

Tekelec Signaling Products Database Administration Manual - IP⁷ Secure Gateway[®]

Table of Chapters

Table of Contents

List of Figures

List of Tables

List of Flowcharts

Chapter 1. Introduction

Chapter 2. IP7 Secure Gateway Overview

Chapter 3. IP7 Secure Gateway Configuration Procedures

Chapter 4. ISUP Variant Table Provisioning

Chapter 5. End Office Support

Chapter 6. Activating Controlled Features

Index

Tekelec Signaling Products

**Database Administration Manual - IP⁷ Secure
Gateway[®]**

**910-4600 Revision E
November 2004**



TEKELEC

© 2003, 2004 TEKELEC
All rights reserved.
Printed in the United States of America

Notice

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

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 or transmitted in any form or by any means, electronic or mechanical, including photocopying or recording, for any purpose without the express written permission of an authorized representative of Tekelec.

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

Trademarks

The Tekelec logo, Eagle, G-Port, and G-Flex, IP⁷, and IP⁷ Secure Gateway are registered trademarks of Tekelec, Inc.

COMMON LANGUAGE is a registered trademark, and Telcordia and CLLI are trademarks of Telcordia Technologies, Inc.

Patents

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

U.S. Patent Numbers:

6,327,350 6,662,017 6,456,845 6,647,113 5,953,404 6,606,379 6,167,129 6,324,183 6,639,981 5,008,929

Ordering Information

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

Table of Contents

Chapter 1. Introduction

Overview	1-2
Manual Organization	1-2
Related Publications	1-3
Documentation Packaging, Delivery, and Updates	1-7
Documentation Admonishments	1-8
Tekelec Technical Services	1-8
Emergency Response	1-9
Maintenance and Administration Subsystem	1-10
Database Partitions	1-11
Fixed Disk Drive	1-12
Removable Cartridge	1-13
List of Acronyms and Abbreviations	1-14

Chapter 2. IP7 Secure Gateway Overview

Introduction	2-2
IP7 Secure Gateway Hardware, Applications, and Functions	2-3
IP Connections	2-5
Point-to-Point Connectivity (IPLIM or IPLIMI Application)	2-20
Point-to-Multipoint Connectivity (SS7IPGW and IPGWI)	2-21
SNMP Agent Implementation	2-28
Mixed Networks Using the ANSI/ITU MTP Gateway Feature	2-32
ISUP Normalization	2-38
IETF Adapter Layer Support	2-46
Overview	2-46
Interaction Between TALI and IETF Connections Within a Single System	2-47
Feature Components	2-48

Chapter 3. IP7 Secure Gateway Configuration Procedures

Overview	3-3
Adding an IP Card	3-16

Card Slot Selection	3-17
Using the FORCE Parameter	3-18
Removing an IP Card	3-31
Configuring an IPGWx Linkset	3-40
Configuring a Mate IPGWx Linkset	3-60
Adding an IP Signaling Link	3-82
Example Signaling Link Configuration	3-89
Enabling the Large System # Links Controlled Feature	3-108
Removing an IP Signaling Link	3-115
Migrating IPLIMx M3UA Signaling Links to IPGWx M3UA Connections	3-125
Changing the IP Protocol Option	3-141
Changing IP Options other than SYNC and SCTPCSUM	3-148
Adding an IP Host	3-153
Removing an IP Host	3-155
Changing an IP Link	3-158
Changing an IP Card	3-173
Adding an IP Route	3-183
Removing an IP Route	3-188
Adding an Application Socket	3-192
Removing an Application Socket	3-202
Changing an Application Socket	3-205
Configuring IP Socket Retransmission Parameters	3-217
Changing a DCM Parameter Set	3-223
Adding an Application Routing Key Containing a Socket	3-228
Adding an Application Routing Key Containing an Application Server	3-240
Removing an Application Routing Key	3-258
Replacing the IP Connections in an Existing Application Routing Key with a Single Socket	3-267
Changing the CIC values in an Existing Application Routing Key	3-275
Changing the Routing Context Value in an Existing Application Routing Key	3-283
Replacing the IP Connections in an Existing Application Routing Key with an Application Server	3-293
Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key	3-307

Table of Contents

Increasing the System-Wide IPGWx Signaling TPS	3-321
Configuring the IP TPS Alarm Threshold	3-328
IETF Adapter Layer Configuration	3-331
Adding an Association	3-332
Removing an Association	3-345
Changing an Association	3-350
Configuring SCTP Retransmission Control for an Association	3-370
Changing an M2PA Timer Set	3-379
Adding an Application Server Process	3-383
Removing an Application Server Process	3-387
Changing an Application Server Process	3-390
Adding an Application Server	3-397
Removing an Application Server	3-407
Changing an Application Server	3-412
Adding a Network Appearance	3-417
Removing a Network Appearance	3-420
Changing the SCTP Checksum Algorithm Option	3-422
Changing a UA Parameter Set	3-451
Chapter 4. ISUP Variant Table Provisioning	
Overview	4-2
Adding New ISUP PSTN Presentation Values	4-6
Changing ISUP Presentation Values	4-11
Removing ISUP Presentation Values	4-13
Changing ISUP Variant Table Entries	4-17
Copying ISUP Variant Table Entries	4-26
Chapter 5. End Office Support	
Overview	5-2
Internal Point Code	5-4
End Office Support Configuration	5-13
Adding an End Node Internal Point Code	5-14
Removing an End Node Internal Point Code	5-18
Chapter 6. Activating Controlled Features	
Introduction	6-2
Enabling Controlled Features	6-2
Enabling a Permanent or Temporary Key	6-3

Temporary Feature Keys6-7
Turning On and Off Controlled Features6-10
Turning On an Enabled Controlled Feature6-10
Turning Off an Enabled Controlled Feature6-12

Index

List of Figures

Figure 1-1. Database Partitions	1-11
Figure 2-1. TCP socket or SCTP Association Database Relationships	2-6
Figure 2-2. IP Connections using a Dual-Slot DCM running the IPLIMx Applications	2-7
Figure 2-3. IP Connections using a Dual-Slot DCM running the IPGWx Applications	2-8
Figure 2-4. IP Connections using an EDCM running the IPGWx Applications	2-9
Figure 2-5. Typical SCTP Association and TCP Socket Configuration	2-10
Figure 2-6. SCTP Association and TCP Socket on the Same IP Card	2-11
Figure 2-7. IP Connections using SSEDCMs running the IPLIMx Applications	2-12
Figure 2-8. Multi-Homed Associations on EDCMs running the IPLIMx Applications	2-14
Figure 2-9. Multi-Homed Associations on EDCMs running the IPGWx Applications	2-15
Figure 2-10. Multi-Homed Association Database Relationships	2-16
Figure 2-11. IP7 Secure Gateway Network (STP Connectivity via MTP-over-IP)	2-20
Figure 2-12. IP Network (SCP Connectivity via TCAP-over-IP)	2-21
Figure 2-13. IP Network (SEP connectivity via ISUP, Q.BICC, and TUP-over-IP)	2-22
Figure 2-14. Complex Network with ANSI, ITU-I, and ITU-N Nodes	2-33
Figure 2-15. 8-bit TOS Field	2-38
Figure 2-16. DS Field	2-38
Figure 2-17. ISUP Normalization Supporting Multiple ISUP Variants	2-39
Figure 2-18. Format of PSTN Presentation	2-43
Figure 2-19. AS/ASP Relationship	2-47

Figure 2-20. TCP Socket/SCTP Association Relationship	2-48
Figure 2-21. SG/MGC/MG Network Diagram	2-48
Figure 2-22. TALI Protocol Stack (IPGWx and IPLIMx)	2-49
Figure 2-23. IPLIMx Protocol Stack with SCTP as the Transport Layer	2-49
Figure 2-24. IPGWx Protocol Stack with SCTP as the Transport Layer	2-50
Figure 2-25. M2PA in the IP ⁷ Signaling Gateway	2-53
Figure 2-26. SCTP Connectivity	2-56
Figure 3-1. Mixed Network with ANSI, ITU-I, and ITU-N Nodes	3-6
Figure 3-2. IP ⁷ Secure Gateway Database Relationships	3-12
Figure 3-3. Typical System Configuration	3-13
Figure 5-1. A System with End Office Support and VXI Node	5-6
Figure 5-2. Network Before a System with End Office, Node P is to Migrate	5-6
Figure 5-3. Network After a System with End Office, Node P has Migrated	5-7
Figure 5-4. Original Network with Deployed System	5-7
Figure 5-5. New Network with a System Using End Office and End Node R	5-8
Figure 5-6. Network before Two Signaling End Points Migrate from PSTN to IP	5-8
Figure 5-7. Network after Two Signaling End Points Migrate from PSTN to IP	5-9
Figure 5-8. The System Simultaneously Acts as STP and End Office	5-10
Figure 5-9. Three Multiple-Element End Office Nodes	5-11
Figure 5-10. Mated Pair Supports Two End Office Nodes	5-12

List of Tables

Table 2-1. Ethernet Interface and Signaling Link Port Combinations	2-7
Table 2-2. Uni-Homed and Multi-Homed Node Combinations	2-13
Table 2-3. SS7 Full Routing Keys per IPGWx Functionality	2-24
Table 2-4. Example SS7 Routing Key Table	2-26
Table 2-5. Routing Key Lookup Hierarchy	2-27
Table 2-6. SNMP Object Groups	2-29
Table 2-7. Deviations from SNMP Protocols	2-31
Table 2-8. Nodes and Point Codes in Complex Network Example	2-34
Table 2-9. ISUP Variants Supported by this Feature	2-40
Table 2-10. Sample SCTP Endpoints	2-58
Table 2-11. Sample SCTP Associations	2-58
Table 2-12. Sample SCTP Associations	2-59
Table 3-1. Typical IP Routing	3-14
Table 3-2. Typical IP Sockets	3-14
Table 3-3. Typical IP Routing Keys (SS7IPGW and IPGWI Applications)	3-15
Table 3-4. Card Type and Card Applications	3-16
Table 3-5. Example Card Configuration	3-17
Table 3-6. Number of Transactions per Second for each SCCP Card	3-18
Table 3-7. SS7 Card Applications and Signaling Link Types	3-19
Table 3-8. Signaling Link Fair Share Example	3-41
Table 3-9. Optional Linkset Parameters	3-43
Table 3-10. Optional Linkset Parameters	3-61
Table 3-11. Number of High-Speed and Low-Speed Links Supported at 100% Traffic	3-84
Table 3-12. Number of High-Speed and Low-Speed Links Supported at 80% Traffic	3-87
Table 3-13. IP Signaling Link Parameter Combinations	3-88
Table 3-14. IP Signaling Link Configuration Table	3-89
Table 3-15. Valid Subnet Mask Parameter Values	3-159
Table 3-16. Valid Subnet Mask Parameter Values	3-184

Table 3-17. DCMPS Values	3-223
Table 3-18. Service Indicator Text String Values	3-228
Table 3-19. Routing Key Parameter Combinations for Adding a Routing Key Containing a Socket	3-230
Table 3-20. Service Indicator Text String Values	3-240
Table 3-21. Routing Key Parameter Combinations for Adding a Routing Key Containing an Application Server	3-242
Table 3-22. Service Indicator Text String Values	3-258
Table 3-23. Routing Key Parameter Combinations for Removing Routing Keys	3-260
Table 3-24. Service Indicator Text String Values	3-267
Table 3-25. Routing Key Parameter Combinations for Replacing the IP Connections in an Existing Application Routing Key with a Single Socket	3-269
Table 3-26. Service Indicator Text String Values	3-275
Table 3-27. Routing Key Parameter Combinations for Changing the Range of CIC Values in an Existing Routing Key	3-277
Table 3-28. Routing Key Parameter Combinations for Splitting the Range of CIC Values in an Existing Routing Key	3-278
Table 3-29. Service Indicator Text String Values	3-283
Table 3-30. Routing Key Parameter Combinations for Changing the Routing Context Value in an Existing Application Routing Key	3-285
Table 3-31. Service Indicator Text String Values	3-293
Table 3-32. Routing Key Parameter Combinations for Replacing the IP Connections in an Existing Application Routing Key with an Application Server	3-295
Table 3-33. Service Indicator Text String Values	3-308
Table 3-34. System-Wide IPGWx Signaling TPS Part Numbers	3-322
Table 3-35. Valid PVALUE Parameter Values if PARM=1	3-452
Table 3-36. Valid PVALUE Parameter Values if PARM=2	3-453
Table 3-37. Valid PVALUE Parameter Values if PARM=3	3-454
Table 4-1. ISUP Variants Supported by this Feature	4-3
Table 4-2. CHG-ISUPVAR-ATTRIB Parameter Combinations	4-20
Table 5-1. Sample IPC Values	5-4
Table 6-1. Sample Controlled Feature Part Numbers	6-3
Table 6-2. Sample Controlled Feature Part Numbers	6-10
Table 6-3. Sample Controlled Feature Part Numbers	6-13

List of Flowcharts

Flowchart 3-1. Adding an IP Card	3-25
Flowchart 3-2. Removing an IP Card	3-38
Flowchart 3-3. Configuring an IPGWx Linkset	3-54
Flowchart 3-4. Configuring a Mate IPGWx Linkset	3-75
Flowchart 3-5. Adding an IP Signaling Link	3-101
Flowchart 3-6. Enabling the Large System # Links Controlled Feature	3-112
Flowchart 3-7. Removing an IP Signaling Link	3-122
Flowchart 3-8. Migrating IPLIMx M3UA Signaling Links to IPGWx M3UA Connections	3-135
Flowchart 3-9. Changing the IP Protocol Option	3-146
Flowchart 3-10. Changing an IP Option That Does Not Require Inhibiting the IP Card	3-152
Flowchart 3-11. Adding an IP Host	3-154
Flowchart 3-12. Removing an IP Host	3-157
Flowchart 3-13. Changing an IP Link	3-168
Flowchart 3-14. Changing an IP Card	3-180
Flowchart 3-15. Adding an IP Route	3-187
Flowchart 3-16. Removing an IP Route	3-191
Flowchart 3-17. Adding an Application Socket	3-199
Flowchart 3-18. Removing an Application Socket	3-204
Flowchart 3-19. Changing an Application Socket	3-212
Flowchart 3-20. Configuring IP Retransmission Parameters	3-222
Flowchart 3-21. Changing an DCM Parameter Set	3-227
Flowchart 3-22. Adding an Application Routing Key Containing a Socket	3-236
Flowchart 3-23. Adding an Application Routing Key Containing an Application Server	3-254
Flowchart 3-24. Removing an Application Routing Key	3-265
Flowchart 3-25. Replacing the IP Connections in an Existing Application Routing Key with a Single Socket	3-274
Flowchart 3-26. Changing the CIC values in an Existing Application Routing Key	3-282

Flowchart 3-27. Changing the Routing Context Value in an Existing Application Routing Key	3-291
Flowchart 3-28. Assigning a New Application Server Name to an Existing Application Routing Key	3-303
Flowchart 3-29. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key	3-315
Flowchart 3-30. Increasing the IPGWx Signaling TPS	3-326
Flowchart 3-31. Configuring the IP TPS Alarm Threshold	3-330
Flowchart 3-32. Adding an Association	3-340
Flowchart 3-33. Removing an Association	3-349
Flowchart 3-34. Changing an Association	3-361
Flowchart 3-35. Configuring an Association for SCTP Retransmission Control	3-377
Flowchart 3-36. Changing an M2PA Timer Set	3-382
Flowchart 3-37. Adding an Application Server Process	3-386
Flowchart 3-38. Removing an Application Server Process	3-389
Flowchart 3-39. Changing an Application Server Process	3-394
Flowchart 3-40. Adding an Application Server	3-402
Flowchart 3-41. Removing an Application Server	3-411
Flowchart 3-42. Changing an Application Server	3-415
Flowchart 3-43. Adding a Network Appearance	3-419
Flowchart 3-44. Removing a Network Appearance	3-421
Flowchart 3-45. Changing the SCTP Checksum Option	3-444
Flowchart 3-46. Changing a UA Parameter Set	3-460
Flowchart 4-1. Adding ISUP PSTN Presentation Value	4-9
Flowchart 4-2. Changing ISUP PSTN Presentation Value	4-12
Flowchart 4-3. Removing ISUP PSTN Presentation Value	4-16
Flowchart 4-4. Changing ISUP Attribute Values	4-24
Flowchart 4-5. Copying ISUP Attribute Values	4-30
Flowchart 5-1. Adding an End Node Internal Point Code	5-17
Flowchart 5-2. Removing an End Node Internal Point Code	5-20
Flowchart 6-1. Enabling a Permanent or Temporary Key	6-6
Flowchart 6-2. Clearing a Temporary Feature Access Key Alarm	6-9
Flowchart 6-3. Turning On an Enabled Controlled Feature	6-12
Flowchart 6-4. Turning Off an Enabled Controlled Feature	6-14

1

Introduction

Overview	1-2
Manual Organization	1-2
Related Publications.....	1-3
Documentation Packaging, Delivery, and Updates.....	1-7
Documentation Admonishments	1-8
Tekelec Technical Services	1-8
Emergency Response	1-9
Maintenance and Administration Subsystem	1-10
Database Partitions.....	1-11
Fixed Disk Drive.....	1-12
Removable Cartridge.....	1-13
List of Acronyms and Abbreviations.....	1-14

Overview

The *Database Administration Manual – IP⁷ Secure Gateway* describes the procedures necessary for database administration personnel or translations personnel to create, modify, display, and maintain the system database, and to configure the system to implement the IP⁷ Secure Gateway.

NOTE: Database administration privileges are password restricted. Only those persons with access to the command class “Database Administration” can execute the administrative functions. Other command classes and the commands allowed by those classes are listed in the *Commands Manual*.

Manual Organization

Throughout this document, the terms database and system software are used. Database refers to all data that can be administered by the user, including shelves, cards, links, routes, global title translation tables, and gateway screening tables. System software refers to data that cannot be administered by the user, including generic program loads (GPLs).

This document is organized into these sections:

Chapter 1, “Introduction,” contains general information about the database and the organization of this manual.

Chapter 2, “IP⁷ Secure Gateway Overview,” describes the basics of the IP⁷ Secure Gateway.

Chapter 3, “IP⁷ Secure Gateway Configuration Procedures,” describes the procedures necessary to configure the system to provide connectivity between SS7 and IP networks, enabling messages to pass between the SS7 network domain and the IP network domain, including the procedures necessary to configure the system to use the SUA, M3UA, and M2PA adapter layers in the IP⁷ Secure Gateway.

Chapter 4, “ISUP Variant Table Provisioning,” describes the procedures necessary to configure the ISUP Variant Tables.

Chapter 5, “End Office Support,” describes the procedures necessary to allow the system to share its true point code (TPC) with an IP-based node without the need for a separate point code for the IP node.

Chapter 6, “Activating Controlled Features,” explains how to enable controlled features with temporary and permanent feature keys, how to clear the alarms for near to expired and expired temporary keys, and how to turned enabled On/Off features on and off.

Related Publications

The *Database Administration Manual – IP⁷ Secure Gateway* is part of the system documentation set and may reference related manuals of this set. The documentation set includes the following manuals:

- The *Commands Manual* contains procedures for logging into or out of an Eagle STP or IP⁷ Secure Gateway system, a general description of the terminals, printers, the disk drive used on the system, and a description of all the commands used in the system. The *Commands Manual* also contains the *Commands Pocket Guide* and the *Commands Quick Reference*.
- The *Commands Error Recovery Manual* contains the procedures to resolve error message conditions generated by the commands in the *Commands Manual*. These error messages are presented in numerical order.
- The *Database Administration Manual – Features* contains procedural information required to configure an Eagle STP or IP⁷ Secure Gateway system to implement these features:
 - X.25 Gateway
 - STP LAN
 - Database Transport Access
 - GSM MAP Screening
 - Eagle Support for Integrated Sentinel
- The *Database Administration Manual - Gateway Screening* contains a description of the Gateway Screening (GWS) feature and the procedures necessary to configure an Eagle STP or IP⁷ Secure Gateway system to support this feature.
- The *Database Administration Manual – Global Title Translation* contains procedural information required to configure an Eagle STP or IP⁷ Secure Gateway system to implement these features:
 - Global Title Translation
 - Enhanced Global Title Translation
 - Variable Length Global Title Translation
 - Interim Global Title Modification
 - Intermediate GTT Load Sharing
- The *Database Administration Manual – LNP* contains procedural information required to configure an Eagle STP system or an IP⁷ Secure Gateway system to implement the local number portability (LNP) feature.

- The *Database Administration Manual – SEAS* contains the procedures that can be performed from the Signaling Engineering and Administration Center (SEAC) or a Signaling Network Control Center (SNCC) to configure the Eagle. These procedures contain a brief description of the procedure, a reference to the procedure in either the *Database Administration Manual – SS7*, *Database Administration Manual – Global Title Translation*, or *Database Administration Manual – Gateway Screening* that contains more information on that procedure, and a flowchart showing the order that the tasks must be performed.
- The *Database Administration Manual – SS7* contains procedural information required to configure an Eagle STP system or an IP⁷ Secure Gateway system to implement the SS7 protocol.
- The *Database Administration Manual – System Management* contains procedural information required to manage the Eagle's database and GPLs, and to configure basic system requirements such as user names and passwords, system-wide security requirements, and terminal configurations.
- The *Dimensioning Guide for EPAP Advanced DB Features* is used to provide EPAP planning and dimensioning information. This manual is used by Tekelec personnel and Eagle customers to aid in the sale, planning, implementation, deployment, and upgrade of EAGLE 5 SAS systems.
- The *ELAP Administration Manual* provides a definition of the user interface to the Eagle LNP Application Processor on the MPS/ELAP platform. The manual defines the methods for accessing the interface, menus, screens available to the user, and describes their impact. It provides the syntax and semantics of user input and defines the output the user receives, including information and error messages.
- The *EPAP Administration Manual* describes how to administer to the Eagle Provisioning Application Processor on the MPS/EPAP platform. The manual defines the methods for accessing the user interface, menus, screens available to the user, and describes their impact. It provides the syntax and semantics of user input and defines the output the user receives, including messages, alarms, and status.
- The *Feature Manual - EIR* provides details of the feature providing network operators with the capability to prevent stolen or disallowed GSM mobile handsets from accessing the network. This manual gives the instructions and information on how to install, use, and maintain the EIR feature on the Multi-Purpose Server (MPS) platform of the Eagle System.
- The *Feature Manual - G-Flex C7 Relay* provides an overview of a feature supporting the efficient management of Home Location Registers in various networks. This manual gives the instructions and information on how to install, use, and maintain the G-Flex feature on the Multi-Purpose Server (MPS) platform of the Eagle System.

Introduction

- The *Feature Manual - G-Port* provides an overview of a feature providing the capability for mobile subscribers to change the GSM subscription network within a portability cluster while retaining their original MSISDNs. This manual gives the instructions and information on how to install, use, and maintain the G-Port feature on the Multi-Purpose Server (MPS) platform of the Eagle System.
- The *Feature Manual - INP* provides information and instructions on how to implement, utilize, and maintain the INAP-based Number Portability (INP) feature on the Multi-Purpose Server (MPS) platform of the Eagle System.
- The *FTP-Based Table Retrieve Application (FTRA) User Guide* describes how to set up and use a PC to serve as the offline application for the Eagle FTP Retrieve and Replace feature.
- The *LNP Database Synchronization Manual - LSMS 6.0/Eagle* describes how to keep the LNP databases at a release 6.0 LSMS and a network element (the Eagle is a network element) synchronized through the use of resynchronization, audits and reconciles, and bulk loads.

NOTE: LNP Database Synchronization Manuals for LSMS release 5.0 and 4.0 can be ordered separately. Contact your sales representative for part number information.

- The *LNP Feature Activation Guide* contains procedural information required to configure the system for the LNP feature using telephone number quantities from 24 million to 96 million telephone numbers.
- The *Maintenance Manual* contains procedural information required for maintaining the Eagle STP system, the IP⁷ Secure Gateway system. The *Maintenance Manual* provides preventive and corrective maintenance procedures used in maintaining the different systems.
- The *Eagle STP with TekServer IAS MPS Platform Software and Maintenance Manual* describes the TekServer core platform features and the MPS customization features that make up the Multi-Purpose Server (MPS) platform software. This manual also describes how to perform preventive and corrective maintenance for the MPS.
- The *Signaling Products Hardware Manual* contains hardware descriptions and specifications of Tekelec's Network Systems Division (NSD) products. These include the Eagle STP system, the IP⁷ Secure Gateway (SG) system, and OEM-based products which include the ASi 4000 Service Control Point (SCP), and the Integrated Sentinel with Extended Services Platform (ESP) subassembly.

The *Signaling Products Hardware Manual* provides an overview of each system and its subsystems, details of standard and optional hardware components in each system, and basic site engineering. Refer to this manual to obtain a basic understanding of each type of system and its related hardware, to locate detailed information about hardware components used in a particular release, and to help configure a site for use with the system hardware.

- The *NSD Installation Manual* contains cabling requirements, schematics, and procedures for installing the Eagle systems along with LEDs, Connectors, Cables, and Power Cords to Peripherals. Refer to this manual to install components or the complete systems.
- The *Signaling Products Integrated Applications Installation Manual* provides the installation information on Frame Floors and Shelves for Integrated Applications Products such as MPS EPAP 4.0, ASi 4000 SCP, and VXi Media Gateway Controller, Integrated and Non-Integrated Sentinel, LEDs, Connectors, Cables, and Power Cords to Peripherals. Refer to this manual to install components or the complete systems.
- The *TekServer Services Platform Hardware Manual* provides general specifications and a description of the TekServer. This manual also includes site preparation, environmental and other requirements, procedures to physically install the TekServer, and troubleshooting and repair of Field Replacable Units (FRUs).
- The *Provisioning Database Interface Manual* defines the programming interface that populates the Provisioning Database (PDB) for the Eagle features supported on the MPS/EPAP platform. The manual defines the provisioning messages, usage rules, and informational and error messages of the interface. The customer uses the PDBI interface information to write his own client application to communicate with the MPS/EPAP platform.
- The *Release Documentation* contains the following documents for a specific release of the system:

Release Notice - Describes the changes made to the system during the lifecycle of a release. The initial Release Notice includes Generic Program Loads (GPLs) only. The final Release Notice provides a list of PRs resolved in a build and all known PRs.

NOTE: The *Release Notice* is maintained solely on Tekelec's Customer Support Website to provide you with instant access to the most up-to-date release information.

Feature Notice - Describes the features contained in the specified release. Also provides the hardware baseline for the specified release, describes the customer documentation set, provides information about customer training, and explains how to access the Customer Service website.

Technical Bulletins - Contains a compilation of updates to methods or procedures used to maintain the system (if applicable).

System Overview - Provides high-level information on SS7, the IP⁷ Secure Gateway, system architecture, LNP, and EOAP.

Master Glossary - Contains an alphabetical listing of terms, acronyms, and abbreviations relevant to the system.

Cross-Reference Index - Lists all first-level headings used throughout the documentation set.

Introduction

- *Previously Released Features* - The Previously Released Features Manual briefly describes the features of previous Eagle and IP7 Secure Gateway releases, and it identifies the release number of their introduction.

Documentation Packaging, Delivery, and Updates

Customer documentation is provided with each system in accordance with the contract agreements.

Customer documentation is updated whenever significant changes that affect system operation or configuration are made.

Customer documentation updates may be issued in the form of an addendum, or a reissue of the affected documentation.

The document part number is shown on the title page along with the current revision of the document, the date of publication, and the software release that the document covers. The bottom of each page contains the document part number and the date of publication.

Two types of releases are major software releases and maintenance releases. Maintenance releases are issued as addenda with a title page and change bars. On the changed pages, the date and document part number are changed. On any unchanged pages that accompany the changed pages, the date and document part number are unchanged.




In the event a software release has minimum affect on documentation, an addendum is provided. The addendum provides an instruction page, a new title page, a change history page, and replacement chapters bearing the date of publication, the document part number, and change bars.

If a new release has a major impact on documentation, such as a new feature, the entire documentation set is reissued with a new part number and a new release number.

Documentation Admonishments

Admonishments are icons and text that may appear in this and other system manuals that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Following are the admonishments, listed in descending order of priority.

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

Tekelec Technical Services

The Tekelec Technical Services department offers a point of contact through which customers can receive support for problems that may be encountered during the use of Tekelec's products. The Tekelec Technical Services department is staffed with highly trained engineers to provide solutions to your technical questions and issues seven days a week, twenty-four hours a day. A variety of service programs are available through the Tekelec Technical Services department to maximize the performance of Tekelec products that meet and exceed customer needs.

To receive technical assistance, call the Tekelec Technical Services department at one of the following locations:

- Tekelec, UK
 Phone (within the UK) 07071232453
 (outside the UK) +44 7071232453 or +44 1784437067.
- Tekelec, USA
 Phone (within the continental US) 800-432-8919
 (outside the continental US) +1 919-460-2150.

Or you can request assistance by way of electronic mail at eaglets@tekelec.com.

Introduction

When your call is received, Technical Services issues a Customer Service Report (CSR). Each CSR includes an individual tracking number. When a CSR is issued, Technical Services determines the classification of the trouble (see Bellcore Generic Requirements, GR-929-CORE, Reliability and Quality Measurements for Telecommunications Systems (RQMS)). The CSR contains the serial number of the system, problem symptoms, and messages. Technical Services assigns the CSR to a primary engineer, who will work to solve the problem. Technical Services closes the CSR when the problem is resolved.

If a critical problem exists, Technical Services initiates emergency procedures (see the following topic, "Emergency Response").

Emergency Response

If a critical service situation occurs, Tekelec Technical Services offers emergency response twenty-four hours a day, seven days a week. The emergency response provides immediate coverage, automatic escalation, and other features to ensure a rapid resolution to the problem.

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

- Failure in the system that prevents transaction processing
- Reduction in system capacity or in system traffic-handling capability
- Inability to restart the system
- Corruption of the database
- Inability to perform maintenance or recovery operations
- Inability to provide any required critical or major trouble notification
- Any other problem severely affecting service, capacity, traffic, and billing. Maintenance capabilities may be defined as critical by prior discussion and agreement with Tekelec Technical Services.

Maintenance and Administration Subsystem

The maintenance and administration subsystem consists of two processors, MASP (maintenance and administration subsystem processor) A and MASP B.

Each MASP is made up of two cards, the GPSM-II card (general purpose service module) and the TDM (terminal disk module).

The GPSM-II card contains the communications processor and applications processor and provides connections to the IMT bus. The GPSM-II controls the maintenance and database administration activity.

The TDM contains the fixed disk drive, the terminal processor for the 16 serial I/O ports and interfaces to the MDAL (maintenance disk and alarm) card which contains the removable cartridge drive and alarm logic. There is only one MDAL card in the maintenance and administration subsystem and it is shared between the two MASPs.

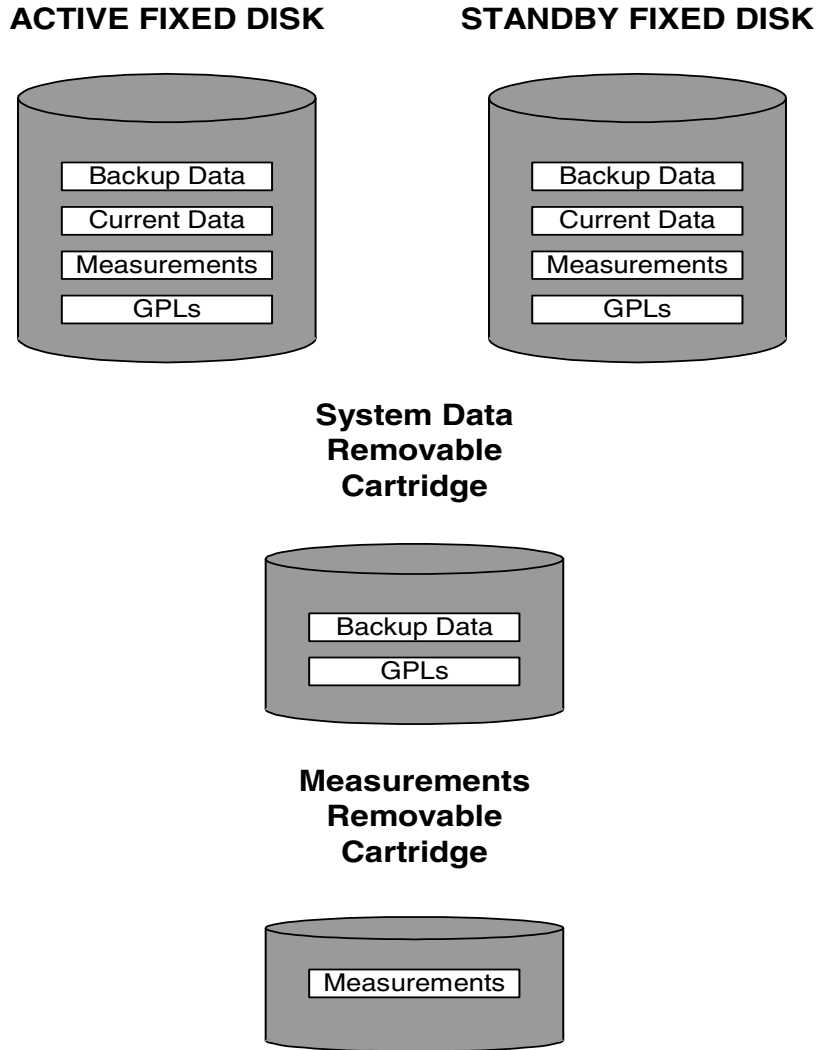
The procedures in the *Database Administration Manual – IP⁷ Secure Gateway* refer to the terms MASP and MDAL. The database commands, such as `rept-stat-db`, refer to the MASP because the MASP controls the input to the TDM and MDAL, and output from the TDM and MDAL. The MDAL is only referred to when inserting or removing the removable cartridge because the removable cartridge drive resides on the MDAL.

For more information on these cards, go to the *Installation Manual*.

Database Partitions

The data that the Eagle uses to perform its functions are stored in two separate areas: the fixed disk drives, and the removable cartridge. The Fixed Disk Drive section on page 1-12 and the Removable Cartridge section on page 1-13 describe these areas and data that is stored on them. These areas and their partitions are shown in Figure 1-1.

Figure 1-1. Database Partitions



Fixed Disk Drive

There are two fixed disk drives on the system. The fixed disk drives contain the “master” set of data and programs for the system. The two fixed disk drives are located on the terminal disk modules (TDMs). Both disks have the same files. The data stored on the fixed disks is partially replicated on the various cards in the system. Changes made during database administration sessions are sent to the appropriate cards.

The data on the fixed disks can be viewed as four partitions.

- Current partition
- Backup partition
- Measurements partition
- Generic program loads (GPLs) partition

The data which can be administered by users is stored in two partitions on the fixed disk, a current database partition which has the tables which are changed by on-line administration, and a backup database partition which is a user-controlled copy of the current partition.

All of the on-line data administration commands effect the data in the current partition. The purpose of the backup partition is to provide the users with a means of rapidly restoring the database to a known good state if there has been a problem while changing the current partition.

A full set of GPLs is stored on the fixed disk in the GPL partition. There is an approved GPL and a trial GPL for each type of GPL in this set and a utility GPL, which has only an approved version. Copies of these GPLs are downloaded to the system cards. The GPL provides each card with its functionality. For example, the **ss7ansi** GPL provides MTP functionality for link interface modules (LIMs).

Measurement tables are organized as a single partition on the fixed disk. These tables are used as holding areas for the measurement counts.

Introduction

Removable Cartridge

A removable cartridge is used for two purposes.

- To hold an off-line backup copy of the administered data and system GPLs
- To hold a copy of the measurement tables

Because of the size of the data stored on the fixed disk drives on the TDMs, a single removable cartridge cannot store all of the data in the database, GPL, and measurements partitions.

To use a removable cartridge to hold the system data, it must be formatted for system data. To use a removable cartridge to hold measurements data, it must be formatted for measurements data. The system provides the user the ability to format a removable cartridge for either of these purposes. A removable cartridge can be formatted on the system by using the **format-disk** command. More information on the **format-disk** command can be found in the *Commands Manual*. More information on the removable cartridge drive can be found in the *Installation Manual*.

The removable cartridge drive is located on the MDAL card in card location 1117.

Additional and preformatted removable cartridges are available from Tekelec Technical Services.

List of Acronyms and Abbreviations

ACMENET	Applications Communications Module with the Ethernet interface
ACT	Activate
ALIASA	ANSI Alias Point Code
ALIASI	ITU International Alias Point Code
ALIASN	ITU National Alias Point Code
ANSI	American National Standards Institute
APC	Adjacent Point Code
APCA	ANSI Adjacent Point Code
APCI	ITU International Adjacent Point Code
APCN	ITU National Adjacent Point Code
APPL	Application
AS	Application Server
ASCII	American Standard Code for Information Interchange
ASP	Application Server Process
AST	Associated State for Maintenance
ATM	Asynchronous Transfer Mode
ATMANSI	The application software for the ATM (high-speed) SS7 signaling links
ATMITU	The application software for the ITU ATM (high-speed) SS7 signaling links
BEI	Broadcast Exception Indicator
BPDCM	Application software for flash memory management on the DCM card
BPS	Bits per Second or Bytes per Second
CCS7ITU	The application software for the ITU SS7 (low-speed) signaling links
CHG	Change
CIC	Circuit Identification Code
CLLI	Common Language Location Identifier
Cmd Rej	Command Rejected

Introduction

CPC	Capability Point Code
CPU	Central Processing Unit
DCM	Database Communication Module
DCMPS	Database Communications Module Parameter Set
DEFROUTER	Default Router
DLT	Delete
DNS	Domain Name Server
DPC	Destination Point Code
DPCA	ANSI Destination Point Code
DPCI	ITU International Destination Point Code
DPCN	ITU National Destination Point Code
DS	Differentiated Service
DTA	Database Transport Access
DTE	Data Terminal Equipment
E1	European equivalent of the North American 1.544 Mbps T1 (Trunk Level 1) except that E1 carries information at 2.048 Mbps.
ECM	Error Correction Method
EDCM	Enhanced-Performance Database Communications Module
ELEI	Exception List Exclusion Indicator
ENT	Enter
EO	End Office
EOAM	Enhanced Operations, Administration, and Maintenance
FAK	Feature Access Key
FTP	File Transfer Protocol
G-FLEX	GSM Flexible Numbering
G-PORT	GSM Portability
GLS	Gateway Loading Services – Application software for the gateway screening loading services
GPL	Generic Program Load
GPSM	General Purpose Service Module

GTT	Global Title Translation
GWS	Gateway Screening
GWSA	Gateway Screening Application
GWSD	Gateway Screening Message Discard
GWSM	Gateway Screening Mode
HMUX	High-Speed Multiplexer
I/O	Input/Output
ICMP	Internet Control Message Protocol
ID	Identity
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IMT	Interprocessor Message Transport
INH	Inhibit
INIT	Initialize
IP	Internet Protocol
IPADDR	IP Address
IPC	Internal Point Code
IPGWI	An ITU version of SS7IPGW application software
IPGWx	Point to multi-point IP ⁷ Secure Gateway application software, referring to SS7IPGW (ANSI) and IPGWI (ITU)
IPLIM	Application software for TCP/IP point-to-point connectivity for ANSI networks
IPLIMI	Application software for TCP/IP point-to-point connectivity for ITU networks
IPLIMx	Point to point IP ⁷ Secure Gateway application software, referring to IPLIM (ANSI) and IPLIMI (ITU)
IS-NR	In Service - Normal
ISUP	ISDN User Part
ITU	International Telecommunications Union
ITU-I	ITU International
ITU-N	ITU National
LAN	Local Area Network

Introduction

LHOST.....	Local Host
LIM	Link Interface Module
LIMATM.....	LIM used with ATM (high-speed) signaling links
LIMCH	A LIM used as a channel card with either the E1 or T1 interfaces
LIMDS0	LIM with a DS0A interface
LIME1	LIM with an E1 Interface
LIME1ATM.....	LIM used with ITU ATM (high-speed) signaling links
LIMOCU	LIM with a OCU interface
LIMT1	LIM with a T1 interface
LIMV35.....	LIM with a V.35 interface
LNP.....	Local Number Portability
LOC.....	Location
LPORT	The TCP or SCTP port number for the local host
LS.....	Linkset
LSMS.....	Local Service Management System
LSN	Linkset Name
LST	Linkset Type
M2PA	SS7 MTP2-User Peer-to-Peer Adaptation Layer
M3UA	SS7 MTP3 Adaptation Layer
MAP.....	Mated Application
MAP.....	Mobile Application Part
MAS	Maintenance and Administration Subsystem
MASP.....	Maintenance and Administration Subsystem Processor
MDAL.....	Maintenance Disk and Alarm Card
MSU	Message Signaling Unit
MTP	Message Transfer Part
MTP2	Message Transfer Part, Level 2
MTP3	Message Transfer Part, Level 3
NA.....	Network Appearance
NE	Near End
NEI.....	Network Element Interface

NI.....	Network Identifier
NMS.....	Network Management System
OCU.....	Office Channel Unit
OOS.....	Out of Service
OOS-MT-DSBLD.....	Out of Service - Maintenance Disabled
OPC.....	Originating Point Code
PC.....	Point Code
PC.....	Personal Computer
PCR.....	Preventive Cyclic Retransmission
PDU.....	Protocol Data Unit
PST.....	Primary State for Maintenance
PSTN.....	Public Switched Telephone Network
REPT-STAT.....	Report Status
RHOST.....	Remote Host
RMV.....	Remove
RPORT.....	The TCP or SCTP port number of the remote host
RST.....	Restore
RTRV.....	Retrieve
SAAL.....	Signaling ATM Adaptation Layer
SCCP.....	Signaling Connection Control Part – Application software for the global title translation (GTT) feature
SCMG.....	SCCP Management
SCRN.....	Screen Set Name
SCTP.....	Stream Control Transmission Protocol
SEAC.....	Signaling Engineering and Administration Center
SEAS.....	Signaling Engineering and Administration System
SGP.....	Signaling Gateway Process
SI.....	Service Indicator
SIO.....	Service Information Octet
SLC.....	Signaling Link Code
SLK.....	Signaling Link
SLS.....	Signaling Link Selector

Introduction

SLSCI	5- to 8-bit SLS Conversion Indicator
SNCC	Signaling Network Control Center
SNM.....	Signaling Network Management
SNMP	Simple Network Management Protocol
SS7.....	Signaling System #7
SS7 DPC.....	SS7 Destination Point Code
SS7ANSI.....	The application software for the ANSI SS7 signaling links
SS7IPGW	The application software for IP ⁷ signaling gateway feature point-to-multipoint connectivity
SS7GX25	The application software for the X.25/SS7 gateway feature
SSEDCM.....	Single-slot EDCM
SSN.....	Subsystem Number
SST	Secondary State for Maintenance
STP	Signal Transfer Point
STP LAN	Feature 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	Application software for the STP LAN feature
SUA.....	SCCP User Adaptation Layer
T1.....	Trunk Level 1
TALI.....	Transport Adaptation Layer Interface
TCA.....	Transfer Cluster Allowed network management message
TCAP	Transaction Capability Application Part
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM.....	Terminal Disk Module
TFA.....	Transfer Allowed network management message
TFC.....	Transfer Controlled network management message
TFATCABMLQ.....	TFA/TCA broadcast minimum link quantity
TFP	Transfer Prohibited network management message

TFR.....	Transfer Restricted network management message
TOS.....	Type of Service
TPC.....	True Point Code
TSET	Transmitter Signaling Element Timing
TSM.....	Translation Services Module
TSN	Transmission Sequence Number
TUP	Telephony User Part
TVG.....	Group Ticket Voucher feature
UA.....	User Adapter
UAM.....	Unsolicited Alarm Message
UAPS.....	User Adapter Parameter Set
UDP.....	User Datagram Protocol
UPU.....	User Part Unavailable message
XCA.....	Extended Changeover Acknowledgement
XCO.....	Extended Changeover
X-list.....	Exception list of non-provisioned members of provisioned cluster.

IP⁷ Secure Gateway Overview

Introduction.....	2-2
IP ⁷ Secure Gateway Hardware, Applications, and Functions	2-3
IP Connections	2-5
Point-to-Point Connectivity (IPLIM or IPLIMI Application).....	2-20
Point-to-Multipoint Connectivity (SS7IPGW and IPGWI).....	2-21
SNMP Agent Implementation	2-28
Mixed Networks Using the ANSI/ITU MTP Gateway Feature	2-32
Nagle's Algorithm	2-37
Type of Service (TOS)	2-37
ISUP Normalization	2-38
IETF Adapter Layer Support	2-46
Overview	2-46
Feature Components.....	2-48
SUA Layer	2-50
M3UA Layer.....	2-52
M2PA Layer.....	2-53
SCTP	2-54
Broader Definition of Connection Four-Tuple	2-54
Multiple Streams.....	2-55
Selective Acknowledgements	2-55

Un-order Delivery Capability2-56
Enhanced Security2-56
SCTP Connectivity Concepts2-56

Introduction

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

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

The IP⁷ Secure Gateway uses sockets or associations to access the IP domain. Sockets or associations identify IP sessions.

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

Address resolution is not performed in the IP to SS7 direction. It is the responsibility of the sending application to ensure that the appropriate SS7 point code information resides in the IP message to allow a valid SS7 message to be constructed for routing to the SS7 network.

IP⁷ Secure Gateway Hardware, Applications, and Functions

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

The IP card can run on the following applications:

- **iplim** or **iplimi** - Both applications support STP connectivity via MTP-over-IP functionality point-to-point connectivity (for more information, see “Connecting STPs Over the IP Network” on page 2-20).

The **iplim** and **iplimi** applications support these types of connections:

- TALI/TCP/IP (B, C, D links)
- M3UA/SCTP/IP (A and E links)
- M2PA/SCTP/IP (A, B, C, D, and E links)
- SCP
- SEP
- SCP/SEP

This type of connection is essentially the same as that of a traditional SS7 point-to-point link, except that the traditional MTP2 and 56Kb/s technology is replaced by IP and Ethernet technology.

The **iplim** application supports point-to-point connectivity for ANSI networks. The **iplimi** application supports point-to-point connectivity for ITU networks. With the optional ANSI/ITU MTP Gateway feature and proper configuration, the system could convert between any of the ANSI, ITU-N, and ITU-I networks, switch traffic between these networks, and perform network management for each of these networks (for more information, see “Mixed Networks Using the ANSI/ITU MTP Gateway Feature” on page 2-32).

The system can support up to 100 cards running the **iplim** and **iplimi** applications.

- **ss7ipgw** and **ipgwi** - These applications support the following types of point-to-multipoint connectivity for networks:
 - SCP connectivity via SCCP/TCAP-over-IP functionality (for more information, see “Connecting to SCPs with SCCP/TCAP Messages Sent Over the IP Network” on page 2-21)
 - SEP connectivity via ISUP, Q.BICC, and TUP-over-IP functionality (for more information, see “Connecting SEPs Using ISUP, Q.BICC, and TUP Messages Over the IP Network” on page 2-22)
 - SCP/SEP connectivity via non-ISUP, non-SCCP, non-Q.BICC, and non-TUP-over-IP functionality (for more information, see “Connecting SCPs and SEPs Using Non-ISUP, Non-SCCP, Non-Q.BICC, and Non-TUP Messages Over the IP Network” on page 2-23)

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

The system can support a maximum of 64 cards running the **ss7ipgw** and **ipgwi** applications.

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

- A Simple Network Management Protocol (SNMP) agent. For more information, see “SNMP Agent Implementation” on page 2-28.
- Message Transfer Part (MTP) status. This function is available only on IP cards that support the **ss7ipgw** or **ipgwi** application. For more information, see “Support for MTP Status Functions” on page 2-28.

IP Connections

IP connections involve the following assignments:

- Transport protocol – The SCTP transport protocol is specified by the **ent-assoc** and **chg-assoc** commands. The TCP transport protocol is specified by the **ent-appl-sock** and **chg-appl-sock** commands.
- Adapter protocol – The M3UA, M2PA, or SUA adapter protocol is specified by the **adapter** parameter of the **ent-assoc** and **chg-assoc** commands. If TCP sockets are provisioned with the **ent-appl-sock** and **chg-appl-sock** commands, the adapter protocol is implicitly defined as TALI.
- One or two near-end (local) hosts – The local host is specified by the **lhost** parameter of the **ent-assoc**, **chg-assoc**, **ent-appl-sock**, and **chg-appl-sock** commands. A second local host can be specified for an association using the **alhost** parameter of the **ent-assoc** and **chg-assoc** commands, allowing the near-end host of the association to be multi-homed. Specifying only one local host for an association allows the association to be uni-homed.
- Far-end (remote) host – The remote host is specified by the **rhost** parameter of the **ent-assoc**, **chg-assoc**, **ent-appl-sock**, and **chg-appl-sock** commands.
- Near-end (local) transport protocol port – The local transport protocol port is specified by the **lport** parameter of the **ent-assoc**, **chg-assoc**, **ent-appl-sock**, and **chg-appl-sock** commands.
- Far-end (remote) transport protocol port – The remote transport protocol port is specified by the **rport** parameter of the **ent-assoc**, **chg-assoc**, **ent-appl-sock**, and **chg-appl-sock** commands.
- SS7 signaling link – specified by the **loc** and **port** parameters of the **ent-slk** command.

The local host is mapped to a particular Ethernet interface on the IP card by linking the local host name of the IP connection to an IP address with the **ent-ip-host** command. The IP address is also assigned to an IP card and to an Ethernet interface on that IP card using the **chg-ip-lnk** command. A signaling link on that card is assigned to the IP connection using the **port** parameter of the **ent-assoc**, **chg-assoc**, **ent-appl-sock**, and **chg-appl-sock** commands and referencing the signaling link port on the IP card.

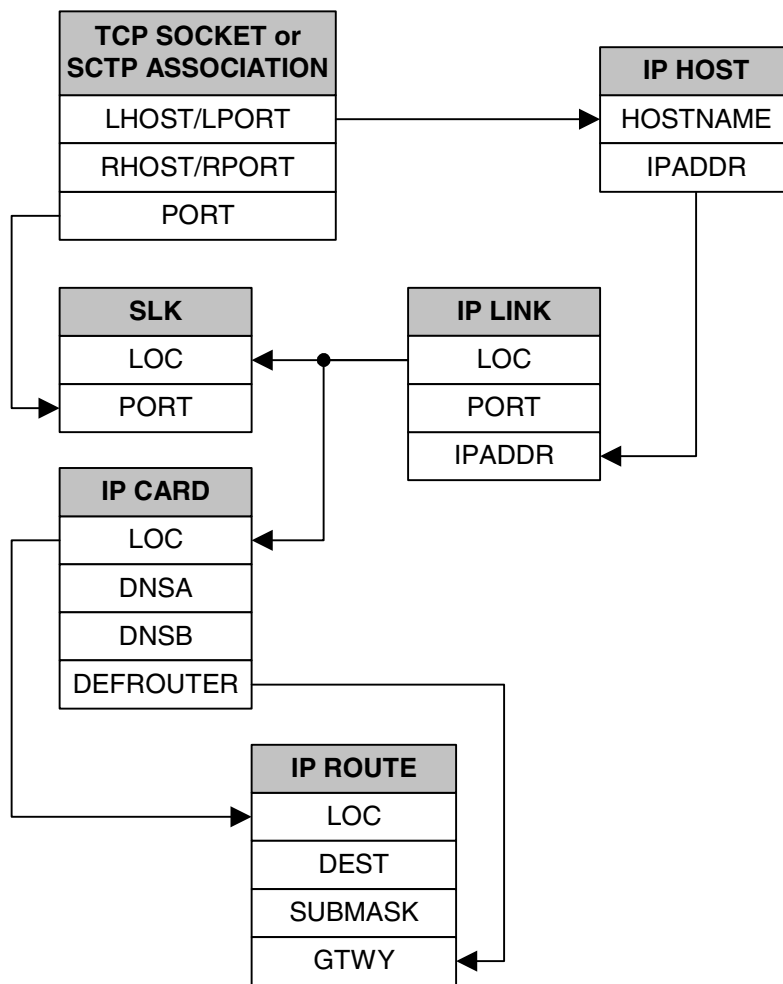
A TCP socket can establish a connection between one local host and one remote host. An SCTP association can establish a connection between one local host and one remote host (a uni-homed association) or between multiple local hosts and a remote host (a multi-homed association). It is possible that the remote host may be multi-homed, but the IP⁷ Secure Gateway allows only one remote host to be specified for a multi-homed association. If an IP node has multiple IP address

associated with it, then an SCTP association originating from this node may take advantage of this added connectivity by establishing an SCTP multi-homed association.

For more information on multi-homed associations, see the Multi-Homed SCTP Associations section on page 2-12 and the Routing section on page 2-17.

Figure 2-1 shows the components of a TCP socket or SCTP association and how these components interact with each other.

Figure 2-1. TCP socket or SCTP Association Database Relationships



There is no direct correlation between signaling link ports and Ethernet interfaces. A card can be using Ethernet interface A and signaling link port B to transmit data to the remote host. Another scenario could have the card using Ethernet interface B and signaling link port A to transmit data to the remote host.

