.0 with these changes:

- The maintenance bus has been removed from the backplane.
- The backplane has been redesigned to distribute the clock signals for the high-speed ATM signaling links at 1.544 Mb/s.
- Two serial port connections (DB-15 connectors) have been added to the control shelf backplane, one providing emergency access to the standby MASP, the other providing a connection to the TDM for critical indications.
- The control shelf backplane now contains four -48VDC power and ground connections (DB-26 connectors). Two of these connectors are labeled Primary A and B and are connected to the fuse and alarm panel. The other two are labeled Secondary A and B and are connected to another power source, allowing the EAGLE to remain in service when replacing the fuse and alarm panel.
- All EAGLE shelves have a binary address to identify the shelf to the system. The control shelf backplane address is permanently configured and cannot be changed. This allows only one control shelf in the EAGLE. The shelf address has been expanded from four bits to six bits, increasing the maximum number of addressable card slots from 250, or 500 signaling links, to a theoretical limit of 1018, or 2036 signaling links. The actual number of addressable card slots is limited by the system software and the hardware configuration of the EAGLE. In Release 23.0, the actual number of addressable card slots is 378, or 756 signaling links, but is limited by the system software to 250 cards, or 500 signaling links.
- To allow the TDMs to determine which version of the control shelf backplane they are connected to, the control shelf backplane uses pins A49, A50, and A52 on connectors P2 and P4 to send a binary signal to the TDMs. On previous backplanes, these pins were left unconnected, creating a binary signal of 111. On this backplane, the least significant bit of the signal, pin A49, is connected to ground, creating a binary signal of 110. This signal corresponds to this version of the control shelf backplane.

Network Surveillance Enhancements (Release 28.0)

Description

The Network Surveillance Enhancement feature adds a new terminal type to the EAGLE system. This terminal type, the Management Terminal (MGMT), provides a machine-to-machine messaging interface between the EAGLE and network Operations Support Systems, OSS. This feature lets the EAGLE integrate more smoothly with most network monitoring devices.

Hardware Requirements

No new hardware is required to support this feature.

New Hardware (Release 23.1)

Description

Release 23.1 introduces improvements to these cards in the EAGLE.

- TDM
- MDAL
- IPMX
- E486 main assembly for the ASM, ACM, LIM, and MCAP card
- E586 main assembly for the TSM-256 and MCAP-256 card

It also introduces a new card into the EAGLE, the integrated LIM-AINF.

The electrostatic discharge (ESD) clips on these cards have been redesigned so they do not bend easily, making the insertion and extraction of the cards easier.

Each card has been redesigned so that the tooling holes and holes used for mechanical attachment cannot be used as functional plated-through holes and provide electrical connections between the conductor layers of the card.

The nut and washer assembly used for attaching the faceplate to each card has been replaced with PEM nuts, reducing the labor required to assemble the card.

A diode has been added to the -48V return path to prevent the TDM from being powered by the other TDM through the connections for the fuse alarms.

The BITS clock recovery circuit on the TDM has been improved to tolerate more noise on the clock input and make the BITS clock recovery circuit more stable.

To ensure that the TDM LED comes on when it is supposed to, the controlling resistor for the LED has been changed from 10K Ohms to 1K Ohms.

These design modifications do not have any impact on the software functionality of these cards.

Integrated LIM-AINF Card

A new card is being introduced to the EAGLE, the integrated LIM-AINF card, P/N 870-1484-xx. The integrated LIM-AINF card contains all the functionality of the LIM-AINF card, P/N 870-1014-xx, and is contained on one board. The AINF applique is not used or required for the integrated LIM-AINF card. No other applique can be used with this card. It can only serve as a LIM. The integrated LIM-AINF contains the three LIM interfaces, DS0, OCU, and V.35 and uses the system software to select the interface, the same as on the old LIM-AINF card.

New Hardware (Release 26.05)

Multi-Purpose Server (MPS)

The MPS hardware system is being deployed in conjunction with the EAGLE STP Database Service Module (DSM) subsystem for both the G-Flex C7 Relay and Intelligent Network Application Part (INAP)-based Number Portability features. (See "G-Flex C7 Relay (Release 26.2)" and "INAP-based Number Portability (INP) (Release 26.05)" for discussion of these features.)

The MPS hardware system includes the MPS, supporting Local Area Network (LAN) devices and associated peripheral units.

Refer to the *NSD Hardware Manual* for current information on the MPS hardware.

Non-ANSI Point Code Support (Release 20.0)

The EAGLE supports the use of the network identifier of “0” to accommodate networks outside of the ANSI network with nonconventional point codes. This network identifier can also be used as a test point code in some applications within the U.S.

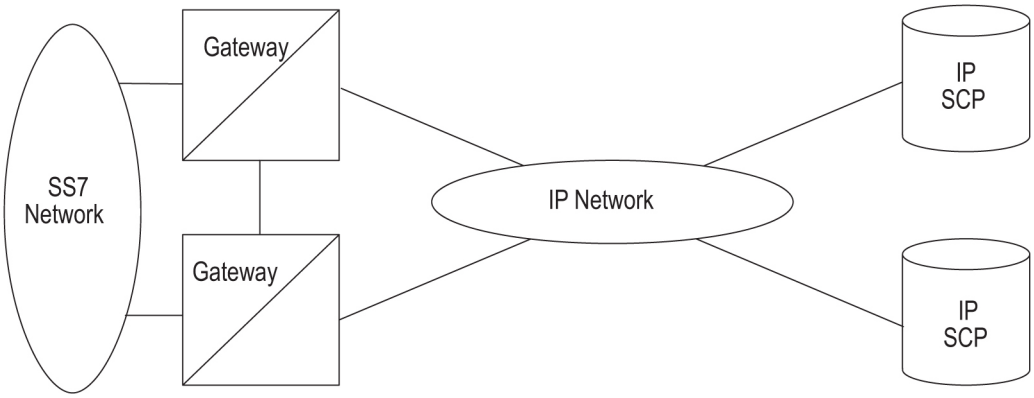
Non-Generation of Duplicate SEAS Autonomous Messages (Release 22.0)

This feature allows only one copy of a SEAS autonomous message to be sent to the first available SEAS port. This prevents duplicate SEAS autonomous message from being sent to the SEAS ports.

Non-SCCP/ISUP Routing (IP^7 Releases 1.0, 2.0)

This feature, which was available only in a laboratory environment in release 1.0, allows SS7 nodes to exchange non-ISUP and non-SCCP protocol messages with one or more TCPIP/IP-based devices residing on an IP network. The following figure shows a network example for this feature. The IP ^{7} Secure Gateway node maps the destination point code and service indicator (non-ISUP, non-SCCP) to a TCP/IP address and port.

Figure 4-40. Non SCCP/ISUP Routing



Notification of Congestion Level Increase (Release 22.0)

When the congestion or discard level on a signaling link increases from one Elevel to the next, the EAGLE issues one of these UIMs to the EAGLE terminals.

UIMs

UIM 264—REPT-LINK-CGST: congestion level 0 to 1

UIM 265—REPT-LINK-CGST: congestion level 1 to 2

UIM 266—REPT-LINK-CGST: congestion level 2 to 3

UIM 270—REPT-LINK-CGST: discard level 0 to 1

UIM 271—REPT-LINK-CGST: discard level 1 to 2

UIM 272—REPT-LINK-CGST: discard level 2 to 3

In release 22.0, when one of these UIMs is issued, the EAGLE sends the SEAS message REPT-LINK-CGST to the SEAS interface.

The threshold of each congestion or discard level is included in the REPT-LINK-CGST message and is defined as the number of MSUs being transmitted on the signaling link or the number of MSUs being discarded because of the congestion.

Notification of Inability to Perform a Global Title Translation (Release 22.0)

Whenever the EAGLE is unable to perform a GTT due to administration table problems, and an MSU is discarded, the EAGLE issues one of these UIMs.

UIMs

UIM 1043 — SCCP did not route - bad translation

UIM 1046 — SCCP did not route - DPC not in MAP tbl

UIM 1049 — SCCP did not route - SS not in MAP tbl

In Release 22.0, when any of these UIMs are issued, the EAGLE sends the REPT-NOTRNS message to the SEAS interface. To control the number of REPT-NOTRNS messages being sent to the SEAS interface, the REPT-NOTRNS message is only sent if less than 10 previous REPT-NOTRNS messages have been sent during a 5 minute period. If 10 REPT-NOTRNS have already been sent during the 5 minute period, no REPT-NOTRNS messages are sent until the 5 minute period has expired. When this 5 minute period expires, a new 5 minute begins and the EAGLE resumes sending REPT-NOTRNS messages.

Notification of Link Set Outage (Release 22.0)

When all signaling links in a linkset become unavailable because of multiple signaling link failures or processor outages, the EAGLE issues UIM 318 - REPT-LKSTO: Link set prohibited.

In Release 22.0, when UIM 318 is issued, the EAGLE sends the SEAS message REPT-LKSTO to the SEAS interface. Included in the REPT-LKSTO message is the number of signaling links that have failed (the primary state of the signaling links is OOS-MT) and the number of signaling links that have been inhibited (the

Notification of Link Set Recovery (Release 22.0)

When the linkset outage condition, reported with UIM 318 or the SEAS REPT-LKSTO message, has been corrected, the EAGLE issues UIM 317 - RCVRY-LKSTO: Link set allowed.

In Release 22.0, when UIM 317 is issued, the EAGLE sends the SEAS message RCVRY-LKSTO to the SEAS interface. Included in the RCVRY-LKSTO message is the number of signaling links in the linkset that are back in service.

Notification of Locally Initiated Database Copy (Release 22.0)

This feature requires the EAGLE to send the REPT-DBCPY message to the SEAS interface any time the EAGLE database is backed up or restored with the EAGLE command **chg-db**. This message is sent regardless of whether the **chg-db** command was entered correctly or completed successfully.

The following table defines the indicators used to show which version of the database the REPT-DBCPY message is reporting about.

Table 4-30. REPT-DBCPY Database Indicators

Database Indicator	SEAS Definition	EAGLE Definition
C	Current active version of the database	The database in the current partition of the fixed disk
P	Primary version of the database	The database in the backup partition of the fixed disk
X	Copy of the database on an external device	The copy of the database on a removable cartridge

A completion code of COMPLD (completed OK) is sent to the SEAS interface when the **chg-db** command completes with no errors.

A completion code of NSD (not started) is sent to the SEAS interface when the **chg-db** command is rejected because of semantic errors.

A completion code of ABTD (aborted) is sent to the SEAS interface when the **chg-db** command fails during execution.

This message is not sent if the EAGLE's **copy-tbl** or **copy-disk** commands are used to overwrite the active database.

Notification of MTP-Level Routing Error (Release 22.0)

When an MSU is discarded because the EAGLE has received the MSU with an undefined point code or an invalid SIO, these UIMs are issued.

UIMs

UIM 1004—MTP rcvd unknown DPC

UIM 1018—MTP rcvd invalid SIO

In Release 22.0, when either of these UIMs are issued, the EAGLE sends the REPT-MTPERR message to the SEAS interface. To control the number of REPT-MTPERR messages being sent to the SEAS interface, the REPT-MTPERR message is only sent if less than 10 previous REPT-MTPERR messages have been sent during a 5 minute period. If 10 REPT-MTPERR have already been sent during the 5 minute period, no REPT-MTPERR messages are sent until the 5 minute period has expired. When this 5 minute period expires, a new 5 minute begins and the EAGLE resumes sending REPT-MTPERR messages.

Notification of Recovery from Link Congestion (Release 22.0)

When the congestion or discard level on a signaling link increases from one level to the next, the EAGLE issues one of these UIMs to the EAGLE terminals.

UIMs

UIM 267—RCVRY-LINK-CGST: congestion level 3 to 2

UIM 268—RCVRY-LINK-CGST: congestion level 2 to 1

UIM 269—RCVRY-LINK-CGST: congestion has cleared

UIM 273—RCVRY-LINK-CGST: discard level 3 to 2

UIM 274—RCVRY-LINK-CGST: discard level 2 to 1

UIM 275—RCVRY-LINK-CGST: discard has cleared

In release 22.0, when one of these UIMs is issued, the EAGLE sends the SEAS message RCVRY-LINK-CGST to the SEAS interface.

The threshold of each congestion or discard level is included in the RCVRY-LINK-CGST message and is defined as the number of MSUs being transmitted on the signaling link or the number of MSUs being discarded because of the congestion.

Number Pooling (Release 24.0)

Number pooling involves assigning a portion of an NPA-NXX, for example a thousands block (NPA-NXX-X), to a service provider (block holder) which is different from the NPA-NXX holder (the code holder). Before number pooling, numbers were assigned to service providers on an NPA-NXX basis. For smaller service providers needing fewer than 10,000 numbers, this method results in many unused, but reserved numbers. Number pooling is used to allow the allocation of numbers on a smaller block basis.

In the EAGLE, a number no longer owned by the NPA-NXX holder can be viewed the same as a number ported to a new service provider. Any or all of the numbers in a given NPA-NXX-X can be ported to the block holder by generating subscription versions with the block holder's data.

The subscription data in the EAGLE has been modified to show which of three LNP types have been assigned to the LNP subscription.

- LSSP – Local Service Provider Portability
- LISP – Local Intra-Service Provider Portability
- POOL – Pooled Block Number Port

In the EAGLE, the LNP subscriptions containing telephone numbers that are ported to an NPA-NXX-X block holder are designated with the LNP type of POOL. Telephone numbers that are ported before having the LNP type assigned to the telephone subscription are assigned the LNP type NONE.

The LNP type is not part of the subscription version data received from the LSMS, but must be assigned to the subscription data using either the **ent-lnp-sub** or the **chg-lnp-sub** commands.

Number Pooling/Efficient Data Representation (EDR) (Release 26.1)

Overview

Currently, the assignment of 10,000 (NPA-NXX) blocks of phone numbers to service providers for number portability results in large numbers of unused phone numbers in the NPA-NXX block, especially for smaller service

providers. To conserve new NPA-NXX blocks of numbers and to provide more efficient use of existing NPA-NXX blocks, pooling of 1000 number blocks was mandated by NANC.

Number Pooling/EDR allows the NPA-NXX service provider holder (code holder) to assign a portion of an NPA-NXX, i.e. a thousand block (NPA-NXX-X), to another service provider (block holder). EDR (allows this thousand block of numbers to be represented as a single record.

Currently, number pooling is implemented in the industry without EDR. This means that when the 1000 number blocks TN's are pooled (ported out from the code holder), the pool of 1000 numbers comes across the NPAC/ LSMS interface as individual records (a 1000 TN port at one time). This can result in interface performance and database utilization problems.

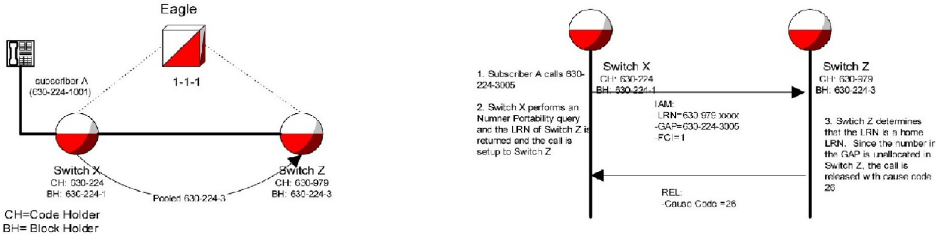
Efficient Data Representation (EDR) was conceived so that pooled 1000 blocks of TN's could be managed as one subscription object. The numbers in a given NPA-NXX-X can be ported from the code holder to the block holder by generating subscription versions with the block holder's data. This type of port is designated with an LNP type of "POOL," which is maintained as part of the subscription version from the SOA to the NPAC to the LSMS and down to the EAGLE.

This feature is dependent upon the North American Numbering Council (NANC) 3.0 release, and the associated feature in LSMS 3.0.

End Office Perspective

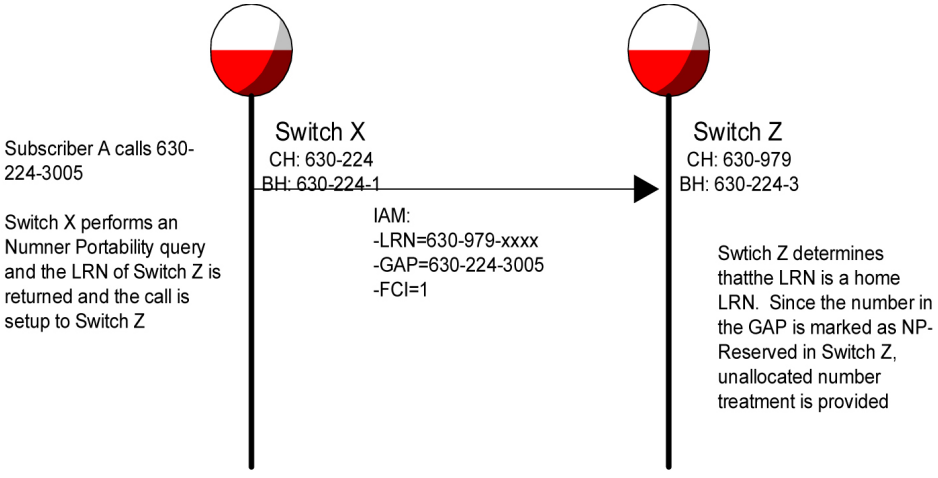
Current switching mechanisms for number portability query and response have been modified to support Number Pooling/EDR. Default routing functionality is maintained.

Because 1000 blocks of TNs are pooled from the code holder to the block holder, special arrangements must made, since the block holder may not have customers for all the 1000 TNs that were pooled.

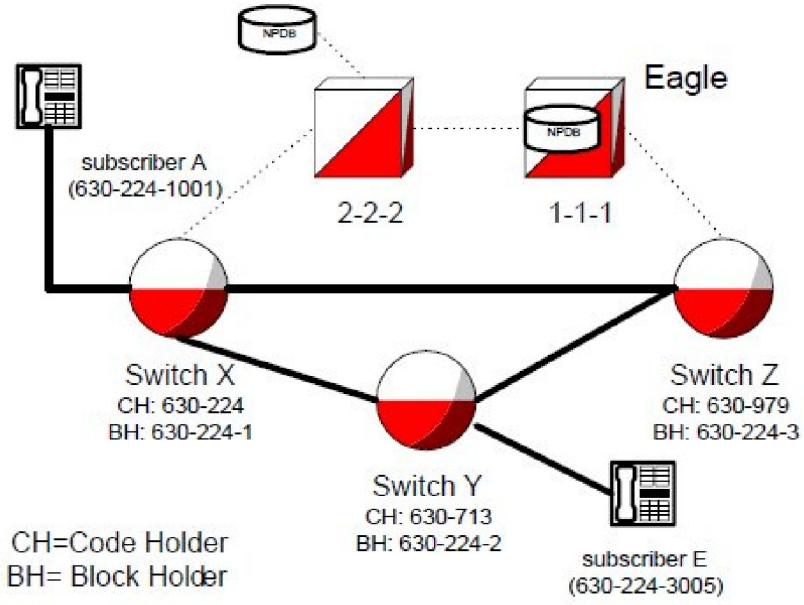


This event would cause both Switch X and Z service providers to think the call was misrouted, when indeed it was not.

To remedy this situation, a NP-Reserved marking is used on Switch Z to suppress code 26 and provide unallocated number treatment (for example, "You have reached a number that is not in use").



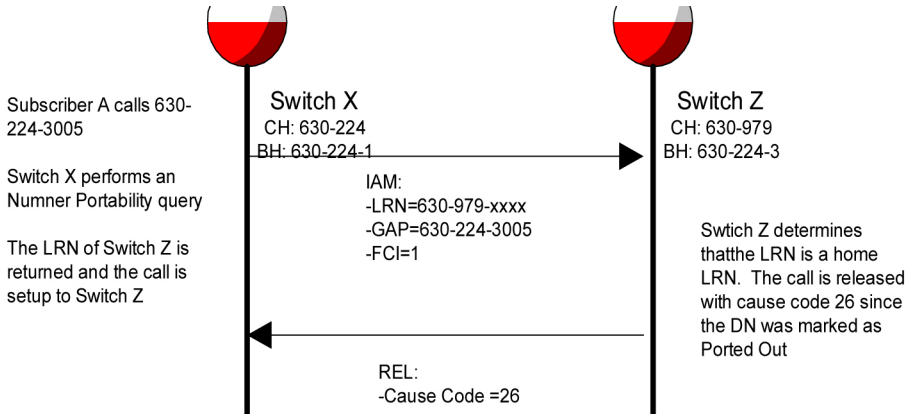
In this scenario, if 630-224-3005 were assigned to subscriber E, switch Z would find subscriber E in the NPDB, and route the call in Switch Z's network. If subscriber E subsequently ports to a new service Provider, Switch Y, the pooled block in Switch Z indicates that 630-224-3005 is ported to Switch Y, and normal LRN routing occurs for the call.



If there is a timing issue with subscription records being updated from the NPAC to each switch's NPDB, errors in routing can occur. For example, if the NPDB for Switch X is not updated due to equipment problems, a call from subscriber A to subscriber E would be routed by Switch X with the LRN received from its non-updated NPDB. Switch Z detects the LRN as a home LRN, and because the GAP is marked as NP-reserved on the switch, Switch Z provides unallocated number treatment. Switch Z should have released the call with cause code 26.

To alleviate this timing issue, when subscriber E ports to Switch Y, the number from the NPAC can be marked as Ported Out. This marking in the preceding example will operate as follows:

When Switch Z receives the call with the home LRN, the number is marked as ported out at Switch X when subscriber E ports. Then, when Switch Z receives the call with the GAP parameter marked as Ported Out, Switch Z will correctly provide cause code 26 treatment.



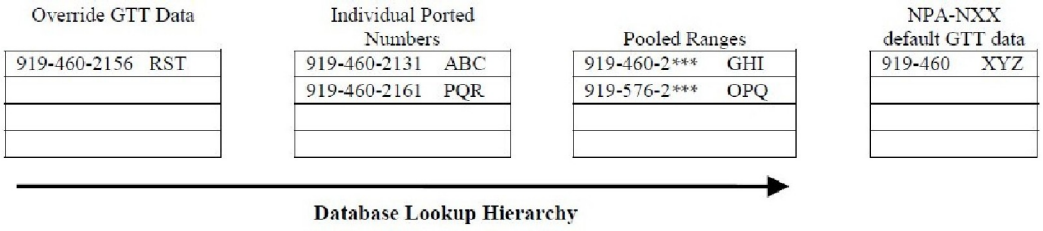
In addition, if subscriber E disconnects service, 630-224-3005 is "snapped back" to Switch Z. Typically, the Ported Out marking is removed, and the NP Reserved Marking is reinstated.

When an NPA-NXX is split, the pooled blocks of 1000 TN's will have the same NPA after the split. This means that if area code 919 was split into 919 and 376 area codes, any pooled numbers (919-460-1xxx,919-345-3xxx, etc) would have the same NPA(919) after the split.

EAGLE Perspective (LNP Database)

From the EAGLE perspective, Number Pooling/EDR can be viewed as another table lookup prior to defaulting to the default GTT data. Pooled ranges become an intermediate step in a TN lookup.

Figure 4-41. Database Lookup Hierarchy



Upgrade Considerations

While no new upgrade requirements have been identified, note that the EAGLE must rely on LSMS to provision newly pooled objects, and remove individual subscription exceptions that are contained within the pooled block, in order to take advantage of the EDR capability. The EAGLE database update performance will depend on method that is used to do it. For High-speed bulk-load/reconcile, the EAGLE database will be updated at 200 TPS and additional time it takes to do the finish-edl process on the EAGLE. If slow-speed reconcile is used, EAGLE will be updated at 2 TPS.

Limitations

The EAGLE must be upgraded to support EDR data records prior to upgrading the OAP. The OAP must be upgraded to support EDR data records prior to upgrading the LSMS.

OAP Upgrade Enhancement (Release 27.2)

The OAP is now self-configuring, for the purpose of determining the OAP operating mode.

OCTRETRN in 30-Minute Measurements Reports (Release 31.4)

The OCTRETRN register is added to the output of the COMP-LINK report for EAGLE for both the Measurements Platform and OAM generated measurements.

The OCTRETRN (octets retransmitted) peg is available on 30 minute intervals. previously, it was only available on 24 hour interval.

Online Cartridge Formatting (Release 20.0)

The EAGLE supports online formatting of the removable cartridge. The removable cartridge can be formatted to hold either system data (the database and the GPLs) or measurements data.

Option for Subsystem Prohibit (Release 29.0)

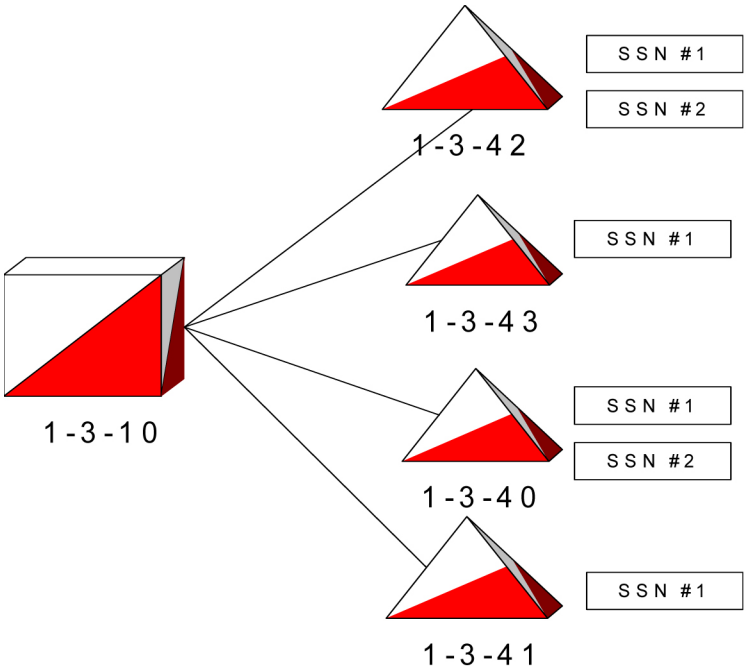
Description

This feature allows the network operator the option to have selected subsystems still marked as prohibited even though an MTP-RESUME has been received (i.e. point code is allowed). This allows a clearer delineation between the concept of a point code and a subsystem for SCCP Management.

NOTE: This feature does not contain any restrictions regarding ITU/ANSI point code formats.

The following figure provides an example of a network view of this feature.

Figure 4-42. SSN Prohibit Option Diagram



In this figure, STP 1-3-10 is set up so that it is load sharing the application denoted by SSN#1 across all SCP's and is in dominant mode (as primary) for SSN#2.

Currently, if point code 1-3-42 goes down, EAGLE marks all SSN's associated with 1-3-42 as prohibited and will broadcast SSP's to nodes contained in the respective CSPC group. The EAGLE will subsequently load share SSN #1 across 1-3-43, 1-3-40, and 1-3-41. Traffic destined for SSN #2 will be served by 1-3-40. This operation does not change for this feature.

Prior to this feature, when point code 1-3-42 came back in service and an MTP-RESUME was received, the EAGLE would:

1. Mark SSN #1 and SSN #2 related to 1-3-42 as allowed and broadcast SSA's to nodes contained in the respective CSPC group. This was done regardless of the actual status of the subsystem within the point code.

2. If SSN #2 was still down at 1-3-42, the EAGLE would wait for a message destined for SSN#2, send the message to SCP 1-3-42 and subsequently receive an SSP for SSN#2 from 1-3-42.

3. EAGLE would then subsequently broadcast SSP's to nodes contained in the respective CSPC group, and initiate SST's to SSN#2 to poll for subsystem status.

This feature changes the behavior in steps 1 and 2 above, when the option is on for both SSN #1 and SSN #2 for 1-3-42 to the following when an MTP-RESUME is received:

1. Send SST's to 1-3-42 concerning SSN #1 and SSN #2 and receive either an SSP or SSA from SCP 1-3-42 concerning SSN #1 or SSN #2.

2. Broadcast SSA/SSP's, depending on the result of the SST's, to nodes contained in the respective CSPC group.

Hardware Requirements

No new hardware is needed to support this feature.

Option for Turning on Class 1 Sequencing (Release 31.6.3)

Description

This feature addresses the problem where messages are sent as Class 1 even though they are not segmented or sequenced and the customer wants to be able to load share these messages among 8 GTT destinations.

The release 36.1.3 feature number 53481 "in-sequence delivery of Class 1 UDT messages," guarantees that Class 1 messages (both XUDT and UDT) are transmitted out of the EAGLE in the same order they are received. A by-product of the initial implementation of this feature is that the existing GTT load sharing mechanism (where a message can be load shared among 8 GTT destinations) no longer works for Class 1 messages. The Class 1 messages can only be delivered to a primary node with backup. This is a change to previous EAGLE behavior where Class 1 UDT messages could be load shared among 8 GTT destinations in the same manner as Class 0 messages.

The original thinking was that if a customer is using Class 1, they should not want them spread out among different end nodes. Even if they did, the thought was that they could simply use Random SLS Generation feature set to "Class 1" to get a load share distribution. However, due to the way the end node processes received traffic, they are unable to use Random SLS set to Class 1. As a result, the behavior of release 31.6 with Class 1 messages will break the current routing mechanism because there is no way to turn off the sequencing algorithm and go back to allowing full load sharing (but not guaranteed sequencing) on these messages.

An option is added to the EAGLE that turns ON/OFF the guaranteed in-sequence delivery of Class 1 (X)UDT messages. When ON, the EAGLE guarantees that these messages are delivered in the order they were received, but the messages will not be GTT load shared. When OFF, the EAGLE is able to GTT load share the messages but does not guarantee in-sequence delivery.

This design provides the option to turn ON/OFF the Class 1 Guaranteed Sequencing Algorithm. This requires storage, a user interface, and conditional logic to control Class 1 sequencing based upon the new parameter setting.

Limitations

EAGLE does not guarantee that Class 1 ITU messages will be delivered in sequence when CLASS1SEQ is ON and RANDSLS is ALL.

Origin-based MTP Routing (Release 35.0)

Description

The Origin-based Message Transfer Part (MTP) Routing feature allows traffic to be routed to the same destination through different networks, depending on the origin of the messages. This flexibility is achieved by enabling EAGLE 5 ISS to be configured to use additional criteria when making MTP routing decisions.

The Origin-based MTP Routing feature provides the following route types:

- DPC + OPC (processed first)
- DPC + originating linkset
- DPC + CIC

  NOTE: DPC + CIC routing is only applicable to ISUP messages that have the CIC field, not as a parameter.
- DPC + SI
- DPC (processed last)

If available, EAGLE 5 ISS always uses the route of a more preferred route type. Route cost is used to choose from routes of the same type. Therefore, a DPC + OPC route with a route cost of 20 is chosen ahead of a DPC + SI route with a route cost of 10.

The Origin-based MTP Routing feature introduces the DPC + OPC, DPC + incoming linkset, and DPC + CIC route types. These route types are considered exception routes, and do not factor into the availability status of a destination. A routeset is a collection of routes to a destination. Each routeset can have up to 6 routes, with 16 links to a route. An exception routeset is a collection of up to 6 exception routes that have the same DPC, exception class and criteria. If all of a destination's DPC-only routes become unavailable, the destination is considered unreachable by EAGLE 5 ISS, even if an exception route to that specific destination is still capable of carrying traffic.

New Concepts

The Origin-based MTP Routing feature introduces the following concepts:

- CIC Handling
- Network management and exception routes
- Congestion handling
- Circular route detection
- Gateway nodes
- SCCP handling

CIC Handling

The Origin-based MTP Routing feature allows exception routes to be entered based on the CIC and/or a range of CIC values. This feature uses the value placed after the routing label for all CIC triggers, instead of a CIC value placed within the mandatory fixed, variable or optional part.

Network Management and Exception Routes

The Origin-based MTP Routing feature operates on an end-to-end scheme instead of point-to-point to prevent impacts to routing. This management method has the following results:

- Adjacent point codes do not have exception routes.
- Exception routes do not factor into the status of a destination. A destination's status is only defined by the standard routes entered.
- If all the DPC-based routes to a destination are unavailable, then the status of the destination is listed as Prohibited even if exception routes are available.
- Preventative and broadcast TFx or TCx are not sent based on the status of exception routes. If an exception route is unavailable, the next exception route is chosen ending in the standard provisioned routes.

Congestion Handling

The CPC is the only identifying characteristic of a TFC message: therefore, the EAGLE 5 ISS cannot determine whether the message is a node or whether the route to the destination is congested.

The Origin-based MTP feature ensures that there are many routesets to a destination. However, the EAGLE 5 ISS is still unable to determine if the TFC is regarding an Exception or Normal route or if the node itself is congested. Therefore, once a TFC is received regarding a node within exception routes provisioned against it, the EAGLE 5 ISS lists all routesets to that destination as congested.

To ensure that the EAGLE 5 ISS has the correct congestion status of the destination, an RCT regarding the destination over each impacted route is sent. This ensures that the destination does not "bounce" in and out of congestion. The EAGLE 5 ISS starts T15 at the beginning of the broadcast and T16 at the completion; if the EAGLE 5 ISS receives a TFC regarding that destination in response to the poll, the EAGLE 5 ISS maintains the congestion level against it, even if it was received over a linkset which is part of an exception routeset.

Circular Route Detection

If the EAGLE 5 ISS detects that traffic originated from a route is to be sent back over the same route, it changes the status of the DPC to Prohibited, so that the linkset does not enter into congestion and potentially impact other valid routes. To reduce the impact to the true route of the DPC, the EAGLE 5 ISS prohibits only the impacted route to a destination, and not the destination itself. This ensures that only the route provisioned as the exception route is impacted if CRD is detected, and all other remaining traffic is able to reach the DPC.

NOTE: The rst-dstn command is the recommended method for clearing this CRD condition.

Gateway and Exception Nodes

The Origin-based MTP Routing feature allows the provisioning of exception routes across networks, where the OPC and DPC do not exist within the same network type (ANSI, ITU-I or ITU-N). However, exception routes are only provisionable through the full point code values, not aliases or clusters.

Each OPC used within a Gateway Exception Routeset must have an alias entry within the destination table for the network where the DPC resides.

SCCP Handling

The Origin-based MTP Routing feature provides the MOBRSCCPOPC SCCP option which allows the OPC to be selected in the routing header, the EAGLE 5 ISS TPC, or the CGPA OPC for SCCP routing.

Hardware Requirements

The Origin-based MTP Routing feature has the following hardware requirement:

- EAGLE 5 ISS cards:
  - LIM-ATM: 870-1293-02
  - EDCM: 870-2372-01
  - MPL/MPL-T: 870-2061-xx
  - E1/T1 MIM: 870-2198-xx
  - HC-MIM: 870-2671-xx
  - TSM: 870-1289-xx, 870-1290-xx, 870-1291-xx, 870-1292-xx
  - DSM: 870-1984-03

    NOTE: The Origin-based MTP Routing feature does not support 2-Port LIM cards or Dual-Slot DCM cards.

Limitations

The Origin-based MTP Routing feature has the following limitations:

- The Origin-based MTP Routing feature cannot be used with LIMDSO/V35/OCU, LIM-E1, or Dual-Slot DCM cards.
- All destinations must have DPC-only routes.
- MTP Low Priority Route Set Test (MLPRST) must be turned on (**`chg-stpopts`** command) before this feature can operate.
- CIC-based routing is supported only for ISUP traffic.
- Adjacent routes cannot have exception routes.
- Exception routes do not factor into the status of a destination. A destination's status is defined only by the standard routes entered.

- If all DPC-based routes to a destination are unavailable, then the status of the destination is listed as Prohibited even if exception routes are available.
- CIC handing considers only the value after the MTP Routing Header and not any values within the ISUP parameters. This includes handling of CIC ranges.
- Full point code OPC criterion always takes precedence before wildcard OPC criterion regardless of the assigned route cost. For example, if an OPC exception criteria of 1-1-1 with a route cost of 20 and 1-1-* with a route cost of 10 are entered, 1-1-1 is used even though 1-1-* has a lower route cost.
- Exception routes for cluster exceptions do not inherit exception routes for the cluster member. Exception routes for the cluster exception must be applied individually if desired.

Origin-based SCCP Routing (Release 35.0)

Description

TheOrigin-based SCCP Routing feature allows EAGLE 5 ISS to route SCCP messages based on CdPA GTA, CgPA GTA, CgPA SSN, CgPA PC, and/or OPC fields.

This feature allows EAGLE 5 ISS to operate in CgPA GTT, Advanced (Adv) CdPA GTT, and CdPA GTT mode. These modes are combined in a GTT Mode hierarchy, which determines the preference of GTT modes and the order in which the fields are searched in incoming MSU.

The following GTT Mode Hierarchy combinations are supported by the Origin-based SCCP Routing feature:

- CdPA only
- Adv CdPA, CdPA
- CgPA, Adv CdPA, CdPA
- Adv CdPA, CgPA, CdPA
- Adv CdPA, CdPA, CgPA
- CgPA, CdPA
- CdPA, CgPA
- CgPA only

The Global Title Translation process starts with the first GTT Mode of the GTT hierarchy. If translation is found there, the whole GTT is stopped. If translation is not found in this first GTT Mode, the GTT process tries to find a translation in the next GTT Mode of the hierarchy.

The GTT Mode hierarchy can be configured on a system wide basis and on a per linkset basis. The system wide option is used to define the default value for all linksets by default. Each linkset can then be configured to use one of the GTT Mode Hierarchies. The linkset option overrides the system default for that linkset only. Any linkset that is not changed continues to use the system default.

In Adv CdPA mode, one or more of the following additional translations can be configured to apply on top of the mandatory CdPA GTA translation: none, CgPA GTA only, CgPA PC only, SELID only, CgPA GTA + OPC, CgPA PC + OPC, SELID + OPC, or OPC only. Each additional translation can have a subsequent translation on CgPA SSN.

In CgPA mode, a CgPA GTA translation with or without a subsequent CgPA SSN translation, or a CgPA PC translation with or without a subsequent CgPA SSN translation search (CgPA GTA and CgPA PC are mutually exclusive) can be configured. The search order is predefined and cannot be changed.

NOTE: The CdPA GTI is always validated before GT starts processing SCCP MSUs. The CgPA GTI is not validated: therefore, when a subsequent lookup in Adv CdPA GTT mode is based on SELID or for CgPA TT, the attempt to find a CgPA GTT Set in the GTTSEL table may fail because of an invalid or unsupported CgPA GTI in the arrived MSU.

Hardware Requirements

The Origin-based SCCP Routing feature has the following hardware requirements:

- The SCCP application must run on a DSM card or higher.
- No SCCP application can be provisioned in the system if TSM cards are used.

Limitations

The Origin-based SCCP Routing feature has the following limitation:

Due to a 150-character limit on command length, a single **`ent/chg-gta`** command may not fit in a single line, especially for range entries with MGTT parameters. If an **`ent-gta`** command does not fit on one line, execute the command with fewer parameters, then execute **`chg-gta`** to modify the translation. If the **`chg-gta`** command does not fit on one line, break it into multiple commands.

5

Features P - Z

Password Aging (Release 21.0)

When a password is changed, either by the user or by a systems administrator, the date that the change took place is entered in the database along with the updated password.

During the login process, after the system has verified that the user has correctly entered the password, the system uses the date the password was changed to compute the number of days that have elapsed since the password was last changed. The password's age is compared against the value of the **page** parameter (maximum password age) of either the **ent-user**, **chg-user**, or **chg-secu-dflt** commands. If the password's age is greater than the value of the **page** parameter, then a password expired message appears in the command area. The user is prompted to enter and verify a new password. If the new password is acceptable, it is entered in the database along with the date that the change took place (the current date as shown by the EAGLE time-of-day clock).

The maximum age of a specific password (**page**) can only be specified with the **ent-user** command or the **chg-user** command. If the **page** parameter is not specified with the **ent-user** command, then the password's age is taken from the system default value. The system default value for the password's age is set with the **page** parameter in the **chg-secu-dflt** command. If the **page** parameter is not specified with the **chg-user** command, then the existing value for the password's age does not change.

The system administrator can set a password's maximum age to 0. This indicates that the password aging is not applied to the password and the password remains valid regardless of how many days have elapsed since it was last changed.

When the user attempts to login with a password that is older than its maximum allowable age, the following message is displayed in the command area after the password has been validated and before the login session is established:

```
Enter new password (password has expired and must be changed) :
```

The user is then prompted to enter and verify a new password. If the password is acceptable, the user is logged on. Otherwise, one of the invalid password error messages is displayed [see " "Password Requirements (Release 21.0)" "] and access to EAGLE is denied.

Password Encryption (Release 21.0)

To prevent passwords from being disclosed, in Release 21.0, the passwords are stored on the system in an encrypted form. The encryption algorithm that is used is a one-way encryption algorithm, meaning once the passwords are encrypted using the algorithm, the passwords cannot be decoded. Also, any passwords temporarily stored in memory are overwritten with null characters as soon as they are no longer needed.

Password Requirements (Release 21.0)

Currently, the only requirement for a password used in the EAGLE is that the password must contain from five to eight alphanumeric characters

In Release 21.0, the rules for passwords have changed to meet Bellcore password requirements. The requirements for passwords can now be configured in the database with the **chg-secu-dflt** command. Passwords on the EAGLE can contain a maximum of 12 characters.

Refer to the *Commands Manual* for current information on commands.

PCS 1900 LNP Query (Release 26.0)

Description

This feature provides for LNP query/response in a PCS wireless environment using the LRN method in order to support Service Provider Number Portability, thus extending EAGLE's LNP capability.

PLNP addresses the following capability in the network:

Call Completion to Ported Number (CCPN)

This network facility allows completion of a call to a ported directory number, when an MSC trigger is used (i.e. the MSC must be an LNP-capable switch). For PLNP, the MSC sends a query containing a DN, which is a 10-digit NANP called party number for a wire-line subscriber. The DN is used to perform an LNP database lookup in order to find the associated LRN.

Feature Functions

In order to support this new capability, PLNP utilizes the following, currently existing, LNP functions:

1. LNP Query processing: This function services LRN queries in real-time and generates associated LRN values. Multiple query types (AIN, IN, IS-41) are supported.

2. LNP Database: The database supports LNP Query and Message Relay processing, though Message Relay functionality is not supported in the industry.

3. SCCP Subsystem Management: SCCP supports local subsystems. This includes routing to a local subsystem, and performing network management when a local subsystem goes online or offline.

4. Database Audit: This periodically audits the LNP Database to ensure that it has not been altered by unapproved mechanisms, and to ensure that all cards have an identical copy of the LNP Database.

5. LNP related Administration: Support is in place to provision the existing LNP services. Support for provisioning the PLNP service has been added to the existing commands.

6. LNP-related Maintenance: Maintenance supports LNP. This includes reporting the status on the LNP subsystem, and generating alarms, measurements, and UIMs. Minor enhancements have been made to the **REPT-STAT-LNP** command.

   No new alarms are introduced for this feature. Although no new measurements or UIMs have been defined, measurements for PLNP will be maintained and reported separately from other LNP query services.

7. LSMS and the LSMS↔EAGLE interface: No impact on these functions.

PLNPQS Details

All the LNP query messages for call completion to ported number received by EAGLE are processed by PLNPQS. PLNPQS receives queries from the subsystem management task, and implements the processing to parse the query, perform the lookup, and generate the response.

LNP Query is performed as follows:

1. The message arrives at EAGLE.

2. If global title is required, and the translation type is PLNP, the data is routed to the local LNP query subsystem and Site ID True Point Code (SID and SS_APPL tables). Only one LNP subsystem exists for all LNP query processing. If SID/SS_APPL data has not been administered, a UIM is generated and the message is discarded.

3. If global title is not required, the message is routed to the appropriate destination, local subsystem if the EAGLE DPC and SSN are the destination, MTP routed for others.

PLNPQS Query Verification

This section shows the process used by EAGLE, as part of PLNPQS, to verify a PLNP query.

A summary of the verification follows.

PLNP will verify the following values in the MTP and SCCP part:

1. MSU is ANSI national, and point codes are national

2. MSU is SCCP UDT message

3. MSU is SCCP Class 0

4. GTI is 0010 when rt-on-gt, or 0000 when rt-on-ssn

5. TT is the provisioned PLNP TT value

6. PC of originating SSP is in route table, extract PC and SSN for use in the response

7. Length of user part sufficient to hold minimum TCAP part

PLNP will verify the following values in the TCAP part:

1. TCAP package is Query with Permission

2. TCAP package length fits within SCCP user part

3. TCAP transaction ID present, and length = 4, extract value for use in the response

4. Component sequence ID present, and length valid

5. Invoke Last component present, and length valid, extract Invoke ID for use in the response

6. PCS ProvideInstructions:Start operation code present
7. Digit ID parameter, Called Party Number present
8. Calling Party Number, LATA, and ORG station are present

PLNPQS Query Decoding

This section shows the process used by EAGLE to decode a PLNP query. The process is identical to the existing EAGLE implementation to decode IN queries, except that:

- the numbering plan for this query is E.164, rather than E.163
- the dialed number must be exactly 10 digits, rather than at least 10

PLNP will verify the following values in the TCAP part:

1. TCAP length valid
2. Parameter Set present, and length valid
3. Service Key present, and length valid
4. Digit ID parameter, Called Party Number is present, length is valid, and the following applies:
    - Type is National
    - Encoding is BCD
    - Numbering Plan is ISDN (E.164)
    - 10 digits present
    - Each digit is correctly encoded (BCD value is 0 to 9, inclusive)

PLNPQS Query Response Generation

PLNPQS response messages can be of the following types: normal messages and error messages.

Normal Responses

This section shows the fields filled in by EAGLE for a "normal" response to a PLNP query. The normal response is sent when the query passes verification and decode, and an LNP database lookup is performed.

Normal responses are identical to the existing EAGLE LNP implementation for IN query/response, except that the numbering plan used for the query and response will be E.164 (ISDN), rather than E.163 (Telephony).

The Routing Number in the normal response is filled in as follows:

- if the database lookup succeeds and returns an LRN, the Routing Number in the response is set to the LRN value (i.e. the DN refers to a ported number).

- if the database lookup fails (i.e. the number is not ported), the DN value from the query is used as the Routing Number in the response.

The normal PLNP response is required to include the Digits(Carrier), and Billing Indicators parameters. These parameters are not essential for number portability, but are mandatory parameters for the response. Each will be set to a benign filler value, as shown in the template.

Error Responses

MTP and SCCP level error responses are unchanged from the existing EAGLE implementation.

The general rule for error responses are as follows:

- Protocol errors in the component portion (incorrect package or component) are reported with a Reject component in a Response package

- Command errors (where the query completed with an error, though the command was received correctly) are reported with a Return Error component in a Response package

Error handling for PLNP will come into play once a message is routed to the PLNPQS for handling as a PLNP request.

Upgrade Considerations

Adding additional measurements to support the feature will result in the SCCP maintenance block being modified. During upgrade, OAM must support the old and new version at the same time. During an upgrade back out, the SCCP card must support polling for the old version.

Since this feature does not change any DMS tables, no table conversion will be required.

All SCCP cards must be upgraded to the release that contains PLNP prior to provisioning the PLNP service.

Limitations

1. When the PLNP feature is enabled, and the PLNP service is provisioned, it is not possible to route PLNP queries arriving as Route on GT to an external node. All Route-on-GT PLNP queries will be processed locally under these conditions. This means that customers will not be able to split processing of PLNP queries across multiple network elements.

   The product is implemented in this manner in order to retain backward compatibility with the current LSMS product. Rather than utilizing the LSMS to provision PLNP service on a per NPA-NXX basis, the PCS query service is enabled/disabled for all messages.

2. Due to limitation 1, when the LNP database is unavailable, EAGLE will return an error response without performing LNP. Network management for these LNP queries will be used to divert future traffic. A summary of the network management response is shown in **Table 5-1** .

Table 5-1. Response When PLNP Is Unavailable

Query MSU Routing Indicator	DPC	Message Handling	Network Management
Rt-on-gt	True point code	generate UDTS	Send UPU
	Capability point code	generate UDTS	Send TFP concerning EAGLE's CPC
Rt-on-ssn	True point code	generate UDTS	Send SSP to OPC concerning DPC
	Capability point code	generate UDTS	None.

3. PLNP only supports ANSI messages.

4. There is no Automatic Code Gapping (ACG) for PLNP. Excessive PCS query messages can cause ACG to be initiated for AIN and IN queries, potentially starving out those services if the excessive PCS query messages continue to be sent to EAGLE.

5. Message Relay is not supported for messages which use the PLNP Translation Type.

PDBA Proxy (EPAP 7.0)

Description

The EPAP PDBA Proxy feature provides a more reliable connection to the EPAP PDBA in the event of a failure of the active PDBA. Connection redundancy is accomplished by allowing the customer's provisioning system to still use a single IP address, even though the connection may logically be to the previously standby PDB.

During normal provisioning operations, one PDBA is active and the other PDBA is in standby. However, from the customer's provisioning system perspective, the active and standby PDBAs are accessible through a single IP address. If the active PDBA fails, the local EPAP B box will forward provisioning updates to the mated PDB.

When the previously active PDBA recovers, it is aware that the standby PDBA has become active and now both active PDBAs need to be reconciled.

The advantages this feature provides are:

1. The customer's G-Flex network can absorb a single EPAP failure and automatically transfer provisioning to the standby PDBA using the same IP address.

2. A means of reconciling both active PDBAs when the failed PDBA becomes available again.

Limitations

1. The EPAP PDBA Proxy feature cannot be installed on a non-provisionable site.

2. This feature does not require the ADR feature.

3. This feature only provides Virtual IP functionality when the EPAP-A fails.

4. Failure of the network connection to both EPAP A and B, or similar failures that take down both devices require the customer's provisioning system to manually connect to the standby PDB's IP address.

Performance Enhancements (IP^7 Release 3.0)

The Performance Enhancements feature provides a set of rules for specifying DCM throughput under different configurations. This feature touches on a wide variety of IP ^{7} Secure Gateway system and application issues.

Primary Aspects

The following items can be considered primary aspects of the Performance Enhancements feature:

- Maximum application capacity per DCM is increased to 3000 MSUs per second, with limitations.
- DCM communications processor MSU throughput capacity is increased to 5000 per second.
- The software-imposed limit to maximum TVG request rate is increased to 5000, which requires a limit on active cards present in the system.
- Application performance is enhanced through the use of Nagle's algorithm on all sockets. For more information on Nagle's algorithm, see "Nagle's Algorithm" .
- Application performance is enhanced through optimizations in the use of shared memory.
- The **msucount** pass-through maintenance command, used with the **pass** command, is enhanced to provide values for average MSUs per second transmitted and received over a period of time.

Secondary Aspects

The following items can be considered secondary aspects of the Performance Enhancements feature:

- The TCP/IP stack is modified such that the timer used for Nagle's algorithm has a much lower time-out, such as 25 milli-seconds rather than 200 milli-seconds.
- Socket message flow control is modified for the higher capacity.
- TCP re-transmissions at the higher capacity is addressed by increasing socket buffer size from 8 kilo-bytes to 16kilo-bytes.
- The card-level congestion control algorithm is modified for the higher capacity.
- The change-over/change-back control algorithm is modified for the higher capacity.

Limitations Summary

Achievement of the maximum application capacity of traffic requires the following:

- No more than 150 active cards may be present in the system.
- Average MSU size of application traffic must be no greater than 120 octets.
- STPLAN copy on outbound messages is not supported at the capacity rate of traffic, but is still supported at rates up to 2000 MSUs per second.
- Nagle's algorithm must be enabled for all traffic-carrying sockets.

Per-Linkset Random SLS (Release 36.0)

Description

The Per-Linkset Random SLS (Signaling Link Selection) feature is an enhancement of the existing Random SLS Generation feature, to allow the user to apply Random SLS generation on selected linksets instead of system-wide to all linksets. The Per-Linkset Random SLS feature provides an STP option that can help to resolve load balancing problems on specific linksets without affecting the entire routing scheme of the EAGLE 5 ISS.

The EAGLE 5 ISS uses the Random SLS option to decide if it has to generate a new SLS value. This randomly generated SLS value is used to select an outgoing linkset and a link to achieve load balancing. Linkset provisioning is enhanced to allow configuring of specific linksets for Random SLS generation.

To use the feature in an upgraded system that has the Random SLS option set to CLASS0 or ALL, the operator must provision the individual linksets and per-linkset options appropriately before changing the STP option to function per linkset.

The Per-Linkset Random SLS feature can operate on both ITU SCCP Class 0 and ITU SCCP Class 1 traffic. The Per-Linkset Random SLS feature allows each linkset to inherit all the options related to SCCP Class 0 and Class 1 traffic that are currently available for the Random SLS Generation feature.

Hardware Requirements

None

Limitations

Different Per-Linkset Random SLS configurations on two linksets that are part of a combined linkset for the routes defined for a destination node might result in undesired SLS distribution. The EAGLE 5 ISS does not prompt or reject the linkset provisioning command if provisioning will result in an undesired SLS distribution.

Persistent Device States (Release 29.0)

Description

This feature provides persistent states for supported EAGLE card, terminal, signal link and TCP/IP link devices. This capability makes it unnecessary to manually log device states prior to an **init-sys**, and retains the OOS-MT-DSBLD device state during an OAM switchover. Supported devices are cards, terminals, SS7 signaling links and TCP/IP data links.