The numbers of signaling link ports and Ethernet interfaces on IP cards varies depending on the card type and application running on the card, as shown in Table 2-1. The sections that follow Table 2-1 describe the IP connections supported by each IP card type. The IP connections described in these sections are either TCP sockets or uni-homed SCTP associations.

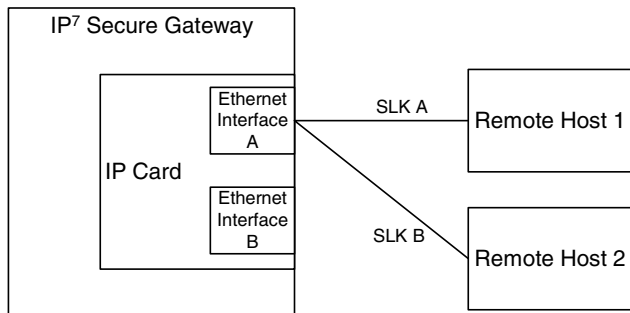
Table 2-1. Ethernet Interface and Signaling Link Port Combinations

Card	Application	Ethernet Interface	Signaling Link Port
Dual-Slot DCM	IPLIMx	A	A and B
	IPGWx	A	A
Single-slot EDCM (SSEDCM)	IPLIMx	A and B	A, B, A1, B1, A2, B2, A3 and B3
	IPGWx	A and B	A

IP Connection on a Dual-Slot DCM Running the IPLIMx Application

Dual-slot DCMs running the IPLIMx applications can have two signaling link ports (A or B) and only one Ethernet interface (A), as shown in Figure 2-2, resulting in a maximum of two IP connections, one for each signaling link, using Ethernet interface A.

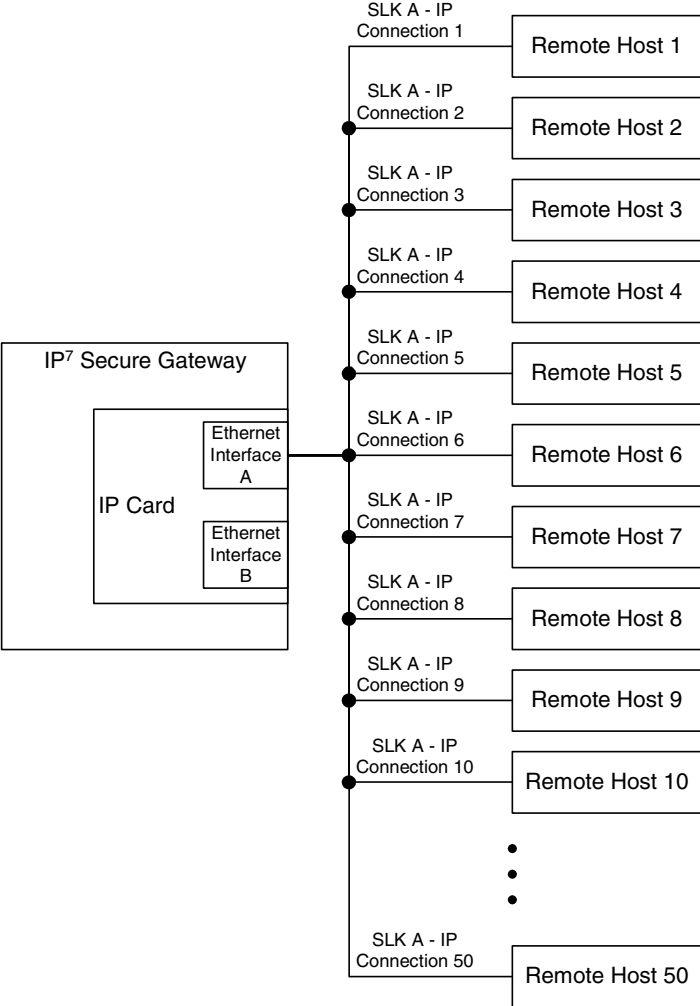
Figure 2-2. IP Connections using a Dual-Slot DCM running the IPLIMx Applications



IP Connection on a Dual-Slot DCM Running the IPGWx Application

Dual-slot DCMs running the IPGWx applications can have only one signaling link port (A) and one Ethernet interface (A). With this card able to support up to 50 IP connections, these 50 connections are established over Ethernet interface A, using signaling link port A, as shown in Figure 2-3.

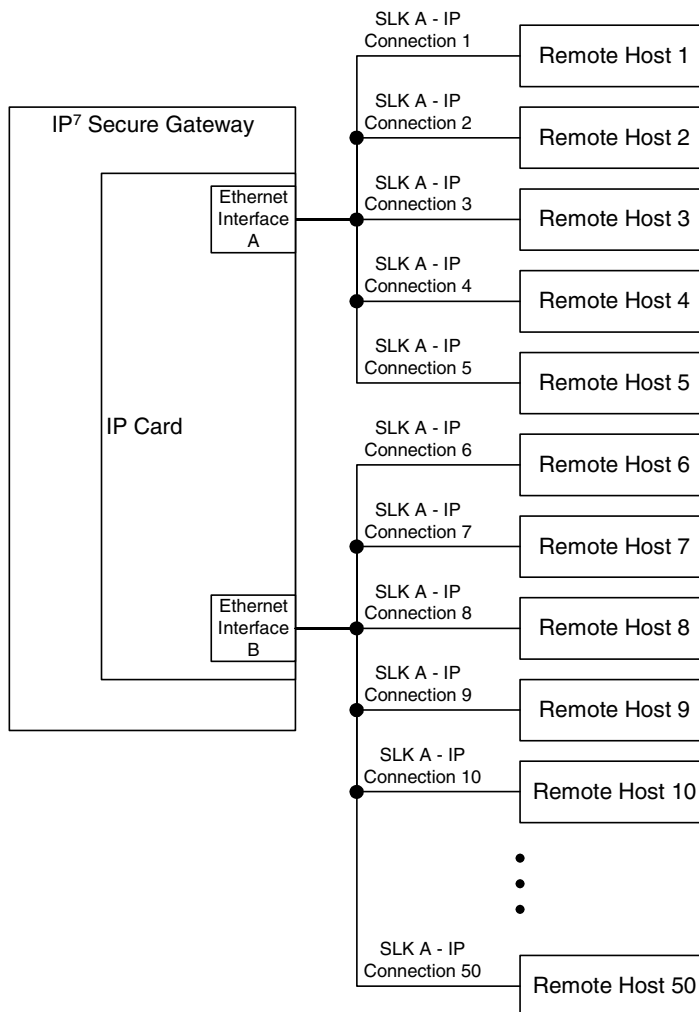
Figure 2-3. IP Connections using a Dual-Slot DCM running the IPGWx Applications



IP Connection on an EDCM Running the IPGWx Application

Single-slot EDCMs running the IPGWx applications can have only one signaling link port (A) and two Ethernet interfaces (A or B). With this card able to support up to 50 IP connections, these 50 connections can be established using both Ethernet interfaces A and B, as shown in Figure 2-4. The number of connections on each Ethernet interface can vary, but the total number connections on both interfaces cannot exceed 50. These 50 connections can also be established using only one Ethernet interface (A or B), if desired. Only signaling link port A is used for the signaling link.

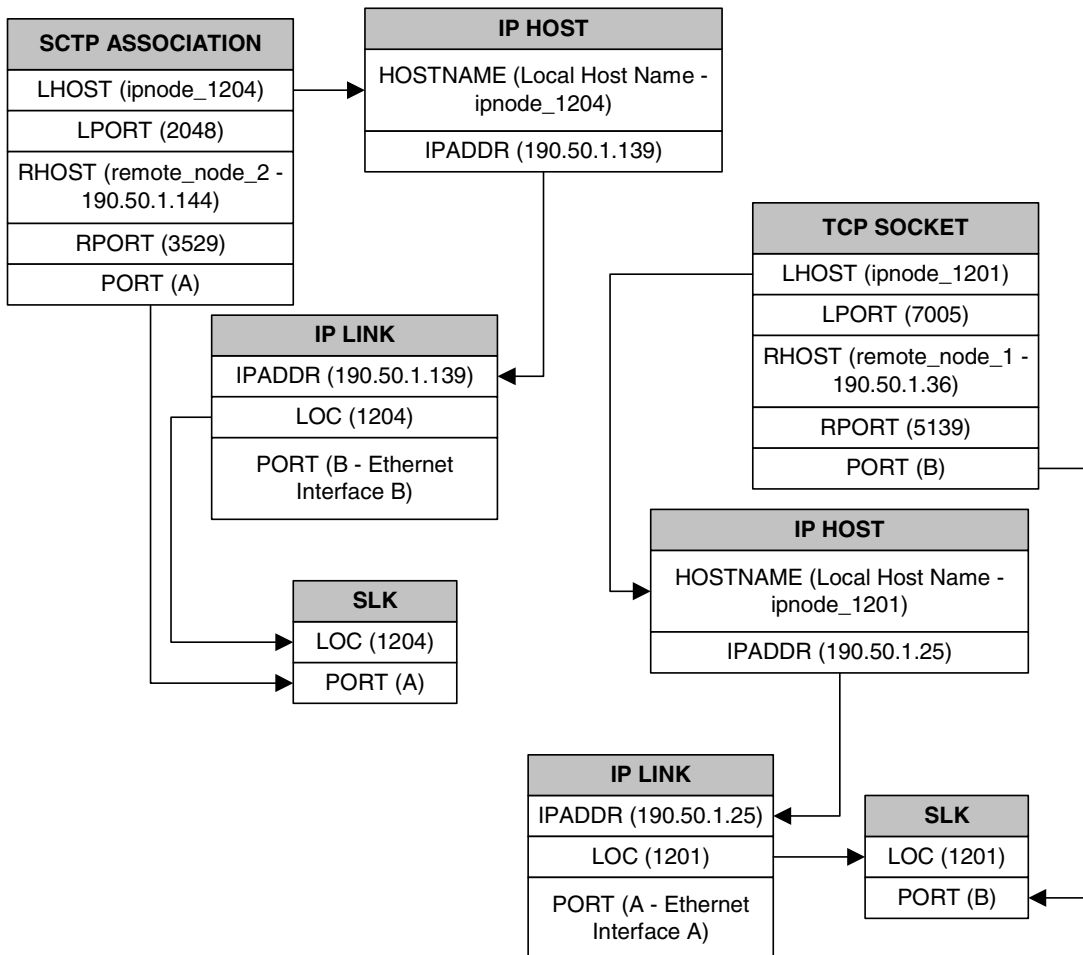
Figure 2-4. IP Connections using an EDCM running the IPGWx Applications



The assignment of the transport protocol (TCP or SCTP) port number is made through the local host port (**lport**) and remote host port (**rport**) parameters of the **ent-appl-sock** or **chg-appl-sock** commands (for a TCP socket), or the **ent-assoc** or **chg-assoc** commands (for an SCTP association). An IP card can have both TCP sockets and SCTP associations assigned to it at the same time. The transport protocol port numbers for TCP sockets are TCP ports. The transport protocol port numbers for SCTP associations are SCTP ports. Port numbers for one transport protocol have no relation to port numbers for the other transport protocol.

Figure 2-5 shows typical IP connection data for a uni-homed SCTP association and a TCP socket and how these components interact with each other.

Figure 2-5. Typical SCTP Association and TCP Socket Configuration

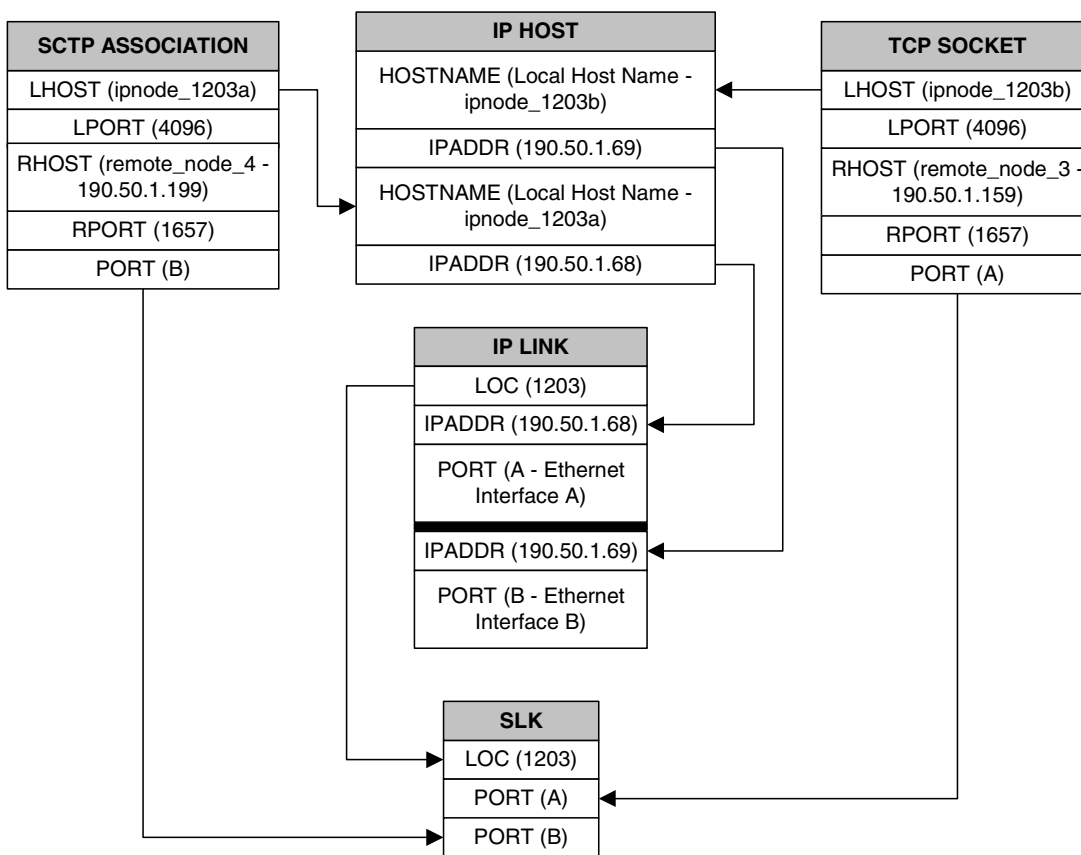


Using the data in Figure 2-5, the IP connection defined by the TCP socket is from local host ipnode-1201 (190.50.1.25), TCP port 7005, to remote host remote-node-1 (190.50.1.36), TCP port 5139, using Ethernet interface A on IP card 1201, and signaling link port B on IP card 1201.

The IP connection defined by the SCTP association is from local host ipnode-1204 (190.50.1.139), SCTP port 2048, to remote host remote-node-2 (190.50.1.144), SCTP port 3529, using Ethernet interface B on IP card 1204, and signaling link port A on IP card 1204.

In another scenario, IP card 1203 could contain a TCP socket and an SCTP association. The connection defined by the TCP socket is from local host ipnode-1203b (190.50.1.69), TCP port 4096, to remote host remote-node-3 (190.50.1.159), TCP port 1657, using Ethernet interface B on IP card 1203, and signaling link port A on IP card 1203. The connection defined by the SCTP association is from local host ipnode-1203a (190.50.1.68), SCTP port 4096, to remote host remote-node-4 (190.50.1.199), SCTP port 1657, using Ethernet interface A on IP card 1203, and signaling link port B on IP card 1203. This IP connection scenario is shown in Figure 2-6.

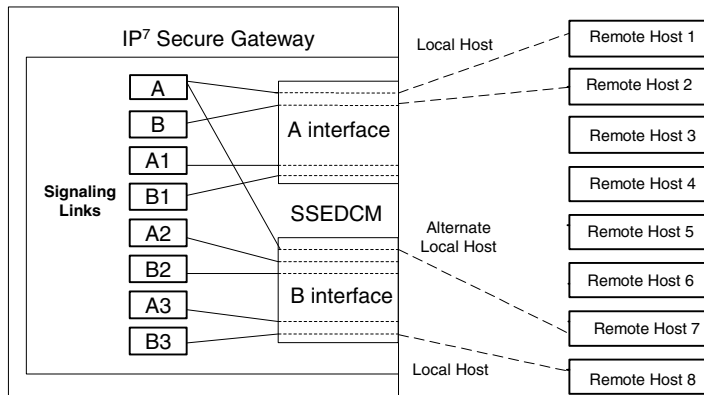
Figure 2-6. SCTP Association and TCP Socket on the Same IP Card



IP Connection on a Single-slot EDCM Running the IPLIMx Application

Single-slot EDCMs (SSEDCMs) running the IPLIMx applications can have 8 signaling link ports (A, B, A1, B1, A2, B2, A3 or B3) and 2 Ethernet interfaces (A or B) resulting in a maximum of 8 IP connections, one for each signaling link. Each link can use either Ethernet interface A or B. The local host and alternate host assigned to a signaling link must use different Ethernet interfaces; they cannot be assigned to the same Ethernet interface. Figure 2-7 shows some ways the 8 signaling links and the 2 Ethernet interfaces can be used to establish IP connections.

Figure 2-7. IP Connections using SSEDCMs running the IPLIMx Applications



Multi-Homed SCTP Associations

If the IP cards are EDCMs, SCTP associations can have two local hosts, and are referred to as multi-homed associations. A multi-homed association uses both Ethernet interfaces on the IP card. Each Ethernet interface is assigned to a local host. Each local host is assigned to a different local network. One of the local hosts is configured with the `lhost` parameter of the `ent-assoc` or `chg-assoc` commands. The second local host, or alternate local host, is configured with the `alhost` parameter of the `ent-assoc` or `chg-assoc` commands. One of the local hosts references one of the Ethernet interfaces on the IP card and the other local host references the other Ethernet interface on the IP card. The multi-homed SCTP association allows the EDCM to communicate with another node over two networks. Traffic is passed to and from the remote node on either local interface on the card.

An SCTP association can be uni-homed also. A uni-homed association uses only one Ethernet interface (A or B), which is assigned to only one local host. This local host is configured with the `lhost` parameter of the `ent-assoc` or `chg-assoc` commands. For a uni-homed association, the `alhost` parameter is not be specified with the `ent-assoc` or `chg-assoc` commands. A uni-homed association allows the IP card to communicate to another node on one network only. Traffic is passed to and from the remote node on the local interface on the card defined by the `lhost` parameter.

The remote node can be either uni-homed or multi-homed, and is not dependent on whether or not the local node (containing the local hosts) is uni-homed or multi-homed. For example, Node A can be uni-homed and can be connected to a multi-homed Node B, or a multi-homed Node A can be connected to a uni-homed Node B. Table 2-2 illustrates the possible combinations.

Table 2-2. Uni-Homed and Multi-Homed Node Combinations

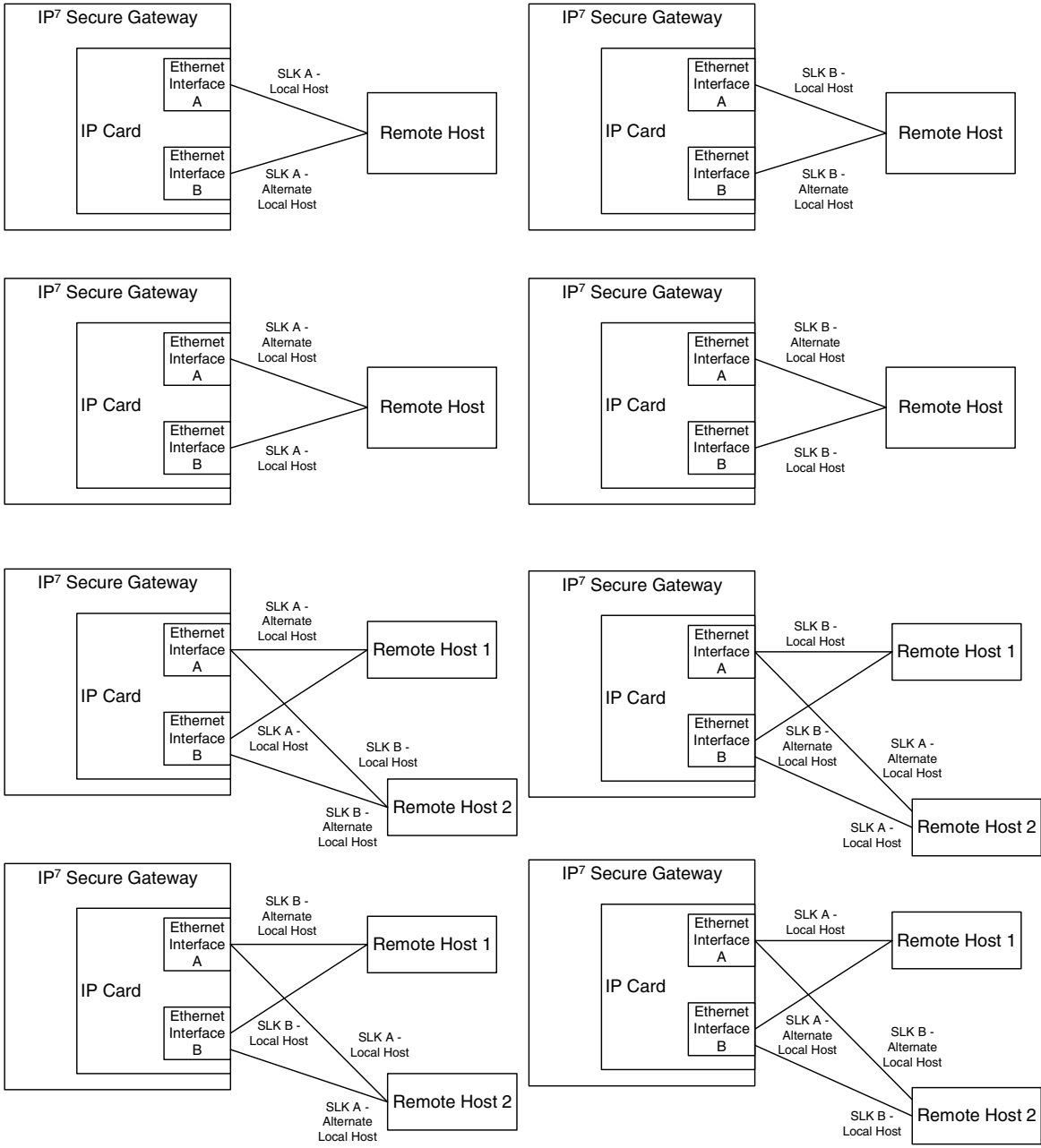
Node A	Node B
Uni-homed	Uni-homed
Uni-homed	Multi-homed
Multi-homed	Uni-homed
Multi-homed	Multi-homed

Multi-Homed Associations on EDCMs Running the IPLIMx Application

A multi-homed association on an IPLIMx card uses both Ethernet interfaces to reach the remote host, but only one signaling link. An association, either uni-homed or multi-homed, can be assigned to only one signaling link. That signaling link can be either signaling link port A or B. The local and alternate local hosts are assigned to each Ethernet interface on the IP card. The IPLIMx cards are limited to one IP connection per signaling link. Since the IPLIMx cards can have two signaling links on the card, two multi-homed associations can be assigned to an IPLIMx card.

Figure 2-8 shows the ways a multi-homed IP connection can be established on an IPLIMx card. The remote hosts can be multi-homed, but only one remote host can be specified for each multi-homed association in the IP⁷ Secure Gateway, so only one remote host is shown in Figure 2-8.

Figure 2-8. Multi-Homed Associations on EDCMs running the IPLIMx Applications



Multi-Homed Associations on EDCMs Running the IPGWx Applications

A multi-homed association on an IPGWx card uses both Ethernet interfaces to reach the remote host, but only one signaling link, signaling link port A on the IPGWx card. The local and alternate local hosts are assigned to each Ethernet interface on the IP card. The IPGWx cards can have up to 50 connections for each IPGWx card. The IPGWx card can contain both uni-homed and multi-homed IP connections, as long as the total number of connections does not exceed 50.

Figure 2-9 shows the way a multi-homed IP connection can be established on an IPGWx card. The remote hosts can be multi-homed, but only one remote host can be specified for each multi-homed association IP⁷ Secure Gateway, so only one remote host is shown in Figure 2-9.

Figure 2-9. Multi-Homed Associations on EDCMs running the IPGWx Applications

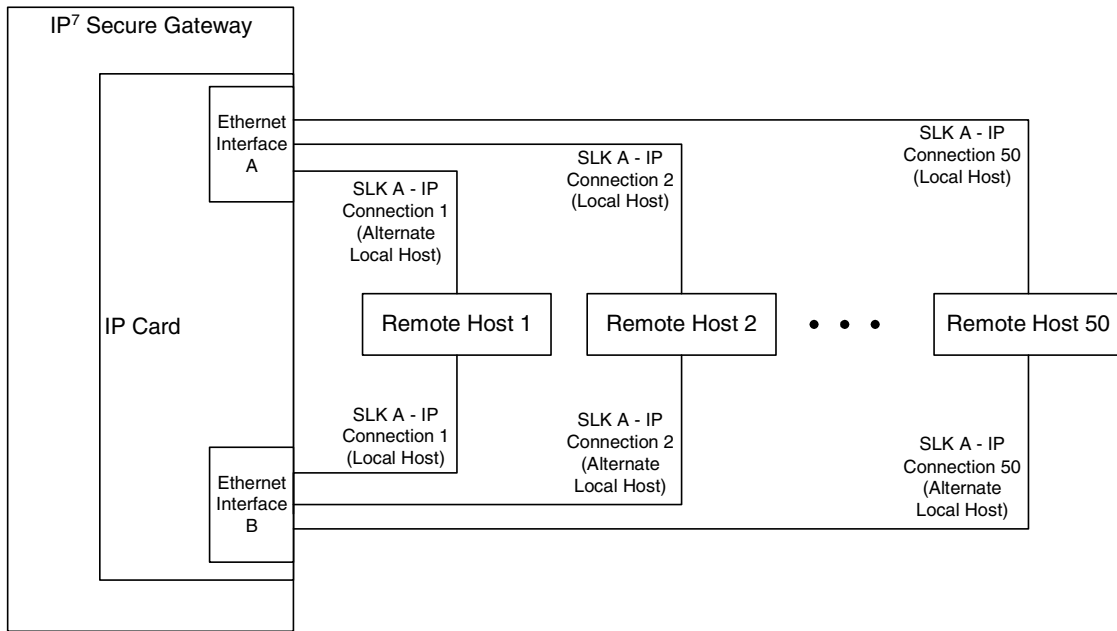
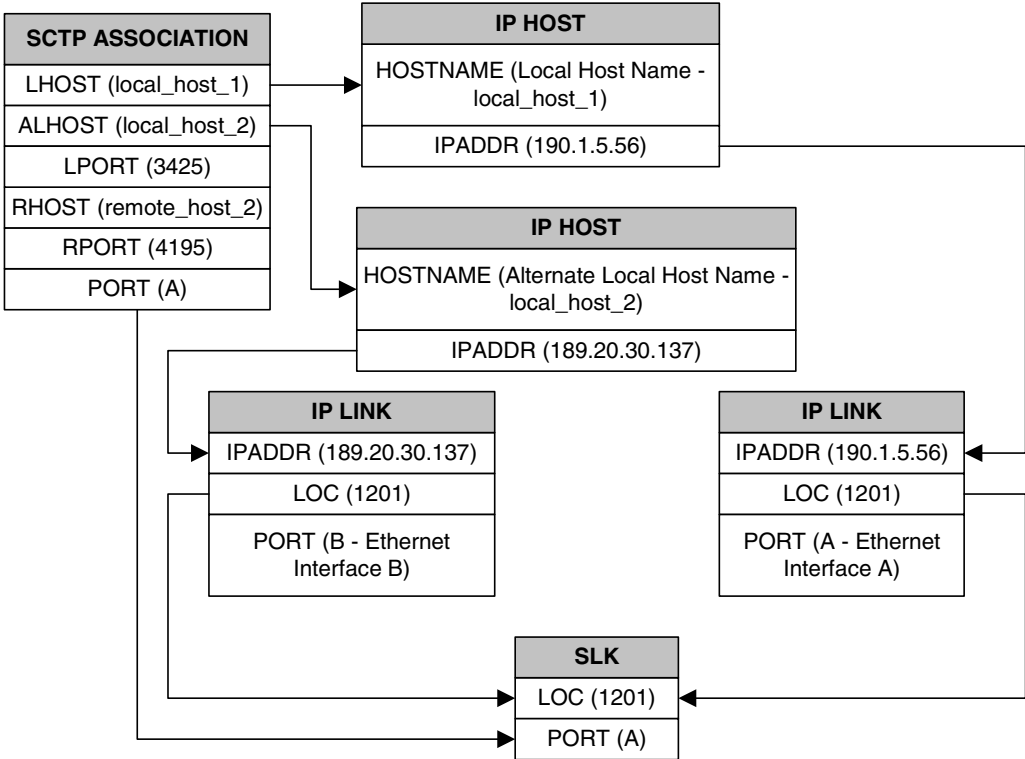


Figure 2-10 shows the components of the multi-homed SCTP association and how these components interact with each other.

Figure 2-10. Multi-Homed Association Database Relationships



Using the data shown in Figure 2-10, the IP connection is defined as a multi-homed association, connecting to a remote host using local hosts 190.1.5.56 and 189.20.30.137 over Sctp port 3425, using signaling link port B on card 1201.

Routing

The IP⁷ Secure Gateway supports two transport protocols – TCP and SCTP. Although both transport protocols are connection oriented, they differ greatly with respect to operation in a multi-homed host environment. The TCP protocol provides for a point-to-point transport connection. The SCTP protocol implements connections with either point to point, point to multi-point, or multi-point to multi-point connectivity capabilities.

A TCP socket connection is defined by an explicit four-tuple – a local IP address, local TCP port, remote IP address and remote TCP port. Once the local IP address is determined for a TCP connection, it binds all subsequent transmissions to this specific IP interface. Once an IP interface is selected for a TCP connection, the TCP connection will fail if the remote host becomes unreachable by this interface. This connection failure occurs on a multi-homed host even if the remote host can still be reached by a different IP interfaces of the multi-homed host.

An SCTP IETF connection – association – has a broader definition than TCP with respect to a multi-homed host. An SCTP IETF association is defined as a four-tuple as follows:

- local host list – one or more of the local host's IP interface addresses
- local SCTP port
- remote host list – one or more of the remote host's IP interface addresses
- remote SCTP port.

Based on this definition for an SCTP IETF connection, and the fact that the IPGWx and IPLIMx applications may utilize both Ethernet interfaces (a multi-homed host), an SCTP IETF association can take advantage of multi-homing and be a multi-homed SCTP endpoint. As a multi-homed endpoint, an SCTP IETF connection remains active and usable as long as at least one of the Ethernet interfaces can be reached by the remote host. Multiple paths through multiple interfaces to the remote host provides a more reliable connection. Thus where a TCP connection would be lost, and if possible, a new one established by the application, the SCTP IETF protocol is designed to make such a network outage transparent to the application.

In previous releases, an SCTP IETF endpoint could only operate as a uni-homed host using only the Ethernet A interface. In this mode, any SCTP transmission received on or transmitted out of the Ethernet B interface are silently discarded. By using the Ethernet B interface, the SCTP protocol running on the IP card can provide SCTP multi-homing endpoint support – that is, when an SCTP IETF association is formed, it may list both the Ethernet A and B IP addresses for the respective interfaces. As a multi-homed association endpoint, SCTP data would be allowed to flow on either of the Ethernet interfaces and thus provide more robust network connectivity.

In order to provide more flexible network connectivity, an association can be configured as follows with respect to the Ethernet interfaces:

- Ethernet A interface only (uni-homed)
- Ethernet B interface only (uni-homed)
- Ethernet A and B interface (multi-homed).

The interface mode is specified by the **lhost** and **alhost** parameters of the **ent-assoc** or **chg-assoc** commands.

In previous releases, the **lhost** parameter of the **ent-assoc** or **chg-assoc** commands is used to define the local IP address of the SCTP IETF association endpoint. The IP address would have to be an IP address associated with an Ethernet A interface. With this release, the IP address may be associated with either the Ethernet A or B interfaces. If it is an Ethernet A interface IP address, and the **alhost** parameter is not specified, then the association operates as a uni-homed SCTP endpoint on Ethernet interface A. If it is an Ethernet B interface IP address, and the **alhost** parameter is not specified, then the association operates as a uni-homed SCTP endpoint on Ethernet interface B. An association is configured as an SCTP multi-homed endpoint by specifying both the **lhost** and **alhost** parameter values with values corresponding to the Ethernet interface IP address for the IP card. The **lhost** and **alhost** parameter values represent the IP addresses specified by the **chg-ip-lnk** command for the specific IP card. Traffic cannot be passed between the Ethernet interfaces on the IP card containing a multi-homed SCTP association. The IP card cannot act as an IP router between the networks defined by the local host and alternate local hosts of a multi-homed association.

A host that is not on the local network, the network identified by the local host's IP address, can be reached only through a gateway router. A gateway router is a device with more than one physical network connection, and can be connected to multiple networks. Unlike a multi-homed host, a gateway router is permitted to route IP messages between the physical Ethernet interfaces on the IP card. The network portion of the gateway router's IP address must be the same as the network portion of the IP address of one of the IP addresses of the Ethernet interfaces on the IP card. The gateway router is configured using the **defrouter** of the **chg-ip-card** command, or using the **ent-ip-rte** command.

Static entries are added to the IP Routing table using the **ent-ip-rte** command. Static routes are usually assigned to give control over which routers are used, allowing different routers to be selected based upon the destination IP address. There are two types of static routes:

- host static IP routes
- network or subnetwork static IP routes.

The default route entry is a special static route. If there is not a specific host or network address in the IP Routing table that matches the destination IP address of an outbound datagram, then the datagram is sent to the default router (gateway) specified by the default route.

An IP route is configured using the `ent-ip-rte` command with the location of the IP card, the IP address of the gateway router (the `gtwy` parameter), and the IP address and subnet mask of the destination (that is, host or network). The IP address of the gateway router must be a locally attached IP address (that is, the gateway IP address must share the network portion of one of the two Ethernet interfaces).

When an IP packet is to be transmitted the IP routing table must be interrogated to determine where to send the IP datagram. If the destination IP address is local to the node (that is, directly reachable by an Ethernet interface), then the IP datagram is transmitted directly to the node with that associated IP address. If the destination IP address is determined to not be local to the node, then it must be routed (that is, sent to a gateway to reach its destination).

IP routing requires accessing the IP routing table to select a route. The destination IP address of the outbound datagram is used to search the IP routing table for the most specific route match. The order for selection is:

1. Host route
2. Subnetwork route
3. Network route
4. Aggregated route
5. Default route.

Based on this selection order if an IP route is found then the outbound IP datagram will be transmitted to the gateway specified by the route. If no IP route is found (where no default route is specified), then the transmission of the datagram fails due to destination unreachable.

The capability to enter static IP routes provides for flexibility and control with respect to controlling network traffic. An IP card can contain up to 64 IP routes. The system can contain up to 1024 IP routes.

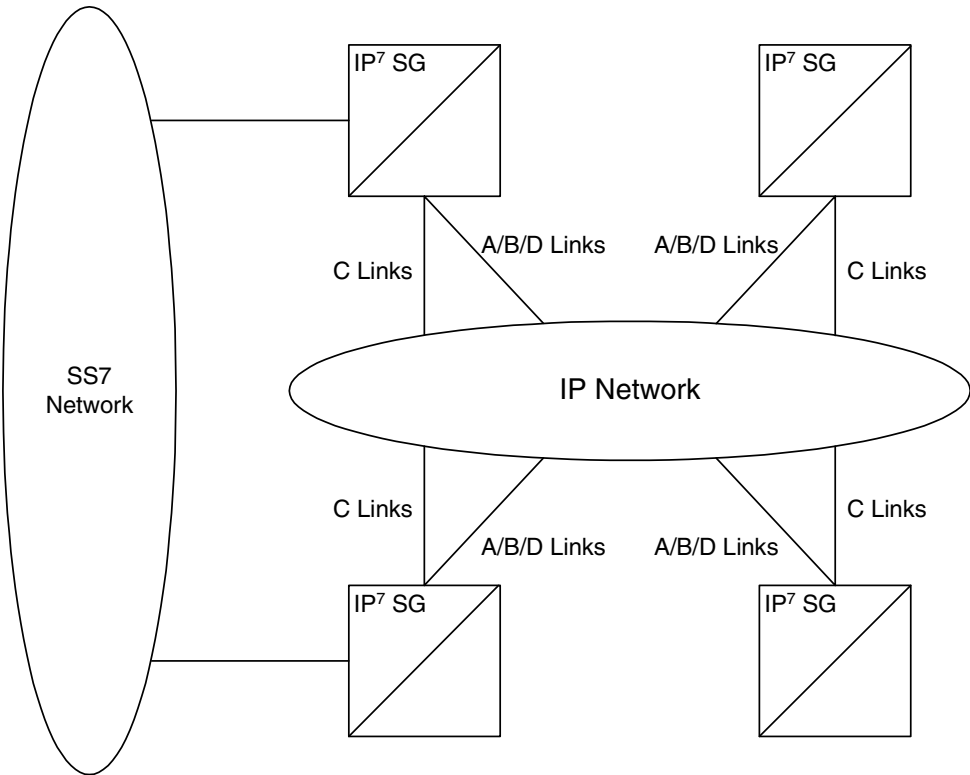
Point-to-Point Connectivity (IPLIM or IPLIMI Application)

The following sections describe the types of point-to-point connectivity provided, and how routing is accomplished, by the `iplim` or `iplimi` application:

Connecting STPs Over the IP Network

This functionality allows the use of an IP network in place of point-to-point SS7 links to carry SS7 MSUs. Figure 2-11 shows a diagram of this type of network. For example, the C links between the mated pair of STPs or A/B/D links between STPs can be replaced by an IP network. The IP⁷ Secure Gateway functionality is deployed on both ends of the link (point-to-point connection). The IP⁷ Secure Gateway converts the SS7 MSUs to IP packets on one end of the link, and IP packets to SS7 MSUs on the other end of the link. The IPLIMx applications supports the TALI/TCP/IP sockets over B, C, and D links, the M3UA/SCTP/IP associations over A and E links, and M2PA/SCTP/IP associations over A, B, C, D, and E links.

Figure 2-11. IP⁷ Secure Gateway Network (STP Connectivity via MTP-over-IP)



Point-to-Multipoint Connectivity (SS7IPGW and IPGWI)

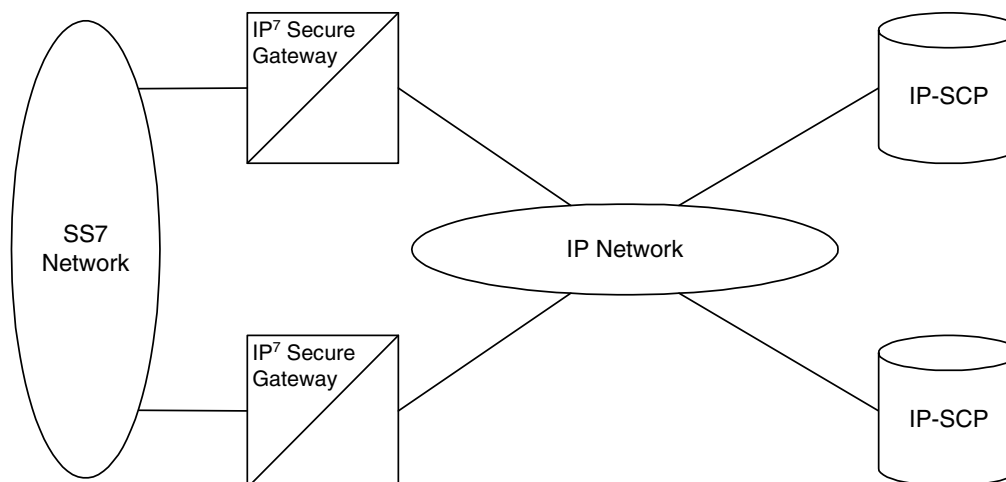
The following sections describe the types of point-to-multipoint connectivity, how routing is accomplished, and the MTP status functions provided by the `ss7ipgw` and `ipgwi` applications:

- “Connecting to SCPs with SCCP/TCAP Messages Sent Over the IP Network” on page 2-21
- “Connecting SEPs Using ISUP, Q.BICC, and TUP Messages Over the IP Network” on page 2-22
- “Connecting SCPs and SEPs Using Non-ISUP, Non-SCCP, Non-Q.BICC, and Non-TUP Messages Over the IP Network” on page 2-23
- “Understanding Routing for SS7IPGW and IPGWI Applications” on page 2-23
- “Support for MTP Status Functions” on page 2-28

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

This functionality allows SS7 nodes to exchange SCCP/TCAP queries and responses with an SCP residing on an IP network. Figure 2-12 shows a diagram of this type of network.

Figure 2-12. IP Network (SCP Connectivity via TCAP-over-IP)



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

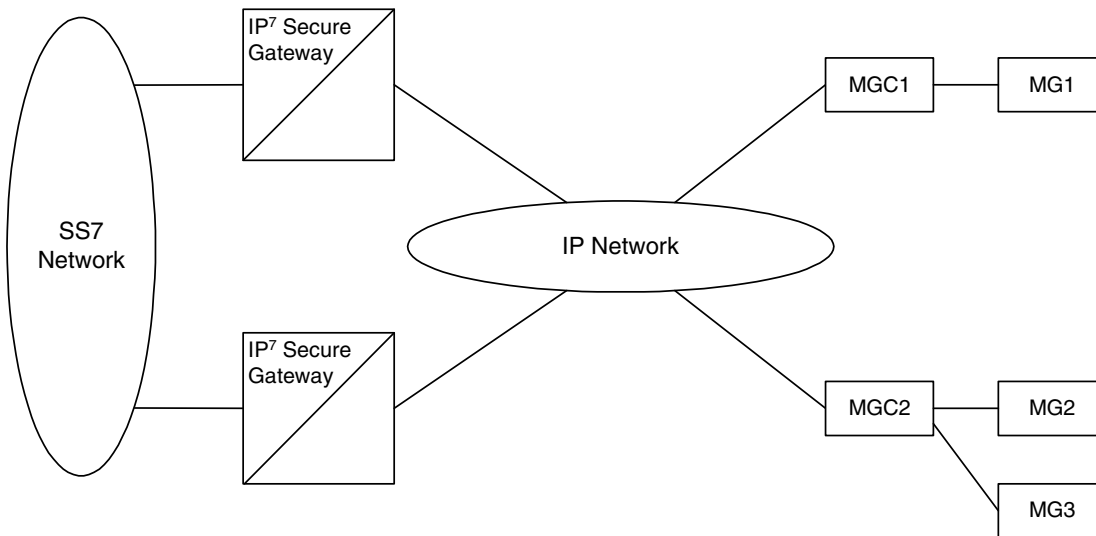
The following sequence of events illustrates this functionality:

1. Traditional SS7 devices route MSUs (such as TCAP Queries) to the system.
2. The system performs a global title translation and forwards the translated MSU to the correct 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 system.
4. The system forwards the TCAP reply back to the sender of the original query.

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

This point-to-multipoint functionality allows SS7 nodes to exchange ISUP, Q.BICC, and TUP protocol messages with one or more signaling end points (class 4 switches, class 5 switches, VoIP gateways, Media Gateway Controllers, or Remote Access Servers) residing on an IP network. Figure 2-13 shows an example of this type of network.

Figure 2-13. IP Network (SEP connectivity via ISUP, Q.BICC, and TUP-over-IP)



The system maps the originating point code, destination point code, and circuit identification code to an IP connection. The SEP is provided the originating and destination point codes in the MTP level 3 routing label as part of the passed protocol.

Connecting SCPs and SEPs Using Non-ISUP, Non-SCCP, Non-Q.BICC, and Non-TUP Messages Over the IP Network

This point-to-multipoint functionality allows SS7 nodes to exchange non-ISUP, non-SCCP, non-Q.BICC, and non-TUP protocol messages with one or more IP-based devices residing on an IP network. The network example is similar to the SCP connectivity via SCCP/TCAP-over-IP functionality example shown in Figure 2-12. The system maps the destination point code, and service indicator (non-ISUP, non-SCCP, non-Q.BICC, non-TUP) to an IP connection.

Understanding Routing for SS7IPGW and IPGWI Applications

The `ss7ipgw` and `ipgwi` applications can use a single point code, called a virtual point code. This code is assigned to a set of IP devices that it connects to. The system distinguishes between the devices within the set by using application routing keys and application sockets or application servers.

Application routing associates SS7 routing keys with sockets or application servers. SS7 routing keys define a filter based on SS7 message data. Application sockets or application servers define the connection between the IP local host/local transport protocol port and IP remote host/remote transport protocol port.

An application server is a logical entity serving a specific routing key. The application server contains a set of one or more unique application server processes, of which one or more is normally actively processing traffic. An application server process is a process instance of an application server and contains an SCTP association. For more information on application servers, application server processes, and SCTP associations, see the IETF Adapter Layer Support section on page 2-46.

If the routing key filter matches the SS7 message presented for routing to the IP network, the SS7 message is sent to the associated application socket or application server.

There may be up to 16 application sockets or one application server associated with each SS7 routing key. One application server can have up to 16 associations. SS7 messages delivered to the IP network using a routing key are distributed over the available application sockets or application server based on the SLS (signaling link selector) value in the SS7 message.

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

Full Routing Keys

For this routing application, all applicable fields in the Message Signaling Unit (MSU) must match the contents of the full routing key. Table 2-3 defines which SS7 message parameters are used to search for a match for full routing keys for each of the functions supported by the `ss7ipgw` and `ipgwi` applications (IPGWx functionality).

Table 2-3. SS7 Full Routing Keys per IPGWx Functionality

IPGWx Functionality (ANSI and ITU)	SS7 Routing Keys
SCP connectivity via TCAP-over-IP	Destination Point Code Service Indicator (=3) Subsystem Number
SEP connectivity via ISUP-over-IP	Destination Point Code Service Indicator (=5) Originating Point Code CIC Range Start CIC Range End
SEP connectivity via Q.BICC-over-IP	Destination Point Code Service Indicator (=13) Originating Point Code CIC Range Start CIC Range End
SEP connectivity via TUP-over-IP (ITU only)	Destination Point Code Service Indicator (=4) Originating Point Code CIC Range Start CIC Range End
SCP/SEP connectivity via non-ISUP, non-SCCP, non-Q.BICC, non-TUP-over-IP	Destination Point Code Service Indicator (any value other than 3, 4*, 5, and 13)
* The service indicator value of 4 can be used in this instance if the DPC is an ANSI point code.	

Partial Routing Keys

Partially specified routing keys are explicitly, but not completely defined. These routing keys ignore some of the contents of the MSU. The parts of the MSU that are ignored are specific. For example, for the 'ignore `cic`' partial-key type, the destination point code (`dpc`), service indicator (`si`), and originating point code (`opc`) must be configured, but the circuit identification code (`cic`) field does not have to be configured. The other types of SS7 partial routing keys are as follows:

- `dpc`, `si`, and `opc` specified (ignore `cic` for CIC-based messages)
- `dpc` and `si` specified (ignore `ssn` for `sccp` messages)
- `dpc` and `si` specified (ignore `opc` and `cic` for CIC-based messages)
- `dpc` specified (ignore all but the `dpc` field)
- `si` specified (ignore all but the `si` field)

Default Routing Keys

Default routing keys do not need any part of the MSU specified. This routing key can be used to carry any SS7 MSU, regardless of the type of MSU or the fields that make up the MSU. The IP⁷ Secure Gateway can support two default routing keys, one created by administrative commands and one entered by Dynamic Routing Key Registration.

Routing Key Tables

Each IP card has a Routing Key table that maps SS7 routing keys to IP connections, as illustrated by the example in Table 2-4. MSUs that match the parameters in a given row are sent over one of the IP connections shown for that row (up to 16 IP connections can be defined for a single routing key). Multiple IP connections for a given row allow load sharing. In addition, multiple routing keys can be used to send traffic to a single IP connection.

Each IP card's Routing Key table can contain up to 1000 entries (if there are any dual-slot DCM cards) or 2500 entries (if all IP cards are SSEDCM cards). Entries in the Routing Key table can be either of the following:

- **Static** — these entries are defined by the user using the `ent-appl-rtkey` command entered through the OAM, saved on disk, and reloaded to each IP card upon reset. Static entries can be full, partial, or default routing keys. The static entries in one IP card's Routing Key table are identical to the static entries in the other IP card's table. Static entries can be changed by the `chg-appl-rtkey` command or deleted by the `dlr-appl-rtkey` command.
- **Dynamic** — these entries are added to or deleted from the table when a remote computer sends a message to the system. Dynamic entries allow an IP connection to automatically direct traffic towards, or away from, itself. A dynamic entry can have the same parameters as a static entry and can be full, partial, or default routing keys. When the `ss7ipgw` or `ipgwi` application transmits an MSU, it looks for a matching dynamic entry before looking for a

static entry. When an IP connection fails, all dynamic entries associated with the IP connection are deleted. The dynamic entries in one IP card's Routing Key table may differ from the other IP card's table depending on messages received from other IP nodes. Dynamic entries can be deleted by receipt of a message from the IP connection, by failure of the IP connection, or by the `dlt-appl-rtkey` command.

Table 2-4 shows a sample Routing Key table that has one static entry and one dynamic entry for an SSCP/TCAP-over-IP connection; one static entry each for an ISUP, Q.BICC, and TUP-over-IP connection; and a non-SSCP/non-ISUP/non-Q.BICC/non-TUP connection.

Table 2-4. Example SS7 Routing Key Table

Location	SS7 Routing Keys						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							
Static	5-5-5	03	6	-	-	-	kchlr11201 kchlr21201 kchlr11203 kchlr21203
1105	5-5-5	03	6	-	-	-	kchlr31205 kchlr41205
ISUP-CIC routing key for ISUP-over-IP connectivity							
Static	5-5-6	05	-	4-4-4	1	100	dnmsc11201 dnmsc21201 dnmsc11203 dnmsc21203
Q.BICC-CIC routing key for Q.BICC-over-IP connectivity							
Static	4363	13	-	5834	48486	48486	lpmsg11204 lpmsg21204 lpmsg31204
TUP-CIC routing key for TUP-over-IP connectivity							
Static	1-44-2	04	-	2-5-1	3948	3948	lpmsg11205 lpmsg21205 lpmsg31205
DPC-SI routing key for non-SSCP/non-ISUP/non-Q.BICC/non-TUP connectivity							
Static	5-5-7	02					sfh1r11204

Routing Key Lookup Hierarchy

To facilitate the delivery of Message Signaling Units (MSUs) that do not match full routing key entries in the Routing Key table, each MSU is processed and delivered according to a specific routing key lookup hierarchy. The hierarchy guarantees that the MSU is delivered to the best possible location based on the MSU's closest match in the Routing Key table, and also prevents MSUs without full routing key matches from being discarded. Table 2-5 defines the routing key lookup hierarchy.

Table 2-5. Routing Key Lookup Hierarchy

Type of MSU	Lookup Order per MSU Type	Segment of MSU that Must Match Routing Key	Routing Key Type
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
SCCP	1	dpc + si + ssn	Full
	2	dpc + si (ignore ssn)	Partial
	3	dpc (ignore si & ssn)	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

When an MSU has an **si** value of 5, 13, or 4 (ITU only), it is a CIC message. Messages with an **si** value of 3 are SCCP messages. All other MSUs are considered OtherSI messages. The system first tries to match each MSU with a full routing key and second with one of the partial keys as numbered in ascending order in the table. Third, if no segment of the routing key matches either full or partial routing keys, the system assigns the MSU a default routing key.

Support for MTP Status Functions

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

This feature enables an IP device to:

- Divert traffic from a secure gateway that is not able to access a point code that the mated secure gateway can access
- Audit point code status
- Build up routing tables before sending traffic
- Be warned about network congestion
- Abate congestion (`ss7ipgw` application only)
- Obtain SS7 User Part Unavailability status

SNMP Agent Implementation

This feature implements a Simple Network Management Protocol (SNMP) agent on each IP card that runs the `ss7ipgw`, `ipgwi`, `iplim`, or `iplimi` applications. 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 IP card. These variables are called managed objects and are stored in a management information base (MIB). The SNMP protocol arranges managed objects into groups. Table 2-6 on page 2-29 shows the groups that are supported.

Table 2-6. SNMP Object Groups

Group Name	Description	Contents
<i>system</i>	Text description of agent in printable ASCII characters	System description, object identifier, length of time since reinitialization of agent, other administrative details
<i>interfaces</i>	Information about hardware interfaces on the IP card	Table that contains for each interface, speed, physical address, current operational status, and packet statistics
<i>ip</i>	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
<i>icmp</i>	Intranetwork control messages, representing various ICMP operations within the IP card	26 scalar objects that maintain statistics for various Internet Control Message Protocol (ICMP) messages
<i>tcp</i>	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
<i>udp</i>	Information about UDP operation	4 scalar objects that maintain UDP-related datagram statistics, and a table that contains address and port information
<i>snmp</i>	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 IP card.
- Responding to *Set* commands sent from an NMS for maintaining the IP card and changing managed objects as specified.
- Sending *Trap* messages to asynchronously notify an NMS of conditions such as a link going up or down. *Traps* provide a way to alert the NMS in a more

timely fashion than waiting for a *Get* or *GetNext* from the NMS. Two hostnames, DCMSNMPTRAPHOST1 and DCMSNMPTRAPHOST2, are utilized to specify the SNMP NMS to which traps are sent. In this release, only the following traps are supported:

- *coldStart*, sent one time only when the IP stack initialization occurs on the IP card as part of boot processing
- *linkUp*, sent when one of the ports on the IP card initially comes up or recovers from a previous failure
- *linkDown*, sent when one of the ports on the IP card fails

When a trap occurs at the IP card agent, the agent sends the trap to each of the SNMP specific host names that can be resolved to an IP address. Resolution is based on configuration data in the **chg-ip-card** command (or default data) which specifies DNS search order and DNS information.

Deviations from SNMP Protocol

Table 2-7 on page 2-31 shows how the system deviates from the standard SNMP protocol definition.

Table 2-7. Deviations from SNMP Protocols

Group	Variable Name	Usage	Deviation
<i>system</i>	<i>sysContact</i>	Text identification of contact information for agent	Cannot be set by <i>Set</i> command; may be set only by chg-sg-opts command.
	<i>sysLocation</i>	Physical location of agent	Cannot be set by <i>Set</i> command; internally set using configuration data already available; set to <CLLI>-<slot of IP card>
	<i>sysName</i>	Administratively assigned name for agent	Cannot be set by <i>Set</i> command; internally set using configuration data already available; set to <CLLI>-<slot of IP card>
<i>interface</i>	<i>ifAdminStatus</i>	Desired state of the interface	Cannot be set by <i>Set</i> command (to ensure that an NMS does not disrupt SS7 traffic by placing an IP interface in a nonoperable state)
<i>ip</i>	<i>ipForwarding</i> <i>ipDefaultTTL</i> <i>ipRoute Dest</i> <i>ipRouteIfIndex</i> <i>ipRouteMetric1-5</i> <i>ipRouteNextHop</i> <i>ipRouteType</i> <i>iprouteAge</i> <i>ipRouteMask</i>	IP route-specific values	Cannot be set by <i>Set</i> command
	<i>ipNetToMediaIfIndex</i> <i>ipNetToMediaPhysAdress</i> <i>ipNetToMediaNetAddress</i> <i>ipNetToMediaType</i>	IP-address specific information	Can be set by <i>Set</i> command, but not saved across IP card reloads
<i>tcp</i>	<i>tcpConnState</i>	State of a TCP connection	Cannot be set by <i>Set</i> command
<i>snmp</i>	<i>snmpEnableAuthenTraps</i>	Indicate whether agent is permitted to generate authentication failure traps	Cannot be set by <i>Set</i> command

Mixed Networks Using the ANSI/ITU MTP Gateway Feature

The optional ANSI/ITU MTP Gateway feature, now also available for IP networks, and the addition of the `iplimi` and `ipgwi` applications enables the IP⁷ Secure Gateway to act as an interface between nodes that support ANSI, ITU-I, and ITU-N protocols. For more information on the ANSI/ITU MTP Gateway feature, contact your Tekelec Sales Representative.

Figure 2-14 on page 2-33 shows an example of a complex network that includes all these types of nodes. Table 2-8 on page 2-34 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.
- The systems are usually deployed as mated pairs. The links connecting the system to its mate are C links. Each system must have a C linkset for each network type that the system connects to. Therefore, in Figure 2-14 on page 2-33, 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 system 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 system 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 2-14. Complex Network with ANSI, ITU-I, and ITU-N Nodes

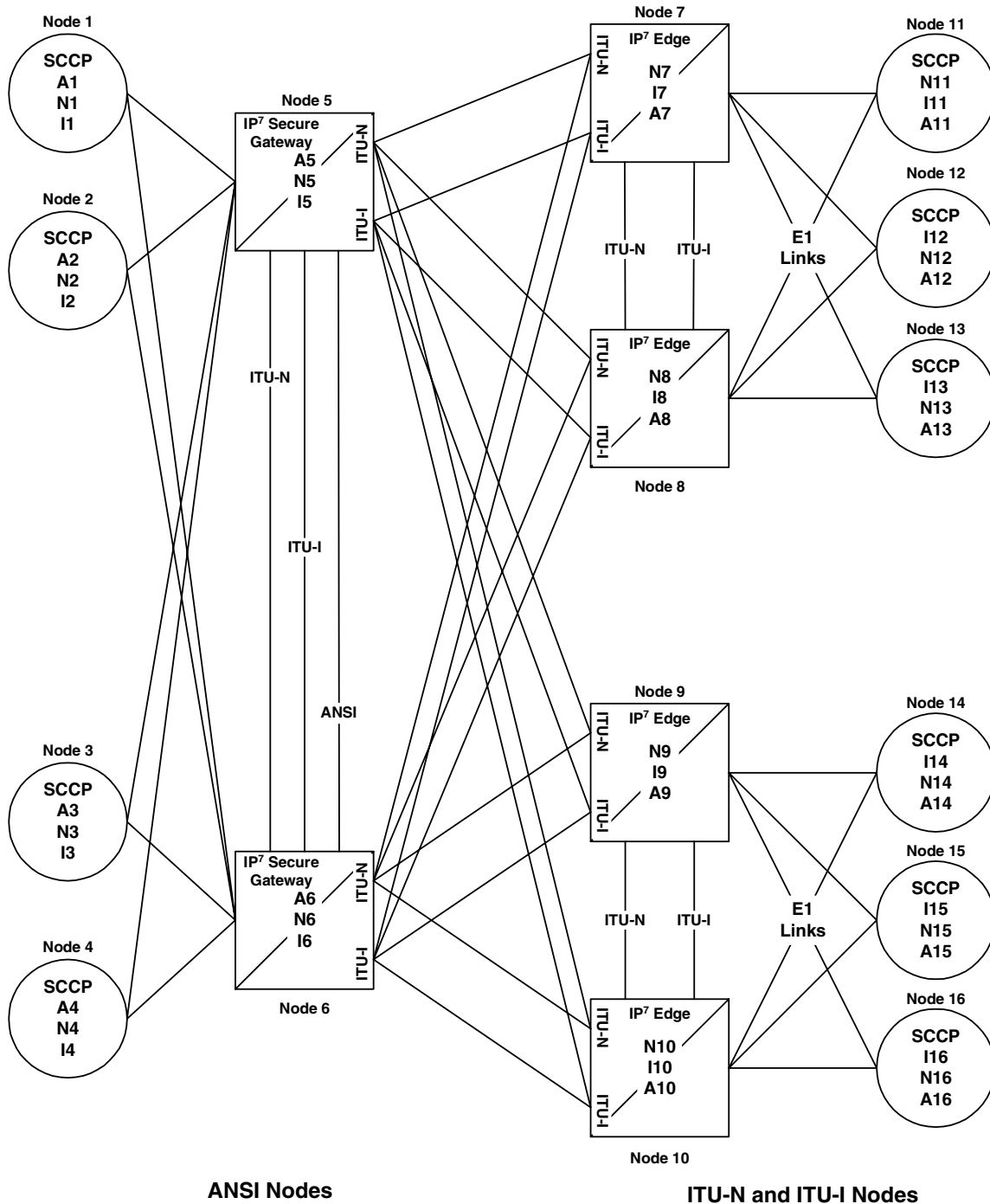


Table 2-8. Nodes and Point Codes in Complex Network Example

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
3	SSP	ANSI	A3	N3, I3
4	SSP	ANSI	A4	N4
5	STP (with IP ⁷ Secure Gateway)	ANSI, ITU-N, ITU-I	A5, N5, I5	
6	STP (with IP ⁷ Secure Gateway)	ANSI, ITU-N, ITU-I	A6, N6, I6	
7	STP (with IP ⁷ Secure Gateway)	ITU-N, ITU-I	N7, I7	A7
8	STP (with IP ⁷ Secure Gateway)	ITU-N, ITU-I	N8, I8	A8
9	STP (with IP ⁷ Secure Gateway)	ITU-N, ITU-I	N9, I9	A9
10	STP (with IP ⁷ Secure Gateway)	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 system’s destination point code table. A TPC is a unique identifier of a node in a network. An STP (with IP⁷ Secure Gateway) must have a TPC for each network type that the system connects to. An 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 a system when that system does not have a TPC for the same network type.

The configured links and point codes in the complex network shown in Figure 2-14 on page 2-33 allows most nodes to communicate with other nodes. However, note that Node 2 cannot communicate with Node 13 or Node 16, or with any node in the ITU-N network because Node 2 does not have an ITU-N alias point code.

Routing and Conversion Within a Single Network Type

The following steps demonstrate how an Eagle routes and converts when an ITU-N node sends an MSU to another ITU-N node. For example, assume that Node 11 in Figure 2-14 on page 2-33 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 IP⁷ Secure Gateway):

1. An ITU-N formatted MSU (which has a network identifier=01b 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 (01b) 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 a system 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” on page 2-35, except for the conversion step.

For example, assume that Node 11 in Figure 2-14 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 IP⁷ Secure Gateway):

1. Perform step 1 through step 3 as shown in “Routing and Conversion Within a Single Network Type” on page 2-35. In this example, assume that the routing function determines that the outgoing link is configured on the IP 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 only network management messages have the Message Transfer Part (MTP) converted. 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.

Nagle's Algorithm

Nagle's Algorithm is a 1-bit, Boolean socket option that controls message packet transmission timing. Nagle's Algorithm applies only to TALI sockets. Sockets can be set to 1 = Enable or 0 = Disable. Nagle's Algorithm is disabled by default for all sockets, which means that every message is transmitted over the Ethernet as soon as possible. When this socket option is disabled, it minimizes the time it takes for messages to be transmitted but increases the overall number of packets transmitted, which results in increased Central Processing Unit (CPU) utilization and less efficient Local Area Network (LAN) utilization.

Enabling Nagle's Algorithm allows the IP stack to hold on to messages for a period of time in an effort to pack multiple messages into a single TCP packet. Though message latency increases, fewer packets are generated and processed, resulting in lower CPU and better LAN utilization. At high rates of traffic through a socket, message latency is minimal because the threshold packet size is reached (messages fill the packet) very quickly, which causes the stack to transmit the packet.

Administrators can choose to enable or disable Nagle's Algorithm depending on the parameters that work best for the system. Nagle's Algorithm also can be toggled between being 1) enabled when the amount of messages that are transmitted is higher than the threshold limit and 2) disabled when transmission rates are lower than the threshold.

For more information on how to set up these features by altering the Database Communication Module Parameter Set (DCMPS), see the *Commands Manual*.

Type of Service (TOS)

This 8-bit, Type of Service (TOS) socket option is also used to prioritize the flow of network traffic. Packets can be routed differently according to the TOS value set in the IP header. The TOS field resides within the message's IP header and identifies the network router's priorities. Tekelec does not specify how the TOS bits should be set. The administrator can choose how to set them. Figure 2-15 on page 2-38 illustrates a TOS field setup. For more information on how to set up these features by altering the Database Communication Module Parameter Set (DCMPS), see the *Commands Manual*.

Figure 2-15. 8-bit TOS Field

7	6	5	4	3	2	1	0
		Reliability	Throughput	Delay	IP precedence		

For Differentiated Service (DiffServ) the TOS field is referred to as the Differentiated Service (DS) field. The priorities of the DS field in the IP header can also be set through socket options. Figure 2-16 illustrates a DS field setup.

Figure 2-16. DS Field

7	6	5	4	3	2	1	0
CU		DSCP					

ISUP Normalization

This feature allows an IP⁷ Secure Gateway to deliver ISUP messages that arrive at the IP⁷ Secure Gateway from the public switched telephone network (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 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 (or what country) the ISUP message originated from or is destined to and what ISUP variant the original PSTN message was formatted in.

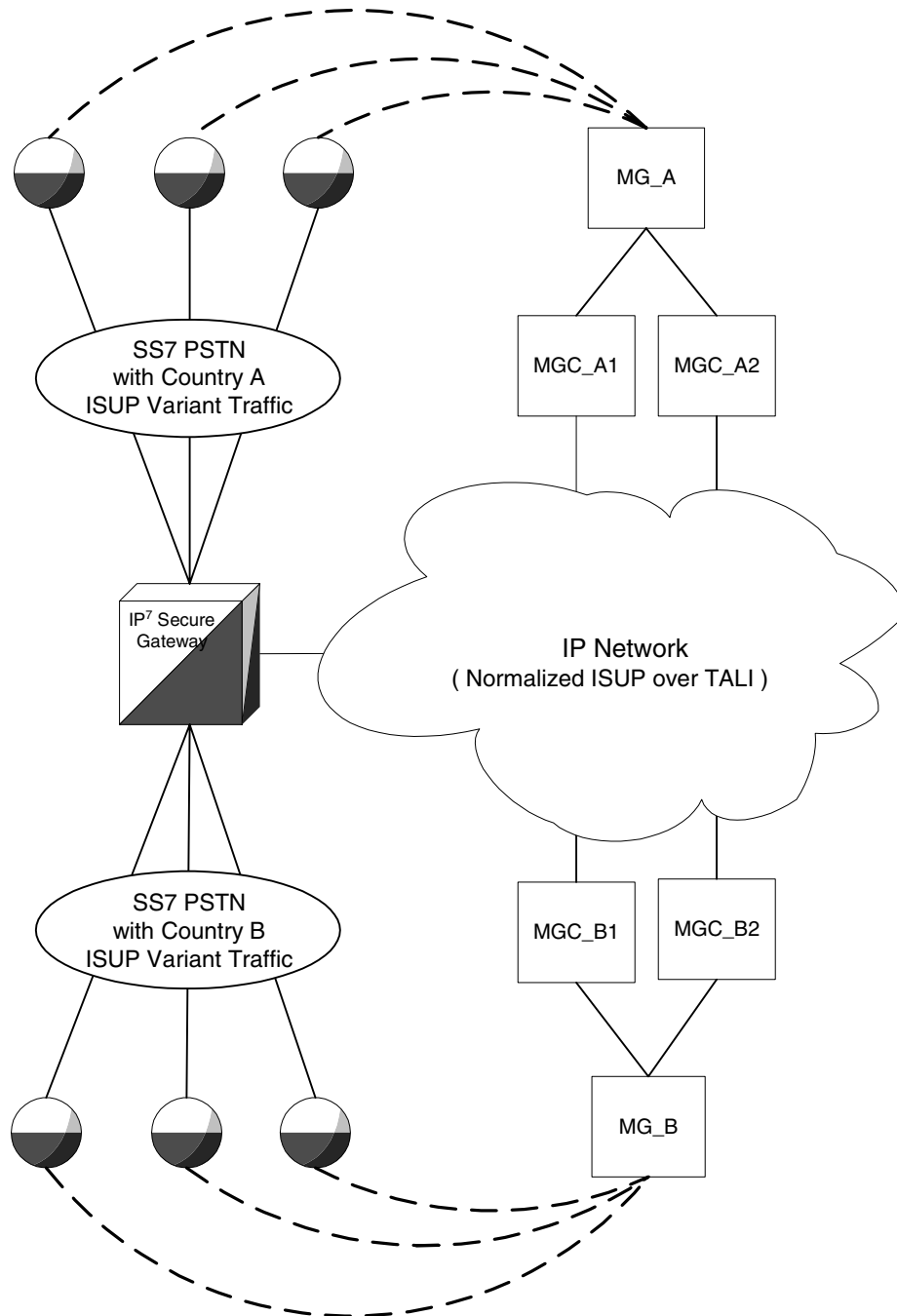
This feature allows an IP device (for example, an MGC providing Class 4 Tandem functionality) connected to an IP⁷ Secure Gateway to perform call setup for multiple countries without knowledge of the various countries' ISUP message formats. The MGC needs only to support encode and decode functionality for the normalized format and does not have to support encode and decode functionality for each ISUP variant.

The IP⁷ Secure Gateway and IP device are able to support these call scenarios:

1. Intra-Country Call
2. Inter-Country Call

This capability is shown in Figure 2-17 on page 2-39.

Figure 2-17. ISUP Normalization Supporting Multiple ISUP Variants



Although Figure 2-17 on page 2-39 shows a separate soft-switch (that is, the Media Gateway/Media Gateway Controller pair) per country, this feature does not prevent a single soft-switch, communicating with a single pair of IPGWI cards, from performing call setup for multiple countries.

Referring to Figure 2-17, the 'normalized ISUP traffic' is used in the communication between the IP⁷ Secure Gateway and the devices on the IP network. The traffic carried over the DS0 links to Country A SSPs and Country B SSPs (on the PSTN side of the IP⁷ Secure Gateway) continues to be formatted in the ISUP national variant format.

Normalized ISUP refers to the ISUP messages that are passed between the IP card running the IPGWI application (IPGWI card) and the IP device when this feature is used. The Normalized ISUP message is based on ETSI V3 ISUP, but provides a method to pass along variant-specific data that does not map cleanly to ETSI V3. This allows the IP device to support decode/state machine/encode capabilities for Normalized ISUP only, rather than having to support these capabilities for multiple ISUP variants. Note that Normalized ISUP messages only exist in the IP network and are never present in the PSTN.

The variant specific information is retained as part of the ISUP normalized TALI message to guarantee that intra-country calling features which require variant specific messages and parameters can continue to work for those intra-country calls.

The normalization function is performed entirely on the IPGWI card in the IP⁷ Secure Gateway. Everything presented to the MGCs that are using this feature is in Normalized ISUP format. Everything that is presented to the MTP3 portion of the IPGWI card (to be routed back to a DS0 link towards the PSTN) is in the format for a specific ISUP variant. Each DS0 LIM (or any LIM in the IP⁷ Secure Gateway other than the IPGWI card) receives MSUs from the PSTN wire and from the IMT in the same ISUP variant format. The DS0 LIMS do not know how to perform ISUP Normalization, and do not even know that it is occurring on the IPGWI cards.

The ISUP Normalization feature supports the normalization of the ISUP variants shown in Table 2-9:

Table 2-9. ISUP Variants Supported by this Feature

ISUP Variant	Part No.	PSTN Category	PSTN ID
ISUP Normalization	893000201	1	*
ITU Q.767 Normalization	893000501	1	1
ESTI V3 Normalization	893000601	1	2
UK PNO-ISC7 Normalization	893000401	1	3
German ISUP Normalization	893000301	1	4
French ISUP Normalization	893-0007-01	1	5

Table 2-9. ISUP Variants Supported by this Feature (Continued)

ISUP Variant	Part No.	PSTN Category	PSTN ID
Sweden ISUP Normalization	893-0008-01	1	6
Belgium ISUP Normalization	893-0009-01	1	7
Netherlands ISUP Normalization	893-0010-01	1	8
Switzerland ISUP Normalization	893-0011-01	1	9
Austria ISUP Normalization	893-0012-01	1	10
Italy ISUP Normalization	893-0013-01	1	11
Ireland ISUP Normalization	893-0014-01	1	12
India ISUP Normalization	893-0015-01	1	13
Malaysia ISUP Normalization	893-0016-01	1	14
Vietnam ISUP Normalization	893-0017-01	1	15
South Africa ISUP Normalization	893-0018-01	1	16
Argentina ISUP Normalization	893-0019-01	1	17
Chile ISUP Normalization	893-0020-01	1	18
Venezuela ISUP Normalization	893-0021-01	1	19
Mexico ISUP Normalization	893-0022-01	1	20
Brazil ISUP Normalization	893-0023-01	1	21
Spain ISUP Normalization	893-0024-01	1	22
Colombia ISUP Normalization	893-0025-01	1	23
Peru ISUP Normalization	893-0026-01	1	24
Hong Kong ISUP Normalization	893-0027-01	1	25
China ISUP Normalization	893-0028-01	1	26
Japan ISUP Normalization	893-0029-01	1	27
Korea ISUP Normalization	893-0030-01	1	28
Taiwan ISUP Normalization	893-0031-01	1	29
Philippines ISUP Normalization	893-0032-01	1	30
Singapore ISUP Normalization	893-0033-01	1	31
Australia ISUP Normalization	893-0034-01	1	32
Reserved for future definition by Tekelec		2 through 4095	
Available for user-defined categories		4095 through 65535	

The Quantity Control feature allows a customer to provision a specified quantity of user-defined variants within the PSTN categories 4096 - 65535. Each Quantity Control Feature is associated with a specific quantity of variants. To provision user-defined variants, it is necessary to purchase the appropriate Feature Access Keys from Tekelec. Variants enabled using the Quantity Control feature do not have associated PSTN Presentation values.

The part number for user-defined variants is 893-0100-nn, where nn is a number ranging from 01 to 20. Use part number 893-0100-01 to order one new variant, 893-0100-05 to order five new variants, and so on.

It is important to understand that for each variant that is supported, only two conversions are needed. For example:

- From ISUP Variant A -> Normalized ISUP
- From Normalized ISUP -> ISUP Variant A

To clarify this, the normalization on the IPGWI card never converts from ISUP Variant A to ISUP Variant B.

However, a call setup scenario could exist where two variants are used. In this case the conversions would go from:

Variant A -> Normalized -> Variant B

But the conversions cannot all occur at once. Two separate conversions occur, possibly on different nodes.

The normalization of ANSI ISUP messages is not supported. The normalization of ISUP MSUs only occur on the cards running the IPGWI application and not the SS7IPGW application.

PSTN Presentation

PSTN presentation is a 32-bit value indicating the format of the MSU Level 3 payload while it exists in the PSTN (see Figure 2-18 on page 2-43). When using this feature, the PSTN presentation is configured in the IP Routing Key table and appears in "XSRV-xnrm" and "XSR-xmtp" packet headers.

The PSTN presentation's primary uses are as follows:

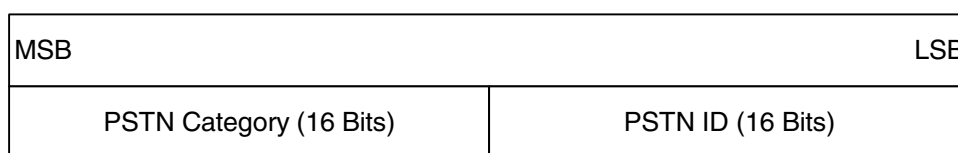
1. To indicate to the IPGWI card how to decode an ISUP MSU received from the PSTN when converting it to Normalized format for transmission over a socket configured for ISUP via XSRV-xmm.
2. To indicate to the IPGWI card how to encode an ISUP MSU for delivery to the PSTN when converting a Normalized ISUP packet received from an IP device.
3. To indicate to an IP device how to decode the Variant Specific portion (Part 2) of a received 'XSRV-xnrm' TALI packet.

4. To indicate to an IP device how to decode the raw MSU payload of a received "XSRV-xmtp" TALI packet (not limited to ISUP messages).

The PSTN Presentation consists of two parts, a PSTN Category and a PSTN ID:

- PSTN Category – provides a way of logically partitioning groups of PSTN IDs
- PSTN ID – provides unique identification of presentations within a given category

Figure 2-18. Format of PSTN Presentation



Some PSTN Categories are reserved for specific vendor's use and definition. For example, IP⁷ Secure Gateway's reserve category #1 for defining ISUP variants supported by this feature. Table 2-9 lists valid PSTN categories and IDs.

The list of Tekelec-defined and user-defined PSTNs can be displayed by using the `rtrv-pstn-pres` command, as illustrated in the following example:

```

PSTNCAT      PSTNID      PSTNDESC
00001        00001        ITU Q.767
00001        00002        ETSI V3
00001        00003        UK PNO-ISC7
00001        00004        GERMAN ISUP
00001        00020        MEXICO
04096        01000        User Defined 4096/1000
    
```

Note that a PSTN Presentation of 0 (that is, Category = 0 and ID = 0) is defined as unknown and is the default value in routing keys and TALI XSRV headers.

Other PSTN Categories are available for implementation specific definition by the customer. For example, customer X may use category 4096 to define a set of PSTN IDs (that is, BTNUP, French TUP, etc.) that exists in its network and are routed over IPGWI links.

The PSTN Presentation (Category, ID, and description) is provisioned using the `ent-pstn-pres` command. This command may be used to define values within the Tekelec-defined range (PSTN Category 0-4095) as long as there exists an associated ON/OFF Control Feature, and its status is ENABLED. This command may be used to define values within the user-defined range (PSTN Category 4096-65535) as long as there exists an associated ISUP Normalization Quantity Control Feature and its status is ENABLED and its capacity is not going to be exceeded.

This command also creates a new entry in the ISUP Variant table initialized to default values. There must be an available entry in the table or this command will be rejected.

The **chg-pstn-pres** command changes the descriptive text of a previously provisioned PSTN Presentation value.

The **dlt-pstn-pres** command deletes a previously provisioned PSTN Presentation value. The entry in the ISUP Variant table associated with the deleted PSTN will be marked as available. All of the associated ISUP messages and parameters that have been provisioned for the PSTN/Variant with the **chg-isupvar-attrib** command will also be deleted.

The user cannot delete the PSTN for Normalized ISUP (ETSI V3).

Deleting the PSTN Category or ID may cause a loss of traffic if SS7IP routing keys exist using that PSTN value. The user should use caution when performing this action and must enter the **force** parameter with the **dlt-pstn-pres** command.

The **chg-isupvar-attrib** command is used to provision the ISUP message and parameter database for a variant based on the PSTN Presentation value. This command will allow the administrator to:

- Specify/change the defined message-type-codes and parameter-codes for the variant.
- Specify/change the optional parameters that are supported for each message-type.
- Specify/change the mandatory-fixed and mandatory-variable-length parameters that are supported for each message-type.
- Specify/change the minimum valid length for each parameter.
- Specify/change for each message or message/parameter combination, a custom "action". An "action" parameter for this command will allow the administrator to specify one of the following three actions:
 - NONE - this is the default and it means the standard "normalization" conversion rules apply, i.e. do nothing special.
 - CONVERT - a special conversion routine will be invoked by software when it receives the message or message/parameter. For the Tekelec-defined variants, there may be certain messages or parameters that require special handling. Tekelec will write special conversion software for these cases. This value may be entered for user-defined variants, however software will ignore it.

- PASSTHRU - If specified with a message, then PASSTHRU means the specified message should be passed through unconverted using the raw MTP3 transfer method. If specified in a message/parameter combination, then PASSTHRU means that parameter, when received in that message, should be passed through to the Normalized section of the message (ignoring the DEFINED/SUPPORTED attributes of the Normalized specification).

The **copy-isupvar-attrib** command copies a “source” variant database to a “destination” variant database. This command provides the user with a quick way to provision a variant by copying a source variant database that has a similar ISUP protocol definition. The user can then use the **chg-isupvar-attrib** command to make the changes for the new protocol.

The PSTN Presentation is used to identify both the source and destination table entries. Both entries must be previously defined PSTN Presentation values, i.e. either a Tekelec-defined PSTN or a user-defined PSTN by the **ent-pstn-pres** command. Use the **rtrv-pstn-pres** command to display the only allowed values for the source and destination PSTNs.

If the source or destination variant is a Tekelec-defined PSTN value, then its associated ON/OFF Control Feature must be ENABLED.

The destination PSTN is not allowed to be Normalized ISUP (ETSI V3).

The **rtrv-isupvar-attrib** command displays the variant database provisioned by the **chg-isupvar-attrib** command. An assortment of displays is possible depending on the filters applied.

The following is an example of a possible output displaying all supported parameters for a specified message in a variant:

PSTNCAT	PSTNID	MSGCODE	ATTRIB	ACTION
00001	00005	04h	DEFINED	CONVERT

MSGCODE	PARMCODE	TYPE	ORDER	ACTION
04h	---	---	-	CONVERT
	10h	MF	1	NONE
	08h	MF	2	NONE
	09h	MV	1	CONVERT
	FEh	MV	2	NONE
	00h	OPT	-	NONE
	01h	OPT	-	NONE

The **chg-appl-rtkey** command accesses the ISUP variant table to determine if the PSTN Presentation value entered is valid. It evaluates both Tekelec-defined and user-defined variant PSTNs.

The “Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key” procedure on page 3-307 shows how to configure the system for ISUP Normalization feature.

IETF Adapter Layer Support

Overview

The current implementation of the IETF adapter layers in the IP⁷ Secure Gateway uses three adapter layers: SUA, M3UA, and M2PA. These adapter layers are assigned to SCTP associations which define the connection to the far end. An SCTP association is defined in the system by the local host name, the local SCTP port, the remote host name, and the remote SCTP port.

The three adapter layers used in the IP⁷ Secure Gateway are supported depending on the type of IP card being used for the IP connection. The SUA adapter layer can be used only on IPGWx cards (cards running either the SS7IPGW or IPGWI applications). The M2PA adapter layer can be used only on IPLIMx cards (cards running either the IPLIM or IPLIMI applications). The M3UA adapter layer can be used on both IPGWx and IPLIMx cards.

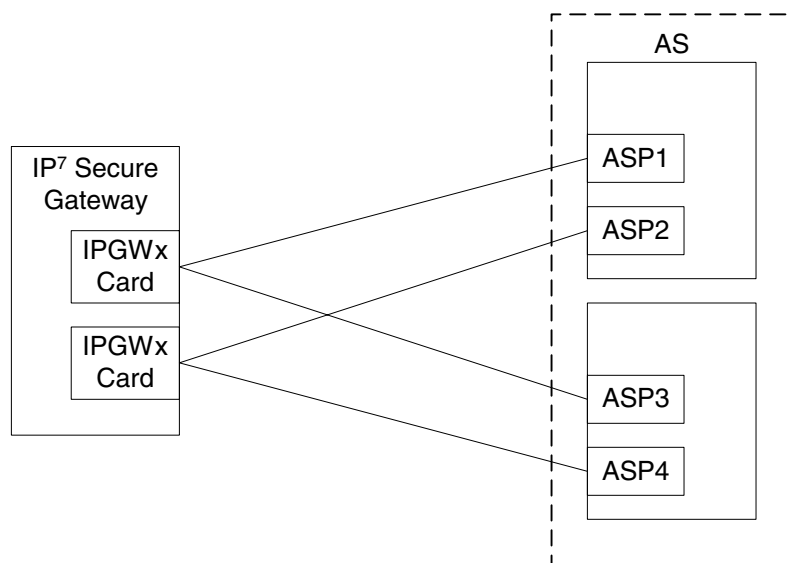
SCTP associations on IPGWx cards, like TCP sockets, use routing keys to distinguish between the IP devices being connected to. TCP sockets are assigned directly to routing keys. SCTP associations cannot be assigned directly to routing keys. To get an SCTP association ultimately assigned to a routing key, the IETF adapter layers use the concept of the application server (AS) and application server process (ASP). The SCTP association is assigned to an ASP, which is a process instance of an application server. One or more ASPs are normally actively processing traffic. A group of ASPs (up to 16) can be assigned to an application server. An application server, a logical entity serving a specific routing key, is assigned to a routing key. This results in assigning the SCTP association, up to a maximum of 16, to a routing key.

The IETF SUA and M3UA adapter layers are supported on IPGWx cards. These adapter layers support the full implementation of the ASP, AS, and routing key for the IP⁷ Secure Gateway. SCTP associations assigned to IPGWx cards can be assigned to ASPs, application servers, and routing keys.

The IETF M3UA and M2PA adapter layers are supported on IPLIMx cards. The M3UA adapter layer does not support the full implementation of the AS (routing keys do not apply to IPLIMx cards), therefore SCTP associations assigned to M3UA links on IPLIMx cards can be assigned only to ASPs. The M2PA adapter layer does not support ASPs or application servers, therefore SCTP associations assigned to M2PA links on IPLIMx cards cannot be assigned to ASPs or application servers.

Figure 2-19 on page 2-47 shows a typical configuration with four connections (SCTP associations) out of the system using IPGWx cards. Each association is connected to a process on the far end.

Figure 2-19. AS/ASP Relationship



Interaction Between TALI and IETF Connections Within a Single System

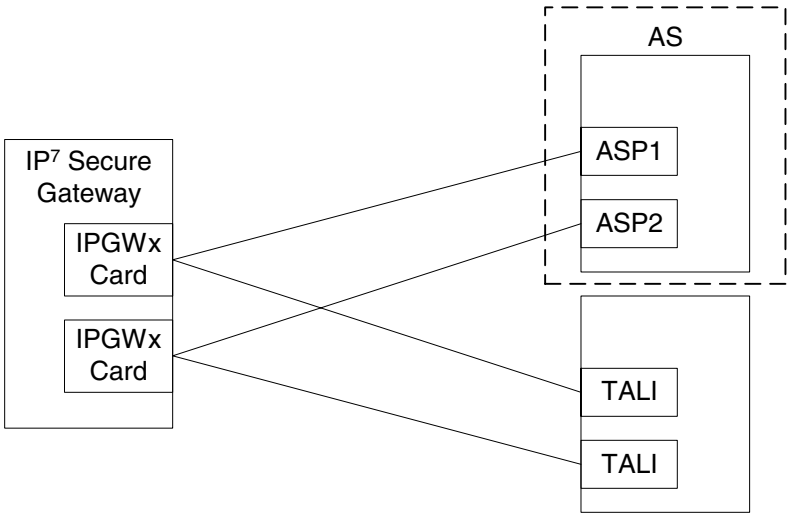
The IP cards in the IP⁷ Secure Gateway can use both TCP sockets (TALI connections) and SCTP associations (IETF connections) to make IP connections to far end devices. An IP connection is defined as either a TCP socket or an SCTP association. The IP⁷ Secure Gateway may contain all TALI connections, all IETF connections, or a combination of both. Figure 2-20 shows that a single system can communicate to far end devices using different adapter layers. Each IP card in the system can support both TCP sockets and application servers. However, on IPGWx cards, only one TCP socket or application server can be assigned to a single routing key.

An IPGWx card can contain a maximum of 50 connections. The IP⁷ Secure Gateway allows a maximum of 64 IPGWx cards, resulting in a maximum of 3200 connections for all IPGWx cards.

An IPLIMx card can have only one connection for each signaling link assigned to the card. The dual-slot DCM can contain only two signaling links, resulting in a maximum of two IP connections on these cards. The single-slot EDCM can contain a maximum of eight signaling links, resulting in a maximum of eight IP connections for this card.

The system can contain a maximum of 4000 IP connections, between IPGWx cards and IPLIMx cards.

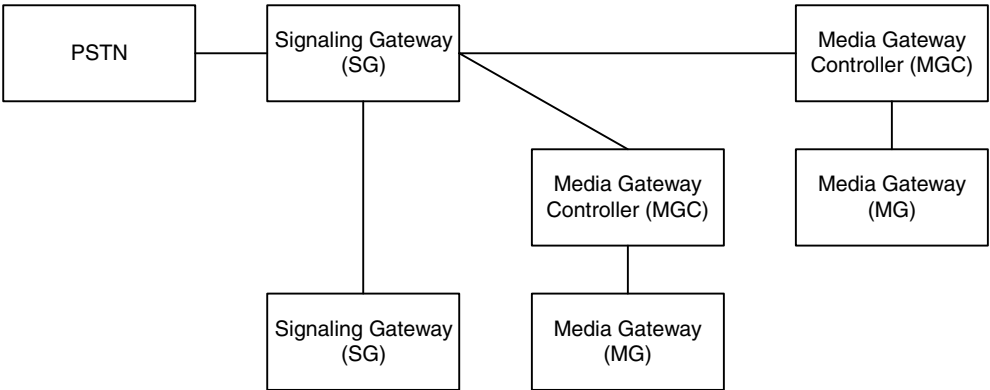
Figure 2-20. TCP Socket/SCTP Association Relationship



Feature Components

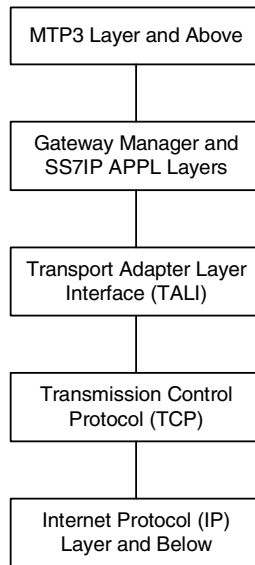
The system with IP⁷ Secure Gateway is used as a signaling gateway between the PSTN and IP networks as shown in Figure 2-21. This figure shows that signaling gateways interface with media gateway controllers (MGCs) and MGCs interface with media gateways (MGs).

Figure 2-21. SG/MGC/MG Network Diagram



If a TCP socket is used to make the IP connection to other devices, the IP⁷ Secure Gateway uses the TALI protocol on top of TCP to communicate to other devices, as shown in Figure 2-22 on page 2-49.

Figure 2-22. TALI Protocol Stack (IPGWx and IPLIMx)



To provide a signaling gateway solution that will be able to communicate with a larger number of IP devices, the system needs to be able to communicate with multiple MGCs which are using SCTP as the transport layer and M3UA, M2PA, or SUA as an adapter layer. On an IPLIMx card, the M3UA and M2PA adapter layers can be used with SCTP as shown in Figure 2-23. On an IPGWx card, the M3UA and SUA adapter layers can be used with SCTP as shown in Figure 2-24 on page 2-50.

Figure 2-23. IPLIMx Protocol Stack with SCTP as the Transport Layer

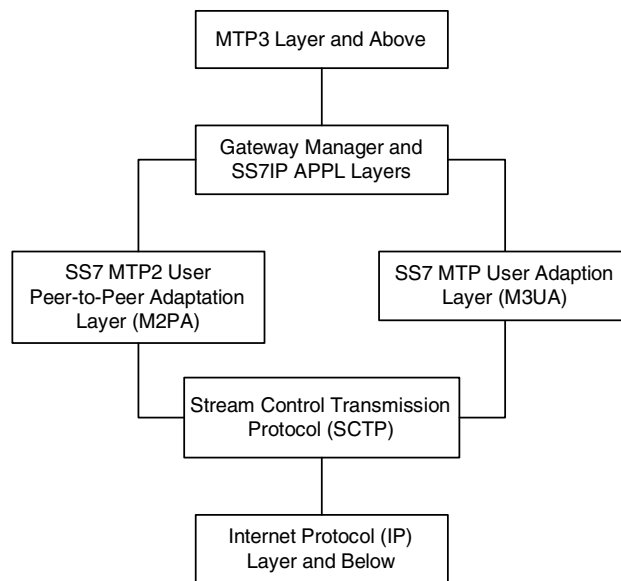
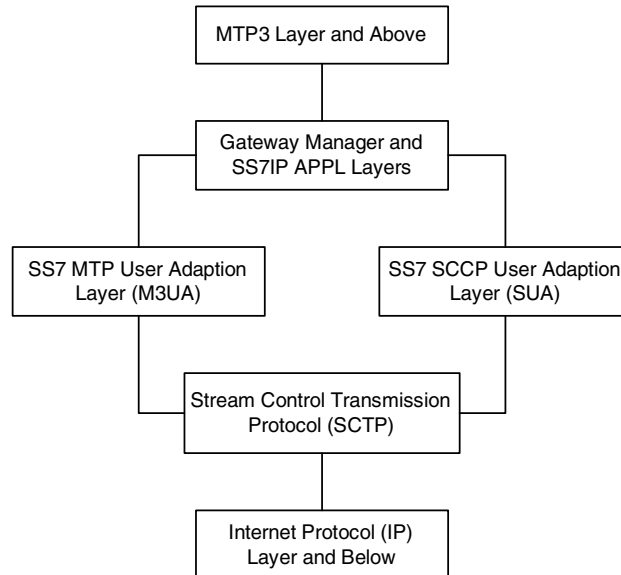


Figure 2-24. IPGW_x Protocol Stack with SCTP as the Transport Layer



The system supports many (mapping & transport) protocol combinations. One connection can be running TALI/TCP while another connection is running M3UA/SCTP, and a third connection is running M2PA/SCTP. These three connections can be on the same card (provided the card is a single-slot EDCM running the IPLIM_x applications, or an IPGW_x card) and even a part of the same routing key (if the card is an IPGW_x card). This mixture allows greater configurability for the user. The IP⁷ Secure Gateway does not support TALI over SCTP, or IETF adapter layers over TCP.

SUA Layer

The SUA layer, only supported on IP cards running either the SS7IPGW or IPGWI applications (IPGW_x cards), 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 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 (for example, TCAP, RANAP, etc.)
- Support for SCCP connectionless service.
- Support for the seamless operation of SCCP-User protocol peers

- Support for the management of SCTP transport associations between a signaling gateway 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

Depending upon the SCCP-users supported, the SUA layer supports the four possible SCCP protocol classes transparently. The SCCP protocol classes are defined as follows:

- Protocol class 0 provides unordered transfer of SCCP-user messages in a connectionless manner.
- Protocol class 1 allows the SCCP-user to select the in-sequence delivery of SCCP-user messages in a connectionless manner.
- Protocol class 2 allows the bi-directional transfer of SCCP-user messages by setting up a temporary or permanent signaling connection.
- Protocol class 3 allows the features of protocol class 2 with the inclusion of flow control. Detection of message loss or mis-sequencing is included.

Protocol classes 0 and 1 make up the SCCP connectionless service. Protocol classes 2 and 3 make up the SCCP connection-oriented service.

The SUA layer supports the following SCCP network management functions:

- Coord Request
- Coord Indication
- Coord Response
- Coord Confirm
- State Request
- State Indication
- Pcstate Indication

The SUA layer provides interworking with SCCP management functions at the signaling gateway for seamless inter-operation between the SCN network and the IP network. This means:

- An indication to the SCCP-user at an application server process that a remote SS7 endpoint/peer is unreachable.
- An indication to the SCCP-user at an application server process that a remote SS7 endpoint/peer is reachable.
- Congestion indication to SCCP-user at an application server process.
- The initiation of an audit of remote SS7 endpoints at the signaling gateway.

M3UA Layer

The M3UA layer, supported on both IPGWx and IPLIMx cards, was designed to fit the need for signaling protocol delivery from an SS7 signaling gateway 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, etc.)
- Support for the seamless operation of MTP3-User protocol peers
- Support for the management of SCTP transport associations and traffic between a signaling gateway 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 M3UA layer at an application server process provides a set of primitives at its upper layer to the MTP3-Users that is the equivalent of those provided by the MTP Level 3 to its local users at an SS7 SEP. In this way, the ISUP or SCCP layer at an application server process is unaware that the expected MTP3 services are offered remotely from an MTP3 Layer at a signaling gateway, and not by a local MTP3 layer. The MTP3 layer at a signaling gateway may also be unaware that its local users are actually remote user parts over the M3UA layer. The M3UA layer extends access to the MTP3 layer services to a remote IP-based application. The M3UA layer does not itself provide the MTP3 services.

The M3UA layer provides the transport of MTP-TRANSFER primitives across an established SCTP association between a signaling gateway and an application server process and between IPSPs. The MTP-TRANSFER primitives are encoded as MTP3-User messages with attached MTP3 Routing Labels as described in the message format sections of the SCCP and ISUP recommendations. In this way, the SCCP and ISUP messages received from the SS7 network are not re-encoded into a different format for transport to or from the server processes. All the required MTP3 Routing Label information (OPC, DPC, and SIO) is available at the application server process and the IPSP as is expected by the MTP3-User protocol layer.

At the signaling gateway, the M3UA layer also provides inter-working with MTP3 management functions to support seamless operation of the signaling applications in the SS7 and IP domains. This includes:

- Providing an indication to MTP3-Users at an application server process that a remote destination in the SS7 network is not reachable.
- Providing an indication to MTP3-Users at an application server process that a remote destination in the SS7 network is now reachable.

- Providing an indication to MTP3-Users at an application server process that messages to a remote MTP3-User peer in the SS7 network are experiencing SS7 congestion
- Providing an indication to MTP3-Users at an application server process that a remote MTP3-User peer is unavailable.

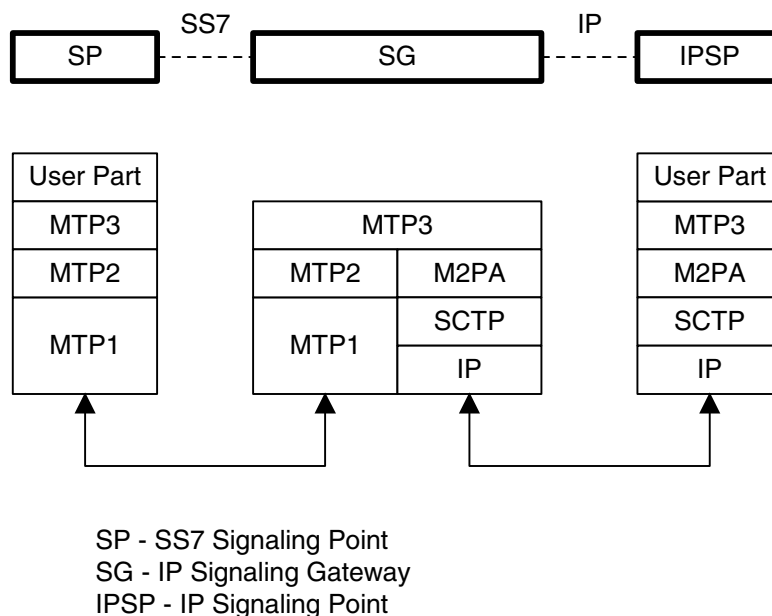
The M3UA layer at the signaling gateway maintains the availability of all configured remote application server processes, in order to manage the SCTP Associations and the traffic between the signaling gateway and application server processes. As well, the Active/Inactive state of remote application server processes is also maintained - Active application server processes are those currently receiving traffic from the signaling gateway.

M2PA Layer

The M2PA layer, supported only on IPLIMx cards, is a peer-to-peer protocol and provides mappings for all SS7 messages. In a peer-to-peer mode, either side of the IP connection may initiate the connection.

The M2PA layer closely matches the SAAL/TALI/TCP/IP Level 2 protocol stack. This allows it to provide all of the Level 2 features expected by MTP3. The M2PA layer lies below MTP3 in the protocol stack. Figure 2-25 shows the protocol layers in three interconnected nodes involving the M2PA layer.

Figure 2-25. M2PA in the IP⁷ Signaling Gateway



The M2PA layer receives the primitives sent from MTP3 to its lower layer. The M2PA layer processes these primitives or maps them to appropriate primitives at the M2PA/SCTP interface. Likewise, the M2PA layer sends primitives to MTP3 like those used in the MTP3/MTP2 interface.

The M2PA layer provides MTP2 functionality that is not provided by SCTP. This includes:

- Reporting of link status changes to MTP3
- Processor outage procedure
- Link alignment procedure

The M2PA layer allows MTP3 to perform all of its Message Handling and Network Management functions with IPSPs as with other SS7 nodes.

The M2PA layer also supports full retrieval because it assigns sequence numbers to all protocol messages and provides for acknowledgements from the M2PA peer. This means that an M2PA signaling link, unlike an M3UA signaling link, is able to execute the Change-Over and Change-Back procedures. The M2PA layer makes use of the SS7 Extended Changeover (XCO) and SS7 Extended Changeover Acknowledgement (XCA) messages in order to communicate 24-bit sequence numbers with the peer. This is very similar to what IPLIMx SAALTAI signaling links currently do.

SCTP

SCTP is a protocol designed to operate on top of a non-reliable protocol such as IP, while providing a reliable data delivery to the SCTP user. The SCTP protocol is designed to be a discrete protocol.

Although SCTP is similar in some respects to the Transport Control Protocol (TCP), it differs in several key areas. The two protocols are similar in that they both provide reliable data delivery over a non-reliable network protocol (IP). The SCTP protocol is a more robust and higher performance protocol than TCP.

Broader Definition of Connection Four-Tuple

The TCP protocol defines a connection via a four-tuple – a specific local IP address, local transport protocol port, a specific remote host IP address and remote transport protocol port. The TCP connection is point-to-point and once the session is established the four-tuple can not change. SCTP uses a similar four-tuple concept, but provides for the local and remote IP address values to be a list of IP addresses. SCTP allows a multi-homed host, with multiple network interfaces and more than one way to reach the far-end host, the capability to make use of this additional network connectivity to support the transport of data via the SCTP protocol. Redundancy through the support of multi-homing session end-points is a major SCTP advantage.

Multiple Streams

TCP is a point-to-point byte stream oriented transport protocol. In such a protocol if a single byte is corrupted or lost, then all data that follows must be queued and delayed from delivery to the application until the missing data is retransmitted and received to make the stream valid. With the TCP protocol, all data being transmitted is affected because there is only one path from end-to-end. The SCTP protocol addresses this limitation by providing the capability to specify more than one transport path between the two end-points. In SCTP, the four-tuple – with the multi-homing feature – defines what the SCTP protocol calls an *association*.

The association is composed of one or more uni-directional transport paths called *streams*. The number of inbound and outbound streams is independent of one another and is determined at session initiation time (for example, an association may be composed of three outbound and one inbound stream). In this scheme, a data retransmission only affects a single stream. If an association is defined with multiple streams and a packet is lost on a specific stream, data transmission on the other streams, which form this association, is not blocked. However, this feature is only beneficial if the upper layer application uses it.

In the IP⁷ Secure Gateway, a maximum of 2 inbound and 2 outbound streams can be defined for an association. Stream 0 in each direction is designated for Link Status messages. Stream 1 is designated for User Data messages. Separating the Link Status and User Data messages onto separate streams allows the adapter layer to prioritize the messages in a manner similar to MTP2. If the peer chooses to configure the association to have only one stream, then the signaling gateway will be able to use only stream 0 for both Link Status messages and User Data messages.

Datagram Stream

While TCP is implemented as a byte-oriented stream protocol, SCTP is based on a datagram-oriented protocol stream. By choosing the datagram as the smallest unit of transport, the SCTP protocol removes the need for the upper layer application to encode the length of a message as part of the message. An SCTP send results in the data being sent as a unit – a datagram – and received at the receiving node as a datagram.

Selective Acknowledgements

TCP acknowledgements are specified as the last consecutive byte in the byte stream that has been received. If a byte is dropped, the TCP protocol on the receiving side cannot pass inbound data to the user until the sender retransmits the lost byte; the stream is blocked. SCTP uses a feature known as *selective acknowledgement* in which each data chunk is identified by a chunk number – the Transmission Sequence Number (TSN) in SCTP terminology – and is explicitly acknowledged at a data chunk granularity. This means that if a data chunk is dropped, only that one data chunk needs to be retransmitted. In SCTP, a dropped

data chunk only effects one stream, since ordered transmission of data is only enforced at the stream and not the association level.

Un-order Delivery Capability

The SCTP protocol provides a mechanism for un-ordered datagram delivery. This feature means that a datagram can be transmitted and received independent of datagram sequencing and thus not delayed while awaiting a retransmission. TCP does not provide an equivalent feature of this type.

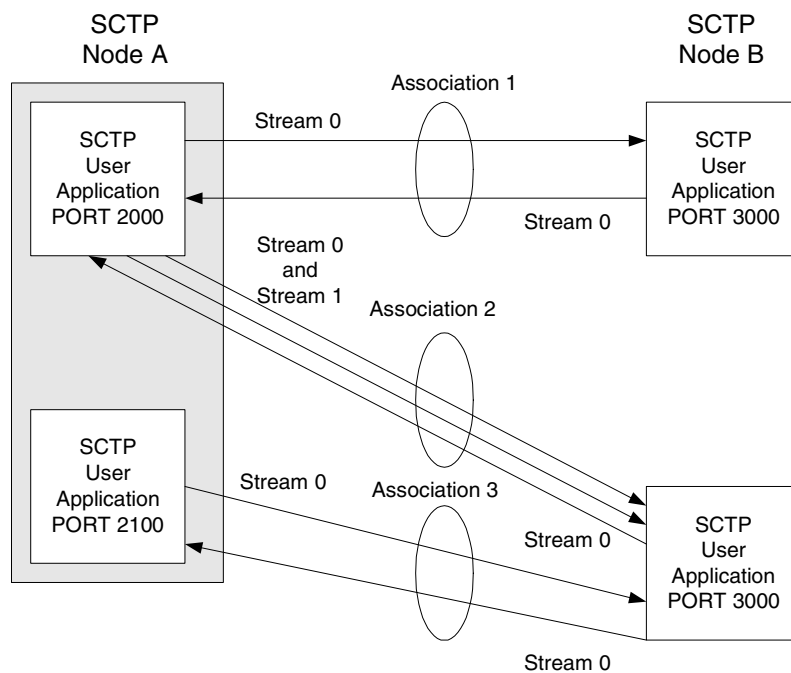
Enhanced Security

The TCP protocol has a known and easily exploitable vulnerability to denial of service attacks (for example, SYN attacks). This weakness is due to the three-way handshake used by the TCP session-establishment protocol. The TCP session establishment method causes system resources to be committed prior to actually establishing the session. SCTP uses a four-way handshake where resources are not committed by the host being contacted until the contacting host confirms that it is actually making a contact request to prevent such attacks.

SCTP Connectivity Concepts

The basic connectivity provided by the SCTP protocol is illustrated by Figure 2-26:

Figure 2-26. SCTP Connectivity



Key elements of the SCTP connection include:

- SCTP Instance
- SCTP Endpoint
- SCTP Association
- SCTP Stream

An SCTP instance is defined by the local SCTP port number. Each local SCTP port number requires its own SCTP instance. An SCTP instance as an entity defines the various SCTP characteristics that will apply to “all” SCTP associations that are created as part of the SCTP instance. These include timeout values, maximum receive windows, and so forth.