During the **init-sys** process, the OAM will restore supported devices to their maintenance states, resulting in an initialized and configured EAGLE. Non-supported devices continue to be processed using the current method.

This feature presents a very efficient mechanism to restore an EAGLE to its pre-init-sys state. This **init-sys** aspect of the feature is controlled by a system wide "restore device" option administered by the craftsperson with the **chg-stpopt** command. Turning off this option causes the current init-sys processing to occur.

NOTE: The default value for this option remains OFF.

With this feature, faster standby-to-active recovery during a switchover operation are possible, since device states are maintained on the standby MASP, and do not require craftsperson intervention following initialization. Disabled or inhibited devices retain their state, provided the PDS data is valid. Otherwise, current switchover processing occurs, and devices may be driven to their default state.

Hardware Requirements

No new hardware is needed to support this feature.

Limitations

Persistent state data will not be maintained on the standby MASP, in the case of different version numbers for the PDS tables in the active and standby MASPs. The PDS table version changes only if there are new devices supported by the PDS, or more information is added to the table for the supported devices.

Point-to-Point Connectivity for ITU Point Codes (IP^7 Release 2.2)

Description

The **iplimi** application provides the same functions for International Telecommunications Union (ITU) point codes as the **iplim** application provides for American National Standards Institute (ANSI) point codes, with the exception of any functions that are supported only by ANSI protocols. (Full Restart, Partial Restart, Adjacent Restart, False Link Congestion, and Circular Routing Detection are ANSI-only features.)

Each **iplimi** link provides one point-to-point connection either to an international ITU network node (ITU-I) or to a national ITU network node (ITU-N) for the purpose of carrying SS7 traffic over a TCP/IP network. These links:

- Can be added to a multiple-link linkset in which the other links can be either **iplimi** links or links of another type, such as **css7itu**.
- Fully support SS7 changeover and changeback procedures, including retrieval.
- Have the standard SS7 restriction of 16 links per linkset.

Mixed Networks Using the ANSI/ITU Gateway Feature

If you have also installed the ANSI/ITU Gateway feature (previously available for SS7 networks only), the addition of the **iplimi** application enables the IP ^{7} Secure Gateway to use the ANSI/ITU Gateway feature for IP networks as well. Using these features enables IP ^{7} Secure Gateway to act as an interface between nodes that support ANSI, ITU-I, and ITU-N protocols. **Figure 5-1** shows an example of a complex network that includes all these types of nodes. **Table 5-2** provides more detail about the nodes, network types, and point codes used in this example.

The following SS7 protocol constraints determine how the network must be configured:

- A linkset is a group of links that terminate into the same adjacent point code. All links in the linkset can transport compatible MSU formats. The network type of the linkset is the same as the network type of the adjacent point code assigned to the linkset.
- When nodes in different networks need to communicate, each node must have either a true point code or an alias point code for each of the network types. For example, if Node 1 (in an ANSI network) needs to communicate to Node 7 (in an ITU-N network), Node 1 must have an ANSI true point code and an ITU-N alias point code, while Node 7 must have an ITU-N true point code and an ANSI alias point code.
- STPs are usually deployed as mated pairs. The links connecting the STP to its mate are C links. Each STP must have a C linkset for each network type that the STP connects to. Therefore, in **Figure 5-1** , Nodes 5 and 6 are connected with three linksets, one each for ANSI traffic, ITU-I traffic, and ITU-N traffic.
- To perform routing, the IP ^{7} Secure Gateway must convert the routing labels in MSUs. To perform this conversion, every destination point code (DPC), originating point code (OPC), and concerned point code must be defined in the routing table. Even if the IP ^{7} Secure Gateway does not route MSUs to these nodes, they must be provisioned in the routing table to provision the alias point codes required in the conversion process.

Figure 5-1. Complex Network with ANSI, ITU-I, and ITU-N Nodes

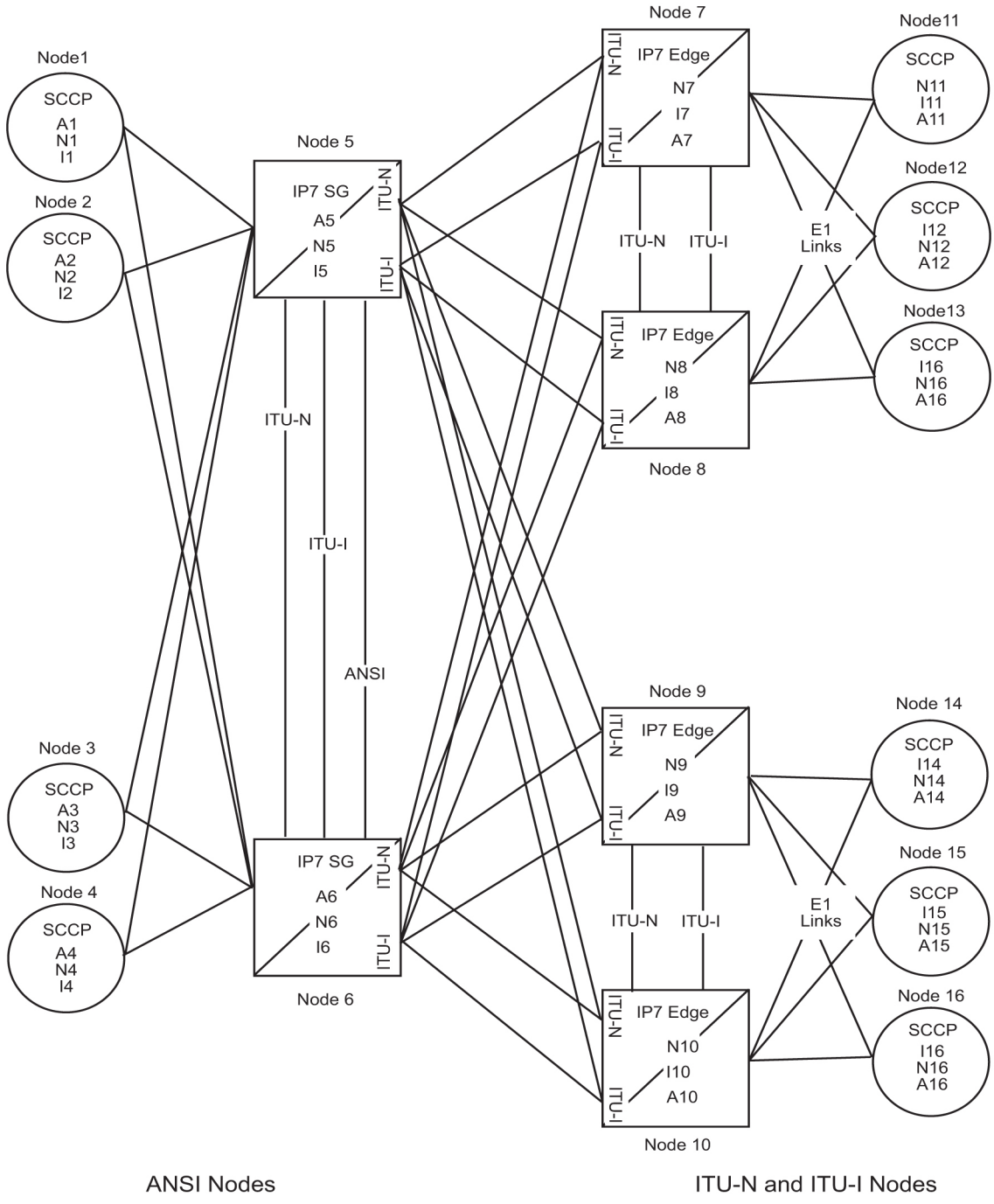


Table 5-2. Nodes and Point Codes in Complex Network Example

Node	Node Type	Network Types Supported	True Point Codes[1]	Alias Point Codes[2]
1	SSP	ANSI	A1	N1, I1
2	SSP	ANSI	A2	I2

Node	Node Type	Network Types Supported	True Point Codes[1]	Alias Point Codes[2]
3	SSP	ANSI	A3	N3, I3
4	SSP	ANSI	A4	N4
5	STP (with IP 7)	ANSI, ITU-N, ITU-I	A5, N5, I5	
6	STP (with IP 7)	ANSI, ITU-N, ITU-I	A6, N6, I6	
7	STP (with IP 7)	ITU-N, ITU-I	N7, I7	A7
8	STP (with IP 7)	ITU-N, ITU-I	N8, I8	A8
9	STP (with IP 7)	ITU-N, ITU-I	N9, I9	A9
10	STP (with IP 7)	ITU-N, ITU-I	N10, I10	A10
11	SSP	ITU-N	N11	I11, A11
12	SSP	ITU-I	I12	N12, A12
13	SSP	ITU-I	I13	N13, A13
14	SSP	ITU-N	N14	I14, A14
15	SSP	ITU-I	I15	N15, A15
16	SSP	ITU-I	I16	N16, A16

Notes:

1. A true point code(TPC) defines a destination in the IP7 Secure Gateway's destination point code table.ATPC is a unique identifier of anode in a network. Each Signal Transfer Point(STP) must have a TPC for each network type that the STP connects to. Each Service Switching Point(SSP) connects to only one type of network, so it has only one TPC.

2. An alias point code is used to allow nodes in other networks to send traffic to and from an STP or SSP when the STP or SSP does not have a TPC for the same network type.

The many configured links and point codes in the complex network shown in **Figure 5-1** allows most nodes to communicate with other nodes. However, note that Node 2 cannot communicate with Node 13 or Node 16 because Nodes 13 and 16 do not have ANSI alias point codes.

Routing and Conversion Within a Single Network Type

The following steps demonstrate how an IP 7 Secure Gateway routes and converts MSUs that one ITU-N node sends to another ITU-N node. For example, assume that Node 11 in **Figure 5-1** sends an MSU to Node 14. The MSU is routed from Node 11 to Node 7 to Node 5 to Node 9 to Node 14. The following steps describe the actions performed at Node 5 (an IP 7 Secure Gateway):

1. An ITU-N formatted MSU (which has a network identifier (NI)=10b and a 14-bit destination point code/ originating point code) is received on an **`iplimi`** card (for this example at location 1103).

2. MSU discrimination is performed with the following substeps:

a. Compare the received network identifier (NI) to the list of valid NIs. (Each configured linkset for a receiving link has a defined list of valid NIs.) If the comparison fails, the MSU is discarded and an STP measurement is logged. In this example, the received NI (10b) is valid for an **iplimi** card.

b. Extract the NI and destination point code (DPC) from the received MSU.

c. Determine whether the destination of the received MSU is this STP. If not (as is the case in this example), the MSU is passed to the STP's routing function.

3. The routing function selects which outgoing link to use by searching a routing table for an entry for the DPC (N14 in this example). The routing table identifies another **iplimi** card (for this example at location 1107) to be used for the outgoing link.

4. Determine whether MSU conversion is required (required when the source network type is not the same as the destination network type). In this example, both Node 11 and Node 14 are ITU-N nodes, so conversion is not required.

5. Forward the MSU across the Interprocessor Message Transport (IMT) bus from location 1103 to location 1107, where the MSU is transmitted out the link towards Node 14.

Routing and Conversion Between Different Network Types

The routing and conversion steps performed by an IP ^{7} Secure Gateway when an ITU-N node sends an MSU to an ITU-I node are the same as the steps shown in Routing and Conversion Within a Single Network Type , except for the conversion step.

For example, assume that Node 11 in **Figure 5-1** sends an MSU to Node 16. The MSU is routed from Node 11 to Node 7 to Node 5 to Node 9 to Node 16. The following steps describe the actions performed at Node 5 (an IP ^{7} Secure Gateway):

1. Perform steps Item 1 through Item 3 as shown in Routing and Conversion Within a Single Network Type . In this example, assume that the routing function determines that the outgoing link is configured on the DCM card at location 1203.

2. Determine whether MSU conversion is required (required when the source network type is not the same as the destination network type). In this example, Node 11 is an ITU-N node and Node 16 is an ITU-I node, so conversion is required. Conversion consists of two phases: Message Transfer Part (MTP) conversion and user part conversion.

3. Perform MTP conversion (also known as routing label conversion). The following parts of the MSU can be affected by MTP conversion:

   - Length indicator—for ITU-N to ITU-I conversion, the length of the MSU does not change
   - Service Information Octet (SIO), Priority—for conversion to ITU, the priority is set to 0. For conversion to ANSI, the priority is set to a default of 0, which can later be changed based on user part conversion.
   - Service Information Octet (SIO), Network Indicator—the NI bits are set to the NI value for the destination node. In this example, NI is set to 00b.

- Routing Label, Destination Point Code (DPC)—the DPC is replaced with the destination's true point code. In this example, N16 is replaced by I16.
- Routing Label, Originating Point Code (OPC)— the OPC is replaced with the appropriate network type's alias point code for the originating node. In this example, N11 is replaced with I11.
- Routing Label, Signaling Link Selector (SLS)—no SLS conversion is required between ITU-I and ITU-N nodes. However, if one of the nodes were an ANSI node, conversion would be required between a 5-bit or 8-bit SLS for ANSI nodes and a 4-bit SLS for ITU nodes.

4. Perform user part conversion, if necessary. Currently, only SCCP traffic and network management messages have additional conversion. All other user parts have their data passed through unchanged.
5. Forward the MSU across the Interprocessor Message Transport (IMT) bus from location 1103 to location 1203, where the MSU is transmitted out the link towards Node 16.

Portability Check for Mobile Originated SMS (Release 29.1)

Description

In GSM networks, when a mobile subscriber sends a short message, or Mobile Originated Short Message Service message (MO SMS), using his or her handset, the message is first deposited in a Short Message Service Center (SMSC). This SMSC is then responsible for determining where the intended recipient, who is also a mobile subscriber, is located. The SMSC accomplishes this by querying the Home Location Register (HLR) of the recipient to determine which Mobile Switching Center (MSC) the subscriber is currently on. Once the location is determined, the SMSC sends the SMS to the recipient.

In a portability environment, this could lead to problems. The SMSC address to which a message is routed is programmed into the GSM mobile handset. When a subscriber ports to another network, the handset is reprogrammed with the SMSC address for the new network. However, the subscriber could then change this address back to the address from his old network. This would cause SMS to be incorrectly sent to the subscriber's old network SMSC, rather than to the new network SMSC. Since the old network would not have billing records for the ported-out subscriber, the subscriber essentially would receive free SMS service.

The Portability Check for Mobile Originated SMS (MNP SMS) feature is designed to prevent such a possibility from occurring. With this feature, the EAGLE filters incoming messages based on MAP Operation Code. If the message is a MO Forward Short Message (MO FSM), the originating subscriber's Mobile Subscriber Integrated Services Digital Network (MSISDN) number (i.e. phone number) is used to search the G-Port Mobile Number Portability database.

If a match is found, indicating the subscriber has been ported-out, the EAGLE uses the destination SMSC address obtained from the SCCP CdPA to search a list of "home network" SMSC addresses. If a match is found, indicating the ported-out subscriber is attempting to send a short message using the old network's SMSC, the message is discarded. An error message is then generated and returned to the originating MSC.

When the MNP SMS feature is on, the EAGLE performs the following functions:

1. EAGLE receives a UDT message.
2. Checks if the service selector matches G-Port. If so, continues to Step 3; else goes to step 16.

3. Checks if the CdPA SSN matches one of the SSNs provisioned with object type as MSC. If so, continues with Step 4. If the CdPA SSN matches one of the SSNs provisioned with object type as HLR, then proceeds to step 17; else goes to Step 11.

4. Checks if the message is a MO Forward Short Message (MO FSM). If so, it continues to step 5; else go to step 11.

5. Checks if PPSMS feature is ON. If so, goes to step 12; else continues with Step 6.

6. Checks if MNPSMS feature is ON. If so, continues to step 7; else goes to step 11.

7. The originating subscriber's Mobile Subscriber Integrated Services Digital Network (MSISDN) number (i.e. phone number) is used to search the G-Port Mobile Number Portability database. If MSISDN Number is found in the PDB/DN table, continue to step 8; else goes to step 11.

8. Checks the portability type of the subscriber. If it matches "Ported-out/ Not Known/ FNPTFN" then continues to step 9. If portability type is "Prepaid-1/Prepaid-2," goes to step 11.

9. Uses SCCP CdPA Address to search the list of "home network" SMSC addresses. If a match is found, indicating the ported-out subscriber is fraudulently attempting to send SMS using the old network's SMSC, then continues to step 10; else goes to step 11.

10. The message will be discarded, UIM #1129 is printed, and an error message generated and returned to the originating MSC. Go to Step 19.

11. It's a fall-through case. Continue with Normal GTT processing: go to step 19.

12. Checks if message is from one of the IN Platforms (PPSMS Servers). If so, goes to step 18; else continues with step 13.

13. The originating subscriber's Mobile Subscriber Integrated Services Digital Network (MSISDN) number (i.e. phone number) is used to search the G-Port Mobile Number Portability database. If MSISDN Number is found in the PDB/DN table, continue to step 14; else go to step 11.

14. Checks the portability type of the subscriber. If it matches "Prepaid1/Prepaid2," go to step 18; else continue with step 15.

15. If the subscriber portability type is "Ported out / FNPTFN/ Not Known" and MNP SMS feature is also ON, goes to step 9; else goes to step 11.

16. Exits from MNP SMS feature functionality and continues with existing processing for other services or GTT.

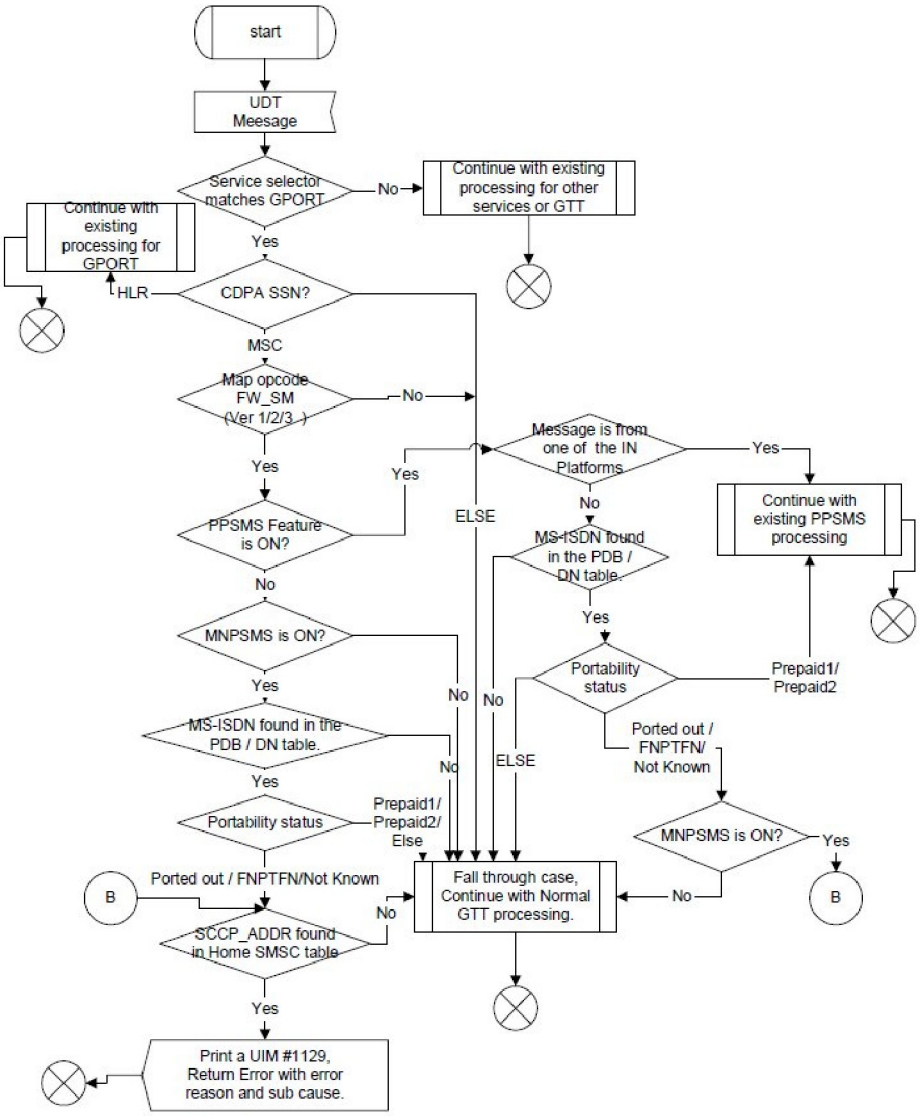
17. Exits from MNP SMS feature functionality and continues with existing processing for GPORT.

18. Exits from MNP SMS feature functionality and continues with existing processing for PPSMS.

19. Exits MNP SMS feature functionality.

The following figure illustrates these functions.

Figure 5-2. Flowchart of MNP SMS Functions



Hardware Requirements

No new hardware is needed to support this feature.

Prepaid Initial Detection Point Query Relay (Release 34.1)

Description

The purpose of the Prepaid Initial Detection Point (IDP) Query Relay feature is to provide a mechanism to insure that prepaid subscribers are accurately charged for their calls in a portability environment.

This feature allows the EAGLE 5 ISS to intercept the SCP number portability database query from the MSC, perform the portability check on the called number, insert the portability information (i.e. Routing Number or HLR Address), and forward the IDP query to a prepaid SCP for processing. When the SCP receives the IDP query, it will have all of the information it needs to accurately charge for and process the call.

For message discrimination on DSM cards, the IDP Relay feature uses the service selector (SRVSEL) framework already present in the EAGLE 5 ISS..

Not all messages for the IDP Relay service will have their outgoing TCAP DN conditioned.

The IDP Relay feature performs the following filters and checks on the intercepted messages to verify that the:

- Service selected is the IDP Relay (**:srvsel=idpr**) service.
- MSU has the ITU TCAP package
- MSU opcode = IDP
- SCCP/TCAP/INAP are successfully decoded
- SK and event BCSM parameters are present and decoded correctly
- CDPN or CDPN (BCD) parameter is present and decoded correctly
- SCCP CDPA exists in the common screening GTA list for the IDP Relay feature
- SK+BCSM exists in the common screening SKBCSM list for the IDP Relay feature
- Number condition of the TCAP is successful based on Table *ID Relay Number Conditioning*..
- Conditioned TCAP DN prefix match exists in the common screening CCNDC list for the IDP Relay feature.
- Prefixnum=4 in the Prefix table and , the SCCP CGPA is checked for a default country code (DEFCC) match.
- Conditioned TCAP DN is found in the RTDB single/ Range table with either an SP or RN entity type.
- Based on the Prefixnum=1, 2, 3, the outgoing TCAP DN is conditioned. See for more details.
- The message is forwarded to the GTT handling based on the original incoming SCCP CDPA.

Table *IDP Relay Number Conditioning* shows the number conditioning performed on the incoming TCAP DN for the IDP Relay feature.

Table 5-3. IDP Relay Number Conditioning

Incoming Address			**Number Conditioning**	**Outgoing Address**	
TCAP DN NAI	**Perform SCCP CGPA DEFCC Check?**	**TCAP DN Format**		**NAI**	**Format**
International	No	<CC><DN>	None Do RTDB Lookup	If PFX3=unknown NAI=unknown	<PFX1><CC><RN><DN>

Incoming Address			Number Conditioning	Outgoing Address	
TCAP DN NAI	**Perform SCCP CGPA DEFCC Check?**	**TCAP DN Format**		**NAI**	**Format**
				Else NAI=International	
National	If PFX4=On	<DN>	Add DEFCC Do RTDB Lookup	If PFX3-unknown NAI-unknown Else NAI=National	<PFX2><RN><DN>
Unknown	No	<IEC><CC><DN>	CSL Delete prefix found, (P1=International), remove it Do RTCB Lookup	NAI=unknown	<IEC><CC><RN><DN>
Unknown	If PFX4=On	<NEC><DN>	CSL delete prefix found, (P1=International), remove it Do RTCB Lookup	NAI=unknown	<NEC><RN><DN>
Unknown	If PFX4=On	<DN>	No CSL delete prefx found, ADD DEFCC Do RTDB Lookup	NAI=unknown	<RN><DN>

NOTE: See the Glossary for a list of terms and acronyms used throughout this document.

Common Screening List

Common Screening Lists are used for screening messages in various features. The IDP Relay feature can screen up to 4 Common Screening Lists.

The Common Screening List lists supported by this command are not considered part of Gateway Screening or GSM MAP Screening.

One or more Common Screening Lists may be associated with a particular feature. Table Sumary of CSL-supported Features. lists each supported feature, the associated screening list names, and other details about the entries that are supported.

Table 5-4. Summary of CSL Supported Features

Feature Name	Screening List Name	Card Type	Parameter	Maximum Number of Entries	Range of Values
Prepaid IDP Query Relay	GT	DSM	DS	50	1 to 15 digits [0-9, a-f, A-F] or none
Prepaid IDP Query Relay	CCNDC	DSM	DS	20	1 to 6 digits [0-9, a-f, A-F] or none
Prepaid IDP Query Relay	SKBCSM	DSM	DS	25	4 digits [0-9, a-f, A-F] or none
Prepaid IDP Query Relay	DELPFX	DSM	DS	10	1 to 5 digits [0-9, a-f, A-F] or none
Prepaid IDP Query Relay	DELPFX	DSM	P1 (National / International)	10	1 digit [0-1], where: 0:= National , 1:= International

Hardware Requirements

The IDP Relay feature cannot be enabled if Application Services Module (ASM) cards or TSM cards are in the system, or if SCCP gpls are entered in the system.

The IDP Relay feature runs on the VSCCP gpl with DSM cards connected to the EPAP. VSCCP GPLs can also be entered once the feature is enabled.

Limitations

The GTT feature must be on before the IDP RELAY feature can be enabled.

The IDP RELAY feature and the LNP feature cannot be enabled at the same time in the system.

```
The IDP RELAY feature cannot be enabled if ASM or TSM cards running the SCCP application are present
in the system.
```

Prepaid SMS Intercept - Phase 1 (Release 28.1)

Mobile operators offering prepaid short message service (SMS) need an efficient way to perform credit checks on the subscriber sending the message, prior to allowing the message to be delivered. Intelligent network (IN) databases are generally used to perform the actual credit check. However, these databases can become overloaded if messages are sent to them for evaluation unnecessarily. An example of such a case is when all short messages, including those from or to contract (postpaid) subscribers, are sent to the IN platform for evaluation. The messages from contract subscribers do not need a credit check; thus this is additional traffic the IN platform must process unnecessarily.

Therefore, additional filtering and screening is needed in the SS7 network to provide a finer granularity in determining which messages actually need to be sent to the IN platform, and which may simply be routed to the SMSC.

The Prepaid SMS Intercept - Phase 1 feature screens incoming messages from MSC based on MAP operation code. If the op-code indicates the message is a MAP_MO_FORWARD_SHORT_MESSAGE (MO_FSM), the sender's MSISDN is retrieved and a database lookup performed. If the MSISDN belongs to a contract subscriber, the message will be routed to the SMSC. If the MSISDN belongs to a prepaid subscriber, the message will be diverted to a third-party IN platform for a credit check before allowing the message to be delivered to the SMSC.

The MAP_FORWARD_SHORT_MESSAGE, referred to as FSM in this document, is a message used to carry a text message (i.e. the "short message") being transmitted from the mobile handset of one subscriber to the mobile handset of another subscriber. In practice, the short message is delivered first to the Short Message Service Center (SMSC) of the sending subscriber. The SMSC is then responsible for sending the short message to the intended recipient. In MAP versions 1 and 2, the FSM message is used for both legs of the delivery. In MAP version 3, a MO_FSM (mobile originated) message is used to deliver the message from the sender to the SMSC, and a MT_FSM (mobile terminated) message is used to deliver the message from the SMSC to the recipient.

Refer to the *Feature Manual - G-Port* for current details on this feature.

Hardware Requirements

No new hardware is needed to support this feature.

Prevention of Congestion from Rerouted Traffic (Release 21.0)

When the status of the route is changed to allowed (when the route was restricted) or restricted (when the route was prohibited), a burst of rerouted traffic can occur on that route, thus congesting the route. To help keep this from happening, the EAGLE in Release 21.0 can control the rate that it broadcasts TFR and TFA messages to adjacent signaling points. This can regulate the amount of traffic the adjacent signaling points can send to the EAGLE when the route becomes allowed or restricted.

The rate that the EAGLE sends the TFR and TFA messages, (the pacing rate), can be configured with the **tfatfrpr** parameter of the **chg-stpopts** command. The value of the **tfatfrpr** parameter is from 0 to 1 second and can be set in 0.1 second intervals. The default value for the **tfatfrpr** parameter is 1 second. A value of 0 for the **tfatfrpr** parameter indicates that the pacing should stop. The pacing of TFR/TCR is stopped and all remaining TFR/TCR are broadcast at once if the current alternate route used to route traffic to the affected point code is in danger of congestion.

The TFA/TCA and TFR/TCR for each affected point code are sent in groups of 20%. For each time period defined by the pacing rate, 20% of the messages that are to be sent to the adjacent signaling points are broadcast to those signaling points.

This feature is applicable only for ANSI signaling links. The pacing is not done towards ITU networks.

If the destination becomes inaccessible or accessible before all of the TFR/TCR messages are broadcast, then the remaining TFR/TCR messages are not sent.

TFA/TFC messages for multiple affected destinations are sent in parallel.

The pacing of TFR/TCR messages is stopped and all remaining TFR/TCR messages are broadcast at once if the current alternate route used to route traffic to the affected point code is in danger of congestion.

The broadcast of TFA/TFR messages sent about X.25 pseudo point codes is controlled by this feature.

Prevention of Link Oscillation (Release 21.0)

A variety of network problems can cause signaling links to oscillate in and out of service causing frequent changeovers and changebacks and excessive network management message generation. If many links simultaneously oscillate, congestion can occur. When the EAGLE begins restoring an out of service signaling link, the EAGLE starts the level 3 T32. If the signaling link fails to return to service before the level 3 T32 timer expires, the EAGLE does not attempt to bring the signaling link into service until the level 3 T32 timer expires. When the level 3 T32 timer expires, the EAGLE attempts to restore the signaling link into service.

The value of the level 3 T32 timer is set with the **chg-l3t** command. The range of values for the level 3 T32 timer is from 60 seconds to 120 seconds. The default value for the level 3 T32 timer is 60 seconds.

The link alignment procedures are not delayed under the following conditions:

1. When a signaling link is manually taken out of service using the **dact-slk** command, the level 3 T32 timer is stopped (if it is running).

2. When the signaling link is brought back into service using the **act-slk** command.

3. When a new signaling link is first aligned.

The level 3 T32 timer can only be assigned to ANSI SS7 linksets and signaling links.

Preventive Cyclic Retransmission (PCR) (Release 20.0)

Preventive cyclic retransmission is one of the two forms of error correction for the SS7 protocol. Basic error correction is the other. Preventive cyclic retransmission is a forward error correction scheme that uses positive acknowledgments to support the forward error correction. Negative acknowledgments are not used for retransmission. PCR is used when the one-way delay on a link is greater than or equal to 15 milliseconds. A typical example is a satellite link.

Each message signal unit transmitted is retained at the transmitting end of the signaling link. Copies of that MSU are transmitted to the receiving end of the signaling link until the transmitting end of the signaling link receives a positive acknowledgment from the receiving end that it has received a good MSU. When the transmitting end of the signaling link has received the positive acknowledgment, the MSU it has retained is discarded.

The PCR feature should be used in the following circumstances:

- When the one-way propagation delay on a signaling link is greater than or equal to 15 milliseconds.

- When the signaling links are established via satellite.

The PCR feature has two modes of operation, normal retransmission and forced retransmission.

Normal Retransmission

The following rules apply to normal PCR:

1. If new MSUs are available, the new signal units are sent.

2. If new MSUs are available and retransmission is occurring, retransmission stops, and the new signal units are sent.

3. If no new MSUs are available to be transmitted, MSUs in the retransmission buffer are retransmitted cyclically.

For this example, assume the following:

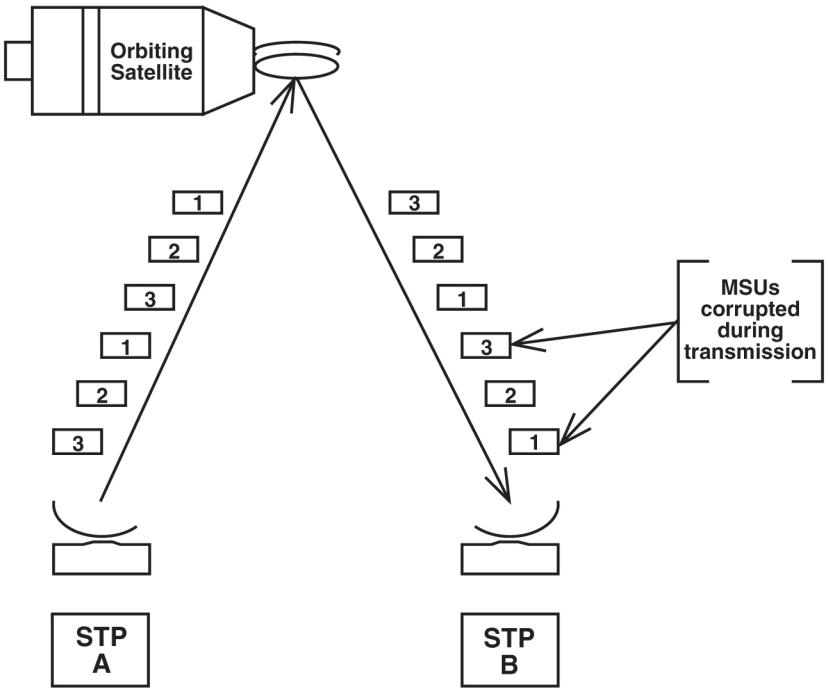
1. There are only 3 new MSUs to be transmitted from STP A to STP B.

2. The transmission buffer is empty.

3. Both STPs are using PCR for error correction.

Figure 5-3 illustrates how normal PCR works.

Figure 5-3. Example of Normal Retransmission with PCR



MSUs 1 through 3 are sent from STP A to STP B and are copied to the retransmission buffer. During transmission, packets 1 and 3 are corrupted before reaching the remote STP B.

STP A knows to retransmit the MSUs in the retransmission buffer since no new MSUs are available. **Figure 5-3** shows several more copies of packets 1 through 3 are retransmitted.

On the receiving side, STP B receives the corrupt MSUs and discards them. Since PCR is used, STP B does not send a negative acknowledgment to STP A. STP B knows that more copies of the packets are arriving.

Under normal conditions, when no message signal units are to be transmitted or cyclically retransmitted, FISUs are sent. In some particular cases, LSSUs, continuous FISUs or flags may be sent.

Example of Basic Error Correction vs. PCR

Figure 5-4 illustrates how PCR outperforms basic error correction when a link experiences a long transmission delay. Assume the delay between the EAGLE and the SSP is 1 second for both basic error correction and PCR. The MSU size is 50 octets, and the transmission speed is 64 Kbps.

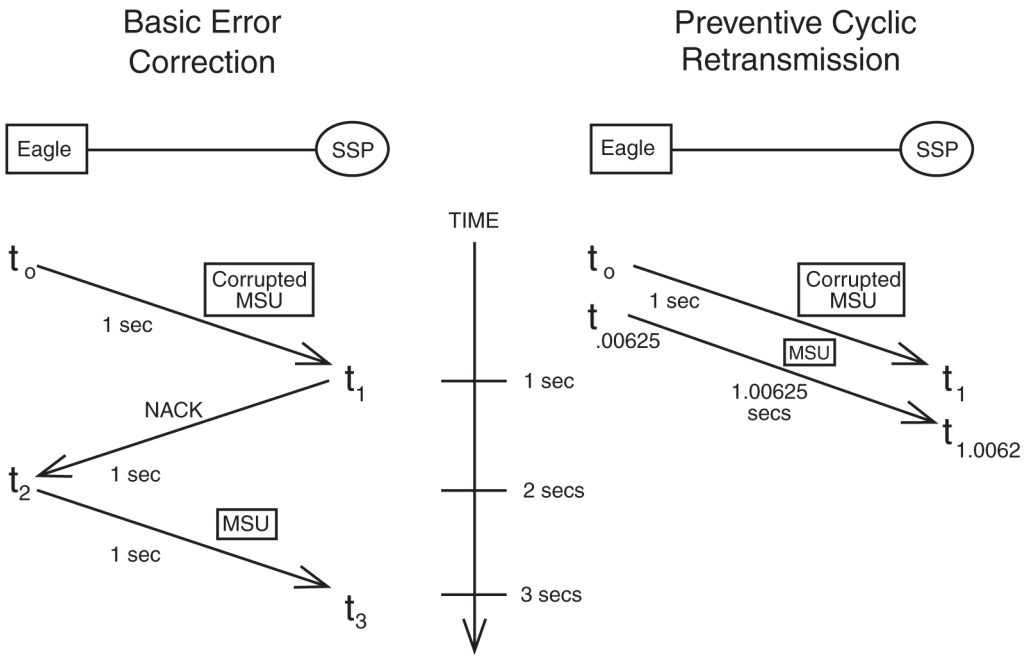
Examine the Basic Error Correction side of the figure. An MSU is sent from the EAGLE to the SSP.

During transmission, the MSU is corrupted. The EAGLE is notified two seconds later that it needs to retransmit the signal unit. Another second later, the valid MSU is received by the SSP. The total amount of time is 3 seconds.

Examine the PCR side of Figure 5-4 . An MSU is sent from the EAGLE to the SSP. During transmission, the MSU is corrupted. Since PCR error correction is used, a negative acknowledgment is not sent. The receiving end knows that another copy is coming. The corrupted MSU arrives at the SSP in 1 second, and the valid MSU arrives 0.00625 seconds later. The total time is 1.00625 seconds. This formula is used to calculate the time interval between the first MSU's arrival and the second MSU's arrival.

$$\frac{8\ \text{bits}}{1\,\text{octet}} \times \frac{1\,\text{second}}{64000\ \text{bits}} \times 50\ \text{octets} = .00625\ \text{seconds to generate another MSU}$$

Figure 5-4. Basic Error Correction vs. PCR



Forced Retransmission

To complement preventive cyclic retransmission, the message signal units available for retransmission are retransmitted with priority when a threshold of outstanding MSUs or a threshold of the number of message signal unit octets available for retransmission has been reached. This is forced retransmission.

With PCR, two thresholds are continuously monitored. These thresholds are the number of message signal units available for retransmission, N_1, and the number of message signal unit octets available for retransmission, N_2.

If the N_1 or N_2 value reaches its threshold, no new message signal units or fill-in signal units are sent, and forced retransmission begins. MSUs in the retransmission buffer are sent in the same order that they were originally transmitted. Retransmission continues until all of MSUs have been retransmitted.

NOTE: All MSUs are sent even if acknowledgments are received during forced retransmission. After all MSUs have been retransmitted, acknowledgments, if any, are processed, and the N_1 and N_2 thresholds are re-evaluated.

If both the N_1 and N_2 values are below the their respective thresholds, the normal PCR procedure can be resumed.

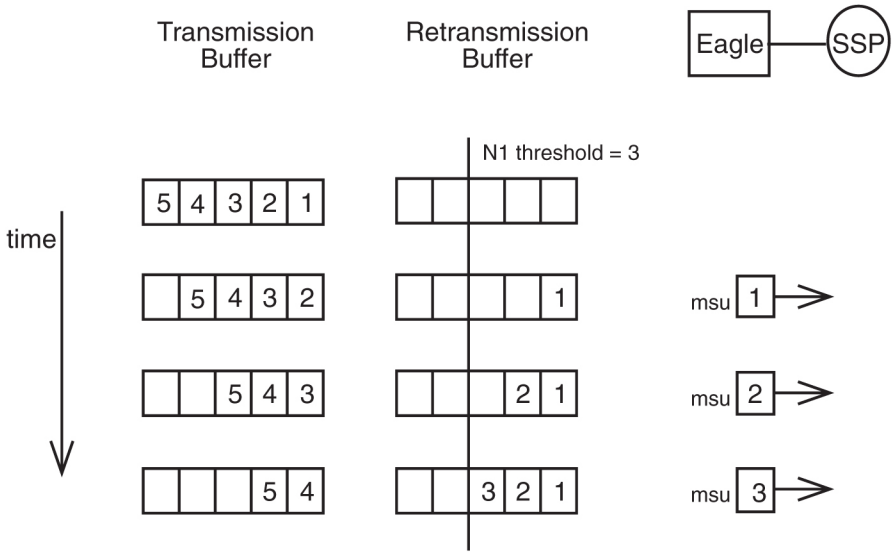
However, if the N_1 or N_2 value is still at its threshold, forced retransmission continues.

Example of Forced Retransmission

The following example shows how forced retransmission occurs. For this example, 5 MSUs are transmitted. Assume the N_1 threshold is 3, and N_2 is 3800 octets. The average MSU size is 50 octets.

Figure 5-5 shows that the EAGLE begins transmitting MSUs to the SSP and copying MSUs to the retransmission buffer.

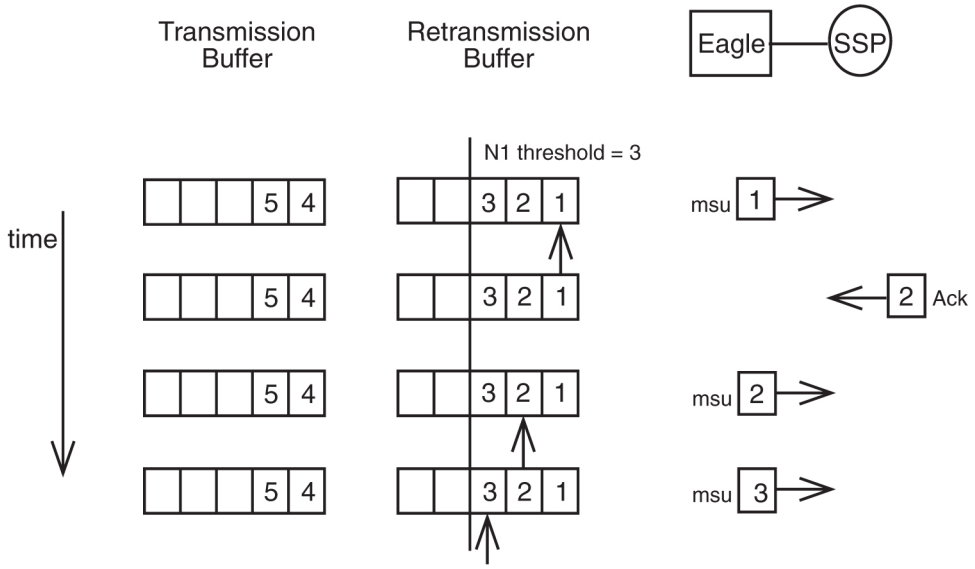
Figure 5-5. Example of Forced Retransmission



At this point, the threshold for unacknowledged MSUs in the retransmission buffer, N_1 has been reached.

Figure 5-6 shows forced retransmission beginning and continuing until all MSUs in the retransmission buffer have been retransmitted.

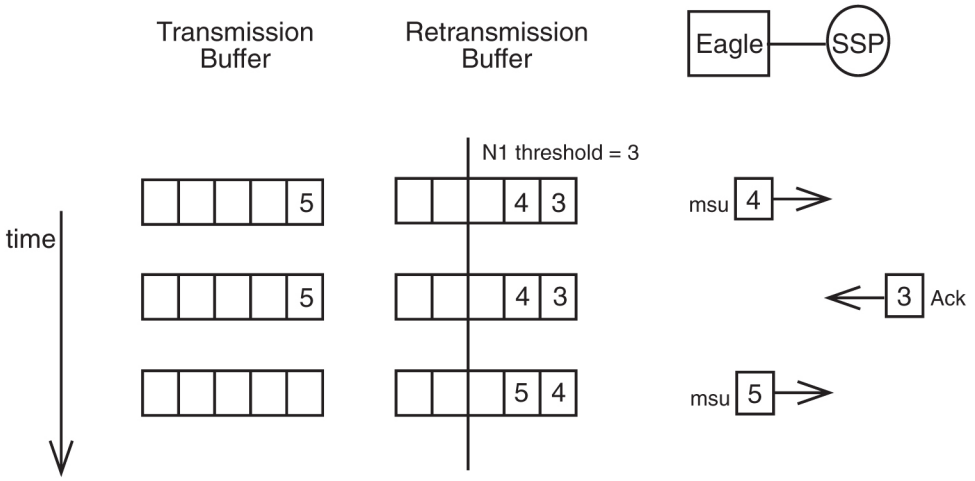
Figure 5-6. Example of Forced Retransmission – All MSUs Retransmitted



An acknowledgment for MSUs 1 and 2 comes in before 2 is retransmitted. This does not affect the retransmission of MSU 2. Forced retransmission dictates that all signal units in the retransmission buffer are retransmitted.

After all MSUs have been retransmitted, N_1 and N_2 are re-evaluated. In this case, acknowledgments for MSUs 1 and 2 have been received; thus, N_1 has been reduced and normal PCR resumes. **Figure 5-7** shows the new MSUs in the transmission buffer being sent.

Figure 5-7. Example of Forced Retransmission – New MSUs Sent

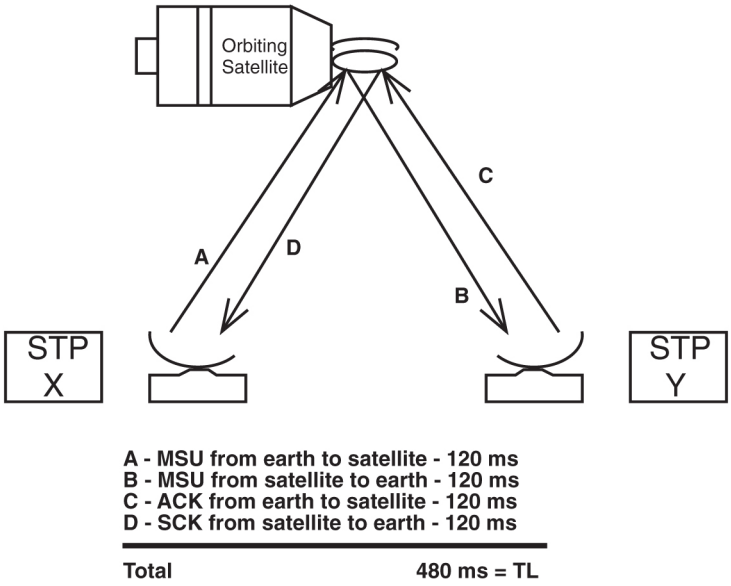


Derivations for N_1 and N_2

The user is responsible for setting the values for N_1 and N_2. The following rules serve as a guide for determining these thresholds.

- N_1 is limited by the maximum numbering capacity of the forward sequence number range which dictates that not more than 127 MSUs can be available for retransmission on 56 Kbps or 64 Kbps signaling links.
- N_2, in the absence of errors, is limited by the signaling link loop delay, T_L. The value of N_2 must ensure that not more than T_L/T_{eb} + 1 MSU octets are available for retransmission.
- T_L is the signaling loop delay, that is, the time between the sending of a message signal unit and the reception of the acknowledgment for this message signal unit in undisturbed operation (see **Figure 5-8**).

Figure 5-8. Determining Value of Signaling Link Loop Delay Timer (T_L)



Assume that T_L = 480 milliseconds or 0.480 seconds. This value is based on a satellite located 22,300 miles above the earth and the signal propagating at a rate of 186,000 miles per second. A minimum of 120 milliseconds are required for a signal to reach a satellite from earth.

- T_{eb} is the emission time of one octet
- Default value for N_1 = 76 outstanding MSUS
- Default value for N_2 = 3800 octets

Table 5-5. Limitations for Various Line Speeds

Channel Speed	T_{eb} = 1 octet / channel speed	(T_L / T_{eb}) + 1 rounded to nearest hundred, T_L = .480 seconds
64 Kbps	1.25 x 10^{-4} seconds	~3800 octets
56 Kbps	1.43 x 10^{-4} seconds	~3400 octets
38.4 Kbps	2.08 x 10^{-4} seconds	~2300 octets

Channel Speed	T_{eb} = 1 octet / channel speed	(T_L / T_{eb}) + 1 rounded to nearest hundred, T_L = .480 seconds
19.2 Kbps	4.17×10^{-4} seconds	~1200 octets
9.6 Kbps	8.33×10^{-4} seconds	~600 octets
4.8 Kbps	1.67×10^{-3} seconds	~300 octets
2.4 Kbps	3.33×10^{-3} seconds	~100 octets

The calculations for the default values assume an average MSU of 50 octets.

Default N_1 calculation:

N_1 = 3800 octets from table above / 50 octets from average MSU = 76 outstanding MSUs

Default N_2 calculation:

$N_2 = T_L/T_{eb} + 1$ = 3800 octets from table above for 64Kbps signaling link.

Priority Processing of Network Management Messages (Release 21.0)

Some of the new protocol features like cluster routing and diversity management have increased the processing complexity of network management functions. Under large failure conditions, it is possible that too many network management functions need to be performed, causing an application processor overload. In the releases prior to release 21.0, if such a condition was encountered, the EAGLE discarded the network management messages regardless of what kind of network management message they were. This method of handling network management messages may have an impact on the network's recovering capability under large scale failure conditions when several critical network management functions must be performed.

This feature provides the capability to prioritize the network management functions to make sure that critical network management functions receive high processing priority under such overload conditions.

During normal operation, the network management functions are processed with equal priority, but the EAGLE closely monitors for excessive unexpected events which may result in an application processor overload. The prioritizing of network management functions is triggered when the application processor overload is experienced on any LIM.

For this feature, the EAGLE collects one measurement, Network Management Messages Discarded due to Network Management Overloading. This measurement collects the number of network management messages discarded when the network management processor overload condition has been reached. Measurements are collected for discarded network management messages at each priority level. This measurement is collected for each signaling link in the system.

The EAGLE generates the following UAMs:

UAMs

- UAM 304 - Network Management Task Priority Discard Threshold Reached (REPT-NMTSK-DSCD) — a minor alarm generated when a network management message is discarded because the application processor of a LIM is overloaded.

- UAM 305 - Recovery from Network Management Task Priority Discard Processing (RECVY-NMTSK-DSCD) — generated when the network management overload condition is cleared.

This feature is applicable only for the ANSI network. Network Management events triggered due to change in status of ITU network elements (links, routes, linksets, destination) are processed on first come first served basis.

Private Point Code (Releases 31.12, 34.0)

Private point codes (PPCs) are used for internal routing within the EAGLE. PPCs may be used for "internal point codes" which are used for the End Office feature, and adjacent point codes for IPGWx linksets. The principle difference between private point codes and non-private is whether the point code is known outside the EAGLE. Point codes within the EAGLE are useful for routing messages within the EAGLE, but when these point codes are non-private, they consume a point code value in the network. By making these point codes private, it is possible to have a point code value indicated as private and still have the same point code value (as not private) available for network configuration.

PPCs must be supported in every supported domain. ANSI, ITU-I, ITU-N, ITUI-Spare, ITUN-Spare, ITUN24 must all support a private version of a point code.

PPCs will be allowed for IPGWx APCs (adjacent point codes). Currently there are special rules for provisioning IPGWx APCs. A special parameter IPGWAPC=YES on the ent-dstn and ent-ls commands allows point codes with otherwise invalid ranges (e.g., ANSI point code 0-0-1) to be used. This parameter also identifies the linkset as one that may only contain IPGWx links. With the implementation of this feature, PPCs will also be allowed for this purpose. The IPGWAPC parameter will remain, however, since not all PPCs are IPGWx APCs.

PPCs will also be allowed for SAPCs on IPGWx linksets. Like IPGWx APCs, SAPCs on IPGWx linksets are not "real" point code, and the network beyond the EAGLE does not need to be aware of them.

PPCs will also be allowed used for the provisioning the End Office feature. In order to support this, PPCs must be allowed for the Remote Application (RMT-APPL) table, and GTT table, in addition to the Destination and Route tables.

Existing Internal Point Codes and IPGW linkset adjacent point codes will not be modified during upgrade. After upgrade, both private and non-private point codes can be used for these purposes.

Note that static routing keys are never needed for RMT-APPL point codes or IPGWx adjacent point codes. For the End Office feature, a true or secondary point code routing key is needed, while for IPGWs adjacent point codes, no routing key is needed.

Limitations

1. This feature does not allow the EAGLE to MTP convert between National and National Spare Point Codes. Likewise, this feature does not allow the EAGLE to MTP convert between International and International Spare Point Codes.

2. In the destination table, an ITU-I alias and an ITU-I Spare alias cannot be defined for the same Point Code, likewise an ITU-N alias and an ITU-N Spare alias cannot be defined for the same point code

3. The feature is not supported on the SEAS interface. Spare point codes are only supported for ITU point codes, and SEAS only supports ANSI point codes. Any Private ANSI point code provisioned using the standard EAGLE command line interface is not displayed by the SEAS VFY- command.

4. ITU National and ITU National Spare Point Code are implemented as separate network domains that can co-exist within the same STP.

5. Spare point codes are not supported for IPGWI sockets using TALI protocols. The spare point code feature may not be enabled if any application sockets have been provisioned on IPGWI cards.

6. The existing implementation of Gateway Screening does not support Group Code (Duplicate Point Codes). Gateway Screening will also not support PPCs.

7. The Spare Point Code and PPC prefix value, s- and p- do not apply to domain type point codes for ANSI and ITU-N24.

8. ITU-N and ITU-N24 Point Codes cannot co-exist as SID Destination True Point Codes and therefore ITU-N Spare and ITU-N24 Point Codes cannot coexist as SID Destination True Point Codes.

9. A single STPOPTS value (cnvcgdi) will be used to control message handling for ITU-I and ITU-I Spare messages when the CgPA PC does not have a required alias

10. A single STPOPTS value (cnvcgdn) will be used to control message handling for ITU-N and ITU-N Spare messages when the CgPA PC does not have a required alias

11. The existing implementation of the SRVSEL command interface to the SRVSEL table does not provide a way to separate MSU traffic for different ITU National Group Code networks. Therefore no provision is made for the SRVSEL command to control the separation of ITU spare and non-spare traffic. The SRVSEL table applies to the EPAP based features G-FLEX, INP, G-PORT, SMS Prepaid, and IS-41 to GSM Migration. Likewise, no provision is made for the GTTSEL command interface to the GTTSEL table to allow separation of ITU spare and non-spare traffic for EGTT, VGTT and MGTT.

Prohibit Removing the Last Route to a Destination if that Destination is being Referenced by Mated Applications or Concerned Signaling Point Code Groups (Release 22.0)

In previous releases when a route was being removed from the database, the EAGLE checked to make sure other routes to the DPC were defined if the DPC of the route was being used by a global title translation. When this condition was detected, the EAGLE issued a message warning that the condition was present, but allowed the route to be removed from the database.

In release 22.0, a new rule has been added to the EAGLE's **dlt-rte** command and the SEAS DLT-RTE command function that does not allow the specified route to be removed from the database if this condition is present. If the user attempts to remove a route under this condition, the command is rejected. On an EAGLE terminal, this error message is displayed.

```
2356 Cmd Rej: Destination referenced by GTT cannot be delete
```

Prohibit the Assigning of a Linkset with Linkset Types A or E to a Cluster Route (Release 22.0)

In previous releases, a user could assign a cluster route to a linkset with a linkset type of either A, B, C, D, or E from both the EAGLE terminal and the SEAS interface. In release 22.0, the only linkset types that can be assigned to a cluster route are B, C, or D. The EAGLE's **ent-rte** command and SEAS ASGN-RTE command function have been changed to allow only these linkset types to be assigned to cluster routes. If the user attempts to assign a cluster route to a linkset with a linkset type of either A or E, the command is rejected. On an EAGLE terminal, the following error message is displayed.

```
E2349 Cmd Rej: Link Set Type invalid for Cluster Destination
```

Provisioning Range for Gateway Screening (Release 22.0)

The values for certain parameters used to configure gateway screening can be entered as a range of values. Allowing a range of values for these parameters reduces the number of entries in the gateway screening tables required to support a particular configuration. The parameters whose values can be entered as a range of values are:

Parameters

- **ni** - the network identifier for an ANSI point code
- **nc** - the network cluster for an ANSI point code
- **ncm** - the network cluster member for an ANSI point code
- **pri** - the message priority in the SIO field of an MSU
- **h0** - the H0 heading code in the SIF field of an MSU
- **h1** - the H1 heading code in the SIF field of an MSU
- **type** - the translation type in the called party address field of an MSU

A range of values for these parameters can be specified for gateway screening commands entered on an EAGLE terminal or on the SEAS interface.

The range of values for a parameter is specified by the two values defining the range separated by two ampersands, &&. The value to the left of the ampersands must be less than the value to the right of the ampersands , for example, **:ni=002&&100**. In this example, the value of the **ni** parameter is all values from 002 to 100, including the values 002 and 100.

A range of values for an ANSI point code parameter can be specified with wildcards (*) or single values for other point code parameters. Table 5-6 shows the valid combinations of these parameter values.

Table 5-6. Valid Value Combinations for ANSI Point Code Parameters

NI	NC	NCM
Single Value	Single Value	Single Value
Single Value	Single Value	Range of Values

NI	NC	NCM
Single Value	Single Value	Wildcard
Single Value	Range of Values	Wildcard
Single Value	Wildcard	Wildcard
Range of Values	Wildcard	Wildcard
Wildcard	Wildcard	Wildcard

A range of values for the **H0** and **H1** heading codes can be specified with wildcards (*) or single values for other heading code parameter. Table 5-7 shows the valid combinations of these parameter values.

Table 5-7. Valid Value Combinations for H0 and H1 Parameters

H0	H1
Single Value	Single Value
Single Value	Range of Values
Single Value	Wildcard
Range of Values	Wildcard
Wildcard	Wildcard

When changing or removing an existing gateway screening entry, the ANSI point code values, priority values, **H0** and **H1** heading code values, or translation type values specified with the command must match the values configured in the database for the specified screening reference. If the specified parameter value in a specific screening reference is part of a range of values for that parameter already configured for that screening reference, the command is rejected.

For example, the database contains a gateway screening entry for the range of allowed OPCs 010-010-010 to 010-010-100 in Allowed OPC screening reference opc1. If an attempt is made to remove or change Allowed OPC screening reference opc1 and the ANSI point code 010-010-025 is specified, the command is rejected because point code 010-010-025 is a part of the point code range configured in the database. To remove or change Allowed OPC screening reference opc1, these point code parameters must be specified with the command, **ni=010**, **nc=010**, **ncm=010&&100**.

If the ANSI point code, priority value, **H0** and **H1** heading code values, or translation type values specified with an enter command is within the range of values already configured for the specified screening reference, the command is rejected. For example, the **ent-scr-opc** command is entered with the point code 010-010-050 assigned to screening reference opc1. If the database contains the range of point codes 010-010-010 to 010-010-100, specified as **ni=010**, **nc=010**, **ncm=010&&100**, the command is rejected. If the database contains an entry for all point codes with the network identifier of 010 and network cluster of 010, **ni=010**, **nc=010**, **ncm=***, the command is rejected.

A range of values can be specified when displaying gateway screening entries. The range of values does not have to match the values configured in the database. The range of values specified with a retrieve command is used to limit the number of entries to search for. There are some restrictions for using ANSI point code values with retrieve commands. Table 5-8 shows the valid combinations of the ANSI point code parameters.

Table 5-8. Valid Parameter Combinations for ANSI Point Code Parameters

NI	NC	NCM
Single value	Single value	Single value, a range of values, a wildcard, or NCM value not specified
Single value	A range of values, a wildcard, or the NC value is not specified	the NCM value is not specified
A range of NI values, a wildcard, or the NI value is not specified	the NC value is not specified	the NCM value is not specified

Quality of Service Enhancements (IP^7 Release 3.0)

It is becoming necessary for networks to employ Quality of Service (QoS) techniques. QoS is a concept that allows elements of data transmission to be measured, improved, and, to some extent, predicted. As networks evolve, consideration must be given to guarantee acceptable levels of bandwidth, jitter, and latency for IP communication protocols, such as VoIP. The QoS enhancements added in release 3.0 provide the solution for these and other network communications parameters.

Quality of Service enhancements provide the ability to set the Type of Service (TOS) field in the IP packet header for QoS routing. This feature does not implement quality of service on it's own. It does, however, provides the customer with the ability to set socket options, including the TOS field bits within the outgoing packet. Tekelec does not specify how the TOS bits should be set or interpreted. It is solely up to the customer to implement QoS using scheme best suited for them, by setting the TOS field bits.

TOS

The 8-bit TOS socket option is used to control the quality of service for network traffic. The intent of QoS is to route packets differently according to the TOS value. TOS is set on outgoing packets. The following sections describe the TOS bit field and give an example of a QoS model.

TOS Bit Field

Figure 5-10 describes the TOS bit field structure. The 8-bit TOS field resides in the IP header (Figure 5-9) and is used to identify different priorities/levels/interactions of service used by network routers, such as low-delay service. The TOS field within the outgoing datagram is set from values in the application socket's protocol control block (PCB). The TOS value defaults to 0 (normal service), since the PCB is initialized to zero. The TOS bits may be set to other values and read using the *setsockopt* and *getsockopt* system calls, which provide access to the TOS byte within the PCB.

Figure 5-9. IP Header Fields

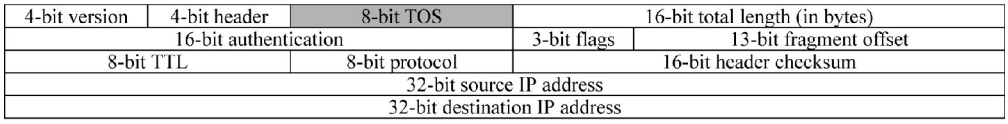


Figure 5-10. TOS Field

7	6	5	4	3	2	1	0
		Reliability	Throughput	Delay	IP precedence		

DS Bit Field

The first network QoS decoding scheme used the TOS bit field description (**Figure 5-10**). Another QoS decoding scheme is the IETF Differentiated Services (DiffServ) model. DiffServ renamed the TOS field to the DS field. **Figure 5-11** describes the DS bit field structure. DS bits 0-5 are reserved for code points (DSCP). The upper two bits (CU) are currently unused. DiffServ code points are broken down into three pools, each pool representing the number of bits used within the DSCP field. Code pool 1, which provides 32 code points, is available for general use, while pools 2 and 3, providing 16 code points, are designated for experimental use only.

Figure 5-11. DS Field

7	6	5	4	3	2	1	0
CU		DSCP					

Figure 5-12. DiffServ Code Point Pool Table

Pool	Code Point Space	Use
1	Xxxxx0	Available
2	xxxx11	Experimental
3	xxxx01	Experimental

This feature allows the customer to modify the full 8-bit TOS socket option to control QoS. The customer is free to implement any QoS model that uses the 8-bit structure within the IP header's TOS/DS bit fields.

Nagle's Algorithm

Nagle's algorithm is currently disabled for all IP [7] Secure Gateway sockets. So every message is transmitted via Ethernet as soon as possible. This means there is a one-TCP-packet-per-MSU relationship. This minimizes message latency, which is very important to Secure Gateway deployment in networks. While minimizing message latency, this mode of operation results in more packets, and therefore more CPU utilization processing packet headers, and also results in less efficient LAN utilization. When Nagle's algorithm is enabled, it allows the TCP/IP stack to hold onto messages for a period of time in an effort to pack multiple messages into a single TCP packet. At the expense of higher message latency, fewer packets are generated and processed, resulting in lower CPU utilization, and the fewer and larger packets result in more efficient LAN utilization. At high rates of traffic through a socket, message latency is minimal, since the threshold packet size is reached (messages fill the packet) very quickly, causing the stack to transmit the packet. At low rates of traffic, a stack timer governs how long a packet will be held prior to transmission. The application of Nagle's Algorithm only affects packet transmission and has no effect on the processing of received packets.

This feature allows the customer to enable or disable Nagle's algorithm. The socket option is defined as a 1-bit Boolean socket option; 1=Enable, 0=Disable.

Feature Implementation

Figure 5-13 illustrates the overall design for implementing the QoS feature. The example shows how an application socket's TOS value can be changed using commands. The example also could be extended to cover

modifying other socket options, including enabling/disabling of Nagle's algorithm. When an application socket is created, it is always assigned to DCMPS parameter set #10, containing the default socket options. Socket options may then be changed using one of the following commands:

chg-appl-sock

In **Figure 5-13** , example 3, an application socket is changed to a different DCMPS parameter set. In this example the new DCMPS parameter set contains a different TOS value. This is accomplished by issuing the following admin command:

```
CHG-APPL-SOCK:SNAME=sockname:DCMPS=new_param_set
```

Changing an open socket to a different DCMPS set forces the socket to use the new DCMPS set's TOS value. This change occurs "on-the-fly." The socket does not need to be closed or inhibited. System call setsockopt() is invoked with the new DCMPS set TOS, thereby updating the affected socket's PCB.

chg-dcmps

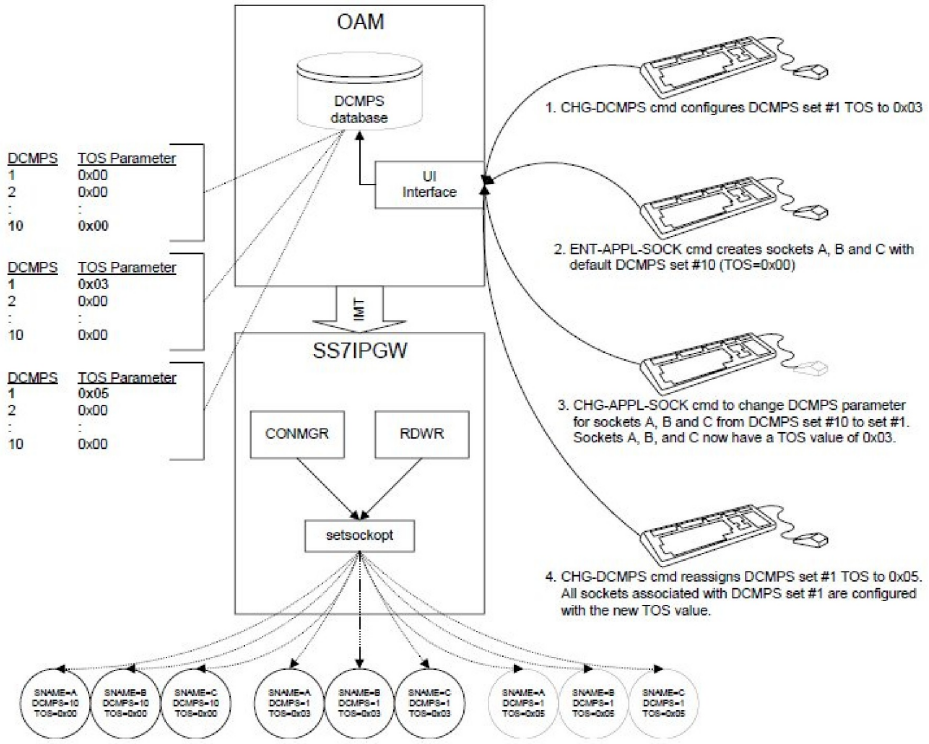
In **Figure 5-13** , example 4, the DCMPS parameter set's TOS parameter is changed to a different value. This causes all sockets using the modified DCMPS parameter set to use the new TOS value. This is accomplished by issuing the following admin command:

```
CHG-DCMPS:SET=setnum:PARM=1:PVALUE=new_tos_value
```

Changing the TOS parameter within a DCMPS set forces all existing sockets using that DCMPS set to use the new TOS value. For all open sockets, this change occurs "on-the-fly." System call setsockopt() is invoked for all sockets using the modified DCMPS set, updating the socket's PCB with the new TOS.

Only sockets affected using the above administration commands allow their socket options to be updated/changed.

Figure 5-13. ToS Setup



Random SLS Generation (Release 28.0)

The Random SLS Generation feature allows operators to overcome some of the ITU protocol limitations by ignoring the SLS value in the incoming SS7 message when selecting an outgoing link for the message. This is accomplished by generating a new 8-bit SLS value that is used internally by the EAGLE to randomly select an outgoing link to the destination.

This feature does not alter the SLS value in the outgoing message; it is the SLS value received in the message. The newly-generated SLS is used for link selection only.

REPT-STAT-CLK Enhancements for Clocking (Release 28.2)

Description

This feature implements the following enhancements:

- New "**`mode=full`**" parameter and report. This report prints out a list of cards that are presenting with a clock failure.

NOTE: HS clock information is included in the new report when a card capable of supporting HS links is provisioned (regardless of link provisioning).

Hardware Requirements

No new hardware is needed to support this feature.

REPT-STAT-TRBL Enhancement (Release 29.0)

This feature is intended to allow users to display only the non-inhibited troubles for captures. This facility allows customers to quickly identify new alarms, versus the old ones they no longer wish to see.

Hardware Requirements

No new hardware is needed to support this feature.

Response to Commands Issued Prior to Login (Release 21.0)

Currently, if a command is entered prior to logging in to the EAGLE that contains a syntax error, the EAGLE responds with a syntax error message. When the user corrects the command and re-enters it, the EAGLE then responds with an authority violation error message. This is annoying to the user. The command would not have been accepted prior to being logged into the EAGLE, regardless of whether it's syntax was correct.

If a command is entered before the user is logged in to the EAGLE, the EAGLE responds with the

```
Command Rejected : Authority violation
```

message regardless of whether the command's syntax is correct.

Revoking a User ID (Release 21.0)

In Release 21.0, the system administrator can prevent the use of a user ID without having to remove it from the database. When a user ID is revoked, any future login attempts with the suspended user ID is rejected with the following message:

```
E2751 Cmd Rej: UserID has been revoked
```

The check for user ID revocation is made during the login process after the user has entered a valid user ID and password combination, and before any checks are made to see if the user's password must be changed.

A user ID is revoked by using the **`revoke=yes`** parameter of the **`chg-user`** command. The **`rtrv-user`** command output report shows which user IDs are revoked.

Revoking a user ID while the user is currently logged on to the system is allowed. In this case, the login session for the user immediately ends and the user is not allowed to enter any other commands.

The EAGLE does not allow user IDs assigned to the security administration command class to be revoked. If this is attempted, the **`chg-user`** command is rejected with the following error message:

```
E2759 Cmd Rej: Revocation of security admin userID not allowed
```

This prevents the system from becoming un-administrable because all user IDs have been revoked.

A revoked user ID can be put back into service using the **revoke=no** parameter with the **chg-user** command.

Routing Key Enhancements (IP^7 Release 3.0)

The Routing Key Enhancements feature provides routing to IP devices with an ITU National or International Point code. In addition, routing for TUP messages is also provided.

Routing Key Enhancements, including the following features:

- Multiple Routing Key Registration allows for the registration of up to three routing keys in a single TALI message.
- Q.BICC Routing provides routing to TCP/IP sockets for BICC messages. BICC messages are very similar to ISUP messages, except the CIC has been expanded to 32 bits. Routing for ANSI or ITU BICC messages is based on SI=13, OPC, DPC, and CIC. The point codes within the routing key must be ANSI, ITU National or ITU International.
- ITU Routing Key Enhancements provide the following additional routing capabilities for international users:
  - — ITU ISUP CIC Routing provides OPC/DPC/CIC routing to IP devices for ITU ISUP messages. Routing for ITU ISUP messages to an IP device is based on SI=5, OPC, DPC, and CIC. The point codes within the ITU ISUP routing key must be either ITU National or ITU International.
  - — ITU DPC-SSN Routing provides DPC/SSN routing to IP devices for ITU SCCP messages. Routing for SCCP messages to an IP device is be based on SI=3, DPC, and Subsystem. The point codes within the ITU SCCP routing key must be either ITU National or ITU International.
  - — ITU DPC-SI Routing provides DPC/SI routing to IP devices for non-ISUP and non-SCCP ITU messages. Routing to ITU point codes on the IP network for non-ISUP and non-SCCP messages is be based on the Destination Point Code and SI indicator, where SI is not 3, 4 (ITU), 5, or 13. A message with SI=4 bound for an ITU National or International point code is assumed to be a TUP message, and is routed as such. The point codes with the ITU DPC-SI routing key must be either ITU National or ITU International.
  - — Telephone User Part (TUP) Routing provides OPC/DPC/CIC routing to IP devices for TUP messages. Routing TUP messages to an IP device with an ITU point code is be based on SI=4, OPC, DPC, and CIC. The point codes within the routing key must be ITU National. An MSU with SI=4 bound for an ANSI point code will continue to be routed on DPC-SI.

RTDB Retrieve (EPAP 9.0)

Description

The RTDB Retrieve feature allows the user to query (from the web GUI) data that resides in the RTDB (Real-Time Database). This feature enables the user to compare data in the PDB (Provisioning Database) with data in the RTDB to verify that they are consistent.

In previous releases of EPAP, queries on EPAP have been supported only by the PDB. The ability to retrieve RTDB data assists in troubleshooting cases where data is absent on EAGLE 5 ISS, but present in the PDB.

Data returned from RTDB is presented on the EPAP GUI in a format that is similar to data from the PDB. This similarity makes it easier to compare data between the two databases when a discrepancy is suspected.

New menu items been added to the EPAP menu:

- Single DNs
- DN Blocks
- Network Entities
- Single IMSIs
- IMEIs
- IMEI Blocks

RTDB retrieval screens are selectively revocable to users and groups by User Interface administrators.

Data can be retrieved while application software is running. Input screens look like the PDBA (Provisioning Database Application) input screen sections for single retrieval of the same data type. Output screens look like the PDBA output screen for the same data type.

A failure message will identify an item as not found if this is the cause of lookup failure.

Hardware Requirements

None.

Limitations

None.

RTRV-RTE/RTRV-DSTN: Support of PC Wildcards (Release 35.0)

Description

The RTRV-RTE/RTRV-DSTN Support of PC Wildcards feature enhances the rtrv-rte command to retrieve destinations by specifying the ** (double asterisk) or *** (triple asterisk) value for the nc and ncm subfields of the ANSI point code as follows:

- **rtrv-rte:dpc=ni-nc-****
- **rtrv-rte:dpc=ni-nc-***
- **rtrv-rte:dpc=ni-**-ni**
- **rtrv-rte:dpc=ni-***-***
- **rtrv-rte:dpcn=*-aa**
- **rtrv-rte:dpcn=nnnnn-***
- **rtrv-rte:dpcn=m1-m2-m3-m4-***

NOTE: If *, **, or * is used for the nc subfield, then *, **, or *** must be also be used for the ncm field.**

A double asterisk in the nc subfield of a network routing point code produces a summary report that shows all point code destinations that are members of the given network (21-**-*). This does not include the specified network routing point code. The following example shows a report generated using two asterisks in the This is the same function that currently exists for the rtrv-dstn command.

Hardware Requirements

The RTRV-RTE/RTRV-DSTN Support of PC Wildcards feature has no hardware requirements.

Limitations

The RTRV-RTE/RTRV-DSTN Support of PC Wildcards feature has no limitations.

RTRV-STP Command (Release 35.0)

Description

The RTRV-STP Command feature provides the new **`rtrv-stp`** command, which provides the functionality of the **`rtrv-bip`**, **`rtrv-gpl`**, **`rtrv-card`**, and **`rept-stat-card`** commands in a single command. The **`rtrv-stp`** command displays the current power consumption and power thresholds for all frames or for a specified frame, allowing users to retrieve the card location, board part number, revision, assembly serial number, DB Size, card type, GPL type, and GPL version for all card locations.

Hardware Requirements

The RTRV-RTE/RTRV-DSTN Support of PC Wildcards feature has no hardware requirements.

Limitations

The **`RTRV-STP`** Command feature has the following limitations:

- Since the Frame Power Consumption value is updated periodically at SCM from the FPBA task, the power consumption value displayed by **`rtrv-stp`** may not be the latest value but the last updated value.
- The **`rtrv-stp`** command may produce 850 Board Part Numbers instead of 870 Board Part Numbers.

RTRV-STP on FTRA

Description

The RTRV-STP on FTRA feature allows a user to retrieve **rtrv-stp** command information in a CSVGEN comma-delimited format, using FTRA Release 4.0. Refer to the *FTP-Based Table Retrieve Application (FTRA) User Guide* in your Release 35.1 Customer Documentation for more information on FTRA.

Hardware Requirements

The RTRV-STP on FTRA feature has no hardware requirements.

Limitations

The RTRV-STP on FTRA feature has no limitations.

RTRV-TBL-CAPACITY Enhancement (Release 29.0)

This enhancement introduces the new command **`rtrv-tbl-capacity`**, which retrieves table use summary information.

Hardware Requirements

No new hardware is needed to support this feature.

SCCP Loop Detection (Release 35.6)

Description

The SCCP Loop Detection feature detects SCCP looping of UDT/XUDT and UDTS/XUDTS messages for all concerned signaling transfer points (STPs).

Normally, an STP sends GTT messages to the capability point codes of mated nodes for load sharing; however, this can result in SCCP Looping if the destination point code (DPC) is the same as the originating point code (OPC) or the point code of any intermediate in the network.

This looping can be resolved by eliminating the use of CPCs and verifying at an intermediate STP whether the OPC of the incoming MSU is the same as the true point code (TPC) of the DPC after GTT. However, CPCs are often used to implement LNP in addition to the SCCP.

The SCCP Loop Detection feature resolves the looping issue by providing a correlation between the MTP-designated point codes for all concerned STPs.

The SCCP Loop Detection feature is provisioned by configuring the Loopset Table and adding a loopset to a Global Title Translation.

The loopset commands define the correlation between MTP-designated point codes and the CPCs of the STPs that detect SCCP looping. The GTT commands allow the administration, deletion, and retrieval of loopset table entries for a particular GTT.

The SCCP Loop Detection feature operates in the Notify and Discard modes. In the Notify (default) mode, the SCCP Loop Detection feature generates a UIM when it detects SCCP looping and does not actually discard the MSU. This UIM allows the operator to capture and verify MSUs throughout the system for SCCP looping. In the Discard mode, the SCCP Loop Detection feature generates a UIM when it detects SCCP looping and discards the MSU.

Hardware Requirements

The SCCP Loop Detection feature requires DSM (4 GB) cards.

Limitations

None.

SCCP Message Type Screening (Release 22.0)

The allowed calling party address (CGPA) screen can screen messages for these SCCP message types: UDT, UDTS, XUDT, and XUDTS. A new parameter, **sccpmt**, has been added to the **ent-scr-cgpa**, **dlt-scr-cgpa**, and **chg-scr-cgpa** commands to configure the allowed CGPA screen to screen for these messages. A new field, SCCPMT, has been added to the output of the **rtrv-scr-cgpa** command to show the SCCP message type in the allowed CGPA screen.

SCCP Service Re-Route Capability (Release 34.3)

Description

The SCCP Service Re-Route Capability feature is designed to re-route G-Flex and G-Port traffic from a node that is unable to process traffic to alternate nodes within an operator network. This feature allows the user to mark the G-Flex or G-Port services OFFLINE, which causes messages to be re-routed to provisioned destinations, either alternate point codes (PCs) or a GTT option. When the user returns either or both services to ONLINE, the services resume processing traffic. The SCCP Service Re-Route Capability feature is optional and doesn't affect normal G-Flex or G-Port functionality.

The G-Flex and G-Port services normally run in tandem with the SCCP service, with no way to halt G-Flex or G-Port without bringing down the entire SCCP service. The SCCP Service Re-Route Capability feature allows the user to mark the G-Flex and/or G-Port services OFFLINE, which re-routes traffic for those services to alternate nodes. The user can mark either or both services ONLINE to cause the service to resume processing traffic.

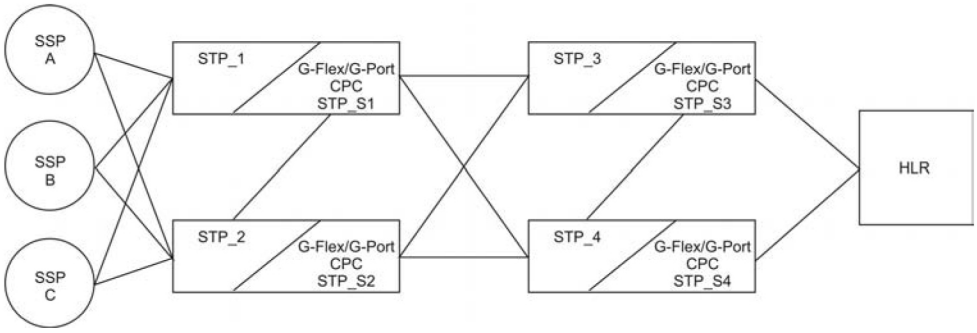
For example, in **Figure 5-14** , G-Flex and G-Port traffic originating from SSP_A, SSP_B, and SSP_C is distributed between STP_1 and STP_2. G-Flex and G-Port traffic is addressed to the relevant service Capability Point Code (CPC) of STP_S1 and STP_S2. GTT traffic is addressed to STP_1 and STP_2.

When the G-Flex/G-Port service is unavailable on STP_1, STP_1 sends a response method TFP message regarding STP_S1. This causes SSP_A to stop using Link_A1 for G-Flex/G-Port traffic. STP_1 can re-route all in-transit G-Flex/G-Port traffic to STPs STP_S2, STP_S3, and STP_S4 if provisioned. SSP_A now sends all of its G-

Flex/G-Port traffic on link_A2. GTT traffic and MTP routed traffic is not impacted. Other SSPs perform similar rerouting.

When G-Flex/G-Port service is available on STP_1, STP_1 responds with a TFA message (when route-set-test message is received) regarding STP_S1. This causes SSP_A to start sending the G-Flex/G-Port traffic through link_A1. Other SSPs perform similar rerouting.

Figure 5-14. G-Flex and G-Port Network Diagram



New Concepts

The SCCP Service Re-Route Capability feature introduces the following new concepts:

- Service State
- Service Re-routing
- Service Capability Point Code

Service State

Service State is an administered state of a RTDB-based service and indicates whether a service is ONLINE or OFFLINE. The SCCP Service Re-Route Capability feature supports Service State for the G-Flex and G-Port services only.

Service State allows a user to mark the G-Flex and G-Port services OFFLINE or ONLINE. If a user identifies a problem with G-Flex or G-Port, they can mark the service OFFLINE to initiate re-routing.

Once the service is returned to ONLINE, the G-Flex or G-Port service starts processing messages if at least one SCCP card is IS-NR.

NOTE: When the SCCP Service Re-Route Capability feature is first turned ON, the G-Flex and G-Port Service States are automatically set to OFFLINE. The user must change the relevant state to ONLINE before any traffic is processed by G-Flex or G-Port.

Service Re-routing

Service Re-routing is an optional function that allows a user to determine the destination of a re-routed message by use of a list of up to seven alternate PCs per domain or the GTT option. The SCCP Service Re-Route Capability feature supports Service Re-routing for the G-Flex and G-Port services only.

Re-routing is activated by marking a service OFFLINE. When a service is OFFLINE, any messages destined to that service are re-routed to available alternate PCs that have been defined for that service. If alternate PCs are not defined, or if none of the PCs are available, then the GTT option is invoked. If the GTT option is YES, then messages destined to that service go to GTT.

Service Capability Point Code

The SCCP Service Re-Route Capability feature provides CPC support for G-Flex and G-Port services. For messages destined to a service, the use of CPCs aids the adjacent nodes in knowing about service outage. When a service is brought down though administrative commands, all traffic destined to this service node performs the following actions:

- Generate response method TFP message to the adjacent node about service CPC. The TFP response to the adjacent node causes the traffic originating nodes to stop sending service traffic to this node. All service traffic coming into this node is sent to the alternate service nodes. Adjacent nodes initiate route-set-test procedures after receipt of the TFP.
- If the messages are destined to EAGLE 5 SAS TPC, then TFP messages are not generated when a service is OFFLINE. Therefore, the originator is not aware of the outage.
- Once the service is back in service on the EAGLE 5 SAS, a TFA is sent to the traffic adjacent nodes in response to route-set-test message. The traffic originating nodes then start sending service traffic to this node.

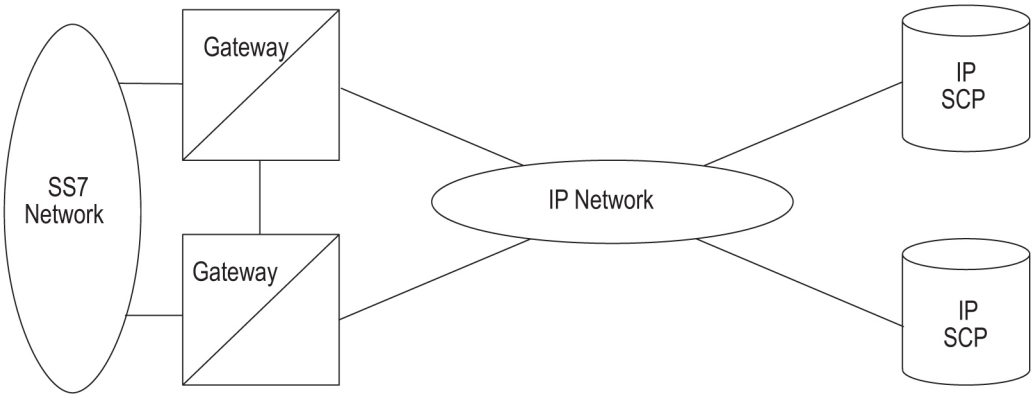
Hardware Requirements

The SCCP Service Re-Route Capability feature runs on DSM cards.

SCCP/TCAP Over IP Gateway for Point-to-Multipoint Connectivity (IP^7 Release 1.0)

The SCCP/TCAP-over-IP feature allows SS7 nodes to exchange SCCP/TCAP Query/Responses with an IP-SCP. The IP ^{7} Secure Gateway manages the point codes and subsystem numbers for the IP-SCP. From the SS7 network perspective, the TCAP queries are routed using these Point Code/SSNs. The signaling gateway maps the Point Code/SSN to one or more TCP sessions, converts the SS7 MSUs to TCP/IP packets by embedding the SCCP/TCAP data inside a TCP/IP packet, and routes it over an IP network. The gateway also manages the application subsystem status from the IP network's perspective and the SS7 network's perspective.

Figure 5-15. SCP Connectivity via TCAP over IP



This feature provides TCP/IP point-to-multipoint connectivity by way of a new GPL, SS7IPGW, running on the DCM which, together with the hardware, provides connectivity to databases (or other switching equipment) for SS7 devices that reside on ethernet TCP/IP networks.

A single DCM card running the **SS7IPGW application** provides connections to multiple IP devices (IP-SCPs, class 4 switches, class 5 switches, VoIP gateways, media gateway controllers, or remote access servers.) Multiple DCM cards running the **SS7IPGW** application are required, with similar configuration, to provide redundancy. The following is a common sequence of events that illustrates the use of point-to-multipoint connectivity:

1. Traditional SS7 devices route MSUs (such as TCAP Queries) to the STP.
2. The gateway performs a global title translation and forwards the translated MSU to the correct TCP/IP device based on point code and SCCP subsystem information in the MSU.
3. The TCAP query is processed at the IP-SCP, and the IP-SCP sends a TCAP reply back to the STP.
4. The STP forwards the TCAP reply back to the sender of the original query.

To provide point-to-multipoint connections, a number of administration steps must first be performed, as follows:

- Links, link sets, destinations and routes to the destinations must be configured.
- The socket connections at each DCM card running the **SS7IPGW** application must be configured.
- The SS7 routing keys that are transported over each defined socket at each card must be configured. SS7 routing keys are filters consisting of values representing the DPC, SI and SSN fields from a incoming MSU message. All MSUs that match the filter are sent to the corresponding socket. The sockets represent TCP sessions. These keys allow for distribution of MSUs on the IP network.

SCCS Interface Support (Release 21.0)

This feature allows the EAGLE to interface to the SCCS terminals using existing EAGLE message input and output formats. The SCCS type is used for some network monitoring and surveillance appliations. The SCCS terminals are the same as KSR terminals, except that a predefined “start-of-message” character is added to indicate the beginning of a new command response or unsolicited message.

Use the Change Terminal (**chg-trm**) command to configure the operational characteristics of the SCCS terminal. Refer to the Commands Manual of your current Documentation Suite.

The following error message is new to this feature:

```
E2149 Cmd Rej: TYPE = SCCS and PRTY=NONE combination is not allowed
```

Refer to the Commands Error Recovery Manual of your current Documentation Suite.

SCTP Checksum Update (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)

Description

Shortly after the introduction of the Stream Control Transmission Protocol (IETF RFC 2960), a fundamental weakness was detected in the Adler-32 checksum[4] algorithm currently used in the RFC. One requirement of an effective checksum is that it evenly and smoothly spreads its input packets over the available check bits. For small packets, Adler-32 provides weak detection of errors.

After much debate and research, the IETF has produced an improved checksum algorithm, CRC-32c, to be used with RFC 2960. The SCTP Checksum Update feature implements this improved algorithm. The SCTP Checksum Update feature provides a choice of SCTP checksum algorithms, and a user interface to both change and display the type of algorithm used.

NOTE: This feature is a SSEDCM-based feature only (P/N 870-2372-01).

The IPGWx and IPLIMx support both SCTP checksum algorithms; the current Adler 32 checksum algorithm and the new CRC-32c checksum algorithm. The CRC-32c Checksum algorithm is implemented on all SCTP-based cards in the IP7 or EAGLE node.

Background

Checksums provide protection against data corruption in the network. The sender of an SCTP packet computes a checksum according to an algorithm. The checksum is placed in the Checksum field residing in the SCTP Common Header (see **Table 5-9**). The receiver then re-computes the checksum, using the same algorithm. The SCTP packet is accepted if the checksum is valid; otherwise, the packet is discarded.

Table 5-9. SCTP Common Header Format

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Source Port Number	Destination Port Number
Verification Tag	
Checksum	

[4] Checksums validate the correctness of the received data—specifically in the SCTP protocol stack, this technique ensures the integrity of the transmitted data from the far-end host.

Adler-32

Adler-32 was the only SCTP checksum algorithm supported and used by the SG prior to this feature. The IETF has determined that the Adler-32 checksum does not provide strong protection against error detection when applied to small packets. Because SCTP protocol signaling messages are typically less than 128 bytes, a better-suited checksum algorithm is needed. This algorithm continues to be supported by the SG.

CRC-32c

Now supported by the SG, the CRC-32c SCTP checksum algorithm solves the limitations of Adler-32. CRC-32c provides better error detection for small packets than does Adler-32.

Hardware Requirements

This feature requires the SSEDCM (P/N 870-2372-01).

SCTP Retransmission Control (Release 28.1) (IP^7 Release 6.0)

This feature offers users a choice of two retransmission policies and enhanced control over the behavior of data retransmissions of SCTP associations in the IP ^{7} SG. This functionality allows users to tailor retransmissions to their networks, on an individual association basis, to address these time-critical protocol constraints.

NOTE: This is a non-orderable feature required for the three IETF Connectivity features and the IPLIM Protocol Support Enhancement feature.

Hardware Requirements

This feature requires a SSEDCM (Single Slot Enhanced DCM).

SEAS Enhancements (Release 26.0)

These enhancements are part of Tekelec's ongoing effort to become SEAS-compliant.

- The EAGLE now supports High Speed Links (ATM-1.536 Mbps) through the SEAS Interface]. (**CHG-slk** is not required to be supported.)
- The EAGLE now supports provisioning of supplier-specific parameters for the following SEAS commands:
  - **ADD/CHG/VFY-LS** (Linkset)
  - **ASGN/CHG/VFY-SLK** (Link)
  - **add/chg/vfy-gtwyls** (Gateway Linkset)
  - **ADD/CHG/VFY-DSTN** for the **NCAI** parameter

NOTE: There is no functionally equivalent EAGLE command for the SEAS commands ADD/CHG/VFY-GTWYLS. Parameters for the link and screen set on the EAGLE will be used to provide the supplier-specific parameter for the ADD/CHG/VFY GTWYLS commands. Supporting screen set names as a supplier-specific parameter is not required.

Affected Commands

add-ls (Linkset)

The parameters in **Table 5-10** are not currently supported by the SEAS definition of the **ADD-LS** command:

Table 5-10. Supplier-Specific Parameters

Supplier-Specific Parameters	Description	Allowed Values
BEI	Broadcast Exception Indicator	YES, NO
GWSA	Gateway Screening Allowed Mode	ON, OFF
GWSM	Gateway Screening Messaging Mode	ON, OFF
GWSD	Gateway Screening Discard Mode	ON, OFF
SCRN	GWS Screen Set Name	AYYY
SLSCI	SLS Conversion Indicator	ON, OFF
ASL8	Adjacent SLS	YES, NO
SLTSET	SLTM Set ID	1 –20
NIS	Network Indicator Spare	ON, OFF
MTPRSE	MTP Restart Equipped	YES, NO

In order to allow users of the SEAS interface the ability to set values for EAGLE- specific parameters, the **unshaded** parameters in **Table 5-10** are allowed to be specified using the SEAS supplier specific parameter block. The GWS- specific parameters are not allowed in the supplier-specific parameter block because they are implemented as part of the supplier-specific parameter block of the GTWYLS entity; see "add-gtwyls (Gateway Linkset)" .

The syntax for supplier-specific parameter "Z" of the SEAS **ADD-LS** command is as follows:

Syntax

```
"[BEI],L3TSET,[SLSCI],[ASL8],[SLTSET],[NIS],[MTPRSE]"
```

The following example is provided to help customers understanding the new capability of specifying supplier-specific parameter blocks via SEAS commands on the EAGLE.

Suppose the user wants to add a linkset where all of the Supplier Specific parameters get set to the default value. This can be done in four different ways:

Input Example

1. **ADD-LS::LS1201:000003:50,RCH::LNSCLLI1201-012001001:A::,G63D45G25-001-07**

2. **ADD-LS::LS1201:000003:50,RCH::LNSCLLI1201-012001001:A:",,,,,,":,G63D45G25-001-07**

3. **ADD-LS::LS1201:000003:50,RCH::LNSCLLI1201-012001001:A:"0,1,0,0,1,0,0":,G63D45G25-001-07**

4. **ADD-LS::LS1201:000003:50,RCH::LNSCLLI1201-012001001:A:",,0,0,1,0,0":,G63D45G25-001-07**

The first method simply leaves out parameter "Z" and the appropriate default values are assigned.

The second method specifies parameter "Z" enclosed in quotes. All the members of the supplier-specific parameter block are optional, and can be omitted (the colons must always be specified if parameter "Z" is specified).

The third method specifies the appropriate default values for each supplier-specific parameter within the block.

The fourth method specifies default values for SLSCI, ASL8, SLTSET, NIS, and MTPRSE. All four commands will result in the same entry created in the EAGLE database.

chg-ls

The following parameters are not currently supported by the SEAS definition of the **CHG-LS** command.

Table 5-11. Supplier-Specific Parameters for chg-ls

Supplier Specific Parameters	Description	Allowed Values
TFATCABMLQ	TFA/TCA Broadcast Min. Link Quantity	0 –16
BEI	Broadcast Exception Indicator	YES, NO
GWSA	Gateway Screening Allowed Mode	ON, OFF
GWSM	Gateway Screening Messaging Mode	ON, OFF
GWSD	Gateway Screening Discard Mode	ON, OFF
SCRN	GWS Screen Set Name	AYYY
SLSCI	SLS Conversion Indicator	ON, OFF
ASL8	Adjacent SLS	YES, NO
SLTSET	SLTM Set ID	1 –20
NIS	Network Indicator Spare	ON, OFF
MTPRSE	MTP Restart Equipped	YES, NO

In order to allow users of the SEAS interface the ability to set values for EAGLE specific parameters the highlighted parameters above are allowed to be specified using the SEAS supplier specific parameter block. The GWS-specific parameters are not allowed in the supplier specific parameter block because they are implemented as part of the supplier-specific parameter block of the GTWYLS entity; see "add-gtwyls (Gateway Linkset)" .

The syntax for supplier-specific parameter "Z" of the SEAS **ADD-LS** command is as follows:

Syntax

```
"[TFATCABMLQ]:[BEI]:L3TSET:[SLSCI]:[ASL8]:[SLTSET]:[NIS]:[MTPRSE]"
```

dlt-ls

There are no supplier specific parameters available for the SEAS **DLT-LS** command.

vfy-ls

There are no supplier-specific parameters available for the SEAS **VFY-LS** command on input. However, the output of the **VFY-LS** command includes the following output for the supplier specific parameter block:

Syntax

```
"TFATCABMLQ:BEI:L3TSET:SLSCI:ASL8:SLTSET:NIS:MTPRSE"
```

add-gtwyls (Gateway Linkset)

In order to allow users of the SEAS interface the ability to set values for EAGLE-specific parameters the **unshaded** parameters in Table 5-12 are allowed to be specified using the SEAS supplier-specific parameter block.

Only GWS-specific parameters are allowed in the supplier specific parameter block. The shaded parameters (with exception to the SCRN parameter) are supported in the Linkset supplier-specific parameter block.

Table 5-12. Supplier-Specific Parameters for add-gtwyls

Supplier Specific Parameters	Description	Allowed Values
BEI	Broadcast Exception Indicator	YES, NO
GWSA	Gateway Screening Allowed Mode	ON, OFF
GWSM	Gateway Screening Messaging Mode	ON, OFF
GWSD	Gateway Screening Discard Mode	ON, OFF
L3TSET	Level 3 Timer Set	1
SCRN	GWS Screen Set Name	AYYY
SLSCI	SLS Conversion Indicator	ON, OFF
ASL8	Adjacent SLS	YES, NO
SLTSET	SLTM Set ID	1 –20
NIS	Network Indicator Spare	ON, OFF
MTPRSE	MTP Restart Equipped	YES, NO
ACTNAME	Stop Action Set Name	Alphanumeric(6)
DESTFLD	Destfld Screening	YES, NO

dlt-gtwyls

There are no supplier-specific parameters associated with the **DLT-GTWYLS** command.

chg-gtwyls

The supplier-specific parameter block for the **CHG-GTWYLS** command is equivalent to the supplier-specific parameter block for the **ADD-GTWYLS** command (see “add-gtwyls (Gateway Linkset)”).

vfy-gtwyls

There are no supplier specific parameters available for the SEAS **VFY-GTWYLS** command on input. However the output of the **VFY-GTWYLS** command will include the following output for the supplier-specific parameter block:

Syntax

```
"[GWSA],[GWSM],[GWSD],[ACTNAME],[DESTFLD],[SCRN]"
```

asgn-slk (Signaling Link)

In order to allow users of the SEAS interface the ability to set values for EAGLE specific-parameters, the EAGLE supports a supplier-specific parameter block for the SEAS command **ASGN-SLK**. The supplier-specific parameter block consists of all the parameters from **Table 5-13** .

Table 5-13. Supplier Specific Parameters of asgn-slk

Supplier Specific Parameters	Description	Allowed Values
L2TSET	Level 2 Timer Set	1-20
L1MODE	Mode of Operation Used to Select Link Clocking Source	DTE, DCE
TSET	Transmitter Signal Element Timing	ON, OFF
ECM	Error Correction Method	BASIC, PCR
PCRN1	Number of MSUs Available For Retransmission Threshold	1-127
PCRN2	Number of MSU Octets Available For Retransmission Threshold	300-35500
LPSET	Link Parameter Set Identifier	1-20
ATMTSEL	ATM Timing Selector	LINE, INTERNAL, EXTERNAL
VCI	Virtual Channel Identifier	0-65535
VPI	Virtual Path Identifier	0-4095
LL	ATM Line Length	0-7

The syntax for supplier-specific parameter "Z" , of the SEAS ASGN-SLK command, is as follows:

Syntax

```
"[L2TSET]:[L Adresse 1MODE]:[TSET]:[ECM]:[PCRN1]:[PCRN2]:[LPSET]:[ATMTSEL]:[VCI]:[VPI]:[LL]"
```

dlt-slk

No supplier-specific parameter support is required for the SEAS **ASGN-SLK** command.

chg-slk

No supplier-specific parameter support is required for the SEAS **CHG-SLK** command.

vfy-slk

There are no supplier-specific parameters available for the SEAS **VFY-SLK** command on input. However, the output of the **VFY-SLK** command includes the following output for the supplier-specific parameter block:

Syntax

```
"[L2TSET]:[L1MODE]:[TSET]:[ECM]:[PCRN1]:[PCRN2]:[LPSET]:[ATMTSEL] :[VCI]:[VPI]:[LL]"
```

SEAS Enhancements, Autonomous Messages (Release 22.0)

The EAGLE in release 22.0 supports these SEAS autonomous messages.

- REPT-GTWYACT - notification that the gateway threshold has been exceeded
- REPT-SCRREJ - notification that an MSU has been discarded because of gateway screening.
- REPT-DBCPY - notification that the EAGLE's database has been either backed up or restored.
- REPT-NOTRNS - notification that the EAGLE is unable to perform a global title translation because of problems with the GTT tables and the MSU has been discarded.
- REPT-MTPERR - notification that the EAGLE cannot perform MTP level routing for a received MSU and that MSU has been discarded.
- REPT-LKSTO - notification that all signaling links in a linkset are unavailable because of multiple signaling link failures or processor outages.
- RCVRY-LKSTO - notification that the EAGLE has recovered from a previously reported linkset outage condition.
- REPT-LINK-CGST - notification that the value *occupancy threshold reached/exceeded* field in the MSU is set to a fixed value regardless of the congestion level being reported.
- RCVRY-LINK-CGST - notification that the value *occupancy threshold reached* field in the MSU is set to a fixed value regardless of the congestion level being reported.

This feature prevents duplicate autonomous messages to be sent to the SEAS ports.

This feature also introduces these new EAGLE commands to configure the thresholds for the REPT-GTWYACT and the REPT-SCRREJ messages.

- **set-gtwy-acthresh** - configures the gateway threshold
- **rtrv-gtwy-acthresh** - displays the current values of the gateway threshold
- **set-scrrej-prmtrs** - configures the quantity of REPT-SCRREJ messages are sent to SEAS
- **rtrv-scrrej-prmtrs** - displays the quantity of REPT-SCRREJ messages are sent to SEAS

These actions can also be performed from the SEAS interface with these SEAS command functions, SET-GTWY-ACTHRESH, RTRV-GTWY-ACTHRESH, SET-SCRREJ-PRMTRS and RTRV-SCRREJ-PRMTRS.

SEAS Gateway Audit Command (CHK-UNREF-ENT) (Release 22.0)

Release 22.0 introduces the **chk-unref-ent** command on the EAGLE and supports the CHK-UNREF-ENT command function on the SEAS interface.

This feature gives users the ability to identify unreferenced entities in the EAGLE's gateway screening entity sets. These unreferenced entities can be dealt with by the user as required.

Unreferenced gateway screening entity sets are those entity sets that are not referenced by another entity with the next screening function identifier (NSFI) and next screening reference (NSR) combination or with the link set screening reference (that is, a screen set used by a link set). Any unreferenced gateway screening entities are displayed by the entity set name (screen set name) and screening reference (NSFI).

The EAGLE's **chk-unref-ent** command uses these parameters.

Parameters

:aftpc= Is the Affected PC/SSN entity set to be checked?

:blkopc= Is the Blocked OPC entity set to be checked?

:blkdpc= Is the Blocked DPC entity set to be checked?

:cdpa= Is the Allowed CDPA entity set to be checked?

:cgpa= Is the Allowed CGPA entity set to be checked?

:destfld= Is the Affected DESTFLD entity set to be checked?

:dpc= Is the Allowed DPC entity set to be checked?

:opc= Is the Allowed OPC entity set to be checked?

:sio= Is the Allowed SIO entity set to be checked?

:tt= Is the Allowed TT entity set to be checked?

:all= Are all the gateway screening entity sets to be checked?

The values for these parameters are either **yes** or **no**, with the default value being **no**.

SEAS Interface Support (Release 21.0)

This feature allows the EAGLE to interface with 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 back 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 command to be entered into the system from a SEAS console.
- Recent change and verify (immediate activation only) for following data entities:
    1. MTP (routes, route sets, signaling links, linksets, point codes, etc.)
    2. GTT (global title translations, subsystems, and mated applications)
    3. 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 minimum of 10 PVCs on a LIMV35 card at data rates of 64 kbps, 56 kbps, 19.2 kbps, 9.6 kbps, 4.8 kbps and 2.4 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 use asynchronous RS-232 ports. An operations system support applications processor (OAP) is used to allow the EAGLE to communicate with the SEAC. The OAP is an adjunct processor that interfaces to a BX.25 link and converts the data stream to an asynchronous serial format. All conversion from SEAS to EAGLE command sets takes place on the EAGLE. Two terminal disk module (TDM) ports (RS-232) running at 19,200 bps connect the OAP to the EAGLE. Two BX.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, and is labeled as OAPF.

The OAP is a TEXAS MICRO™ Intelligent Processor Unit Telecommunications Server, model 9605 (Sparc 05, 85 MHz processor) and contains:

- 32 megabytes of RAM
- a 1.02 gigabyte hard drive using a SCSI interface
- a 1.44 megabyte floppy disk drive, a high-speed serial interface (HSI) SBUS card (with 4 synchronous ports)
- RS-232C-extender SBUS communications board (with 4 asynchronous ports).

The OAP is powered from the OAP frame’s fuse and alarm panel with -48 VDC.

The OAP uses the following software to allow the EAGLE to communicate with the SEAC:

- SUN™ Solaris version 2.4 operating system
- SunLink Solaris version 9 for X.25
- The SEAS application software.

NOTE: Some of the names of the EAGLE measurement counters have been changed to match the names used by SEAS. Table 5-14 shows the names of the measurement counters that have changed and the measurement reports and entity types that contain these counters.

Table 5-14. Changed EAGLE Measurement Names

Measurement Report	Measurement Entity Type	Current Measurement Name	New Measurement Name
ALL	STP	IMSINVDPC	MSINVDPC
ALL	STP	IMSINVSIO	MSINVSIO
COMP	LINK	DURLNKUNV	DRLKOTG
COMP	LINKSET	MSURGTT	MSUSRGTT
COMP	LINKSET	OCTRQGTT	OCTRCGTT
MTCD, MTCDTH	LINK	LNKAVALT	LNKAVAIL
MTCD, MTCDTH	LINK	DRLNKINH	DRLKINHB
MTCD, MTCDTH	LINK	SURCVERR	MSURCERR
MTCD, MTCDTH	LINK	NEGACKRCV	NEGACKS
MTCD, MTCDTH	LINK	NEARMGINH	NEARMGIH
MTCD, MTCDTH	LINK	NDCLFABN	NDCFLABN
MTCD, MTCDTH	LINK	NDCLFXDA	NCDFLXDA
MTCD, MTCDTH	LINK	NDCLFXER	NDCFLXER
MTCD, MTCDTH	LINK	NDCLFXDC	NDCFLXDC

SEAS Verify Signaling Route-Set Status and SCCP Application Status Command (VFY-SRSAPST) (Release 22.0)

Release 22.0 supports the VFY-SRSAPST command function on the SEAS interface which is used to display the status of the current MTP signaling routesets, the status of individual routes, and the status of the SCCP application subsystem for specified destinations and applications that the EAGLE routes traffic to. This feature reduces the need to use non-SEAS EAGLE commands with the SEAS Flow-Through command to display this information.