In Figure 2-26 on page 2-56 there are three hosts: SCTP node A, node B and node C. Node A has two SCTP instances: local SCTP port 2000 and 2100. Both node B and node C have a single SCTP instance, local SCTP port 3000 and 3000 respectively. The fact that both node B and C are using port 3000 does not tie them together in any way.

An SCTP endpoint is defined as the logical sender/receiver of SCTP packets. On a multi-homed host, an SCTP endpoint is represented to its peers as a combination of a set of eligible destination transport addresses to which SCTP packets can be sent and a set of eligible source transport addresses from which SCTP packets can be received. All transport addresses used by an SCTP endpoint must use the same port number, but can use multiple IP addresses. A transport address used by an SCTP endpoint must not be used by another SCTP endpoint. In other words, a transport address is unique to an SCTP endpoint.

The concept of SCTP instance clarifies this definition. In Figure 2-26 on page 2-56, IP addresses are not shown, but to illustrate this definition, assume the following:

- Node A is multi-homed having two network interface cards with IP addresses 192.168.110.10 and 192.168.55.10
- Node B has a single network interface card with IP address of 192.168.110.20
- Node C is multi-homed having two network interface cards with IP addresses 192.168.110.30 and 192.168.55.30

Based on these IP addresses from above and the defined port numbers for Figure 2-26 on page 2-56, there are four SCTP endpoints (Table 2-10).

Table 2-10. Sample SCTP Endpoints

Node	Local IP Address	Local SCTP Port
Node-1	192.168.110.10 192.168.55.10	2000
Node-1	192.168.110.10 192.168.55.10	2100
Node-2	192.168.110.20	3000
Node-3	192.168.110.30 192.168.55.30	3000

An SCTP association is defined as a protocol relationship between SCTP endpoints, composed of the two SCTP endpoints and protocol state information including verification tags and the currently active set of Transmission Sequence Numbers (TSNs), etc. An association can be uniquely identified by the transport addresses used by the endpoints in the association. Two SCTP endpoints must not have more than one SCTP association between them at any given time.

Based on this definition, given the endpoints listed above and Figure 2-26 on page 2-56, there are three defined SCTP associations.

Table 2-11. Sample SCTP Associations

Association	Local IP Address	Local SCTP Port	Remote IP Address	Remote SCTP Port
Association-1	192.168.110.10 192.168.55.10	2000	192.168.110.20	3000
Association-2	192.168.110.10 192.168.55.10	2000	192.168.110.30 192.168.55.30	3000
Association-3	192.168.110.10 192.168.55.10	2100	192.168.110.30 192.168.55.30	3000

An SCTP stream is defined as a uni-directional logical channel established from one to another associated SCTP endpoint, within which all user messages are delivered in sequence except for those submitted to the unordered delivery service.

NOTE: The relationship between stream numbers in opposite directions is strictly a matter of how the applications use them. It is the responsibility of the SCTP user to create and manage these correlations if they are so desired.

Based on this definition and Figure 2-26 on page 2-56, there are a total of seven streams for the three associations.

Table 2-12. Sample SCTP Associations

Association	Stream Number	Local IP Address	Local SCTP Port	Remote IP Address	Remote SCTP Port
Association-1	Stream 0 Out	192.168.110.10 192.168.55.10	2000	192.168.110.20	3000
Association-1	Stream 0 In	192.168.110.10 192.168.55.10	2000	192.168.110.20	3000
Association-2	Stream 0 Out	192.168.110.10 192.168.55.10	2000	192.168.110.30 192.168.55.30	3000
Association-2	Stream 1 Out	192.168.110.10 192.168.55.10	2000	192.168.110.30 192.168.55.30	3000
Association-2	Stream 0 In	192.168.110.10 192.168.55.10	2000	192.168.110.30 192.168.55.30	3000
Association-3	Stream 0 Out	192.168.110.10 192.168.55.10	2100	192.168.110.30 192.168.55.30	3000
Association-3	Stream 0 In	192.168.110.10 192.168.55.10	2100	192.168.110.30 192.168.55.30	3000

3

IP⁷ Secure Gateway Configuration Procedures

Overview	3-3
Adding an IP Card	3-16
Removing an IP Card	3-31
Configuring an IPGWx Linkset	3-40
Configuring a Mate IPGWx Linkset	3-60
Adding an IP Signaling Link	3-82
Enabling the Large System # Links Controlled Feature.....	3-108
Removing an IP Signaling Link.....	3-115
Migrating IPLIMx M3UA Signaling Links to IPGWx M3UA Connections	3-125
Changing the IP Protocol Option	3-141
Changing IP Options other than SYNC and SCTPCSUM	3-148
Adding an IP Host.....	3-153
Removing an IP Host	3-155
Changing an IP Link	3-158
Changing an IP Card.....	3-173
Adding an IP Route.....	3-183
Removing an IP Route	3-188
Adding an Application Socket.....	3-192
Removing an Application Socket.....	3-202

Changing an Application Socket3-205

Configuring IP Socket Retransmission Parameters3-217

Changing a DCM Parameter Set.....3-223

Adding an Application Routing Key Containing a Socket.....3-228

Adding an Application Routing Key Containing an Application
Server 3-240

Removing an Application Routing Key3-258

Replacing the IP Connections in an Existing Application Routing Key
with a Single Socket 3-267

Changing the CIC values in an Existing Application Routing Key3-275

Changing the Routing Context Value in an Existing Application
Routing Key 3-283

Replacing the IP Connections in an Existing Application Routing Key
with an Application Server 3-293

Changing the PSTN Presentation and Normalization Attributes
in an Application Routing Key..... 3-307

Increasing the System-Wide IPGWx Signaling TPS3-321

IETF Adapter Layer Configuration.....3-331

Adding an Association.....3-332

Removing an Association3-345

Changing an Association3-350

Configuring SCTP Retransmission Control for an Association3-370

Changing an M2PA Timer Set.....3-379

Adding an Application Server Process.....3-383

Removing an Application Server Process3-387

Adding an Application Server3-397

Removing an Application Server3-407

Changing an Application Server3-412

Adding a Network Appearance3-417

Removing a Network Appearance.....3-420

Changing the SCTP Checksum Algorithm Option.....3-422

Changing a UA Parameter Set3-451

Overview

The IP card supports the following applications:

- The **iplim** application, which supports point-to-point connectivity for ANSI networks
- The **iplimi** application, which supports point-to-point connectivity for ITU networks
- The **ss7ipgw** application, which supports point-to-multipoint connectivity for ANSI networks
- The **ipgwi** application, which supports point-to-multipoint connectivity for ITU networks.

The system must be configured to support connectivity to the ANSI and/or ITU IP network. Configuration consists of:

- IP configuration, consisting of these items configured in this chapter and Chapters 4 and 5:

Chapter 3

- IP card - a dual-slot DCM or single-slot EDCM, includes the IP addresses of the Ethernet interfaces and the default router on the card.
- IP transactions per second (applies only to **ss7ipgw** and **ipgwi** applications)
- IPGWx linksets
- IP signaling links
- IP options (required only for **ss7ipgw** and **ipgwi** applications)
- IP host
- IP link
- IP application sockets
- DCM parameter set
- IP application routing key (optional and applies only to the **ss7ipgw** and **ipgwi** applications).
- IP routes
- IP associations
- IP application servers

- IP application server processes
- Network appearances
- M2PA timer sets
- UA parameter sets

Chapter 4 – PSTN presentation data and ISUP variant provisioning

Chapter 5 – End node internal point codes

- SS7 configuration, consisting of the following items:
 - Destinations - see Chapter 2, “Configuring Destination Tables,” in the *Database Administration Manual - SS7*.
 - IPLIMx Linksets - see Chapter 3, “SS7 Configuration,” in the *Database Administration Manual - SS7*
 - Routes - see Chapter 3, “SS7 Configuration,” in the *Database Administration Manual - SS7*

The procedures shown in this chapter use a variety of commands. If more information on these commands is needed, go to the *Commands Manual* to find the required information.

The following steps provide a summary of all the entities that must be configured for the `iplim`, `iplimi`, `ss7ipgw`, and `ipgwi` applications. These entities must be provisioned in the order that they are shown. Steps 4, 16, 17, and 18 apply only to the `ss7ipgw` and `ipgwi` applications. Skip these steps for the `iplim` and `iplimi` applications.

1. Make sure that the required shelf is in the database with the `rtrv-shlf` command. If it is not in the database, add it with the `ent-shlf` command. For a detailed procedure, refer to the *Database Administration Manual - System Management*.
2. Make sure the cards that the signaling links will be assigned to are in the database with the `rtrv-card` command. These cards must be IP cards (card type `dcm`) and must have the `ss7ipgw`, `ipgwi`, `iplim`, or `iplimi` application assigned to them. If these cards are not in the database, add them with the `ent-card` command, specifying the `dcm` card type (`:type=dcm`) and one of these applications (`appl=ss7ipgw`, `appl=ipgwi`, `appl=iplim`, or `appl=iplimi`).
3. Verify the IP options with the `rtrv-sg-opts` command. If the options are not correct, change them with the `chg-sg-opts` command. All options except the `sctpchecksum` option (SCTP checksum algorithm) are valid only for `ss7ipgw` and `ipgwi` applications. The `sctpchecksum` option applies to the `iplim`, `iplimi`, `ss7ipgw`, and `ipgwi` applications.

4. If the `ss7ipgw` or `ipgwi` application is to be administered and you have purchased the ISUP-over-IP (`ipisup`) feature or the Dynamic Routing Key (`dynrtk`) feature, verify that the appropriate feature is turned on (`ipisup=on` or `dynrtk=on`) using the `rtrv-feat` command. If the appropriate feature is off, turn it on with the `chg-feat` command.

NOTE: Before turning on the ISUP-over-IP feature (`ipisup`) or the Dynamic Routing Key feature, make sure you have purchased these features. If you are not sure whether you have purchased the ISUP-over-IP feature or the Dynamic Routing Key feature, contact your Tekelec Sales Representative or Account Representative.

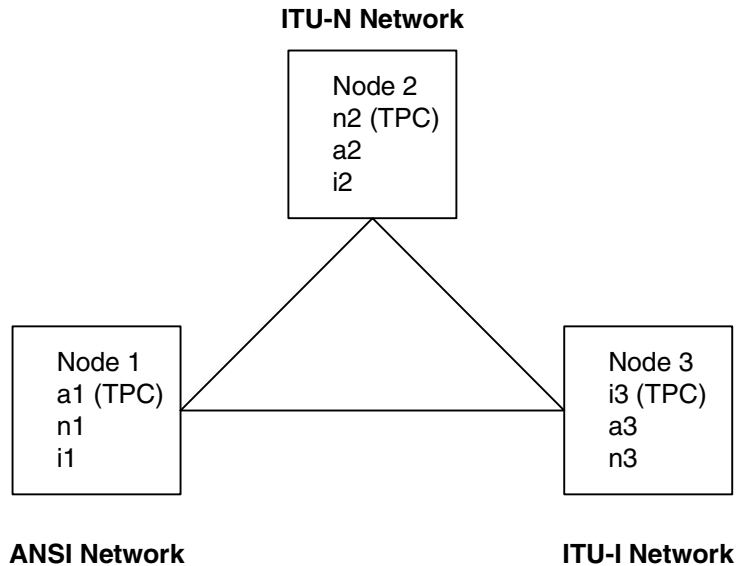
Once a feature has been turned on with the `chg-feat` command, the feature cannot be turned off.

Steps 4, 6, 17, 18, and 19 are valid only for `ss7ipgw` and `ipgwi` applications.

5. The network configuration for the system requires linksets, SS7 routes, and destinations. These entities use point codes and these point codes must be defined in the database. When nodes in different networks wish to communicate, each node must have either a true point code (TPC) or an alias point code for each of the two network types involved. For example, if node 1 in an ANSI network wishes to communicate with node 2 in an ITU-N network, node 1 must have an ANSI TPC and an ITU-N alias point code; and node 2 must have an ITU-N TPC and an ANSI alias point code.

Figure 3-1 shows an example of a mixed network with ANSI, ITU-I, and ITU-N nodes. Each node has one true point code and two alias point codes.

Figure 3-1. Mixed Network with ANSI, ITU-I, and ITU-N Nodes



Adjacent point codes (using the `ipgwapc` parameter) and virtual point codes must be defined for the `ss7ipgw` and `ipgwi` related links. For adjacent point codes, the specified point codes must not be reused anywhere in the SS7 network, with the exception that they can be used in a mated node with the IP⁷ Secure Gateway.

Verify that the necessary point codes are in the database with the `rtrv-dstn` command. If they are not in the database, add them with the `ent-dstn` command.

NOTE: An ITU-N point code can be either a 14-bit ITU-N point code (defined by the `ent-dstn` command's `dpcn` parameter), or a 24-bit ITU-N point code (defined by the `ent-dstn` command's `dpcn24` parameter). The system can contain either type of ITU-N point code, but not both at the same time.

6. The amount of IP transactions per second the system supports can be set using the `enable-ctrl-feat` command. The amount set by the `enable-ctrl-feat` command applies to the entire system, and only to IPGWx linksets. The amount of IP transactions per second can be set in amounts of 200, 400, 600, 1,000, and from 2,000 to 112,000 in increments of 2000 transactions per second.

Steps 4, 6, 17, 18, and 19 are valid only for `ss7ipgw` and `ipgwi` applications.

7. The linksets that will contain the signaling links must be in the database. 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 adjacent point code assigned to the linkset determines the network type of the linkset. These linksets must be assigned an adjacent point code (APC) that is in the SS7 domain. Verify this with the **rtrv-ls** command. If the APC is in the SS7 domain, the entry **SS7** is shown in the **DOMAIN** field of the output.

Mated IP⁷ Secure Gateways are connected through C links. Since each destination can be reached only over linksets that match that destination's network type, mated IP⁷ Secure Gateways require a C-link linkset for each network the STP is connected to. For systems with three true point codes (TPCs), there needs to be a C linkset to transport ANSI formatted MSUs, a C linkset to transport ITU-N formatted MSUs, and a C linkset to transport ITU-I formatted MSUs. A TPC uniquely identifies the IP⁷ Secure Gateway in the network.

Linksets associated with the **ss7ipgw** or **ipgwi** application (IPGWx linksets) must specify an adjacent point code (**apc**) with the **ipgwapc** parameter set to **yes** and the **mtprse** parameter set to **no**. IPGWx linksets must also specify the amount of IP transactions per second (with the **iptps** parameter) the linkset is allowed to use. The sum of the IP transactions per second for all IPGWx linksets cannot exceed the amount of IP transactions per second configured in step 6 with the **enable-ctrl-feat** command. Alarm thresholds for the IP transactions per second for the IPGWx linkset and the signaling links in the IPGWx linkset can also be set. IPGWx linksets can also have a mate IPGWx linkset assigned to it.

Verify that the necessary linksets are in the database with the **rtrv-ls** command. If the necessary linksets are not in the database, add them with the **ent-ls** command or change existing linksets with the **chg-ls** command.

8. The signaling links must be in the database. Verify this with the **rtrv-slk** command. The signaling links are assigned to linksets from step 7, and to IP cards with the **ss7ipgw**, **ipgwi**, **iplim**, or **iplimi** application, from step 2. If the IP card's application is **iplim** or **ss7ipgw**, then the linkset's APC must be an ANSI APC. If the IP card's application is **ipgwi** or **iplimi**, then the linkset's APC can be either an ITU international APC or an ITU national APC. Signaling link ports A1, A2, A3, B1, B2, and B3 can be assigned only to SSEDCCM cards running either the **iplim** or **iplimi** applications.

If the card's application is either the **iplim** or **iplimi**, and the signaling link is assigned to a TALI socket, the **ipliml2=saaltali** parameter must be specified for the signaling link. If the signaling link is assigned to a SCTP association, the **ipliml2=m3ua** or **ipliml2=m2pa** parameter must be specified for the signaling link.

If the necessary links are not in the database, add them with the **ent-slk** command. IPGWx linksets can have only one signaling link if these linksets have a mate assigned to it, or is the mate of another IPGWx linkset. Eight signaling links can be assigned to an IPGWx linkset if the IPGWx linkset is not the mate of another IPGWx linkset, or does not have a mate IPGWx linkset assigned to it.

9. The point codes assigned to each of the IP destinations must also be assigned to an SS7 route. An SS7 route must also be assigned to the linksets containing the adjacent point code. Verify this with the `rtrv-rte` command. If the necessary SS7 routes are not in the database, add them to the database with the `ent-rte` command, specifying a point code assigned to an IP destination, from step 5, and a linkset, from step 7. When setting up SS7 routes to the `ss7ipgw` or `ipgwi` application point codes, the only SS7 route that should be configured for those 'virtual point codes' is the direct route using the `ss7ipgw` or `ipgwi` related linkset.
10. Local IP hosts must be in the database. Verify the hosts with the `rtrv-ip-host` command. The IP host associates host names with IP addresses. This connection establishes a relationship between the IP card related information and the socket/association related information. If the necessary IP hosts are not in the database, add them with the `ent-ip-host` command.
11. When the IP cards are added to the database in step 2, IP link parameters for the IP cards are assigned default parameter values. These parameter values can be displayed by the `rtrv-ip-lnk` command. These values can be changed with the `chg-ip-lnk` command.
12. When the IP cards are added to the database in step 2, there are IP parameters that control the IP stack that are assigned default values. These parameter values can be displayed by the `rtrv-ip-card` command. These values can be changed with the `chg-ip-card` command.
13. Make sure that the application sockets are defined in the database. Verify this with the `rtrv-appl-sock` command. Sockets specify a connection between a local host/TCP port and a remote host/TCP port. If the necessary sockets are not in the database, add them with the `ent-appl-sock` command. A number of socket-related fields in the database are set to default values when the `ent-appl-sock` command is entered. These defaults can be displayed using the `rtrv-appl-sock` command after the `ent-appl-sock` command is executed. These default values can be changed with the `chg-appl-sock` command. IP cards with the `iplim` or `iplimi` application are allowed to have two IP connections (SCTP associations or TALI sockets). IP cards with the `ss7ipgw` or `ipgwi` application are allowed to have up to 50 IP connections (SCTP associations or TALI sockets).
14. Verify the DCM parameter set associated with each socket with the `rtrv-dcmps` command. The DCM parameters can be changed with the `chg-dcmps` command.

NOTE: Set number 10 is a default parameter set and cannot be changed. In order to change the DCM parameters set for a socket using set number 10, use the `chg-appl-sock` command to change the DCM parameter set to a different set number, and then use the `chg-dcmps` command to modify the new set.

15. The SCTP association is defined by the combination of a local host, local SCTP port, remote host and remote SCTP port. The SCTP associations are displayed in the database with the **rtrv-assoc** command. If the necessary associations are not in the database, add them with the **ent-assoc** command. A number of association-related fields in the database are set to default values when the **ent-assoc** command is entered. These defaults can be displayed using the **rtrv-assoc** command after the **ent-assoc** command is executed. These default values can be changed with the **chg-assoc** command.

An SCTP association can be either a multi-homed association or a uni-homed association. A multi-homed association uses both the A and B Ethernet interfaces on the IP card (a single-slot EDCM). One of the Ethernet interfaces on the IP card (for example, Ethernet A) is associated with the local host configured with the **lhost** parameter of the **ent-assoc** or **chg-assoc** command.

The other Ethernet interface on the same IP card (for example, Ethernet B) is associated with an alternate local host configured with the **alhost** parameter of the **ent-assoc** or **chg-assoc** command. The **lhost** and **alhost** parameter values represent the IP addresses associated with both Ethernet interfaces on the IP card.

A uni-homed association uses only one of the Ethernet interfaces on the IP card which is associated with the **lhost** parameter of the **ent-assoc** or **chg-assoc** command. The **alhost** parameter (alternate local host) is not used. The **lhost** parameter value represents the IP address associated with the Ethernet interface being used on the IP card.

Dual-slot EDCM cards with the **iplim** or **iplimi** application are allowed to have two IP connections (SCTP associations or TALI sockets). Single-slot EDCM cards with the **iplim** or **iplimi** application are allowed to have eight IP connections (SCTP associations or TALI sockets). IP cards with the **ss7ipgw** or **ipgwi** application are allowed to have up to 50 IP connections (SCTP associations or TALI sockets).

16. An application server process is a process instance of an application server and contains an SCTP association. The application server processes are displayed using the **rtrv-asp** command. If the necessary application server process is not in the database, add the application server process with the **ent-asp** command.

When an application server process is added to the database, UA parameter set 10 is assigned to the application server process. There are 10 UA parameter sets that can be assigned to an application server process, but the UA parameter set assignment can be changed, using the **chg-asp** command, only if the application server process contains an M3UA association. The values assigned to each UA parameter set can be changed, except for UA parameter set 10, using the **chg-uaps** command.

17. The application server contains a set of one or more unique application server processes, of which one or more is normally actively processing traffic. The application servers are displayed using the **rtrv-as** command. If the necessary application server is not in the database, add the application server with the **ent-as** command. If the application server processes assigned to application server contain M3UA associations, with the **open=yes** parameter, then the same UA parameter set must be assigned to all of the application server processes in the application server.
18. If the **ss7ipgw** or **ipgwi** application is to be administered and if static routing keys are desired, make sure that they are defined in the database for each socket or application server related to the **ss7ipgw** or **ipgwi** application. Verify the routing keys with the **rtrv-appl-rtkey** command. Routing keys specify MSU filters for a corresponding socket or application server. If the desired static routing keys are not in the database, add them with the **ent-appl-rtkey** command.
19. If the PSTN presentation data is to be changed for the routing key, the controlled feature associated with the PSTN presentation data must be enabled. The **rtrv-ctrl-feat** command shows whether or not the controlled features are enabled. If any of the required controlled features are not enabled, enter the **enable-ctrl-feat** command with the feature part number and the feature access key for the required controlled feature. The status of these controlled features is set to **on** with the **chg-ctrl-feat** command.

The **ent-pstn-pres** command can be used to define PSTN presentation data, in addition to the values shown in the **rtrv-pstn-pres** output, within either the Tekelec-defined range of PSTN categories, or the user-defined PSTN categories. The ISUP message and parameter database for an ISUP variant, defined by the PSTN presentation data, can be displayed using the **rtrv-isupvar-attrib** command, and changed with the **chg-isupvar-attrib** command. The PSTN presentation data, and ISUP normalization setting, can be changed using the **chg-appl-rtkey** command and is displayed using the **rtrv-appl-rtkey** command.

Steps 4, 6, 17, 18, and 19 are valid only for **ss7ipgw** and **ipgwi** applications.

20. If the IP card is a single-slot EDCM, static IP routes can be provisioned in the database with the **ent-ip-rte** command. The static IP routes are displayed using the **rtrv-ip-rte** command. The static IP routes provide more flexibility in selecting the path to the remote destination and reduces the dependence on default routers.

21. An internal point code can be provisioned to provide routing to an IP end office node. The internal point codes are displayed with the **rtrv-rmt-app1** command. The internal point code value must be in the DPC table, shown in the **rtrv-dstn** output. If the necessary internal point codes are not in the database, add them with the **ent-rmt-app1** command.
22. The network appearance field identifies the SS7 network context for the message, for the purpose of logically separating the signaling traffic between the SGP (signaling gateway process) and the ASP (application server process) over a common SCTP (stream control transmission protocol) association. This field is contained in the DATA, DUNA, DAVA, DRST, DAUD, SCON, and DUPU messages. The network appearances are displayed with the **rtrv-na** command. The internal point code value must be in the DPC table, shown in the **rtrv-dstn** output. If the necessary network appearances are not in the database, add them with the **ent-na** command. If the network appearance contains an ITU-N point code with group codes, the group code must be assigned to a secondary point code shown in the **rtrv-spc** output.

Figure 3-2 on page 3-12 shows the relationships of the database elements that are configured in these procedures.

Figure 3-2. IP⁷ Secure Gateway Database Relationships

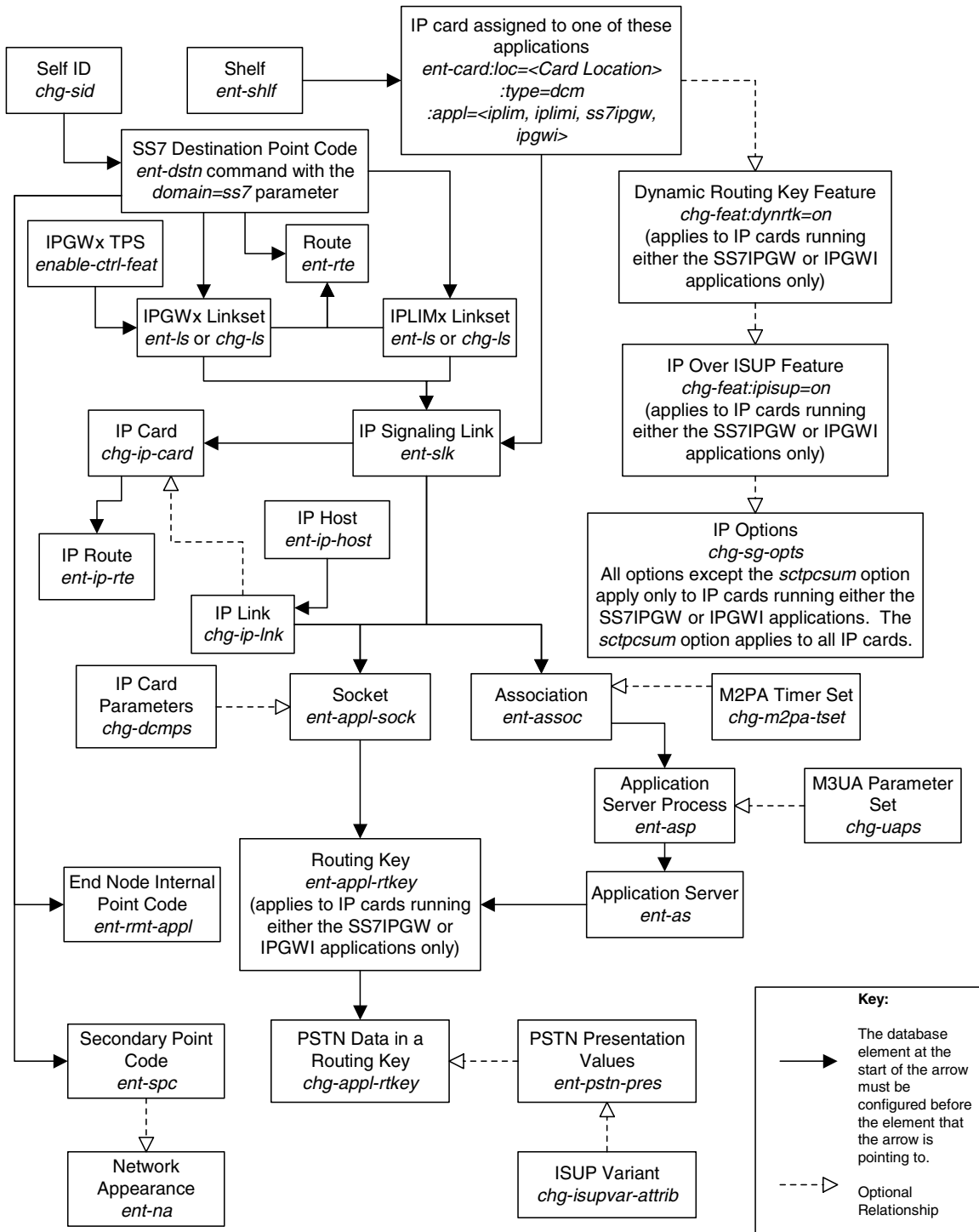


Figure 3-3 shows a typical network configuration and Tables 3-1, 3-2, 3-3 (following Figure 3-3) show the table information that would exist in the system with point code 2-2-2 after provisioning is completed.

Figure 3-3. Typical System Configuration

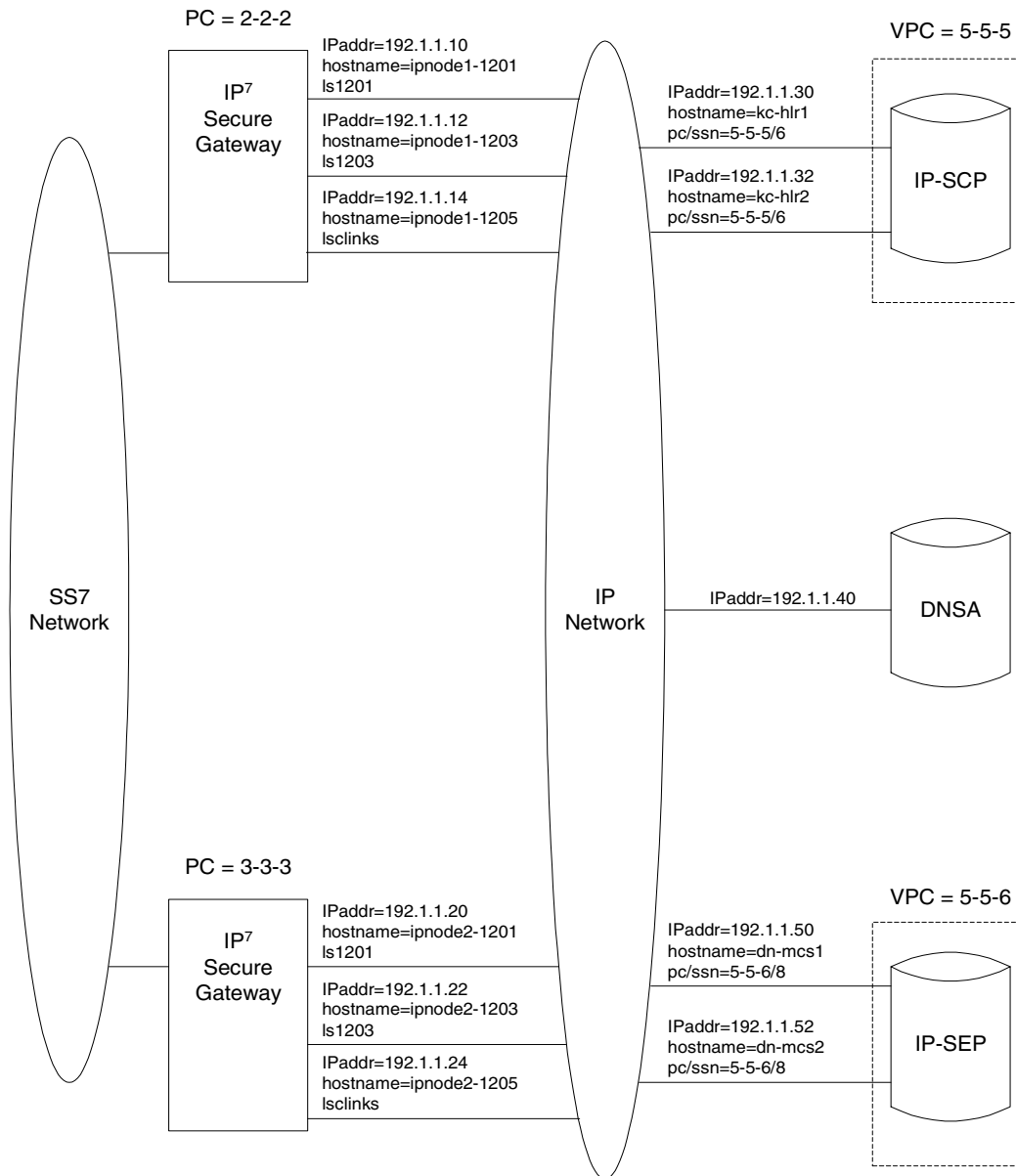


Table 3-1. Typical IP Routing

Destination	SS7 Route	Relative Cost
3-3-3	lsclinks	10
5-5-5	ls1201	10
	ls1203	10
	lsclinks	20
5-5-6	ls1201	10
	ls1203	10
	lsclinks	20

Table 3-2. Typical IP Sockets

Local IP Config			Remove IP Config		Local Socket Information	
Local Hostname	Client/Server	TCP Port	Hostname	TCP Port	Socket Name	DCM Parameter Set
ipnode-1201	S	7000	kc-hlr1	7000	kchlr11201	1
	S	7002	kc-hlr2	7002	kchlr21201	1
	S	7003	dn-msc1	7003	dnmsc11201	1
	S	7004	dn-msc2	7004	dnmsc21201	1
ipnode-1203	S	7005	kc-hlr1	7005	kchlr11203	1
	S	7006	kc-hlr2	7006	kchlr21203	1
	S	7007	dn-msc1	7007	dnmsc11203	1
	S	7008	dn-msc2	7008	dnmsc21203	1
ipnode1-1204	S	7009	lp-msg1	7009	lpmsg11204	1
	S	7010	lp-msg2	7010	lpmsg21204	1
	S	7011	lp-msg3	7011	lpmsg31204	1
ipnode1-1205	S	7012	lp-msg1	7012	lpmsg11205	1
	S	7013	lp-msg2	7013	lpmsg21205	1
	S	7014	lp-msg3	7014	lpmsg31205	1
ipnode1-1206	C	7001	ipnode2	7001	ipnode21206	1

IP⁷ Secure Gateway Configuration Procedures

Table 3-3. Typical IP Routing Keys (SS7IPGW and IPGWI Applications)

SS7 Routing Keys						IP Sockets that carry traffic for that Routing Key
SS7 DPC	SS7 SI	SS7 SSN	SS7 OPC	CIC Start	CIC End	Socket Name
5-5-5	3	6	-	-	-	kchlr11201 kchlr21201 kchlr11203 kchlr21203
5-5-6	5	-	4-4-4	1	100	dnmsc11201 dnmsc21201 dnmsc11203 dnmsc21203
1-44-2	4	-	2-5-1	3948	3948	lpmsg11205 lpmsg21205 lpmsg31205
4346	13	-	5834	48486	48486	lpmsg11204 lpmsg21204 lpmsg31204

Adding an IP Card

This procedure is used to add an IP card to the database using the **ent-card** command. The IP card is a Database Communications Module (DCM) or a single-slot Enhanced-Performance Database Communications Module (EDCM) and may not be in the database. The shelf to which the card is to be added, must be in the database.

The **ent-card** command uses these parameters.

:loc – The location of the card being added to the database.

:type – The type of card being added to the database.

:appl – The application software or GPL that is assigned to the card.

Table 3-4 shows the valid card type and card applications (**appl**) for the **ent-card** command in this procedure. The table also shows the card's part number and the maximum number of cards that the database can contain.

Table 3-4. Card Type and Card Applications

Card Name	Card Type (:type)	Application Type (:appl)	Network Type	Maximum Number of Cards in the Database
Dual-Slot DCM (870-1945-xx)	dcm	iplim/iplmi ss7ipgw/ipgwi	ANSI/ITU	100*
Single-Slot EDCM (870-2372-xx)			ANSI/ITU	64 †
<p>* If the system contains less than 700 signaling links, the maximum number of cards running either the iplim or iplmi application, or combinations of the iplim and iplmi applications is 41.</p> <p>† The system may contain a maximum of 64 single-slot EDCMs running either the ss7ipgw or ipgwi application, or combinations of the ss7ipgw and ipgwi applications. If DCMs are present in the system, there can be a maximum of 2 cards running the ss7ipgw application and 2 cards running the ipgwi application.</p>				

:force – If the global title translation feature is on, the **force=yes** parameter allows the LIM to be added to the database even if the current SCCP transactions-per-second threshold (see the **chg-th-sccp** command description in the *Commands Manual*) is unable to support the additional SCCP transaction-per-second capacity created by adding the IP card. The default value for this parameter is **no**, which does not allow the IP card to be added to the database unless there are enough SCCP cards in the database. If the global title translation feature is not on, this parameter has no meaning and should not be used. This parameter only applies to IP cards running the **iplim** or **iplmi** applications.

NOTE: For more information on using the `force` parameter, see “Using the FORCE Parameter” on page 3-18.

If the `force=yes` parameter is used to add an IP card to the database, it is recommended that you increase the SCCP transactions-per-second capacity of the system by adding additional SCCP cards to the database after the IP card is added to avoid losing GTT traffic.

If the card application is `ss7ipgw` or `ipgwi` and you have purchased the ISUP-over-IP (`ipisup`) feature or the Dynamic Routing Key (`dynrtk`) feature, verify that the appropriate feature is turned on (`ipisup=on` or `dynrtk=on`) using the `rtrv-feat` command. If the appropriate feature is off, turn it on with the `chg-feat` command. For more information on these features, refer to section “Understanding Routing for SS7IPGW and IPGWI Applications” on page 2-23.

NOTE: Before turning on the ISUP-over-IP feature (`ipisup`) or the Dynamic Routing Key feature, make sure you have purchased these features. If you are not sure whether you have purchased the ISUP-over-IP feature or the Dynamic Routing Key feature, contact your Tekelec Sales Representative or Account Representative.

Once a feature has been turned on with the `chg-feat` command, the feature cannot be turned off.

Card Slot Selection

The dual-slot DCM occupies two card slots and can be inserted any card slot in the extension shelf except slots 08 and 18. The dual-slot DCM card requires that the next adjacent slot be empty and not provisioned in the database. For example, if dual-slot DCM cards are inserted into slots 03 and 06, slots 04 and 07 must be empty and not provisioned in the database. Because slots 09 and 10 contain the HMUX cards, the dual-slot DCM card cannot be inserted into slots 08, 09, or 10. Slot 18 cannot be used because it is the last slot in the shelf. The dual-slot DCM card can be inserted in the control shelf, but only in slots 01 through 07, and 11, following the same rules as the extension shelf. Slots 1113 through 1118 are reserved for MASPs A and B and the MDAL card.

The single-slot EDCM can be inserted into any card slot, except for card slots that must remain empty to accommodate dual-slot cards, slots 09 and 10 in each shelf, and slots 1113 through 1118.

The examples in this procedure are used to add the cards shown in Table 3-5 to the database.

Table 3-5. Example Card Configuration

Card Type	Application	Card Location
dcm	iplim	1202*
dcm	iplimi	1308*

Table 3-5. Example Card Configuration

Card Type	Application	Card Location
dcm	iplim	1311
dcm	iplimi	1313
dcm	ss7ipgw	1315
dcm	ipgwi	1317
* These cards are single-slot EDCMs.		

Using the FORCE Parameter

When LIMs or IP cards are added to the database and the Global Title Translation feature is on, the system must contain enough SCCP cards to handle the number of SCCP transactions per second the SS7 cards (LIMs or IP cards) will send to the SCCP cards.

The Global Title Translation feature is on if the entries **SCCP** or **VSCCP** are shown in the **APPL** field of the **rtrv-card** command output. The entry **GTT = on** in the **rtrv-feat** command output also shows that the Global Title Translation feature is on.

An SCCP card is either a TSM running the SCCP application, or a DSM running the VSCCP application. Table 3-6 shows the maximum number of transactions per second that an SCCP card can handle.

Table 3-6. Number of Transactions per Second for each SCCP Card

Type of SCCP Card	Transactions per Second
TSM	850
DSM	1700

The system uses the live SCCP transactions-per-second and the number of SCCP transactions the SS7 card can deliver to the SCCP cards to determine if the additional LIM card transactions-per-second rating will exceed the SCCP transactions-per-second threshold. Table 3-7 shows the card types that can be in the database, card applications that can be assigned to these cards, the type of signaling link that is assigned to the card running that application, and the number of SCCP transactions the card can deliver to an SCCP card. Please refer to Tables 3-6 and 3-7 to determine the transactions-per-second rating of a card.

Table 3-7. SS7 Card Applications and Signaling Link Types

Card Type	Card Application	Signaling Link Assigned to the Card	Number of SCCP Transactions per Second
limds0	ss7ansi, ss7gx25, ccs7itu	Low-speed signaling link	53
limocu	ss7ansi, ss7gx25, ccs7itu	Low-speed signaling link	53
limv35	ss7ansi, ss7gx25, ccs7itu	Low-speed signaling link	53
limds0 (Multi-Port LIM)	ss7ansi	Low-speed signaling link	186
lime1 & limch (2-port LIM-E1)	ss7ansi, ccs7itu	E1 signaling link	53
lime1, limt1, limch (8-port E1/T1 MIM)	ss7ansi, ccs7itu	E1 and T1 signaling links	53
limatm	atmansi	High-speed signaling link	480
lime1atm	atmitu	E1 ATM high-speed signaling link	480
dcm	iplim, iplimi	IP Link	1000

The `rept-stat-sccp` output shows the status of the SCCP cards and the GTT (Global Title Translation), G-Flex (GSM Flexible Numbering), or INP (INAP-based Number Portability) services executing on those cards. This command also displays the SCCP capacity threshold, in the **System TPS Alarm Threshold** field, and the average SCCP capacity, in the **SCCP Service Average MSU Capacity** field. The **MSU USAGE** field shows the percentage of MSUs each SCCP card is processing.

```

rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
SCCP SUBSYSTEM REPORT IS-NR          Active      -----
SCCP Cards Configured=2  Cards IS-NR=2
System TPS Alarm Threshold = 80% Total Capacity
System Peak SCCP Load = 550 TPS
System Total SCCP Capacity = 1700 TPS

CARD   VERSION   PST      SST      AST      MSU USAGE  CPU USAGE
-----
1101   114-001-000  IS-NR    Active   -----    47%        54%
1301   114-001-000  IS-NR    Active   -----    34%        31%
-----
SCCP Service Average MSU Capacity = 41%      Average CPU Capacity = 43%
Command Completed.
    
```

If the `mode=perf` parameter is specified with the `rept-stat-sccp` command, the general SCCP traffic performance including the total number of SCCP transactions per second the system currently contains. The SCCP capacity threshold is shown in the **System TPS Alarm Threshold** field, and the average SCCP capacity is shown in the **AVERAGE MSU USAGE** field.

```

rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
SCCP SUBSYSTEM REPORT IS-NR      Active      -----
SCCP Cards Configured=2  Cards IS-NR=2
System TPS Alarm Threshold = 80% Total Capacity
System Peak SCCP Load = 550 TPS
System Total SCCP Capacity = 1700 TPS

```

TPS STATISTICS

```

=====
CARD   CPU      TOTAL    CLASS 0   Class 1
      USAGE  MSU RATE TVG RATE  TVG RATE
-----
1101   54%      850      770       80
1301   31%      490      400       90
-----

```

```

AVERAGE MSU USAGE = 44%
AVERAGE CPU USAGE = 24%
TOTAL MSU RATE     = 1440

```

STATISTICS FOR PAST 30 SECONDS

```

=====
TOTAL TRANSACTIONS:  5400
TOTAL ERRORS:       5
Command Completed.

```

For more information on the **rept-stat-sccp** command, go to the *Commands Manual*.

When a new SS7 card is being added to the database, the number of transactions per second the new SS7 card is expected to deliver to the SCCP card is added to the average number of transactions per second the existing SS7 cards are delivering to the SCCP cards. If this sum is above the SCCP card threshold, the **ent-card** command is rejected with command rejected error message E3715.

```

E3715 Cmd Rej: SYSTEM CURRENT RATED TPS UNABLE TO SUPPORT ADDITIONAL SS7
CARD - USE FORCE=YES

```

A warning message is also displayed in the scroll area of the terminal display.

```

WARNING: Insufficient system TPS to support addition of new SS7 card.

```

The SS7 card can still be added to the database by adding more SCCP cards to the database, by raising the SCCP alarm threshold with the **chg-th-sccp** command, or by specifying the **force=yes** parameter with the **ent-card** command. When the **force=yes** parameter is specified, the **ent-card** command is accepted, but the warning message is displayed in the scroll area of the terminal display.

If the system does not have enough SCCP cards in the database and the **force=yes** parameter is used with the **ent-card** command, it is recommended that the required number of SCCP cards be added to the database after the SS7 card is added to avoid losing GTT traffic.

To add more SCCP cards to the database, perform the “Adding an SCCP Card” procedure in the *Database Administration Manual - Global Title Translation*.

Procedure

1. Display the cards in the database using the `rtrv-card` command. This is an example of the possible output. Cards should be distributed throughout the system for proper power distribution. Refer to the *Installation Manual* for the shelf power distribution.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CARD  TYPE      APPL      LSET NAME  PORT SLC  LSET NAME  PORT SLC
1101  TSM          SCCP      -----  --  --  -----  --  --
1102  TSM          GLS       -----  --  --  -----  --  --
1113  GSPM         EOAM
1114  TDM-A
1115  GSPM         EOAM
1116  TDM-B
1117  MDAL
1118  RESERVED
1201  LIMDS0      SS7ANSI   sp2        A    0    sp1        B    0
1203  LIMDS0      SS7ANSI   sp3        A    0    -----  --  --
1204  LIMDS0      SS7ANSI   sp3        A    1    -----  --  --
1206  LIMDS0      SS7ANSI   nsp3       A    1    nsp4       B    1
1207  LIMV35      SS7GX25   nsp1       A    0    -----  --  --
1208  LIMV35      SS7GX25   nsp1       A    1    -----  --  --
1216  ACMENET     STPLAN   -----  --  --  -----  --  --
1301  LIMDS0      SS7ANSI   sp6        A    1    sp7        B    0
1302  LIMDS0      SS7ANSI   sp7        A    1    sp5        B    1
1303  DCM         IPLIM     ipnode1    A    0    ipnode3    B    1
1305  DCM         IPLIM     ipnode4    A    0    -----  --  --
1307  ACMENET     STPLAN   -----  --  --  -----  --  --
```

The cards should be distributed throughout the system for proper power distribution. Refer to the *Installation Manual* for the shelf power distribution.

If the global title translation feature is on, verify that the database contains SCCP cards (cards running the SCCP or VSCCP applications and shown by the entries **SCCP** and **VSCCP** in the **APPL** field) to support the number of LIMs or IP cards the database will contain when the new IP card is added to the database. If the `rtrv-card` command output shows the entry **SCCP** or **VSCCP** in the **APPL** field, then the global title translation field is on. An SCCP card cannot be in the database if the global title translation feature is not on. The **GTT** field in the `rtrv-feat` command output also shows whether or not the global title translation feature is on.

If the system contains a large number of cards, go to step 3 and execute the `rept-stat-sccp` command. Using the `rept-stat-sccp` command can make it easier to determine the number of SCCP cards because the `rept-stat-sccp` command only displays the cards running the SCCP or VSCCP applications, the SCCP cards.

If there are not enough SCCP cards, the **force=yes** parameter must be specified with the `ent-card` command. Additional SCCP cards can be added to the database by performing the “Adding an SCCP Card” procedure in the *Database Administration Manual - Global Title Translation*.

If there are no SCCP cards shown in the `rtrv-card` output, go to step 3 to verify whether or not the Global Title Translation feature is on.

- Verify that the card to be entered has been physically installed into the proper location (see the Card Slot Selection section on page 3-17).



CAUTION: If the version of the BPDCM GPL on the IP card does not match the BPDCM GPL version in the database when the IP card is inserted into the card slot, UAM 0002 is generated indicating that these GPL versions do not match. If UAM 0002 has been generated, perform the alarm clearing procedure for UAM 0002 in the *Maintenance Manual* before proceeding with this procedure.

NOTE: If step 1 shows SCCP cards in the database, skip this step and go to step 4.

- Verify whether or not that the global title translation feature is on, by entering the `rtrv-feat` command. If the global title translation feature is on, the entry `GTT = on` appears in the `rtrv-feat` command output.

NOTE: The `rtrv-feat` command output contains other fields that are not used by this procedure. If you wish to see all the fields displayed by the `rtrv-feat` command, see the `rtrv-feat` command description in the *Commands Manual*.

NOTE: If the Global Title Translation feature is not on, skip this step, and go to step 5.

- Display the status of the SCCP cards by entering the `rept-stat-sccp` command. This is an example of the possible output.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
SCCP SUBSYSTEM REPORT IS-NR          Active      -----
      SCCP Cards Configured= 1  Cards IS-NR= 1  Capacity Threshold = 80%
      CARD  VERSION      PST              SST          USAGE
      -----
      1101  114-002-001  IS-NR              Active        56%
      -----
SCCP Service Average Capacity = 56%
Command Completed.
```

NOTE: If the application being assigned to the card is either IPLIM or IPLIMI, skip steps 5 and 6, and go to step 7.

- If the ISUP-over-IP (`ipisup`) feature or the Dynamic Routing Key (`dynrtk`) feature are to be used, verify that these features are on by entering the `rtrv-feat` command. If the `rtrv-feat` command was performed in step 3, do not execute this command here, but use the output from step 3 to determine these features are on. If the ISUP-over-IP feature is on, the `ipisup` field is set to `on`. If the Dynamic Routing Key feature is on, the `dynrtk` field is set to `on`.

NOTE: The `rtrv-feat` command output contains other fields that are not used by this procedure. If you wish to see all the fields displayed by the `rtrv-feat` command, see the `rtrv-feat` command description in the *Commands Manual*.

NOTE: If the features you wish to use are already on, skip this step and go to step 7.

6. Turn the ISUP-over-IP or Dynamic Routing Key features by entering one of these commands, depending of which features are already on, and which ones you wish to turn on.

To enable the ISUP-over-IP feature, enter this command.

```
chg-feat:ipisup=on
```

To enable the Dynamic Routing Key feature, enter this command.

```
chg-feat:dynrtnk=on
```

To enable both features, enter this command.

```
chg-feat:ipisup=on:dynrtnk=on
```

NOTE: Once the ISUP-over-IP feature or Dynamic Routing Key features are turned on with the `chg-feat` command, they cannot be turned off.

NOTE: The ISUP-over-IP feature and Dynamic Routing Key features must be purchased before turning them on. If you are not sure whether you have purchased the ISUP-over-IP feature or Dynamic Routing Key features, contact your Tekelec Sales Representative or Account Representative.

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
CHG-FEAT: MASP A - COMPLTD
```

7. Add the card using the `ent-card` command. If the Global Title Translation feature is on, and the outputs of either the `rtrv-card` command (step 1) or the `rept-stat-sccp` command (step 4) shows that there are not enough SCCP cards to support the number of LIMs or IP cards the database will contain when the new IP card is added to the database, the `force=yes` parameter must be specified with the `ent-card` command. For more information on using the `force` parameter, see "Using the FORCE Parameter" on page 3-18. For this example, enter these commands.

```
ent-card:loc=1202:type=dcn:appl=iplim
```

```
ent-card:loc=1308:type=dcn:appl=iplim
```

```
ent-card:loc=1311:type=dcn:appl=iplim
```

```
ent-card:loc=1313:type=dcn:appl=iplimi
```

```
ent-card:loc=1315:type=dcn:appl=ss7ipgw
```

```
ent-card:loc=1317:type=dcn:appl=ipgwi
```

When each of these commands have successfully completed, this message should appear.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
ENT-CARD: MASP A - COMPLTD
```

- Verify the changes using the **rtrv-card** command with the card location specified. For this example, enter these commands.

rtrv-card:loc=1202

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CARD  TYPE      APPL      LSET NAME      PORT SLC LSET NAME      PORT SLC
1202  DCM          IPLIM          -----      --  --  -----      --  --
```

rtrv-card:loc=1308

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CARD  TYPE      APPL      LSET NAME      PORT SLC LSET NAME      PORT SLC
1308  DCM          IPLIM          -----      --  --  -----      --  --
```

rtrv-card:loc=1311

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CARD  TYPE      APPL      LSET NAME      PORT SLC LSET NAME      PORT SLC
1311  DCM          IPLIM          -----      --  --  -----      --  --
```

rtrv-card:loc=1313

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CARD  TYPE      APPL      LSET NAME      PORT SLC LSET NAME      PORT SLC
1313  DCM          IPLIMI          -----      --  --  -----      --  --
```

rtrv-card:loc=1315

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CARD  TYPE      APPL      LSET NAME      PORT SLC LSET NAME      PORT SLC
1315  DCM          SS7IPGW          -----      --  --  -----      --  --
```

rtrv-card:loc=1317

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CARD  TYPE      APPL      LSET NAME      PORT SLC LSET NAME      PORT SLC
1317  DCM          IPGWI          -----      --  --  -----      --  --
```

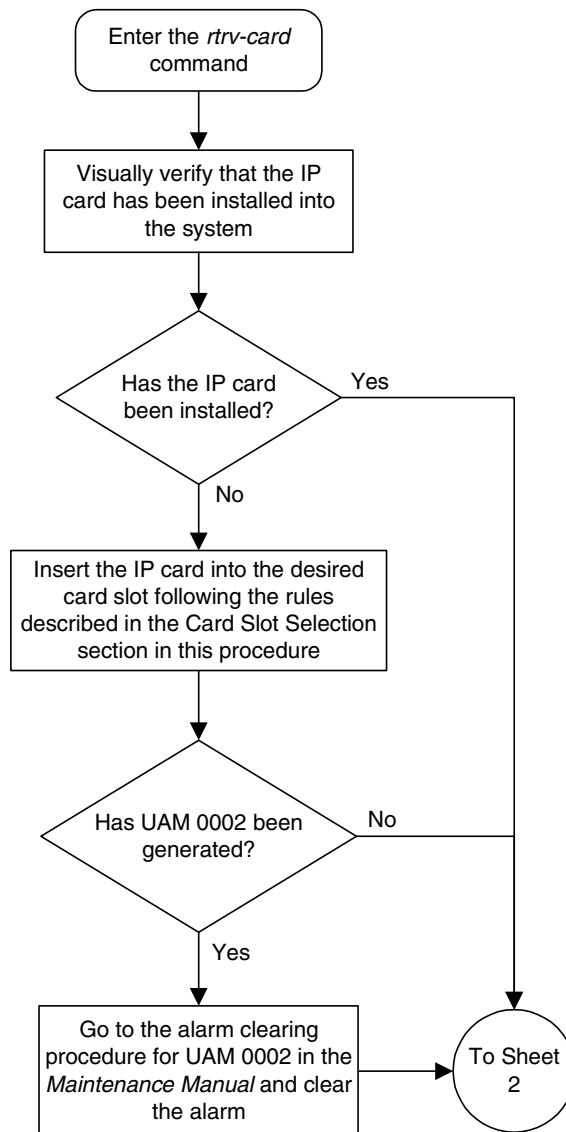
- Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

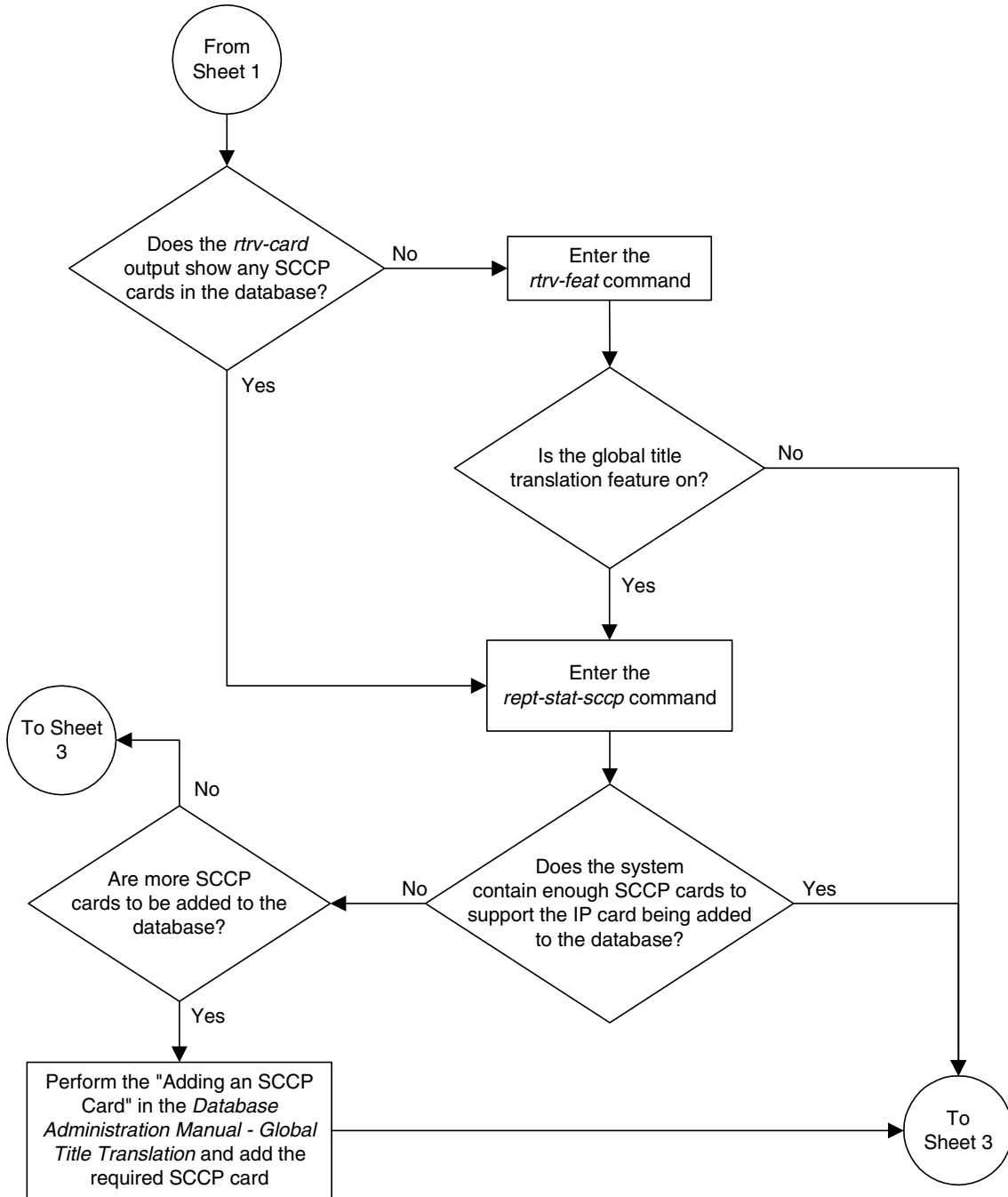
- If you wish to change the quantity of static and dynamic routing keys in the database, perform the "Changing IP Options other than SYNC and SCTPCSUM" procedure on page 3-148. Otherwise, this procedure is finished.

Flowchart 3-1. Adding an IP Card (Sheet 1 of 6)

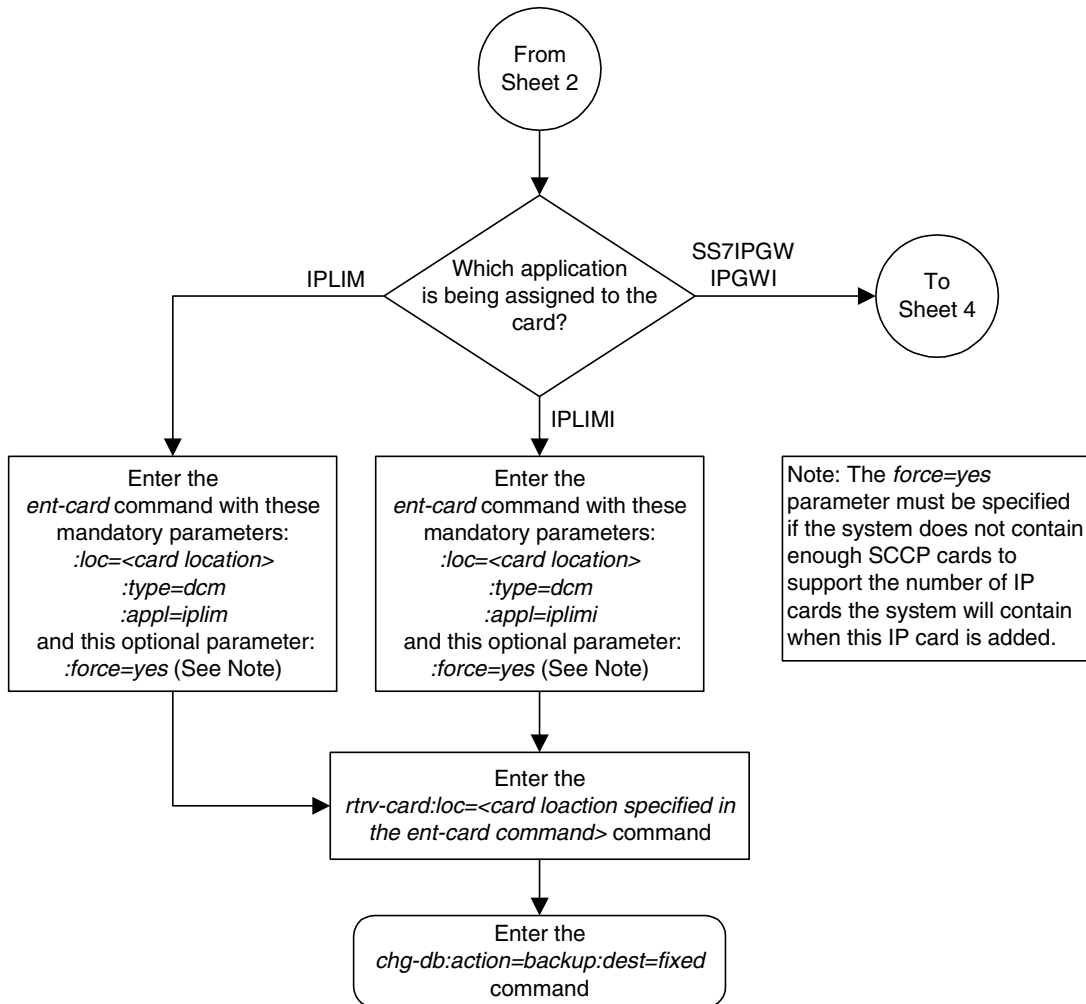
NOTE: Before executing this procedure, make sure you have purchased the ISUP-over-IP feature and Dynamic Routing Key features. If you are not sure whether you have purchased the ISUP-over-IP feature or Dynamic Routing Key features, contact your Tekelec Sales Representative or Account Representative.



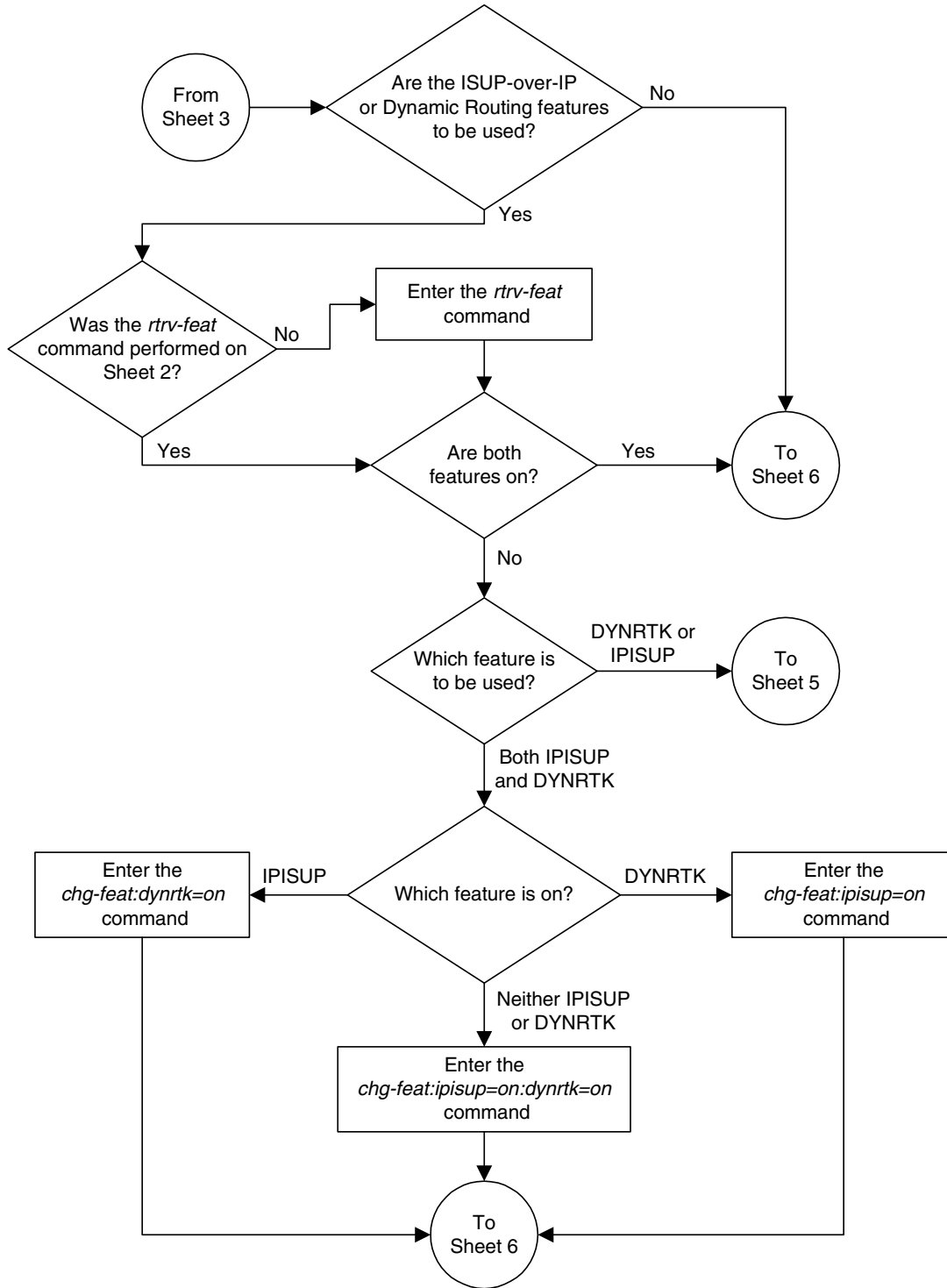
Flowchart 3-1. Adding an IP Card (Sheet 2 of 6)



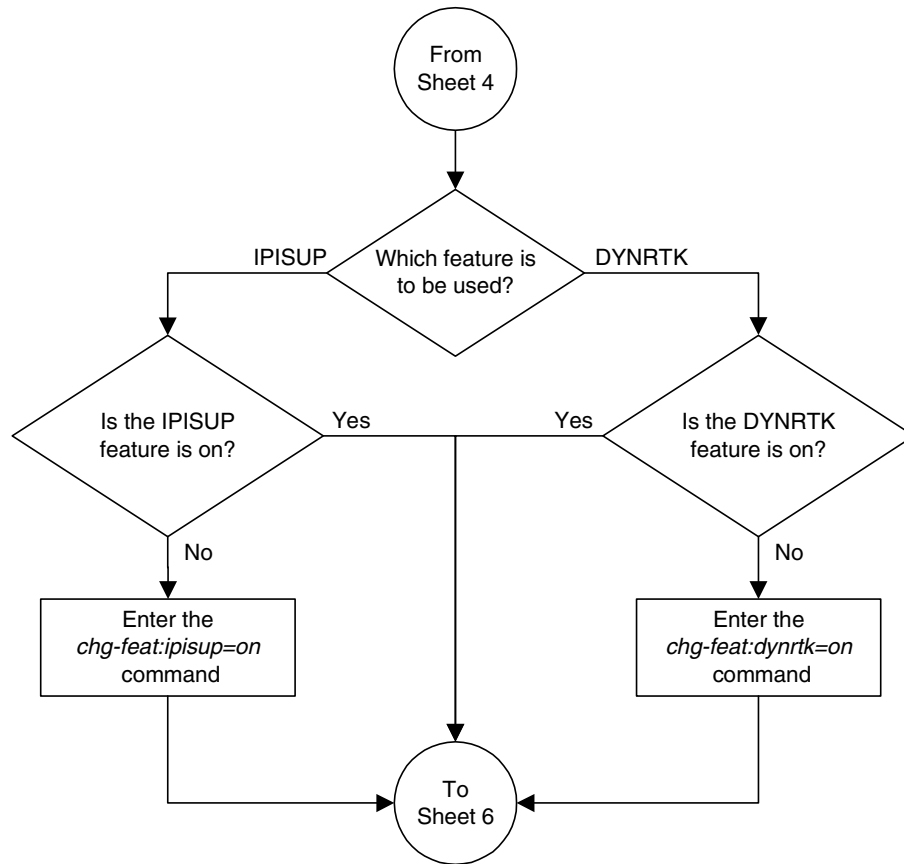
Flowchart 3-1. Adding an IP Card (Sheet 3 of 6)



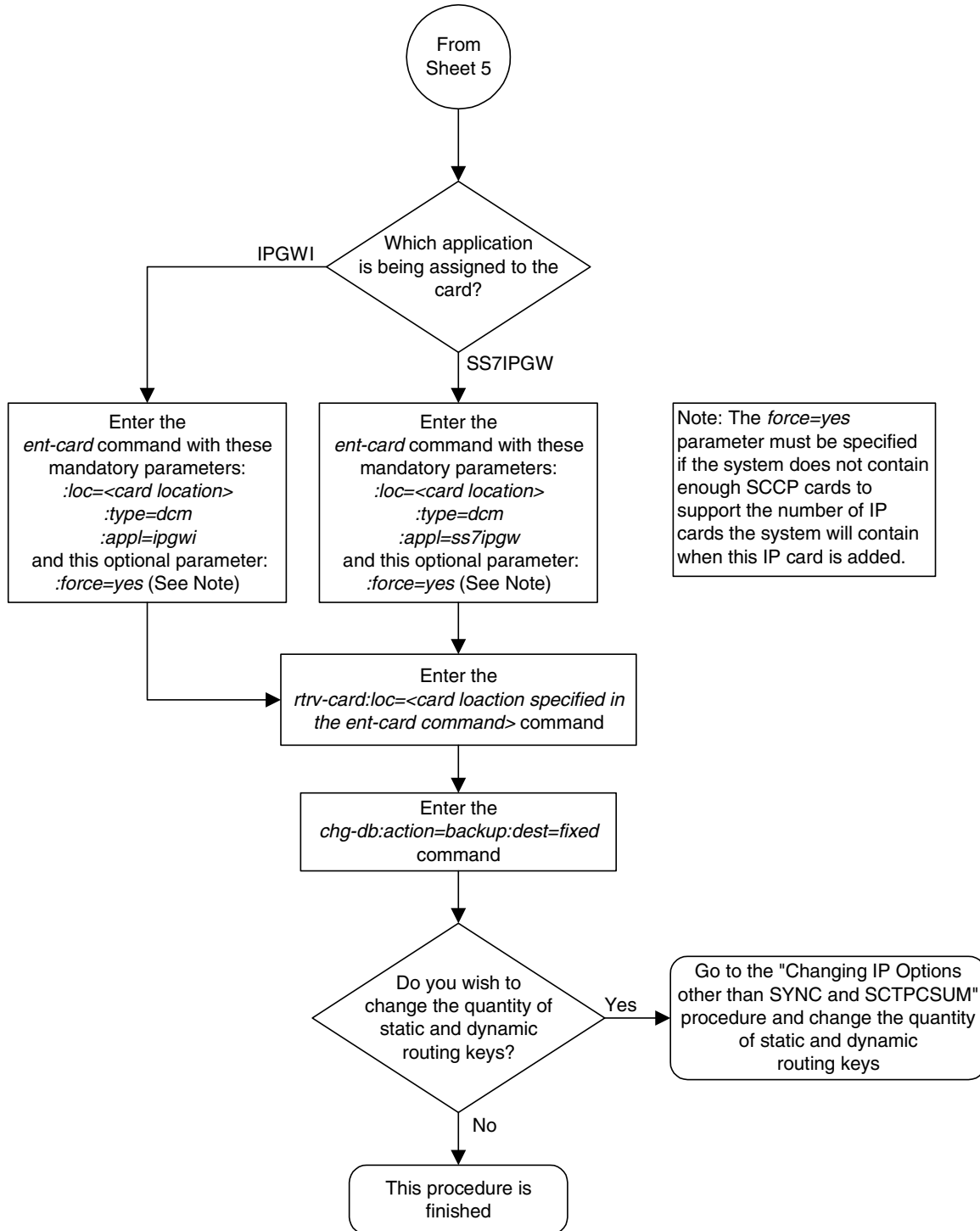
Flowchart 3-1. Adding an IP Card (Sheet 4 of 6)



Flowchart 3-1. Adding an IP Card (Sheet 5 of 6)



Flowchart 3-1. Adding an IP Card (Sheet 6 of 6)



Removing an IP Card

Use this procedure to remove an IP card, a card running one of these applications: `iplim`, `iplimi`, `ss7ipgw`, `ipgwi`, from the database using the `dlc-card` command.

The card cannot be removed if it does not exist in the database. Prior to removing the card from the database, the signaling links assigned to the card must be removed.



CAUTION: If the IP card is the last IP card in service, removing this card from the database will cause traffic to be lost.

Procedure

1. Display the cards in the database using the `rtrv-card` command. This is an example of the possible output.

```
rlghncxa03w 04-12-15 16:34:56 GMT EAGLE5 31.10.0
CARD  TYPE      APPL      LSET NAME      PORT  SLC  LSET NAME      PORT  SLC
1101  TSM          SCCP      -----      --   --  -----      --   --
1102  TSM          GLS       -----      --   --  -----      --   --
1103  ACMENET     STPLAN   -----      --   --  -----      --   --
1104  ACMENET     STPLAN   -----      --   --  -----      --   --
1113  GSPM        EOAM
1114  TDM-A
1115  GSPM        EOAM
1116  TDM-B
1117  MDAL
1201  LIMDS0     SS7ANSI   lsn1           A     0    lsn2           B     1
1202  LIMV35     SS7GX25   lsngwy         A     0    -----      --   --
1203  LIMV35     SS7ANSI   lsn2           A     0    lsn1           B     1
1204  LIMATM     ATMANSI   atmgwy         A     0    -----      --   --
1205  DCM        IPLIM     ipnode1        A     0    ipnode3        B     1
1207  DCM        IPLIM     ipnode2        A     0    -----      --   --
1303  DCM        IPLIM     ipnode1        A     0    ipnode3        B     1
1305  DCM        IPLIM     ipnode4        A     0    -----      --   --
```

Determine the cards to be removed from the database. The examples in this procedure are used to remove the IP cards in card locations 1205 and 1207.

The card location is shown in the `CARD` field of the `rtrv-card` command output. Dashes in the `PORT A LSET` or `PORT B LSET` fields mean that no signaling link has been assigned to the respective port.

2. Display the status of the SS7 signaling links assigned to the IP cards you wish to remove. Enter the **rept-stat-slk** command and specify the card location (**CARD** column) and port (**PORT** column) shown in step 1. The status of the signaling link is indicated in the PST field.

For this example, enter the following commands:

```
rept-stat-slk:loc=1205:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1205,A   ipnode1   -----  IS-NR    Avail    ----
  ALARM STATUS      = No Alarms.
  UNAVAIL REASON    = --
Command Completed.
```

```
rept-stat-slk:loc=1205:port=b
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1205,B   ipnode3   -----  IS-NR    Avail    ----
  ALARM STATUS      = No Alarms.
  UNAVAIL REASON    = --
Command Completed.
```

```
rept-stat-slk:loc=1207:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1207,A   ipnode2   -----  IS-NR    Avail    ----
  ALARM STATUS      = No Alarms.
  UNAVAIL REASON    = --
Command Completed.
```

If the signaling link status is in-service normal (IS-NR), go to step 3.

If the signaling link status is out-of-service maintenance-disabled (OOS-MT-DSBLD), go to step 4.

3. Deactivate any links shown in step 2 whose state is not OOS-MT-DSBLD using the **dact-slk** command. For this example, enter these commands.

```
dact-slk:loc=1205:port=a
```

```
dact-slk:loc=1205:port=b
```

```
dact-slk:loc=1207:port=a
```

When these commands have successfully completed, this message appears.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
Deactivate Link message sent to card
```

- Verify the new link status. Enter the **rept-stat-slk** command and specify card location and port of the signaling link. The status of the signaling link is indicated in the **PST** field.

For this example, enter the following commands:

```
rept-stat-slk:loc=1205:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1205,A   ipnode1   -----  OOS-MT-DSBLD Avail  ----
ALARM STATUS      = * 0236 REPT-LKS:not aligned.
UNAVAIL REASON    = NA
Command Completed.
```

```
rept-stat-slk:loc=1205:port=b
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1205,B   ipnode3   -----  OOS-MT-DSBLD Avail  ----
ALARM STATUS      = * 0236 REPT-LKS:not aligned.
UNAVAIL REASON    = NA
Command Completed.
```

```
rept-stat-slk:loc=1207:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1207,A   ipnode2   -----  OOS-MT-DSBLD Avail  ----
ALARM STATUS      = * 0236 REPT-LKS:not aligned.
UNAVAIL REASON    = NA
Command Completed.
```

- Display the cards that are in service with the **rept-stat-card:stat=nr** command. For this example, enter the following command.

```
rept-stat-card:stat=nr
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 16:43:42 GMT EAGLE5 31.10.0
CARD  VERSION      TYPE  APPL      PST      SST      AST
1101  114-003-000    TSM   SCCP      IS-NR    Active   ---
1102  114-003-000    TSM   GLS       IS-NR    Active   ---
1103  114-002-000    ACMENET STPLAN  IS-NR    Active   ---
1109  114-003-000    HMUX   BPHMUX    IS-NR    Active   ---
1110  114-003-000    HMUX   BPHMUX    IS-NR    Active   ---
1113  114-002-000    GPSP   EOAM      IS-NR    Active   ---
1114  114-002-000    TDM                    IS-NR    Active   ---
1115  114-002-000    GPSP   EOAM      IS-NR    Active   ---
1116  114-002-000    TDM                    IS-NR    Active   ---
1117  114-002-000    MDAL                    IS-NR    Active   ---
1201  114-003-000    LIMDS0 SS7ANSI   IS-NR    Active   ---
1202  114-002-000    LIMV35 SS7GX25   IS-NR    Active   ---
1203  114-003-000    LIMV35 SS7ANSI   IS-NR    Active   ---
1204  114-003-000    LIMATM ATMANSI   IS-NR    Active   ---
1205  114-001-000    DCM    IPLIM     IS-NR    Active   ---
1207  114-001-000    DCM    IPLIM     IS-NR    Active   ---
1209  114-003-000    HMUX   BPHMUX    IS-NR    Active   ---
1210  114-003-000    HMUX   BPHMUX    IS-NR    Active   ---
```

1303	114-001-000	DCM	IPLIM	IS-NR	Active	---
1305	114-001-000	DCM	IPLIM	IS-NR	Active	---
1309	114-003-000	HMUX	BPHMUX	IS-NR	Active	---
1310	114-003-000	HMUX	BPHMUX	IS-NR	Active	---

6. If the signaling link assigned to the card to be removed from the database is the last signaling link in a linkset, the **force=yes** parameter must be used when deleting the link with the **dlt-slk** command. Verify the number of links in the linkset using the **rtrv-ls** command and specifying the linkset name (shown in step 1 in the **PORT A LSET** field) for the respective link. For this example, enter the following commands.

rtrv-ls:lsn=ipnode1

This is an example of the possible output

```
rlghncxa03w 04-12-28 16:31:35 GMT EAGLE5 31.10.0
                                L3T SLT                                GWS GWS GWS
LSN          APCA  (SS7)  SCRNL  SET SET BEI LST LNKS ACT MES DIS SLSCI NIS
ipnode1      240-020-000  scr1  1   1  yes A   2   off off off yes  off

                                IPGWAPC MATELSN      IPTPS LSUSEALM SLKUSEALM
                                no          -----   ---   ---   ---

                                L2T          L1          PCR  PCR
                                SET  BPS      MODE TSET  ECM   N1   N2

                                LOC  PORT SLC TYPE      SET  BPS      MODE TSET  ECM   N1   N2

                                LP          ATM
                                SET  BPS      TSEL          VCI   VPI   LL

                                LOC  PORT SLC TYPE      SET  BPS      TSEL          VCI   VPI   LL

                                LP          ATM          E1ATM
                                SET  BPS      TSEL          VCI   VPI   CRC4 SI SN

                                LOC  PORT SLC TYPE      IPLIML2
                                1205 A    0  IPLIM  SAALTALI
                                1303 A    0  IPLIM  SAALTALI

                                LOC  PORT SLC TYPE

                                L2T          L1          PCR  PCR  E1   E1
                                SET  BPS      ECM   N1   N2  LOC  PORT TS

                                LOC  PORT SLC TYPE      SET  BPS      ECM   N1   N2  LOC  PORT TS

                                L2T          L1          PCR  PCR  T1   T1
                                SET  BPS      ECM   N1   N2  LOC  PORT TS

Link set table is ( 10 of 1024) 1% full
;
```

rtrv-ls:lsn=ipnode2

This is an example of the possible output

```
rlghncxa03w 04-12-28 16:31:35 GMT EAGLE5 31.10.0
                                L3T SLT                                GWS GWS GWS
LSN          APCA  (SS7)  SCRNL  SET SET BEI LST LNKS ACT MES DIS SLSCI NIS
ipnode2      240-030-000  scr1  1   1  yes A   2   off off off yes  off

                                IPGWAPC MATELSN      IPTPS LSUSEALM SLKUSEALM
                                no          -----   ---   ---   ---

                                L2T          L1          PCR  PCR
                                SET  BPS      MODE TSET  ECM   N1   N2

                                LOC  PORT SLC TYPE      SET  BPS      MODE TSET  ECM   N1   N2
```


IP7 Secure Gateway Configuration Procedures

```

LOC  PORT  SLC  TYPE          LP          ATM
SET  BPS          TSEL          VCI    VPI    LL

LOC  PORT  SLC  TYPE          LP          ATM          E1ATM
SET  BPS          TSEL          VCI    VPI    CRC4  SI  SN

LOC  PORT  SLC  TYPE          IPLIML2
1207 A      0  IPLIM          SAALTALI

LOC  PORT  SLC  TYPE

LOC  PORT  SLC  TYPE          L2T          PCR  PCR  E1  E1
SET  BPS          ECM    N1  N2  LOC  PORT  TS

LOC  PORT  SLC  TYPE          L2T          PCR  PCR  T1  T1
SET  BPS          ECM    N1  N2  LOC  PORT  TS

```

Link set table is (10 of 1024) 1% full

rtrv-ls:lsn=ipnode3

This is an example of the possible output

```

rlghncxa03w 04-12-28 16:31:35 GMT EAGLE5 31.10.0
                                L3T  SLT          GWS  GWS  GWS
LSN          APCA  (SS7)  SCRN  SET  SET  BEI  LST  LNKS  ACT  MES  DIS  SLSCI  NIS
ipnode3      240-020-000  scr1  1   1   yes  A   2   off  off  off  yes  off

IPGWAPC  MATELSN          IPTPS  LSUSEALM  SLKUSEALM
no          -----      ---   ---       ---

LOC  PORT  SLC  TYPE          L2T          L1          PCR  PCR
SET  BPS          MODE  TSET  ECM    N1  N2

LOC  PORT  SLC  TYPE          LP          ATM
SET  BPS          TSEL          VCI    VPI    LL

LOC  PORT  SLC  TYPE          LP          ATM          E1ATM
SET  BPS          TSEL          VCI    VPI    CRC4  SI  SN

LOC  PORT  SLC  TYPE          IPLIML2
1205 A      0  IPLIM          SAALTALI
1303 A      0  IPLIM          SAALTALI

LOC  PORT  SLC  TYPE

LOC  PORT  SLC  TYPE          L2T          PCR  PCR  E1  E1
SET  BPS          ECM    N1  N2  LOC  PORT  TS

LOC  PORT  SLC  TYPE          L2T          PCR  PCR  T1  T1
SET  BPS          ECM    N1  N2  LOC  PORT  TS

```

Link set table is (10 of 1024) 1% full

7. Inhibit the card using the **inh-card** command and specifying the card location. If the IP card to be inhibited contains the only signaling link in the linkset that is in service, the **force=yes** parameter must also be specified. For this example, enter these commands.

```
inh-card:loc=1205
```

```
inh-card:loc=1207:force=yes
```

When these commands have successfully completed, this message appears.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
Card has been inhibited.
```

8. Verify the changes with the **rept-stat-card** command. This is an example of the possible output.

```
rlghncxa03w 04-12-27 16:43:42 GMT EAGLE5 31.10.0
CARD  VERSION      TYPE      APPL      PST          SST          AST
1101  114-003-000    TSM       SCCP      IS-NR        Active       ---
1102  114-003-000    TSM       GLS       IS-NR        Active       ---
1103  114-002-000    ACMENET   STPLAN    IS-NR        Active       ---
1109  114-003-000    HMUX     BPHMUX    IS-NR        Active       ---
1110  114-003-000    HMUX     BPHMUX    IS-NR        Active       ---
1113  114-002-000    GPMS      EOAM      IS-NR        Active       ---
1114  114-002-000    TDM              IS-NR        Active       ---
1115  114-002-000    GPMS      EOAM      IS-NR        Active       ---
1116  114-002-000    TDM              IS-NR        Active       ---
1117  114-002-000    MDAL              IS-NR        Active       ---
1201  114-003-000    LIMDS0    SS7ANSI   IS-NR        Active       ---
1202  114-002-000    LIMV35    SS7GX25   IS-NR        Active       ---
1203  114-003-000    LIMV35    SS7ANSI   IS-NR        Active       ---
1204  114-003-000    LIMATM    ATMANSI   IS-NR        Active       ---
1205  114-001-000    DCM       IPLIM     OOS-MT-DSBLD  Isolated    ---
1207  114-001-000    DCM       IPLIM     OOS-MT-DSBLD  Isolated    ---
1209  114-003-000    HMUX     BPHMUX    IS-NR        Active       ---
1210  114-003-000    HMUX     BPHMUX    IS-NR        Active       ---
1303  114-001-000    DCM       IPLIM     IS-NR        Active       ---
1305  114-001-000    DCM       IPLIM     IS-NR        Active       ---
1309  114-003-000    HMUX     BPHMUX    IS-NR        Active       ---
1310  114-003-000    HMUX     BPHMUX    IS-NR        Active       ---
```

9. Remove the signaling links on the specified card by using the **dlt-slk** command. If the output of step 6 shows that the signaling link being removed is the last signaling link in a linkset, the **force=yes** parameter must be used. For this example, enter these commands.

```
dlt-slk:loc=1205:port=a
dlt-slk:loc=1205:port=b
dlt-slk:loc=1207:port=a:force=yes
```

When these commands have successfully completed, this message appears.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
DLT-SLK: MASP A - COMPLTD
```

10. Remove the card from the database using the **dlt-card** command. The **dlt-card** command has only one parameter, **loc**, which is the location of the card. For this example, enter these commands.

```
dlt-card:loc=1205
dlt-card:loc=1207
```

When these commands have successfully completed, this message appears.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
DLT-CARD: MASP A - COMPLTD
```

11. Verify the changes using the **rtrv-card** command and specifying the card that was removed in step 10. For this example, enter these commands.

```
rtrv-card:loc=1205
rtrv-card:loc=1207
```

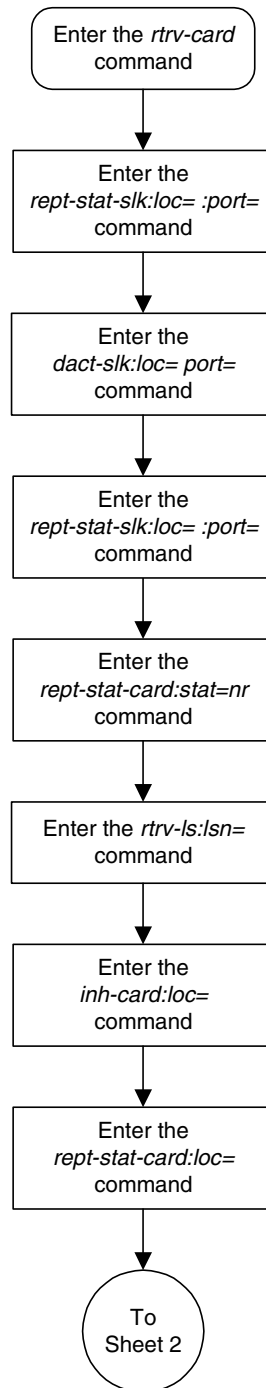
When these commands have successfully completed, this message appears.

```
E2144 Cmd Rej: Location invalid for hardware configuration
```

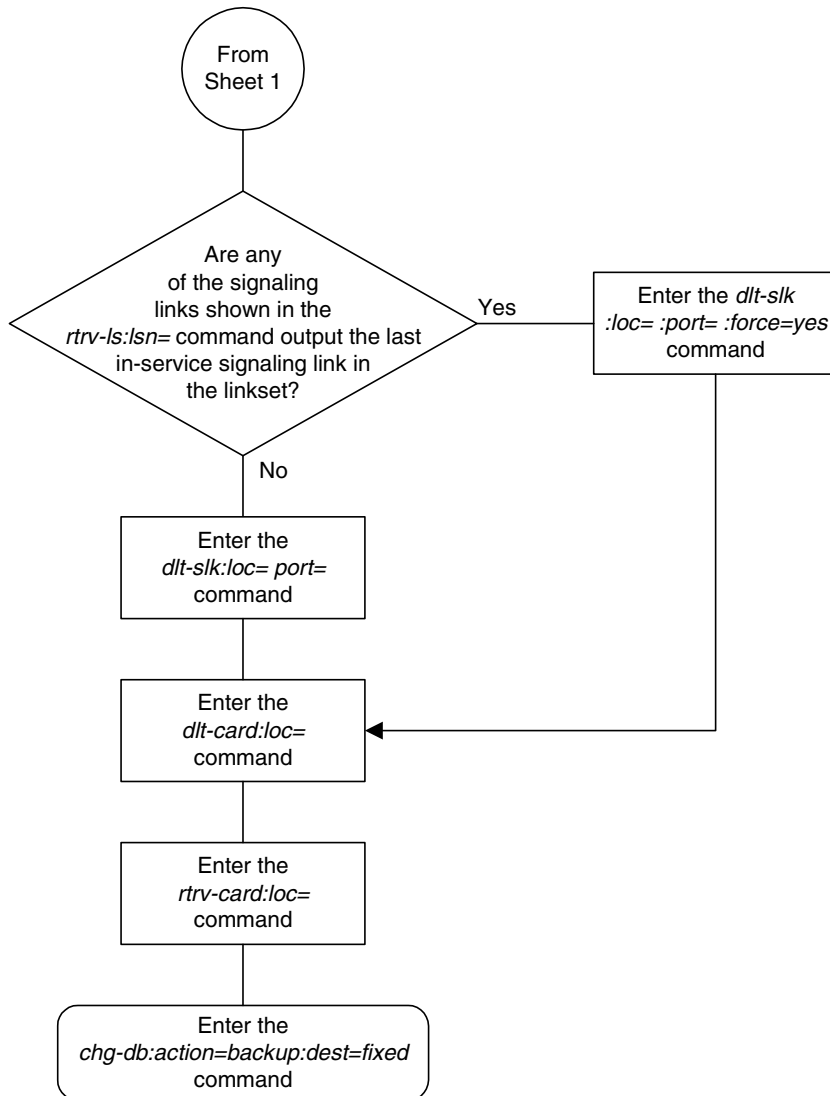
12. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-2. Removing an IP Card (Sheet 1 of 2)



Flowchart 3-2. Removing an IP Card (Sheet 2 of 2)



Configuring an IPGWx Linkset

This procedure is used to configure IPGWx linksets in the system using the `ent-1s` or `chg-1s` commands with these parameters. An IPGWx linkset is a linkset that contains signaling links running either the SS7IPGW or IPGWI applications.

NOTE: This procedure is not used to configure a mate IPGWx linkset, with the `mate1sn` and `action` parameters. To configure a mate IPGWx linkset, perform the “Configuring a Mate IPGWx Linkset” procedure on page 3-60.

:1sn – The name of the linkset. The linkset name can contain up to 10 characters, with the first character being a letter. However, the SEAS interface supports only eight characters. If this linkset is displayed on the SEAS interface and the linkset name contains more than eight characters, only the first eight characters in the linkset name are shown. If this linkset name contains more than eight characters, and is specified with the linkset commands on the SEAS interface, only the first eight characters can be specified.

:apc/apca/apci/apcn/apcn24 – Adjacent point code – the point code identifying the node that is next to the system

NOTE: See the “Point Code Formats” section in the *Database Administration Manual - SS7* for a definition of the point code types that are used on the system and for a definition of the different formats that can be used for ITU national point codes.

NOTE: The `apc/apca/apci/apcn/apcn24` parameter must be specified with the `ent-1s` command. Specifying this parameter with the `chg-1s` command is required only if the adjacent point code of the linkset is being changed. See the “Changing an SS7 Linkset” procedure in the *Database Administration Manual - SS7* for more information on changing the adjacent point code of the linkset.

:1st – The linkset type of the specified linkset - The `1st` parameter must be specified with the `ent-1s` command. Specifying this parameter with the `chg-1s` command is required only if the linkset type of the linkset is being changed.

:ipgwapc – IP Gateway Adjacent Point Code indicator. Specify the `ipgwapc=yes` parameter to provide SS7 linkset definition compatibility for gateway connections to IP-SCPs. This parameter can be specified only for, and must be specified for linksets containing signaling links assigned to either the SS7IPGW or IPGWI applications. The default is `ipgwapc=no`.

NOTE: The `ipgwapc` parameter can be specified only with the `ent-1s` command.

To provision ISUP-CIC routing keys, the `ipgwapc=yes` parameter and the IP Gateway ISUP routing feature must be turned on. Verify this with the `rtrv-feat` command. If the IP Gateway ISUP routing feature is turned on,

the `ipisup` field should be set to `on`. If the IP Gateway ISUP routing feature is not turned on, enter the `chg-feat:ipisup=on` command.

NOTE: Once the IP Gateway ISUP routing feature is turned on with the `chg-feat` command, it cannot be turned off.

NOTE: The IP Gateway ISUP routing feature must be purchased before you turn the feature on with the `chg-feat` command. If you are not sure if you have purchased the IP Gateway ISUP routing feature, contact your Tekelec Sales Representative or Account Representative.

`:iptps` – The quantity of IP TPS (transactions per second) that is assigned to the IPGWx linkset, from 100 to 112,000. The total amount of IP TPS for all IPGWx linksets cannot exceed the system-wide IP TPS value shown in the `rept-stat-iptps` output. For more information on the system-wide IP TPS value, see the “Increasing the System-Wide IPGWx Signaling TPS” procedure on page 3-321.

`:lsusealm` – The linkset’s IP TPS alarm threshold, from 10 to 100 percent of the linkset’s IP TPS. When this threshold is reached, a major alarm (UAM 0115) is generated. When the linkset’s IP TPS falls below this threshold, UAM 0115 is automatically cleared and UAM 0118 is generated.

`:slkusealm` – The signaling link IP TPS alarm threshold, from 10 to 100 percent of the signaling link’s fair share of the linkset’s IP TPS or from 10 to 100 percent of the IPGWx card’s capacity (2000 TPS). This threshold is reached when the signaling link’s actual usage exceeds the percentage of the signaling link’s fair share of the linkset’s IP TPS or the percentage of the IPGWx card’s capacity.

A signaling link's fair share of linkset’s IP TPS is the linkset’s IP TPS divided by the number of in-service links in the linkset. For example, if the linkset IP TPS is 4000 and there are 4 signaling links in the linkset, all in-service, then the signaling link's fair-share would be 1000 IP TPS ($4000/4=1000$). Table 3-8 shows this calculation for a linkset with 1, 2, 3 and 4 in-service signaling links.

Table 3-8. Signaling Link Fair Share Example

Number of In-Service Signaling Links	Linkset IP TPS	Signaling Link Fair Share of the Linkset IP TPS
4	4000	1000
3	4000	1333
2	4000	2000
1	4000	4000

When this threshold is exceeded, a minor alarm (UAM 0116) is generated. When the amount of traffic on the signaling link falls below this threshold, UAM 0116 is automatically cleared and UAM 0119 is generated.

The signaling link IP TPS alarm shows that the linkset IP TPS is set too low for the linkset or that the IPGWx card's capacity has been exceeded. Setting the signaling link IP TPS alarm threshold lower than the linkset IP TPS alarm threshold can give the user an earlier indication that the linkset IP TPS is inadequate or that traffic is not balanced across the links in the linkset.

:multgpc – specifies whether multiple group codes (for 14-bit ITU-N point codes) are supported for the linkset. When this parameter value is **yes**, secondary adjacent point codes whose group codes are different from the adjacent point code of the linkset can be assigned to the linkset. If the parameter value is **no**, the group code of the secondary adjacent point code must be the same as the group code of the linkset's adjacent point code. For more information on secondary adjacent point codes, go to the "Configuring an ITU Linkset with a Secondary Adjacent Point Code (SAPC)" procedure in the *Database Administration Manual - SS7*.

This parameter only applies to linksets whose adjacent point codes are either ITU international point codes or ITU national point codes. All the signaling links in this linkset must be assigned to cards running either the IPLIMI or IPGWI applications. For more information on assigning signaling links to cards running the IPLIMI or IPGWI applications, go to the "Adding an IP Signaling Link" procedure on page 3-82.

The ITU duplicate point code feature must be on before this parameter can be specified. Verify this with the **rtrv-feat** command. If the ITU duplicate point code feature is turned on, the **itupuppc** field should be set to **on**. If the ITU duplicate point code feature is not turned on, enter the **chg-feat:itupuppc=on** command.

NOTE: Once the ITU duplicate point code feature is turned on with the **chg-feat** command, it cannot be turned off.

The ITU duplicate point code feature must be purchased before you turn the feature on with the **chg-feat command. If you are not sure if you have purchased the ITU duplicate point code feature, contact your Tekelec Sales Representative or Account Representative.**

The adjacent point code (APC) for the linkset must be defined in the database, must be in the SS7 domain and cannot match the point code or capability point code of the system. The domain of the point code is shown in the **DOMAIN** field in the output of the **rtrv-dstn** command. The point code of the system is shown in the **PCA**, **PCN**, **PCN24**, or **PCI** fields and the capability point code of the system are shown in the **CPCA**, **CPCN**, **CPCN24**, or **CPCI** fields in the output of the **rtrv-sid** command. An ANSI adjacent point code must be a full point code and cannot be a cluster point code or a network routing point code.

If the APC is not in the destination point code table, go to the “Adding a Destination Point Code” procedure in the *Database Administration Manual - SS7* and add the APC to the destination point code table.

For IPGWx linksets, more than one device may be attached to the LAN and have IP connections to the IP card running either the SS7IPGW or IPGWI application. Thus each IPGWx linkset is adjacent to all devices on the LAN (or adjacent to no device on the LAN, depending on your point of view). To provide a scheme allowing this point-to-multipoint connection and maintain consistent SS7 linkset definition rules, a virtual APC is required. This virtual APC is a real SS7 point code that is not used anywhere else in the SS7 network. Virtual APCs assigned to SS7IPGW linksets are ANSI point codes. Virtual APCs assigned to IPGWI linksets are either ITU-I or ITU-N point codes (either 14-bit or 24-bit ITU-N point codes). Virtual point codes can be reused on more than one switch. For example, a mated set of switches, each with two related links, could share two virtual point codes instead of requiring four. DPCs and linksets related to the virtual APC must be defined with the `ipgwapc` parameter set to `yes`.

For provisioning of ISUP-CIC routing keys, the `ipgwapc=yes` parameter and the IP Gateway ISUP routing feature must be turned on. Verify this with the `rtrv-feat` command. If the IP Gateway ISUP routing feature is turned on, the `ipisup` field should be set to `on`. If the IP Gateway ISUP routing feature is not turned on, enter the `chg-feat:ipisup=on` command.

NOTE: Once the IP Gateway ISUP routing feature is turned on with the `chg-feat` command, it cannot be turned off.

The IP Gateway ISUP routing feature must be purchased before you turn the feature on with the `chg-feat` command. If you are not sure if you have purchased the IP Gateway ISUP routing feature, contact your Tekelec Sales Representative or Account Representative.

Other Optional Parameters

Other optional parameters, shown in Table 3-9, can be used with the `ent-1s` or `chg-1s` commands but do not need to be used in this procedure. These parameters are discussed in more detail in either the “Adding an SS7 Linkset” or Changing an SS7 Linkset” procedures in the *Database Administration Manual - SS7*. The `matel1sn` parameter is discussed in more detail in the “Configuring a Mate IPGWx Linkset” procedure on page 3-60.

Table 3-9. Optional Linkset Parameters

clli	sltset	l3tset	scrn	gwsa	gwsm
gwsd	bei	nis	itutfr	mtprse*	slsci
asl8	slsrsb	slsobit	tfatcabmlq	gmscrn	sapci
sapcn	sapcn24	action	matel1sn		
* The <code>mtprse</code> parameter cannot be specified for an IPGWx linkset.					

Canceling the RTRV-LS and RTRV-DSTN Commands

Because the `rtrv-ls` and `rtrv-dstn` commands used in this procedure can output information for a long period of time, the `rtrv-ls` and `rtrv-dstn` commands can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-ls` and `rtrv-dstn` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-ls` or `rtrv-dstn` commands were entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-ls` or `rtrv-dstn` commands were entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-ls` or `rtrv-dstn` commands were entered, from another terminal other than the terminal where the `rtrv-ls` or `rtrv-dstn` commands were entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the system-wide IP TPS usage report, and the IPGWx linksets, by entering the `rept-stat-iptps` command. This is an example of the possible output.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.6.0
IP TPS USAGE REPORT
-----
          THRESH  CONFIG      TPS      PEAK      PEAKTIMESTAMP
-----
SYSTEM
RLGHNCXA03W 100%   30000  TX:   7200    7600  04-06-10 11:40:04
                   RCV:   7200    7600  04-06-10 11:40:04
-----
LSN
LSGW1101      80%   10000  TX:   7200    7600  04-06-10 11:40:04
                   RCV:   7200    7600  04-06-10 11:40:04
LSGW1103      80%   10000  TX:   6700    7600  04-06-10 11:40:04
                   RCV:   6500    7600  04-06-10 11:40:04
LSGW1105      80%   10000  TX:   7300    7450  04-06-10 11:40:04
                   RCV:   7300    7450  04-06-10 11:40:04
-----
Command Completed.
```

If the sum of the IP TPS of all the IPGWx linksets is equal to the configured IP TPS amount shown in this report:

- No new IPGWx linksets can be added
- The linkset IP TPS of any IPGWx existing linkset cannot be increased.

If a new IPGWx linkset is being added in this procedure, and the IP TPS value for this linkset allows the sum of the IP TPS of all the IPGWx linksets to exceed the configured IP TPS amount shown in this report, the new IPGWx linkset cannot be added.

If an existing IPGWx IP TPS value is being changed in this procedure, and the IP TPS value for this linkset allows the sum of the IP TPS of all the IPGWx linksets to exceed the configured IP TPS amount shown in this report, the IPGWx linkset IP TPS value cannot be changed.

To add a new IPGWx linkset or change the IP TPS value of an existing IPGWx linkset when the resulting sum of IP TPS values for all IPGWx linksets will exceed the IP TPS amount shown in this report, the system-wide IP TPS amount must be increased, or the linkset IP TPS of some or all the IPGWx linksets must be reduced to allow for the new IP TPS value for the linkset configured in this procedure.

To increase the system-wide IP TPS amount, perform the “Increasing the System-Wide IPGWx Signaling TPS” procedure on page 3-321. If the system-wide IP TPS amount is 112000, shown in the **CONFIG** column in the **SYSTEM** section of this report, the system-wide IP TPS amount cannot be increased. Skip step 2 and go to step 3.

If the linkset IP TPS values of the IPGWx linksets need to be reduced, perform step 2.

-
2. Reduce the IP TPS values of some or all the IPGWx linksets by entering the **chg-ls** command with the name of each linkset being changed from step 1, and the new IP TPS value. For this example, enter these commands.

```
chg-ls:lsn=ls gw1101:iptps=6000
```

```
chg-ls:lsn=ls gw1103:iptps=6000
```

When the **chg-ls** command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-17 16:23:21 GMT EAGLE5 31.6.0  
Link set table is ( 13 of 1024) 1% full  
CHG-LS: MASP A - COMPLTD
```

NOTE: If the `multgc` parameter is not being specified for the linkset, skip steps 3, 4, 5, and 6, and go to step 7. If the `multgc` parameter value is being changed to `no`, skip steps 3, and 4, and go to step 5. The `multgc` parameter can be specified only for linksets with either ITU-I or 14-bit ITU-N APCs, and linksets that contain signaling links running either the IPLIMI or IPGWI applications.

- To specify the `multgc=yes` parameter with the `ent-ls` or `chg-ls` commands, the ITU Duplicate Point Code feature must be on. For the ITU Duplicate Point Code feature to be on, the Multiple Point Code feature must be on. Enter the `rtrv-feat` command to verify that either of these features are on. The entry `MPC = on` in the `rtrv-feat` command output shows that the Multiple Point Code feature is on. The entry `ITUDUPPC = on` in the `rtrv-feat` command output shows that the ITU Duplicate Point Code feature is on. In this example, both features are off.

NOTE: The `rtrv-feat` command output contains other fields that are not used by this procedure. If you wish to see all the fields displayed by the `rtrv-feat` command, see the `rtrv-feat` command description in the *Commands Manual*.

NOTE: If the ITU Duplicate Point Code feature is on (`ITUDUPPC = on`), skip this step and go to step 5.

- Turn the ITU Duplicate Point Code feature on, and the Multiple Point Code feature if necessary, by entering one of these commands.

To turn the ITU Duplicate Point Code feature on only.

```
chg-feat:ituduppc=on
```

To turn both the ITU Duplicate Point Code and Multiple Point Code features on.

```
chg-feat:mpc=on:ituduppc=on
```

NOTE: Once the ITU Duplicate Point Code and Multiple Point Code features are turned on with the `chg-feat` command, they cannot be turned off.

The ITU Duplicate Point Code and Multiple Point Code features must be purchased before you turn either of these features on with the `chg-feat` command. If you are not sure if you have purchased these features, contact your Tekelec Sales Representative or Account Representative.

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLES 31.6.0
CHG-FEAT: MASP A - COMPLTD
```

NOTE: If the `multgc` parameter value is not being changed, is being changed to `yes`, or if a new linkset is being added, skip steps 5 and 6, and go to step 7.

5. If the `multgc` parameter value is changed to `no`, the linkset can contain only one secondary adjacent point code. An ITU international linkset can contain only one 14-bit ITU national secondary adjacent point code. If the ITU international linkset contains more than one 14-bit ITU national secondary adjacent point code, all but one of these 14-bit ITU national secondary adjacent point codes must be removed from the linkset. An ITU national linkset can contain only one ITU international secondary adjacent point code. All 14-bit ITU-N secondary adjacent point codes must be removed from the linkset. All routes to these secondary adjacent point codes must be removed from the database before the secondary adjacent point codes can be removed.

Display the routes using the secondary adjacent point code being removed from the linkset with the `rtrv-rte` command, specifying the secondary adjacent point code being removed as the value of the `dpc` parameter.

For this example, enter these commands.