Security Log Increase (Release 26.05)

Security Logging is used to store the commands that are issued on EAGLE, either using the EAGLE terminal, or via SEAS Port. The Security Logging facility also stores additional information about the command, such as, date/time received, terminal on which received, UserID, and result of the command execution.

The Security Log Increase feature increases the Log size from 10K entries to 50K entries.

Increasing the FTA (File Transfer Area)

The FTA is used to store the security logs and the hourly and daily measurements (weeks worth of measurements data [5]). The FTA is designed to contain four security logs, each of size 2.5 MB (10K entries * 256 record size). Since the size of the security log has been increased from 10K to 50K, the FTA has been increased by at least 40MB. Hence the FTA has been increased to 100MB to accommodate this feature.

Upgrade Considerations

Before the upgrade, entire security log *must* be uploaded. The procedure to upload the security log follows:

1. Issue the **REPT-STAT-SECULOG** command to determine which security log should be uploaded. Under normal operating conditions, the standby OAM's security log should always contain 0 in the ENTRIES column, and thus should never need uploading. However, if the standby OAM's log contains one or more un-uploaded entries, it should be uploaded as well.

2. Issue the **COPY-SECULOG** command with appropriate parameters to cause the log to be copied to the FTA area. Note the name of the file that is created in the FTA area, and also the location 1114/1116 of the FTA area which received the copy. This information will be displayed in the scroll area at the successful conclusion of the **COPY-SECULOG** command.

   If the security log has to be ported onto a PC, the following two steps need to be performed as well

3. On an EAGLE terminal that is being emulated on a suitably-equipped PC (e.g. a PC running ProComm), issue the **ACT-FILE-TRNS:LOC=xxxx** command, specifying xxxx as the location 1114 or 1116 of the FTA area containing the log to be uploaded.

4. Start a Kermit download session on the PC. If using ProComm, this is accomplished by selecting the "Online" menu item, then "Kermit command", then "Get file". At this point a dialog box will be presented asking for the name of the file to be transferred. Enter the name of the file noted during the **COPY-SECULOG** command in step 3, and press the OK button to transfer the file from the EAGLE to the PC.

Limitations

Due to the circular nature of the security logs, if the security log is not uploaded when it is full, it will start to overwrite the contents. Hence the security log should be uploaded when "log full" alarm is raised. This feature does not affect any other GPL's running on other cards.

Selective Alarm Inhibiting (Release 22.0)

This feature allows the user to turn off major and minor alarms for specific devices. Critical alarms cannot be turned off. The following are examples of situations where a user may want to turn off alarms.

- When repeated alarms from malfunctioning equipment could mask valid alarms, for example, a signaling link that is out of service because of a physical break that cannot be repaired for days, the alarm for that signaling link can be turned off.

- The EAGLE database is being configured. Alarms are generated immediately after entries are entered into the database. If these alarms are ignored and a problem develops that requires immediate attention, that problem may be ignored.

Alarms can only be turned off for these devices or entities.

- cards in the database
- signaling links in the database
- linksets in the database
- EAGLE terminals
- system clock
- TCP/IP data links in the database
- customer defined troubles
- SEAS X.25 links

When the system has alarms only for devices that have their alarms turned off, all the alarm indicators (visual and audible) are turned off. If alarms exist for devices that have not been turned off, or for entities whose alarms cannot be turned off, the alarm indicators remain on.

The alarm indicators are turned on only for devices or entities that do not have their alarms turned off, or that cannot be turned off.

When an alarm is turned off, no unsolicited alarm messages (UAMs) are generated for the device when an alarm condition for that device is detected.

When an alarm is turned off, UIM 0004 is displayed to inform the user that the alarm for the specified device has been turned off. In this example, the alarms for card 1201 have been turned off.

UAM

```
RLGHNCXA03W 97-06-07 14:56:48 EST Rel 22.0.0
5005.0004    CARD 1201 SS7ANSI     Device alarms inhibited
```

If an alarm is turned off, it remains off even if the MASP is reset.

A count of the alarms that are turned off is shown in the alarm status region of the VT320 display terminal (**Figure 5-16**). The alarm status region (**Figure 5-17**) of the terminal display contains four boxes with numbers underneath. The boxes contains the labels for the alarm types and the numbers show the number of each type of alarm that has been detected on the EAGLE.

- CRIT - critical alarms - Indicates a severe, service-affecting condition has occurred and that immediate corrective action is needed, regardless of the time of day or the day of the week

- MAJR - major alarms - Indicates a serious disruption of service or the failure of important circuits is taking place. These troubles require attention and response to restore or maintain system capability
- MINR - minor alarms - Indicates a trouble, but does not have a serious effect on service.
- INH - inhibited alarms - alarms that have been turned off.

Figure 5-16. EAGLE Terminal Display

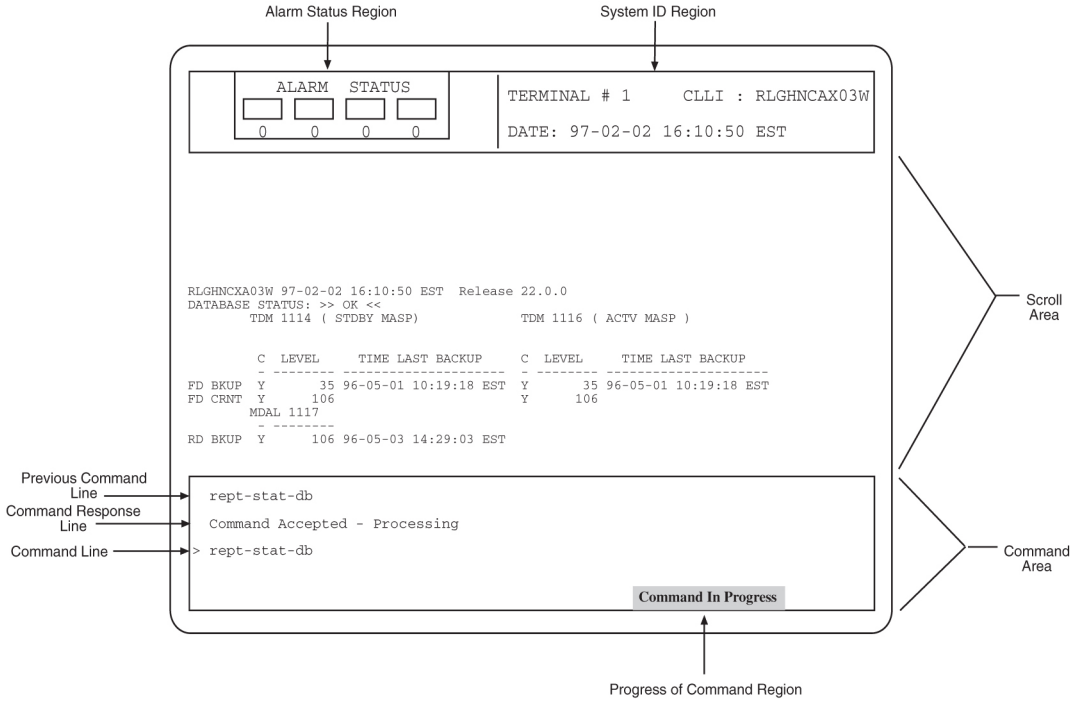


Figure 5-17. Alarm Status Region of the EAGLE Terminal Display

Selective Homing of EPAP RTDBs (Release 29.0)

Currently, the RTDBs on an EPAP (A or B) will look for and receive updates from the local PDBA process on the local EPAP A (PDBA on the same MPS node as the RTDB), regardless of whether it is the active or standby PDB. An RTDB will only receive updates from the remote PDBA process on the mate MPS node if the local PDBA cannot be accessed.

Some customers would prefer to have all RTDBs within an "MPS System" (both nodes of a mated pair, or even multiple nodes within several mated pairs) always receiving updates from the active PDBA process, regardless of whether it is the local or remote PDBA.

The Selective Homing of EPAP RTDBs feature implements an EPAP configuration option that allows the customer to choose whether the RTDBs on a given MPS node will receive updates from a specific PDBA process (which may or may not be active), or from the active PDBA process (which may or may not be local). This option is selectable via the EPAP UI.

The terminology "specific PDBA" is used instead of "local PDBA," because architectures may result in an MPS without a PDB on EPAP A, in which case the RTDBs on that node would not have a "local PDBA." Specific homing would specify the IP addresses of the MPSs with the first and second choices of PDBA. In a two-node MPS system, this maps directly to "local" homing.

Hardware Requirements

No new hardware is required to support this feature.

Enhancements to the User Interface

A new section will be added to the RTDB Status screen of the EPAP UI to display the RTDB Homing policy for both RTDBs on the MPS.

The PDBA Status sections of both the RTDB Status and PDBA status screens will be enhanced to display the current RTDB clients.

Upgrade Considerations

This feature does not impact the EPAP 1.x/2.x to 3.0 upgrade. New EAGLEs may not be included for provisioning until all affected sites have been upgraded to EPAP 3.0. RTDB homing policy may not be changed until all affected sites have been upgraded to EPAP 3.0. Interaction with EAGLE is not affected by this feature.

Simplifying BIP (Board ID PROM) for EAGLE STP Boards (Release 23.1)

This feature changes the 7- and 8-digit serial numbers currently used to identify a board in the EAGLE to serial numbers that contain 7, 8, 11, 12, and 14 digits. The serial number is contained in the board ID PROM on each board in the EAGLE.

The 7- and 8-digit serial numbers are used on older systems and require no changes to support. The 11-digit serial number is presently used by Tekelec manufacturing, but was not fully supported by the EAGLE system software. The 12-digit serial number adds a special character to the serial number used by manufacturing. The 14-digit serial number uses four digits to show the year that the board was manufactured. All the serial number formats are compliant with the Year 2000 feature.

Table 5-15 shows the format of each of the five serial number formats.

Table 5-15. Serial Number Formats

Serial Numbers	Formats
7-digit serial number	ywwxxxx
8-digit serial number	yywwxxxx

Serial Numbers	Formats
11-digit serial number	nnnyywwxxxx
12-digit serial number	nnnyyww*xxxx
14-digit serial number	nnnyyyyww*xxxx
y = year digit (0 - 9) w = week digit (0 - 9) n = product identifier digit (0 - 9) x = serial number digit (0 - F hexadecimal) * = special character (0 - 9, a - z, or A - Z, alphanumeric characters)	

Hourly Status Message Report

The indicator INHAUDB has been added to the Condition Type field of the Hourly Status Message Report. This indicator shows that the user has manually turned off the alarms for this device. The date and time that the alarm for the device was turned off is displayed in the report. The report also includes the alarm status periodic reminder added to the end of the report to summarize the status of the alarms.

Output Example

```
    RLGHNCXA03W 97-06-07 15:00:00 EST Rel 22.0.0
    5023.0000 REPT COND CARD
    "CARD 1201:,MTCEINT-0,,97-06-07,14:58:24,,,,"
    "CARD 1202:0013,,SA,97-06-07,14:44:38,,,,**"
    "CARD 1203:0013,,SA,97-06-07,14:44:38,,,,**"
    "CARD 1204:0013,,SA,97-06-07,14:44:38,,,,**"
    "CARD 1206:0013,,SA,97-06-07,14:44:38,,,,**"
    "CARD 1207:0034,,NSA,97-06-07,14:52:56,,,,* "
    "CARD 1208:0013,,SA,97-06-07,14:44:38,,,,**"
    "CARD 1216:0013,INHAUDB,NSA,97-06-07,13:44:38,,,,"
    "CARD 1101:0034,MTCEINT-0,NSA,97-06-07,14:52:56,,,,* "
    "CARD 1115:0143,,NSA,97-06-07,14:57:52,,,,* "
;
    RLGHNCXA03W 97-06-07 15:00:02 EST Rel 22.0.0
    5034.0000 REPT COND ALARM STATUS
    "ALARMS:INHIBITED,0,17,8"
    "ALARMS:ACTIVE,2,0,0"
    "ALARMS:TOTAL,2,17,8"
    "ALARMS:STATUS,AUDIBLE,SILENT,SILENT"
```

The alarm status periodic reminder contains four fields, ALARMS:INHIBITED, ALARMS:ACTIVE, ALARMS:TOTAL, and ALARMS:STATUS.

The ALARMS:INHIBITED field shows the number of alarms of each type that have been turned off.

The ALARMS:ACTIVE field shows the number of alarms of each type that are active and not turned off.

The ALARMS:TOTAL field shows the total number of alarms of each type that the EAGLE has detected.

Following each of these fields are three numbers separated with commas. These numbers show the number of each alarm type the EAGLE has detected. The first number shows the number of critical alarms. The second number shows the number of major alarms. The third number shows the number of minor alarms.

The ALARMS:STATUS field shows whether the critical, major, and minor alarms are silent or audible.

In this example, the EAGLE has 17 major alarms and 8 minor alarms turned off, 2 critical alarms active for a total alarm count of 2 critical alarms, 17 major alarms, and 8 minor alarms. Only the critical alarms are audible.

Single Slot Enhanced DCM (Release 28.1) (IP^7 Release 6.0)

The dual-slot DCM card (870-1945-03) occupies two slots on the EAGLE; the single slot EDCM (SSEDCM, 870-2372-01) card occupies only one slot. Unlike the DCM Card, the single slot EDCM card can be provisioned in any slot. Only IPLIMx and IPGWx applications are allowed to run on the single slot EDCM Card. The DCM card can always be hot-swapped with a single slot EDCM card.

Refer to the *NSD Hardware Manual* for current details of the SSEDCM.

Hardware Requirements

This release introduces a new DCM type family board called the Single Slot EDCM (SSEDCM). Just as the name implies, the SSEDCM card occupies only one slot in an EAGLE shelf, as opposed to the dual-slot DCM boards. The provisioning rules for a DCM type board allow provisioning of any slot where a DCM type board can physically be inserted.

SLAN on E5-ENET Assembly (Release 37.0)

Description

The SLAN on E5-ENET Assembly feature supports running the **stpla**n application on the E5-ENET card.

The SLAN on E5-ENET Assembly feature allows the E5-ENET card to support the features currently implemented on the DCM card (SSEDCM, or EDCM-A assembly).

The E5-ENET card running the **slanhc** GPL and the **stplan** application is referred to as the E5-SLAN card.

NOTE: The DCM, SSEDCM, EDCM-A, and E5-SLAN cards run the stplan application. The vwxslan application is no longer used.

Because the DCM card and the E5-SLAN card are both provisioned with card type **dcm** and the **stplan** application, the two cards can be “hot-swapped” without re-provisioning the card information in the system.

NOTE: Hot-swapping the DCM and E5-SLAN cards requires cable adaptors.

HIPR cards must be installed in each shelf where E5-SLAN cards are installed. At least two cards running the **stplan** application must be provisioned in the EAGLE 5 ISS to provide “n+1” redundancy. A maximum of 32 STPLAN/E5-SLAN cards can be provisioned.

If a shelf contains HMUX cards, then E5-SLAN cards must be provisioned in shelves adjacent to that shelf. The optimum configuration is to provision half of the E5-SLAN cards in the previous shelf and half in the next shelf.

The SLAN on E5-ENET Assembly feature allows the link speed and duplex configuration to be set either automatically or manually. The **`auto`** parameter in the **`ent-dl`**k command can be set to **yes** to enable auto-negotiation, which configures speed and duplex for the link automatically. The **`duplex`** and **`spee`**d parameters in the **`ent-dlk`** command can be used to set duplex and speed manually.

If auto-negotiation is enabled, the E5-SLAN card operates at 12,000 TVG grants per second when the IP port operates at 100 Mbps full duplex, and at 1200 TVG grants per second when the IP port operates at 10 Mbps full or half duplex, or 100 Mbps half duplex.

Thermal management and alarming provisions are provided for the E5-SLAN card.

Feature Control Requirements

None.

Hardware Requirements

The SLAN on E5-ENET Assembly feature has the following hardware requirements:

- HIPR cards must be installed at card locations 9 and 10 in the shelf where the E5-SLAN card is installed.
- Backplane cable adaptors

Limitations

- The **-m**, **-p**, and **-h** suboptions of the **-d** option for the **`netstat`** command are not supported for the E5-SLAN card.
- The E5-SLAN card does not preserve memory across boots. The application will not remain intact across card boots.
- The performance of the E5-SLAN card is limited by the data rate of the Ethernet port and the capability of the external LAN/WAN.

Spare Point Code (Release 31.12)

The EAGLE ITU International/National Spare Point Code feature allows a network operator to use the same Point Codes across two networks (either ITU-I or ITU-N). The feature also enables National and National Spare traffic to be routed over the same linkset. The EAGLE uses the MSU Network Indicator (NI) to differentiate the same point code of one network from the other. In accordance with the SS7 standard, unique Network Indicator values are defined for ITU-I, ITU-N, ITU-I Spare, and ITU-N Spare Point Code types.

The EAGLE currently provides full support for four types of point codes:

- ANSI, ITU-National (NI=10binary)
- ITU-National 24-bit
- ITU-International (NI=00 binary)
- ITU National Spare PCs (NI=11 binary) can be primarily supported via a combination of the following two items:

1. Support for ITU-National Spare can be set on a per linkset basis using the linkset NIS parameter. If set, the EAGLE will allow receipt of messages with NI=11binary on the designated linkset and will force all outgoing messages on that linkset to have NI=11binary.

2. The Duplicate Point Code routing feature, combined with the Multiple Point Code Support feature, can be used to create a separate routing group for a National Spare Point Code network.

While these two functions can be combined to support ITU National Spare Point Code routing, there are limitations described as follows:

- The EAGLE cannot distinguish between messages with different network indicators received over the same linkset. For example, the EAGLE will route a message with DPC = 1-1-1 (NI=10binary) the same way as a message with DPC = 1-1-1 (NI=11binary).

- Forcing the user to use the Duplicate PC Routing feature requires that all linksets in the system be placed in one of the defined groups.

The Spare Point Code Support feature addresses the above limitations. by The feature provides a new PC sub type named Spare. The spare point code supports the ITU-N Spare and ITU-I Spare Point Code feature.

Additionally, this feature requires a single linkset to support multiple outgoing network indicators (e.g. 11 binary, 00 binary). In turn, messages are routed according to the Point Code on the outgoing node that corresponds to the associated network indicator.

Limitations

1. This feature does not allow the EAGLE to MTP convert between National and National Spare Point Codes. Likewise, this feature does not allow the EAGLE to MTP convert between International and International Spare Point Codes.

2. In the destination table, an ITU-I alias and an ITU-I Spare alias cannot be defined for the same Point Code, likewise an ITU-N alias and an ITU-N Spare alias cannot be defined for the same point code

3. The feature is not supported on the SEAS interface. Spare point codes are only supported for ITU point codes, and SEAS only supports ANSI point codes. Any Private ANSI point code provisioned using the standard EAGLE command line interface is not displayed by the SEAS VFY- command.

4. ITU National and ITU National Spare Point Code are implemented as separate network domains that can co-exist within the same STP.

5. Spare point codes are not supported for IPGWI sockets using TALI protocols. The spare point code feature may not be enabled if any application sockets have been provisioned on IPGWI cards.

6. The existing implementation of Gateway Screening does not support Group Code (Duplicate Point Codes). Gateway Screening will also not support PPCs.

7. The Spare Point Code and PPC prefix value, s- and p- do not apply to domain type point codes for ANSI and ITU-N24.

8. ITU-N and ITU-N24 Point Codes cannot co-exist as SID Destination True Point Codes and therefore ITU-N Spare and ITU-N24 Point Codes cannot coexist as SID Destination True Point Codes.

9. A single STPOPTS value (cnvcgdi) will be used to control message handling for ITU-I and ITU-I Spare messages when the CgPA PC does not have a required alias

10. A single STPOPTS value (cnvcgdn) will be used to control message handling for ITU-N and ITU-N Spare messages when the CgPA PC does not have a required alias

11. The existing implementation of the SRVSEL command interface to the SRVSEL table does not provide a way to separate MSU traffic for different ITU National Group Code networks. Therefore no provision is made for the SRVSEL command to control the separation of ITU spare and non-spare traffic. The SRVSEL table applies to the EPAP based features G-FLEX, INP, G-PORT, SMS Prepaid, and IS-41 to GSM Migration. Likewise, no provision is made for the GTTSEL command interface to the GTTSEL table to allow separation of ITU spare and non-spare traffic for EGTT, VGTT and MGTT.

Split Allowed CGPA Table (Release 22.0)

The Allowed CGPA screen has been changed in Release 22.0 to allow for different next screening values depending on the value of the routing indicator (ri) parameter. These options are summarized in Table 5-16 .

Table 5-16. Next Screening Options for the Allowed CGPA Screen

RI	NSFI
GT, *	STOP, TT
DPC, *	STOP, CDPA

The messages can be screened on the routing indicator (RI) field. In previous releases, the routing indicator was included in the Allowed CGPA screening entry, but was not part of the screening process. This allowed only one message routing indicator value, or range of values, for each Allowed CGPA entry with a specific **sr**/**ni**/**nc**/**ncm**/**sccpmt**/**ssn** parameter combination. In Release 22.0, different routing indicator values can be specified for an Allowed SIO entry with a specific **sr**/**ni**/**nc**/**ncm**/**sccpmt**/**ssn** parameter combination, along with different next screening values for each entry. For example, the Allowed SIO screen in Release 22.0 can contain the following entries.

Output Example

```
RLGHNCXA03W 97-06-07 15:58:16 EST Rel 22.0.0
SCREEN = ALLOWED CGPA
SR    NI       NC       NCM      SSN      RI   SCCPMT   NSFI    NSR/ACT
IEC   240      001      010      012      DPC  017      CDPA    NSR1
IEC   240      001      010      012      GT   017      TT      NSR2
```

Split of Allowed SIO Table (Release 22.0)

The Allowed SIO screen has been changed in Release 22.0 to allow for different next screening values depending on the value of the service indicator (**si**) parameter. These options are summarized in Table 5-17 .

Table 5-17. Next Screening Options for the Allowed SIO Screen

SI	NIC	PRI	H0	H1	NSFI
00	single value or wildcard	single value, range, or wildcard	single value, range, or wildcard	single value, range, or wildcard	DESTFLD, DPC, BLKDPC, STOP
01, 02	single value or wildcard	single value, range, or wildcard	single value, range, or wildcard	single value, range, or wildcard	DPC, BLKDPC, STOP

SI	NIC	PRI	H0	H1	NSFI
03	single value or wildcard	single value, range, or wildcard	Not Specified	Not Specified	CGPA, CDPA, DPC, BLKDPC, STOP
04 - 15	single value or wildcard	single value, range, or wildcard	Not Specified	Not Specified	DPC, BLKDPC, STOP

Also in Release 22.0, messages can be screened on the message priority (PRI) field. In previous releases, the message priority was included in the Allowed SIO screening entry, but was not part of the screening process. This allowed only one message priority value, or range of values, for each Allowed SIO entry with a specific **sr**/**si**/**nic**/**h0**/**h1** parameter combination. In Release 22.0, different message priority values can be specified for an Allowed SIO entry with a specific **sr**/**si**/**nic**/**h0**/**h1** combination, along with different next screening values for each entry.

SS7 Message Rejection Due to Screening (Release 22.0)

The EAGLE produces these UIMs to alert the user that an MSU has been discarded because of gateway screening.

UIMs

- UIM 1005 — GWS rcvd OPC that is not allowed
- UIM 1006 — GWS rcvd DPC that is not allowed
- UIM 1007 — GWS rcvd OPC that is blocked
- UIM 1008 — GWS rcvd DPC that is blocked
- UIM 1009 — GWS rcvd SIO that is not allowed
- UIM 1010 — GWS rcvd a priority that is not allowed
- UIM 1011 — GWS rcvd TFC, AFTPC not in routing tbl
- UIM 1012 — GWS rcvd Clg Party that is not allowed
- UIM 1013 — GWS rcvd Cld Party that is not allowed
- UIM 1014 — GWS rcvd Translation Type not allowed
- UIM 1015 — GWS rcvd SCMG with not allowed AFTPC

These messages cannot be received at the SEAC unless the SEAS port is configured to receive unsolicited system maintenance messages. In release 22.0, when any of these UIMs are generated, the REPT-SCRREJ message is sent to SEAS, regardless of the configuration of the SEAS port to alert the user at the SEAC that the EAGLE has discarded an MSU because of gateway screening.

This feature allows the user to limit how many of these UIMs are sent to the EAGLE terminals and how many REPT-SCRREJ messages are sent to SEAS. This limit is configured with the **set-scrrej-prmtrs** command to control the number of UIMs sent to the EAGLE terminals, and with the SET-SCRREJ-PRMTRS command function on the SEAS interface to limit the number of REPT-SCRREJ messages are sent to SEAS.

SS7 over High-Speed Signaling Link (Release 23.0)

The ATM high-speed signaling link feature introduces signaling links transmitting at 1.544 Mb/s. Before Release 23.0, the fastest transmission speed on a signaling link was 64 kb/s. This feature uses the ATM (asynchronous transfer mode) protocol to implement this feature. ATM is a specific packet-oriented transfer mode that uses an asynchronous time-division multiplexing technique to multiplex information flow in fixed blocks called cells.

Tekelec's implementation of ATM differs from the Bellcore ATM model in these ways.

- The AAL5CP protocol support (primarily segmentation and reassembly of user data PDUs) is provided by the hardware, from the AATM applique of the high-speed ATM signaling link card, not from the software. The AATM applique also provides CRC10 support for OAM F5 ATM cell flows.

- The ATM driver is not a defined block in the protocol model, but is needed in the Tekelec implementation to control and interface with the AATM applique. The ATM driver provides the software interface to the AAL5CP hardware functionality. The ATM driver also provides the ATMM (ATM layer management) functions that are supported in the EAGLE.

- As a part of providing new ATM (MTP-level 2 equivalent) functions into the existing EAGLE software (based on MTP-3 and MTP- 2, not MTP-3 and SAAL), some of the interfaces to and from MTP level 3 are to and from the MAAL (management ATM adaptation layer), rather than the SSCF (service specific coordination function) handling all MTP-3 interaction.

SS7 SCCP-User Adaptation Layer (SUA) Request for Comment (RFC) (Release 31.10)

The current SUA Draft Version 3 support on the IPGWx GPL will be enhanced to comply with SUA RFC with the following feature highlights:

- SUA Draft Version 3 support on the IPGWx GPL is REPLACED with support for SUA RFC

- Support SCCP Connectionless messages via SUA CLDT and CLDR. Connection Oriented messages are not supported

- Support SUA Signaling Network Management Messages

- Limited support for Routing Context - up to 4 Routing Contexts per ASP (SUA and M3UA).

Hardware Requirements

The EDCM (single-slot) P/N 870-2372-01 Rev E is required for SUA RFC.

Limitations

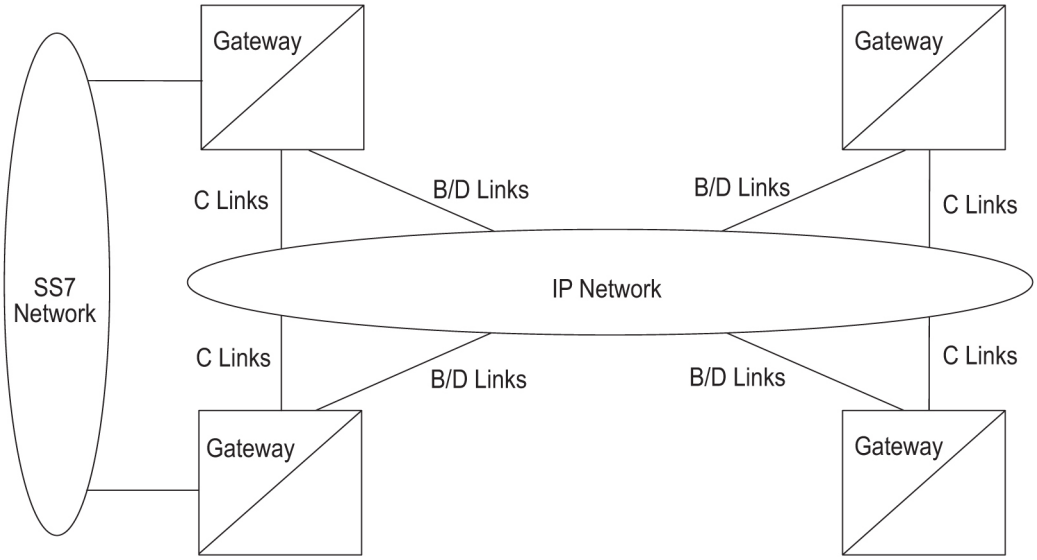
- The version of SUA implemented in this release is NOT backward compatible with the SUA version currently available on EAGLE releases.

- Only the Connections Message transfer part of the SUA protocol is supported for class 0 and class 1 SCCP messages.
- Limited support for Routing Context - up to 4 Routing Contexts per ASP (SUA and M3UA).
- To remove a routing context from a routing key, the routing key must be deleted and re-entered.

SS7-Over-IP Gateway for Point-to-Point Links (IP^7 Release 1.0)

This feature allows the use of an IP network in place of point-to-point SS7 links to carry SS7 MSUs. For example, the C links between a mated pair of STPs or B/D Quad links between STPs can be replaced by an IP transport network with gateway STPs deployed on both ends of the link. The 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. Full MTP level 3 functionality is provided with this feature.

Figure 5-18. STP Connectivity via MTP over IP



This feature provides single TCP/IP point-to-point connectivity by way of a new GPL, IPLIM, running on the DCM which, together with the hardware, provides a TCP/IP point-to-point connection to carry SS7 traffic.

To provide point-to-point connections, a number of administration steps must be performed, as follows:

- Links, link sets, destinations, and routes to those destinations via the existing EAGLE SS7 administration capabilities must be configured.
- Socket connections that should be created at each IPLIM card must be configured.

Unlike the point-to-multipoint configuration, the user is not required or allowed to configure SS7 Routing Key associations for **IPLIM** socket connections. A single socket exists on the DCM card running the **IPLIM** application. All SS7 traffic is carried over the single socket.

STC on E5-ENET Assembly (Release 37.0)

Description

The STC on E5-ENET Assembly feature supports the use of the E5-ENET card as an STC card running the **eroute** application.

The STC on E5-ENET Assembly feature allows the E5-ENET card to support the functions currently implemented on the STC card (SSEDCM, DCM, or EDCM-A assembly) for the EAGLE 5 Integrated Monitoring Support feature.

The E5-ENET card running the **erthc** GPL and the **eroute** application is referred to as the E5-STC card.

Because the SSEDCM STC card and the E5-STC card are both provisioned with card type stc and the eroute application, the two cards can be “hot-swapped” without re-provisioning the card information in the system.

NOTE: Hot-swapping the SSEDCM and E5-STC cards requires cable adaptors.

A minimum of two cards running the eroute application must be provisioned in the EAGLE 5 ISS to support the EAGLE 5 Integrated Monitoring Support feature (“n+1” to provide redundancy). A maximum of 32 STC/E5-STC cards can be provisioned.

HIPR cards must be installed in each shelf where E5-STC cards are installed.

If a shelf contains HMUX cards, then E5-STC cards must be provisioned in shelves adjacent to the shelf that contains the cards being monitored. The optimum configuration is to provision half of the E5-STC cards in the previous shelf and half in the next shelf.

If IP signalling links are being monitored, then only single-slot STC cards can be provisioned. HIPR cards must be used in the shelves where the IP links are located.

The E5-STC card operates at 12,000 TVG grants per second when the IP port operates at 100 Mbps full duplex, and at 1200 TVG grants per second when the IP port operates at 10 Mbps full or half duplex, or 100 Mbps half duplex. The E5-STC card is preconfigured to use auto-negotiation to set duplex and speed automatically.

Thermal management and alarming provisions are provided for the E5-STC card.

Feature Control Requirements

None.

Hardware Requirements

The STC on E5-ENET Assembly feature has the following hardware requirements:

- Two HIPR cards must be installed in the shelf where the E5-STC card is installed.
- Backplane cable adaptors

Limitations

The STC on E5-ENET Assembly feature has the following limitations:

- The suboptions {**-m**, **-p**, **-h**} of the -d option for the **`netstat`** command are not supported for E5-STC card.
- The E5-STC card does not preserve memory across card boots: therefore, the application does not remain intact across card boots.
- The performance of the E5-STC card is limited by the data rate of the Ethernet port and the capability of the external LAN/WAN.

STP LAN Feature (Release 20.0)

The EAGLE STP LAN feature allows the EAGLE to support a TCP/IP connection from any interface shelf to external hosts. Message signal units (MSUs) processed by the EAGLE can be copied and directed through the LAN interface to an external server or microcomputer application.

The STP LAN feature is an optional feature that is off by default. To use the STP LAN feature, it must be turned on by entering the appropriate command. Once this feature is turned on, it cannot be turned off.

This feature requires a new circuit card, the application communication module (ACM) card. The ACM card provides an Ethernet interface at the interface shelf backplane and the processing power required to support message encapsulation and TCP/IP support.

The Ethernet connection uses an adapter that is connected to a single port media access unit (MAU). The MAU is attached to the backplane interface connector of the ACM and supports standard Ethernet function.

From the MAU, the user may attach any compatible host system. The host system must be using TCP/IP as the higher layer protocol and must support 10BASE2 Ethernet as the transmission method.

The EAGLE software on the ACM card receives SS7 MSUs from the LIMs and ASM-SCCP cards and copies those MSUs into memory on the ACM card. The copied MSU is encapsulated and transmitted using TCP/IP packets and Ethernet to the host computer. The host computer is responsible for reassembling the original message and processing the data.

This feature is designed to provide an open system architecture, allowing third parties to design applications that can be attached as adjuncts to the EAGLE STP.

The gateway screening feature provides a copy function. When an MSU passes all screening criteria, the MSU is allowed to pass through the EAGLE STP out to the SS7 network. With the copy function, the MSU is copied, and the copy is sent through the STP LAN interface to a host application. This allows the host to track which MSUs from an external network were allowed to pass through the EAGLE.

The entire MSU is copied, including the MTP, which allows the host application to process the entire message. Total octet counts, including MTP level 2 and level 3, can be tallied and used for a variety of external measurements.

Messages from an X.25 signaling link reflect the translated message. The message is passed to the interface, and the screening and copy functions for an X.25 packet are invoked, after the EAGLE has completed protocol conversion. The result is an SS7 message that can be processed by the external application.

One ACM card is capable of servicing a maximum of 30 link interface modules (LIMs), regardless of the LIM type. This allocation is determined by the EAGLE's internal load balancing algorithm that is capable of reassigning LIMs to other ACM cards in the event an ACM card should fail, or if the traffic rate to a single ACM changes significantly.

Typically you should provision extra ACM cards for redundancy. By provisioning extra ACM cards, the load balancing software ensures that when an ACM card fails, the LIMs assigned to the failed ACM card are reassigned to another ACM card, providing it has been configured. The EAGLE STP can support up to 32 ACM cards.

The IP addresses of adjacent hosts are entered into the EAGLE by using the EAGLE database administration commands. The EAGLE also provides load balancing for all ACM cards. A threshold is set through the database

administration commands for each card, which determines when the EAGLE begins shedding traffic from the specified ACM card and redistributes that traffic to another ACM card.

This method of load balancing allows the user to configure each ACM card with a threshold, and provides an automatic mechanism by which traffic can be evenly distributed over multiple ACM cards. In addition to load balancing, this feature also reassigns traffic when an ACM card fails, so that all traffic can still be supported even when an ACM card fails. The ACM cards are capable of handling approximately 400 messages per card.

STPLAN Port to DCM (Release 26.0)

This feature ports existing STPLAN functionality to the DCM (Database Communications Module) hardware platform. The DCM provides the EAGLE with two 10/100 Base-Tx IEEE 802.3/Ethernet ports capable of carrying IP traffic.

This feature provides:

- the same functionality as STPLAN on ACM
- the same command interface
- the same network interfaces (single 10BaseT port; no 100BaseT)
- the same provisioning rules as for the ACM

NOTE: The DCM is NOT a drop-in replacement for ACM. If a DCM is used as a replacement for an ACM card, the replacement is not a “plug-in” type replacement. The STPLAN card and datalink must be reprovisioned. Also, fans and a new GPL for the DCM are required.

Hardware Requirements

The DCM card currently takes up two slots in the EAGLE shelf card cage due to the large heat sink on the top of the DCM card. Because of this, the DCM cannot be provisioned in any arbitrary slot. Because certain slots in the card cage are adjacent to the cage sides, and/or are adjacent to metal supports welded into the card cage, these slots cannot be used to house a DCM card.

Also, the DCM card requires a substantial amount of power. Due to the way the EAGLE fuses power pairs of card slots, the DCM should always be provisioned into an odd-numbered card slot. For example, fuse 1A provides power to both slots 1101 and 1102. The combined current draw for both of these slots must not exceed 3A or the fuse may blow. Inserting a DCM into slot 1102 when there is another card in 1101 could cause the total current requirements for both of these slots to exceed 3A.

Additionally, the shelf equipped with the DCM card must be equipped with fans in order to keep the card from overheating.

Fan Assembly

The fan assembly is provided with the EOAP and is also a necessary item for the DCM.

Note that the airflow provided by the Fan Assembly is approximately 100 cubic feet per second.

STPLAN SSEDCM Capacity Increase (Release 34.0)

Description

This feature allows the user to select either 10 Mbps or 100 Mbps for the data link speed of the Ethernet connection on the Single Slot Enhanced Database Communication Module (SSEDCM) STPLAN card.

Hardware Requirements

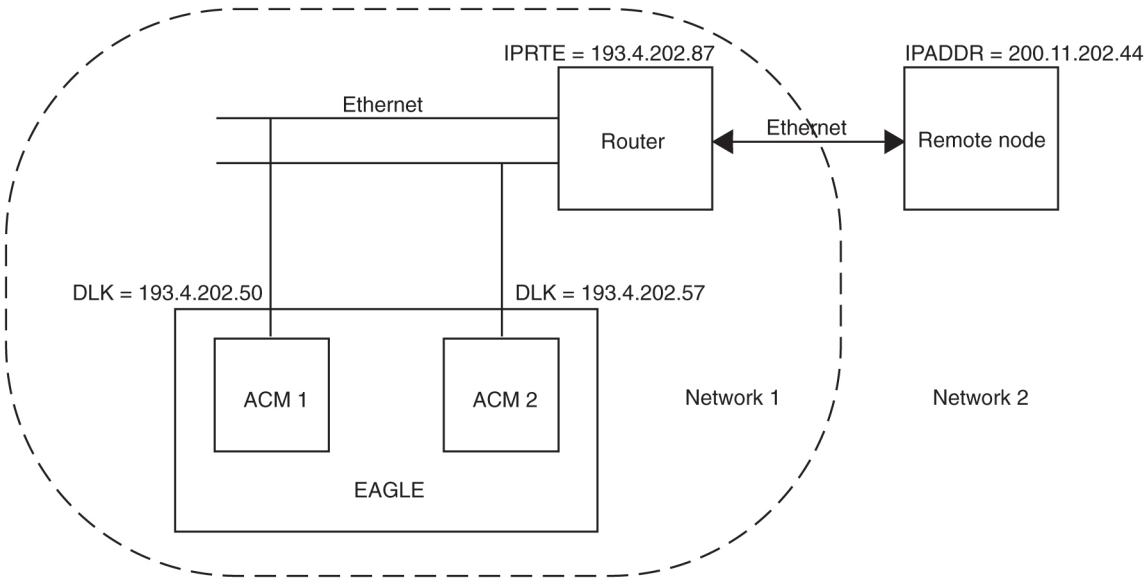
The VXWSLAN card is required for 100 Mbps data links.

STPLAN with Default Router (Release 23.0)

The STPLAN application allows the user to selectively copy received messages to a remote host for further processing. The external link consists of an Application Communication Module (ACM) equipped with an Ethernet interface using the TCP/IP protocol to communicate to an external processing device. Each ACM card supports a single destination host. In previous releases, each ACM and corresponding host had to be in the same network. This feature allows messages to be sent to a remote host on a different network using a TCP/IP router between the ACM and the corresponding host. Messages destined for a host in a different network or subnetwork are sent to the default router for routing. Messages destined for a host that is in the same network as the TCP/IP data link is not sent to the router but is sent directly to the remote host. The router is not part of the EAGLE.

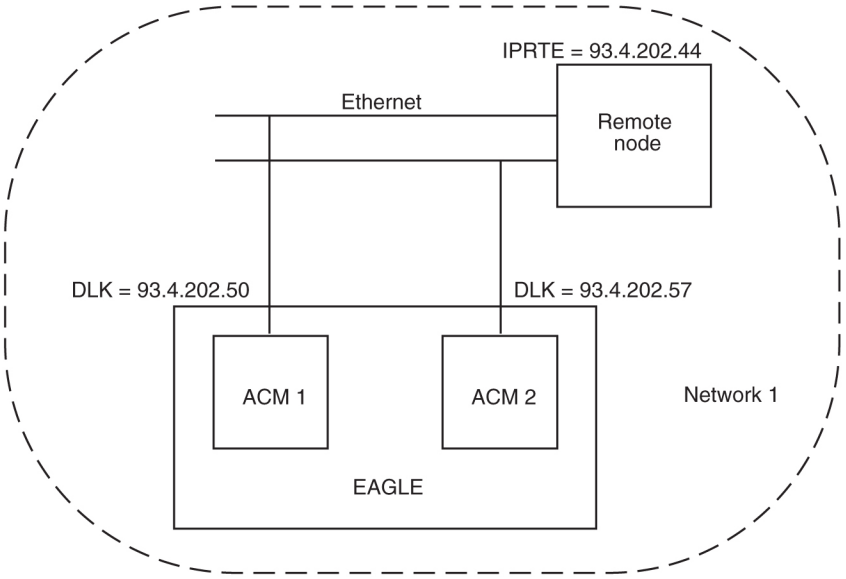
Figure 5-19 shows an example of using a router with the STPLAN feature. ACMs 1 and 2, with IP addresses 193.4.202.50 and 193.4.202.57, need to route their traffic to the remote host at IP address 200.11.202.44. The ACMs and the remote host are in two different networks, the network ID of the ACMs is 193.4.202 and the network ID of the remote host is 200.11.202. The EAGLE can only connect to TCP/IP nodes that are in the same network as the EAGLE. A TCP/IP router is placed in between the EAGLE and the remote host. The TCP/IP router is located in the same network as the EAGLE, with the IP address of 193.4.202.87. The messages can now be sent to the remote host through the TCP/IP router.

Figure 5-19. STPLAN Router Example



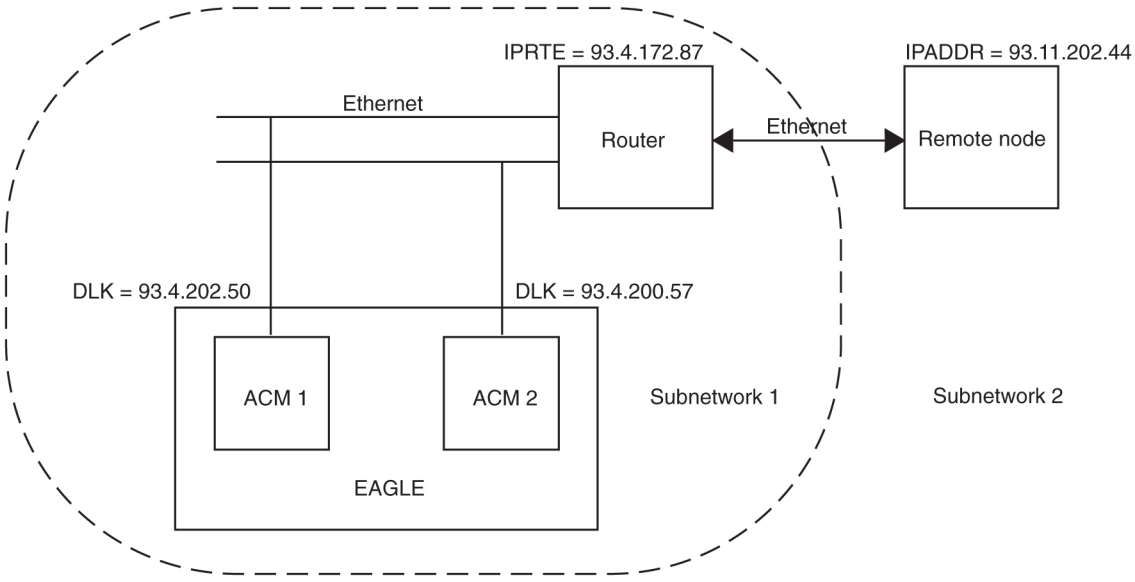
The EAGLE requires that a default router be entered when the class and network ID of the data link's IP address and the host's IP address do not match or when subnet routing is used. The EAGLE cannot tell whether the user has deployed a large network or is using subnet routing. In a large network, no TCP/IP routers are required because all the nodes are directly connected to a single Ethernet network as shown in Figure 5-20 .

Figure 5-20. STPLAN in a Large Network



If a user is using subnet routing and therefore multiple Ethernet networks, TCP/IP routers are required and must be configured in the EAGLE as shown in Figure 5-21 .

Figure 5-21. STPLAN Network with Subnet Routing



The EAGLE cannot distinguish between a large network and the use of subnet routing, and cannot detect the omission of a TCP/IP router. For example, the IP addresses of the TCP/IP data links and the remote node are the same in Figure 5-20 and Figure 5-21 . In Figure 5-20 , the remote node is in the same network as the TCP/IP data links, so no TCP/IP router is needed. In Figure 5-21 , the user is using subnet routing. The remote

node is in one subnetwork, and the TCP/IP data links are in another subnetwork. Even though the network portion of the IP addresses of the TCP/IP data links and the remote node are the same (93, a Class A IP address), a TCP/IP router is required because the user is using subnet routing.

If, when the user is configuring STPLAN according to the network in Figure 5-21 , the TCP/IP router is not configured with the **ent-ip-node** command, the EAGLE will not detect that the TCP/IP router has been omitted. No warnings will be given that the TCP/IP router has been omitted. The data link will be unable to function since it will not be able to connect to the TCP/IP node. The EAGLE sees the remote node as a TCP/IP node in the same network as the TCP/IP data links, because of the class of the IP addresses, and does not require the user to specify the **iprte** parameter of the **ent-ip-node** command.

SUA DAUD with SSN Support (Release 37.0)

Description

The SUA DAUD with SSN Support feature allows the EAGLE 5 ISS to update SCCP cards on the status of remote subsystems connected to the EAGLE 5 ISS and to use destination state audit (DAUD) messages that contain the **ssn** parameter to query the status of any subsystem.

The SUA DAUD with SSN Support feature enables to the EAGLE 5 ISS to perform the following functions:

- Update the SCCP cards with the status of remote subsystems to indicate whether the subsystems are allowed or prohibited
- Determine the status of any subsystem using destination audit (DAUD) messages that contain the **ssn** parameter.

When a node for a remote subsystem becomes available or unavailable, then the SUA DAUD with SSN Support feature allows the MAP table, maintained on the EAGLE 5 ISS SCCP cards, to be updated with the new status.

When a DAUD message containing an ssn parameter is sent over an SUA association to the EAGLE 5 ISS, Gateway Screening is performed by a card that contains the SS7IPGW, IPGWI, or IPGHC GPLs. The message is then sent to the SCCP card to query the availability status of the subsystem. The EAGLE 5 ISS sends one of the following responses based on the subsystem status:

- Status is available—Destination Available (DAVA) message
- Status is unavailable—Destination Unavailable (DUNA) message
- Status cannot be determined—Subsystem Status Unknown error message

Feature Control Requirements

None.

Hardware Requirements

None.

Limitations

The SUA DAUD with SSN Support feature has the following limitations:

- DAUD messages that contain the SSN parameter are not subjected to the Gateway Screening service.
- Subsystem status updates are implemented only when the route key is full SCCP (DPC-SI[3]-SSN). If a subsystem is present on a remote ASP connected by an AS that has only DPC or DPC-SI route key, then the IPGWx code does not send updates on the status for the remote subsystem to the SCCP management module.

Support 12 Million Ported Numbers (Releases 24.0, 25.0)

This feature is not supported in initial shipments of Release EAGLE 25.0. Tekelec will issue a notice when the feature becomes available.

The Support for 12 Million Ported Numbers feature allows the EAGLE to contain and process 12 million ported telephone numbers for the local number portability (LNP) application. Before Release 25.0, the EAGLE could contain only four million ported telephone numbers.

NOTE: For Release 24.0, the EAGLE supports only 4 million ported telephone numbers.

For the EAGLE database to contain up to 12 million ported telephone numbers, six **lnp 4digit** database objects must be in the database. Each **lnp 4digit** database object consists of two tables, one in the current partition and one in the backup partition of the database. The EAGLE database currently contains one **lnp 4digit** database object containing up to two million ported telephone numbers. This database object contains the database tables named **lnp_4dig.tbl** and **lnp_4dig.bkp**.

Refer to the *Database Administration Manual - LNP* and the *LNP Database Synchronization Manual* for the current details on this feature.

Support Changing the Linkset Name (Release 28.0)

With this feature, the EAGLE supports changing the linkset name via an EAGLE terminal or SEAS, without having to delete or change any other data associated with the linkset (e.g. **ent-ls** command parameters, links, routes).

The ability to change the linkset name via SEAS is supported via the following methods:

- A supplier-specific parameter for the **chg-ls** and **chg-gtwyls** commands
- Flow-through

All EAGLE data that referenced the old linkset name will now reference the new linkset name, except for *old* entries in the security log.

Support CHG-GTT to change the GTA (Release 35.0)

Description

The Support CHG-GTT to change the GTA feature enhances the **chg-gtt** and **chg-gta** commands to a GTT or EGTT range to be extended or reduced with a single command instead of deleting the original range and entering a new range.

For example, extending the range **5551234-5554567** to **5551234-5559999** can be performed in one command, using the **chg-gtt** or **chg-gta** command.

Likewise, reducing the range **5551234-5552999** to **5551234-5554567** can be performed in one command, using the **chg-gtt** or **chg-gta** command.

Hardware Requirements

The Support CHG-GTT to change the GTA feature has no hardware requirements.

Limitations

The Support CHG-GTT to Change the GTA feature has the following limitations:

- Range consolidation or 'self-healing' ranges, (**5551234-5554567** and **5554668-5559999**, for example) remain two entries. A user can delete **5554668-5559999**, then enter **chg-gtt** for **5551234-5554567** to be changed to **5551234-5559999**, but this action requires two commands.
- Overlapping ranges are rejected, (**5551234-5554567** and **5557000-5559999**, for example). The user cannot use **chg-gta** on the first entry such that the EGTA is greater than **5556999**, because it would create overlapping GTT entries. The same applies for single GTT entries.

Support for 2000 ITU Links per Node (Release 35.1)

Description

The Support for 2000 ITU Links per Node feature increases the total capacity of an EAGLE 5 ISS node from 1500 to 2000 links.

NOTE: Although the Support for 2000 ITU Links per Node feature increases the total capacity of the node, the increase applies to ITU links only. The maximum number of ANSI links that can be supported by the node remains 1500.

This feature requires a Feature Access Key.

Hardware Requirements

The Support for 2000 ITU Links per Node feature has the following hardware requirements:

- HIPR cards installed on every provisioned shelf in the system
- The following link/card counts are supported:
  - — Maximum 115 LIM-ATM cards
  - — Maximum 100 IPLIM cards
  - — Maximum 64 IPGWx cards
  - — Maximum 64 SE-HSL links

Limitations

The Support for 2000 ITU Links per Node feature has the following limitations:

- This feature is supported for ITU links only. STP-LAN and ANSI links are not supported.
- The following cards are not supported for ITU configurations above 1500 links/node: MPL, MPL-T, LIM-ATM.
- The following cards are not supported for any configuration above 1500 links/node: LIM-DS0, LIM-OCU, LIM-V.35, LIM-AINF, LIM-ILA, LIM-EILA

Support for 32 Prepaid SMS Intercepts (EPAP 9.0)

Description

The Support for 32 Prepaid SMS Intercepts feature increases the number of supported Prepaid SMS Intercepts from 8 to 32.

Supported GTT (Global Title Translation) destinations have been expanded to 32, and IN SCP (Intelligent Network Service Control Point) platforms and EPAP portability types have been expanded to 32 from 8.

The PPSMS (Pre-paid Short Message Service) Phase 1 feature uses a G-Port DN portability type (PT) field to identify the types of prepaid subscribers whose originated short messages (as part of SMS) need to be intercepted and forwarded to a corresponding intelligent network platform for verification.