```
rtrv-rte:dpcn=11213-de
```

This is an example of the possible output.

```
rlghncxa03w 04-12-07 11:43:04 GMT EAGLE5 31.6.0
DPCI        ALIASI        ALIASN        CLLI        LSN        RC APCI
11213-de    -----
                lsn3        10 11213-de
```

```
rtrv-rte:dpcn=12114-fr
```

This is an example of the possible output.

```
rlghncxa03w 04-12-07 11:43:04 GMT EAGLE5 31.6.0
DPCI        ALIASI        ALIASN        CLLI        LSN        RC APCI
12114-fr    -----
                lsn3        10 12114-fr
```

```
rtrv-rte:dpcn=12115-uk
```

This is an example of the possible output.

```
rlghncxa03w 04-12-07 11:43:04 GMT EAGLE5 31.6.0
DPCI        ALIASI        ALIASN        CLLI        LSN        RC APCI
12115-uk    -----
                lsn3        10 12115-uk
```

If the secondary adjacent point code is assigned to a route, that route must be removed from the database. Perform the "Removing a Route" procedure in the *Database Administration Manual - SS7* to remove the route from the database.

- Remove the secondary adjacent point codes specified in step 5 from the linkset with the **chg-ls** command with the **sapcn** and the **action=delete** parameters. For this example, enter these commands.

```
chg-ls:lsn=lsn3:sapcn=11213-de:action=delete
chg-ls:lsn=lsn3:sapcn=12114-fr:action=delete
chg-ls:lsn=lsn3:sapcn=12115-uk:action=delete
```

When the **chg-ls** command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-17 16:23:21 GMT EAGLE5 31.6.0
Link set table is ( 13 of 255) 5% full
CHG-LS: MASP A - COMPLTD
```

NOTE: If an existing linkset is being changed, skip steps 7 through 12, and go to step 13.

- Display the point code and capability point code of the system by using the **rtrv-sid** command. This is an example of the possible output.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.6.0
PCA          PCI          PCN          CLLI          PCTYPE
001-001-001  1-200-6          13482        rlghncxa03w  OTHER

CPCA
002-002-002      002-002-003      002-002-004      002-002-005
002-002-006      002-002-007      002-002-008      002-002-009
004-002-001      004-003-003      144-212-003

CPCA (LNP)
005-005-002      005-005-004      005-005-005

CPCI
1-001-1          1-001-2          1-001-3          1-001-4

CPCN
02091            02092            02094            02097
02191            02192            11177
```

- Display the adjacent point code of the new linkset in the destination point code table by using the **rtrv-dstn** command and specifying the point code

For this example, enter this command.

```
rtrv-dstn:dpca=009-002-003
```

This is an example of the possible output.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.6.0
DPCA          CLLI          BEI ELEI  ALIASI          ALIASN          DOMAIN
010-020-005  ----- no --- -----             -----             SS7

          SPC          NCAI
          -----          ----
```

Destination table is (29 of 2000) 1% full

If the adjacent point code is not shown in the **rtrv-dstn** command output, the following output is displayed.

DPCA CLLI BEI ELEI ALIASI ALIASN/N24 DOMAIN

No destinations meeting the requested criteria were found

Destination table is (29 of 2000) 1% full

If the adjacent point code is not in the destination point code table, perform the "Adding a Destination Point Code" procedure in the *Database Administration Manual - SS7* and add the adjacent point code to the destination point code table.

9. Display the current linksets in the database using the `rtrv-ls` command. This is an example of the possible output.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.6.0
                L3T SLT                GWS GWS GWS
LSN            APCA   (SS7)  SCRN  SET SET BEI LST LNKS ACT MES DIS SLSCI NIS
ele2           001-207-000  none  1  1  no  B   6   off off off no   off
elm1s1        001-001-001  none  1  1  no  A   7   off off off no   off
elm1s2        001-001-002  none  1  1  no  A   7   off off off no   off
ls1305        000-005-000  none  1  1  no  A   1   off off off no   off
ls1307        000-007-000  none  1  1  no  A   1   off off off no   off
lsgw1101      008-012-003  none  1  1  no  A   1   off off off no   off
lsgw1103      003-002-004  none  1  1  no  A   1   off off off no   off
lsgw1105      009-002-003  none  1  1  no  A   1   off off off no   off

                L3T SLT                GWS GWS GWS
LSN            APCA   (X25)  SCRN  SET SET BEI LST LNKS ACT MES DIS SLSCI NIS

                L3T SLT                GWS GWS GWS
LSN            APCI   (SS7)  SCRN  SET SET BEI LST LNKS ACT MES DIS SLSCI NIS
ele2i         1-207-0      none  1  1  no  B   4   off off off ---  on
ls1315        0-015-0      none  1  1  no  A   1   off off off ---  off
ls1317        0-017-0      none  1  1  no  A   1   off off off ---  on
elm2s1        1-011-1      none  1  1  no  A   7   off off off ---  off
elm2s2        1-011-2      none  1  1  no  A   7   off off off ---  off

                L3T SLT                GWS GWS GWS
LSN            APCN   (SS7)  SCRN  SET SET BEI LST LNKS ACT MES DIS SLSCI NIS

                L3T SLT                GWS GWS GWS
LSN            APCN24 (SS7)  SCRN  SET SET BEI LST LNKS ACT MES DIS SLSCI NIS

Link set table is (13 of 1024) 1% full.
```

NOTE: If you do not wish to use the IP Gateway ISUP routing feature, skip steps 6 and 7, and go to step 8.

10. Verify that the IP Gateway ISUP routing feature is on by entering the `rtrv-feat` command. The entry `IPISUP = on` in the `rtrv-feat` command output shows that the IP Gateway ISUP routing feature is on.

NOTE: The `rtrv-feat` command output contains other fields that are not used by this procedure. If you wish to see all the fields displayed by the `rtrv-feat` command, see the `rtrv-feat` command description in the *Commands Manual*.

NOTE: If the IP Gateway ISUP routing feature is on (`IPISUP = on`), skip this step and go to step 8.

11. Turn the IP Gateway ISUP routing feature on by entering this command.

```
chg-feat:ipisup=on
```

NOTE: Once the IP Gateway ISUP routing feature is turned on with the `chg-feat` command, it cannot be turned off.

NOTE: The IP Gateway ISUP routing feature must be purchased before you turn the feature on with the `chg-feat` command. If you are not sure if you have purchased the IP Gateway ISUP routing feature, contact your Tekelec Sales Representative or Account Representative.

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.6.0
CHG-FEAT: MASP A - COMPLTD
```

12. Add the new linkset to the database using the `ent-1s` command. The new linkset must meet these conditions.

- The name of this linkset cannot be used by another linkset – the linkset configuration is shown in the output of step 11.
- The APC of the new linkset must be in the destination point code table, but cannot be either the system's point code or the system's capability point code – shown in the outputs of steps 7 and 8.
- These parameters and values must also be specified for the IPGWx linkset:

```
- ipgwapc=yes
- lst=<a,b,c,d,e>
- iptps=<100-112000>
```

NOTE: The `iptps` parameter value must be divisible by 10. The sum of all the linkset IP TPS values, including the value for this linkset, cannot exceed the system-wide IP TPS value shown in the `rept-stat-iptps` output in step 1.

- The `mtprse=yes` parameter cannot be specified for an IPGWx linkset.
- The optional parameters `lsusealm` (the linkset's IP TPS alarm threshold) and `slkusealm` (the signaling link IP TPS alarm threshold) can be specified with the `ent-1s` command. The default value for the `lsusealm` parameter is 100%, and the default value for the `slkusealm` parameters is 80%.
- The `multgc=yes` parameter can be specified only for IPGWx linksets that will contain signaling links running the IPGWI application.

NOTE: There are other optional parameters that can be specified with the `ent-ls` command, but are not required for an IPGWx linkset. These parameters and their usage are discussed in the "Configuring a Mate IPGWx Linkset" procedure on page 3-60 and in the "Adding an SS7 Linkset" procedure in the *Database Administration Manual - SS7*.

For this example, enter this command.

```
ent-ls:lsn=lsqw1107:apca=010-020-005:lst=a:ipgwpc=yes
:iptps=4000:lsusealm=70:slkusealm=70
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-17 16:23:21 GMT EAGLE5 31.6.0
Link set table is ( 14 of 1024) 1% full
ENT-LS: MASP A - COMPLTD
```

NOTE: If you do not wish to change an existing IPGWx linkset, skip steps 13 and 14, and go to step 15.

NOTE: If the `slkusealm` parameter for the linkset is not being changed, skip step 13 and go to step 14.

13. Display the signaling link alarm threshold for the linkset being changed by entering the `rept-stat-iptps` command with the name of the linkset being changed. For this example, enter this command.

```
rept-stat-iptps:lsn=lsqw1105
```

This is an example of the possible output.

```
rlghncxa03w 04-12-17 16:23:21 GMT EAGLE5 31.6.0

IP TPS USAGE REPORT
```

		THRESH	CONFIG		TPS	PEAK	PEAKTIMESTAMP

LSN							
LSGW1105		80%	10000	TX:	7300	7450	04-06-10 11:40:04
				RCV:	7300	7450	04-06-10 11:40:04

LOC	PORT						
1105	A	80%	----	TX:	7300	7450	04-06-10 11:40:04
				RCV:	7300	7450	04-06-10 11:40:04

Command Completed.

14. Change the existing linkset using the **chg-ls** command and these parameters.

- The name of the linkset being changed, shown in the **rept-stat-iptps** output in step 1.
- **iptps=<100-112000>**

NOTE: The **iptps** parameter value must be divisible by 10. The sum of all the linkset IP TPS values, including the value for this linkset, if this value is changed, cannot exceed the system-wide IP TPS value shown in the **rept-stat-iptps** output in step 1.

- The **mtrpse=yes** parameter cannot be specified for an IPGWx linkset.
- The optional parameters **lsusealm** (the linkset's IP TPS alarm threshold) and **slkusealm** (the signaling link IP TPS alarm threshold) can be specified with the **chg-ls** command.
- The **multgc=yes** parameter can be specified only for IPGWx linksets that contain signaling links running the IPGWI application.

NOTE: There are other optional parameters that can be specified with the **chg-ls** command, but are not required for an IPGWx linkset. These parameters and their usage are discussed in the "Configuring a Mate IPGWx Linkset" procedure on page 3-60 and in the "Adding an SS7 Linkset" procedure in the *Database Administration Manual - SS7*.

For this example, enter this command.

```
chg-ls:lsn=lsgw1105:iptps=14000:lsusealm=70:slkusealm=70
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-17 16:23:21 GMT EAGLE5 31.6.0
Link set table is ( 14 of 1024) 1% full
CHG-LS: MASP A - COMPLTD
```

15. Verify the changes using the **rtrv-ls** command specifying the linkset name specified in either steps 12 or 14 with the **lsn** parameter. For this example, enter these commands.

```
rtrv-ls:lsn=lsgw1105
```

This is an example of the possible output.

```
rlghncxa03w 04-12-17 11:43:04 GMT EAGLE5 31.6.0

          L3T SLT          GWS GWS GWS
LSN      APCA  (SS7)  SCRN  SET SET BEI LST LNKS ACT MES DIS SLSCI NIS
lsgw1105  009-002-003  none  1  1  no  A  1  off off off no  off

          CLLI          TFATCABMLQ MTPRSE ASL8
          -----  1          no          no

IPGWAPC  MATELSN  IPTPS  LSUSEALM  SLKUSEALM
yes      -----  14000  70      %  70      %
```

IP7 Secure Gateway Configuration Procedures

```

          L2T          L1          PCR PCR
LOC PORT SLC TYPE SET BPS MODE TSET ECM N1 N2

          LP          ATM
LOC PORT SLC TYPE SET BPS TSEL VCI VPI LL

          LP          ATM          E1ATM
LOC PORT SLC TYPE SET BPS TSEL VCI VPI CRC4 SI SN

LOC PORT SLC TYPE IPLIML2

LOC PORT SLC TYPE
1105 A 0 SS7IPGW

          L2T          PCR PCR E1 E1
LOC PORT SLC TYPE SET BPS ECM N1 N2 LOC PORT TS

          L2T          PCR PCR T1 T1
LOC PORT SLC TYPE SET BPS ECM N1 N2 LOC PORT TS

```

Link set table is (14 of 1024) 1% full

rtrv-ls:lsn=lsgw1107

This is an example of the possible output.

rlghncxa03w 04-12-17 11:43:04 GMT EAGLE5 31.6.0

```

          L3T SLT          GWS GWS GWS
LSN      APCA (SS7) SCRN SET SET BEI LST LNKS ACT MES DIS SLSCI NIS
lsgw1107 010-020-005 none 1 1 no A 0 off off off no off

```

```

CLLI      TFATCABMLQ MTPRSE ASL8
----- 1          no      no

```

```

IPGWAPC MATELSN IPTPS LSUSEALM SLKUSEALM
yes      ----- 4000 70 % 70 %

```

```

          L2T          L1          PCR PCR
LOC PORT SLC TYPE SET BPS MODE TSET ECM N1 N2

          LP          ATM
LOC PORT SLC TYPE SET BPS TSEL VCI VPI LL

          LP          ATM          E1ATM
LOC PORT SLC TYPE SET BPS TSEL VCI VPI CRC4 SI SN

LOC PORT SLC TYPE IPLIML2

LOC PORT SLC TYPE

          L2T          PCR PCR E1 E1
LOC PORT SLC TYPE SET BPS ECM N1 N2 LOC PORT TS

          L2T          PCR PCR T1 T1
LOC PORT SLC TYPE SET BPS ECM N1 N2 LOC PORT TS

```

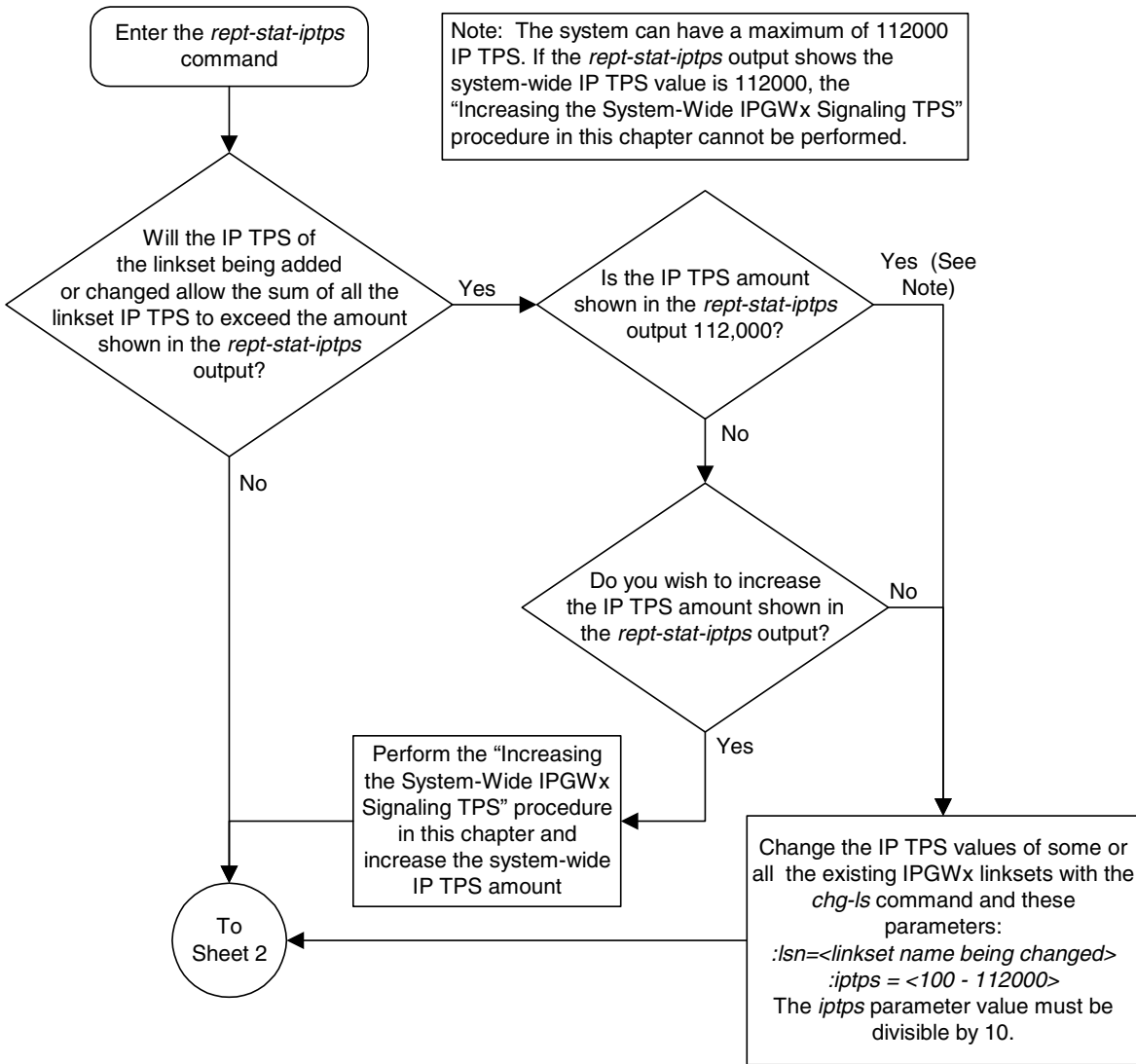
Link set table is (14 of 1024) 1% full

16. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```

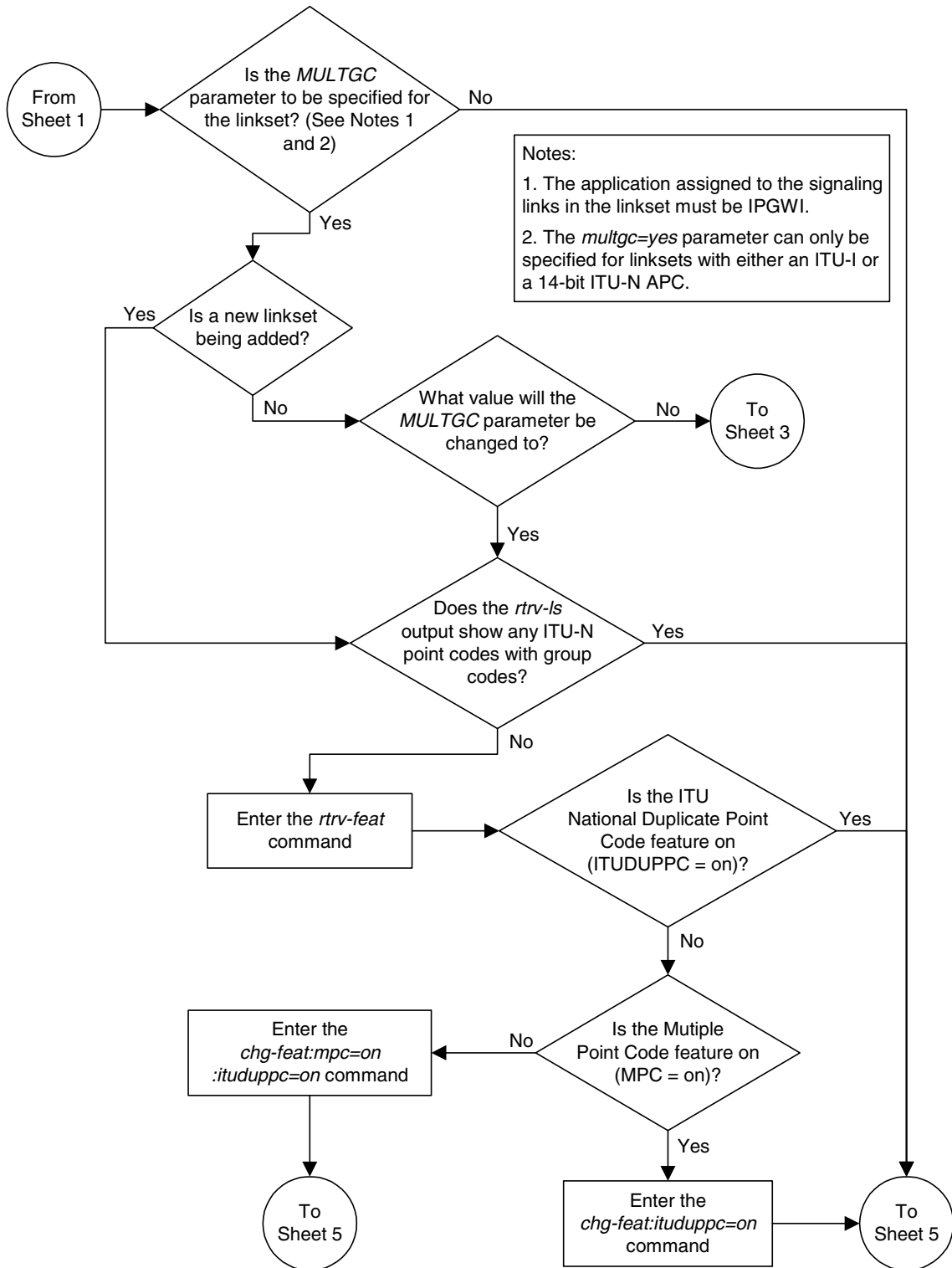
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
    
```

Flowchart 3-3. Configuring an IPGWx Linkset (Sheet 1 of 6)

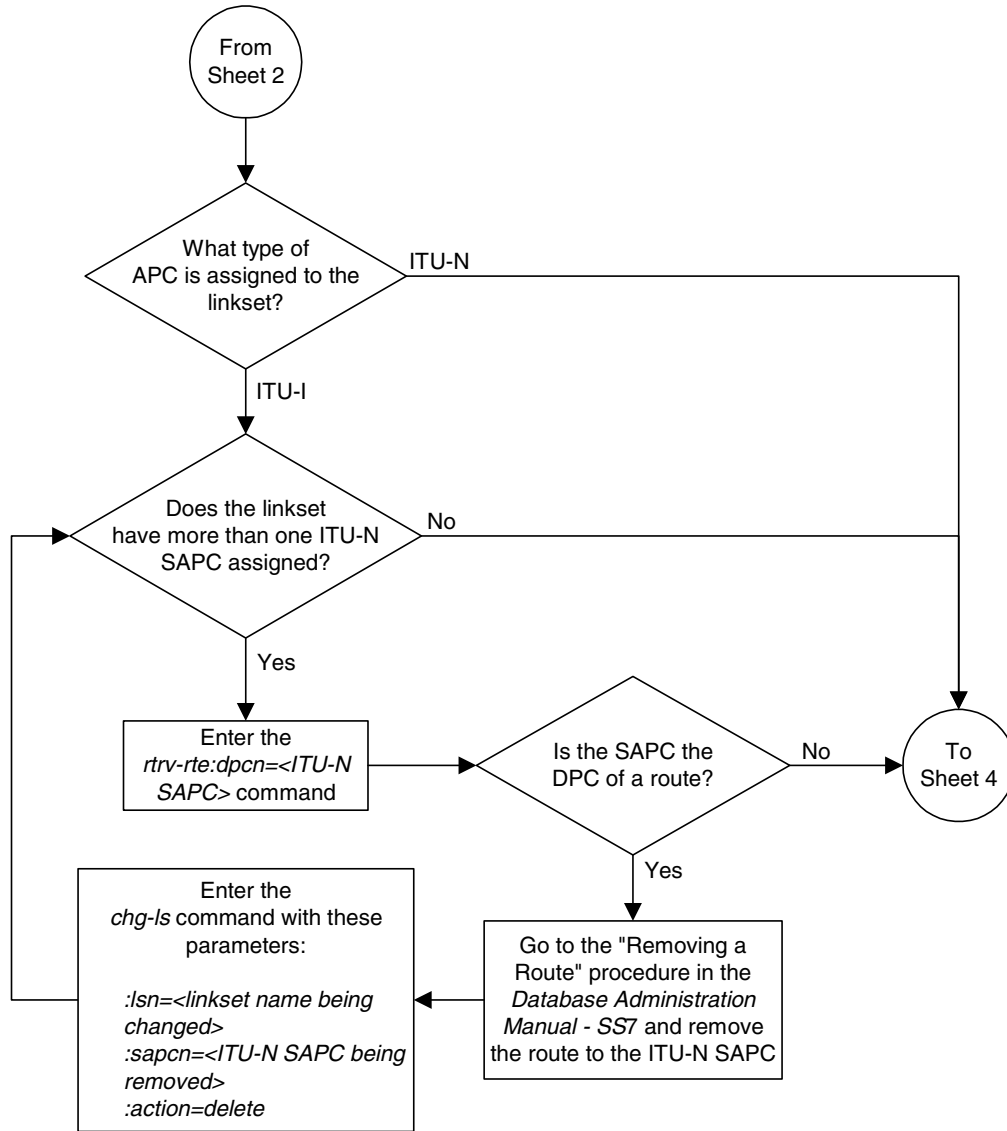


7

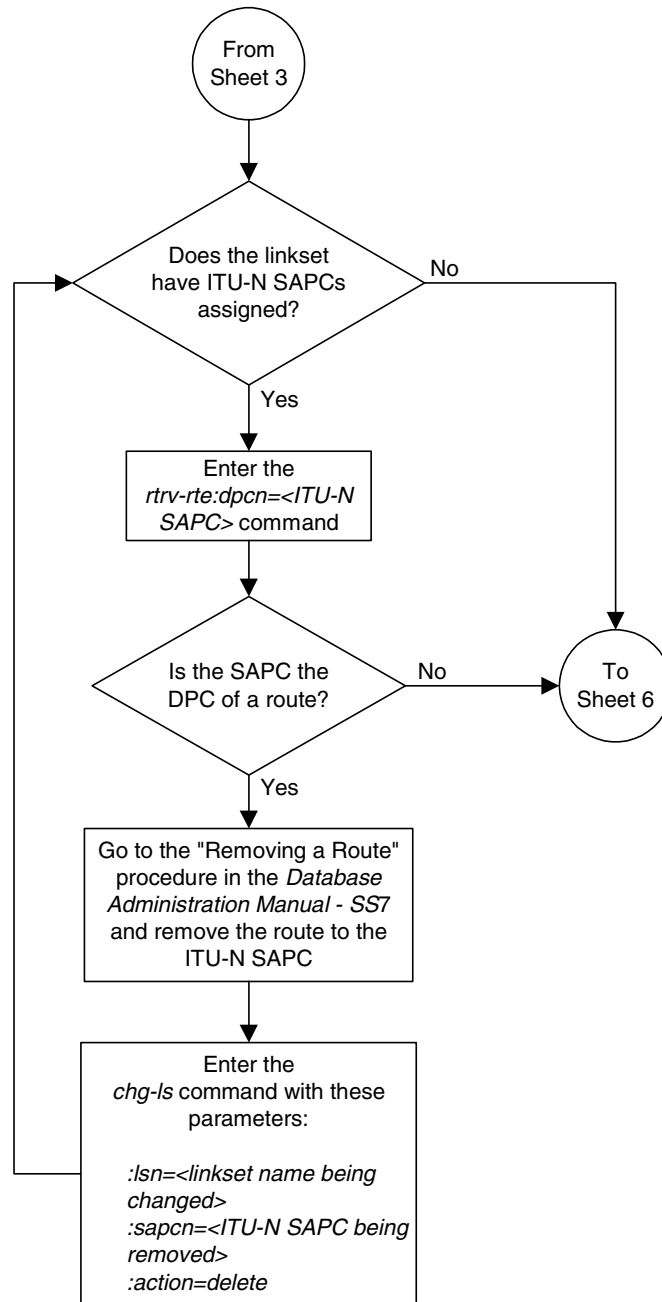
Flowchart 3-3. Configuring an IPGWx Linkset (Sheet 2 of 6)



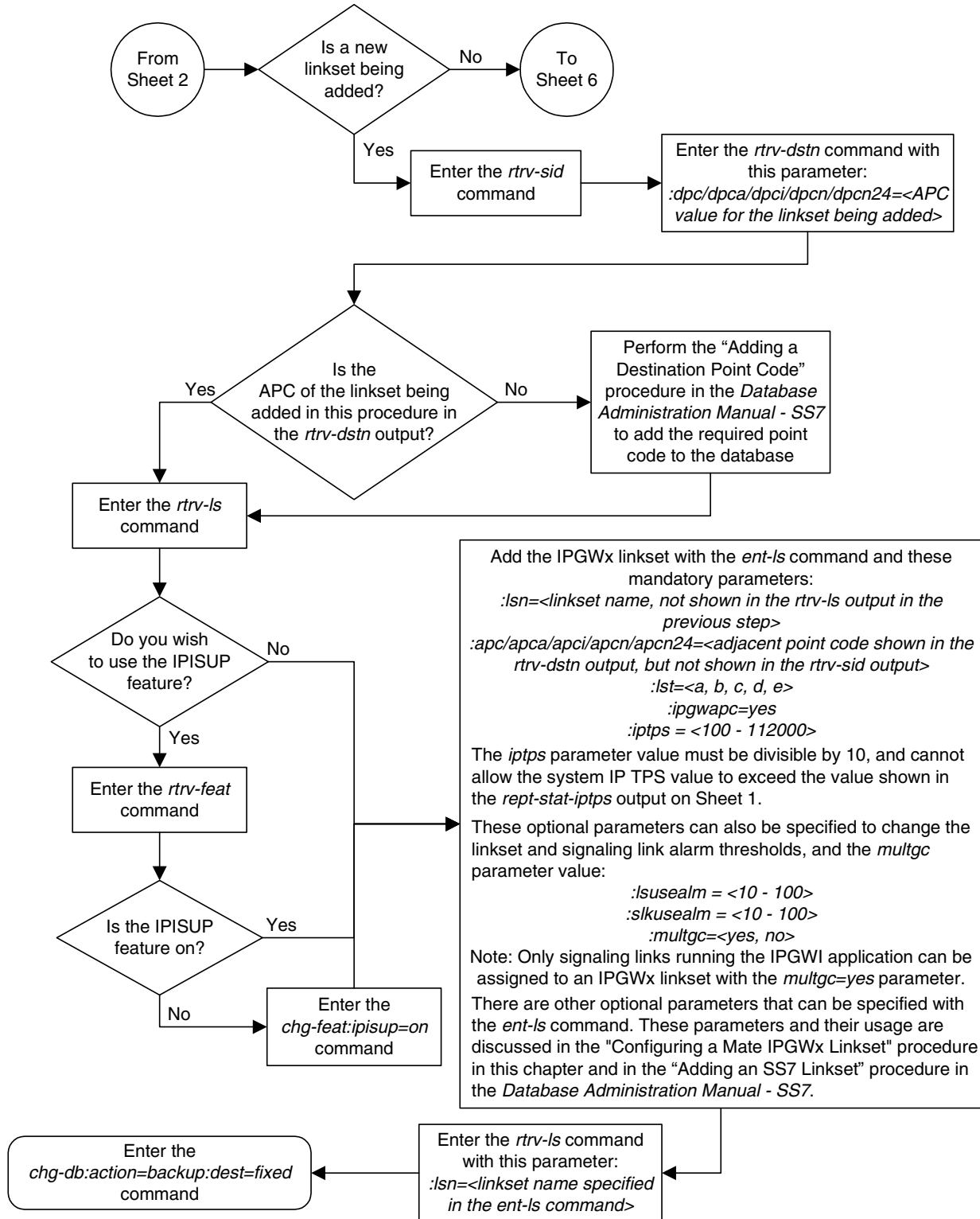
Flowchart 3-3. Configuring an IPGWx Linkset (Sheet 3 of 6)



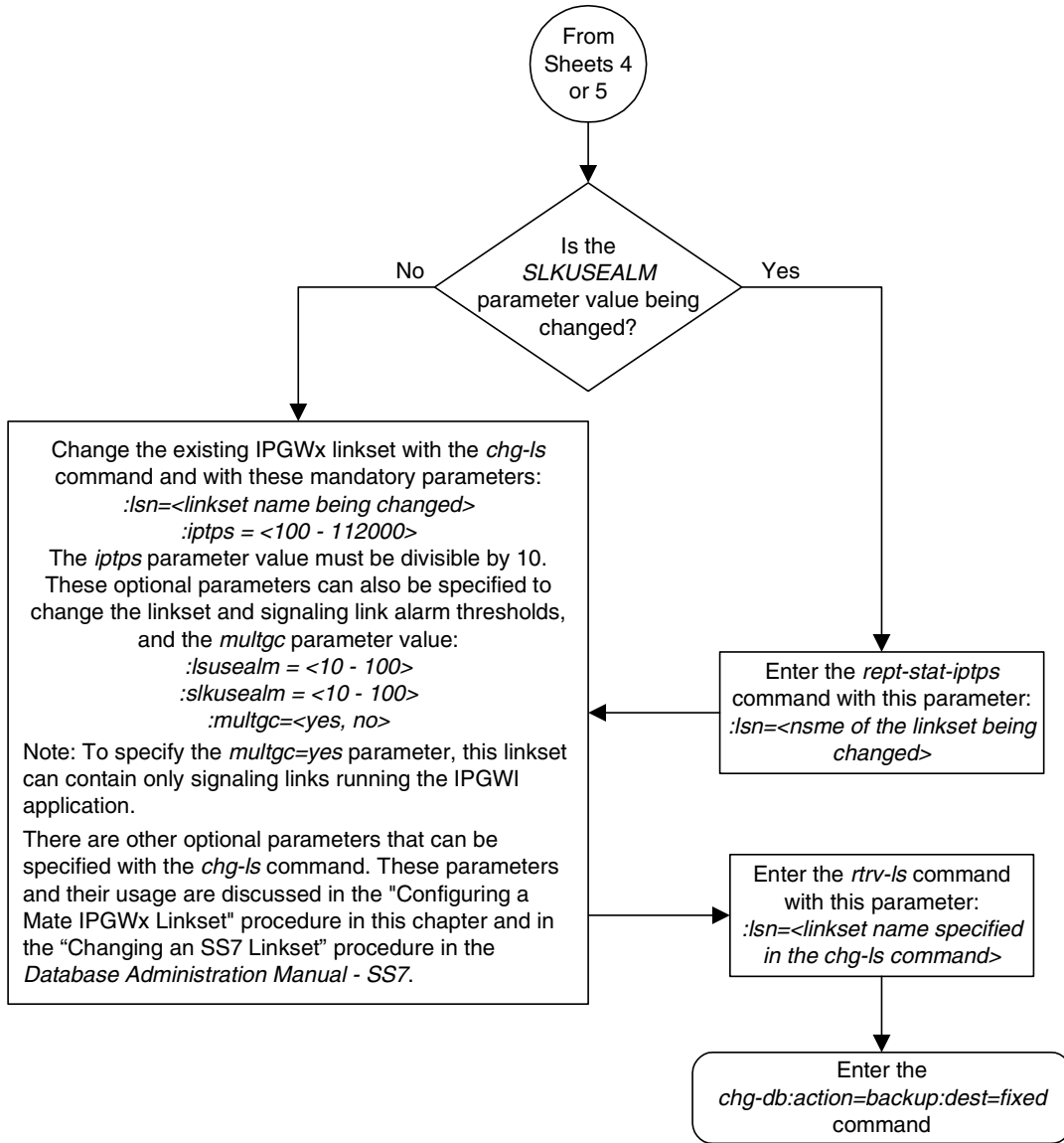
Flowchart 3-3. Configuring an IPGWx Linkset (Sheet 4 of 6)



Flowchart 3-3. Configuring an IPGWx Linkset (Sheet 5 of 6)



Flowchart 3-3. Configuring an IPGWx Linkset (Sheet 6 of 6)



Configuring a Mate IPGWx Linkset

This procedure is used to configure a mate IPGWx linkset to an existing IPGWx linkset **chg-1s** command with these parameters.

:lsn – The name of the linkset. The linkset name can contain up to 10 characters, with the first character being a letter. However, the SEAS interface supports only eight characters. If this linkset is displayed on the SEAS interface and the linkset name contains more than eight characters, only the first eight characters in the linkset name are shown. If this linkset name contains more than eight characters, and is specified with the linkset commands on the SEAS interface, only the first eight characters can be specified.

:mate1sn – The name of the mate IPGWx linkset.

:action – to add (**action=add**) or remove (**action=delete**) the mate IPGWx linkset to the IPGWx linkset specified by the **lsn** parameter.

NOTE: This procedure is not used to configure an IPGWx linkset, with the **ipgwapc**, **iptps**, **lsusealm** and **slkusealm** parameters. To configure an IPGWx linkset with these parameters, perform the “Configuring an IPGWx Linkset” procedure on page 3-40.

An IPGWx linkset is a linkset that contains signaling links assigned to IPGWx cards. IPGWx cards are cards running either the SS7IPGW or IPGWI applications.

The Eagle allows an IPGWx linkset to contain up to 8 IPGWx signaling links, and as a result, 8 IPGWx cards. This increases the amount of traffic that can be delivered to a single IP node compared to the two-card combined IPGWx linkset deployments used in previous releases. An IPGWx linkset containing up to 8 IPGWx signaling links is the preferred method of configuring IPGWx linksets (see the “Configuring an IPGWx Linkset” procedure on page 3-40). This method is required if more than two IPGWx signaling links are to be used in the linkset.

To provide backward compatibility with pre-existing two-card combined IPGWx linkset deployments, the Eagle also provides for a mate IPGWx linkset. A mate IPGWx linkset consists of one IPGWx linkset assigned to another IPGWx linkset using the **mate1sn** parameter of the **chg-1s** command. To assign a mate IPGWx linkset to another IPGWx linkset, both linksets can contain no more than one signaling link. While mate IPGWx linksets can be configured using this procedure, the preferred method of configuring two-card IPGWx deployments is to configure a two-link non-mated linkset using the “Configuring an IPGWx Linkset” procedure on page 3-40.

Each linkset in the mated pair must either contain no mate linksets, or can reference the other linkset in the mated pair. For example, to assign linkset **LSN2** to IPGWx linkset **LSN1** as a mate linkset, linkset **LSN1** cannot contain any mate linksets. Linkset **LSN2** can have linkset **LSN1** as a mate, otherwise linkset **LSN2** cannot have any mate linksets assigned to it.

The mate linkset name is displayed in the `rtrv-ls:lsn=<linkset name>` command output. If either linkset contains more than one signaling link, all but one of the signaling links must be removed from these linksets or other linksets must be chosen. Perform the “Removing an IP Signaling Link” procedure on page 3-115 to remove any signaling links from the linkset. If new linksets must be configured for this procedure, perform the “Configuring an IPGWx Linkset” procedure on page 3-40.

Before a mate IPGWx linkset can be added to an IPGWx linkset, the card containing the IPGWx signaling link assigned to the linkset being changed, and the signaling link assigned to that card must be placed out of service.

Before a mate IPGWx linkset can be removed from an IPGWx linkset, the card containing the IPGWx signaling link assigned to the mate linkset, and the signaling link assigned to that card must be placed out of service.

The network type of the adjacent point code of the mate IPGWx linkset must be the same type as the linkset the mate is assigned to. For example, if a mate IPGWx linkset is assigned to an IPGWx linkset with an ITU-I adjacent point code, the mate IPGWx linkset must have an ITU-I adjacent point code.

Other Optional Parameters

Other optional parameters, shown in Table 3-10, can be used with the `chg-ls` command but do not need to be used in this procedure. These parameters are discussed in more detail in the “Changing an SS7 Linkset” procedures in the *Database Administration Manual - SS7*. The `iptps`, `lsusealm`, and `slkusealm` parameters are discussed in more detail in the “Configuring an IPGWx Linkset” procedure on page 3-40.

Table 3-10. Optional Linkset Parameters

cli	sltset	l3tset	scrn	gwsa
gwsn	gwsd	bei	nis	itutfr
mtp ^{rs} e*	slsci	asl8	slsrsb	slsocbit
multgc	tfatcabmlq	gmscrn	sapci	sapcn
sapcn24	iptps	lsusealm	slkusealm	
* The mtp ^{rs} e parameter cannot be specified for an IPGWx linkset.				

Procedure

1. Display the system-wide IP TPS usage report, and the IPGWx linksets, by entering the **rept-stat-iptps** command. This is an example of the possible output.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.6.0
IP TPS USAGE REPORT
-----
                THRESH  CONFIG          TPS      PEAK      PEAKTIMESTAMP
-----
SYSTEM
RLGHNCXA03W  100%    30000  TX:   7200    7600    04-06-10 11:40:04
                RCV:   7200    7600    04-06-10 11:40:04
-----
LSN
LSGW1101      80%     6000  TX:   5100    5500    04-06-10 11:40:04
                RCV:   5100    5500    04-06-10 11:40:04
LSGW1103      80%     6000  TX:   5200    5500    04-06-10 11:40:04
                RCV:   5200    5500    04-06-10 11:40:04
LSGW1105      80%    14000  TX:   7300    7450    04-06-10 11:40:04
                RCV:   7300    7450    04-06-10 11:40:04
LSGW1107      70%     4000  TX:   3200    3500    04-06-10 11:40:04
                RCV:   3200    3500    04-06-10 11:40:04
-----
Command Completed.
```

2. Display the linkset that is being changed by entering the **rtrv-ls** command with a linkset name shown in the **rept-stat-iptps** output in step 1. For this example, enter this command.

rtrv-ls:lsn=lsgw1103

This is an example of the possible output.

```
rlghncxa03w 04-12-17 11:43:04 GMT EAGLE5 31.6.0
LSN          APCA  (SS7)  SCRN  L3T SLT          GWS GWS GWS
lsgw1103     003-002-004  none  1   1  no  A   1   off off off no  off

CLLI          TFATCABMLQ MTPRSE ASL8
-----          1           no   no

IPGWAPC  MATELSN  IPTPS  LSUSEALM  SLKUSEALM
yes          ----- 10000   70    %  70    %

LOC  PORT  SLC  TYPE          L2T          L1          PCR  PCR
          SET  BPS  MODE TSET  ECM  N1  N2

LOC  PORT  SLC  TYPE          LP          ATM
          SET  BPS  TSEL          VCI  VPI  LL

LOC  PORT  SLC  TYPE          LP          ATM          E1ATM
          SET  BPS  TSEL          VCI  VPI  CRC4 SI SN

LOC  PORT  SLC  TYPE          IPLIML2

LOC  PORT  SLC  TYPE
1103 A    0   SS7IPGW
```

IP7 Secure Gateway Configuration Procedures

```

                L2T          PCR PCR  E1  E1
LOC  PORT SLC TYPE  SET  BPS   ECM  N1  N2  LOC  PORT TS
                L2T          PCR PCR  T1  T1
LOC  PORT SLC TYPE  SET  BPS   ECM  N1  N2  LOC  PORT TS

```

Link set table is (14 of 1024) 1% full

If this linkset has a mate linkset assigned to it, the name of the mate linkset is shown in the **MATELSN** field of the **rtrv-ls** output, as shown in the following output.

rtrv-ls:lsn=lsgw1103

This is an example of the possible output.

rlghncxa03w 04-12-17 11:43:04 GMT EAGLE5 31.6.0

```

                L3T SLT          GWS GWS GWS
LSN          APCA  (SS7)  SCRN  SET SET BEI LST LNKS ACT MES DIS SLSCI NIS
lsgw1103     003-002-004  none  1  1  no  A  1  off off off no  off

CLLI          TFATCABMLQ MTPRSE ASL8
----- 1          no  no

IPGWAPC  MATELSN  IPTPS  LSUSEALM  SLKUSEALM
yes      lsgw1107  10000  70  %  70  %

                L2T          L1          PCR PCR
LOC  PORT SLC TYPE  SET  BPS   MODE TSET  ECM  N1  N2

                LP          ATM
LOC  PORT SLC TYPE  SET  BPS   TSEL          VCI  VPI  LL

                LP          ATM          E1ATM
LOC  PORT SLC TYPE  SET  BPS   TSEL          VCI  VPI  CRC4 SI SN

LOC  PORT SLC TYPE  IPLIML2

LOC  PORT SLC TYPE
1103 A  0  SS7IPGW

                L2T          PCR PCR  E1  E1
LOC  PORT SLC TYPE  SET  BPS   ECM  N1  N2  LOC  PORT TS

                L2T          PCR PCR  T1  T1
LOC  PORT SLC TYPE  SET  BPS   ECM  N1  N2  LOC  PORT TS

```

Link set table is (14 of 1024) 1% full

NOTE: If the linkset being changed has no signaling links, or only one signaling link assigned to it, or if the mate linkset is being removed from the linkset being changed, skip step 3 and go to step 4.

- To assign a mate linkset to this linkset, and the linkset contains more than one signaling link, all but one of these signaling links must be removed from the linkset. Perform the "Removing an IP Signaling Link" procedure on page 3-115 to remove these signaling links.

If you do not wish to change this linkset, either choose another linkset from the **rept-stat-iptps** output in step 1, and repeat step 2, and 3 if necessary, or perform the "Configuring an IPGWx Linkset" procedure on page 3-40 and add a new linkset. Go to step 4.

- If a mate linkset is being added in this procedure, display the mate linkset from the IPGWx linksets shown in the **rept-stat-iptps** output in step 1.

If a mate linkset is being removed in this procedure, display the mate linkset shown in the **MATELSN** column of the **rtrv-ls** output in step 2.

For this example, enter this command.

rtrv-ls:lsn=lsgw1107

This is an example of the possible output.

```
rlghncxa03w 04-12-17 11:43:04 GMT EAGLE5 31.6.0
```

LSN	APCA	(SS7)	SCRN	SET	SET	BEI	LST	LNKS	ACT	MES	DIS	SLSCI	NIS
lsgw1107	003-002-004		none	1	1	no	A	1	off	off	off	no	off

CLLI	TFATCABMLQ	MTPRSE	ASL8
-----	1	no	no

IPGWAPC	MATELSN	IPTPS	LSUSEALM	SLKUSEALM
yes	-----	10000	70	% 70 %

LOC	PORT	SLC	TYPE	L2T	BPS	L1	TSET	ECM	PCR	PCR
				SET		MODE			N1	N2

LOC	PORT	SLC	TYPE	LP	BPS	ATM	TSEL	VCI	VPI	LL
				SET						

LOC	PORT	SLC	TYPE	LP	BPS	ATM	TSEL	VCI	VPI	E1ATM	CRC4	SI	SN
				SET									

LOC	PORT	SLC	TYPE	IPLIML2

LOC	PORT	SLC	TYPE
1107	A	0	SS7IPGW

LOC	PORT	SLC	TYPE	L2T	BPS	ECM	PCR	PCR	E1	E1	
				SET			N1	N2	LOC	PORT	TS

LOC	PORT	SLC	TYPE	L2T	BPS	ECM	PCR	PCR	T1	T1	
				SET			N1	N2	LOC	PORT	TS

Link set table is (14 of 1024) 1% full

NOTE: If the the mate linkset is being removed from the linkset being changed, skip step 5 and go to step 6.

5. To use the linkset shown in step 4 as a mate, the network type of the adjacent point code of the linkset shown in step 4 must be the same as the network type of the linkset shown in step 2. The linkset shown in step 4 must not have more than one signaling link assigned to it.

If the linkset contains more than one signaling link, all but one of these signaling links must be removed from the linkset. Perform the "Removing an IP Signaling Link" procedure on page 3-115 to remove these signaling links.

If you do not wish to change this linkset, or if the network type of the adjacent point codes of both linksets are not the same, either choose another linkset from the `rept-stat-iptps` output in step 1, and repeat step 4, and 5 if necessary, or perform the "Configuring an IPGWx Linkset" procedure on page 3-40 and add a new linkset. Go to step 6.

If the network types of the adjacent point codes of both linksets are the same, and the mate linkset contains no more than one signaling link, do not perform the actions in this step. Go to step 6.

NOTE: If the linkset that the mate linkset is being added to has no signaling links (see the `rtrv-ls` output in step 2), skip steps 6 through 16, and go to step 17.

NOTE: If the mate linkset is being removed in this procedure, and has no signaling links (see the `rtrv-ls` output in step 4), skip steps 6 through 16, and go to step 17.

6. Display the status of the card containing the signaling link assigned to the linkset being changed by entering the `rept-stat-card` command with the card location shown in the `LOC` field in the `rtrv-ls` output in step 2 (for adding a mate linkset) or in the `rtrv-ls` output in step 4 (for removing a mate linkset). For this example, enter one of these commands.

`rept-stat-card:loc=1103` (for the adding a mate linkset example)

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD VERSION      TYPE  APPL  PST      SST      AST
1103  114-000-000  DCM   SS7IPGW IS-NR     Active   -----
  ALARM STATUS    = No Alarms.
  BPDCM GPL       = 002-102-000
  IMT BUS A       = Conn
  IMT BUS B       = Conn
  SLK A  PST      = IS-NR          LS=lsgw1103  CLLI=-----
  SCCP TVG RESULT = 24 hr: -----, 5 min: -----
  SLAN TVG RESULT = 24 hr: -----, 5 min: -----
Command Completed.
```

rept-stat-card:loc=1107 (for the removing a mate linkset example)

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD VERSION      TYPE      APPL      PST      SST      AST
1107 114-000-000  DCM      SS7IPGW  IS-NR    Active   -----
  ALARM STATUS    = No Alarms.
  BPDCM GPL       = 002-102-000
  IMT BUS A       = Conn
  IMT BUS B       = Conn
  SLK A   PST     = IS-NR      LS=lsgw1103  CLLI=-----
  SCCP TVG RESULT = 24 hr: -----, 5 min: -----
  SLAN TVG RESULT = 24 hr: -----, 5 min: -----
Command Completed.
```

NOTE: If the status of the card shown in **PST** field in the **rept-stat-card** output in step 6 is **OOS-MT-DSBLD**, skip steps 7 through 16, and go to step 17.

7. Display the status of the signaling link assigned to the card shown in step 6 by entering the **rept-stat-slk** command with the card location used in step 6 and the **port=a** parameter. For this example, enter one of these commands.

rept-stat-slk:loc=1103:port=a (for the adding a mate linkset example)

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1103,A   lsgw1103  -----  IS-NR    Avail   -----
  ALARM STATUS    = No Alarms.
  UNAVAIL REASON  = NA
Command Completed.
```

rept-stat-slk:loc=1107:port=a (for the removing a mate linkset example)

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1107,A   lsgw1107  -----  IS-NR    Avail   -----
  ALARM STATUS    = No Alarms.
  UNAVAIL REASON  = NA
Command Completed.
```

NOTE: If the status of the signaling link shown in the **PST** field of the **rept-stat-slk** output in step 7 is **OOS-MT-DSBLD**, skip steps 8 through 15, and go to step 16.

8. Any in-service IP connections on the signaling link shown in step 7 must be placed out of service. The recommended method is to have the far end node place these IP connections out of service. Have the far-end node for the signaling link shown in step 7 perform these actions:
 - Place the TALI sockets in the NEA-FEP state.

- Place the M3UA or SUA associations in either the ASP-INACTIVE or ASP-DOWN state.

NOTE: If you choose to perform this step, skip steps 9 through XX, and go to step DACT-SLK.

9. Display the IP link associated with the signaling link shown in step 7 by entering the **rtrv-ip-lnk** command with the location and port of the signaling link. For this example, enter one of these commands.

rtrv-ip-lnk:loc=1103:port=a (for the adding a mate linkset example)

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.6.0
LOC  PORT IPADDR          SUBMASK          DUPLEX  SPEED  MACTYPE AUTO
1103  A    192.003.001.010      255.255.255.128  HALF   10    802.3  NO
```

rtrv-ip-lnk:loc=1107:port=a (for the removing a mate linkset example)

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.6.0
LOC  PORT IPADDR          SUBMASK          DUPLEX  SPEED  MACTYPE AUTO
1107  A    192.001.001.010      255.255.255.128  HALF   10    802.3  NO
```

10. Display the IP host information associated with the IP link by entering the **rtrv-ip-host** command with the IP address shown in step 9. For this example, enter one of these commands.

rtrv-ip-host:ipaddr=192.001.001.010 (for the adding a mate linkset example)

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.6.0

IPADDR          HOST
192.1.1.10      IPNODE1_1103
```

IP Host table is (10 of 512) 2% full

rtrv-ip-host:ipaddr=192.003.001.010 (for the removing a mate linkset example)

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.6.0

IPADDR          HOST
192.3.1.10      IPNODE1_1107
```

IP Host table is (10 of 512) 2% full

11. Display the socket associated with the local host name shown in step 10 by entering the `rtrv-appl-sock` command. For this example, enter one of these commands.

`rtrv-appl-sock:localhost=ipnode1_1103` (for the adding a mate linkset example)

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.6.0
SNAME KC_HLR1_1103
LINK      A
LHOST     IPNODE1_1103
RHOST     KC_HLR2
LPORT     7000           RPORT     7001
SERVER    YES           DCMP5     1
REXMIT    FIXED        RTT       60
OPEN      YES           ALW       YES
```

IP Appl Sock/Assoc table is (4 of 4000) 1% full

`rtrv-appl-sock:localhost=ipnode1_1107` (for the removing a mate linkset example)

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.6.0
```

IP Appl Sock/Assoc table is (4 of 4000) 1% full

NOTE: If the specified socket name is not in the database, the `rtrv-appl-sock` output shows no socket information as show above.

NOTE: If there is no socket shown in step 11, or the `open` and `alw` parameter values of the socket shown in step 11 are `no`, skip this step and step 13, and go to step 14.

12. Change the `alw` parameter values in the socket shown in step 11 using the `chg-appl-sock` command with the `alw=no` parameters, as necessary.

For example, enter this command.

`chg-appl-sock:sname=kc_hlr1_1103:alw=no`

CAUTION: This command impacts network performance and should only be used during periods of low traffic.

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.6.0
CHG-APPL-SOCK: MASP A - COMPLTD
```

Repeat this step for all sockets shown in step 11.



13. Change the **open** parameter values in the socket shown in step 11 using the **chg-appl-sock** command with the **open=no** parameters, as necessary.

For example, enter this command.

```
chg-appl-sock:sname=kc_hlr1_1103:open=no
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.6.0
CHG-APPL-SOCK: MASP A - COMPLTD
```

Repeat this step for all sockets shown in step 11.

14. Display the association associated with the local host name shown in step 10 by entering the **rtrv-assoc** command. For this example, enter one of these command.

```
rtrvs-assoc:lhost=ipnode1_1107 (for the removing a mate linkset example)
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.6.0
ANAME ASSOC1
  PORT      A
  ADAPTER   M3UA          VER      M3UA RFC
  LHOST     IPNODE1_1107
  ALHOST    ---
  RHOST     GW100.NC.TEKELEC.COM
  LPORT     1030              RPORT    1030
  ISTRMS    2                OSTRMS   2
  RMODE     LIN          RMIN     120          RMAX     800
  RTIMES    10            CWMIN    3000
  OPEN      YES          ALW      YES
```

```
IP Appl Sock/Assoc table is (4 of 4000) 1% full
```

```
rtrv-assoc:lhost=ipnode1_1103 (for the adding a mate linkset example)
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.6.0
```

```
IP Appl Sock/Assoc table is (4 of 4000) 1% full
```

NOTE: If the specified association name is not in the database, the **rtrv-assoc** output shows no association information as show above.

NOTE: If there is no association shown in step 14, or the `open` and `alw` parameter values of the association shown in step 14 are `no`, skip this step and step 16, and go to step 17.

15. Change the `alw` parameter values in the association shown in step 14 using the `chg-assoc` command with the `alw=no` parameters, as necessary.

```
chg-assoc:aname=assoc1:alw=no
```



CAUTION: This command impacts network performance and should only be used during periods of low traffic.

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.6.0
CHG-ASSOC: MASP A - COMPLTD
```

Repeat this step for all associations shown in step 14.

16. Change the `open` parameter values in the association shown in step 14 using the `chg-assoc` command with the `open=no` parameters, as necessary.

```
chg-assoc:aname=assoc1:open=no
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.6.0
CHG-ASSOC: MASP A - COMPLTD
```

Repeat this step for all associations shown in step 14.

17. Deactivate the signaling link assigned to the IP card using the `dact-slk` command. For example, enter one of these commands:

```
dact-slk:loc=1103:port=a (for the adding a mate linkset example)
```

```
dact-slk:loc=1107:port=a (for the removing a mate linkset example)
```



CAUTION: This command impacts network performance and should only be used during periods of low traffic.

After this command has successfully completed, this message appears.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
Deactivate Link message sent to card.
```

18. Inhibit the IP card using the `inh-card` command. For example, enter one of these commands.

```
inh-card:loc=1103 (for the adding a mate linkset example)
```

```
inh-card:loc=1107 (for the removing a mate linkset example)
```

This message should appear.

```
rlghncxa03w 04-06-28 21:18:37 GMT EAGLE5 31.10.0
Card has been inhibited.
```

19. Change the linkset shown in step 2 with the **chg-ls** command. If a mate IPGWx linkset is being added, use the **matelsn** and **action=add** parameters with the **chg-ls** command. If a mate IPGWx linkset is being removed, use the **matelsn** and **action=delete** parameters with the **chg-ls** command.

To add a mate linkset in this example, enter this command.

```
chg-ls:lsn=lsgw1103:matelsn=lsgw1107:action=add
```

To remove a mate linkset in this example, enter this command.

```
chg-ls:lsn=lsgw1103:matelsn=lsgw1107:action=delete
```

NOTE: There are other optional parameters that can be specified with the **chg-ls** command, but are not required for an IPGWx linkset. These parameters and their usage are discussed in the "Configuring an IPGWx Linkset" procedure on page 3-40 and in the "Changing an SS7 Linkset" procedure in the *Database Administration Manual - SS7*.

When the **chg-ls** command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-17 16:23:21 GMT EAGLE5 31.6.0
Link set table is ( 14 of 1024) 1% full
CHG-LS: MASP A - COMPLTD
```

20. Verify the changes using the **rtrv-ls** command specifying the linkset name specified in step 19 with the **lsn** parameter. For this example, enter this command.

```
rtrv-ls:lsn=lsgw1103
```

This is an example of the possible output.

```
rlghncxa03w 04-12-17 11:43:04 GMT EAGLE5 31.6.0

LSN          APCA  (SS7)  SCRN  L3T  SLT          GWS  GWS  GWS
lsgw1103     003-002-004  none  1    1    no  A    1    off off off no  off

          CLLI          TFATCABMLQ  MTPRSE  ASL8
          -----  1          no      no

IPGWAPC  MATELSN  IPTPS  LSUSEALM  SLKUSEALM
yes      lsgw1107  10000  70      %  70      %

          L2T          L1          PCR  PCR
          SET  BPS    MODE  TSET  ECM   N1   N2

          LP          ATM
          SET  BPS    TSEL          VCI   VPI   LL

          LP          ATM          E1ATM
          SET  BPS    TSEL          VCI   VPI  CRC4  SI  SN

          LOC  PORT  SLC  TYPE          IPLIML2

          LOC  PORT  SLC  TYPE
          1103  A    0    SS7IPGW
```

IP⁷ Secure Gateway Configuration Procedures

```

          L2T          PCR PCR  E1  E1
LOC  PORT SLC TYPE  SET  BPS   ECM  N1  N2  LOC  PORT TS
          L2T          PCR PCR  T1  T1
LOC  PORT SLC TYPE  SET  BPS   ECM  N1  N2  LOC  PORT TS

```

Link set table is (14 of 1024) 1% full

If the mate linkset was removed in step 19, the MATELSN column of the rtrv-ls output should contain dashes, as shown in the following example.

rtrv-ls:lsn=lsgw1103

This is an example of the possible output.

rlghncxa03w 04-12-17 11:43:04 GMT EAGLE5 31.6.0

```

          L3T SLT          GWS GWS GWS
LSN      APCA  (SS7)  SCRNR SET SET BEI LST LNKS ACT MES DIS SLSCI NIS
lsgw1103 003-002-004 none 1 1 no A 1 off off off no off

```

```

CLLI      TFATCABMLQ MTPRSE ASL8
----- 1          no      no

```

```

IPGWAPC  MATELSN  IPTPS  LSUSEALM  SLKUSEALM
yes      ----- 10000  70      % 70      %

```

```

          L2T          L1          PCR PCR
LOC  PORT SLC TYPE  SET  BPS   MODE TSET  ECM  N1  N2

```

```

          LP          ATM
LOC  PORT SLC TYPE  SET  BPS   TSEL          VCI  VPI  LL

```

```

          LP          ATM          E1ATM
LOC  PORT SLC TYPE  SET  BPS   TSEL          VCI  VPI  CRC4 SI SN

```

```

LOC  PORT SLC TYPE  IPLIML2

```

```

LOC  PORT SLC TYPE
1103 A  0  SS7IPGW

```

```

          L2T          PCR PCR  E1  E1
LOC  PORT SLC TYPE  SET  BPS   ECM  N1  N2  LOC  PORT TS

```

```

          L2T          PCR PCR  T1  T1
LOC  PORT SLC TYPE  SET  BPS   ECM  N1  N2  LOC  PORT TS

```

Link set table is (14 of 1024) 1% full

NOTE: If the linkset shown in step 20 does not have a signaling link assigned to it, skip steps 21 through 25, and go to step 26.

21. Allow the IP card that was inhibited in step 18 using the **alw-card** command. For example, enter one of these commands.

alw-card:loc=1103 (for the adding a mate linkset example)

alw-card:loc=1107 (for the removing a mate linkset example)

This message should appear.

```
rlghncxa03w 04-06-28 21:21:37 GMT EAGLE5 31.10.0
Card has been allowed.
```

22. Activate the signaling link from step 17 using the **act-slk** command. For example, enter one of these commands.

act-slk:loc=1103:port=a (for the adding a mate linkset example)

act-slk:loc=1107:port=a (for the removing a mate linkset example)

The output confirms the activation.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Activate Link message sent to card
```

NOTE: If steps 12 and 13 were not performed, skip this step and go to step 24.

23. Change the **open** and **alw** parameter values for all the sockets that were changed in steps 12 or 13 using the **chg-appl-sock** command with the **open=yes** and **alw=yes** parameters.

For example, enter this command.

chg-appl-sock:sname=kc_hlr1_1103:open=yes:alw=yes

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.6.0
CHG-APPL-SOCK: MASP A - COMPLTD
```

NOTE: If steps 15 and 16 were not performed, skip this step and go to step 25.

24. Change the **open** and **alw** parameter values for all the associations changed in steps 15 or 16 using the **chg-assoc** command with the **open=yes** and **alw=yes** parameters.

chg-assoc:aname=assoc1:open=yes:alw=yes

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.6.0
CHG-ASSOC: MASP A - COMPLTD
```

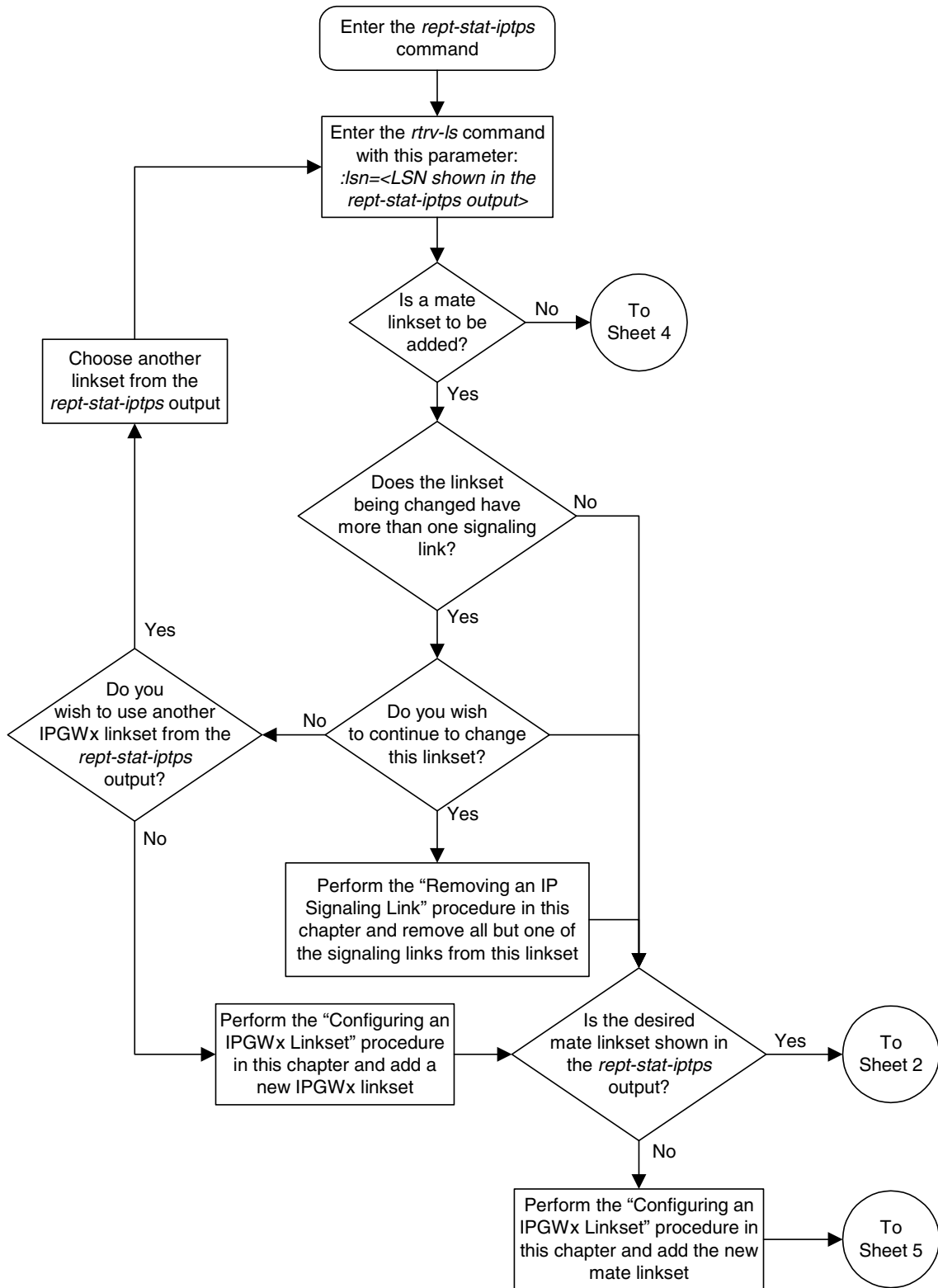
25. Have the far-end node for the signaling link shown in step 20 perform these actions to place the IP connections on the signaling link into service:

- Place the TALI sockets in the NEA-FEA state.
- Place the M3UA or SUA associations in the ASP-ACTIVE state.

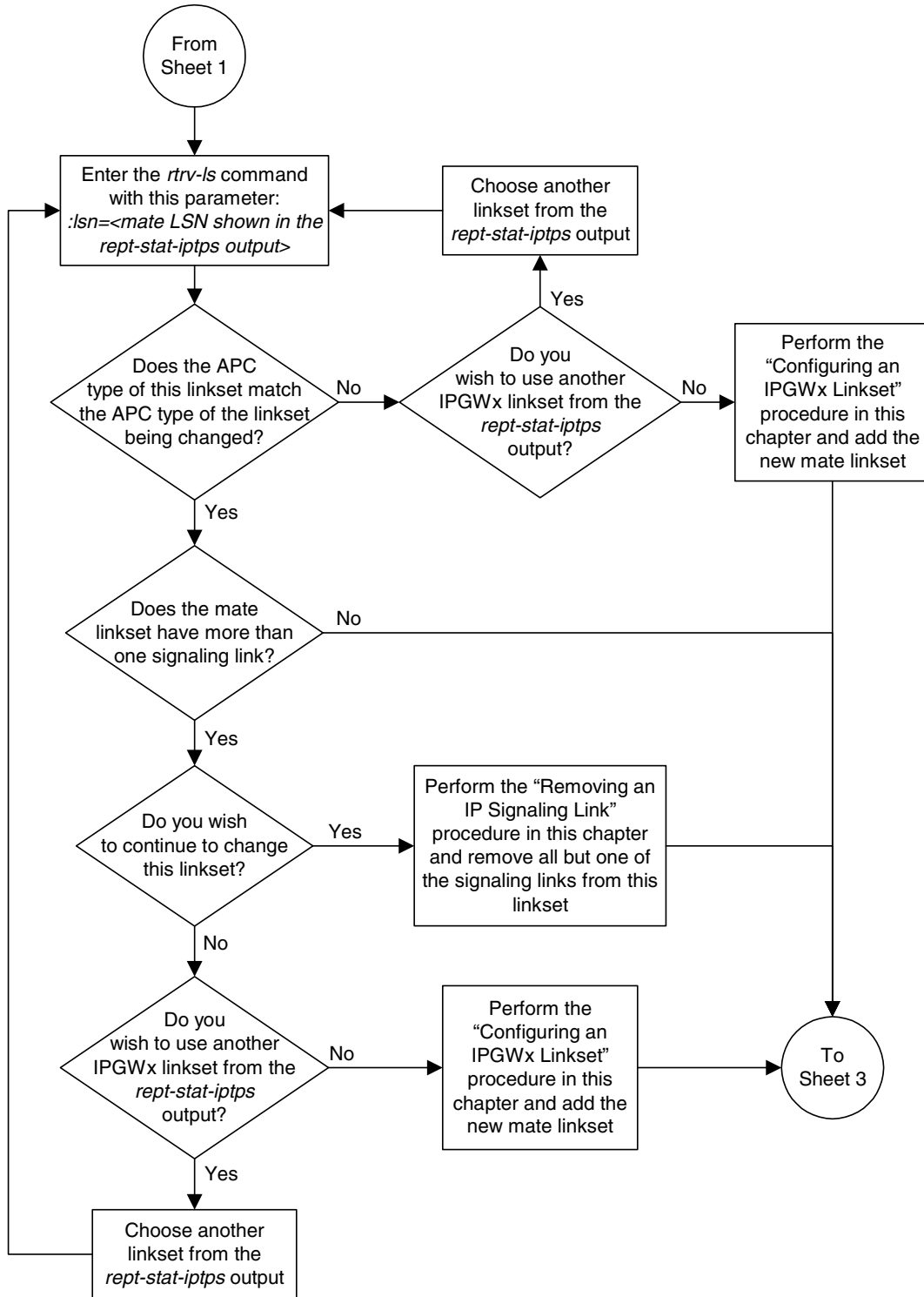
26. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

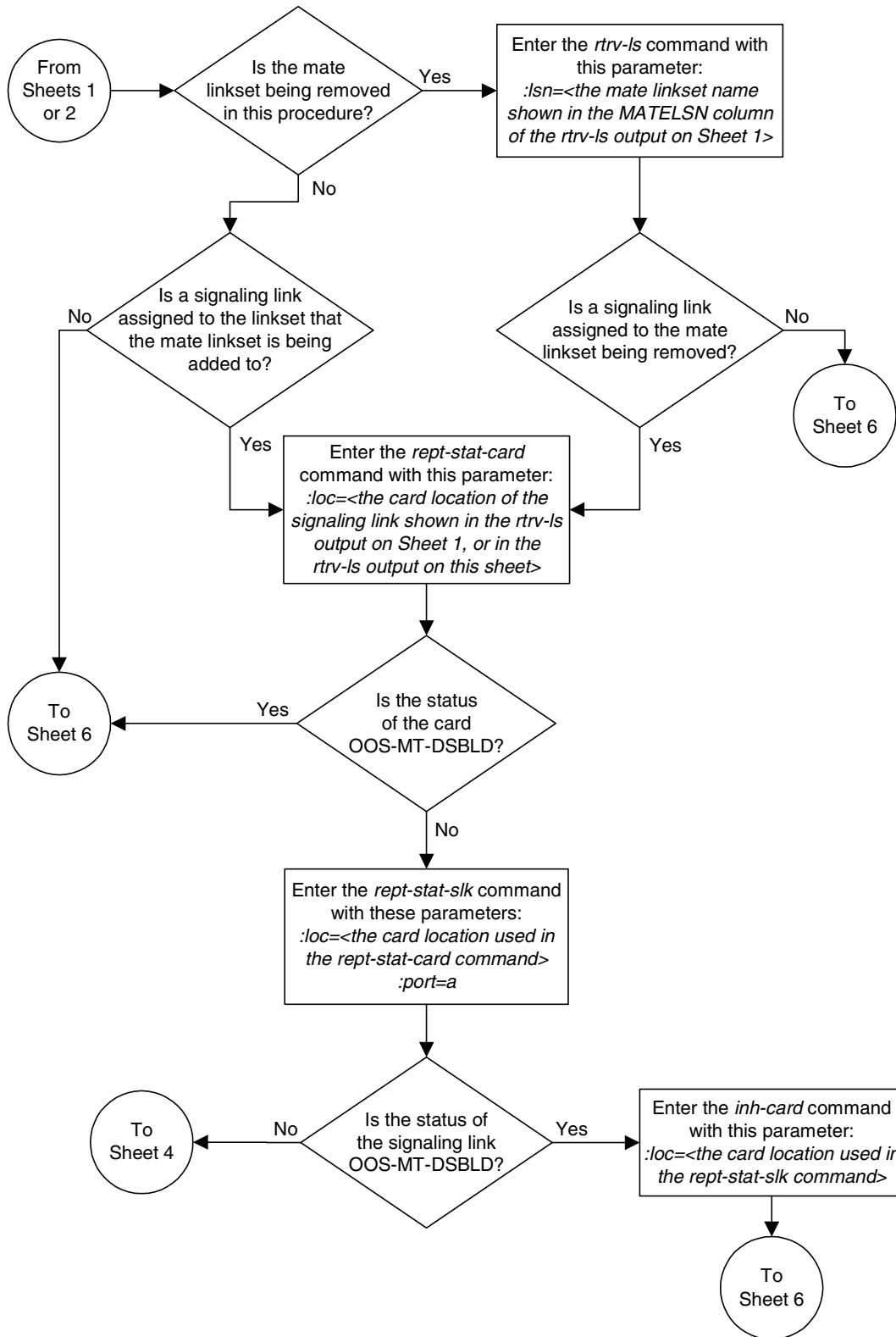
Flowchart 3-4. Configuring a Mate IPGWx Linkset (Sheet 1 of 7)



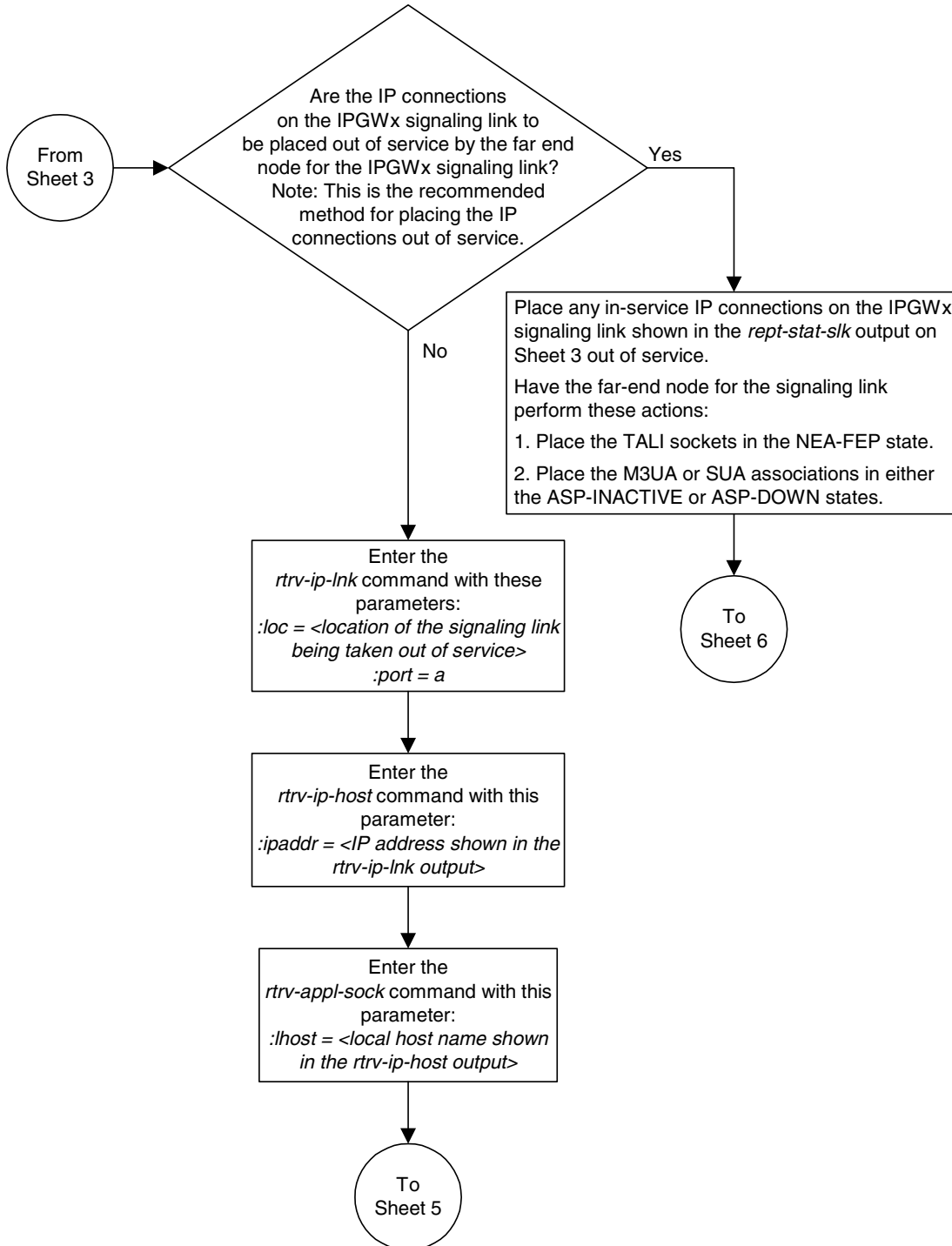
Flowchart 3-4. Configuring a Mate IPGWx Linkset (Sheet 2 of 7)



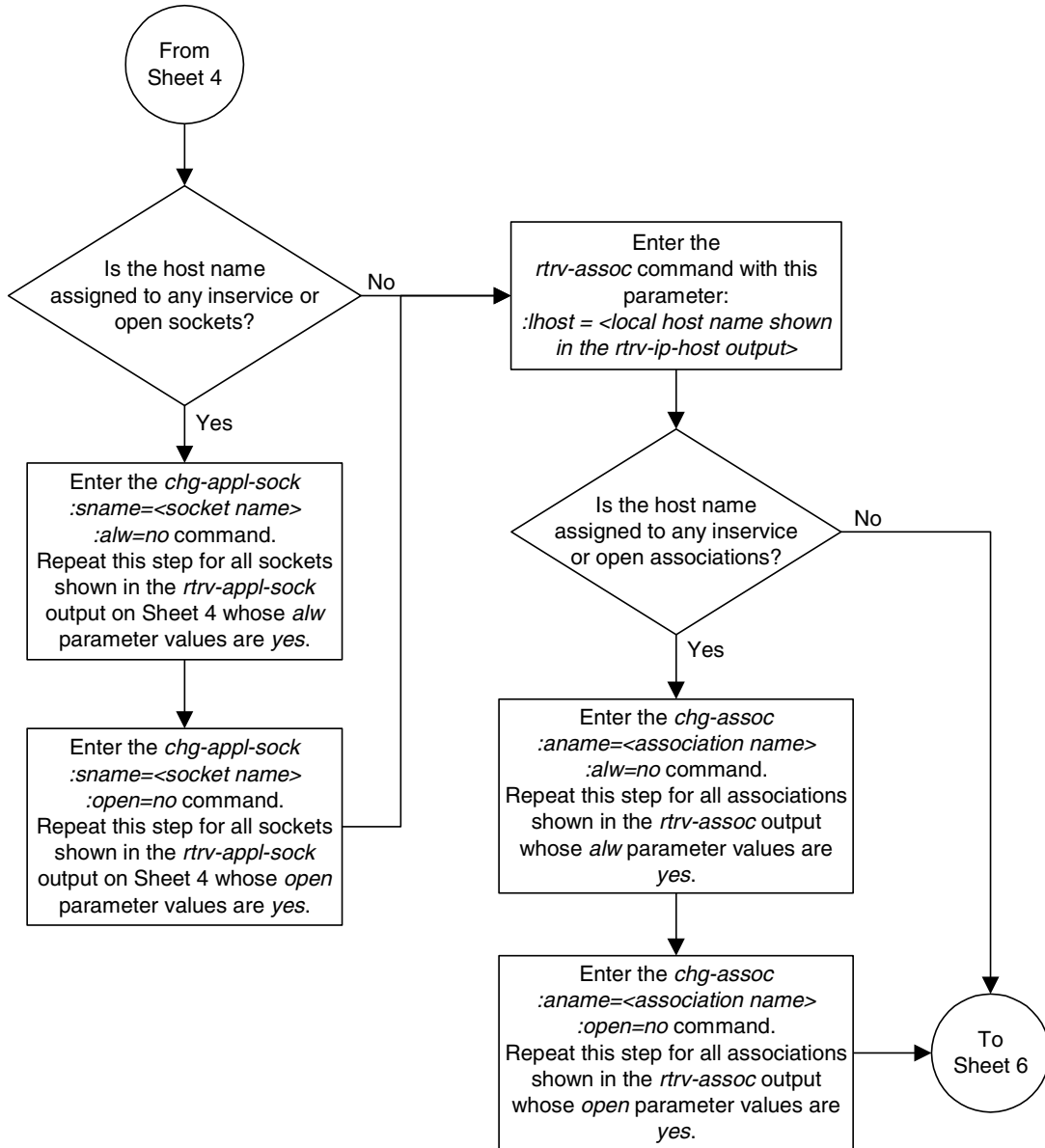
Flowchart 3-4. Configuring a Mate IPGWx Linkset (Sheet 3 of 7)



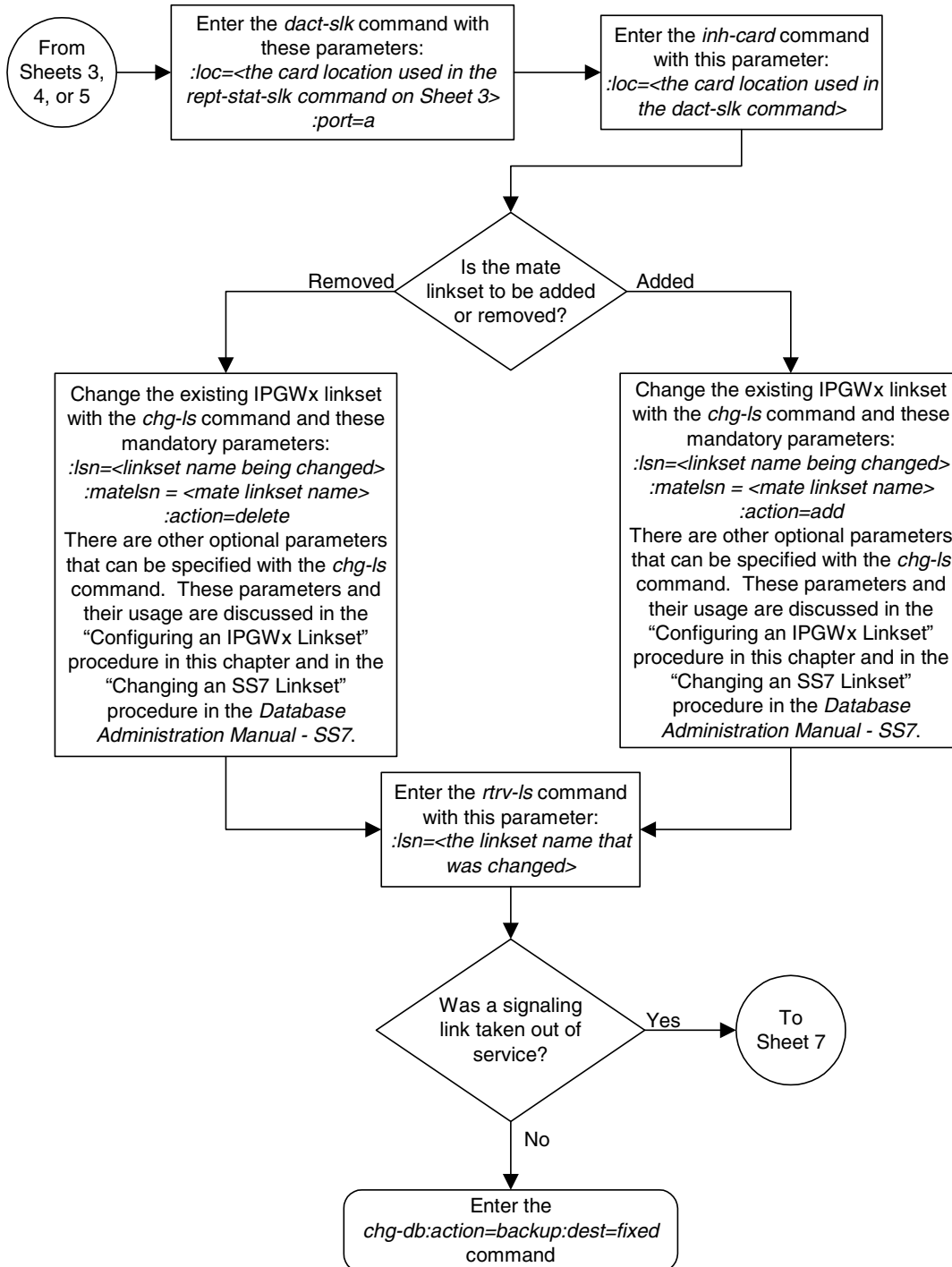
Flowchart 3-4. Configuring a Mate IPGWx Linkset (Sheet 4 of 7)



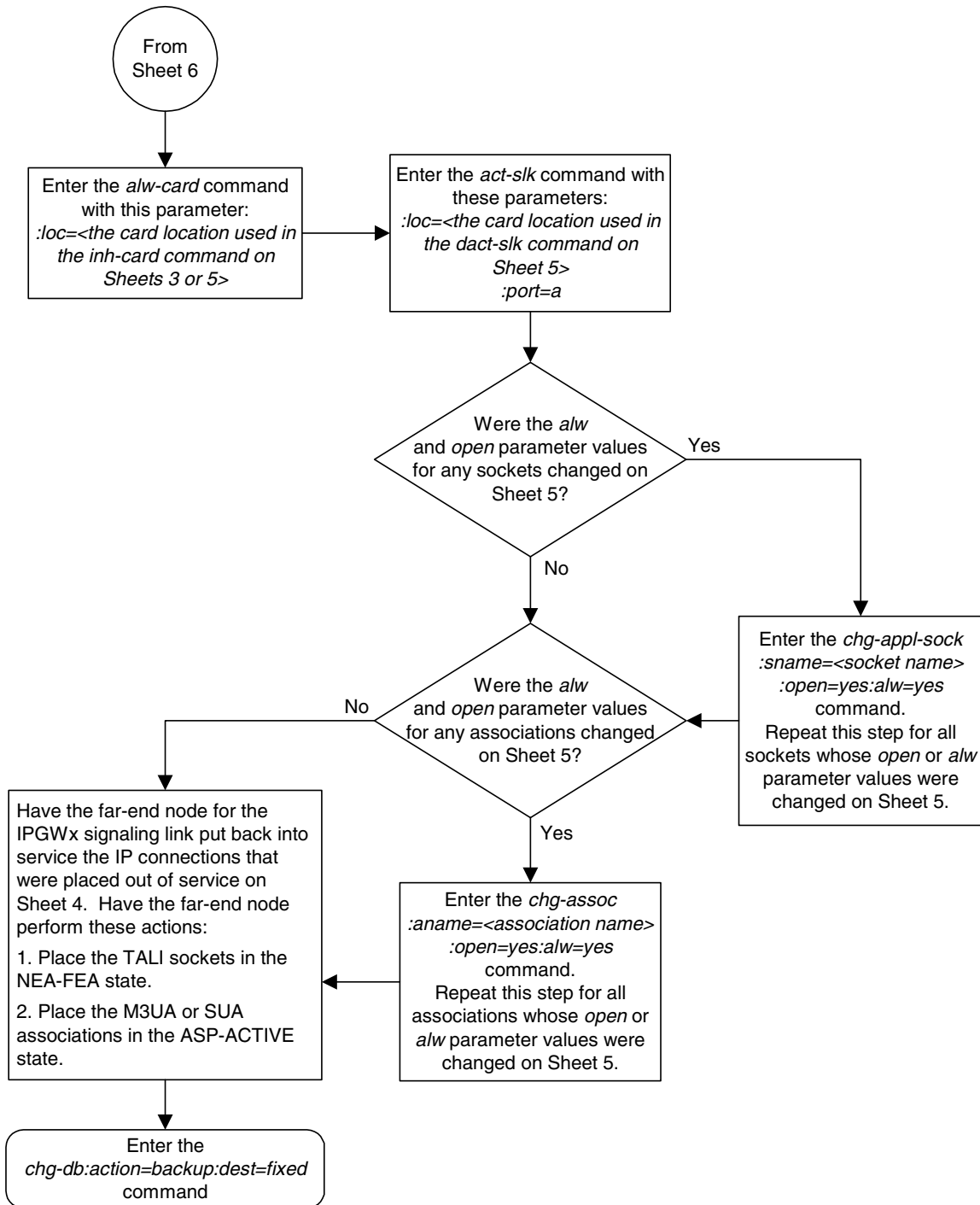
Flowchart 3-4. Configuring a Mate IPGWx Linkset (Sheet 5 of 7)



Flowchart 3-4. Configuring a Mate IPGWx Linkset (Sheet 6 of 7)



Flowchart 3-4. Configuring a Mate IPGWx Linkset (Sheet 7 of 7)



Adding an IP Signaling Link

This procedure is used to add an IP signaling link to the database using the `ent-slk` command. To add other types of signaling links to the database, go to one of these procedures:

The `ent-slk` command uses these parameters.

- `:loc` – The card location of the IP card that the IP signaling link will be assigned to. The cards specified by this parameter are DCMs running the IPLIM, IPLIMI, SS7IPGW, or IPGWI applications.
- `:port` – The port on the card specified in the `loc` parameter.
- `:lsn` – The name of the linkset that will contain the signaling link.
- `:slc` – The signaling link code. The SLC must be unique within the linkset. It must be the same at both the system location and the distant node.
- `:ipliml2` – The L2 protocol stack to be assigned to the IP signaling link, either SAALTAI (the default value), M3UA, or M2PA.

The `ent-slk` command also contains these parameters, `l2tset`, `l1mode`, `bps`, `tset`, `ecm`, `pcrn1`, `pcrn2`, `lpset`, `atmtsel`, `vci`, `vpi`, `ll`, `elatmcr4`, `elatmsi`, `elatmsn`, `ts`, `elport`, `elloc`, `tlport`, and `tlloc`. These parameters are used only for configuring low-speed, ATM high-speed, E1, and T1 signaling links and are not used in this procedure. For more information on configuring these types of signaling links, see the *Database Administration Manual - SS7*.

These items must be configured in the database before an IP signaling link can be added:

- Shelf – see “Adding a Shelf” in the *Database Administration Manual - System Management*.
- Card – see “Adding an SS7 LIM” in the *Database Administration Manual - System Management*.
- Destination Point Code – see “Adding a Destination Point Code” in the *Database Administration Manual - SS7*.
- Linkset – see either “Configuring an IPGWx Linkset” on page 3-40 (for an IPGWx linkset), or “Adding an SS7 Linkset” in the *Database Administration Manual - SS7* (for an IPLIMx linkset).

Verify that the link has been physically installed (all cable connections have been made).

To configure the system to perform circular routing detection test on the signaling links, “Configuring Circular Route Detection” procedure in the *Database Administration Manual - SS7*.

NOTE: Circular route detection is not supported in ITU networks.

To provision a system with more than 500 signaling links, the system must have certain levels of hardware installed. See the System Requirements for Systems Containing more than 500 Signaling Links section on page 3-83 and the

Additional System Requirements for Systems Containing more than 700 Signaling Links section on page 3-83 for more information on these hardware requirements.

The system can contain a mixture of low-speed, E1, T1, ATM high-speed, and IP signaling links. The Determining the Number of High-Speed and Low-Speed Signaling Links section on page 3-84 describes how to determine the quantities of the different types of signaling links the system can have.

System Requirements for Systems Containing more than 500 Signaling Links

To provision a system with more than 500 signaling links (currently the system can have capacities of 700, 1200, or 1500 signaling links), the following requirements must be met:

- TDM, P/N 870-0774-10 or later, installed in card locations 1114 and 1116.
NOTE: If an external high-speed master clock source other than RS-422 is being used for E1, T1, ANSI ATM, or E1 ATM high-speed signaling links, TDMs 870-0774-15 or later must be installed in card locations 1114 and 1116, and the TDM Global Timing Interface options must be configured. For more information, see the “Configuring the Options for the TDM Global Timing Interface” procedure in the *Database Administration Manual - SS7*.
- Control Shelf Backplane, P/N 850-0330-06 or later
- 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 to the desired quantity above 500 signaling links, installed according to the provisioning rules for the increased capacity in the Determining the Number of High-Speed and Low-Speed Signaling Links section on page 3-84. The system can contain a mixture of 2-port LIMs, ATM high-speed LIMs, Multiport LIMs, and E1/T1 MIMs.

For more information on these hardware components, go to the *Installation Manual*.

Additional System Requirements for Systems Containing more than 700 Signaling Links

To provision a system with more than 700 signaling links (currently the system can have capacities of 1200 or 1500 signaling links), the following additional requirements must be met:

- The Measurements Platform feature must be enabled. Perform these procedures in the *Database Administration Manual - System Management* to enable the Measurements Platform Feature:
 - “Adding an MCPM”
 - “Configuring the IP Communications Link for the Measurements Platform Feature”
 - “Adding an FTP Server”

- To provision more than 1200 signaling links, the Large System # Links controlled feature must be enabled for 1500 signaling links. For more information on enabling this feature, go to “Enabling the Large System # Links Controlled Feature” procedure on page 3-108.

Determining the Number of High-Speed and Low-Speed Signaling Links

The system contain either a maximum of 1500, 1200, 700, or 500 signaling links, depending the hardware that is installed. The method of determining the number of high-speed and low-speed signaling links that can be in the system is shown in the next three sections.

1500 or 1200 Signaling Link System

A 1500 or 1200 signaling link system can contain the following quantities of signaling links:

- 1200 low-speed signaling links
- 115 high-speed ATM signaling links (signaling links assigned to either ATMANSI or ATMITU applications)
- 100 signaling links assigned to either the IPLIM or IPLIMI applications.
- 64 single-slot EDCMs running either the **ss7ipgw** or **ipgwi** application, or combinations of the **ss7ipgw** and **ipgwi** applications. If DCMs are present in the system, there can be a maximum of 2 cards running the **ss7ipgw** application and 2 cards running the **ipgwi** application.

Table 3-11 shows the combinations of high-speed signaling links and low-speed signaling links allowed in the system.

Table 3-11. Number of High-Speed and Low-Speed Links Supported at 100% Traffic

Number of High-Speed ATM Signaling Links	Number of Low-Speed Signaling Links	Number of IP Signaling Links	Number of Low-Speed Signaling Links
0	1500	0	1500
0	1200	0	1200
1	1199	1	1199
5	1195	5	1195
15	1185	15	1185
20	1180	20	1180
30	1165	30	1165
40	1150	40	1040

Table 3-11. Number of High-Speed and Low-Speed Links Supported at 100% Traffic (Continued)

Number of High-Speed ATM Signaling Links	Number of Low-Speed Signaling Links	Number of IP Signaling Links	Number of Low-Speed Signaling Links
60	1110	60	880
80	1025	80	720
90	950	90	560
100	875	100	400
115	800		

700 Signaling Link System

If a 700 signaling link system contains a mixture of high-speed and low-speed signaling links, the system can contain a maximum number of 100 high-speed signaling links. If the system contains 100 high-speed signaling links, there can be a maximum of 600 low-speed signaling links, and 41 of these high-speed signaling links can be IP LIMs. The rest of the high-speed signaling links (up to 59) must be high-speed ATM signaling links (signaling links assigned to either ATMANSI or ATMITU applications). For every high-speed signaling link provisioned in the database, up to 100, the maximum number of low-speed signaling links allowed in the system decreases by one. For every low-speed signaling link that is provisioned in the database over the quantity of 600, the maximum number of high-speed signaling links allowed in the system decreases by one. For example, if the system contains 29 high-speed signaling links, the system can contain a maximum of 671 low-speed signaling links.

500 Signaling Link System

The total number of high-speed and low speed signaling links that can coexist in a system is based only on the size of the system, for example, how many cards and card types versus how many slots there are available.

The bandwidth that the system can handle is based on:

- the speed of the IMT and
- the traffic mix
 - number and average size of through-switched MSUs
 - number and average size of MSUs that require global title translation

The system allows a mixture of high-speed and low-speed signaling links. The addition of a high-speed signaling link in the system decreases the number of low-speed signaling links the system can support.

The system supports a maximum of 41 high-speed ATM/ signaling links (either ATMANSI or ATMITU) or IPLIM/IPLIMI high-speed signaling links.

To determine the number of low-speed signaling links a system can contain, based on the number of high-speed signaling links the system has, use the lesser number (rounded down to the nearest whole number) from one of these two formulas.

a. $L = 500 - H$ (for multi-port LIMs) or $L = 500 - (H \times 2)$ (for 2-port LIMs)

L = the number of low-speed signaling links allowed in the system

500 = the maximum number of signaling links allowed in the system

H = the number of high-speed signaling links in the system

b. $L = 32,768,000 - (H \times 786,432) / 45,875$

L = the number of low-speed signaling links

H = the number of high-speed signaling links

32,768,000 = 500 signaling links \times 64 kbps

786,432 = 12 DS0 channels \times 64 kbps

45,875 = 56 kbits \times 0.80

To determine the number of high-speed signaling links a system can contain, based on the number of low-speed signaling links the system has, use the lesser number (rounded down to the nearest whole number) from one of these two formulas.

a. $H = 500 - L$ (for multi-port LIMs) or $H = (500 - L) / 2$ (for 2-port LIMs)

L = the number of low-speed signaling links allowed in the system

500 = the maximum number of signaling links allowed in the system

H = the number of high-speed signaling links in the system

b. $H = 32,768,000 - (45,875 \times L) / 786,432$

L = the number of low-speed signaling links

H = the number of high-speed signaling links

32,768,000 = 500 signaling links \times 64 kbps

786,432 = 12 DS0 channels \times 64 kbps

45,875 = 56 kbits \times 0.80

Table 3-12 shows the number of high-speed signaling links and low-speed signaling links allowed in the system.

Table 3-12. Number of High-Speed and Low-Speed Links Supported at 80% Traffic

Number of High-Speed Links	Number of Low-Speed Links Supported		Number of High-Speed Links	Number of Low-Speed Links Supported	
	Multi-Port LIMs	2-Port LIMs		Multi-Port LIMs	2-Port LIMs
0	500	500	21	354	354
1	499	498	22	337	337
2	498	496	23	320	320
3	497	494	24	302	302
4	496	492	25	285	285
5	495	490	26	268	268
6	494	488	27	251	251
7	493	486	28	234	234
8	492	484	29	217	217
9	491	482	30	200	200
10	490	480	31	182	182
11	489	478	32	165	165
12	488	476	33	148	148
13	487	474	34	131	131
14	474	472	35	114	114
15	457	457	36	97	97
16	440	440	37	80	80
17	422	422	38	62	62
18	405	405	39	45	45
19	388	388	40	28	28
20	371	371	41	11	11

IP Signaling Link Parameter Combinations

Table 3-13 shows the two types of IP signaling links that can be provisioned in the database with the `ent-slk` command in this procedure, and the parameters and values that can be used to provision each type of IP signaling link.

Table 3-13. IP Signaling Link Parameter Combinations

IPGWx Signaling Link	IPLIM Signaling Link
Mandatory Parameters	
:loc = location of the IP card with one of these applications: SS7IPGW or IPGWI; and the DCM card type. ^{1, 2}	:loc = location of the IP card with one of these applications: IPLIM or IPLIMI; and the DCM card type. ^{1, 2}
:port = A	:port = A, A1, A2, A3, B, B1, B2, or B3 ³
:lsn = linkset name ^{4, 5, 6}	:lsn = linkset name ^{4, 8}
:slc = 0 - 15 ^{5, 6}	:slc = 0 - 15 ⁷
Optional Parameters	
	:ipliml2 = saaltali, m3ua, or m2pa ^{7, 8} default value = saaltali
Notes:	
<ol style="list-style-type: none"> 1. If the <code>multgc=yes</code> parameter is assigned to the linkset, the card's application must be IPLIMI or IPGWI. 2. If the <code>ipgwapc=yes</code> parameter is assigned to the linkset, the card's application must be SS7IPGW or IPGWI. 3. The ports A1, A2, A3, B1, B2, or B3 can be specified only if the card is a single-slot EDCM. 4. If the card's application is IPLIMI or IPGWI, the linkset adjacent point code must be ITU. If the card's application is IPLIM or SS7IPGW, the linkset adjacent point code must be ANSI. The domain of the linkset adjacent point code must be SS7. 5. A linkset can contain only one signaling link assigned to the SS7IPGW or IPGWI applications if the linkset contains a mate IPGWx linkset, or is the mate of an IPGWx linkset. 6. If the linkset does not have a mate IPGWx linkset assigned to it, or is not the mate of an IPGWx linkset, the linkset can contain up to 8 signaling links assigned to the SS7IPGW or IPGWI applications. 7. If the <code>ipliml2=m3ua</code> parameter is specified for the signaling link, all signaling links in the linkset must contain the <code>ipliml2=m3ua</code> parameter. The <code>mtprse</code> value of the linkset containing signaling links with the <code>ipliml2=m3ua</code> parameter must be <code>no</code>. If the <code>ipliml2=saaltali</code> or <code>ipliml2=m2pa</code> parameter is specified for the signaling link, this signaling link can be in a linkset that contains non-IPLIMx signaling links. The card's application must be either IPLIM or IPLIMI. 8. Signaling links containing the <code>ipliml2=saaltali</code> parameter value cannot be assigned to linksets containing 24-bit ITU-N APCs (APCN24) or SAPCs (SAPCN24). 	

Example Signaling Link Configuration

This examples used in this procedure are based on the examples shown in Table 3-14.

Table 3-14. IP Signaling Link Configuration Table

SLK		LSN	SLC	TYPE	IPLIML2
LOC	PORT				
2202	A	LSNIP1	0	IPLIM	SALLTALI
2204	B	LSNIP2	0	IPLIM	M3UA
2205	A	LSNIP1	1	IPLIM	M2PA
2207	A	LSNIP3	0	SS7IPGW	N/A
2211	A	LSNIP4	0	IPGWI	N/A
2213	A	LSNIP5	0	IPLIMI	M2PA
2215	A	LSNIP2	1	IPLIM	M3UA

Canceling the `rept-stat-slk` and `rtrv-slk` Commands

Because the `rept-stat-slk` and `rtrv-slk` commands used in this procedure can output information for a long period of time, the `rept-stat-slk` and `rtrv-slk` commands can be canceled and the output to the terminal stopped. There are three ways that the `rept-stat-slk` and `rtrv-slk` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rept-stat-slk` or `rtrv-slk` commands were entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rept-stat-slk` or `rtrv-slk` commands were entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rept-stat-slk` or `rtrv-slk` commands were entered, from another terminal other than the terminal where the `rept-stat-slk` or `rtrv-slk` commands were entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current signaling link configuration using the `rtrv-slk` command. This is an example of the possible output.

```

rlghncxa03w 04-12-19 21:16:37 GMT EAGLE5 31.6.0
      L2T          L1          PCR PCR
LOC  PORT LSN      SLC TYPE  SET  BPS  MODE TSET  ECM  N1  N2
1201 B   lsa1       0  LIMDS0  1  56000  --- ---  BASIC ---  -----
1203 B   lsa2       0  LIMDS0  1  56000  --- ---  BASIC ---  -----
1205 A   lsa3       0  LIMV35  3  64000  DCE  ON   BASIC ---  -----
1207 A   lsn1207a   0  LIMDS0  1  56000  --- ---  BASIC ---  -----
1207 B   lsn1207b   0  LIMDS0  1  56000  --- ---  BASIC ---  -----
1214 A   lsn1214a   0  LIMV35  2  64000  DTE  --- PCR  76  3800
1214 B   lsa3       1  LIMV35  3  64000  DCE  ON   BASIC ---  -----

      LP          ATM
      SET  BPS    TSEL      VCI  VPI  LL
LOC  PORT LSN      SLC TYPE  SET  BPS    TSEL      VCI  VPI  LL

      LP          ATM          E1ATM
      SET  BPS    TSEL      VCI  VPI  CRC4 SI SN
LOC  PORT LSN      SLC TYPE  SET  BPS    TSEL      VCI  VPI  CRC4 SI SN

No Links Set up.

LOC  PORT LSN      SLC TYPE  IPLIML2

No Links Set up.

LOC  PORT LSN      SLC TYPE

No Links Set up.

      L2T          PCR PCR  E1  E1
      SET  BPS    ECM  N1  N2  LOC  PORT TS
LOC  PORT LSN      SLC TYPE  SET  BPS    ECM  N1  N2  LOC  PORT TS

No Links Set up.

      L2T          PCR PCR  T1  T1
      SET  BPS    ECM  N1  N2  LOC  PORT TS
LOC  PORT LSN      SLC TYPE  SET  BPS    ECM  N1  N2  LOC  PORT TS

No Links Set up.

SLK table is (7 of 500) 1% full.

```

NOTE: If the `rtrv-slk` output in step 1 shows that the maximum number of signaling links is 1500, skip step 2 and go to step 3.

NOTE: If the `rtrv-slk` output in step 1 shows that the maximum number of signaling links is 1200, and the signaling link being added increases the number beyond 1200, do not perform step 2, but go to “Enabling the Large System # Links Controlled Feature” procedure on page 3-108 and enable the Large System # Links controlled feature for 1500 signaling links. Then go to step 3.

NOTE: If the `rtrv-slk` output in step 1 shows that the maximum number of signaling links is either 500, 700, or 1200, and the signaling link being added will not increase the number beyond the quantity shown in the `rtrv-slk` output in step 1, skip step 2 and go to step 3.

2. Display the status of the Large System # Links controlled feature by entering the `rtrv-ctrl-feat` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.6.0
The following features have been permanently enabled:
```

Feature Name	Partnum	Status	Quantity
IPGWx Signaling TPS	893012814	on	20000
ISUP Normalization	893000201	on	----
Command Class Management	893005801	on	----
LNP Short Message Service	893006601	on	----
Intermed GTT Load Sharing	893006901	on	----
XGTT Table Expansion	893006101	off	----
XMAP Table Expansion	893007701	off	----

The following features have been temporarily enabled:

Feature Name	Partnum	Status	Quantity	Trial Period Left
Zero entries found.				