In EPAP 9.0, the PPSMS Phase 2 feature expands the PT range to support 32 types of prepaid subscribers.

For PPSMS, the PT parameter on the **`ent_sub`**, **`upd_sub`**, and **`rtrv_sub`** commands identifies a DN as one of 32 types needing PPSMS intercept.

Hardware Requirements

None.

Limitations

None.

Support for IP7 8.0 Gateway Features (EAGLE Release 30.0/ IP7 Secure Gateway Release 8.0)

Description

EAGLE Release 30.0 supports the feature content of IP ^{7} Secure Gateway Release 8.0 (i.e. SCTP Checksum Update, M3UA Protocol Enhancements), as well as all IP ^{7} content supported by EAGLE Release 29.x.

Support for 32 Prepaid SMS Intercept Platforms (Release 37.0)

Description

The Support for 32 Prepaid SMS Intercept Platforms feature enhances the capability of the EAGLE 5 ISS to support routing from 3 to a maximum of 32 Intercept Platforms and increases the number of Prepaid Portability Types by the EPAP to 32 to specifically identify a subscriber with an SCP.

The Support for 32 Prepaid SMS Intercept Platforms feature increases the number of Prepaid Portability Type (PPT) subscribers and Intelligent Network (IN) SCP Point Code + Routing Indicator (PC + RI) translations that can be supported by the Prepaid SMS Intercept Phase 1 (PPSMS) feature to 32. Each translation corresponds to an IN platform and can be either ITU-N, ITU-I or a combination of the two.

Any subscriber that is not one of the 32 PPTs is considered to be a postpaid/contract subscriber.

The Support for 32 Prepaid SMS Intercept Platforms feature allows any Mobile Station Integrated Services Digital Number (MSISDN) in the RTDB to be associated with any of the 32 PPTs. Each PPT can then be associated with any of the IN platforms.

Loadsharing can be performed across 8 of the IN platforms, using the MAP and MRN tables. If the Transaction-Based Weighted GTT feature is turned on, then loadsharing can be performed across all 32 platforms.

If the Flexible GTT Loadsharing (FGTTLS) feature is turned on, then lookup in the MAP or MRN table is performed using the set ID (SETID) obtained from the PPSOPTS table. If the FGTTLS feature is turned off, then lookup is performed on only the default MAP or MRN set.

NOTE: The Support for 32 Prepaid SMS Intercept Platforms feature removes the dependency of the PPSMS feature on the G-Port feature. PPSMS can now be enabled without enabling G-Port.

Feature Control Requirements

The Support for 32 Prepaid SMS Intercept Platforms feature is enabled when the PPSMS feature is enabled. The G-Port feature does not have to be enabled before enabling the PPSMS feature.

Hardware Requirements

None.

Limitations

None.

Support for LSMS Audit Enhancements (Release 26.1)

LSMS users need a method of auditing locally provisioned data as well as data that is sent from the NPAC to the LSMS and subsequently sent to the EAGLE. Currently the following data cannot be audited from the LSMS and raises concerns about database consistencies.

- Default GTT
- Override GTT
- NPA-NXX Split Data

This feature provides support for the LSMS audit of default GTT, override GTT, and NPA-NXX split data residing at the EAGLE. The LSMS audits the data, which is locally provisioned at the LSMS, against the data at the EAGLE LNP databases. EAGLE support allows LSMS retrieval of the data from the EAGLE database. (The LSMS will offer a mechanism to reconcile any discrepancies detected.)

In previous releases, even though the EAGLE allows the LSMS to provision Default GTT, Override GTT, or service provider database entries, it provided no mechanism to allow the LSMS to retrieve the DB entities that it has provisioned. This hampered the LSMS from determining exactly what was present in the EAGLE LNP DB for these entity types: the LSMS could add and delete these entity types, but could not retrieve them.

This feature rectifies this situation by adding the following new commands to facilitate additional auditing capabilities at the LSMS:

- **`vfy-lnp-6ddt`**
- **`vfy-lnp-lrnovr`**
- **`vfy-split-npa`**

These commands are used similarly to the existing **`vfy-lnp-10dt`** command:

- They are sent by the LSMS to the EAGLE via the OAP across the OAP↔EAGLE serial interface (also known as the "2 TN/sec channel," or the "slow channel").
- They support retrieval of a single DB entity (see section 3.1.2 on page 13)
- The command response is returned to the LSMS via the OAP, and is formatted similarly to the **`vfy-lnp-10dt`** output (i.e. machine-readable).

See “Component Interaction Scenario” more information on these commands.

Auditing the EAGLE via High-Speed Audit

EAGLE Release 25.0 introduced a new feature, "Enhanced Bulk Download & Audit," which allows the LSMS to audit the subscription component of the EAGLE's LNP DB at a very high speed, using an ethernet connection that directly connects the LSMS and EAGLE. This audit proceeds as follows:

1. LSMS tells EAGLE, via the ethernet connection, what range of subscriptions are to be returned. A starting and ending NPANXX is specified, and all subscriptions provisioned within that range are returned.

2. The BLM card on the EAGLE (which has a complete copy of the EAGLE LNP DB resident in its RAM memory) retrieves each subscription in the start/end range from its database, computes a checksum for the subscription, and returns the subscription's TN (i.e. its “key”) and computed checksum to the LSMS, again using the ethernet connection

3. LSMS computes a checksum for each of the requested subscriptions, and then compares them against the checksum returned by the EAGLE:

    - Matching checksums indicate that the subscription information on the EAGLE exactly matches the information on the LSMS.

    - Mismatching checksums indicate that the EAGLE has the subscription in its database, but that one or more attributes of the subscription (e.g. LRN) are different. The LSMS should update the subscription information in the EAGLE to bring the EAGLE into sync with the LSMS.

    - If the EAGLE does not return a TN/checksum pair for a subscription that the LSMS has, this indicates that the EAGLE is missing the subscription. The LSMS should add the subscription to the EAGLE database.

    - If the EAGLE returns a TN/checksum pair for a subscription that the LSMS does not have in its database, this indicates that the EAGLE still has a subscription that should have been deleted. The LSMS should delete the wayward subscription from the EAGLE's database.

The Support LSMS Audit Enhancements feature also allows auditing, via the high-speed ethernet link, of the EAGLE's database components:

- default GTT (NPANXX)

- override GTT (LRN)

- NPA split

The auditing of the default GTT, override GTT, and NPA split database entities takes place in a manner similar to that described above for subscriptions, i.e. LSMS will request checksums for a range of entities, and the EAGLE returns the information (DB entity key/checksum) via the high-speed ethernet connection.

Component Interaction Scenario

As mentioned, the new auditing and provisioning capabilities that these features provide can take place over either the OAP serial channel, or over the high-speed IP channel. The following scenarios describe the sequence of events that occur over each.

New Audit Capabilities via OAP Serial Channel

In the following list, the item numbers correspond to the *circled* numbers in **Figure 5-22** .

1. The user at the LSMS terminal decides to audit something via the serial OAP connection: override GTT, default GTT, Split NPA, subscriptions, etc. The user enters auditing parameters (e.g. start/end range, etc.) at LSMS GUI screen.

2. The LSMS sends a request to the OAP requesting the first DB entity to be retrieved for audit. The OAP converts this request into a "SEAS-like" command (e.g., **vfy-lnp-6ddt**).

3. A SEAS-like retrieval command is forwarded to the EAGLE.

4. The EAGLE retrieves the requested DB entity from the active OAM fixed disk and formats the data into a response using "SEAS-like" syntax.

5. A “SEAS-like” response is sent to the OAP in ASCII format

6. The OAP converts and transmits the ASCII response into a format suitable for the LSMS.

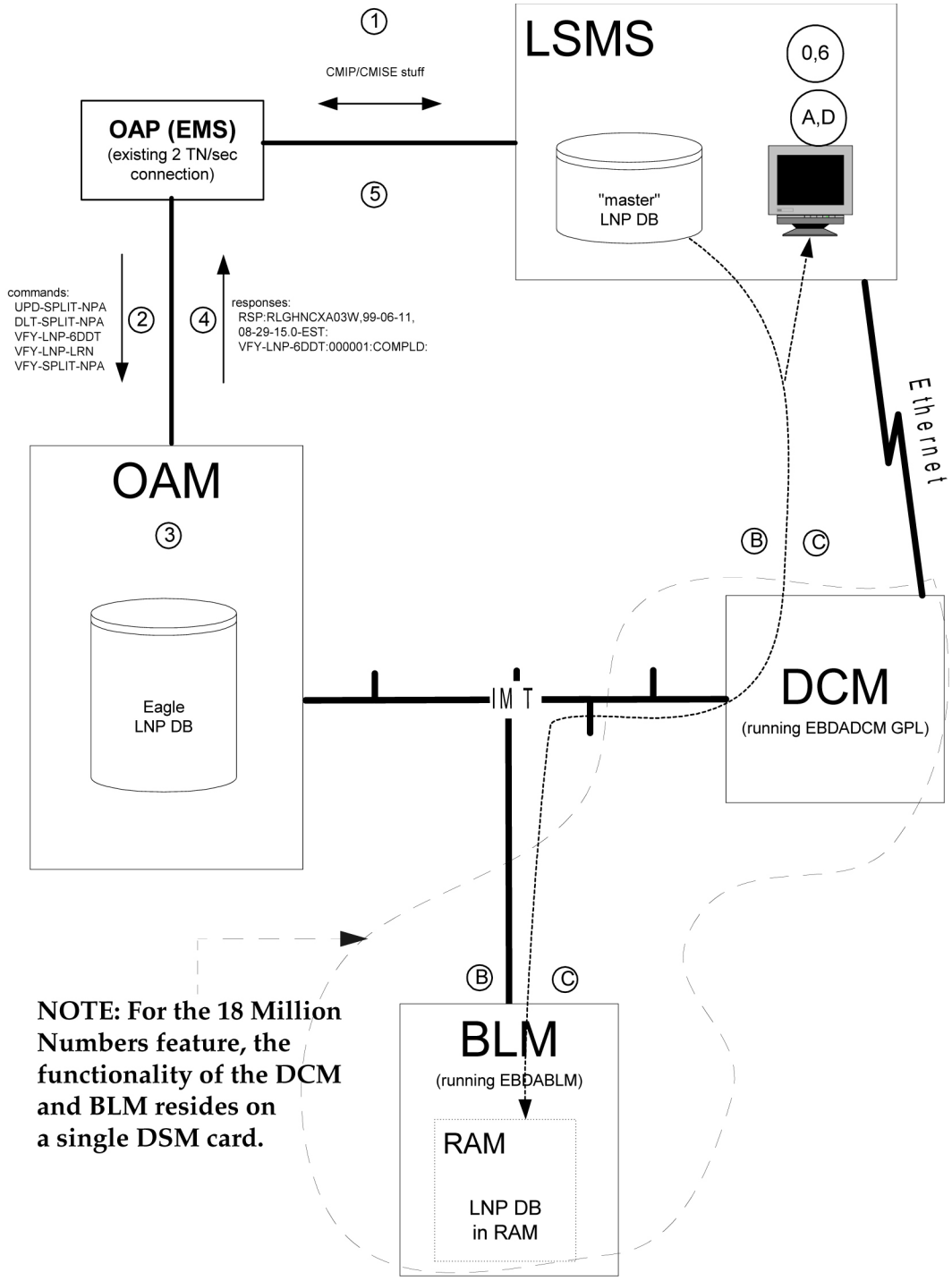
7. The LSMS compares the EAGLE DB entity against its own database, and displays discrepancy information to the user at the LSMS console.

This retrieve/compare/display cycle repeats until all DB entities have been audited, or until the LSMS user cancels the audit.

Should the LSMS user elect to reconcile the problem(s) detected by the audit, the reconcile commands (e.g. **upd-split-npa**, etc) are sent to the EAGLE using the same OAP serial connection. If the EAGLE database was severely out of sync, the LSMS operator can elect to reconcile the problem using the Enhanced Bulk Download feature.

Note that the LSMS operator has a choice as to how any DB updates are sent to the EAGLE: the LSMS operator can choose to send them either via the serial connection (makes sense if the number of commands to be sent is small), or via the high-speed IP connection (makes sense if the number of commands is very large).

Figure 5-22. LSMS Auditing/Split Provisioning: Sequence of Events



New Audit Capabilities via High-Speed IP Channel

The items in the following lettered list correspond to the *circled* letters in **Figure 5-22** :

1. The user at the LSMS terminal decides to audit something via the high-speed LSMS↔EAGLE IP connection: override GTT, default GTT, Split NPA, subscriptions, etc. The user enters auditing parameters (e.g. start/end range, etc.) at LSMS GUI screen.

2. The LSMS sends a request to EAGLE's DCM card (running EBDADCM GPL) via the IP connection, which is forwarded across IMT to EAGLE's BLM card (running EBDABLM GPL).

3. The BLM card retrieves requested DB entities (e.g. Override GTT entries), generates a CRC-32 checksum for each entity, and returns the entity key (e.g. for Override GTT entity, the key would be the LRN) and its corresponding checksum to the DCM, which is then forwarded to the LSMS via the high-speed IP connection.

4. The LSMS retrieves the corresponding DB entity from its own database, computes the CRC-32 checksum, then compares the checksum against what the EAGLE has provided. Any mismatching of the checksums indicates that what the EAGLE has for this entity is different than what the LSMS has. Furthermore, the DB entity keys that are returned from the EAGLE allow the LSMS to detect superfluous entries in, and entries that are missing from, the EAGLE LNP DB. All discrepancies are displayed to the LSMS operator.

This retrieve/checksum/compare/display cycle repeats until all DB entities have been audited, or until the LSMS user cancels the audit.

Should the LSMS user elect to reconcile the problem(s) detected by the audit, the reconcile commands (e.g. **upd-split-npa**, etc.) would likely be sent to the EAGLE using the OAP serial connection. If the EAGLE database was severely out of sync, the LSMS operator could elect to reconcile the problem using the Enhanced Bulk Download feature.

Limitations

The new verify (**vfy-xxxxx**) commands mentioned above do not support the retrieval of ranges of database entries. Instead, each command accepts the key of a single database entity to be retrieved. The command output shows the details of the single database entity that was specified, assuming that the entity exists, or error information (if it doesn't).

Support for LSMS Split Provisioning (Release 26.1)

NPA-NXX splits currently are provisioned locally at the LSMS and at the EAGLE. This is not the optimum method of provisioning LNP data, as the LSMS can service multiple EAGLEs, making coordination of entering split data cumbersome.

This feature allows NPA-NXX Split data to be provisioned at the LSMS and forwarded to the EAGLE, instead of being provisioned at the EAGLE separately. This feature supports a single point NPA Split administration from the LSMS.

Over OAP Serial Channel

This feature implements a set of commands that allow the LSMS to provision and query NPA split information at the EAGLE, using the connection that exists between the EAGLE↔LSMS provided by the OAP. These new commands are:

- **upd-split-npa**

- **dlt-split-npa**
- **vfy-split-npa**

See the *Commands Manual* for more information on these commands.

Via Enhanced Bulk Download

This feature supports downloading of NPA split information to the EAGLE as part of a high-speed bulk download. This existing high-speed bulk download facility has been expanded to allow NPA split information to be downloaded.

Limitations

The new verify (**vfy-xxxxx**) command mentioned above does not support the retrieval of ranges of database entries. Instead, each command accepts the key of a single database entity to be retrieved. The command output shows the details of the single database entity that was specified, assuming that the entity exists, or error information (if it doesn't).

Support for Matching Self-ID Rule in SEAS CHG-SID (Release 22.0)

In previous releases the SEAS ASGN-SID and CHG-SID command functions could change the self ID point code and CLLI of the EAGLE if either SEAS command were entered. From the SEAS interface, only the ASGN-SID command function can change the point code and CLLI of the self ID. The CHG-SID command function is not supposed to change the point code or CLLI of the EAGLE, but those parameters are used to verify whether they match the current point code and CLLI of the EAGLE.

This feature adds a rule to the SEAS CHG-SID command function on the EAGLE that requires that the specified point code and CLLI to match the current self ID point code and CLLI of the EAGLE. If they do not match the current values, the CHG-SID command attempt is rejected.

This gives customers using the SEAS interface protection against accidental changing of the EAGLE's self ID. This feature does change the functions of the SEAS ASGN-SID and EAGLE **chg-sid** commands.

Support for MTP Status Functions (IP^7 Release 2.0)

This feature, available only on DCM cards that support the **ss7ipgw** application, 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 SS7 network congestion
- Abate congestion
- Obtain SS7 User Part Unavailability status

Support for Provisioning Multiple EPAPs (Release 29.0)

Currently, it is only possible to provision a single mated pair of MPS nodes, where each MPS node contains one EPAP A and one EPAP B. EPAP A contains a PDB and an RTDB. EPAP B contains only an RTDB. For customers who need to deploy more than one pair of MPSs, this requires them to provision each pair separately.

Many customers desire the ability to add more MPSs without having to change their provisioning system, or provision from multiple sources.

This feature is transparent to the PDBI clients. Each client can provision data in the same manner, no matter if it is provisioning a single MPS pair, or multiple MPS pairs.

With EPAP 3.0, customers may choose to add EAGLEs to their network without changing the way that they provision data. EPAP Software updates the Real-time databases at the additional sites. The two MPSs that contain the PDB are called "provisionable" because these are the sites to which the customer provisioning application may connect. The additional MPSs are called "non-provisionable."

Newly added non-provisionable MPSs will use the Selective Homing of EPAP RTDBs feature to specify the PDB(s) from which to receive updates.

Hardware Requirements

The MPS platform is required to support the ability to install both provisionable and non-provisionable EPAP MPSs.

Enhancements to the User Interface

With the addition of Support for Provisioning multiple EPAP RTDBs, references to the "Local" and "Remote" PDB may no longer have meaning. These references will be changed throughout the text UI and GUI to specify the IP address of the PDB being identified.

Upgrade Considerations

This feature does not impact the EPAP 1.x/2.x to 3.0 upgrade. New EAGLEs may not be included for provisioning until all affected sites have been upgraded to EPAP 3.0. Interaction with EAGLE is not affected by this feature.

Support for SCCP XUDT/XUDTS Messsages, In-Sequence Delivery of Class 1 SCCP UDT/XUDT Messages (Release 31.6)

Description

With the introduction of various new applications in the wireless industry, the size of application data on top of SCCP layer has increased to a point where it does not fit in a single MTP message. This has led to the requirement of segmentation and reassembly of the SS7 messages - both at SCCP level and at higher application levels (like TCAP). These messages are carried over SCCP class 0 protocol and SCCP class 1 protocol. Class 1 is used when the sequence of the segments of the message and number of message within the same transaction or dialogue needs to be guaranteed at the arriving node.

The EAGLE distributed architecture and internal method of load sharing across SCCP processing cards means that one message of a sequence could arrive at one SCCP card for processing, while another message in the same sequence could arrive at a different SCCP card for processing. Depending upon the current loads and buffer levels in the two SCCP cards, it is possible that the second message may complete SCCP processing and arrive at the outgoing link ahead of the first message. Thus, the second message will arrive at the destination before the first, and the end node will be unable to process the sequence.

The In-sequence Delivery of SCCP Messages feature addresses the in-sequence delivery requirement of SCCP protocol class 1 message.

The Support of SCCP Extended User Data (XUDT)/Extended User Data Service (XUDTS) messages feature addresses the processing of EAGLE destined XUDT/XUDTS messages and in-sequence delivery requirement of SCCP XUDT/XUDTS protocol class 1 messages.

Long User Data (LUDT)/Long User Data Service (LUDTS) messages along with other non-UDT/XUDTS SCCP messages will not be supported by SCCP. UIM 1023 is generated on the incoming LIM card when LUDT/LUDTS messages is received and is destined to EAGLE. MTP routed LUDT/LUDTS messages will continue to be supported by EAGLE. However, GWS, TT mapping and Network Security features will not support LUDT/LUDTS messages.

EAGLE support is provided for the following features and functions when processing XUDT/XUDTS messages:

- GTT, EGTT, VGTT
- All supported link types, including E1/T1 MIM, E1-ATM HSL, IPLIMx, and IPGWx
- Multiple and duplicate point codes
- SLAN and Sentinel Copy
- G-Flex
- LNPMR services for Class 1 UDT messages
- INMPR services (but not INPQ)
- G-Port, G-Port Message Relay, and IS-41 to GSM Migration - XUDT/XUDTS messages are supported as long as the G-Port GSN SRI or PPSMS query or IS-41 Loc Req messages are not segmented. If a query is

segmented, it will treated as a G-Port non-SRI or IS-41 non-Loc REq message and message relay will be performed using the SCCP CDPA portion of the message.

The In-sequence delivery of SCCP messages feature addresses the in-sequence delivery requirement of SCCP protocol class 1 message.

The Support of SCCP XUDT/XUDTS messages feature addresses the processing of EAGLE destined XUDT/ XUDTS messages and in-sequence delivery requirement of SCCP XUDT/XUDTS protocol class 1 message.

- Both ANSI and ITU Class 1 UDT and XUDT/XUDTS (both Class 0 and Class 1) messages are supported.

Limitations

- The NP, EIR, LNP, PPSMS, MNPSMS and MAP Screening features that use TCAP data do not support XUDT/XUDTS messages.
- EAGLE does not perform re-ordering of XUDT/XUDTS Segmented messages.
- EAGLE does not perform any conversion of XUDT/XUDTS to UDT message and vice versa.
- The Weighted SCP Load Balancing and IGTTLS features do not support load sharing of messages across equal cost destinations for Class 1 UDT/ XUDT/XUDTS messages (when **randsls** is OFF or CLASS0)
- EAGLE supports XUDTS messages as long as the message length is <=272 bytes.

Support for Secure Gateway Functionality through IP^7 7.0 (Release 29.0)

EAGLE Release 29.0 supports the feature content of IP ^{7} Secure Gateway Release 7.0 (i.e. IP User Interface: Telnet Support and FTP Retrieve and Replace.

Support for TALI Architecture (IP^7 Release 4.0)

Each release of the IP ^{7} Secure Gateway is built to the current level of the Transport Adapter Layer Interface (TALI) protocol. This release of the IP ^{7} Secure Gateway supports TALI Release 3.0.

Support for the CLLI Parameter for Adding or Changing Linksets (Release 22.0)

In Release 22.0, the EAGLE accepts the FE-CLLI parameter when adding a linkset, changing a linkset, and displaying linksets on the SEAS interface. The FE-CLLI of the point code is not stored in the linkset table, but in the destination point code table.

When the FE-CLLI is specified while adding a linkset or changing a linkset's attributes from the SEAS interface, the FE-PC and FE-CLLI are compared with entries in the destination point code table of the EAGLE. If the specified values match an entry in the destination point code table, the command adding the linkset is accepted. If either

value does not match any entries in the destination point code table, the command is rejected. When changing a linkset's attributes from the SEAS interface, the FE-CLLI value cannot be changed.

The EAGLE's linkset configuration commands, **ent-ls**, **chg-ls**, and **rtrv-ls**, have also been changed to support this feature. The **clli** parameter has been added to the **ent-ls** and **chg-ls** commands. If the value of the **clli** parameter, specified with either the **ent-ls** or **chg-ls** commands, does not match the value of the CLLI of the adjacent point code, shown in the destination point code table by the **rtrv-dstn** command, the command is rejected with this error message.

Error Message

```
E2335 Cmd Rej: CLLI is not identical to that of matching Destination
```

The output of the EAGLE's **rtrv-ls** command has been changed to support this feature. The following is an example of the output of the **rtrv-ls** command if a CLLI has been assigned to the adjacent point code of the linkset.

Support for the New Linkset Name Parameter for Changing the Attributes of a Route (Release 22.0)

The linkset name parameter (**nlsn**) has been added to the EAGLE's **chg-rte** command and to the SEAS CHG-RTE command function. This eliminates the requirement on the EAGLE to remove an existing linkset and re-enter the linkset with a different linkset name to change the linkset name.

Error Messages

The following error messages displayed on the EAGLE terminal have been added to the **chg-rte** command.

- Either the **nlsn**, or **rc** parameters must be specified with the **chg-rte** command. In neither of these parameter are not specified, the command is rejected and this error message is displayed.

```
E2136 Cmd Rej: At least one optional parameter is required
```

- The new linkset specified by the **nlsn** parameter cannot be assigned to any existing routes. If the new linkset is assigned to any existing routes, the command is rejected and this message is displayed.

```
E2355 Cmd Rej: Linkset already assigned to route
```

- If a new link set name (**nlsn**) is specified in the **chg-rte** command, that link set name must be defined in the linkset table. If the new linkset name is not defined in the linkset table, the command is rejected and this error message is displayed.

```
E2346 Cmd Rej: Linkset not defined
```

- If a new link set name (**nlsn**) is specified in the **chg-rte** command, that linkset must contain at least one signaling link. If the new linkset does not contain at least one signaling link, the command is rejected and this error message is displayed.

```
E2128 Cmd Rej: Linkset assigned to route must have at least one link
```

- The new linkset specified by the **nlsn** parameter can be assigned to an adjacent point code that is a cluster point code as long as the linkset type of this linkset is either B, C, or D. If the linkset type of the linkset that is assigned to a cluster point code is either A or E, the command is rejected and this error message is displayed.

```
E2349 Cmd Rej: Link Set Type invalid for Cluster Destination
```

Support for Up to 41 IPLIMx DCMs (IP^7 Release 2.2)

The IP ^{7} Secure Gateway supports up to 41 DCMs that run either the **iplim** application or the **iplimi** application. In previous releases, the limit of DCM cards supported for the **iplim** application was six.

In addition, the IP ^{7} Secure Gateway can support two DCMs that run the **ss7ipgw** application.

Support G-Flex at 1700 TPS per DSM (ANSI only) (Release 31.6)

This feature allows the DSM card to run at 1700 TPS when the G-Flex feature is turned on in an ANSI environment. Only G-Flex can be on to achieve the 1700 TPS per DSM.

This feature provides an STP option to allow the DSM card to run at 1700 TPS when the G-Flex feature is turned on in an ANSI environment.

Limitations

- G-Flex at 1700 TPS per DSM is supported only when G-Flex is the only database feature active and there are no ITU service selectors provisioned.

Support Java 1.5 on EPAP (EPAP 9.0)

Description

The EPAP GUI has been upgraded to be compatible with Java 1.5. The EPAP GUI now requires Java 1.5 or later.

If your browser does not , when you attempt to connect to the EPAP GUI, your browser will be prompted to install Java 1.5. The Java installation process is described in the *EPAP Administration Manual*.

Hardware Requirements

None.

Limitations

None.

Support LSMS Disaster Recovery (Release 23.1)

When a disaster occurs and the main LSMS is disabled, the user can switch from the main LSMS to an optional shadow LSMS. The shadow LSMS is a geographically remote LSMS that actively receives data from the NPACs. The shadow LSMS serves as a backup to the main LSMS. The shadow LSMS is continually queuing the transactions for the OAPs. The OAPs are configured to receive data only from the main LSMS. Before the switchover can occur, the shadow LSMS must be in stable condition. The shadow LSMS should have no active alarms or hardware failures and cannot be in the recovery mode with any NPAC.

Once the health of the shadow LSMS is confirmed, the OAPs must be disassociated from the main LSMS and associated with the shadow LSMS. When an OAP tries to establish the association with the shadow LSMS, the resynchronization procedure automatically begins.

Before Release 23.1, changing the association of the OAP and LSMS was performed manually from the OAP and often required the assistance of Tekelec Technical Services. This feature allows a user to use the EAGLE terminal to change the association of the OAPs and the main LSMS and shadow LSMS. Two new commands have been introduced to change the OAP LSMS association, **chg-oap-config** and **rtrv-oap-config**.

chg-oap-config

The **chg-oap-config** command is used to change the LSMS association with the OAP in the EAGLE database.

rtrv-oap-config

This command displays OAP configuration information in the EAGLE database.

Auditing the OAP Database

In order to keep OAP database synchronized with the EAGLE, a checksum is created using all of the OAP configuration data stored on the EAGLE. The OAP also calculates this checksum based on the data it has. This checksum is returned by the OAP with every forced maintenance poll allowing the EAGLE to compare and act on the result. If the checksum values do not agree, the EAGLE generates a minor alarm (UAM 0364) within 10 seconds:

Support of E1 Master Clock Interface for SS7 Signaling Links (Optional) (Release 22.2)

As an option for Release 22.2, the E1 Master Clocking TDM card provides support for Master E1 clocking. The TDM-E1 card supports master clocking of high-speed links at E1 speeds (2.048Mbits/sec) and provides E1 clocks to all cards in the EAGLE system.

Upgrade Considerations

The following considerations must be taken into account when upgrading to this option:

- Customers with Release 22.2 hardware who want to add the Master Timing support option must upgrade their TDM to the TDM-E1.
- Customers who choose to upgrade a system currently using DS-0 links will not have these links available after upgrade when using Master clocking.

Support of E1 Interface for SS7 Signaling Links (Optional) (Releases 22.2, 24.0)

The E1 Interface card (E1/Channel appliqué) provides a 2.048 Mbit/sec E1 interface that complies with ITU-T recommendations G.703, G.704, and G.706.

Refer to the *Database Administration Manual - SS7* for current information on this feature.

Suppression of Gateway Measurements on Non-Gateway Linksets (Release 25.0)

Release 25.0 adds the capability to exclude non-gateway linksets from the P_GTWY schedule. The exclusion can be applied to reports going to the terminal interface, the SEAS interface, both, or neither. The P_GTWY measurement schedule allows for the collection and reporting of gateway-related data from the STP. The P_GTWY schedule, as currently implemented in the EAGLE, provides measurement data on all linksets defined in the linkset table.

This new feature, however, provides the EAGLE with the capability of optionally reporting only on linksets that are defined as gateway linksets. Gateway linksets are linksets that have a screenset assigned to them, or that have been defined as gateway linksets via SEAS.

The implementation of this feature does not change the measurement data provided by the schedule, but rather controls which linksets are included in the report. This feature also does not change the SEAS command interface to the EAGLE for the collection of the P_GTWY schedule.

The optional capability is controlled by a new field, **gtwy_ls_fltr**, which is located in the measurement control table, and can be initialized to independently control reports for EAGLE HMI and SEAS interfaces.

Synchronous E1 High Speed Link (SE-HSL) (Release 34.0)

Description

The Synchronous E1 High Speed Link (SE-HSL) feature provides “unchannelized” E1 high-speed link interfaces (as defined in ITU-T Q.703 Annex-A) where time-slot 0 is used for framing and error control, and the remainder of the bandwidth equivalent to 31 channels of 64 Kbps data is used as a single data link yielding a total capacity of 1.984 Mbps. SE-HSL links can be used to connect two signaling points that require bandwidth greater than that provided by 8 low-speed links. The HC-MIM card is used as an SE-HSL card; any 2 of the 8 HC-MIM card ports can be used for SE-HSL E1 interfaces.

The SE-HSL feature supports the following functions:

- Timing modes (external master and line), HDB3 and AMI encoding, and CRC4 encoding.
- Local and line loopback testing at the port level.
- Provisionable FISU/LSSU rate to ensure a minimum density of signaling units on outbound links. The default rate is 1 signaling unit per millisecond.
- The new apcntype linkset parameter to support changeover messages for ITU National links in China and outside of China.

- A Feature Access Key must be enabled to provide a maximum of 4, 8, 16, 32, 40, 48, 56, or 64 SE-HSL signaling links in the system. A mixture of channelized links and SE-HSL links is not supported on an HC-MIM card.
- Linkset commands—The rtrv-ls output shows LSN headings for adjacent point code types ITU-N and ITU-N 24-bit that are used for changeover processing (the ent-ls and chg-ls commands indicate the type with the new apctype parameter).
- E1 commands—The rtrv-e1 command output shows headings LINKCLASS and MINSURATE (these are new E1 command parameters for SE-HSL). The LINKCLASS parameter indicates whether the HC-MIM card is used for “channelized” E1 links or for “unchannelized” SE-HSL E1 links. In EAGLE 5 SAS Release 34.0, the LINKCLASS parameter default value CHAN (“channelized”) always appears in the rtrv-e1 output; dashes always appear in the MINSURATE column.
- MTP Level Timer commands—The number of level 2 timer sets has increased from 20 to 30. The rtrv-l2t command output shows the default values for the Level 2 timers in each of the 30 timer sets.

Hardware Requirements

The HC-MIM card is used as the SE-HSL card to run software that provides “unchannelized” E1 functions.

Each shelf that contains at least one HC-MIM card must contain HIPR cards in slots xy09 and xy10 (x is the frame, y is the shelf).

Each shelf that contains at least one HC-MIM card must contain a fan tray assembly. The fan feature bit must be turned on in the EAGLE 5 SAS.

Limitations

The SE-HSL feature inherits all the limitations of HC-MIM as listed in the HC-MIM “Limitations” section

The SE-HSL feature does not support the following functions:

- PCR for satelite links
- Link Fault Selection (LFS) testing

During the Changeover/Changeback/Controlled rerouting, the source card on EAGLE 5 SAS buffers the signaling data destined for the concerned link until the Changeover/Changeback/Controlled rerouting procedure is completed. This could take as long as two seconds. Therefore a queue large enough to buffer two seconds worth of data is required on the source card. When the link is operating at 1 Erlang, two seconds worth of data amounts to 21564 MSUs. An SE-HSL enabled card can support two HSLs, therefore two queues of size 21564 are reserved on the source card.

Another aspect is rerouting the on-hold data off the source card. Rerouting this much data has ramifications associated with it. SE-HSL supports buffering and rerouting at 0.4 Erlang to avoid the possibility of congestion or discard. Above 0.4 Erlang, buffering and rerouting may result into congestion or loss of data.

SE-HSL supports timers T1-T6 values up to 550 milliseconds. However, setting the T1-T6 times to 550 msec opens a possibility for mis-sequencing. EAGLE 5 SAS supports only one Layer 3 timer set. Once provisioned for high-speed links, all the links in the system use the T1-T6 limit of 550 milliseconds.

TALI “A” Link Connectivity (Release 28.0)

Description

This feature provides the capability to interface the EAGLE STP with an SCP by utilizing the TALI/IP protocol stack and the TCAP-over-IP feature of the merged Secure Gateway code. Specifically, this feature provides a TCAP-over-IP interface for SCP connectivity using TALI 3.0. This will allow the EAGLE to perform the SS7 interface functions of the SCP, eliminating the need for the IP7 Front End in this application.

The EAGLE STP uses the following features from the IP7 Secure Gateway feature set.

- TCAP Over IP Gateway Connectivity to IP-SCPs
- Feature key support
- TALI 3.0

The TCAP-over-IP feature allows SS7 nodes to exchange SCCP/TCAP Query/Responses with an IP enabled SCP. The Secure Gateway will map the Point Code/SSN to one or more TCP sessions, convert the SS7 MSUs to TCP/IP packets by embedding the SCCP/TCAP data inside a TCP/IP packet, and route it over an IP (IPGTWY) network.

For more information on the TALI A Link Connectivity feature, refer to the Database Administration Manual - SS7.

New Hardware Required

No new hardware is required for this feature.

TALON Development Kit (IP^7 Release 2.0)

Release 2.0 of the IP ^{7} Secure Gateway also optionally includes the TALON Release 2.0 Development Kit. This kit includes:

- iGate, which includes:
  - — iGate clients, which provide the client-side implementation of the Transport Adapter Layer Interface (TALI) protocol, Release 2.0.
  - — Application message queues, which hold messages sent between the iGate clients and the customer’s application.
  - — iGate controller, which controls starting and stopping of iGate clients.
  - — iGate command line interface, through which the user enters commands to start up, shut down, and reconfigure iGate components, to send TALI service and management messages, and to obtain status and measurements.

- TALON Assessor, a tool used to test and verify an implementation of the TALI Release 2.0 protocol. The Assessor can implement both sending and receiving messages as either a TALI client or server, as well as provide logging and measurements.

- ISDN User Part (ISUP) Access Library, a collection of C^{++} classes that allow customers to rapidly develop C^{++} applications that need to encode and decode ISUP messages. This library allows customer's applications to either set or get the value of an ISUP message or parameter without needing to directly access the bit stream of the ISUP message. Customers can compile their applications in the library, connect to TALON iGate queues, and then receive, parse, process, and send ISUP messages.

For more information about the TALON Development Kit, refer to the TALON Release 2.0 User Manual, which is included on the CD-ROM that contains the TALON software.

TDM Global Timing Interface (Release 31.6)

The TDM Global Timing Interface (TDM-GTI) is used with an enhanced, backward compatible, TDM card providing the following added functions:

- Ability to generate high speed master clocks from a recovered E1/T1 clock

- Ability to optionally reload the clock Logic Cell Array (LCA) bitfile when the mated GPSM-II is initialized.

TDM-GTI provides the ability to generate high speed master clocks from a recovered E1/T1 clock, in addition to the RS422 clock.

Temporary Alarm Inhibiting and Offline Functions (Release 25.0)

Overview

These features provide a two-part enhancement to the Selective Alarm Inhibit feature introduced with Release 22.0. First, the craftsperson can choose to have an alarm inhibited until the problem is fixed and the alarm clears (Temporary Alarm Inhibiting).

Second, these features give the craftsperson the mechanism for inhibiting critical alarms (Offline Functions). This is useful when a critical alarm has been investigated, the cause is known, and the critical alarm expected based on the current network. By allowing acknowledgment of specified critical alarms, new critical alarms are not masked.

Currently, alarms are inhibited until the inhibit is manually removed (Permanent Inhibit). Temporary Alarm Inhibiting lets the user specify a temporary inhibit indicating that the inhibition of the alarm should be cancelled when the condition clears. This allows a new occurrence of the same alarm to be issued.

A craftsperson may choose to inhibit existing alarms or future alarms in order to focus on higher severity or unknown alarms. A craftsperson may choose to inhibit alarms for various reasons, including:

- In a special maintenance situation where repeated alarms from malfunctioning equipment would tend to mask more critical unknown alarms (e.g. an out-of-service link due to a physical break that cannot be repaired for days).

- In the situation where the system is being provisioned. Currently alarms are generated immediately after entities are entered into the database. The craftsperson probably ignores these alarms while the system is being configured. Ignoring alarms due to entry of entities could result in the masking of alarms that may require immediate attention.

- In a situation where the craftsperson, while working on repeating alarms from malfunctioning equipment, might tend to mask more critical additional alarms. The craftsperson will want to temporarily inhibit the repeating alarms. When the repeating alarm is cleared, it will be uninhibited, and the craftsperson will be able to see it if it reoccurs.

- In a situation where a device is going to be put offline, or is offline and the repeated critical alarms associated with the offline equipment would tend to mask more critical alarms.

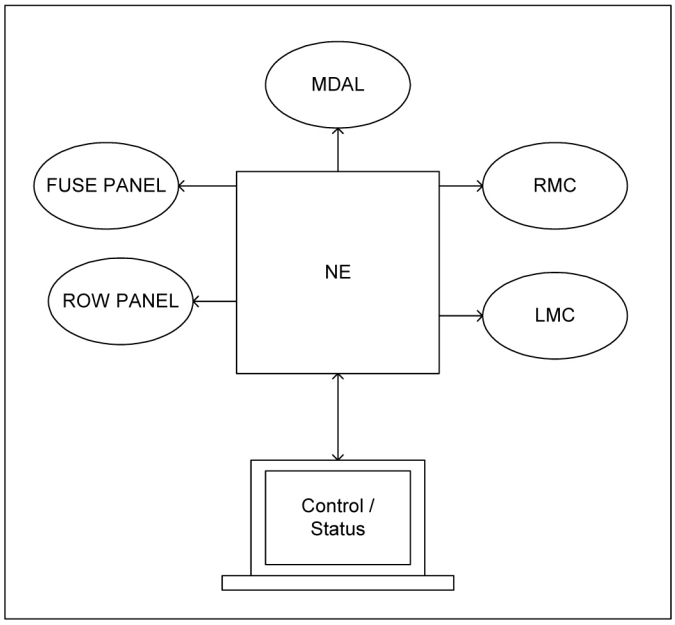
The method for inhibiting alarms is the same, regardless of the reason for inhibition. The craftsperson can either turn off (i.e. Temporary Inhibit or Permanent Inhibit) or turn on (i.e. Uninhibit) specified alarms through command entry. Permanent alarms are persistent.

Alarm System Functionality

There are four Alarm Indicators and one Control/Status display in the system. The fuse panels and row panels have lights to indicate alarms. The Local Maintenance Center and Remote Maintenance Center have signals that can be monitored for alarms.

All of these indicators have separate lines for critical, major, and minor alarms. The Control/Status Display is in the Status Area of the VT320 Screen. The same data is available through the **`rept-stat-alm`** command.

Figure 5-23. Alarm Indicators



Customer Use Scenario

A typical case where these features are needed follows:

- In an office with alarms that cannot be repaired quickly, "stuck alarm" (e.g. a cut link)...
- and only the remote maintenance center will be monitoring the alarms.

Because the alarms have not been repaired, all the indicators continue to be active (i.e. lights/signals on). When a new alarm arrives that is not for the device that has the "stuck alarm," the RMC indicator cannot accurately inform the maintenance personnel that a new alarm has occurred.

These features allow the maintenance personal to inhibit the "stuck alarm" that will turn off the appropriate alarm indicators. Now, at the RMC, the indicators will be cleared (i.e. lights off), and any alarm generated for a device that does not have its alarms inhibited will activate the indicators (i.e. lights on).

The mechanism for clearing the indicators is by inhibiting the alarms for the failed devices. When all devices that have alarms have had their alarms inhibited, the indicators are cleared.

The RMC indicators in the following table presents one possible scenario that illustrates the use of the inhibit alarm feature (i.e. Offline Functions) Without the ability of having a cleared indicator, the RMC personnel might not react as quickly as possible to the subsequent link failure.

NOTE: This example does not address the output generated to the RMC maintenance channel. When link 4107 port B failed, the system generated the appropriate output message.

Table 5-18. Example of Inhibit Alarms Use

ACTION	CONTROL COUNTS (Inhibited)			RMC INDICATOR		
	CRIT	MAJR	MINR	CRIT	MAJR	MINR
System clear -- no failed devices in the system	0	0(0)	0	off	off	off
A span is cut at 4:50pm -- cannot be repaired for 10 hours						
Link 1201, A generates alarm because of physical failure	0	1(0)	0	off	ON	off
Link 2318, B generates alarm because of physical failure	0	2(0)	0	off	ON	off
Link 5205, B generates alarm because of physical failure	0	3(0)	0	off	ON	off
Link Set ls1234 generates alarm because all links in link set are Out of Service	0	4(0)	0	off	ON	off
User inhibits alarm for link set ls1234	0	4(1)	0	off	ON	off
User inhibits alarm for link 1201,A	0	4(2)	0	off	ON	off
User inhibits alarm for link 2318,B	0	4(3)	0	off	ON	off
User inhibits alarm for link 5205,B	0	4(4)	0	off	off	off
User turns control over to the Remote Maintenance Center for the night.						
New alarm -- Link 4107, B fails not due to physical span failure	0	5(4)	0	off	ON	off

ACTION	CONTROL COUNTS (Inhibited)			RMC INDICATOR		
	CRIT	MAJR	MINR	CRIT	MAJR	MINR
RMC reacts to the event and investigates the failure						

The scenario presented in the following table illustrates the use of the temporary inhibit alarm feature. Without the ability of having a cleared indicator, the RMC personnel might not react as quickly as possible to the subsequent link failure.

NOTE: This example does not discuss the output generated to the RMC maintenance channel. When link 4107 port B failed, the system generated the appropriate output message.

Table 5-19. Example of Temporary Alarm Inhibit Use

ACTION	CONTROL COUNTS (Inhibited)			RMC INDICATOR		
	CRIT	MAJR	MINR	CRIT	MAJR	MINR
System clear -- no failed devices in the system	0	0(0)	0	off	off	off
A span is cut at 4:50pm – cannot be repaired for 10 hours						
Link 1201, A generates alarm because of physical failure	0(0)	1(0)	0	off	ON	off
Link 2318, B generates alarm because of physical failure	0(0)	2(0)	0	off	ON	off
Link 5205, B generates alarm because of physical failure	0(0)	3(0)	0	off	ON	off
Link Set ls1234 generates alarm because all links in link set are Out of Service	0(0)	1(0)	0	off	ON	off
DPC prohibited critical alarm	1(0)	4(0)		ON		
User temporarily inhibits critical alarm	1(1)	4(0)		off		
User temporarily inhibits alarm for link set ls1234	1(1)	4(1)	0	off	ON	off
User temporarily inhibits alarm for link 1201,A	1(1)	4(2)	0	off	ON	off
User temporarily inhibits alarm for link 2318,B	1(1)	4(3)	0	off	ON	off
User temporarily inhibits alarm for link 5205,B	1(1)	4(4)	0	off	off	off
User turns control over to the Remote Maintenance Center for the night.						
New alarm – Link 4107, B fails not due to physical span failure	1(1)	5(4)	0	off	ON	off
RMC reacts to the event and investigates the failure	1(1)	5(4)	0	off	ON	off

Link 4107, B failure and physical span failure corrected.	1(1)	4(4)	0	off	off	off
Link 1201, Span fixed, alarm cleared	1(1)	3(3)	0	off	off	off
Link 2318, Span fixed, alarm cleared	1(1)	2(2)	0	off	off	off
Link 5205, Span fixed, alarm cleared	1(1)	1(1)	0	off	off	off
Link Set ls1234 has no failed links, all alarms cleared.	1(1)	0(0)	0	off	off	off
DPC prohibited – critical alarm cleared	0(0)			off	off	off
A span is cut at 4:00 am – cannot be repaired for 10 hours						
Link 1201, A generates alarm because of physical failure	0(0)	1(0)	0	off	ON	off
Craftsperson knows the span failure has reoccurred.						

Administration

Two commands, **`inh-alm`** and **`unhb-alm`**, which were created in Release 22.0, have been enhanced to accommodate the Temporary Inhibit feature and the Offline Functions feature in Release 25.0. These changes allow for the following:

- The craftsperson will be allowed to temporarily inhibit the alarms on a device. The alarms will be inhibited until the alarm is cleared, at which point the device's alarms no longer will be inhibited.
- If a device's alarms are inhibited, the craftsperson will not be able to re-inhibit the same device's alarms. This is important for the scenario where the craftsperson tries to change a permanently inhibited alarm on a device to be temporarily inhibited. The craftsperson must uninhibit the alarms and inhibit them more precisely.
- A craftsperson is provided with a mechanism to inhibit critical alarms. This mechanism includes first allowing the STP option **`critalminh`**, which allows the inhibiting of critical alarms.
- When a craftsperson inhibits an alarm and specifies that critical alarms will be inhibited, the effect is that critical, major and minor alarms are all inhibited. If the craftsperson inhibits an alarm and specifies that major alarms will be inhibited, the effect is that major and minor alarms are all inhibited.

See "Thresholding of UIM Messages (Release 25.0)" more information on the **`inh-alm`** and **`unhb-alm`** commands.

Administration Rules:

1. A device must exist as a database or system-fixed entity.
2. You cannot inhibit an already inhibited device.
3. You cannot uninhibit an uninhibited device.

4. Normal database rules apply for an administration change to the database.

The command handler parameter combinations for the **`inh-alm`** and **`unhb-alm`** appear in the following table.

Table 5-20. Device/Parameter Command Matrix

	No parameters	**LOC**	**PORT**	**LSN**	**ID**	**DPC**	**DPCA**	**DPCI**	**DPCN**
CARD		1101..6118.							
SLK		1101..6118	A and B						
LS				Link Set Names					
ROUTE						nnn-ccc-mmm	nnn-ccc-mmm	z-aaa-i	nnnnn
TRM			1..16						
SYSCLK	No parameters								
DLK		1101..6118							
CDT					1..16				
LSMSQ3			A1,A2,B1, B2						
SEASX25			A1,A2,B1, B2						

Maintenance

There are several actions that the maintenance system must control:

- Visual Indicator Control
- Visual Control Area banner display of the inhibited alarm count
- Suppression of alarm output
- Generation of Inhibit Message
- **`rept-stat`** command changes
- Hourly Status Report changes

Each is discussed in the following sections.

Control Area Changes

There are four boxes on the VT320 Control Area, of which only three were used prior to Release 21.0. The fourth currently displays the number of devices that have alarms inhibited. Viewed from left to right on the screen, they indicate Critical, Major, and Minor alarms, and the number of devices that have alarms inhibited.

Suppression of Output

Suppression of the output occurs when the function call is made to "generate unsolicited alarm output." This prevents any changes to the analysis code. Within the "generate unsolicited output," the action has been changed to "generate unsolicited alarm with no output." This function is used during OAM initialization to set alarms without generating output, and effectively suppresses the output.

New UAMs

Two UAM's inform the user that the device has had its alarms inhibited:

```
    RLGHNCXA03W 99-07-07 00:57:31 EST Rel 25.0.0
    0100.0294    CARD 1201 SS7ANSI     REPT-ALMINH: alarm output Perm
inhibited
;
    RLGHNCXA03W 99-07-07 00:57:31 EST Rel 25.0.0
    0100.0296    CARD 1201 SS7ANSI     REPT-ALMINH: alarm output Temp
inhibited
;
```

Status Command Changes

Device Status Commands

The associated state of a card is displayed as "ALMINH" when a card's alarms are inhibited.

The '**stat**' option for these commands has been extended to support 'ALMINH', which displays all cards whose alarms are inhibited. When the Associated State is set to ALMINH, it is overwritten by other states (e.g. BIP) until the inhibition is removed.

See the *Commands Manual* for more information.

Hourly Status Report

The Condition Type field in the Hourly Status Report has the INHAUDB value added to possible values. The full list of Condition Types follows.

1. SCMMA - The device has been disabled due to manual maintenance action (e.g. **inh-card**). This condition applies regardless of previous alarm state.

2. MTCEINT-0 - The reported device is off-normal (ANR), but there is no alarm associated with this device. An alarmed condition for another device typically impacts the state of this device, e.g. OOS links affect linksets, OOS DLKs affect SLAN cards.

3. MAN - The reported device is off-normal (OOS-MT), but there is no alarm associated with this device. The off-normal condition was caused manually, e.g. **ent-dstn** command entry.

4. NULL - No specific 'cond type' is currently supported for this release. There is sufficient information to ascertain the device condition from the report. The craftsperson may use **rept-stat-xxx** command(s) to collect further information.

5. INHAUDB - The user has manually inhibited alarms for this device. The time when the device was inhibited is recorded, and displayed during the hourly report.

The Hourly Status Report includes the alarm status periodic reminder added at its end. A new status indicates alarms that have been inhibited.

Output Example

```
    RLGHNCXA03W 99-07-07 00:57:31 EST Rel 25.0.0
    5023.0000 REPT COND CARD
    "CARD 1201:,MTCEINT-0,,96-11-19,14:58:24,,,"
    "CARD 1202:0013,,SA,96-11-19,14:44:38,,,**"
    "CARD 1203:0013,,SA,96-11-19,14:44:38,,,**"
    "CARD 1204:0013,,SA,96-11-19,14:44:38,,,**"
    "CARD 1206:0013,,SA,96-11-19,14:44:38,,,**"
    "CARD 1207:0034,,NSA,96-11-19,14:52:56,,,* "
    "CARD 1208:0013,,SA,96-11-19,14:44:38,,,**"
    "CARD 1216:0013,INHAUDB,NSA,96-11-19,13:44:38,,,"
    "CARD 1101:0034,MTCEINT-0,NSA,96-11-19,14:52:56,,,* "
    "CARD 1115:0143,,NSA,96-11-19,14:57:52,,,* "

    RLGHNCXA03W 99-07-07 00:57:31 EST Rel 25.0.0
    5034.0000 REPT COND ALARM STATUS
    "ALARMS:TEMP INHIBITED,1,3,4"
    "ALARMS:PERM INHIBITED, 2,14,4
"

    "ALARMS:ACTIVE,2,0,0"
    "ALARMS:TOTAL,5,17,8"
    "ALARMS:STATUS,AUDIBLE,SILENT,SILENT"
```

Note that the alarm status is shown in the following sequence: critical, major, and minor. Thus the bold text means there are two critical alarms, fourteen major alarms, and 4 minor alarms.

Thresholding of UIM Messages (Release 25.0)

Description

This feature suppresses the generation of a UIM message when it exceeds a certain user-settable threshold. It allows the user to set, delete, or display the UIM threshold and interval on a per-UIM number basis.

The thresholding capability provided by this feature is limited by the systemwide threshold of 4 UIMs per second, i.e. any threshold set using this new feature is superseded by the systemwide threshold, which is not administrable.

In support of this feature, the following commands have been created:

- **set-uim-acthresh** (to set UIM threshold and interval)
- **rtrv-uim-acthresh** (to display the UIM threshold and interval)

- **`dlt-uim-acthresh`** (to delete the UIM threshold and interval)

In addition, a UIM logging feature has been introduced primarily as a complement to the UIM Thresholding feature. (The UIM Thresholding feature allows for the suppression of UIM messages when they exceed a certain user settable threshold. The user can define the threshold such that no UIM's will be displayed.) The new logging feature provides a way to retrieve all the UIM messages that would have been printed, even those not displayed due to the UIM threshold feature.

The craftsperson can retrieve the logged UIMs with the **`rtrv-log`** command, using the new value "UIM" for the **`type`** parameter.

The UIMs are stored on disk only by the active OAM. However, the UIMs that were stored on the standby when it was active can be retrieved with the **`rtrv-log`** command.

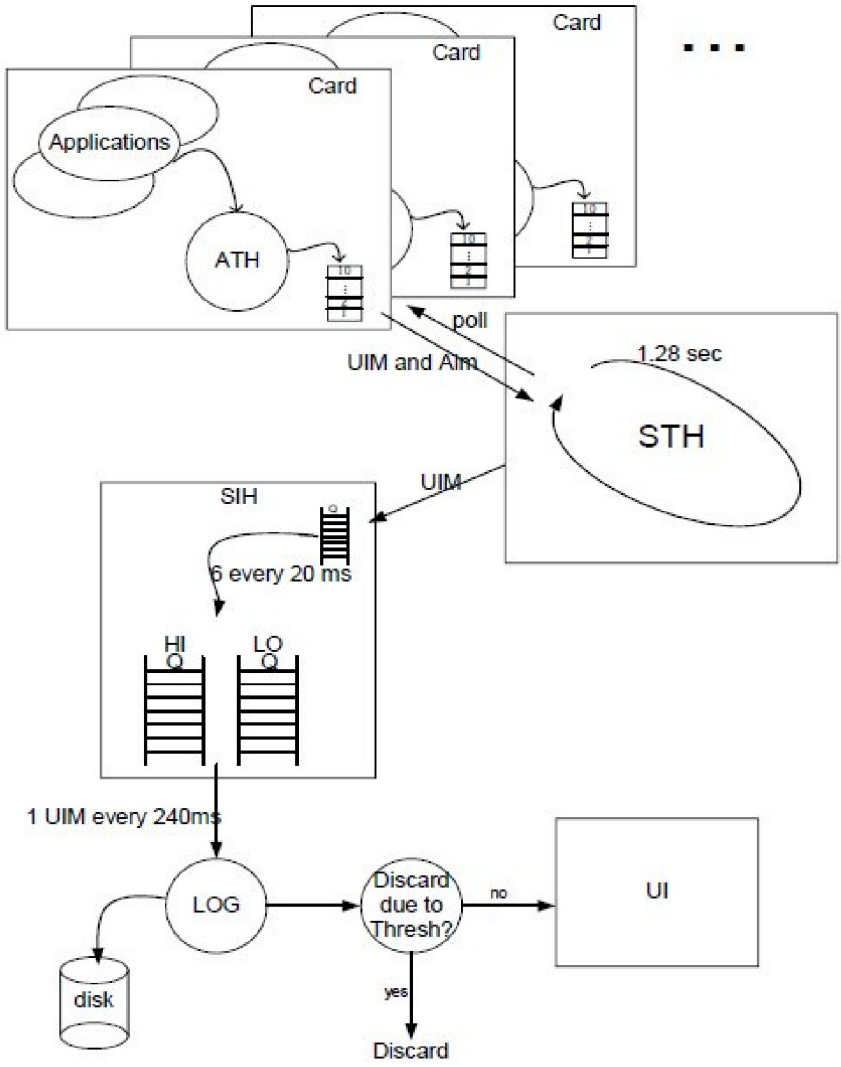
UIM logging occurs on a continuous basis. When the UIM log is full, the oldest event is overwritten by the newest event. A total of 65,536 UIMs can be maintained in the log. This represents a history of time of 4.55 hours, at a maximum creation rate of 4 UIMs per second. The term "creation rate" is defined here as UIMs that are printed or would have been printed if the UIM Threshold feature was not used.

Creation of UIMs

Figure 5-24 shows how UIMs are generated throughout the system. It is important to note that the point where the decision is made to discard UIMs due to thresholding has changed with this feature.

The applications running on cards send UIMs and alarms to the ATH application. The ATH application on every card is polled by STH every 1.28 seconds for the UIM and Alarm information on those cards. Each ATH has a buffer of a total of 10 UIMs and Alarms it can send to the STH during that interval. The STH forwards all the UIMs to SIH for handling. SIH processes 6 UIMs every 20ms. If SIH decides the UIM should be printed, it places the UIM on the HI or LO queues. SIH then paces the output to UI at a rate of approximately 4 UIMs per second.

Figure 5-24. Depiction of UIM Creation, Logging, and Thresholding



Upgrade Considerations

The UIM logging feature requires that a new file be created and initialized during upgrade from any pre-release 25.0 EAGLE. This new file holds the history of UIM events. If this file is not created in a release 25.0 EAGLE, the OAM will detect the absence of the file and automatically disable logging. The OAM does so by entering the DISABLED logging-state, and will remain in that state until the OAM reboots and can then access the file. If the OAM is in the DISABLED logging state for UIM logging, it means it can not log UIMs.

The new file is 11 Mbytes in size and can hold 65,536 UIMs.

Changed Event Log Command

The **`rtrv-log`** command retrieves records from one of the logs generated by the Maintenance system; it selects these records based on a span of time or a specific log file index.

Prior to Release 25.0, the only log supported was the Alarm Log.

As of Release 25.0, the **type** parameter can be used to retrieve the events of either the Alarm log (**type=alarm**) or the UIM log (**type=uim**), but not both. The default is **alarm**.

Refer to the *Commands Manual* for current usage information.

Limitations

The implementation of the UIM logging feature contains the following limitations. These limitations may need to be communicated to the Customer and are candidates for future feature enhancements:

1. Due to the fact that the HI priority queue gets serviced before the low priority queue in SIH, the events may not be logged in the order in which they occurred (put another way, their timestamps might not be ordered due to the nature of SIH). Also, when the time/date is changed (e.g. with the set-time command) the display of these records may appear (from the date-time stamp) to been written in the incorrect order. Taking both these into consideration, there is a timestamp for when the UIM occurred and when the UIM was logged. This aids the retrieval of UIMs.

2. The information in the Log is not self-evident. Technical documentation and/or files must be provided to allow such a file to be analyzed off the EAGLE.

3. UIMs are written only to the UIM Log on the active OAM. However, events that were logged previously on the current standby (when it was the active) can be retrieved with the **rtrv-log** command.

4. The writing of UIMs to the Log will continue, unaffected, during a removal of the Log via either a **copy-tbl** or with the Kermit facility.

5. The Log will not be included in the BACKUP/RESTORE capability.

6. The repairing of the Log must be accomplished by a **copy-tbl** command from the removable, should the Log become corrupted.

Time Stamps for rept-stat-trbl Report (Release 31.6)

The **display=timestamp** parameter value has been added to the **rept-stat-trbl** command, to display all alarms with the date and time when the alarm was logged.

Only one parameter value for **display** is allowed in the command at one time. Therefore, timestamps cannot be displayed for just inhibited or active alarms (**display=inhb** and **display=act**).

The **display=timestamp** parameter value of the **rept-stat-trbl** command displays all alarms with the date and time when the alarm was logged.

Time-Based Inhibit Alarm (Release 35.0)

Description

The Time-Based Inhibit Alarm feature allows alarms at or below a configurable severity to be suppressed on a device for a configurable period. This feature allows only desired alarms to be viewed during testing or other maintenance activities.

Hardware Requirements

The Time-Based Inhibit Alarm feature has no hardware requirements.

Limitations

The Time-Based Inhibit Alarm feature has no associated limitations.

Transaction-based GTT Loadsharing (Release 36.0)

Description

TheTransaction-based GTT Loadsharing feature (TBGTTLS) is an enhancement to intermediate and final Global Title Translation load-sharing. The Transaction-based GTT Loadsharing feature enables GT-routed messages that are part of the same transaction to be loadshared to the same destination in a MAP group or MRN group.

The Transaction-based GTT Loadsharing feature uses the transaction parameter to control loadsharing for Class 0 and Class 1 SCCP messages. The Transaction-based GTT Loadsharing feature also controls loadsharing for unit data (UDT) and extended unit data (XUDT) messages.

EAGLE 5 ISS generates a unique key for each MSU when transaction-based GTT loadsharing is performed. This key, called the MSUKey, is a unique 4-byte number. The value of the MSUKey depends on the selected transaction parameter. The transaction-based GTT loadsharing algorithm ensures that message signal units (MSUs) that have the same MSUKey value are routed to the same destination within the Entity Set.

- For UDT messages, the key is based on MTP, SCCP or TCAP transaction parameters
- For XUDT messages, the key is based on MTP parameters or SCCP parameters
- For TCAP, the TCAP ID is the MSUKey value.
- For SCCP in XUDT/XUDTS and UDT/UDTS messages, the last 4 bytes of the GTA field of CdPA in the inbound MSU are the MSUKey.
- For MTP in XUDT/XUDTS and UDT/UDTS messages, the last 3 bytes of incoming OPC and 1 byte of SLS are combined to create a unique MSUKey. This structure applies to both ANSI and ITU point codes. This is the default parameter for performing TBGTTLS.

The EAGLE 5 ISS provides multiple forms of Intermediate and Final GTT. loadsharing. These loadsharing modes are determined by the relative cost of each entity in the Entity Set. Of the possible configurations (Solitary,

Dominant, Load-Shared, and Combined Load-Shared/Dominant), TBGTTLS affects only entities that work in the Load-Shared and Combined Load-Shared/Dominant loadsharing modes.

- In Load-Shared mode, the entire Entity Set is a part of one RC group and MSUs are load-shared based on the transaction parameter within the entities in the Entity Set. If none of the entities in the Entity Set are available for routing, the message is dropped and a UDTS/XUDTS message is generated if “return on error” is set in the SCCP message. A UIM is generated to notify the user that the MSU has been dropped.

- In Combined Load-Shared/Dominant mode, TBGTTLS is initially applied to the RC group, where the PC/PC+SSN belongs that is obtained as a result of GTT.

  — If none of the entities are available for routing within that particular RC group, the next higher cost RC group shall be chosen and TBGTTLS is applied to the new RC group. This process is repeated until there is no available entity in the Entity Set for routing.

  — If none of the entities are available for routing, the message shall be dropped and a UDTS/XUDTS message is generated if “return on error” is set in the SCCP message. A UIM is generated to notify the user that the MSU has been dropped.

A feature access key (FAK) for part number 893017101 is required to enable the Transaction-based GTT Loadsharing feature.

- The GTT feature must be on before TBGTTLS can be enabled.

- After the feature is enabled and turned on, it cannot be turned off.

- No temporary FAK is allowed for the feature.

Hardware Requirements

The Transaction-based GTT Loadsharing feature has the following hardware requirements:

- DSM cards

- TSM cards that run the SCCP application cannot be provisioned if the feature is enabled. The feature cannot be enabled if TSM cards that run the SCCP application are configured in the system.

Limitations

The Transaction-based GTT Loadsharing feature has the following limitations:

- If the Transaction-based Loadsharing and Weighted GTT Loadsharing features are both enabled, then transaction-based loadsharing has higher priority. This guarantees that messages of a single transaction are loadshared to the same entity within the MAP group or MRN group.

- For transaction-based routing, loadsharing can be guaranteed only when incoming messages are well distributed over MTP/SCCP/TCAP parameters. When the incoming traffic is well distributed using the MTP/SCCP/TCAP parameters, then EAGLE 5 ISS will distribute traffic (at least 1,000 messages) in accordance with load sharing applicable to the MAPSET/MRNSET with an allowed deviation of +/-5%”. If a new entry is added or an existing entry is deleted from an RC group within a Entity Set while MSUs are

getting routed to one of the entities in that particular RC group, the EAGLE 5 ISS might not be able to maintain the load share distribution and allowed deviation for the loadshared traffic.

- When the Transaction-based GTT Loadsharing feature and the Weighted GTT Loadsharing feature are both on, the following scenario can occur:

  — An RC group (for example, RC1) becomes prohibited and all of its traffic is rerouted to an alternate RC group (for example, RC2).

  — A node comes up in RC1 (which was the initial destination for an MSU routed base on TBGTTLS), but the weight percentage of RC1 is still below the in-service weight threshold.

  RC1 is still considered prohibited and traffic is not sent to the node in RC1.

- If the number of available entities within the RC group differs between successive MSU transmissions, all the MSUs that are getting routed to alternate destination (because the primary destination was not available) get rerouted, even if the entity that has become unavailable is not the destination entity for those MSUs.

- When the Primary Destination is inhibited and the traffic is failed over, the node state might not be maintained if other nodes also fail.

- When an entity is added to a group or deleted from a group, so that the number of entities in the group changes, the assignments within the group could all change.

Translation Type Mapping (Release 21.0)

Certain SCCP messages contain a called party address parameter that contains a translation type field. The translation type field indicates the type of global title processing the EAGLE must perform. The values used within any particular network may be different than the standardized values that are defined for internetwork applications.

The translation type mapping feature maps standardized internetwork translation type values to intranetwork translation type values used within any particular network. This feature also maps intranetwork translation type values to standardized internetwork translation type values.

The only SCCP messages that are affected by translation type mapping are UDT and XUDT messages, received or transmitted, whose global title indicator is 0010 (ANSI/ITU) or 0100 (ITU). Other messages that contain the called party address parameter are not affected. For example, UDTS messages are assumed to be MTP routed and need not be examined. XUDTS messages are either MTP routed or use one translation type value indicating global title to point code translation and should not be mapped.

The translation type mapping feature is configured for any linkset, however, translation type mapping has no effect on messages in X.25 linksets, since this feature has not been implemented for X.25 linksets. There is currently no specification for translation type mapping in ITU networks, therefore, the EAGLE provides the same translation type mapping function as for ANSI networks.

Translation type mapping is performed on each LIM in the linkset. Incoming translation type mapping is performed before global title translation, gateway screening, or the MSU copy associated with the STP LAN feature. Outgoing translation type mapping is performed after global title translation, gateway screening, and the MSU copy associated with the STP LAN feature.

When outgoing translation type mapping is provisioned and the MSU is copied for the STP LAN feature, the copied MSU is mapped. This is done because the mapped translation type may have a different meaning in the local network, causing the MSU to be interpreted incorrectly.

If the database transport access feature is being used, and the MSU encapsulated by the gateway screening redirect function contains a translation type that must be mapped on an incoming basis, the encapsulated MSU contains the mapped translation type. The translation type of the new MSU is obtained from the gateway screening redirect table.

The EAGLE supports 64 translation type mappings for each linkset. This includes both incoming and outgoing translation type mappings. Since the EAGLE supports a total of 255 linksets, the total number of translation type mappings that can be provisioned in the EAGLE is 16,320.

A new measurement report has been created to report the new daily measurements of the linkset, the **mtcd-lnkse**t measurement report. Three new measurements are collected and reported.

- ZTTMAP — translation type mapping translations performed - The total number of translation type mappings performed by the entire STP maintained over 30 minute intervals. This is displayed in the **systot-stp** report.

- ZTTMAPI — translation type mapping translation performed - MSUs received on the gateway linkset - The number of incoming translation type mappings performed per linkset over 30 minute and daily intervals. These are displayed in the **comp-lnkset** report every 30 minutes and the daily **mtcd-lnkset** report.

- ZTTMAPO —þtranslation type mapping translation performed - MSUs transmitted on the gateway link set - The number of outgoing translation type mappings performed per linkset over 30 minute and daily intervals. These measurements are displayed in the **comp-lnkset** report every 30 minutes and the daily **mtcd-lnkset** report.

Triggerless LNP (Release 24.0)

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

Refer to the *Database Administration Manual - LNP* for current configuration information on this feature.

TSM Warm Restart and Incremental Loading (Release 26.0)

Overview

In prior releases, when a TSM/BLM card running the SCCP/EBDABLM GPL boots unexpectedly or is manually booted (i.e. init-card), the GPL and the database on the card are reloaded from the OAM. The reload time is significantly affected by the LNP database size, which requires approximately 5 minutes for every one million ported numbers.

However, a complete LNP data reload may not be required if the LNP database on the card is coherent at the time of the reset. If no LNP updates occur from the time the TSM/BLM goes off-bus to the time comes back on the bus, the LNP database on the card is the same as the LNP database on the OAM.

In the event LNP updates occur while the TSM card is not in service, the Incremental Loading feature tracks the updates, and applies them to the card when it is ready.

In either case, a complete data reload may be unnecessary if the on-card LNP database is at or near the same level as the OAM LNP database. Warm restart bypasses data loading of the LNP database only. GPL and non-LNP table data/dynamic data loading is unaffected. Incremental loading applies only to LNP updates, non-LNP database updates are not supported.

Warm Restart

The Warm Restart feature modifies the default EAGLE operation to preserve the LNP database during a TSM/ BLM card reset provided the requirements for performing a warm restart are met (see the following table). Those requirements are that:

- power to the card is uninterrupted
- card level checks determine a warm restart is allowed
- card database level is the same as the OAM database level or can be incrementally loaded to the current level
- LNP audit is ON and has run at least once (otherwise all LNP checksums on the OAM are unknown)
- card database is coherent at the time of reset and the LNP database audit during card initialization passes

Table 5-21. Conditions for Performing Warm Restart

Condition	Description
POWER ON	Power on reset (card is pulled and reinserted).
XILINX VERSION	M256 Xilinx program version has changed from previous version.
DB VERSION	LNP Database version has changed from previous version. On-line Memory allocation (alloc-mem), import or bulk downloads (chg-db), or changes from release to release may alter the DB version.
DB LEVEL	DB level not supported or difference exceeds incremental loading capability. Caused by reset of OAMs or if the number of updates exceeds the incremental loading capability.
DB STATUS	DB status of the card is incoherent at the time of a reset. Can be caused by a failed network card update or a reset during a database update to the card.
HW ERROR	Hardware error bit checks on the card fail during card initialization.
AUDIT FAILED	Checksum comparisons of the LNP database fail during card initialization. Data on the card is determined to be corrupted after the reset (was not yet detected by normal auditing).
AUDIT TIMEOUT	LNP initialization audit timed out (SW failure).
NO AUDIT	Unable to perform LNP audit. LNP audit not on (LNP Options has AUDIT=OFF. Or, the rate of LNP updates exceeds LNP audit's ability to compute checksums (excessive unknown checksums). This is more likely on a small database where there are fewer checksums. The percentage of known checksums must be 99% or more. The percentage is based on the number of checksums in use, which is smaller for small databases (such as 2 MIL TNs or less).

Condition	Description
USER REQUEST	User initiated **`init-card`** or **`init-sys`** command reload type cold. The default restart type for these commands is a cold or full LNP data reload. User must specify **`data=persist`** for warm restart on command.
UNKNOWN / OTHER	Unknown or other type of software failure.

Incremental Loading

The Incremental Loading/Warm Restart feature modifies the reload procedure for an LNP database card (i.e. TSM). The LNP database will remain persistent as long as power is not removed from the card. In the event of a card reload, the TSM will check to see if an LNP database full reload is required. If a full reload is required, the OAM will be allowed to continue to process LNP updates from the LSMS to the other TSM cards. The OAM will track the database changes required for the reloading TSM card and apply those updates when the TSM is ready to be placed back in service.

This circumvents the need to inhibit LNP updates in most cases. The requirements to perform these operations are:

- A database level and restart type indication from the restarting card can be accepted and processed.
- Card requests for both warm and cold restarts can be processed.
- Changes in the OAM LNP database can be tracked and applied on an "as needed" basis per reloading card.
- DB operations (e.g., init card with DATA = PERSIST/REFRESH) can be processed properly.
- OAM can temporarily inhibit LNP updates for a small period of time in order to complete the loading process when necessary with out losing EOAP/OAP status or Q.3 association with the LSMS.
- Incremental loading will support up to 25 TSM cards and 1 BLM card for incremental loading purposes.

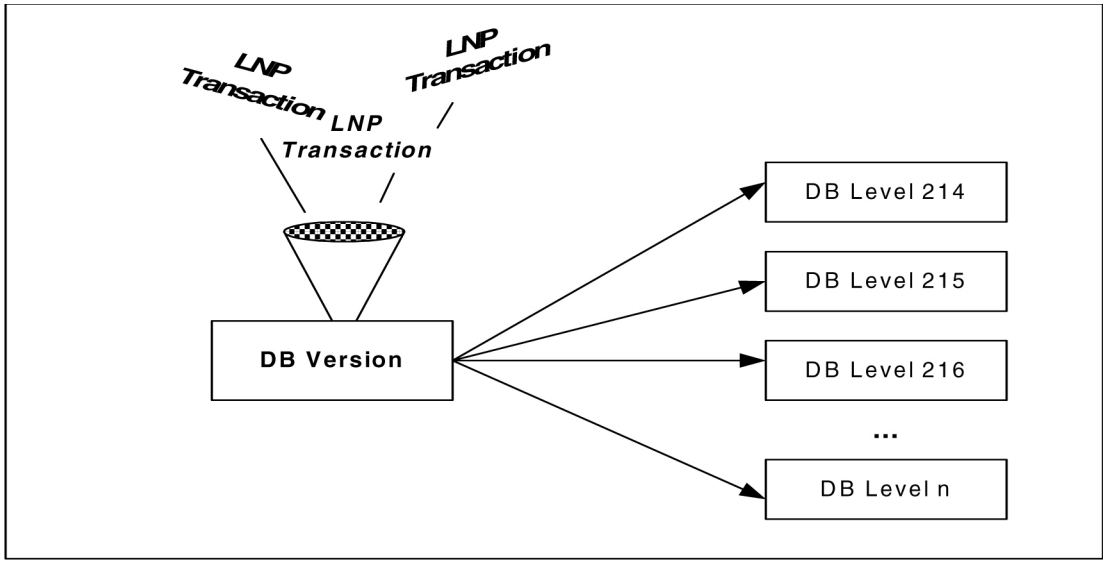
Maintenance

The following sections describe the maintenance changes required as part of the Warm Restart and Incremental Loading features.

Loading Process

The loading process involves the continuous tracking of LNP database changes and applying those changes to cards that are coming into service. Changes to the LNP database occur each time that an LNP transaction takes place. A single LNP transaction (i.e., change) can affect multiple LNP tables. Each LNP transaction generates a new level within the same version of the LNP database (see). In other words, each LNP database version can go through a number of levels (changes).

Figure 5-25. Database Levels



Applying the LNP data to the card(s) may be done either incrementally or as a full database restoration: cards at the same LNP database version but at different database levels can be incrementally loaded while cards at a different LNP database version must receive a full database download.

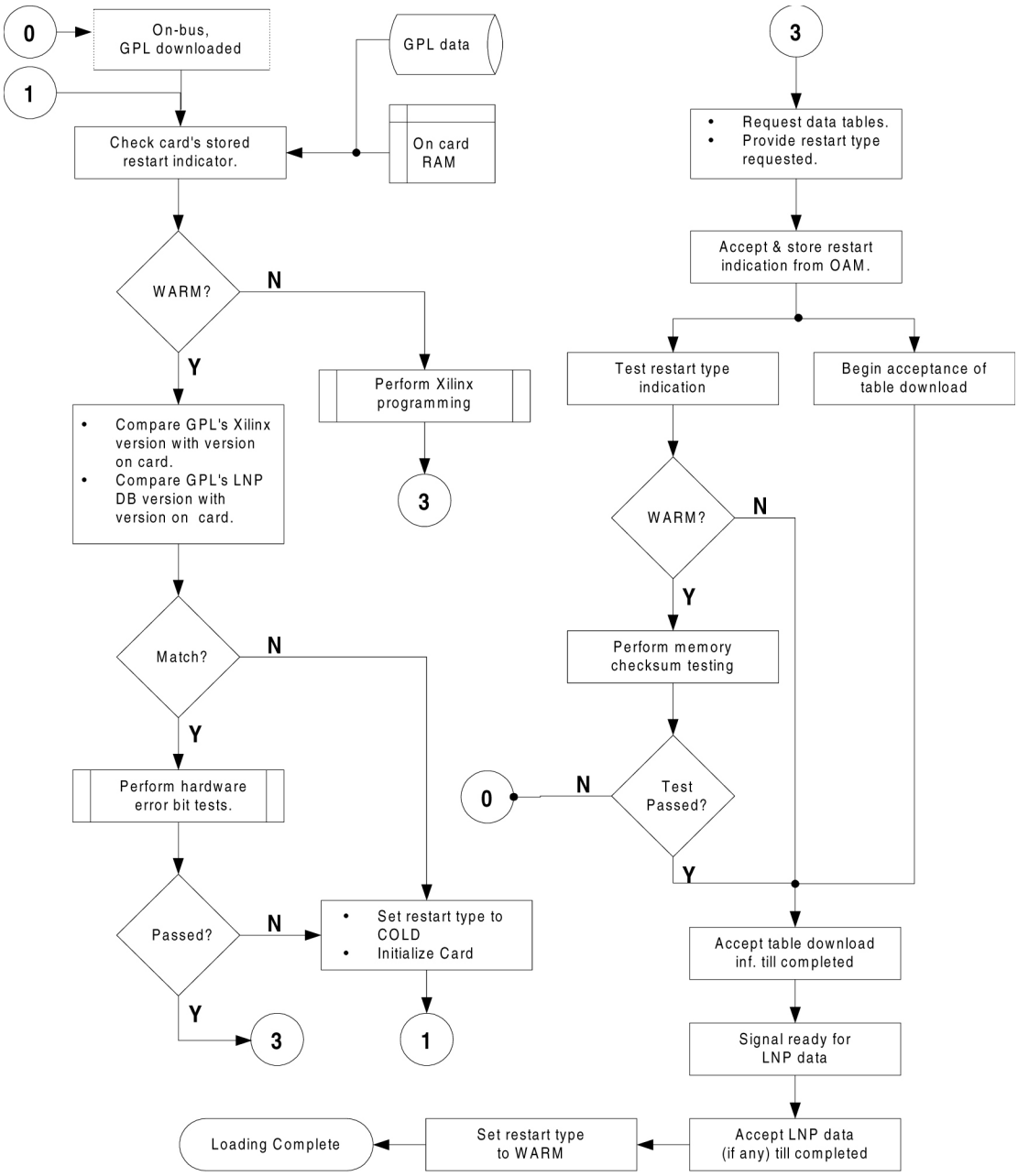
In order to track LNP database changes for incremental loading, a table of database levels and modified memory pages will be maintained by OAM. This will allow cards at varying database levels to be incrementally downloaded with a subset of the entire database. As the data changes in time, the changes are to be tracked and then applied to the appropriate card(s) that are in an active load list. Note that all cards appearing within a particular load list will receive the same dataset.

The following subsections discuss the approaches for delivering the LNP data to the appropriate cards and for tracking LNP database alterations.

Card Loading For Warm Restarts

System loading for the SCCP/EBDABLM GPL at the TSM/BLM card will be modified to determine whether to perform a warm or cold restart. The following figure depicts the SCCP/EBDABLM on-card decision making process for this feature.

Figure 5-26. On-Card Warm Restart Decision Flow



The figure shows that the check for the stored restart type is performed first. The restart type value shall always be warm by default. This value can be set to cold by either an indication to the card from the user (i.e., a forced cold restart) or by the card when some error condition occurred (e.g., LNP database versions did not match). The warm restart type may also be changed at some point during the restart process.

For example, the OAM may determine that the request for a warm restart cannot be honored and deliver an indication for a cold restart (i.e., a full LNP download).

The decision process involves several checks to verify eligibility for a warm restart request. If all of the criteria are met, the request for a warm restart is made. In order to minimize delays in the download process, the SCCP/

EBDABLM GPLs shall perform the memory checksum tests in parallel with the data table loading whenever a warm restart is in progress.

Once the non-LNP tables have been loaded and the checksum tests have passed, an indication of the card's readiness to receive LNP data will be raised. At this point, OAM will begin delivery of the LNP tables followed by a new checksum table.

The OAM must be in agreement (i.e., there is no cause to override the request), then the warm restart is performed and an incremental download of the LNP database is carried out if required. The criteria for OAM to be in agreement are as follow:

- The cards reported database level is not greater than the OAMs current database level.
- The cards reported database level must be in the DB Level Transition List (card can be incrementally loaded).
- There are approximately 99% known LNP AUDIT checksums (sufficient to perform on card audit).

SCCP/EBDABLM GPL Impacts

The SCCP and EBDABLM GPLs will be modified to incorporate the decision making ability with regards to the type of restart needed (see figure). Specifically, the decision to request a warm restart will be made if:

- M256 Xilinx is programmed and the bit file has not changed.
- LNP database version has not changed.
- Hardware error bit checks on the card do not fail.
- Checksum comparisons of the LNP database do not fail. Each applicable card shall be able to compare the LNP database on the card to the LNP database on the OAM.
- **`init-card`** or **`init-sys`** command with a reload type of COLD was not requested.

The SCCP and EBDABLM GPLs, operating on the TSM/BLM cards respectively, shall be capable of storing, retrieving, and reporting pertinent information for the restart decision process using non-volatile memory.

The software will maintain, at a fixed memory location, the:

- Xilinx program changed indication.
- LNP database version.
- LNP checksum table.
- Restart request type (warm, cold).

The initialization sequence of the application software must not reprogram the M256 Xilinx. The M256 Xilinx is unable to maintain DRAM data integrity during the reprogramming process. The Xilinx shall be reprogrammed only if a cold restart is to be performed. In addition, if the Xilinx is already programmed and the version has not changed, the DRAM check bit initialization shall be bypassed.

An LNP checksum table is downloaded by the OAM at the end of the download process. This table will be preserved in memory and used to verify the LNP database during the next restart operation.

When a warm restart is requested and agreed upon by OAM, an incremental loading of the LNP database will be performed if required. Should a cold restart be requested or a warm restart request be overridden by OAM, a full LNP database download will be performed.

OAM Impacts

In order for the SCCP/EBDABLM restart type request to be processed during card loading, the OAM GPL will require modifications. The changes will involve:

- All information necessary for the card to determine if it can perform a warm restart will be delivered in the initial download to the card.
- Reacting to a specific restart request type from an authorized card.
- Tracking changes to the LNP database will occur at all times.
- Possibly performing an early card deletion from load list for warm restart if a different restart type is required.
- Downloading the LNP checksum table at the end of the loading process.
- LNP Audit checksum table and incremental load list is cleared upon an import or restore.

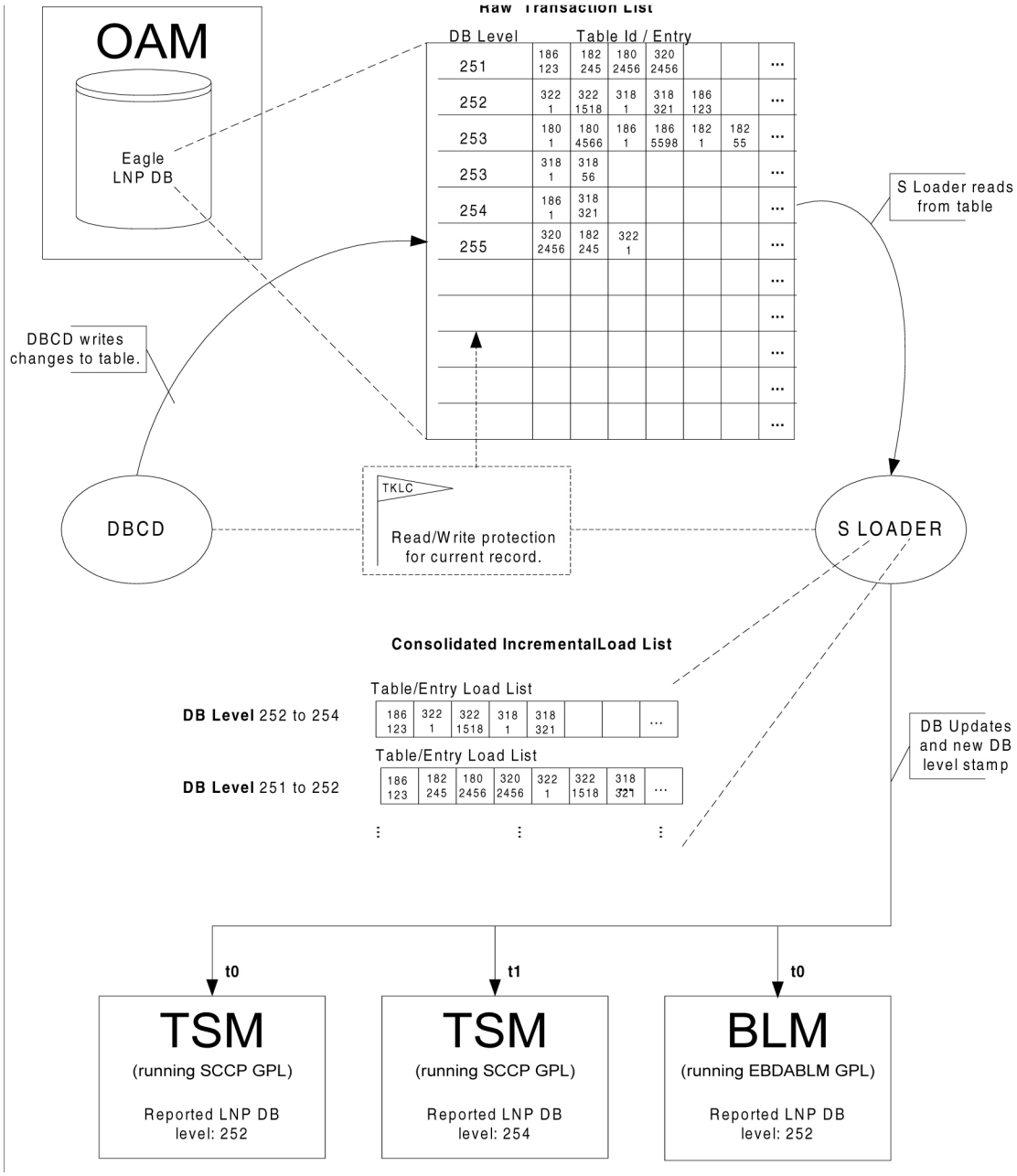
The SCCP/EBDABLM GPL will report its current database level to OAM (see Database Levels and On-Card Warm Restart Decision Flow). The OAM must verify that the database level has not incremented beyond an acceptable point for incremental loading. The restart type may be overridden by the OAM and an indication of such will be delivered back to the restarting card in the form of all LNP database data being delivered.

In addition, if a cold restart is required and the card cannot be incrementally loaded, LNP updates and LNP audits must be ignored by the affected card.

Tracking LNP Changes for Incremental Loading

In order to provide an incremental download of LNP data, modifications to the database must be tracked. The database change engine (DBCD) will write the modified table ids and record entry numbers into a table as changes occur.

Figure 5-27. LNP Data Tracking and Loading Overview



Each LNP database change generates a new database level. The new level shall become the current level and all level entities associated with the LNP transaction will be indicated with the same database level table entry. The table shall be circular so that changes can be tracked and applied to the cards in a continuous manner.

If the number of entities is exceeded within a database level record, the record will me marked as continued and the next entry will contain the same database level, thus extending the database level record entry.

System Loader will read the database transition to determine which entities are to be downloaded to a particular card based upon its reported database level. A protective mechanism shall be used to prevent the System Loader task from reading a record while it is being written to.

System Loader shall create card load lists and associate the database level entities that must be downloaded based upon database levels. Each time period (i.e., an iteration in time, t0, t1, etc., where tn = tn - tn-1) will represent some number of database levels: the set of changes that occurred within a given time period. System Loader shall have one list that is the "active list". The active list will represent the cards that are currently receiving LNP data. System Loader shall also maintain additional lists of cards that are waiting for an LNP data download at other DB levels (see LNP Data Tracking and Loading Overview). Once a list becomes the active list, no new entries shall be made. Any cards requesting LNP data would have to be placed into a new/other list.

Cards will be assigned to a particular load list based upon their reported database level as well as the time of their request for LNP data. Thus, a card reporting a level of 259, for example, may be placed in a list being formed for level 257 in order to grant its request for data without delay. While this methodology would download data that is not needed by some cards within the group, it prevents cards from waiting for a new list to be formed and takes into account that there is a finite number of lists available.

When Incremental Loading detects that a small amount if time is needed to complete a TSM/BLM download to reach the current DB Level then Incremental Loading will automatically inhibit LNP updates for the time needed to complete the download. Thereby avoiding continuous circular incremental loading of sustained 2TN modifications.

LNP Audit

In order to guarantee the integrity of the LNP database, the TSM/BLM cards shall perform an audit of their LNP database during a warm restart. To achieve this the following changes to the LNP audit process on the OAM and TSM/BLM cards are required:

- TSM/BLM cards shall be capable of ignoring RADB LNP update and LNP audit messages during data loading.
- LNP checksum table shall be downloaded to all TSM/BLM cards during data loading.
- LNP audit's checksum table shall be maintained on the OAM and TSM/BLM cards.

A warm restart is allowed only if LNP audit has completed an audit of the current database at least once and the LNP checksums are approximately 99% known.

LNP AUDIT considers each of the LNP database tables to be segmented into "pages" where a page is defined as the number of table records that can be read into a 32KB buffer using a single disk operation. A "dirty page" is a page that has recently been modified during a database update for which the associated LNP audit checksum is unknown.

During card initialization LNP audit shall checksum the LNP database and compare against the LNP checksum table maintained on the TSM/BLM card. As a result, the LNP checksum table must be downloaded to all TSM/BLM cards during data loading and must be maintained on the TSM/BLM cards during database updates and audit queries.

Currently the checksum table is not loaded to the cards. When a LNP database update occurs the checksums on the card will be set unknown for any dirty pages. When a dirty page is audited the LNP checksum table on the card is updated accordingly by storing the recalculated checksum in the table. During data loading LNP updates and audit notifications shall be ignored at the card: currently a LNP update during loading would reset the TSM/BLM card.

During the warm restart process dirty pages will not be audited, as the checksums for the dirty pages are unknown. The LNP checksums must be approximately 99% known or a warm restart is not permitted (currently a maximum of 250 dirty pages). This initial audit to determine if a warm restart is allowed is performed using the current LNP checksum table in the card's persistent database.

If the checksum compare fails a card reset and full GTT and LNP data reload shall be performed. No application trouble or obituaries will result; the card will simply restart the loading process. The existing LNP audit process currently generates 1 checksum calculation every 1.36 seconds. Typically, LNP updates will dirty the same page(s) as previous updates and thus require significantly fewer writes to disk when collected over multiple updates.

LNP audit does not audit recently changed dirty pages, thus allowing them to be collected over multiple updates. Performance measurements of the existing LNP audit showed on average 5 or fewer unknown checksums (total) for typical sequential updates during 2 TN/sec operation.

If an incremental load to the card is required during a warm restart, the incremental load will complete and then a final audit shall be performed prior to data load complete and going IS-NR. This final audit includes pages dirtied prior to the reset only (checksum is unknown in the persistent LNP checksum table prior to the download of the new LNP checksum table).

A cold restart will result in no pages being audited following the incremental load. Should this final checksum compare fail, indicating that the warm restart failed, a full LNP data reload shall be attempted.

The LNP checksum table shall be reloaded to the cards only after incremental loading is complete and LNP updates have been inhibited. The cards will then complete the audit process for all dirty pages not initially audited during the warm restart verification.

The LNP download and audit timeline for a warm restart is depicted in Database Levels and On-Card Warm Restart Decision Flow).

Hardware Requirements

The Warm Restart and Incremental Loading functions require existing EAGLE hardware; no new or additional hardware is required for these features. All modifications are at the software level.

- TSM (SCCP) card
- BLM (EBD&A) card.
- MCAP (OAM) card.

The TSM/BLM cards must be equipped with enough daughterboard memory to load the entire LNP database. The daughterboard requirements for the EBD&A BLM card are exactly the same as the memory requirements for a TSM card running the SCCP application.

Upgrade Considerations

Warm restart shall be supported following upgrade to release 26.0. Warm restart shall not be supported during Release 26.0 upgrade. The warm restart feature provides new functionality at the card level for maintaining over a reset the database level, status, checksum, and other information, which is required to determine if a warm restart should be allowed. Without this functionality the integrity of the LNP database cannot be verified. As a result warm restart cannot be supported during the initial upgrade to Release 26.0.

Subsequent upgrades will have the capability to perform a warm restart of TSM/BLM cards provided the warm restart conditions as outlined by this document are met. Additional conditions imposed on a warm restart would include:

- card-level capability for converting the existing LNP database if the upgrade requires any LNP table conversions.

- ability to download new LNP tables during a warm restart which are not defined in the source release database on the card.

Currently, new feature development that requires table conversions is written only for the OAM database and the data is loaded to the cards following conversion. In order to perform a warm restart during an upgrade requiring LNP table conversions, the conversion functions must also be written for the TSM/BLM cards. If the LNP database version does not change and no table conversions are required, upgrades after release 26.0 will be capable of warm restart provided the network conversion utilizes the **`data=persist`** parameter when initializing TSM/BLM cards.

Dependencies

The warm restart and incremental loading features must be implemented together for a complete solution to exist. These features have no other dependencies.

Limitations/Restrictions

1. LNP audit must be ON and have run at least once to completion. If LNP audit is not turned on, all LNP checksums on the OAM are set to unknown. A warm restart is allowed only if LNP audit has completed an audit of the current database at least once and the LNP checksums are approximately 99% known. Without the LNP checksums in a known state, the database on the TSM/BLM cards cannot be verified following the reset. Warm restart may not be allowed if a worse-case 2 TNs is maintained.

   Sustained 2 TNs on a small database will prevent a warm restart. Fewer checksums are in use for a small database. As a result, an update will make a greater percentage of the in-use checksums unknown. Thus the percentage known of the checksums depends on the size of the database.

2. Non-LNP database provisioning which affects the TSM/BLM cards (such as GTT updates to the TSM cards or alloc-mem 4 digit object updates to all TSM/BLM cards) during loading may result in a card reset. Unlike the continuous stream of LNP updates automatically applied to the EAGLE from the LSMS, non-LNP updates are controllable by the customer. The customer must decide whether to suspend these updates during TSM/BLM loading based on minimum service and their current priorities.

   If the update being applied affects tables already loaded, the card will not reset (i.e. the database class of the update was already loaded by the card).

3. Card loading, including Incremental Loading, is inhibited while the import and restore operations are in progress.

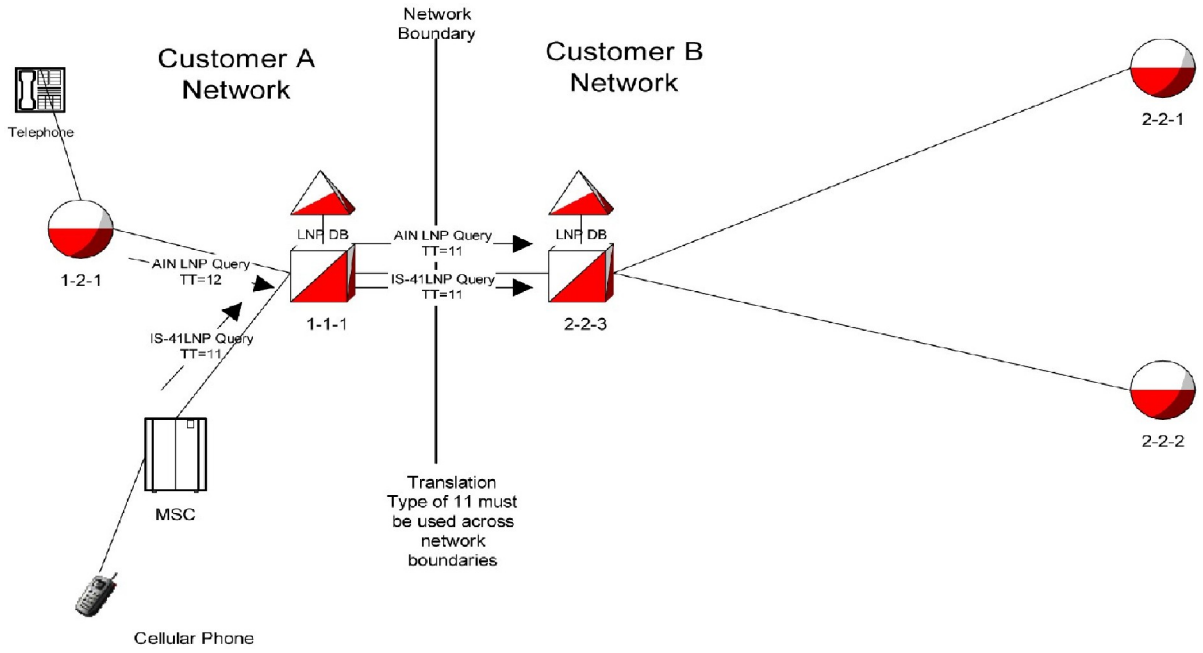
4. Database btree rotations will limit the time tracking capabilities by causing excessive database level entities and multiple database level records to be stored for a single database level.

TT Independence for LNP Queries (EAGLE Release 30.0/IP7 Secure Gateway Release 8.0)

Description

Currently, the translation type in the query message is used to determine the type of LNP query (AIN, IN, WNP) for correct decoding and response formulation. LNP queries between networks are defined to use TT=11, regardless of the protocol used. Also, there are other cases where the TT alone may not be enough to determine the type of protocol being used, thus making it impossible to correctly decode all queries. Refer to Figure 5-28 .

Figure 5-28. Inter-Network Support for LNP Queries



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

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

With the TT Independence for LNP Queries feature, the LNP subsystem will be able to determine the protocol of the query based on other fields in the SS7 message, rather than relying on the TT value. This allows the same translation type to be used for multiple protocols. It allows a query between two networks to be properly handled. (All LNP queries between networks are defined to be TT 11.)

Hardware Requirements

No new hardware is needed to support this feature.

Upgrade Considerations

While this feature does not affect the upgrade process, note that all SCCP cards must be upgraded to the release that contains the TT Independence for LNP Queries feature, prior to provisioning the LNPQS service.

Limitations

With the implementation of TT Independence, PLNP Queries with TT associated with LNPQS will be processed and pegged as IN LNP Queries.

Despite the fact that the legacy EAGLE's interface allows the provisioning of the LNP NPANXX table's Default Translation (MRGT) using the command **ent-lnp-npanxx**, this should not be done for LNP services. Thus, EAGLE will *not* use the NPANXX Default Translation for LNP Queries, even if this data is provisioned.

TUP Message Type Screening (Release 31.6)

Telephone User Part (TUP) protocol is a predecessor to Integrated Services Digital Network (ISDN) User Part (ISUP) that remains in use for some market areas. ISUP and TUP share the same screen function table. TUP is supported for Gateway Screening (GWS) by overloading the ISUP screening table. To use TUP screening, the screen set defines the screening order to have an SIO table with the rule SI=4 for TUP to screen the TUP messages. This SIO screening reference is specified in the **ent-scr-isup** command as the next screening reference (**nsr**) value in a screening reference for TUP message types.

Point Code screening of DPC and BLKDPC can be used with the overload of the ISUP screen function with TUP, as long as an SIO screen comes first. To do this there should be an SIO rule for SI=4 to screen for TUP protocol and another rule with SI=5 for ISUP protocol, these two rules must also have separate Next Screen Functions. This allows the screening rules after the SIO to have two separate streams, one that ends with true ISUP, the other that ends with TUP overloading ISUP.

To use TUP screening, the screen set defines the screening order to have an SIO table with the rule SI=4 for screening the TUP messages.

Limitations

- Point Code screening of DPC and BLKDPC can be used with the overload of the ISUP screen function with TUP, as long as an SIO screen comes first. To do this there must be an SIO rule for **si=4** to screen for TUP protocol and another rule with **si=5** for ISUP protocol. These two rules must also have separate Next Screen functions. This allows the screening rules after the SIO to have two separate streams, one that ends with true ISUP and the other that ends with TUP overloading ISUP in the screening table.

- For the Support TUP Message Type Screening feature, the LSONISMT ISUP and TUP messages are pegged by message type only. There is potential for overlap because TUP and ISUP share a common message type value and the screens are set up to screen this value. Therefore there is no way to know whether the message was ISUP or TUP from a measurements point of view. The UIMs generated include the SIO value, but measurement reports do not.

- For the Support TUP Message Type Screening feature, the potential for overlap of message type values for ISUP and TUP also applies to the screening function. Care must be given to provision the screenset order with SIO screen rules to separate SI=4 (for TUP) and SI=5 (for ISUP) prior to the ISUP screening function.

Although the **-scr-isup** commands support the two separate parameters **isupmt** and **tupmt**, the parameters are handled by the database as the common generic parameter named **isupmt**.

Two-Point IPLIMx (EAGLE 27.1, IP^7 Release 2.2)

Two-point IPLIMx allows a single DCM card loaded with the **iplim** application or the **iplimi** application to support two point-to-point links. In previous releases, each point-to-point link required a separate DCM card.

Two sockets can be provisioned for each DCM card that runs an **iplim** application or **iplimi** application. One socket is associated with the A port and one with the B port. In this case, a port is a signaling link. Both sockets use the same physical interface connection and the same IP address.

Refer to the Database Administration Manual - SS7 for current information on this feature.

Unregistered Routing Key Treatment (IP^7 Release 3.0)

Unregistered Routing Key Treatment (URKT) provides options for routing misdirected ISUP messages, as well as options for routing other signaling information types such as SCCP and TUP. New Partial and Default routing key types have been introduced to improve the treatment of unregistered routing keys. Supported Partial keys include: DPC+SI+OPC for CIC traffic, DPC+SI for CIC and SCCP traffic, DPC only, and SI only for CIC, SCCP, and MTP3-Other traffic.

Each Partial and Default routing key is associated with a socket, or a list of sockets.

A hierarchy of lookups occurs for each MSU that does not match a full entry in the routing key table. **Table 5-22** clarifies how a hierarchical lookup that attempts to deliver each MSU to the best location is performed. Before the lookups can begin, the type of MSU must be determined based on the following:

- Type of MSU equals CIC when the MSU has an SI value of 5, 13 (ANSI and ITU) or 4 (ITU only).
- Type of MSU equals SCCP when the MSU has an SI value of 3 (ANSI and ITU).
- Type of MSU equals Other SI for all other MSUs.

Table 5-22. Unregistered Routing Key Hierarchy

MSU Type	Lookup Order	Portion of MSU that Must Match Routing Key	Full/ Partial/ Default
CIC	1	DPC + SI + OPC + CIC	Full
	2	DPC + SI + OPC (*ignore CIC)*	Partial
	3	DPC + SI *(ignore OPC & CIC)*	Partial
	4	DPC *(ignore SI, OPC & CIC)*	Partial
	5	SI *(ignore DPC & OPC & CIC)*	Partial
	6	None	Default

MSU Type	Lookup Order	Portion of MSU that Must Match Routing Key	Full/ Partial/ Default
SCCP	1	DPC + SI + SSN	Full
	2	DPC + SI *(ignore SSN)*	Partial
	3	DPC *(ignore SI, OPC & CIC)*	Partial
	4	SI *(ignore DPC & SSN)*	Partial
	5	None	Default
OtherSI	1	DPC + SI	Full
	2	DPC *(ignore SI)*	Partial
	2	SI *(ignore DPC)*	Partial
	3	None	Default

The hierarchy is intended to guarantee that the MSU is delivered to the best possible location, based on closest match to the MSU content. An MSU that does not match a routing key is discarded.

Update Validation (Release 34.0)

Description

The Update Validation feature provides additional data validation checks prior to applying an update or change from the RTDB at the EPAP or ELAP to the RTDB on the DSM cards. These additional checks are designed to prevent overwriting of existing data records with new data records when operators are provisioning new subscribers.

Hardware

No new hardware is required for this feature.

Upgrade Procedure Enhancements (Release 22.0)

With release 22.0, current EAGLE users of release 20.0 can be upgraded directly to release 22.0 without having to be upgraded to release 21.0 or release 21.1. Users of Release 21.0 and 21.1 can be upgraded directly to Release 22.0.

The upgrade procedure is executed in two parts.

- Database and GPL Upgrade — the current databases are converted to the release 22.0 format and the GPLs are upgraded with the release 22.0 GPLs.

- Network Upgrade — distributes the upgraded GPLs through out the system and distributes the converted databases to the upgraded GPLs.

The upgrade procedure uses the **act-upgrade** command and, if upgrading from a release 20.0 system, the **init-network** command. The upgrade procedure also uses these items.

- A removable cartridge containing the release 22.0 software.
- A removable cartridge containing the software of the current release (20.0, 21.0, or 21.1).
- A spare TDM containing the current databases for the current release (20.0, 21.0, or 21.1).

The **act-upgrade** command converts the current, release 20.0, 21.0, or 21.1, database on the active MASP to a release 22.0 database and controls the MASPs during the upgrade process.

The **act-upgrade** command has only one parameter, **action**, which details the type of upgrade action to be performed. The **action** parameter has three values, **convertoam**, **oamcomplete** and **dbstatus**.

The **action=convertoam** parameter converts the databases on both the active and standby MASPs.

The **action=oamcomplete** parameter sets the upgrade phase to phase 3, sets the database to coherent on the active and standby fixed disks, and places the SEAS terminal ports back in service.

The **action=dbstatus** parameter displays the status of all the database partitions on both the active and standby MASPs. The output is identical to the output of the **rept-stat-db:display=version** command.

No Reportable Downtime on Network Restart

Release 22.0 provides for network restarts of the EAGLE STP, using the **init-network** command, that require less than 30 seconds of nodal isolation and thus do not require reporting of any STP downtime (GR-929-CORE, section 3.1.1, page 3-3). This enhancement prevents reportable downtime for both network restarts due to unusual conditions and for network restarts during in-service upgrades.

Network restart is the procedure that allows all non-MASP cards to be rebooted and restored to service in an orderly and controlled fashion with the intent to minimize network nodal isolation time, the time during which an EAGLE STP is unable to communicate to another node in the network (no signaling links are aligned).

Currently, if an EAGLE STP LIM running the SS7ANSI application is rebooted, it takes approximately 42 seconds to reload the card, align the signaling link, and restart traffic on that signaling link. Thus, with the goal to minimize network nodal isolation to be less than 15 seconds during in-service network upgrades and abnormal conditions requiring network restarts, the network restart process initiated by the **init-network** command will be as follows:

1. Before the network restart process can be started, the MASPs must be in one of two possible states, either the GPL status of the MASPs should be in the Upgrade Phase 3 Mode; or the MASPs must be in full function mode. If the MASPs are not in the proper state, the command is rejected with this message.

   Error Message

   ```
   E2980 Cmd Rej: Must be in upgrade phase 3 or full function mode
   ```

   The term Upgrade Phase 3 Mode means that the MASPs are running the approved GPLs, but the other network processors are only prepared to be upgraded. The Upgrade Phase 3 Mode is reached by entering the **act-upgrade:action=oamcomplete** command during the upgrading process.

The term Full Function Mode means that the MASPs are running the approved GPLs. The full function mode is the normal operating mode for the MASPs.

2. The system chooses two LIMs running either the SS7ANSI or CCS7ITU applications equipped with an in-service active link based on the best available priority scheme. Each LIM must have one signaling link in an in-service active state. These LIMs are referred to as the alternate cards. These LIMs are the first to be preloaded and eventually crossloaded during the network initialization.

   The best available priority scheme used by the **init-network** command is as follows:

   All the LIMs running either the SS7ANSI or CCS7ITU applications are searched to create a list of a maximum of four LIMs sorted by highest priority link type, with each LIM containing at least one active signaling link. The priority of link types are C, B, A, D, and E in that order. LIMs with two active signaling links, that contain the same link type as LIMs with one active link, are given priority in the list.

   After the list has been created, the LIMs are identified as alternate or main cards. If four cards are in the list, then two cards are the alternate cards, and two cards are the main cards. If three cards are in the list, then two cards are the alternate cards, and one is the main card. If two cards are in the list, then one card is an alternate card, and one card is the main card. If only one card is in the list, then it is the main card and there is no alternate card. If no cards are in the list, then the **init-network** command is rejected with this message.

   Error Messages

   ```
   E2981 Cmd Rej: Already in nodal isolation
   ```

   The **init-network** command requires the four LIMs running either the SS7ANSI or CCS7ITU applications with at least one active signaling link on each LIM. If four LIMs are not available in the EAGLE, the **force=yes** parameter must be specified with the **init-network** command. If the **init-network** command is entered with less than four LIMs available, and the **force=yes** parameter is not specified, the command is rejected with this message.

   ```
   E2371 Cmd Rej: Force parameter is required
   ```

3. The value of the **mtprsit** (MTP restart timer) parameter of the **chg-stpopts** command is checked. If the value of this timer is less than 30 seconds, the **init-network** command is rejected with this message.

   Error Message

   ```
   E2983 Cmd Rej: STPOPTS table MTPRSIT value must be at least 30000.
   ```

   This makes sure that the MTP restart timer does not expire when the **init-network** command is executed and disabling the MTP restart feature.

4. The system sets the Inhibit Dynamic Data Loading indicator on the LIMs (running the SS7ANSI, CCS7ITU, or SS7GX25 applications) ACMs, and ASMs running the SCCP application.

   The term dynamic data loading applies to all of the LIMs (running the SS7ANSI, CCS7ITU, or SS7GX25 applications) ACMs, and ASMs running the SCCP application; and refers to software used to hunt for a card that already has its application software loaded and to crossload dynamic data from that card. Dynamic data is the data maintained on the main assemblies of the LIMs, ACMs, and ASMs that change in response to system conditions.

5. The system reloads all the ASMs running the GLS application and one of the ASMs running the SCCP application, if there is more than one ASM running the SCCP application.

6. After the all the ASMs running the GLS application have been reloaded, and the one ASM running the SCCP application has been preloaded. Then the alternate cards are reloaded. After the alternate cards have been reloaded and are waiting to crossload the dynamic data, then all the other LIMs, ACMs, and ASMs running the SCCP application, excluding the main cards, are reset.

7. When these LIMs, ACMs, and ASMs have completed resetting, the system resets the main cards.

8. The system removes the Inhibit Dynamic Data Loading indication first on the preloaded ASM running the SCCP application and the alternate cards. This allows all the LIMs, ACMs and ASMs running the SCCP application to complete crossloading and align.

9. All cards reset become active, and traffic is restarted.

Upgrading the Application Processor of the Main Assemblies from the Intel 286/386 to the Intel 486 Microprocessor (Release 20.0)

The main assembly for the EAGLE's link interface modules (LIMs), applications services modules (ASMs) and application communications modules (ACMs), has been upgraded to the Intel 486 (32 bit, 25 Mhz) microprocessor, replacing the Intel 286 (16 bit, 16 or 20 Mhz) microprocessor. Using the Intel 486 microprocessor more than doubles the internal processing capability of each LIM, ASM, or ACM, and provides 4295 Megabytes of addressable memory map versus just 1 Megabyte for the Intel 286 microprocessor in the non-protected mode. The new design also includes field upgradable socketed memory space to accommodate up to 68 Megabytes of RAM for each main assembly.

Intel 486-based modules are currently being shipped to customer sites for all new EAGLE STP installations. These are fully backward compatible with the existing Intel 286-based LIMs, ASMs, and ACMs, and function identically when equipped with all pre-Release 20.0 software, now in use on more than 90 installed EAGLE STPs. EAGLE STPs equipped with the Intel 486-based modules are hardware-ready for all features currently being developed or planned through 1997.

Use IMT Bus Instead of MBUS (Release 23.0)

In previous releases, the maintenance bus (MBUS) has been used to communicate with the cards in the EAGLE without using the IMT bus. The maintenance bus was used to connect or disconnect cards from the IMT bus and to reinitialize the cards in the EAGLE. The maintenance bus was carried on the "A" clock cable from the control shelf to the extension shelves.

In Release 23.0, the maintenance bus has been removed from the EAGLE, and the messages that were sent across the maintenance bus are now sent on the IMT bus. The maintenance bus can now be used for other purposes, such as distributing the clock signals for the high-speed ATM signaling links.

The commands now using the IMT bus instead of the maintenance bus are: **`init-card`**, **`init-sys`**, **`disc-imt`**, **`conn-imt`**, **`inh-imt`**, and **`alw-imt`**. The operation and performance of these commands from a user's perspective has not changed.

User-Initiated Keyboard Locking (Release 22.0)

In Release 22.0, a user will be able to secure the terminal while temporarily away from the terminal without having to log off the terminal with a new command, **lock**.

When the **lock** command is entered, the keyboard is immediately locked, the *Command Executed* response appears in the command information area of the terminal display, a *KEYBOARD LOCKED* indicator is displayed in the lower-right portion of the VT320 terminal (this indication is not displayed on KSR terminals), and a counter of consecutive failed attempts to unlock the terminal is set to 0. The following message appears in the scroll area of the terminal.

```
Terminal keyboard is locked. Enter UNLOCK command to unlock.
```

When the terminal keyboard is locked, the only input allowed on the keyboard is the **unlock** command which is used to unlock the keyboard. If any command other than the unlock command is entered while the keyboard is locked, the command is rejected with the following message.

```
E2004 Cmd Rej: Keyboard is locked. Enter UNLOCK command
```

This message is displayed regardless of whether or not the command contained any command syntax errors. In addition, while the keyboard is locked, only these terminal function keys are enabled.

- F6 - refresh screen
- F8 - toggle scroll lock
- F11 - toggle between VT320 and KSR terminal modes

Other terminal function keys are ignored. If one of these function key is pressed no error message is displayed.

When the **unlock** command is entered, the user is prompted for the user's password with the following message.

```
Enter LOGIN password to unlock keyboard :
```

The password that must be entered is the password of the user that was logged on to the terminal when the **lock** command was entered.

If the password entered at the **unlock** command prompt does not match the password of the user logged on to the terminal, then the **unlock** command is rejected with the following error message.

```
E2765 Cmd Rej: Invalid password. Keyboard is locked. Enter UNLOCk command.
```

Each time the **unlock** command is entered, the system increments the counter of consecutive failed unlock command attempts by 1. If the counter equals or exceeds the login failure threshold for the terminal port as defined by the **mxinv** parameter of the **chg-trm** command, then the following message is issued to each terminal able to receive unsolicited system administrator messages.

```
Info: xxxxxxxxxx successive UNLOCK failures on port yy
```

where:

xxxxxxxxx = the number of consecutive failed **unlock** command attempts (0 - 4,294,967,295)

yy = the number (1 - 16) of the terminal port on which the failed **unlock** command attempt occurred.

In addition, for every consecutive **unlock** command failure that is an even multiple of login failure threshold value, assuming the login failure threshold is greater than 0 (for example, if the value of the login failure threshold

is 3, the even multiple of this value is 6), the terminal port is disabled for the period time specified by the **dural** parameter of the **chg-trm** command.

If any commands are entered during the period of time when the terminal port is disabled, the commands are rejected with the following message.

Error Messages

```
E2770 Cmd Rej: Port temporarily disable due to excessive UNLOCK failures.
```

Specifying a value of 0 for the **mxinv** parameter turns off the temporary terminal port lockout feature and no messages regarding **unlock** command failures and login failures are issued and the terminal port is not disabled. If the value of the **mxinv** parameter is greater than 0 and the value of the **dural** parameter is 0, the EAGLE issues the information message reporting the number of consecutive login failures when that number exceeds the value of the **mxinv** parameter, but the terminal port is not disabled.

If the password entered at the prompt from the **unlock** command matches the password of the user that is logged on to the terminal, the keyboard is unlocked. The following message is displayed in the scroll area of the terminal,

```
Info: Keyboard unlocked. xxxxxxxxxx UNLOCK commands were attempted.
```

where xxxxxxxxxx is the number of times the **unlock** command was entered on the terminal.

Any terminal subject to idle terminal monitoring whose keyboard is subsequently locked will not be disabled as long as the keyboard remains locked. As soon as the keyboard is unlocked, the terminal's counter of accumulated idle time is reset to 0 and idle terminal monitoring resumes.

SEAS terminals (a terminal port with the **type=seas** parameter specified) cannot be locked. The **lock** command checks the terminal type of the terminal that the **lock** command is entered on. If the **lock** command is entered on a SEAS terminal, the command is rejected with the following message.

```
E2766 Cmd Rej: Command cannot be executed on a SEAS terminal
```

The **unlock** command can be entered on a SEAS terminal, however it is always rejected with the following message because SEAS terminals cannot be locked. No password prompt is issued to the SEAS terminal.

```
E2767 Cmd Rej: Keyboard is not locked
```

Any time a user is automatically logged off a terminal while the keyboard is locked, the keyboard will be unlocked. This includes automatic logoffs that are caused by:

- changing terminal characteristics
- inhibiting or allowing the terminal with the **rmv-trm** or **rst-trm** commands
- executing either the **chg-user** or **dlt-user** commands
- communications loss to the terminal

The system administrator can unlock a locked terminal by taking the terminal out of service with the **rmv-trm** command, then restoring the terminal to service with the **rst-trm** command.

While the keyboard is locked, only inputs to the terminal are monitored. Outputs destined for the terminal continue to be output regardless of the state of the keyboard lock.

The **rept-stat-user** command shows which terminals are currently locked with the entry *lock* in the COMMAND field of the output. The following is an example of the output of the **rept-stat-user** command.

```
USER ID          TERM #  IDLE SINCE           COMMAND          STATE
EAGLE               8    97-06-07 06:45:23    lock             IDLE
REPORT COMPLETED
```

Using the DPC/SSN Parameters and GTA Range in Displaying Global Title Translations (Release 22.0)

This feature enhances both the SEAS *VFY-GTT* and EAGLE **rtrv-gtt** commands to support specific values for the **pc** and **ssn** parameters, as well as the end range for the **gta** parameter. This enhancement allows customers with large GTT data bases to limit the amount of output for each verify request, thus avoiding the possibility of reaching the 400K UAL limit.

The **pc**, **ssn**, and **egta** parameters have been added to EAGLE's **rtrv-gtt** command.

The SEAS *VFY-GTT* command now supports the **dpc**, **ssn**, and **&&-gta** parameters.

The EAGLE does not support the relative cost parameter. When this parameter is specified on the SEAS interface, the EAGLE ignores this parameter. The value 50 is displayed in the *VFY-GTT* output because this parameter is mandatory in the output syntax.

The EAGLE only supports one DPC-SSN combination for each global title translation (GTT). A specific DPC-SSN entered with a specific global title address for this command must match the one existing for the specified global title address. However, because only one DPC-SSN combination is allowed per GTT, specifying ** for either the DPC or the SSN for a specific global title address results in the same response as if the specific values were entered.

Variable-Length Global Title Translation (Release 26.1) (IP^7 Release 2.2)

The IP ^{7} Secure Gateway supports either of the following types of global title translation:

- Standard GTT determines which translation table to use based solely on the Translation Type (TT) contained in the SCCP called party address.
- Enhanced GTT determines which translation table to use based on the TT, Numbering Plan (NP), Nature of Address Indicator (NAI), and Global Title Indicator (GTI), all of which are contained in the SCCP called party address.

For either type of global title translation, each translation table has a fixed length for the numbers it includes.

In previous releases, if the IP ^{7} Secure Gateway received a number that had fewer digits than were defined in the table, the IP ^{7} Secure Gateway did not perform the GTT. In this release, if the IP ^{7} Secure Gateway receives a number that has fewer digits than are defined in the table, the IP ^{7} Secure Gateway pads the called party address with special non-decimal characters so that the length of the called party address matches the length used by the table.

(In either release, if the IP ^{7} Secure Gateway received a number that had more digits than were defined in the table, the IP ^{7} Secure Gateway used as many digits as were defined for the table; for example, if a given translation table contained called party addresses of length 10 and an MSU with a called party address of length 12 was received, the IP ^{7} Secure Gateway used the first 10 digits.)

If the user specifies an individual entry or range of entries on the **ent-gtt** command (used to provision a standard GTT translation table) or on the **ent-gta** command (used to provision a enhanced GTT translation table) with a value that has fewer digits than the predefined length of the table, the IP ^{7} Secure Gateway adjusts the internal representation of the specified value to match the length of the table.

Whenever a global title address is displayed, it is displayed as it was entered at the terminal.

Variable Length GTT (Release 26.1)

Description

Variable Length GTT provides customers the ability to provision Global Title entries of varying lengths to a single Translation Type or GTT Set. In prior releases, only Fixed Length GTT was supported, meaning that all Global Title entries assigned to a single Translation Type or GTT Set had to be the same length.

With Variable Length GTT, customers can assign Global Title entries of up to 10 different lengths to a single Translation Type or GTT Set. These lengths are not defined when entering the Translation Type or GTT Set. As the entries are entered, the software keeps track of the length, allowing only 10 different lengths.

When 10 different lengths are specified for a Translation Type or GTT Set, only Global Title entries with lengths matching those defined are allowed. That is, if the craftsperson has entered 10 different lengths and a new entry is entered with a length that does not match one already entered, the new one will not be allowed.

This feature is controlled with a feature bit. This feature bit may be set independently of whether Enhanced GTT is used or not.

In addition to satisfying the needs of European customers, this feature provides U.S. customers with an easier method of provisioning GTT data, since shorthand ranges can be used to represent large groups of GTAs. Thus more specific GTAs can be provisioned as exceptions to these larger groups.

Consider the following example:

Table 5-23. Variable GTT Example

TT	GTA	EGTA	PC-SSN	XLAT	RI
11	0	9	1-1-1	DPC	GT
11	9193	9194	1-1-2	DPC	GT
11	919460	919460	1-1-3, 23	DPCSSN	SSN
11	9193800000	9193800999	1-1-4, 25	DPCSSN	SSN
11	9193831000	9193833999	1-1-4, 25	DPCSSN	SSN

In this example, the customer wishes to perform final GTT on all numbers matching the last three entries. Note the shorthand used in the third entry, as this single entry represents all numbers beginning with the first six digits of 919460, i.e. 9194600000 - 9194609999. Any number not matching the last three entries requires intermediate GTT, and is routed to different nodes based on the ranges specified. The first entry provides a "default" for all GTAs not matching more specific GTAs entries for this translation type.

As another example, consider the possibility that an MSU comes in with the address "9193805000". The address is a 10-digit number, and therefore would first get looked up on the 10-digit tree. In this example, these would fail. The 6-digit tree would be looked up next. This would fail, too. Finally, the address would match the 4-digit range of 9193 to 9194.

Upgrade Considerations

This section considers the software upgrade requirements of the Variable Length GTT feature, which involves a database upgrade. The database upgrade is impacted by the following changes:

- With this feature, the previous implementation of "Padded Variable Length GTT" becomes obsolete. An upgrade path is provided for customers who have this feature activated. (See "Hardware Required" for more information.)
- Removing any padded entries from the GTT database and entering them into new trees for the corresponding GTT Set also impacts the GTT_SET table entry size.
- If the PVGTT and LNP features are on, a DSM is required (see "Hardware Required" for more information).

Hardware Required

This feature has the same hardware requirements, provisioning rules, and ratios as does GTT. However, in order to meet performance requirements, the card required for this feature may need to be upgraded. The choice of hardware will be determined by the sales team based on the current customer database and needs. The hard and fast rule is:

- If LNP is OFF, a TSM should be able to provide the desired performance.
- If LNP is ON, a DSM is needed.

At a minimum, the Variable GTT feature requires TSM cards for SCCP functionality prior to turning on the feature bit. Due to the possible combinations available with SCCP features, Table 5-22 can be used to clarify the required hardware for VGTT, as well as other SCCP features.

Table 5-24. VGTT Required Hardware

Feature	Required Hardware
VGTT	TSMs (N+2)
EGTT	TSMs (N+1)
VGTT + EGTT	TSMs (N+2)
G-PORT, G-FLEX, INP	DSMs (N+1)
VGTT/LNP	DSMs (N+1)
LNP (<12 million)	TSM (N+1)
LNP (>12 million)	DSM (N+1)
GTT	ASM/TSM (N+1)

Warning Message When LIMs Added with Insufficient TSMs (Release 25.0)

This feature enforces the current TSM provisioning rules of one TSM at a minimum for every 16 LIMs when a LIM is added. When a LIM is added, if there are not enough TSMs, a warning message is displayed. The craftsperson then has the option to override the warning, forcing the card to be entered.

Per the EAGLE engineering rules, a minimum of 1 SCCP (ASM or TSM) card is required for each group of 16 low-speed LIMs, with one additional SCCP card required per system for N+1 redundancy.

Since one HSL can provide the data transfer capability of approximately 16 DS0s, 2 HSL ATM cards can be supported by a minimum of 1 SCCP card.

The feature enforces the minimum configuration.

When a low-speed LIM card (ss7ansi, ccs7itu, ss7gx25) or a high-speed LIM card (atmansi) is entered via the **ent-card** command, the number of provisioned SCCP cards is evaluated to ensure that the minimum required configuration is maintained. The minimum configuration value is one SCCP card for each multiple of 16 LSLs, or 2 HSLs, rounded up.

One additional ASM/TSM card is required to maintain N+1 redundancy.

The warning is accomplished via command error or other means, and does not produce an alarm.

The craftsperson must explicitly override the warning to provision a card that breaks the required configuration rule. When this is done, the warning still is displayed.

When the warning is overridden, the event is logged in the security log.

Weighted GTT Loadsharing (Release 36.0)

Description

The Weighted GTT Loadsharing feature is an enhancement to intermediate and final Global Title Translation loadsharing. Provisioning provides control over MAP and MRN entities so that unequal route costs can be defined within a loadsharing group. Provisioning also controls loadsharing groups so that if insufficient capacity is available within a loadsharing group, the group is not used.

A feature access key (FAK) for part number 893017001 is required to enable the Weighted GTT Loadsharing feature.

- The GTT feature must be on before the WGTTLS feature can be enabled.
- After the feature is enabled, it can be turned on and turned off.
- No temporary FAK is allowed for the feature.

The Weighted GTT Loadsharing feature controls loadsharing through the MAP and MRN entities within a MAP group or MRN group. MAP entities distribute MTP-routed GTT traffic to the final destination. MRN entities relay MTP-routed GTT traffic to other nodes for further GTT processing.

The Weighted GTT Loadsharing feature provides the following two methods to control the distribution of GTT traffic through MAP or MRN groups:

- Individual weighting for each RC group entity

  Individual weighting assigns different load capacities, in the range of 1 to 99, to the entities of an RC group. Each entity receives a percentage of the network traffic proportionate with its weight relative to the total weight of the RC group.

- In-service threshold of each RC group

  The in-service threshold is the minimum percentage of the total of the provisioned weights of an RC group that must be available for the RC group to receive network traffic. An in-service threshold of 1% means that the group will be used if any member is available. The entire RC group is considered unavailable for network traffic if the percentage of the available weights is less than the in-service threshold. The RC group is considered available if the percentage of the available weights is greater than or equal to the in-service threshold. If an RC group is available, network traffic can be sent to any available entity in the RC group.

WGTTLS adds 2 new modes for loadsharing:

- Weighted Load-Share
- Weighted Combined Load-Share.

WGTTLS can be turned on and off after it is enabled. The feature operates as follows:

- If weights are not assigned to a group, the original mode (Solitary, Dominant, Load-Shared, or Combined Load-Shared/Dominant) is used.
- If WGTTLS is enabled and turned on, and weights are assigned to entities within an MRN group or a MAP group in Load-Shared mode, Weighted Load-Share mode is used.
- If WGTTLS is enabled and turned on, and weights are assigned to entities within an MRN group or a MAP group in Combined Load-Shared/Dominant mode, Weighted Combined Load-Share mode is used.

Hardware Requirements

The Weighted GTT Loadsharing feature has the following hardware requirement:

- DSM cards
- TSM cards that run the SCCP application cannot be provisioned if the feature is enabled. The feature cannot be enabled if TSM cards that run the SCCP application are configured in the system.

Limitations

The Weighted GTT Loadsharing feature has the following limitations:

- Outbound traffic distribution is affected by incoming traffic distribution. If the OPC, SLS, and incoming Link ID do not span a diverse range, then weighted distribution may not be able to be maintained. Maintaining the same DPC for the transaction is given priority. This affects SCCP Class 1 Sequenced traffic only. It does not affect Class 0, or Class 1 with **sccpopts:class1seq=off**, which are balanced regardless of OPC, SLS, and incoming Link ID.

- When weights are assigned or changed in an MRN or MAP group that is handling transaction-based traffic, the destination assignment of some transactions will change. This may cause some MSUs of the transaction to be directed to one destination and some to another destination.

- If all RC groups in a MAP or MRN Group are Threshold-Prohibited, traffic loss will occur, even though some entities within the group are available. The decision to avoid congestion takes precedence over the routing all traffic.

Wireless Number Portability (Release 23.1)

This feature enhances the Local Number Portability feature to allow wireless service providers to query the LNP database for ported telephone numbers. The query is used to find the location routing number associated with the ported telephone number so the telephone call can be routed to its proper destination.

The Wireless Number Portability feature can only be used for ANSI messages. The Wireless Number Portability feature is not defined for ITU messages.

When a query arrives at the EAGLE from a wireless service provider, it is examined for a translation type associated with the wireless number portability translation type service.

If the query contains a wireless number portability translation type (the route on GT routing indicator) and requires global title translation, the query is routed to the local LNP query subsystem at the EAGLE's true point code.

The local LNP query subsystem processes the query to find the location routing number associated with the telephone number contained in the query. A response is sent to the originator of the query with the location routing number for the ported telephone number.

This type of query cannot be routed to an external node. This means that the processing of Wireless Number Portability queries cannot be split across multiple network elements.

If global title translation is not required and if the destination of the query is the EAGLE's destination point code and subsystem, the query is routed to the local subsystem. If the destination of the query is not the EAGLE's destination point code and subsystem, the query is routed to the destination point code in the query.

The Wireless Number Portability feature must be turned on with the **chg-feat** command and must have the translation types sent from wireless service providers configured in the database with the **ent-lnp-serv** command.

Weighted SCP Load Balancing (Release 27.2)

The Weighted SCP Load Balancing feature allows the user to enter up to eight PC/SSNs into a mated PC/SSN group. Previously, only two mated PC/SSN could be entered. The Mated PC/SSN group can be identified by specifying any PC/SSN within the group. This feature also increases the number of SSN's per PC to 12.

With this feature, EAGLE now supports four different modes for PC/SSN groups:

- Solitary

- Dominant

- Load Shared

- Combined Dominant/Load Shared (new)

Combined Dominant/Load Shared mode is new for this feature; the other modes are existing modes. Previously, the mode was determined by the multiplicity parameter. This parameter is no longer used. Instead, the mode is determined by the relative cost of the PC/SSNs.

A group of replicated PC/SSNs are in Combined Load Sharing/Dominant Mode when at least two of the PC/SSNs have the same relative cost, and another node subsystem in the group has a different relative cost. For example, the user enters the mated PC/SSNs in Table 5-25 :

Table 5-25. MAP for Combined Load Share Mode

PC/SSN	Relative Cost
1-1-0/10	10
1-1-1/10	10
1-1-2/10	20
1-1-3/10	20

The user then enters the Translations in Table 5-26 :

Table 5-26. Translations for Combined Load Share Mode

Translation Type	GTA	PC/SSN
10	000 to 999	1-1-0/10

In this example, if both 1-1-0/10 and 1-1-1/10 are available, EAGLE will evenly distribute MSUs for TT 10 to 1-1-0/10 and 1-1-1/10. If 1-1-0/10 fails, EAGLE will send all MSUs to 1-1-1/10. If both 1-1-0/10 and 1-1-1/10 fail, EAGLE will evenly distribute the MSUs to 1-1-2/10 and 1-1-3/10.

EAGLE will not guarantee sequencing when Combined Load Sharing/Dominant mode is used. MSUs with the same SLS values may be sent to different nodes.

Hardware Requirements

There are no additional hardware requirements for this feature.

Upgrade Considerations

- During upgrade, the adjacency parameter is deleted, and the **srm** parameter remains unchanged.
- During upgrade for mated subsystems in dominant mode, the primary subsystem is assigned a relative cost of 10, and the backup subsystem is assigned a relative cost of 50.
- During upgrade for mated subsystems in shared mode, both subsystems are assigned a relative cost of 50.
- During upgrade for subsystems in solitary mode, the subsystem is assigned a relative cost of 10.
- During upgrade, the multiplicity parameter is deleted.

Limitations

- The EAGLE is not required to support the 2-step NetPilot GTT feature.
- The EAGLE does not guarantee MSU sequencing when Load Sharing is used. MSUs with the same SLS values may be sent to different nodes.

X.25/SS7 Gateway Feature (Release 20.0)

Overview

The EAGLE X.25/SS7 gateway feature connects SS7 and X.25 networks. This enables applications to connect using different transport services. The gateway converts each X.25 packet to SS7 MSU and routes it to an SS7 network. SS7 MSU going the other way are converted to X.25 packets. The gateway is physically positioned between the SS7 network and X.25 network, and it transports messages from one network to the other using the services of SS7 SCCP (Signaling Connection Control Part) protocol.

The X.25/SS7 gateway feature is an optional feature that is turned off by default. To use the X.25/SS7 gateway feature, it must be turned on by entering the appropriate command. Once this feature is turned on, it cannot be turned off.

The gateway supports the following two types of connectivity to the X.25 node.

- Direct connectivity
- Connectivity through a public or private data network

The EAGLE supports 1024 logical channels. All X.25 entities are assigned an SS7 point code and SCCP subsystem number. The individual X.25 connections on the EAGLE are assigned X.25 addresses, as well as alias point codes. These are then mapped in the EAGLE routing table to logical channels. This allows X.25 messages (which use connection-oriented procedures) to be routed and maintained in the SS7 network (which uses connectionless procedures).

The EAGLE uses a LIM equipped with a 486 processor and a generic program load (GPL). The LIM supports the DS0A or OCU, and V.35 interfaces at these lines speeds.

- DS0A at 56 and 64 kbps
- OCU at 56 and 64 kbps
- V.35 at 4.8, 9.6, 19.2, 56, and 64 kbps

The X.25 gateway feature requires that any data that is transmitted must be sent on a connection. A connection represents a route between two application entities (one in the X.25 domain and one in the SS7 domain). It must exist before any messages can be transferred. The connection can be one of three types:

- PVC (permanent virtual circuit): A fixed connection that can only be altered through administration.

- SVCA (switched virtual circuit-automatic): A connection established by the STP as soon as the X.25 gateway card initializes.
- SVCR (switched virtual circuit-remote): A connection established by the X.25-user end when necessary.

Automatic SVCs (SVCAs) are assigned when the X.25 LIM card is booted. The virtual connection is based on information in the routing tables of the EAGLE. The X.25 destination (DE) and the SS7 node must be defined in the EAGLE database in advance.

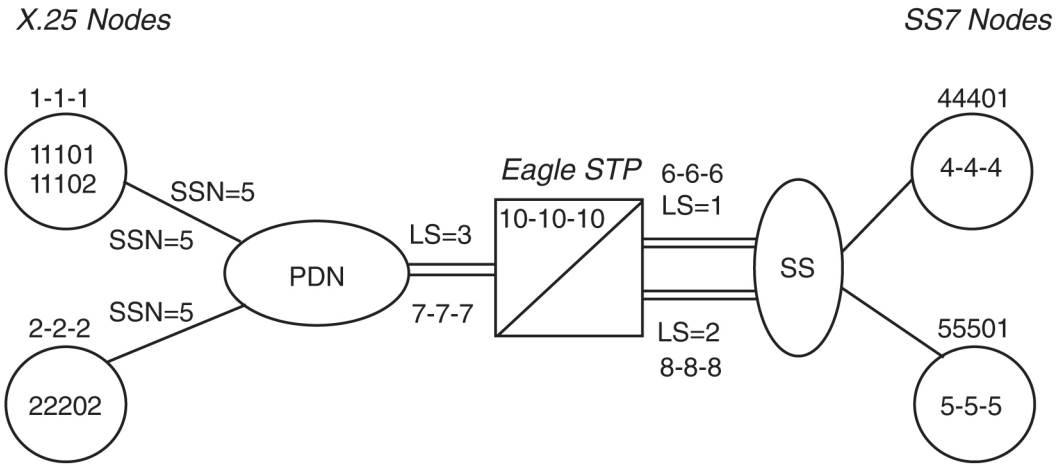
Remote SVCs (SVCRs) are assigned on an as-needed basis. This means when an incoming message from the X.25 network or the SS7 network is received, a “virtual” destination and originating point code are assigned.

For these connections, a route must be defined through administration. Every application entity that can be connected through the gateway must be defined. The association between the application entities must also be defined.

In addition to the normal MTP and SCCP processing, the X.25 gateway feature provides two new components for the STP – gateway routing and protocol conversion.

An X.25 link appears to the STP as though it is an SS7 link. Adjacent point codes are either the originating point code of the X.25 distant end (if the connection is direct), or a virtual point code (if the connection is through a network). This is equivalent to routing through an adjacent STP to the signaling points connected to it. See **Figure 5-29** .

Figure 5-29. Gateway Network



As messages travel from the X.25 network to the SS7 network, the gateway determines the destination point code (DPC) and adds the SS7 SCCP and MTP envelopes to the TCAP message. The gateway determines the virtual circuit and removes the SCCP and MTP envelopes on messages transmitted from the SS7 network side to an X.25 destination.

Other attributes of the gateway are as follows:

- Each X.25 link supports up to 255 logical channels as SVCs or PVCs or a combination.
- All X.25 network-initiated calls are accepted when the calling X.25 node is correctly defined in the STP.
- Gateway screening is supported from the X.25 to the SS7 network.

- Routing does not occur through the X.25 gateway between two X.25 points.
- X.25 networks that do not supply the calling address in the call request are not supported for network-initiated connections.

Message Conversion

The EAGLE performs message conversion for all traffic in both directions. The message conversion removes and adds protocol envelopes used by the X.25 and SS7 networks. The data portion of the message is not changed. The MTP/SCCP of SS7 is converted to X.25 and reverse, depending upon the traffic direction.

Address Mapping

Messages originating from the SS7 network destined for the X.25 network can be routed by the destination point code (DPC) assigned to the X.25 entity in the X.25 routing table (called Xpc). This allows SS7 entities to address the X.25 network without knowing X.25 addresses.

The X.25 routing table provides the X.25 address of each X.25 entity, an SS7 point code for each of the X.25 entities, a subsystem number for SCCP routing, the method of routing to be used (Xpc or normal SS7 routing) and the logical channel to be used between each of the specified X.25 entities and the SS7 entities.

Routing by the X.25 point code assignment allows many SS7 entities to communicate to one X.25 entity without each SS7 entity having to know the X.25 address, and allows all SS7 entities to connect to the X.25 entity over one logical channel. This provides for easier routing table administration. Without this capability, every possible connection between X.25 and SS7 entities would have to be defined in the EAGLE X.25 routing table.

To support the gateway function, the entities within the X.25 network must be assigned an SS7 point code. This point code is assigned in the EAGLE X.25 routing table using EAGLE administration commands. The routing table specifies the X.25 address, the SS7 point code assigned to both the X.25 entities and any SS7 entities which need to connect to X.25, a subsystem number for the X.25 entities, and the logical channel to be used on the X.25 link for connections between the specified entities. Full point code routing is used to route packets to a pseudo X.25 point code.

Each EAGLE connection to the X.25 network is assigned an X.25 address as well. This allows routing of data from the X.25 network to the SS7 network. An SCCP subsystem number is assigned to the X.25 destination to enable global title translation to the X.25 entity.

Logical channels are also assigned in the X.25 routing table. Each X.25 entity must be assigned an SS7 destination, to allow logical channel assignments to be made for the connection. If there are to be several SS7 entities connecting to the X.25 entity over the same logical channel, a wild card entry can be made in the routing table. This allows any SS7 entity to establish a connection over the specified logical channel, but only one connection can be made at any one time.

X.25 Gateway Routing

X.25 gateway routing is performed through four different functions:

- Connection determination
- X.25 connection control

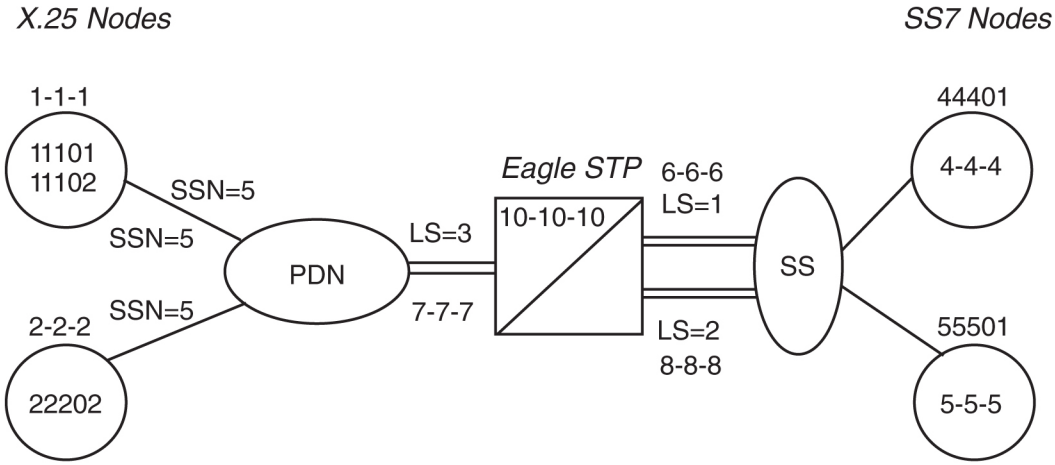
- Same-link management
- Logical channel to network management mapping

Connection Determination

The destination address for X.25 is defined as a destination element (X.25 DE). An X.25 DE is an object on the X.25 network to which a connection can be made and has a point code assigned to it. An X.25 link can be either point-to-point (direct) or through an intermediary network. A destination for SS7 is a point code, plus an optional subsystem number (SSN).

A destination for X.25 is dependent upon whether a connection is established . A *connection* is defined as a pair of destinations that are exchanging messages. The destination for X.25 is an X.25 address before connection, and a logical channel (LC) after connection. One of the destinations must be in the X.25 domain and the other in the SS7 domain. See **Figure 5-30** .

Figure 5-30. X.25 Gateway Connection Determination



The connection is determined using the gateway routing table. This process can be divided by whether the message arrives from the X.25 side (inbound) or the SS7/MTP side (outbound):

- Inbound messages:

  If the logical channel on which the message arrives is in the connected state, it already points to an entry in the gateway routing table. The destination point code (DPC) is the value in the SS7 point code field. The origination point code (OPC) is the value in the X.25 point code field.

  For an incoming SVC, the X.25 user must first establish the connection.

- Outbound messages:

  The DPC is used to locate the connection on which to send the message. The order of the lookup in the routing table is as follows:

  1. The STP locates an entry in the X.25 point code field that matches the DPC. If no entry is found for that point code, the gateway produces MRN #1140 and the MSU is discarded.

2. The STP verifies that the OPC matches the SS7 point code field. If there is no match, the gateway produces MRN #1134 and the MSU is discarded.

3. Once the connection entry is found in the gateway routing table, the STP examines the card address field and proceeds as follows:

If...	then...
the card address is the same as the card that receives the MSU,	the process is complete and the message passes to format conversion.
the card address is not the same card that receives the MSU,	the STP passes the MSU to “single link” management for the card defined in the card address field.

X.25 Connection Control

There is an additional routing requirement, connection routing and control, that is different from SS7 routing. The X.25 requires that a connection be present between the gateway and the X.25 DE before any messages can be exchanged. A connection is established depending upon when and where the connection is made.

A fixed connection route is defined through administration and can be either PVC (permanent virtual circuit), SVCA (switched virtual circuit-automatic) or SVCR (switched virtual circuit – remote). If the connection type field is PVC, the PVC is already established when the link is initialized through provisioning in the PDN and STP. The PVC remains in effect while the link is operational.

If the connection type field is SVCA, the connection is established by the designated LIM card (defined in the location field) immediately after the link becomes initialized. It is possible that the remote end becomes available during this cycle, and makes the connection from the remote end. The remote end could make the connection to any card. The connection remains in effect while the link is operational or until the remote end fails or clears the connection.

If the connection type field is SVCR, the connection can only be made by the X.25 DE as follows:

If an X.25 DE wants to send a message to an SS7 node, and the STP has not established a connection to that node, it attempts to establish one before sending the message. The X.25 DE establishes the connection by sending a call request to the STP with identification in the calling address field, and the SS7 node in the called address field.

When the STP receives the incoming call, the STP verifies both the calling and called addresses using the X.25 address and SS7 address fields. If the STP finds an entry for the X.25 address pair, it checks to see if a connection is active.

If...	then...
the connection is active,	the STP clears the incoming call.
the connection is not active,	it is set as active.
an entry for the X.25 address pair is not found,	the STP checks the X.25 Destination Table to see if the designated X.25 addresses are present.
both addresses are present (the caller is in the X.25 domain and the called address is in the SS7 domain),	the connection is established and a temporary entry is added to the database.

Same Link Management

X.25 requires that if there is a set of links into a PDN (or directly to an X.25 DE), a response to a request must be returned on the same link and logical channel as the request was received. Because MTP routing does not use a particular link on a linkset, it is likely that a response would go to a non-originating LIM. Same link management assures that the message is sent out on the same link. This is achieved by each LIM informing all other LIMs when the state of a connection changes.

Logical Channel to Network Management Mapping

The EAGLE X.25/SS7 gateway provides management procedures for failed X.25 logical channels. This feature allows traffic destined for failed logical channels to be rerouted to an alternate route.

When configuring logical channel to network management mapping (LC2NM), you must determine if the X.25 entity is expecting associated queries and responses to use the same logical channel or if they may be assigned to different logical channels. If associated queries and responses can be received over different logical channels, load balancing and failure recovery through alternate routing is supported.

Year 2000 Compliance (Release 23.1)

Overview

This feature ensures that there are no date-related problems with the EAGLE or created by the EAGLE on or after January 1, 2000. The date shown in all outputs from the EAGLE continue to be shown as two digits.

The EAGLE performs all date and time-of-day operations within the range of dates from January 1, 1995 to December 31, 2036. January 1, 1995 was chosen as the starting date for the range of dates because several EAGLE features implemented with Release 21.1 have it as the defined start date.

All EAGLE software has been modified to represent all dates unambiguously (that is, the year represented as 00 means the year 2000). The digits 95 through 99 represent the years 1995 through 1999. The digits 00 through 36 represent the years 2000 through 2036. For all software modifications in this feature, the date representations have been made to comply with the date formats shown in *Data Elements and Exchange Formats - Information Exchange - Representation of Dates and Time, ISO 8601, 1998*. The EAGLE software that is fully compliant with the requirements of the Year 2000 feature does not need to be modified to comply with *Data Elements and Exchange Formats - Information Exchange - Representation of Dates and Time, ISO 8601, 1998*.

Each year that is divisible by four is a leap year, with the exception of those years that end in “00,” such as 1900. The one exception is that years that are divisible by 400 are leap years, such as 1600 and 2000. The EAGLE recognizes the year 2000 as a leap year.

This section is divided into two parts:

- The first part, Year 2000 EAGLE Compliance shows how the Year 2000 feature applies to the EAGLE.
- The second part, OAP Year 2000 Compliance shows how it applies to the OAP.

Year 2000 EAGLE Compliance

This section lists the Year 2000 requirements, conditional requirements, and objectives that the EAGLE complies with as defined in the Bellcore document, *Year 2000 Generic Requirements: Systems and Interfaces, GR-2945-CORE, Issue 1, BELLCORE, December, 1996*.

The compliance matrix is a table listing the requirement number, objective number, or conditional requirement number as defined in the Bellcore document, the EAGLE's level of compliance with the requirement, objective, or conditional requirement, and any comments that may apply to these items.

A requirement is a feature or function of an STP that Bellcore has determined must be a part of the STP to function properly. A requirement is identified in this appendix with the letter R in parentheses, (R).

A conditional requirement is a feature or function of an STP that Bellcore has determined is necessary in certain applications, depending on how the STP is deployed. A conditional requirement may depend on other requirements, objectives, or conditional requirements. A conditional requirement is identified in this appendix with the letters CR in parentheses, (CR).

An objective is a feature or function of an STP that Bellcore has determined is a desirable feature or function for the STP to have, but not required to have. An objective is identified in this appendix with the letter O in parentheses, (O).

There are four levels of compliance used in this compliance matrix.

- Fully compliant
- Partially compliant
- Not compliant
- Not applicable

The table caption for each table refers to the section of the *Year 2000 Generic Requirements: Systems and Interfaces, GR-2945-CORE, Issue 1, BELLCORE, December, 1996* document where the item can be found.

Table 5-27. Section 2.1. Date-Sensitive Criteria – System Integrity

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 2-1	Fully Compliant	
(R) 2-2	Fully Compliant	The minimum range for the EAGLE is 1/1/95 - 12/31/36
(R) 2-3	Not Applicable	The EAGLE does not perform date conversions, computations, and comparisons using the Gregorian Calendar.
(R) 2-4	Fully Compliant	
(R) 2-5	Fully Compliant	
(R) 2-6	Fully Compliant	
(R) 2-7	Fully Compliant	

Table 5-28. Section 2.2. Date-Sensitive Criteria – Application Integrity

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 2-8	Fully Compliant	
(R) 2-9	Fully Compliant	
(R) 2-10	Fully Compliant	
(R) 2-11	Not Applicable	The EAGLE does not perform delayed execution.
(R) 2-12	Fully Compliant	
(R) 2-13	Fully Compliant	
(R) 2-14	Fully Compliant	
(R) 2-15	Fully Compliant	
(R) 2-16	Not Applicable	No hashing or random number generation is performed.
(R) 2-17	Fully Compliant	
(O) 2-18	Fully Compliant	
(R) 2-19	Fully Compliant	
(R) 2-20	Fully Compliant	

Table 5-29. Section 3. User Interface

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 3-1	Fully Compliant	
(R) 3-2	Fully Compliant	
(R) 3-3	Fully Compliant	
(R) 3-4	Fully Compliant	
(O) 3-5	Partially Compliant	When two digits are used, Year is displayed in unambiguous format, 95 - 99 represents the 20th century, 00 - 36 represents the 21st century.
(R) 3-6	Fully Compliant	
(R) 3-7	Fully Compliant	
(R) 3-8	Fully Compliant	

Table 5-30. Section 4. Machine-to-Machine Interface

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(O) 4-1	Not Applicable	The EAGLE will comply with this objective if an external communication system uses the ISO 8601 date format.
(O) 4-2	Not Applicable	The EAGLE will comply with this objective if an external communication system uses the ISO 8601 date format.
(R) 4-3	Not Applicable	See the "OAP Compliance Matrix" section .
(CR) 4-4	Fully Compliant	
(CR) 4-5	Fully Compliant	
(CR) 4-6	Fully Compliant	
(CR) 4-7	Fully Compliant	
(R) 4-8	Not Applicable	The EAGLE does not support BAF/MDR records.
(R) 4-9	Not Applicable	The EAGLE does not support BAF/MDR records.
(R) 4-10	Not Applicable	The EAGLE does not interact with an MSR system.
(R) 4-11	Not Applicable	The EAGLE does not generate MWI Control operations.
(R) 4-12	Not Applicable	The EAGLE does not perform ISDN PRI signaling
(R) 4-13	Not Applicable	The EAGLE does not interact with an MSR system.

Table 5-31. Section 5. Management Function Areas

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 5-1	Fully Compliant	
(R) 5-2	Not Applicable	See the "OAP Compliance Matrix" section .
(CR) 5-3	Fully Compliant	
(CR) 5-4	Fully Compliant	
(CR) 5-5	Not Applicable	The EAGLE does not perform delayed activation.
(CR) 5-6	Not Applicable	The EAGLE does not perform scheduled configuration data change.
(CR) 5-7	Not Applicable	The EAGLE does not perform reservation configuration data change.
(R) 5-8	Fully Compliant	
(R) 5-9	Fully Compliant	
(CR) 5-10	Not Applicable	The EAGLE does not perform delayed activation.
(R) 5-11	Fully Compliant	
(R) 5-12	Fully Compliant	

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(CR) 5-13	Not Applicable	The EAGLE does not support automatic backups.
(CR) 5-14	Not Applicable	The EAGLE does not support automatic backups.
(CR) 5-15	Not Applicable	The EAGLE does not support automatic backups.
(CR) 5-16	Not Applicable	The EAGLE does not support automatic backups.
(CR) 5-17	Fully Compliant	
(O) 5-18	Fully Compliant	
(CR) 5-19	Fully Compliant	
(CR) 5-20	Fully Compliant	
(CR) 5-21	Not Applicable	The EAGLE does not support automatic backups.
(CR) 5-22	Fully Compliant	
(CR) 5-23	Fully Compliant	
(CR) 5-24	Fully Compliant	
(CR) 5-25	Not Applicable	The EAGLE's database restore does not involve date sensitive data.
(CR) 5-26	Fully Compliant	
(CR) 5-27	Fully Compliant	
(R) 5-28	Fully Compliant	
(R) 5-29	Not Applicable	The EAGLE does not perform delayed activation.
(R) 5-30	Fully Compliant	
(R) 5-31	Fully Compliant	
(R) 5-32	Fully Compliant	
(R) 5-33	Not Applicable	The EAGLE does not perform delayed activation.
(CR) 5-34	Not Applicable	The EAGLE does not perform delayed activation.
(R) 5-35	Fully Compliant	
(R) 5-36	Fully Compliant	
(R) 5-37	Fully Compliant	
(R) 5-38	Fully Compliant	
(R) 5-39	Fully Compliant	
(R) 5-40	Fully Compliant	
(R) 5-41	Fully Compliant	
(R) 5-42	Fully Compliant	

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 5-43	Fully Compliant	
(R) 5-44	Fully Compliant	
(R) 5-45	Fully Compliant	
(R) 5-46	Fully Compliant	
(R) 5-47	Fully Compliant	
(R) 5-48	Fully Compliant	
(R) 5-49	Fully Compliant	
(R) 5-50	Not Applicable	The EAGLE does not allow a grace period.
(R) 5-51	Fully Compliant	
(R) 5-52	Fully Compliant	
(R) 5-53	Fully Compliant	
(R) 5-54	Fully Compliant	
(R) 5-55	Fully Compliant	
(R) 5-56	Fully Compliant	
(R) 5-57	Fully Compliant	
(R) 5-58	Fully Compliant	The EAGLE currently does not use cryptography algorithms.
(R) 5-59	Not Applicable	The EAGLE does not have any X.509 applications.
(R) 5-60	Not Applicable	The EAGLE does not have any X.509 applications.
(R) 5-61	Not Applicable	The EAGLE does not have any X.509 applications.
(R) 5-62	Not Applicable	The EAGLE does not have any X.509 applications.
(R) 5-63	Not Applicable	The EAGLE does not have any X.509 applications.
(R) 5-64	Not Applicable	The EAGLE does not have any X.509 applications.
(R) 5-65	Not Applicable	The EAGLE does not have any smart or token card function involving time.

Table 5-32. Section 6. Applications and Functions

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 6-1	Not Applicable	The EAGLE does not have any smart or token card services.
(CR) 6-2	Not Applicable	The EAGLE does not provide this function or application.
(R) 6-3	Not Applicable	The EAGLE does not provide this function or application.
(R) 6-4	Not Applicable	The EAGLE does not provide this function or application.

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 6-5	Not Applicable	The EAGLE does not provide this function or application.
(R) 6-6	Not Applicable	The EAGLE does not provide this function or application.
(R) 6-7	Not Applicable	The EAGLE does not provide this function or application.
(R) 6-8	Not Applicable	The EAGLE does not provide this function or application.
(R) 6-9	Not Applicable	The EAGLE does not provide this function or application.
(R) 6-10	Not Applicable	The EAGLE does not provide this function or application.
(R) 6-11	Not Applicable	The EAGLE does not provide this function or application.
(R) 6-12	Not Applicable	The EAGLE does not provide this function or application.
(R) 6-13	Not Applicable	The EAGLE does not provide this function or application.

Table 5-33. Section 7. Process-Oriented Criteria

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 7-1	Fully Compliant	
(R) 7-2	Fully Compliant	
(R) 7-3	Fully Compliant	
(R) 7-4	Fully Compliant	
(R) 7-5	Fully Compliant	
(R) 7-6	Fully Compliant	
(R) 7-7	Fully Compliant	
(R) 7-8	Fully Compliant	
(R) 7-9	Fully Compliant	
(R) 7-10	Fully Compliant	
(R) 7-11	Fully Compliant	
(R) 7-12	Partially Compliant	Tekelec’s Quality procedures are used.
(R) 7-13	Fully Compliant	
(R) 7-14	Fully Compliant	
(R) 7-15	Fully Compliant	
(R) 7-16	Fully Compliant	
(R) 7-17	Fully Compliant	
(R) 7-18	Fully Compliant	

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(CR) 7-19	Fully Compliant	
(R) 7-20	Fully Compliant	
(R) 7-21	Fully Compliant	
(R) 7-22	Fully Compliant	
(R) 7-23	Fully Compliant	
(R) 7-24	Fully Compliant	
(R) 7-25	Fully Compliant	
(R) 7-26	Fully Compliant	
(R) 7-27	Not Applicable	The EAGLE product uses maintenance releases for software fixes and not patches.
(R) 7-28	Fully Compliant	
(R) 7-29	Fully Compliant	

Table 5-34. Section 8. System Reliability and Quality Criteria

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 8-1	Not Applicable	The EAGLE will be fully compliant.
(O) 8-2	Not Applicable	The EAGLE will be fully compliant.
(R) 8-3	Not Applicable	The EAGLE will be fully compliant.
(R) 8-4	Not Applicable	The EAGLE will be fully compliant.
(O) 8-5	Not Applicable	The EAGLE will be fully compliant.
(R) 8-6	Not Applicable	The EAGLE will be fully compliant.
(R) 8-7	Fully Compliant	
(O) 8-8	Fully Compliant	The EAGLE conforms to all system reliability and quality criteria as documented by Reliability and Quality Statistics.
(R) 8-9	Fully Compliant	
(O) 8-10	Fully Compliant	The EAGLE conforms to all system reliability and quality criteria as documented by Reliability and Quality Statistics.
(R) 8-11	Fully Compliant	
(O) 8-12	Fully Compliant	The EAGLE conforms to all system reliability and quality criteria as documented by Reliability and Quality Statistics.
(R) 8-13	Fully Compliant	
(O) 8-14	Fully Compliant	The EAGLE conforms to all system reliability and quality criteria as documented by Reliability and Quality Statistics.

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 8-15	Fully Compliant	
(O) 8-16	Fully Compliant	
(R) 8-17	Fully Compliant	
(O) 8-18	Fully Compliant	The EAGLE conforms to all system reliability and quality criteria as documented by Reliability and Quality Statistics.
(R) 8-19	Fully Compliant	
(O) 8-20	Fully Compliant	The EAGLE conforms to all system reliability and quality criteria as documented by Reliability and Quality Statistics.
(R) 8-21	Fully Compliant	
(O) 8-22	Fully Compliant	The EAGLE conforms to all system reliability and quality criteria as documented by Reliability and Quality Statistics.
(R) 8-23	Fully Compliant	The EAGLE conforms to all system reliability and quality criteria as documented by Reliability and Quality Statistics.

OAP Year 2000 Compliance

This section lists the software changes that have been made to the OAP so that no date-related problems occur on the OAP on or after January 1, 2000.

All OAP component software has been modified to represent all dates unambiguously according to the date formats shown in *Data Elements and Exchange Formats - Information Exchange - Representation of Dates and Time, ISO 8601, 1998.* All dates that include years but do not currently provide explicit representation of the century have been modified to represent a date according to the calendar date format YYYYMMDD. Date and time information in SEAS traffic through the OAP to the EAGLE STP will not have its format modified in the data stream translation. This will ensure compliance with the SEAS 7.0 standard.

Each year that is divisible by four is a leap year, with the exception of those years that end in “00,” such as 1900. The one exception is that years that are divisible by 400 are leap years, such as 1600 and 2000. The OAP recognizes the year 2000 as a leap year.

There are three interfaces that cross the boundaries of the OAP to external entities. These are OAP to LSMS, OAP to EAGLE, and OAP to SEAS. In instances where a date must be received or transmitted across these boundaries with less than a four-digit year, the OAP components have been modified to accept or provide a date that is unambiguous. These modifications have been performed within the confines of SEAS 7.0 compatibility.

OAP Compliance Matrix

This section lists the Year 2000 requirements, conditional requirements, and objectives that the OAP and its components comply with as defined in the Bellcore document, *Year 2000 Generic Requirements: Systems and Interfaces, GR-2945-CORE, Issue 1, BELLCORE, December, 1996.* This section is divided into two parts. The first section details specific compliance requirement areas that pertain to one or more of the OAP components. The second section addresses requirements that pertain to the life cycle, quality, and reliability of the system as a whole.

The compliance matrix is a table listing the requirement number, objective number, or conditional requirement number as defined in the Bellcore document, the OAP's level of compliance with the requirement, objective, or conditional requirement, and any comments that may apply to these items.

A requirement is a feature or function of the OAP that Bellcore has determined must be a part of the OAP to function properly. A requirement is identified in this appendix with the letter R in parentheses, (R).

A conditional requirement is a feature or function of the OAP that Bellcore has determined is necessary in certain applications, depending on how the OAP is deployed. A conditional requirement may depend on other requirements, objectives, or conditional requirements. A conditional requirement is identified in this appendix with the letters CR in parentheses, (CR).

An objective is a feature or function of the OAP that Bellcore has determined is a desirable feature or function for the OAP to have, but not required to have. An objective is identified in this appendix with the letter O in parentheses, (O).

There are four levels of compliance used in this compliance matrix.

- Fully compliant
- Partially compliant
- Not compliant
- Not applicable

The table caption for each table refers to the section of the *Year 2000 Generic Requirements: Systems and Interfaces, GR-2945-CORE, Issue 1, BELLCORE, December, 1996* document where the item can be found.

Table 5-35. Section 2.1. Date-Sensitive Criteria – System Integrity

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 2-1	Not Applicable	No two-digit date representations or usage of **`tm_yr`**.
(R) 2-2	Fully Compliant	Date reporting is based on Solaris time functions, which use **`time_t`**. The Tekelec Installation Utilities and the NEBS alarm daemon do not apply to this requirement. All other OAP components comply with this requirement.
(R) 2-3	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 2-4	Fully Compliant	The Tekelec Installation Utilities and the Artecon Arteport kernel level device driver do not apply to this requirement. All other OAP components comply with this requirement.
(R) 2-5	Fully Compliant	
(R) 2-6	Fully Compliant	The Tekelec Installation Utilities do not apply to this requirement. All other OAP components comply with this requirement.

Table 5-36. Section 2.2. Date-Sensitive Criteria – Application Integrity

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 2-7	Fully Compliant	Date/time comparisons, where present, are based on **`time_t`** values. The Tekelec Installation Utilities and the Artecon Arteport kernel level device driver do not apply to this requirement. All other OAP components comply with this requirement.
(R) 2-8	Fully Compliant	The Tekelec Installation Utilities, the Artecon Arteport kernel level device driver, and the NEBS alarm daemon do not apply to this requirement. All other OAP components comply with this requirement.
(R) 2-9	Fully Compliant	Only the Tekelec EMS Agent, Tekelec UAL/X25/Disk status refresh and notification daemon, and the NEBS alarm daemon apply to this requirement and fully comply with this requirement. All other OAP components do not apply to this requirement.
(R) 2-10	Not Applicable	The Solaris operating system is responsible for any **`cron`** initiated processes.
(R) 2-11	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 2-12	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 2-13	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 2-14	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 2-15	Fully Compliant	All date and time stamps are based on Solaris time calls and contain four digits for the year. The Tekelec Installation Utilities, the Artecon Arteport kernel level device driver, and the NEBS alarm daemon do not apply to this requirement. All other OAP components comply with this requirement.
(R) 2-16	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 2-17	Not Applicable	Analysis of the source code has determined that all timers use Solaris **`time_t`** values.
(O) 2-18	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 2-19	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 2-20	Not Applicable	This requirement has been determined to be not applicable by analysis.

Table 5-37. Section 3. User Interface

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 3-1	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 3-2	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 3-3	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 3-4	Not Applicable	This requirement has been determined to be not applicable by analysis.

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(O) 3-5	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 3-6	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 3-7	Not Applicable	The Solaris system clock is used.
(R) 3-8	Not Applicable	The Solaris operating system does use **tm_yr** values.

Table 5-38. Section 4. Machine-to-Machine Interface

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(O) 4-1	Fully Compliant	The OAP will comply with this requirement if an external communications system uses the ISO 8601 format. Only the Tekelec EMS Agent, Tekelec RS232 Asynchronous Send/Receive daemon, and UAL logical channel over X.25 daemon components apply to this objective and fully comply with this objective. All other OAP components do not apply to this objective.
(O) 4-2	Fully Compliant	The OAP will comply with this requirement if an external communications system uses the ISO 8601 format. Only the Tekelec EMS Agent, Tekelec RS232 Asynchronous Send/Receive daemon, and UAL logical channel over X.25 daemon components apply to this objective and fully comply with this objective. All other OAP components do not apply to this objective.
(R) 4-3	Fully Compliant	ASN.1 (X.208) is used. Only the Tekelec EMS Agent applies to this requirement and fully complies with this requirement. All other OAP components do not apply to this requirement.
(CR) 4-4	Fully Compliant	For information that OAP stores and processes as date field information, SEAS protocol or ASN.1 (X.208) is used. Only the Tekelec EMS Agent, Tekelec RS232 Asynchronous Send/Receive daemon, and Bellcore UAL logical channel over X.25 daemon components apply to this conditional requirement and fully comply with this conditional requirement. All other OAP components do not apply to this conditional requirement.
(CR) 4-5	Fully Compliant	For information that OAP stores and processes as date field information, SEAS protocol or ASN.1 (X.208) is used. Only the Tekelec EMS Agent, Tekelec RS232 Asynchronous Send/Receive daemon, and Bellcore UAL logical channel over X.25 daemon components apply to this conditional requirement and fully comply with this conditional requirement. All other OAP components do not apply to this conditional requirement.
(CR) 4-6	Fully Compliant	For information that OAP stores and processes as date field information, SEAS protocol or ASN.1 (X.208) is used. Only the Tekelec EMS Agent, Tekelec RS232 Asynchronous Send/Receive daemon, and Bellcore UAL logical channel over X.25 daemon components apply to this conditional requirement and fully comply with this conditional requirement.

Bellcore Requirement	Level of Compliance	Comments/Exceptions
		All other OAP components do not apply to this conditional requirement.
(CR) 4-7	Fully Compliant	For information that OAP stores and processes as date field information, SEAS protocol or ASN.1 (X.208) is used. Only the Tekelec EMS Agent, Tekelec RS232 Asynchronous Send/Receive daemon, and Bellcore UAL logical channel over X.25 daemon components apply to this conditional requirement and fully comply with this conditional requirement. All other OAP components do not apply to this conditional requirement.
(R) 4-8	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 4-9	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 4-10	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 4-11	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 4-12	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 4-13	Not Applicable	This requirement has been determined to be not applicable by analysis.

Table 5-39. Section 5. Management Functional Areas

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 5-1	Not Applicable	This requirement only applies to the Solaris operating system.
(R) 5-2	Not Applicable	This requirement only applies to the Solaris license manager.
(CR) 5-3	Not Applicable	No configuration data reporting is provided that is dependent on the start-date/time for the collection determined by analysis.
(CR) 5-4	Not Applicable	This requirement has been determined to be not applicable by analysis.
(CR) 5-5	Not Applicable	This requirement has been determined to be not applicable by analysis.
(CR) 5-6	Not Applicable	The analysis of the source code determined that there is no configuration data change that is scheduled by date/time.
(CR) 5-7	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 5-8	Not Applicable	All dates reported are based on the Sparc 5 system clock.
(R) 5-9	Not Applicable	All dates reported are based on the Sparc 5 system clock.
(CR) 5-10	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(R) 5-11	Fully Compliant	Only the Tekelec EMS Agent and Bellcore UAL logical channel over X.25 daemon components apply to this requirement and fully comply with this requirement. All other OAP components do not apply to this requirement.
(R) 5-12	Fully Compliant	Only the Tekelec EMS Agent and Bellcore UAL logical channel over X.25 daemon components apply to this requirement and fully comply with this requirement. All other OAP components do not apply to this requirement.

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(CR) 5-13	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(CR) 5-14	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(CR) 5-15	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(CR) 5-16	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(CR) 5-17	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(O) 5-18	Not Applicable	This objective has been determined to be not applicable by analysis.
(CR) 5-19	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(CR) 5-20	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(CR) 5-21	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(CR) 5-22	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(CR) 5-23	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(CR) 5-24	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(CR) 5-25	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(R) 5-26	Fully Compliant	The system software download is performed as part of the installation process, which is manually initiated and is performed on demand. Only the Tekelec installation utility applies to this requirement and fully complies with this requirement. All other OAP components do not apply to this requirement.
(R) 5-27	Fully Compliant	Only the Tekelec installation utility applies to this requirement and fully complies with this requirement. All other OAP components do not apply to this requirement.
(R) 5-28	Fully Compliant	Per Tekelec upgrade procedure using trial/approved nondestructive upgrade procedures. Only the Tekelec installation utility applies to this requirement and fully complies with this requirement. All other OAP components do not apply to this requirement.
(R) 5-29	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 5-30	Not Applicable	Dependent on the Sparc 5 system clock and Solaris date/time functions.
(R) 5-31	Not Applicable	This requirement is for network traffic management.
(R) 5-32	Not Applicable	This requirement is for network traffic management.
(R) 5-33	Not Applicable	This requirement has been determined to be not applicable by analysis.
(CR) 5-34	Not Applicable	This conditional requirement has been determined to be not applicable by analysis.
(R) 5-35	Not Applicable	This requirement has been determined to be not applicable by analysis.

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 5-36	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 5-37	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 5-38	Not Applicable	This requirement only applies to the Solaris operating system.
(R) 5-39	Not Applicable	This requirement only applies to the Solaris operating system.
(R) 5-40	Not Applicable	Password aging is handled by the Solaris operating system.
(R) 5-41	Not Applicable	Notification of password expiration is handled by the Solaris operating system.
(R) 5-42	Not Applicable	Password updates are handled by the Solaris operating system.
(R) 5-43	Not Applicable	All process tracking is handled by the Solaris operating system.
(R) 5-44	Not Applicable	All process tracking is handled by the Solaris operating system.
(R) 5-45	Not Applicable	File creation dates are handled by the Solaris operating system.
(R) 5-46	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 5-47	Not Applicable	All time stamps are the results of Solaris calls and use four-digit dates for the year.
(R) 5-48	Not Applicable	This requirement applies to the Solaris operating system.
(R) 5-49	Not Applicable	This requirement applies to the Solaris operating system.
(R) 5-50	Not Applicable	This requirement applies to the Solaris operating system.
(R) 5-51	Fully Compliant	Only the Tekelec EAGLE REPT-UIM autonomous event report daemon and the NEBS alarm daemon components apply to this requirement and fully complies with this requirement. All other OAP components do not apply to this requirement. Also applies to the Solaris operating system.
(R) 5-52	Not Applicable	This requirement applies to the Solaris operating system.
(R) 5-53	Not Applicable	This requirement applies to the Solaris operating system.
(R) 5-54	Not Applicable	The Solaris operating system is responsible for this security authentication requirement.
(R) 5-55	Not Applicable	The Solaris operating system is responsible for this security authentication requirement.
(R) 5-56	Not Applicable	The Solaris operating system is responsible for this security authentication requirement.
(R) 5-57	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 5-58	Not Applicable	
(R) 5-59	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 5-60	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 5-61	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 5-62	Not Applicable	This requirement has been determined to be not applicable by analysis.

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 5-63	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 5-64	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 5-65	Not Applicable	This requirement has been determined to be not applicable by analysis.

Table 5-40. Section 6. Applications and Functions

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 6-1	Not Applicable	This requirement has been determined to be not applicable by analysis.
(CR) 6-2	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 6-3	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 6-4	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 6-5	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 6-6	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 6-7	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 6-8	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 6-9	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 6-10	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 6-11	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 6-12	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 6-13	Not Applicable	This requirement has been determined to be not applicable by analysis.

OAP System Compliance

The remaining two sections of GR-2945-CORE deal with Process-Oriented Criteria and System Reliability and Quality Criteria. Each of these requirements has been evaluated for applicability and compliance on system/ program level for the OAP.

Table 5-41. Section 7. Process-Oriented Criteria

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 7-1	Fully Compliant	
(R) 7-2	Fully Compliant	
(R) 7-3	Fully Compliant	
(R) 7-4	Fully Compliant	

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 7-5	Fully Compliant	
(R) 7-6	Fully Compliant	
(R) 7-7	Fully Compliant	
(R) 7-8	Fully Compliant	
(R) 7-9	Fully Compliant	
(R) 7-10	Fully Compliant	
(R) 7-11	Fully Compliant	
(R) 7-12	Partially Compliant	Tekelec's Quality Procedures are used.
(R) 7-13	Fully Compliant	
(R) 7-14	Fully Compliant	
(R) 7-15	Fully Compliant	
(R) 7-16	Fully Compliant	
(R) 7-17	Fully Compliant	
(R) 7-18	Fully Compliant	
(CR) 7-19	Fully Compliant	
(R) 7-20	Fully Compliant	
(R) 7-21	Fully Compliant	
(R) 7-22	Fully Compliant	
(R) 7-23	Fully Compliant	
(R) 7-24	Fully Compliant	
(R) 7-25	Fully Compliant	
(R) 7-26	Fully Compliant	
(R) 7-27	Fully Compliant	OAP updates are only performed by updates, not be patches
(R) 7-28	Fully Compliant	
(R) 7-29	Fully Compliant	

Table 5-42. Section 8. System Reliability and Quality Criteria

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 8-1	Fully Compliant	
(O) 8-2	Fully Compliant	

Bellcore Requirement	Level of Compliance	Comments/Exceptions
(R) 8-3	Fully Compliant	
(R) 8-4	Not Applicable	This requirement has been determined to be not applicable by analysis.
(O) 8-5	Not Applicable	This objective has been determined to be not applicable by analysis.
(R) 8-6	Not Applicable	This requirement has been determined to be not applicable by analysis.
(R) 8-7	Fully Compliant	
(O) 8-8	Fully Compliant	
(R) 8-9	Fully Compliant	
(O) 8-10	Fully Compliant	
(R) 8-11	Fully Compliant	
(O) 8-12	Fully Compliant	
(R) 8-13	Fully Compliant	
(O) 8-14	Fully Compliant	
(R) 8-15	Fully Compliant	
(O) 8-16	Fully Compliant	
(R) 8-17	Fully Compliant	
(O) 8-18	Fully Compliant	
(R) 8-19	Fully Compliant	
(O) 8-20	Fully Compliant	
(R) 8-21	Fully Compliant	
(O) 8-22	Fully Compliant	
(R) 8-23	Fully Compliant	

Glossary

A

A	Ampere
AAL5CP	ATM Adaptation Layer 5 Common Port
AATM	ATM Appliqué
ACG	Automatic Call Gapping
ACK	Data Acknowledgement
ACM	Address Complete Message
ACM	*Application Communications Module*
ACT	Activate
AERM	Alignment Error Rate Monitor
AFTPC	Affected Point Code
AIN	Advanced Intelligent Network
AINF	Application Interface Appliqué
AINPQ	ANSI-41 INP Query
Allowed DPC	The gateway screening entity that identifies the destination point codes that are allowed to receive SS7 messages from the EAGLE 5 ISS. Messages containing the specified destination point codes go on to the next step in the gateway screening process, or are allowed into the network if the gateway screening process stops with this entity.
Allowed OPC	The gateway screening entity that identifies the originating point codes that are allowed to send SS7 messages into the network. Messages containing the specified originating point codes go on to the next step in the gateway screening process, or are allowed into the network if the gateway screening process stops with this entity.
Allowed SIO	The gateway screening entity that identifies the type of MSUs (ISUP, TUP, TCAP, and so forth) that are allowed into the network. The message type is determined by the network indicator code (NIC), priority (PRI), and service indicator (SI) fields of the signaling information octet (SIO) field in the MSU, and the H0 and H1 heading codes of the signaling information field of the MSU. Messages containing the specified message type go on to the next step in the gateway screening process, or are allowed into the network if the gateway screening process stops with this entity.
Allowed TT	The gateway screening entity that identifies the SCCP messages that have a specified translation type value in the called party address. SCCP messages containing specified translation type in the called party address go on to the next step in the gateway screening process, or are allowed into the network if the gateway screening process stops with this entity.
ALM	Alarm Card
AMI	Alternate Mark Inversion
ANSI	American National Standards Institute
APC	Adjacent Point Code
APC	Application Processing Chassis
API	Application Interface

API	Application Programming Interface
APLI	ACSE Presentation Layer Interface
A-Port	ANSI-41 Mobile Number Portability
AS	Application Server
ASL8	Adjacent SLS 8-bit Indicator
ASM	Application Services Module
ASP	Application Server Process
ASP	Application Service Part
ASP	Abstract Service Primitive
Association	An association refers to an SCTP association. The association provides the transport for protocol data units and adaptation layer peer messages.
AST	Associated State The associated state of an entity.
ATH	Application Trouble Handler
ATI	Any Time Interrogation
ATM	Asynchronous Transfer Mode
ATMANSI	The application used for high-speed ANSI ATM signaling links.
ATM HSL	Asynchronous Transfer Mode High Speed Link
ATM HSL	ATM High Speed Link (a DS1 link in EAGLE)
ATMITU	The application used for high-speed E1 ATM signaling links.
ATMM	ATM Layer Management

B

BAF	Bellcore AMA Format
BCD	Binary Coded Decimal
BEI	Broadcast Exception Indicator
BIB	Backward Indicator Bit
BICC	Bearer Independent Call Control
BIP	Board Identification PROM
BITS	Building Integrated Timing System
BLKDPC	Blocked Destination Point Code
BLKOPC	Blocked Originating Point Code
BLM	Bulk Load Module
BPDCM	The communication software used in place of the IMT GPL on the Database Communications Module (DCM), Database Services Module (DSM), and General Purpose Services Module (GPSM-II).
BPHCAP	The communication software used in place of the IMT GPL on the LIMATM and E1 ATM.
BPHMUX	The communication software used on the High Speed Multiplexer (HMUX) card.
BSD	Berkeley Software Distribution
BSN	Backward Sequence Number

C

CAP	Communication & Application Processor

CAS	Channel Associated Signaling
CC	Connection Confirmed
CC	Country Code
CCS	Common Channel Signaling
CCS7ITU	The generic program load and application for the ITU SS7 signaling links that is used with card types **`limds0, limch, limocu, limv35, lime1, and limt1`**.
CD	Carrier Detect
CD	Compact Disk
CdPA	Called Party Address
CDU	CAP Downloadable Utility
CET	Customer Environment Test
CgPA	Calling Party Address
Changeback	A network management event that takes the traffic that was rerouted because of a changeover when a signaling link has failed and places that traffic back on that signaling link when that signaling link comes back into service.
Changeover	A network management event that routes traffic from a failed signaling link to another signaling link that can carry the traffic.
Channel	A single Time-Division-Multiplexed (TDM) timeslot within a channelized E1/T1 port. Generically, channels can be used for transporting signaling, digitized voice, or data information. Unused channels typically are filled with defined idle codes designed to maintain sufficient ones density to ensure frame-level synchronization.
Checksum	Provides protection against data corruption in the network. The sender of a packet computes a checksum according to an algorithm. The receiver then re-computes the checksum, using the same algorithm. The packet is accepted if the checksum is valid; otherwise, the packet is discarded.
CI	Clock Interface Card
CI	Critical Status Indicator
CIC	Carrier Identification Code
	A 4-digit code that controls the routing applied to a message.
CIC	Circuit Identification Code
CLASS	Custom Local Area Signaling Service
CLASS	Custom Local Area Subscriber Services
CLDR	SUA Connectionless Data Response
	A message used for carrying SS7 UDTS/XUDTS messages.
CLDT	SUA Connectionless Data Transfer
	A message used for carrying SS7 UDT/XUDT messages.
CLLI	Common Language Location Identifier
Cluster	A group of signaling points whose point codes have identical values for the network and cluster fields of the point codes. A cluster entry in the routing table is shown as an asterisk (*) in the member field of the point code, for example, 111-011-*. Cluster entries can be provisioned only as ANSI destination point codes.
CM	Cluster Management
CMIP	Common Management Information Protocol
CNAM	Calling Name Delivery Service
CNCF	Calling Name Conversion Facility

CNIP	Calling Name Identification Presentation
Coherency	The operational status of the database. Coherency is an indication of whether the update to the database was successful. Each database has a coherency indicator. When an update is attempted, the coherency indicator is set to "incoherent" before the actual update is executed. When the update has been successfully completed, the coherency indicator is changed to coherent. If the update is not successful, the coherency indicator is not changed. If the coherency indicator is incoherent, this could be an indication of possible internal coherency problems when a restart is executed (for example, an index table was updated, but the corresponding data storage table was not modified).
Command Class	A set of commands that are assigned to a user or to a terminal port. Command classes are assigned to a user with the **chg-user** or **ent-user** commands to control the commands that user can execute. Command classes are assigned to a terminal port with the **chg-secu-trm** command to control the commands that can be executed on a particular terminal.
Control Shelf	The shelf in the EAGLE 5 ISS that contains the Maintenance and Administration Subsystem. The Maintenance and Administration Subsystem contains 5 cards: 2 CAM cards, 2 TDMs (Terminal Disk Modules), and 1 MDAL (Maintenance Disk and Alarm) card. This shelf is designated as Shelf 1100 and cannot be added or removed from the database.
COO	Changeover Order
CPC	Capability Point Code
CPU	Central Processing Unit
CR	Cluster Routing
CR	Connection Request
CRC	CAM Redundancy Controller
CRC	Cyclic Redundancy Check
CRMD	Cluster Routing and Management Diversity A feature in the EAGLE 5 ISS that allows MSUs to be routed to a cluster of point codes and enhances the management of the SS7 traffic to the cluster of point codes.
CSL	Common Screening List
CSPC	Concerned Signaling Point Code
CSR	Customer Service Request
CSU	Channel Service Unit
CU	Currently Unused

D

daemon	A process that runs in the background and performs a specified operation at predefined times or in response to certain events.
Database	All data that can be administered by the user, including cards, destination point codes, gateway screening tables, global title translation tables, links, LNP services, LNP service providers, location routing numbers, routes, shelves, subsystem applications, and 10 digit telephone numbers.
DB	Database
DB	Daughter Board
DB	Documentation Bulletin
DBCD	Database Change and Display
DC	Direct Current

DCE	Data Communication Equipment
	The data communication equipment associated with the transmission of data from one device to another. Examples of data communication equipment are modems, remote terminals, and communications processors.
DCM	Database Communication Module
	The DCM provides IP connectivity for applications. Connection to a host is achieved through an ethernet LAN using the TCP/IP protocol.
DEFCC	Default Country Code
DESTFLD	The point code in the affected destination field (the concerned signaling point code) of incoming MTP network management messages from another network that are allowed into the EAGLE 5 ISS.
Destination	The node to which the signaling link traffic is routed. This destination is identified by a point code, either a full point code or a cluster point code.
DIMM	Dual Inline Memory Module
DIP	Dual In-Line Package
	Used more to refer to a type of switch. A DIP switch is a series of tiny switches whose housing has the same shape as a chip.
DIP	Dual Inline Package
DLK	Data Link
	TCP/IP Data Link
DLT	Delete
DMS	Disk Management System
DN	Directory number
	A DN can refer to any mobile or wireline subscriber number, and can include MSISDN, MDN, MIN, or the wireline Dialed Number.
DPC	Destination Point Code
	The point code of the signaling point to which the MSU is routed. This point code can be adjacent to the EAGLE 5 ISS, but does not have to be.
DPCA	Destination Point Code ANSI
DPCI	Destination Point Code International
DPCN	Destination Point Code National
DRA	Destination Routing Address
DRAM	Dynamic Random Access Memory
	A type of memory chip that has to be refreshed periodically.
DS	Differentiated Service
DS0	Digital Signal Level-0 (64 Kbits/sec or 56 Kbits/sec)
	A basic digital signaling rate of 64 Kbits/sec, corresponding to the capacity of one voice-frequency-equivalent channel.
DS0A	Digital Signal Level - 0
DSM	Database Service Module.
DSCP	Differentiated Service Code Point
DSCS	Digital Signal Customer Service
DSO	Fault sectionalization tests, a series of far-end loopback tests to identify faulty segments of an SS7 transmission path up to and including the remote network element.
DSU	Data Service Unit

DTA	Database Transport Access A feature in the EAGLE 5 ISS that encapsulates specific MSUs into the data portion of SCCP within a new SS7 MSU and sends the new MSU to the destination using global title translation. The EAGLE 5 ISS uses gateway screening to determine which MSUs are used by the DTA feature.
DTE	Data Terminal Equipment The equipment associated with the entering and retrieving data from a computer system or a data communications system. A video display terminal is an example of data terminal equipment.

E

E1	The European equivalent of T1 that transmits digital data over a telephone network at 2.048 Mbps.
E5-E1T1	EPM-based E1/T1 Multi-Channel Interface Module An EPM-based card that provides E1 and T1 connectivity. The E5 indicates the card is for existing EAGLE 5 control and extension shelves. E1T1 is an abbreviation for the ITU E1 and ANSI T1 interfaces. Thus the nomenclature defines the shelves where the card can be used and the physical interface that it provides.
E5-ENET	EPM-based Ethernet card A high capacity single-slot IP signaling card (EPM card plus Gig Ethernet PMC cards).
E5IS	EAGLE 5 Integrated Monitoring Support The EAGLE 5 Integrated Monitoring Support feature allows the network traffic on the EAGLE 5 ISS's signaling links to be monitored by an ESP (extended services platform) or IMP (integrated message feeder) without additional intrusive cabling. Message Signaling Units (MSUs), alarms, and events are copied to the Sentinel/IMF to provide the network traffic monitoring. The monitored traffic is delivered to the Sentinel/IMF using the EAGLE'S STCs (Signaling Transport Cards) which are connected to the ESP/IMF subsystem by Ethernet links. The ESP/IMF subsystem delivers the monitored traffic to the Sentinel/IMF.
EBDA	Enhanced Bulk Download and Audit
EBDABLM	The application used by the TSM or DSM to store the LNP database downloaded from the LSMS for the Enhanced Bulk Download function. This GPL does not support 24-bit ITU-N point codes.
EBDADCM	The application used by the DCM to transmit the LSMS LNP database at high speed over an Ethernet connection for the Enhanced Bulk Download function. This GPL does not support 24-bit ITU-N point codes.
EBI	Extended Bus Interface
ECAM	Enhanced Clock, Alarm, and Maintenance card
EDCM	Enhanced DCM
EDCM	Enhanced Database Communication Module
EDR	Efficient Data Representation
EDR	Enhanced Data Representation
EGMS	Enhanced GSM MAP Screening
EGTT	Enhanced Global Title Translation
EILA	Enhanced Integrated LIM Appliqué
EIR	Equipment Identity Register
ELAP	EAGLE LNP Application Processor

ELEI	Exception List Exclusion Indicator
ELF	EAGLE Load Format
EMDC	Element Measurement and Data Collection Application
	This application is used by the DCM card for CMIP/OSI measurement collection interface as defined by Telcordia GR-376.
EMS	Element Management System
	A system used to provide a top level management view of the network elements.
EMSALM	Element Management System Alarm Monitor
EO	End Office
EOAM	Enhanced Operation, Administration, and Maintenance
	The application used by the GPSM-II card for enhanced OAM functions.
EOAP	Embedded Operation Support System Applications Processor
	Also, Enhanced OSS Application Process.
EOT	End of Table
EPAP	EAGLE Provisioning Application Processor
EPM	Embedded Platform Module
	A single-slot card that is similar to the high-capacity blade except that it uses a lower-power CPU and thus does not require external fan trays or extra power.
EROUTE	The application used on the Sentinel Transport Card (STC) for the EAGLE 5 ISS with Integrated Sentinel feature. The Sentinel product does not support 24-bit ITU-N point codes.
ESD	Electro-Static Discharge
ESP	Expanded Services Platform
ETSI	European Technical Standards Institute

F

FAK	Feature Access Key.
FAN	Command for cooling fan feature. The EAGLE 5 ISS will report on the alarm conditions of the fan assemblies. Once you have turned on the feature, you cannot turn it off. The feature applies to any and all fans installed within the system. When replacing a fan assembly, the feature should already be turned on.
FC	Fully Compliant
FCI	Forward Call Indicator
FE	Feature Engineer
FIB	Forward Indicator Bit
FISU	Fill-In Signal Unit
FISU	Fill In Signal Unit.
FPC	*Full Point Code.*
FPGA	Field-Programmable Gate Array
FSM	Finite State Machine
FTA	File Transfer Area.
FTP	Feature Test Plan
FTP	File Transfer Protocol.
FTRA	FTP-based Table Retrieve Application

An application that runs in a PC outside of the EAGLE 5 ISS and that communicates with the EAGLE 5 ISS through the IPUI feature and the FTP Retrieve and Replace feature.

G

GA	General Availability
GAP	Generic Address Parameter
GB	Gigabyte — 1,073,741,824 bytes
G-Flex	GSM Flexible numbering A feature that allows the operator to flexibly assign individual subscribers to HLRs and route signaling messages, based on subscriber numbering, accordingly.
GLS	Generic Loading Services An application that is used by the TSM cards for downloading gateway screening to LIM cards.
GMT	Greenwich Mean Time
GN	Generic Name
GPF	General Purpose Frame
GPL	Generic Program Load
G-Port	GSM Mobile Number Portability A feature that provides mobile subscribers the ability to change the GSM subscription network within a portability cluster, while retaining their original MSISDN(s).
GPSM	General Purpose Service Module
GPSM-II	General Purpose Service Module
GSM	Global System for Mobile Communications
GSMSCRN	GSM MAP Screening. A feature that allows the user to provision which MAP subsystem numbers are affected, which MAP operations codes to screen, which origination points are allowed, and which error messages to use.
GT	Global Title Routing Indicator
GTA	Global Title Address
GTI	Global Title Translation Indicator
GTT	Global Title Translation.
GUI	Graphical User Interface
GWS	Gateway Screening.
GWSA	Gateway Screening Action
GWSA	Gateway Screening Application
GWSD	Gateway Screening Message Discard
GWSM	Gateway Screening Messages
GWSM	Gateway Screening Mode
GX25	X.25 Gateway A software feature that allows the system to send and receive traffic to and from an X.25 network, and convert the packet to a Signaling System #7 Message Signaling Unit (SS7 MSU).

H

HCAP	High-Speed Communications & Applications Processor
HC-MIM	High Capacity Multi-Channel Interface Module
HDB3	High Density Bipolar 3 Encoding
HIPR	High-Speed IMT Packet Router
HLR	Home Location Register
HMI	Human-to-Machine Interface
HMUX	High-Speed Multiplexer
HS	High Speed
HSL	High-Speed Links
HSOP	High Speed Operation Protocol
HW	Hardware

I

IAM	Initial Address Message
IC	Integrated Circuit
ICMP	Internet Control Message Protocol
ID	Identity
ID	Identity, identifier
IDP	Initial detection point
IEC	Inter-Exchange Carrier
IEC	International escape code
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGM	IS41 GSM Migration
IGTTLS	Intermediate Global Title Translation Load Sharing
ILA	Integrated LIM Appliqué
IMEI	International Mobile Equipment Identifier
IMF	Integrated Message Feeder
	A data acquisition system similar to Sentinel.
IMSI	International Mobile Station Identifier
IMT	Inter-Module-Transport
	The communication software that operates the inter-module-transport bus on all cards except the LIMATM, DCM, DSM, and HMUX.
IMTA	Internal Message Transport Address
IMT Bus	Interprocessor Message Transport Bus
IN	Intelligent Network
INAP	Intelligent Network Application Protocol
INH	Inhibit
INP	INAP-based Number Portability
INP	Intelligent Network (IN) Portability
INP	INAP-based Number Portability
INPQ	INAP Number Portability Query Processing Subsystem
IP	Intelligent Peripheral

IP	Internet Protocol
IP^7	Tekelec's Internet Protocol to SS7 Interface
IP Address	The location of a device on a TCP/IP network. The IP Address is a number in dotted decimal notation which looks something like [192.168.1.1].
IPC	Internal Point Code
IPGWAPC	IP Secure Gateway Adjacent Point Code
IPGWI	An application that is used by the DCM/SSEDCM card for IP point-to-multipoint connectivity within an ITU-I or ITU-N network. The system allows a maximum of 64 cards to be assigned the IPGWI application.
IPGWx	Point-to-multipoint MTP-User signaling (e.g. ISUP, TCAP) over IP capability. Typically used for A link connectivity which require routing keys. Far End not required to support MTP3. The IPGWx GPL (IPGWI, SS7IPGW) run on the DCM/SSEDCM hardware.
IPGWx IP TPS	In addition to the IPGWx system IP TPS, there is a configurable per-linkset IP TPS, which must sum across all linksets to no more than the IPGWx system IP TPS.
IPLIM	The application used by the DCM/SSEDCM card for IP point-to-point connectivity for ANSI point codes.
IPLIMx	Point-to-point MTP3 and MTP3-User signaling over IP capability. Typically used for B-C-D links but can be used for A links but does not have routing key functionality. Far End required to support MTP3. The IPLIMx GPL (IPLIMI, IPLIM) run on the DCM/SSEDCM hardware.
IPMX	IMT Power and Multiplexer card
IPNE	Internet Protocol Network Element
IPS	Internet Protocol Services
IPSM	IP Services Module
	A card that provides an IP connection for Telnet and FTP-based Table Retrieve applications. The IPSM is a GPSM-II card with a one Gigabyte (UD1G) expansion memory board in a single-slot assembly running the IPS application.
IPSP	IP Server Process
IPSP	IP Server Process
	A process instance of an IP-based application. An IPSP is essentially the same as an ASP, except that it uses MU3A in a peer-to-peer fashion. Conceptually, an IPSP does not use the services of a signaling gateway.
IS-41	Interim Standard 41, same as and interchangeable with ANSI-41.
IS-ANR	In Service - Abnormal
	The entity is in service but only able to perform a limited subset of its normal service functions.
ISCC	Integrated Serial Communications Controller
ISDN	Integrated Services Digital Network
IS-NR	In Service - Normal
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ISS	Integrated Signaling System
ISUP	ISDN User Part
ITU	International Telecommunications Union
ITUDUPPC	ITU National Duplicate Point Code

	This feature applies only to 14-bit ITU national point codes. This feature allows an EAGLE 5 ISS mated pair to route traffic for two or more countries that may have overlapping point code values.

K

Key	For the ICNP feature, a unique DS value used to access a table entry, consisting of a number length and number type.
KHz	Kilo Hertz (1000 Hertz)
KSR	Keyboard Send/Receive Mode

L

LAN	Local Area Network See also STP LAN.
LATA	Local Access Transport Area
LB	Load Balancing
LBP	Far-End Loop Back Point
LBP	Loopback Point The point on the signaling link at which each loopback test ends is called the far-end loopback point. A far-end loopback point (LBP) is achieved when the remote link element (RLE) sends the received data back to the transmitter, allowing the transmitter to verify the received data.
LC	Logical Channel
LC2NM	Logical Channel to Network Management
LCA	Logic Cell Array
LED	Light Emitting Diode
LFS	Link Fault Sectionalization
LI	Length Indicator
LIDB	Line Information Database
LIM	Link Interface Module
LIM-AINF	A link interface module (LIM) with the AINF interface.
LIM-ATM	A link interface module (LIM) with the ATM interface.
LIM-DS0	A link interface module (LIM) with the DS0A Appliqué.
LIM-E1	A link interface module (LIM) with the E1 Appliqué.
LIM-OCU	A link interface module (LIM) with the OCU Appliqué.
LIM-OCU	LIM-Office Channel Unit Applique
Link	Signaling Link
LLT	Latching LFS Test
LNP	Local Number Portability
LNPMR	LNP Message Relay
LNPQS	LNP Query Service
LNP SMS	LNP Short Message Service
Load Sharing	A type of routing used by global title translation to route MSUs This type of routing is used when a second point code and subsystem is defined for the primary point code and subsystem. Traffic is shared equally between the replicated point codes and subsystems.

LOCREQ	Location Request Message
LRN	Location Routing Number
	A 10 digit number identifying the new location of the ported 10 digit telephone number.
LS	Link Set
LSB	Least Significant Bit
LSL	Low-speed Link
LSMS	Local Service Management System
LSN	Link Set Name
LSS	Local Subsystem
LUDT	Long User Data
LUDTS	Long User Data Services

M

M256	256 Megabyte Memory Expansion Card
M2PA	SS7 MTP2-User Peer-to-Peer Adaptation Layer
M3UA	SS7 MTP3-User Adaptation Layer
MAAL	Management ATM Application Layer
MAC	Media Access Control
MAN	Metropolitan Area Network
MAP	Mated Application Part
MAP	Mobile Application Part
MAS	Maintenance and Administration Subsystem
	A set of cards located in the Control Shelf, used to provide a central management point for the EAGLE 5 ISS. The MAS provides user interface, maintenance communication, peripheral services, alarm processing, system disk interface, and measurements using the following three subassemblies: GPSM-II, TDM, and MDAL.
MASP	Maintenance and Administration Subsystem Processor
MAU	Media Access Unit
MBUS	Maintenance Bus
MB	Megabyte — A unit of computer information storage capacity equal to 1,048, 576 bytes.
MCAP	Maintenance Communications & Applications Processor
MCP	Measurement Collection Processor
	This application is used by the MCPM card for the Measurements Platform feature.
MCPM	Measurement Collection and Polling Module
MDAL	Maintenance Disk and Alarm Card
MDN	Mobile Dialed Number
MDN	Mobile Directory Number
MEA	Memory Extension Applique
MEA	Mismatch of Equipment and Attributes
MEAS	Measurements
MGC	Media Gateway Controller
MGTT	Modified Global Title Translation
MHz	Megahertz

MIB	Management Information Database
MIM	Multi-Channel Interface Module
MIN	Mobile Identification Number
MMI	Man-Machine Interface
MNP	Mobile Number Portability
MO	Magneto Optical
MO	Managed Object
MO	Mobile Originated
MPC	Mate Point Code
	Multiple Point Code
MPL	Multi-port LIM
MPS	Multi-Purpose Server
MR	Message Relay
MRC	MAS Redundancy Controller
MRC	Message Routing under Congestion
MRG	Message Relay Group
MRGT	Message Relay Global Title Translation
MRN	Message Reference Number
	Mated Relay Node
MRN Group	The MRN entities in an entity set that are used for traffic distribution.
MRN Set	A group of entities in the MRN table that are used to distribute final GTT traffic.
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	Mobile Station International Subscriber Directory Number
	The MSISDN is the number dialed by someone trying to reach the subscriber.
MSRN	Mobile Station Roaming Number
MSS	Maximum Segment Size
MSU	Message Signaling Unit
MTP	Message Transfer Part
MTP	Module Test Plan
MTP2	Message Transfer Part, Level 2
MTT	Mapped SS7 Message Translation Type
MTT	Message Text Table
MTU	Maximum Transmission Unit

N

NA	North America
NAI	Nature of Address Indicator
NAIV	NAI Value
NANC	North American Numbering Council
NANP	North American Numbering Plan
NC	Network Cluster
NC	Network Code

NCAI	Nested Cluster Allowed Indicator
NCM	Network Cluster Member
NCR	Nested Cluster Routing A feature that allows the system to support full point code entries on different routes within a cluster.
NDC	Network destination code
NDC	Network Data Collection
NE	Network Element
NE	North East
NEBS	Network Equipment Building Systems
NEC	National Escape Code
NEI	Network Element Interface
NGT	New Global Title
NI	Network Indicator
NIC	Network Identifier Code
NIC	Network Information Center
NLT	Nonlatching LFS Test
NM	Network Management
NMS	Network Management System
NP	Number Plan
NP	Numbering Plan
NP	Number Portability
NPA	Number Plan Area.
NPAC	Number Portability Administration Center
NPANXX	The area code and office prefix of a telephone number. For example, with the telephone number 919-555-1212, the digits 919 are the area code (NPA) and the digits 555 are the office prefix (NXX).
NPDB	Number Portability Database
NPREQ	Number Portability Request Query
NPV	Numbering Plan Value
NSR	Next Screening Reference

O

OAM	Operations, Administration, and Maintenance
OAP	The application running on the OAP used for the SEAS and LNP features. The LNP feature can be enabled only for a quantity of 2 to 12 million numbers. This GPL does not support 24-bit ITU-N point codes. See also Operations Support System Application Processor.
OAPF	Operations System Support / Applications Processor Frame
OCU	Office Channel Unit
OOS-MT	Out of Service - Maintenance
OPC	Originating Point Code
OS	Operating System
OS	Operations Systems

OSI	Open System Interconnection

P

PC	Point Code.
PCB	Printed Circuit Board
PCR	Preventive Cyclic Retransmission
PCS	Personal Communications Service (North American GSM)
PCS	Personal Communication Service
PDB	Provisioning Database
PDBA	Provisioning Database Application
PDBI	Provisioning Database Interface
PDN	Packet Data Network
PDN	Public Data Network
PDS	Persistent Device States
PDU	Protocol Data Unit
PIP	Party Information Parameter
PLNP	The Personal Communications Service (PCS) 1900 LNP Query (PLNP) feature provides for LNP query/response in a PCS wireless environment using the LRN method to support Service Provider Number Portability.
PLNPQS	LNPQS support provided for PLNP.
PPC	Private Point Code.
PPSMS	Prepaid Short Message Service
PPSMS	Prepaid Short Message Service Intercept
PRI	Primary Rate Interface
PRI	Priority
PRI	Primary Rate ISDN
PROM	Programmable Read Only Memory
PST	Primary State
PSTN	Public Switched Telephone Network.
PT	Portability Type
PVC	Permanent Virtual Circuit
PVC	Permanent Virtual Connection
PVC	Permanent Virtual Circuit
PVGTT	Padded Variable Global Title Translation

Q

QAF	Q Adapter Function

R

RADB	Remote Agent Database
RAM	Random Access Memory A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes.

RC	Relative Cost
RC	Restriction Criteria
RCx	A Signaling-Route-Set-Test for either a prohibited or restricted cluster network management message.
RD	Receive Data
RD	Removable Disk
Restricted	The network management state of a route, link set, or signaling link that is not operating properly and cannot carry all of its traffic. This condition only allows the highest priority messages to sent to the database entity first, and if space allows, followed by the other traffic. Traffic that cannot be sent on the restricted database entity must be rerouted or the traffic is discarded.
RFC	Request for Comment
RI	Routing Indicator
RJ	Registered Jack
RLE	Remote Link Element.
RN	Routing Number
ROM	Read Only Memory
Route	A path to another signaling point.
Routing Key	A set of SS7 parameter and parameter values that uniquely define the range of signaling traffic to be handled by a particular Application Server. For example, where all traffic directed to an SS7 DPC, OPC and ISUP CIC_range(s) or SCCP SSN is to be sent to a particular Application Server, that SS7 data defines the associated Routing Key.
RS	Requirement Specification
RSM	Remote Switching Module
RSR	Reset Request
RST	Route Set Test
RTDB	DSM Real-time database
RTE	Route
RTO	Retransmission Timeout
RTT	Ready to Test
RTT	Round Trip Time
RTT	Round Trip Time

S

SAAL	Signaling ATM Adaptation Layer
SAS	Storage Access Services
SBR	Subsystem Backup Routing
SCCP	Signaling Connection Control Part
SCCS	Switching Control Center System
SCM	System Configuration Manager
	System Configuration Matrix.
SCP	Service Control Point.
SCRC	SCCP Routing Control

Screen Set	A gateway screening table containing a list of rules, or screening references. The screening references indicate the screening action that is to be performed on a message in a specific linkset.
SCRN	Screen Set Name
SCSI	Small Computer System Interface
SCTP	Stream Control Transmission Protocol
SE-HSL	Synchronous E1 High Speed Link
SEAC	Signaling Engineering and Administration Center
SEAS	Signaling Engineering and Administration System 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.
Security Log	The security log is a circular file, located on each MASP, containing a record of each command entered on a EAGLE 5 ISS terminal, the name (user ID) of the person entering the command, the date and time the command was entered, and the terminal port that the command was entered on. This record can investigate unauthorized activities that may take place on the EAGLE 5 ISS, or when problems occur, this record can examine the commands that were entered before the problem occurred to check if one or more of those commands caused the problem.
SF	Super Frame
SIF	Service Information Field
SG	Secure Gateway
SI	Service Indicator
SIGTRAN	The name given to an IETF working group that produced specifications for a family of protocols that provide reliable datagram service and user layer adaptations for SS7 and ISDN communications protocols. The most significant protocol defined by the SIGTRAN group was the Stream Control Transmission Protocol (SCTP), which is used to carry PSTN signalling over IP. The SIGTRAN group was significantly influenced by telecommunications engineers intent on using the new protocols for adapting VoIP networks to the PSTN with special regard to signaling applications. Recently, SCTP is finding applications beyond its original purpose wherever reliable datagram service is desired.
SIH	System Information Handlers
SIO	Service Information Octet
SIO	Service Information Octet.
SIPO	Status Indicator - Processor Outage
SK	South Korea
SLAN	STP LAN
SLAN	Signaling Transfer Point Local Area Network.
SLC	Signaling Link Code
SLS	Signaling Link Selector
SLSCI	SLS Conversion Indicator
SLTA	Signaling Link Test Acknowledgment
SLTC	Signaling Link Test Controller
SM	Short Message
SMPP	Short Message Peer to Peer

SMS	Short Message Service
SMSC	Short Message Service Center
SMSREQ	SMS Request Message
SNAI	Service Nature of Address Indicator
SNM	Signaling Network Management.
SNMP	Simple Network Management Protocol.
SNR	Subsystem Normal Routing
SOA	Service Order Administration
SOG	Subsystem Out-of-Service Grant
SOR	Support of Optimal Routing
SOR	System Out of Service Request
SP	Service Provider
SP	Signaling Point
SPC	Secondary Point Code
	Spare Point Code
SPC	Signaling Point Code
SPC	Stored Program Control
SPID	Service Provider ID
Split NPA	Split Number Planning Area
	A process that forces two different NPANXXs to reference the same last 4 digits of a 10 digit ported telephone number in the database. When either NPANXX is updated, the 10 digit ported telephone numbers in each NPANXX with the same last 4 digits are updated. When the NPANXX is split, all existing NPANXX data for the NPANXX being split is copied to the new NPANXX.
SRAM	Static Random Access Memory
SRI	Send Routing Information
SRI	Send_Route_Information Message
SRM	Subsystem Routing Messages
SRT	Subsystem Routing Status Test
SS	Subsystem
SS7	Signaling System #7
SS7ANSI	SS7 ANSI
	An application used by the LIM cards and the E1/T1 MIM card for the MTP functionality.
SS7GX25	X.25/SS7 Gateway
	An application used by the LIM cards for the X.25/SS7 gateway feature. This GPL does not support 24-bit ITU-N point codes.
SS7IPGW	SS7 IP Gateway
	An application used by the DCM/SSEDCM card for IP point-to-multipoint capability within an ANSI network.
SSCF	Service Specific Coordination Function.
SSCOP	Service Specific Connection Oriented Protocol.
SSEDCM	Single Slot Enhanced Data Communications Module
SSH	Secure Shell
SSN	Subsystem Number

SSN	SS7 Subsystem Number
SSP	Subsystem Prohibited network management message.
	Subsystem Prohibited SCCP (SCMG) management message. (CER) Service Switching Point (SS7 Network)
SST	Secondary State
	Subsystem Status Test network management message. Subsystem Status Test SCCP (SCMG) management message. (CER)
SST	Subsystem Status Test
STC	Sentinel Transport Card
STC	Signaling Transport Card.
STH	System Trouble Handler
STP	Signal Transfer Point.
STP LAN	A feature in the EAGLE 5 ISS that copies MSUs selected through the gateway screening process and sends these MSUs over the Ethernet to an external host computer for further processing.
STPLAN	Signaling Transfer Point Local Area Network
	The generic program load and application used by the ACM card to support the STP LAN application. This GPL does not support 24-bit ITU-N point codes.
SUA	SS7 SCCP-User Adaptation Layer
SUA	SCCP User Adaptation Layer
SUERM	Signal Unit Error Rate Monitor
SVC	Switched Virtual Circuit
	A temporary virtual circuit that is set up and used only as long as data is being transmitted. Once the communication between the two hosts is complete, the SVC disappears. In contrast, a permanent virtual circuit (PVC) remains available at all times.
SVCA	Automatic Switched Virtual Circuit
SVCR	Remote Switched Virtual Circuit
SW	Software
SW	South West

T

T1	Transmission Level 1
	A T1 interface terminates or distributes T1 facility signals for the purpose of processing the SS7 signaling links carried by the E1 carrier. A leased-line connection capable of carrying data at 1,544,000 bits-per-second.
TALI	Transport Adapter Layer Interface (RFC 3094)
TBGTTLS	Transaction-based GTT Loadsharing
TCA	Transfer Cluster Allowed
TCAP	Transaction Capabilities Application Part
TCP	Transfer-Cluster-Prohibited
TCP	Transfer Control Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TCR	Transfer Cluster Restricted

TCU	Table Creation Utility
TDM	Terminal Disk Module.
TDMA	Time Division Multiple Access
TFR	Transfer Restricted
TLNP	Triggerless LNP
TN	Telephone Number
	A 10 digit ported telephone number.
TOCA	Timing Output Composite Automatic
TOS	Type of Service
TPC	True Point Code
TPD	Tekelec Platform Development
TPS	Transactions Per Second
Transaction-based GTT Loadsharing	A feature that enables GTT-routed messages that are part of the same transaction to be loadshared to the same destination in a MAP or MRN group.
TSC	Time Slot Counter
TSM	Translation Service Module
TPC	True Point Code
TR	Technical Reference
TRA	Traffic Restarting Allowed
TRBL	Trouble
TRM	Termination Response Mode
TRW	Traffic Restarting Waiting
TSC	Time Slot Counter Synchronization
TSM	Translation Services Module
TSPC	True or Secondary Point Code
TT	Translation Type.
TUP	Telephone User Part
TVG	Group Ticket Voucher

U

UA	ETF User Adaptation Layers
UAL	User Application Layer
UAM	Unsolicited Alarm Message.
UAPS	UA Parameter Set
UDP	User Datagram Protocol
UDT	Unit Data Transfer
UDTS	Unit Data Transfer Service
UI	User Interface
UIM	Unsolicited Information Message
UPL	User Program Layer
UPU	User Part Unavailable

V

V.35	ITU Interface Recommendation, V.35 The interface used with the LIMV35 card.
VCC	Virtual Channel Connection
VGTT	Variable Length GTT A feature that provides the ability to provision global title entries of varying lengths to a single translation type or GTT set. Users are able to assign global title entries of up to 10 different lengths to a single translation type or GTT set.
VGTT	Variable (length) Global Title Translation
VLR	Visitor Location Register
VSCCP	VxWorks Signaling Connection Control Part The application used by the DSM card to support the G-Flex, G-Port, INP, EIR, and LNP features. If the G-Flex, G-Port, INP, or LNP feature is not turned on, and a DSM card is present, the VSCCP GPL processes normal GTT traffic.
VXWSLAN	An application used by the DCM card to support the STP LAN application. This GPL does not support 24-bit ITU-N point codes.

W

WAN	Wide Area Network
WGTTLS	Weighted GTT Loadsharing
WLNP	Wireless Local Number Portability
WNP	Wireless Number Portability
WSMSC	Wireless Short Message Service Center

X

XLAT	Translate Indicator
X-list	A list of non-provisioned members of provisioned cluster that are either restricted or prohibited for SS7 traffic.
XGTT	Expanded GTT (GTT Table Expansion).
XMAP	Expanded MAP Table
XUDT	Extended Unit Data
XUDT	Extended User Data
XUDTS	Extended Unit Data Service
XUDTS	Extended User Data Service