The following features have expired temporary keys:

Feature Name	Partnum
Zero entries found.	

If the Large System # Links controlled feature is not enabled or on, go to “Enabling the Large System # Links Controlled Feature” procedure on page 3-108 and enable Large System # Links controlled feature for 1500 signaling links. Then go to step 3.

3. Display the current linkset configuration using the `rtrv-ls` command. This is an example of the possible output.

```

rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.6.0
                                     L3T SLT                               GWS GWS GWS
LSN          APCA   (SS7)  SCRN  SET SET BEI LST LNKS  ACT MES DIS SLSCI NIS
ele2         001-207-000  none  1  1  no  B   6   off off off no   off
ls1305      000-005-000  none  1  1  no  A   1   off off off no   off
ls1307      000-007-000  none  1  1  no  A   1   off off off no   off
el1m1s1     001-001-001  none  1  1  no  A   7   off off off no   off
el1m1s2     001-001-002  none  1  1  no  A   7   off off off no   off

                                     L3T SLT                               GWS GWS GWS
LSN          APCA   (X25)  SCRN  SET SET BEI LST LNKS  ACT MES DIS SLSCI NIS

                                     L3T SLT                               GWS GWS GWS
LSN          APCI   (SS7)  SCRN  SET SET BEI LST LNKS  ACT MES DIS SLSCI NIS
ele2i       1-207-0      none  1  1  no  B   4   off off off ---  on
ls1315      0-015-0      none  1  1  no  A   1   off off off ---  off
ls1317      0-017-0      none  1  1  no  A   1   off off off ---  on
el1m2s1     1-011-1      none  1  1  no  A   7   off off off ---  off
el1m2s2     1-011-2      none  1  1  no  A   7   off off off ---  off

                                     L3T SLT                               GWS GWS GWS
LSN          APCN   (SS7)  SCRN  SET SET BEI LST LNKS  ACT MES DIS SLSCI NIS

                                     L3T SLT                               GWS GWS GWS
LSN          APCN24 (SS7)  SCRN  SET SET BEI LST LNKS  ACT MES DIS SLSCI NIS

Link set table is (10 of 1024) 1% full.
;

```

If the required linkset is not in the database, perform one of these procedures to add the linkset to the database:

- To add an IPGWx linkset – the “Configuring an IPGWx Linkset” procedure on page 3-40.
- To add an IPLIMx linkset (a linkset that will contain signaling links assigned to cards running either the IPLIM or IPLIMI applications) – the “Adding an SS7 Linkset” procedure in the *Database Administration Manual - SS7*.

If you plan to use a linkset shown in this step, go to step 4.

If a new linkset is being added in this step, skip step 4 and go to step 5.

4. Display the linkset that the signaling link is being assigned to using the `rtrv-ls` command, specifying the name of the linkset that the signaling link is being assigned to. For this example, enter this command.

```
rtrv-ls:lsn=lsnipgw
```

This is an example of the possible output.

```

rlghncxa03w 02-12-17 11:43:04 GMT EAGLE5 31.6.0
                                     L3T SLT                               GWS GWS GWS
LSN          APCI   (SS7)  SCRN  SET SET BEI LST LNKS  ACT MES DIS SLSCI NIS
lsipgw      2968          none  1  1  no  A   1   off off off ---  off

```

IP7 Secure Gateway Configuration Procedures

```

CLLI          TFATCABMLQ  MTPRSE  ASL8  SLRSRB  MULTGC  ITUTFR
----- 1          no      ---  1      yes     off

IPGWAPC  MATELSN  IPTPS  LSUSEALM  SLKUSEALM
no      -----  ---  ---  ---

LOC  PORT  SLC  TYPE          L2T          L1          PCR  PCR
SET  BPS  MODE  TSET  ECM  N1  N2

LOC  PORT  SLC  TYPE          LP          ATM          VCI  VPI  LL
SET  BPS  TSEL

LOC  PORT  SLC  TYPE          LP          ATM          VCI  VPI  CRC4  SI  SN
SET  BPS  TSEL

LOC  PORT  SLC  TYPE          IPLIML2
1317 A      0  IPLIMI  SAALTALI

LOC  PORT  SLC  TYPE

LOC  PORT  SLC  TYPE          L2T          PCR  PCR  E1  E1
SET  BPS  ECM  N1  N2  LOC  PORT  TS

LOC  PORT  SLC  TYPE          L2T          PCR  PCR  T1  T1
SET  BPS  ECM  N1  N2  LOC  PORT  TS

SAPCI
1-10-1

SAPCN
1234-aa
1235-bb
1200-zz

```

Link set table is (13 of 1024) 1% full.

Linksets can contain a mixture of signaling link types unless the signaling links in the linkset have the `ipliml2=m3ua` parameter value assigned, or if the card application is SS7IPGW or IPGWI. If the signaling links in the linkset have the `ipliml2=m3ua` parameter value assigned, then all signaling links in the linkset must have the `ipliml2=m3ua` parameter assigned.

If an IPGWx signaling link is being added, skip the remainder of this step and go to step 5.

A signaling link containing the `ipliml2=saaltali` parameter cannot be assigned to a linkset containing a 24-bit ITU-N adjacent point code. Either choose another linkset without a 24-bit-ITU-N adjacent point code from the `rtrv-1s` output in step 3, or add a new IPLIMx linkset by performing the "Adding the SS7 Linkset" procedure in the *Database Administration Manual - SS7*.

If you do not wish to assign the signaling link to this linkset, go to the "Adding the SS7 Linkset" procedure in the *Database Administration Manual - SS7* and add the IPLIMx linkset to the database with these parameters:

- For signaling links with the `ipliml2=m3ua` parameter, add the linkset with the `mtpmse=no` parameter.
- For signaling links without the `ipliml2=m3ua` parameter, the value of the `mtpmse` parameter can be either `yes` or `no`.

NOTE: If an IPLIMx signaling link is being added, skip steps 6 through 9, and go to step 10.

NOTE: If the IPGWx linkset contains any IPGWx signaling links, skip step 6 and go to step 7.

6. If you wish to assign an IPGWx signaling link to a linkset contains no signaling links, but the `IPGWAPC` value is no, perform the "Removing a Linkset Containing SS7 Signaling Links" procedure in the *Database Administration Manual - SS7* and remove the linkset, then go to the "Configuring an IPGWx Linkset" procedure on page 3-40 and re-enter the new linkset with the `ipgwapc=yes` parameter. Skip steps 7 through 9 and go to step 10.
-

7. If the desired linkset, shown in the `rtrv-ls` output in step 5, has a mate IPGWx linkset assigned, or is the mate to another IPGWx linkset, the desired linkset can contain only one signaling link.

If the desired linkset does not have a mate IPGWx linkset assigned, or is not the mate of another IPGWx linkset, the desired linkset can contain up to 8 IPGWx signaling links. No other signaling link types can be in an IPGWx linkset.

If you wish to assign more than one IPGWx signaling link to an IPGWx linkset that has a mate linkset assigned, the mate to this linkset must be removed. Perform the "Configuring a Mate IPGWx Linkset" procedure on page 3-60 and remove the mate linkset from the linkset you wish to assign the IPGWx signaling link to. If you do not wish to use this linkset, perform the "Configuring an IPGWx Linkset" procedure on page 3-40 and add a new IPGWx linkset.

If the desired IPGWx linkset does not have a mate assigned, go to step 7.

If the desired linkset has a mate linkset assigned, and contains an IPGWx signaling link, perform the "Configuring a Mate IPGWx Linkset" procedure on page 3-60 and add a new IPGWx linkset. Skip steps 8 and 9, and go to step 10.

- If you wish to assign more than one IPGWx signaling link to an IPGWx linkset that is a mate to another IPGWx linkset, this linkset must be removed from the other linkset as a mate.

To verify if the linkset you wish to use is the mate of another IPGWx linkset, enter the **rept-stat-iptps** command to display the names of all the IPGWx linksets. This is an example of the possible output.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.6.0
IP TPS USAGE REPORT
-----
                THRESH  CONFIG          TPS      PEAK      PEAKTIMESTAMP
-----
SYSTEM
RLGHNCXA03W  100%    30000  TX:   7200    7600    04-06-10 11:40:04
                RCV:   7200    7600    04-06-10 11:40:04
-----
LSN
LSGW1101      80%     6000  TX:   5100    5500    04-06-10 11:40:04
                RCV:   5100    5500    04-06-10 11:40:04
LSGW1103      80%     6000  TX:   5200    5500    04-06-10 11:40:04
                RCV:   5200    5500    04-06-10 11:40:04
LSGW1105      80%    14000  TX:   7300    7450    04-06-10 11:40:04
                RCV:   7300    7450    04-06-10 11:40:04
LSGW1107      70%     4000  TX:   3200    3500    04-06-10 11:40:04
                RCV:   3200    3500    04-06-10 11:40:04
-----
Command Completed.
```

- Enter the **rtrv-ls:lsn=<IPGWx linkset name from the rept-stat-iptps output>** to verify if the desired linkset is the mate of another IPGWx linkset. For this example, enter this command.

rtrv-ls:lsn=lsgw1103

This is an example of the possible output.

```
rlghncxa03w 04-12-17 11:43:04 GMT EAGLE5 31.6.0
LSN          APCA  (SS7)  SCRN  L3T SLT          GWS GWS GWS
lsgw1103     003-002-004  none  1  1  no  A  1  off off off no  off
CLLI          TFATCABMLQ MTPRSE ASL8
-----  1          no  no
IPGWAPC  MATELSN  IPTPS  LSUSEALM  SLKUSEALM
yes      lsgw1107  10000  70  %  70  %
LOC  PORT  SLC  TYPE          L2T          L1          PCR  PCR
SET  BPS  MODE  TSET  ECM  N1  N2
LOC  PORT  SLC  TYPE          LP          ATM
SET  BPS  TSEL          VCI  VPI  LL
LOC  PORT  SLC  TYPE          LP          ATM          E1ATM
SET  BPS  TSEL          VCI  VPI  CRC4  SI  SN
LOC  PORT  SLC  TYPE          IPLIML2
```

IP7 Secure Gateway Configuration Procedures

```
LOC  PORT  SLC  TYPE
1103  A      0    SS7IPGW

LOC  PORT  SLC  TYPE          L2T          PCR  PCR  E1  E1
SET  BPS   ECM  N1  N2   LOC  PORT  TS

LOC  PORT  SLC  TYPE          L2T          PCR  PCR  T1  T1
SET  BPS   ECM  N1  N2   LOC  PORT  TS
```

Link set table is (14 of 1024) 1% full

If the name of the linkset you wish to use is not shown in the **MATELSN** field of the **rtrv-ls** output, repeat this step until all the IPGWx linksets have been displayed, or until a linkset has been found that has the linkset you wish to use assigned as a mate. If the linkset you wish to use is not the mate of another IPGWx linkset, go to step 10.

If the name of the linkset you wish to use is shown in the **MATELSN** field of the **rtrv-ls** output, perform the "Configuring a Mate IPGWx Linkset" procedure on page 3-60 to remove this linkset from the other linkset as a mate. Then go to step 10.

If the desired linkset is the mate of another IPGWx linkset, and you do not wish to use this linkset, perform the "Configuring an IPGWx Linkset" procedure on page 3-40 and add a new IPGWx linkset. Then go to step 10.

-
10. Add the signaling link to the database using the **ent-slk** command. Use Table 3-13 on page 3-88 as a guide for the parameters that can be specified with the **ent-slk** command. For this example, enter these commands.

```
ent-slk:loc=2202:port=a:lsn=lsnlp1:slc=0:ipliml2=saaltali
ent-slk:loc=2204:port=b:lsn=lsnlp2:slc=0:ipliml2=m3ua
ent-slk:loc=2205:port=a:lsn=lsnlp1:slc=1:ipliml2=m2pa
ent-slk:loc=2207:port=a:lsn=lsnlp3:slc=0
ent-slk:loc=2211:port=a:lsn=lsnlp4:slc=0
ent-slk:loc=2213:port=a:lsn=lsnlp5:slc=0:ipliml2=m2pa
ent-slk:loc=2215:port=a:lsn=lsnlp2:slc=1:ipliml2=m3ua
```

When each of these commands have successfully completed, this message should appear.

```
rlghncxa03w 04-12-07 08:29:03 GMT  EAGLE5 31.6.0
ENT-SLK: MASP A - COMPLTD
```

11. Verify the changes using the `rtrv-slk` command. This is an example of the possible output.

```

rlghncxa03w 04-12-19 21:16:37 GMT EAGLE5 31.6.0

LOC  PORT  LSN          SLC TYPE      L2T          L1           PCR  PCR
                                SET  BPS        MODE TSET    ECM  N1   N2
1201 A    ls01          0  LIMDS0    1  56000    --- ---  BASIC ---  ---
1201 B    lsa1          0  LIMDS0    1  56000    --- ---  BASIC ---  ---
1202 B    ls02          0  LIMV35    2  64000    DTE ---  BASIC ---  ---
1203 A    ls03          0  LIMDS0    3  56000    --- ---  BASIC ---  ---
1203 B    lsa2          0  LIMDS0    1  56000    --- ---  BASIC ---  ---
1204 B    ls01          1  LIMDS0    1  56000    --- ---  BASIC ---  ---
1205 A    lsa3          0  LIMV35    4  64000    DCE ON   BASIC ---  ---
1206 A    ls02          1  LIMV35    2  64000    DTE ---  BASIC ---  ---
1207 A    lsn1207a     0  LIMDS0    1  56000    --- ---  BASIC ---  ---
1207 B    lsn1207b     0  LIMDS0    1  56000    --- ---  BASIC ---  ---
1208 B    ls03          1  LIMDS0    3  56000    --- ---  BASIC ---  ---
1212 A    ls04          0  LIMV35    4  64000    DTE ---  BASIC ---  ---
1213 B    ls05          0  LIMDS0    5  56000    --- ---  BASIC ---  ---
1214 A    lsn1214a     0  LIMV35    2  64000    DTE ---  PCR  76  3800
1214 B    lsa3          1  LIMV35    4  64000    DCE ON   BASIC ---  ---
1215 A    ls05          1  LIMDS0    5  56000    --- ---  BASIC ---  ---
1301 B    ls06          0  LIMV35    6  56000    DTE ---  BASIC ---  ---
1304 B    ls06          1  LIMV35    6  56000    DTE ---  BASIC ---  ---
1308 A    ls06          2  LIMV35    6  56000    DTE ---  BASIC ---  ---
1311 A    ls01          2  LIMDS0    1  56000    --- ---  BASIC ---  ---
1311 A1   ls05          2  LIMDS0    5  56000    --- ---  BASIC ---  ---
1311 B    ls03          2  LIMDS0    3  56000    --- ---  BASIC ---  ---
1311 B1   ls07          1  LIMDS0    7  56000    --- ---  BASIC ---  ---
1313 A    ls07          0  LIMDS0    7  56000    --- ---  BASIC ---  ---
1315 A    lsn5          0  LIMV35   11  64000    DTE OFF  BASIC ---  ---
1317 A    lsi7          0  LIMV35   11  64000    DTE OFF  BASIC ---  ---

LOC  PORT  LSN          SLC TYPE      LP           ATM          VCI  VPI  LL
                                SET  BPS        TSEL
No Links Set up.

LOC  PORT  LSN          SLC TYPE      LP           ATM          E1ATM  VCI  VPI  CRC4  SI  SN
                                SET  BPS        TSEL
No Links Set up.

LOC  PORT  LSN          SLC TYPE      IPLIML2
2202 A    lsnlp1     0  IPLIM  SAALTALI
2205 A    lsnip1     1  IPLIM  M2PA
2204 B    lsnlp2     0  IPLIM  M3UA
2213 A    lsnip5     0  IPLIMI M2PA
2215 A    lsnlp2     1  IPLIM  M3UA

LOC  PORT  LSN          SLC TYPE
2207 A    lsnlp3     0  SS7IPGW
2211 A    lsnlp4     0  IPGWI

LOC  PORT  LSN          SLC TYPE      L2T          PCR  PCR  E1  E1
                                SET  BPS        ECM  N1   N2  LOC  PORT  TS
No Links Set up.

LOC  PORT  LSN          SLC TYPE      L2T          PCR  PCR  T1  T1
                                SET  BPS        ECM  N1   N2  LOC  PORT  TS
No Links Set up.

SLK table is (38 of 1500) 3% full.

```


12. If any cards contain the first signaling link on a card, those cards must be brought into service with the **rst-card** command, specifying the location of the card. For this example, enter these commands.

```
rst-card:loc=2202
rst-card:loc=2204
rst-card:loc=2205
rst-card:loc=2207
rst-card:loc=2211
rst-card:loc=2213
rst-card:loc=2215
```

When each of these commands have successfully completed, this message should appear.

```
rlghncxa03w 04-12-23 13:05:05 GMT EAGLE5 31.6.0
Card has been allowed.
```

13. Activate all signaling links on the cards using the **act-slk** command, specifying the card location and port of each signaling link. For this example, enter these commands.

```
act-slk:loc=2202:port=a
act-slk:loc=2204:port=b
act-slk:loc=2205:port=a
act-slk:loc=2207:port=a
act-slk:loc=2211:port=a
act-slk:loc=2213:port=a
act-slk:loc=2215:port=a
```

When each of these commands have successfully completed, this message should appear.

```
rlghncxa03w 04-12-07 08:31:24 GMT EAGLE5 31.6.0
Activate Link message sent to card
```

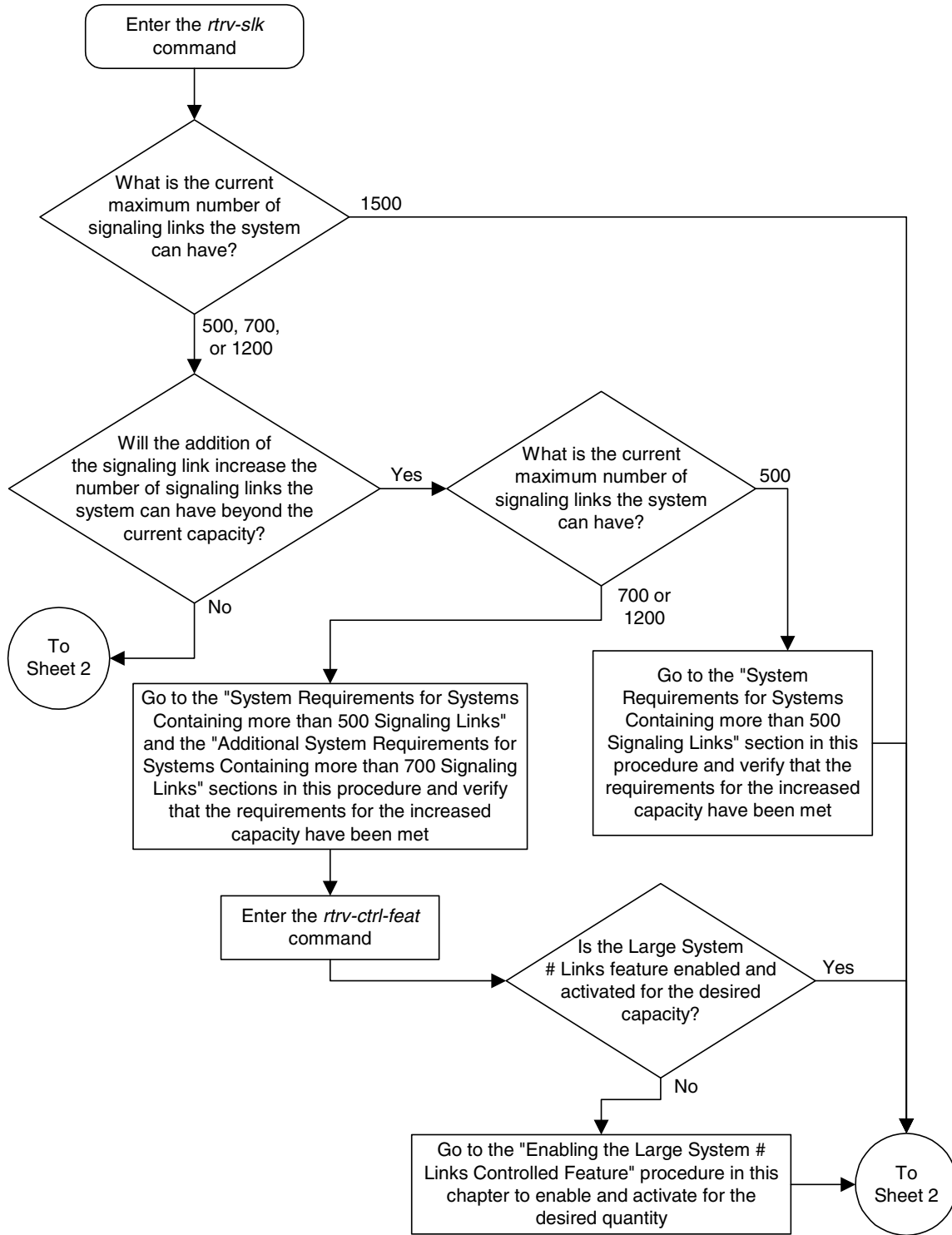
14. Check the status of the signaling links added in step 8 using the **rept-stat-slk** command. The state of each signaling link should be in service normal (IS-NR) after the link has completed alignment (shown in the **PST** field). This is an example of the possible output.

```
rlghncxa03w 04-12-19 21:16:37 GMT EAGLE5 31.6.0
SLK      LSN      CLLI      PST      SST      AST
1201,A   ls01     ls01c1li  IS-NR    Avail    ----
1201,B   lsa1     -----  IS-NR    Avail    ----
1202,B   ls02     ls02c1li  IS-NR    Avail    ----
1203,A   ls03     ls03c1li  IS-NR    Avail    ----
1203,B   lsa2     -----  IS-NR    Avail    ----
1204,B   ls01     ls01c1li  IS-NR    Avail    ----
1205,A   lsa3     -----  IS-NR    Avail    ----
1206,A   ls02     ls02c1li  IS-NR    Avail    ----
1207,A   lsn1207a -----  IS-NR    Avail    ----
1207,B   lsn1207b -----  IS-NR    Avail    ----
1208,B   ls03     ls03c1li  IS-NR    Avail    ----
1212,A   ls04     ls04c1li  IS-NR    Avail    ----
1213,B   ls05     lsn5c1li  IS-NR    Avail    ----
1214,A   lsn1214a -----  IS-NR    Avail    ----
1214,B   lsa3     -----  IS-NR    Avail    ----
1215,A   ls05     lsn5c1li  IS-NR    Avail    ----
1301,B   ls06     ls06c1li  IS-NR    Avail    ----
1304,B   ls06     ls06c1li  IS-NR    Avail    ----
1308,A   ls06     ls06c1li  IS-NR    Avail    ----
1311,A   ls01     ls01c1li  IS-NR    Avail    ----
1311,A1  ls05     lsn5c1li  IS-NR    Avail    ----
1311,B   ls03     ls03c1li  IS-NR    Avail    ----
1311,B1  ls07     ls07c1li  IS-NR    Avail    ----
1313,A   ls07     ls07c1li  IS-NR    Avail    ----
1315,A   lsn5     -----  IS-NR    Avail    ----
1317,A   lsi7     -----  IS-NR    Avail    ----
2202,A   lsnlp1   -----  IS-NR    Avail    ----
2204,B   lsnlp2   -----  IS-NR    Avail    ----
2205,A   lsnlp1   -----  IS-NR    Avail    ----
2207,A   lsnlp3   -----  IS-NR    Avail    ----
2211,A   lsnlp4   -----  IS-NR    Avail    ----
2213,A   lsnlp5   -----  IS-NR    Avail    ----
2215,A   lsnlp2   -----  IS-NR    Avail    ----
```

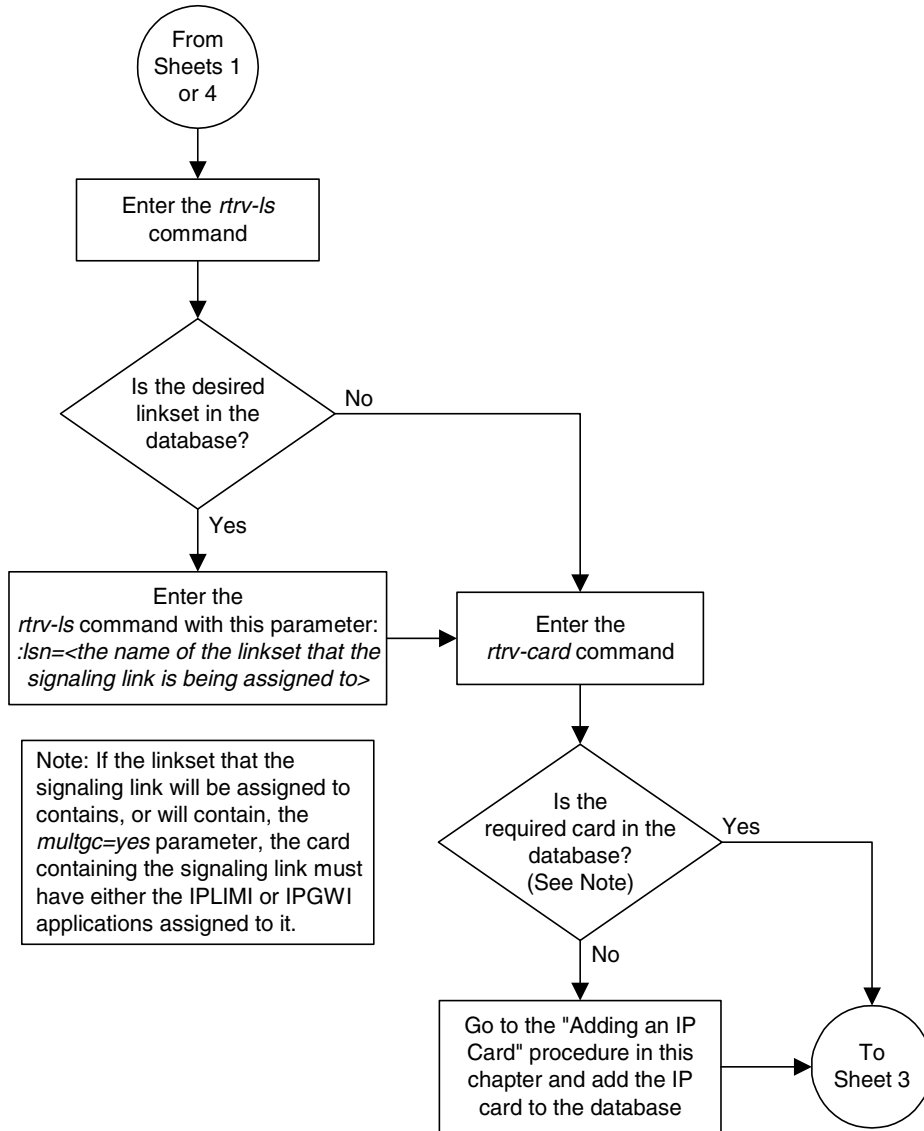
15. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

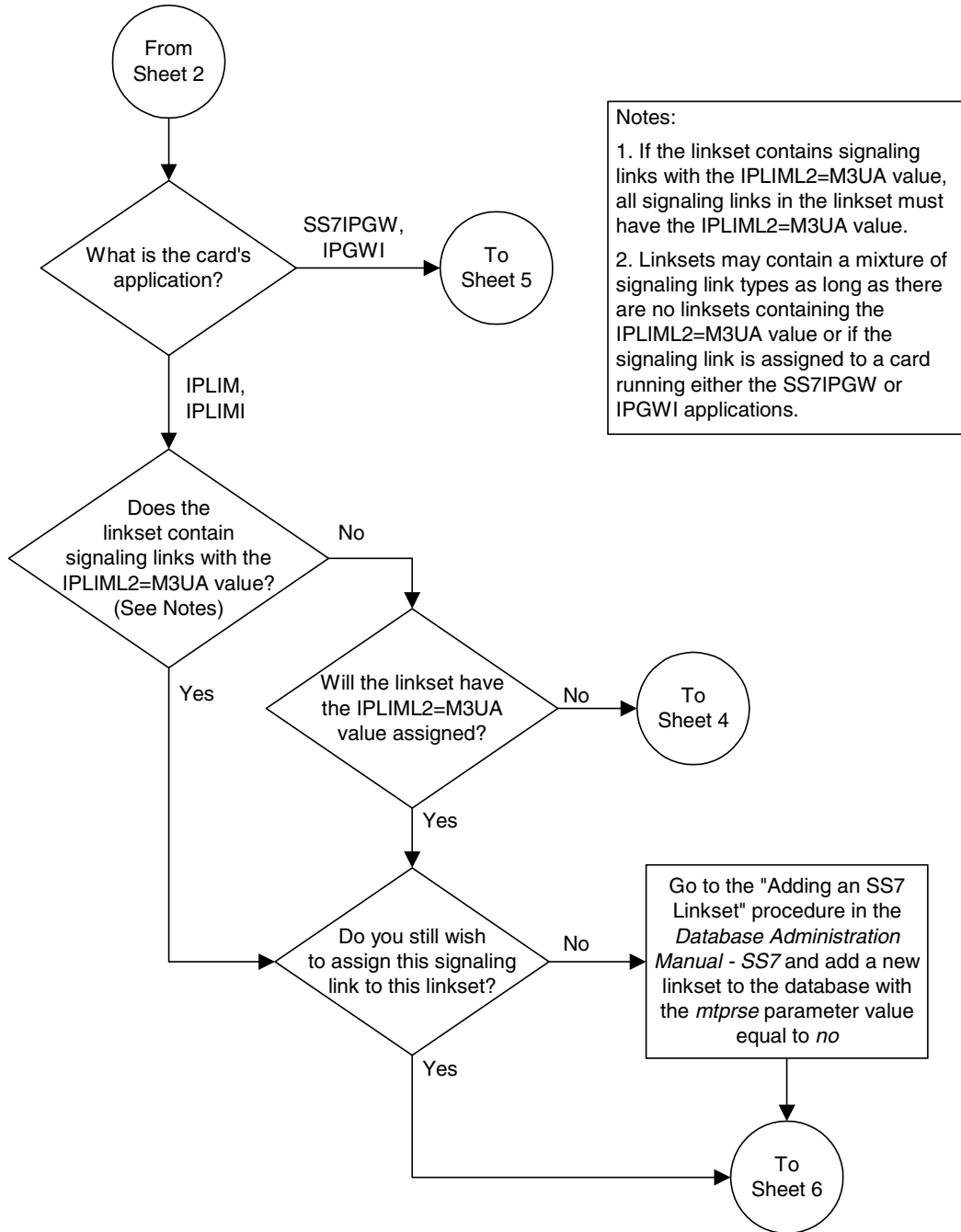
Flowchart 3-5. Adding an IP Signaling Link (Sheet 1 of 7)



Flowchart 3-5. Adding an IP Signaling Link (Sheet 2 of 7)



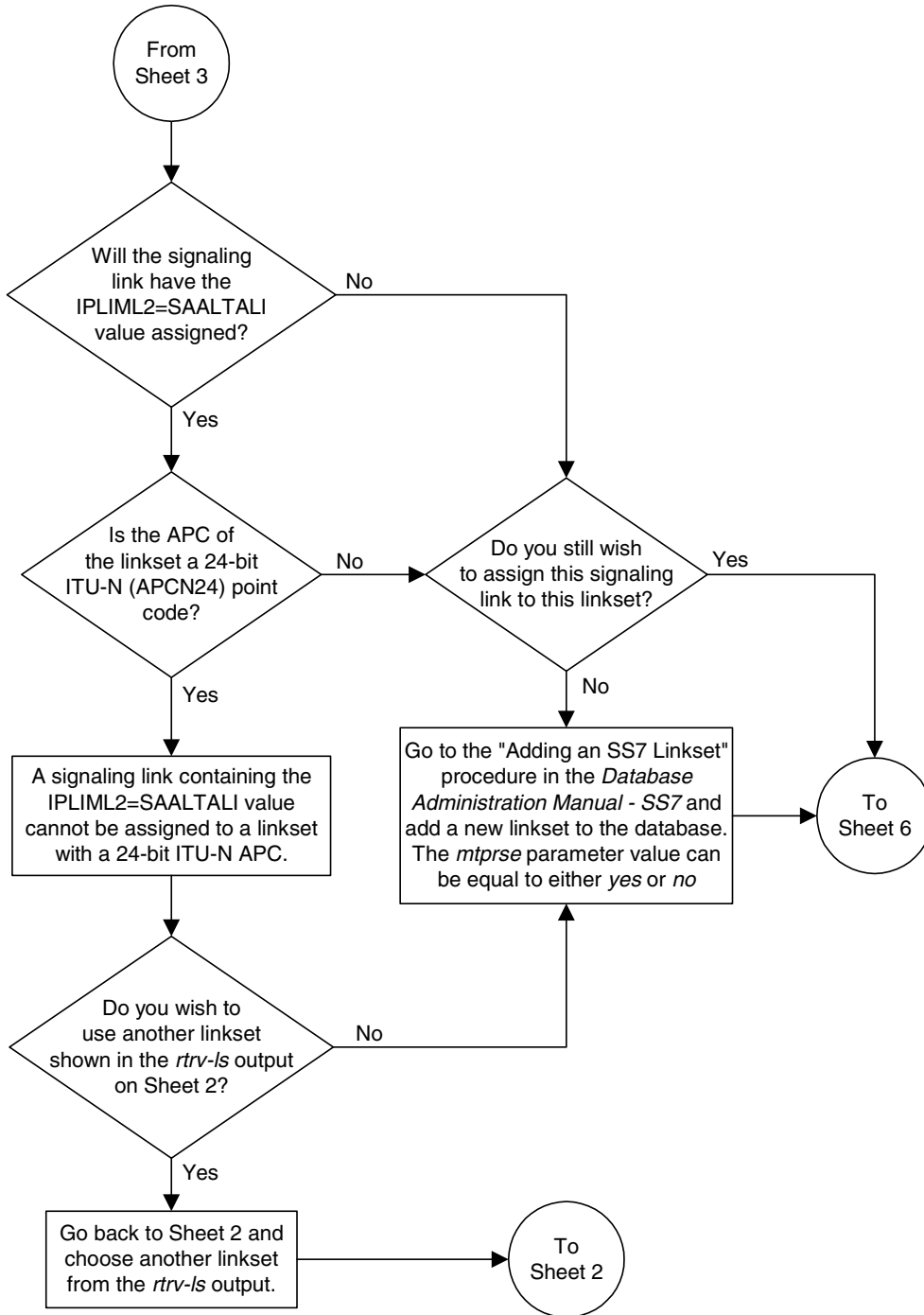
Flowchart 3-5. Adding an IP Signaling Link (Sheet 3 of 7)



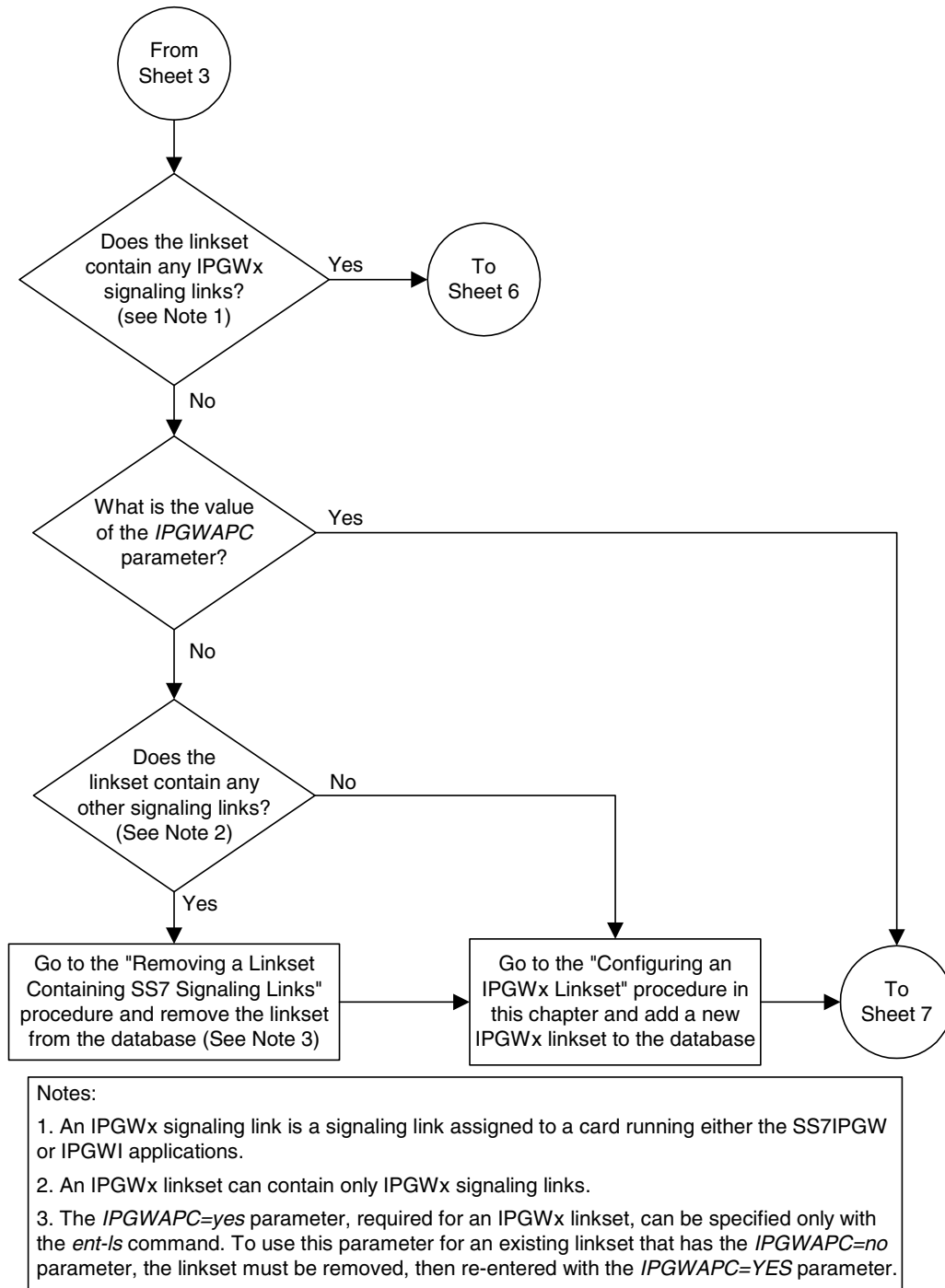
Notes:

1. If the linkset contains signaling links with the IPLIML2=M3UA value, all signaling links in the linkset must have the IPLIML2=M3UA value.
2. Linksets may contain a mixture of signaling link types as long as there are no linksets containing the IPLIML2=M3UA value or if the signaling link is assigned to a card running either the SS7IPGW or IPGWI applications.

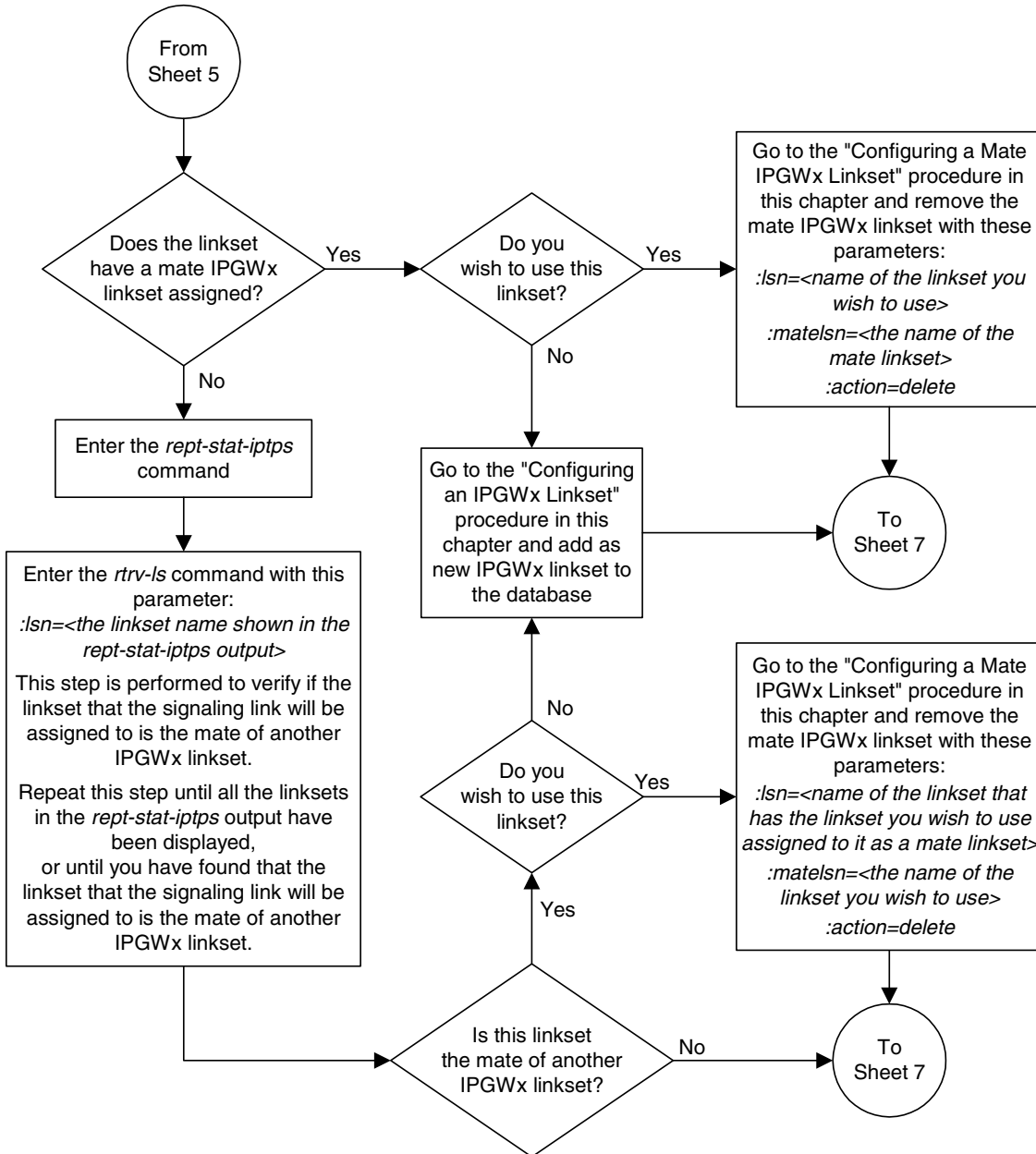
Flowchart 3-5. Adding an IP Signaling Link (Sheet 4 of 7)



Flowchart 3-5. Adding an IP Signaling Link (Sheet 5 of 7)



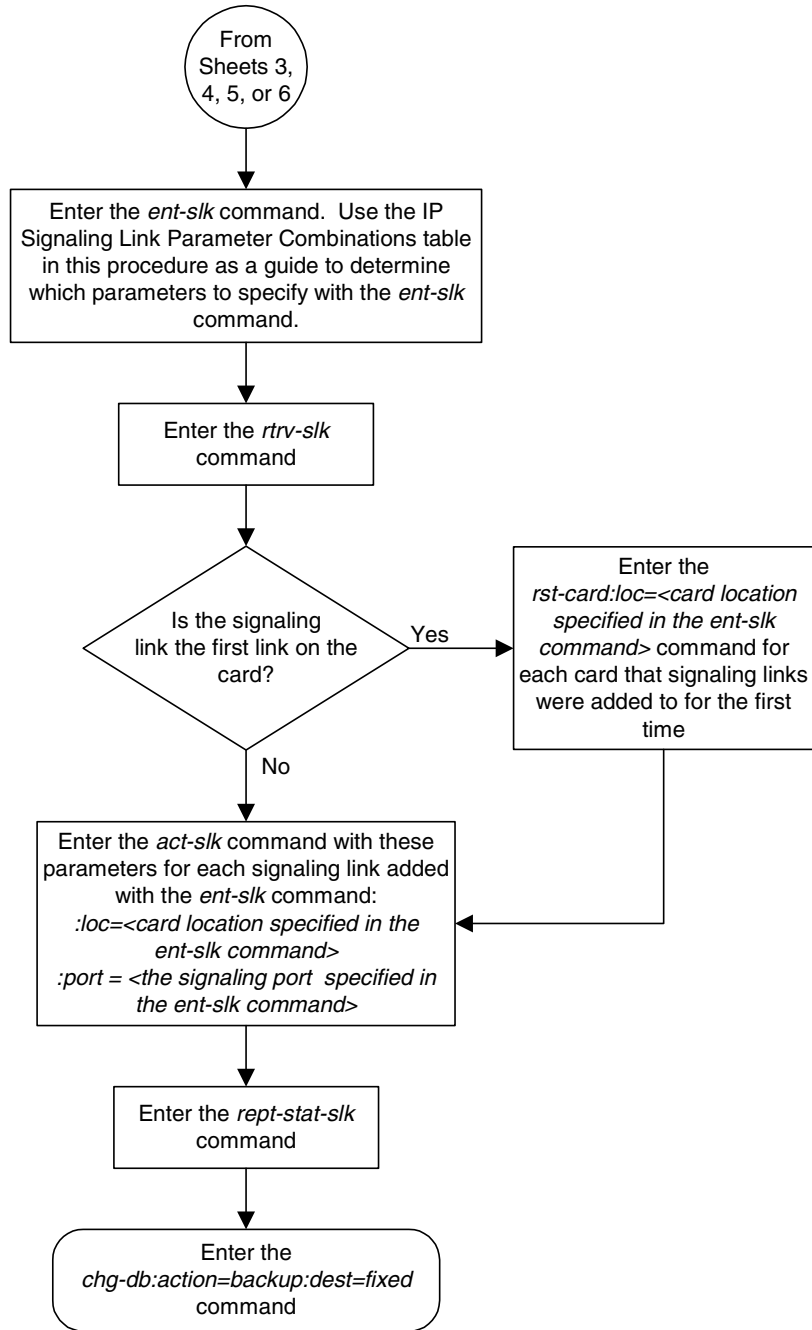
Flowchart 3-5. Adding an IP Signaling Link (Sheet 6 of 7)



Notes:

1. An IPGWx linkset can contain only one IPGWx signaling link if the IPGWx linkset has a mate IPGWx linkset assigned to it, or is the mate to an IPGWx linkset.
2. If the IPGWx linkset is not the mate to another IPGWx linkset, or does not have a mate IPGWx linkset assigned, the IPGWx linkset can contain up to 8 IPGWx signaling links.

Flowchart 3-5. Adding an IP Signaling Link (Sheet 7 of 7)



Enabling the Large System # Links Controlled Feature

This procedure is used to enable the Large System # Links controlled feature using the feature's part number and a feature access key.

The feature access key for the Large System # Links controlled feature is based on the feature's part number and the serial number of the system, making the feature access key site-specific.

This feature allows the system to contain up to 1500 signaling links. The part number for this feature is 893-0059-01.

The **enable-ctrl-feat** command enables the controlled feature by inputting the controlled feature's access key and the controlled feature's part number with these parameters:

: fak – The feature access key generated by Tekelec's feature access key generator, and supplied to you when you purchase or temporarily try a controlled feature. The feature access key contains 13 alphanumeric characters and is not case sensitive.

: partnum – The Tekelec-issued part number associated with the controlled feature. The part number is a 9-digit number, not including dashes; the first three digits must be 893 (that is, 893xxxxxx, where x is a numeric value).

The **enable-ctrl-feat** command requires that the database contain a valid serial number for the system, and that this serial number is locked. This can be verified with the **rtrv-serial-num** command. The system is shipped with a serial number in the database, but the serial number is not locked. The serial number can be changed, if necessary, and locked once the system is on-site, by using the **ent-serial-num** command. The **ent-serial-num** command uses these parameters.

: serial – The serial number assigned to the system. The serial number is not case sensitive.

: lock – Specifies whether or not the serial number is locked. This parameter has only one value, **yes**, which locks the serial number. Once the serial number is locked, it cannot be changed.

NOTE: To enter and lock the system's serial number, the **ent-serial-num** command must be entered twice, once to add the correct serial number to the database with the **serial** parameter, then again with the **serial** and the **lock=yes** parameters to lock the serial number. You should verify that the serial number in the database is correct before locking the serial number. The serial number can be found on a label affixed to the control shelf (shelf 1100).

This feature cannot be temporarily enabled (with the temporary feature access key).

Once this feature is enabled with the `enable-ctrl-feat` command, the feature is also activated. The `chg-ctrl-feat` command is not necessary to activate the feature.

This feature cannot be disabled with the `chg-ctrl-feat` command and the `status=off` parameter.

Procedure

1. Display the status of the Large System # Links controlled feature by entering the `rtrv-ctrl-feat` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.6.0
The following features have been permanently enabled:
```

Feature Name	Partnum	Status	Quantity
IPGWx Signaling TPS	893012814	on	20000
ISUP Normalization	893000201	on	----
Command Class Management	893005801	on	----
LNP Short Message Service	893006601	on	----
Intermed GTT Load Sharing	893006901	on	----
XGTT Table Expansion	893006101	on	400000
XMAP Table Expansion	893007710	off	----
Routesets	893006401	on	6000

The following features have been temporarily enabled:

Feature Name	Partnum	Status	Quantity	Trial Period Left
Zero entries found.				

The following features have expired temporary keys:

Feature Name	Partnum
Zero entries found.	

If the `rtrv-ctrl-feat` output shows that the controlled feature is permanently enabled for the desired quantity or for a quantity that is greater than the desired quantity, no further action is necessary. This procedure does not need to be performed.

NOTE: If the `rtrv-ctrl-feat` output in step 1 shows any controlled features, or if the Large System # Links controlled feature is enabled for a quantity that is less than the desired quantity, skip steps 2 through 5, and go to step 6.

2. Display the serial number in the database with the `rtrv-serial-num` command. This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.6.0
System serial number = nt00001231
```

System serial number is not locked.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.6.0
Command Completed
```

NOTE: If the serial number is correct and locked, skip steps 3, 4, and 5, and go to step 6. If the serial number is correct but not locked, skip steps 3 and 4, and go to step 5. If the serial number is not correct, but is locked, this feature cannot be enabled and the remainder of this procedure cannot be performed. Contact Tekelec Technical Services to get an incorrect and locked serial number changed. See “Tekelec Technical Services” on page 1-8. The serial number can be found on a label affixed to the control shelf (shelf 1100).

3. Enter the correct serial number into the database using the `ent-serial-num` command with the `serial` parameter.

For this example, enter this command.

```
ent-serial-num:serial=<system's correct serial number>
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.6.0
ENT-SERIAL-NUM:  MASP A - COMPLTD
```

4. Verify that the serial number entered into step 3 was entered correctly using the `rtrv-serial-num` command. This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.6.0
System serial number = nt00001231
```

System serial number is not locked.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.6.0
Command Completed
```

If the serial number was not entered correctly, repeat steps 3 and 4 and re-enter the correct serial number.

5. Lock the serial number in the database by entering the `ent-serial-num` command with the serial number shown in step 2, if the serial number shown in step 2 is correct, or with the serial number shown in step 4, if the serial number was changed in step 3, and with the `lock=yes` parameter.

For this example, enter this command.

```
ent-serial-num:serial=<system's serial number>:lock=yes
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.6.0
ENT-SERIAL-NUM:  MASP A - COMPLTD
```

6. Enable the Large System # Links controlled feature for the desired quantity with the **enable-ctrl-feat** command specifying the part number corresponding to the new quantity of signaling links and the feature access key. To increase the number of signaling links the system can contain to 1500, enter this command.

```
enable-ctrl-feat:partnum=893005901:fak=<feature access key>
```

NOTE: A temporary feature access key cannot be specified to enable this feature.

NOTE: The values for the feature access key (the **fak** parameter) are provided by Tekelec. If you do not have the controlled feature part number or the feature access key for the feature you wish to enable, contact your Tekelec Sales Representative or Account Representative.

When the **enable-crtl-feat** command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.6.0
ENABLE-CTRL-FEAT: MASP B - COMPLTD
```

7. Verify the changes by entering the **rtrv-ctrl-feat** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.6.0
The following features have been permanently enabled:
```

Feature Name	Partnum	Status	Quantity
IPGWx Signaling TPS	893012814	on	20000
ISUP Normalization	893000201	on	----
Command Class Management	893005801	on	----
LNP Short Message Service	893006601	on	----
Intermed GTT Load Sharing	893006901	on	----
XGTT Table Expansion	893006101	on	4000000
XMAP Table Expansion	893007710	on	3000
Large System # Links	893005901	on	1500
Routesets	893006401	on	6000

The following features have been temporarily enabled:

Feature Name	Partnum	Status	Quantity	Trial Period Left
Zero entries found.				

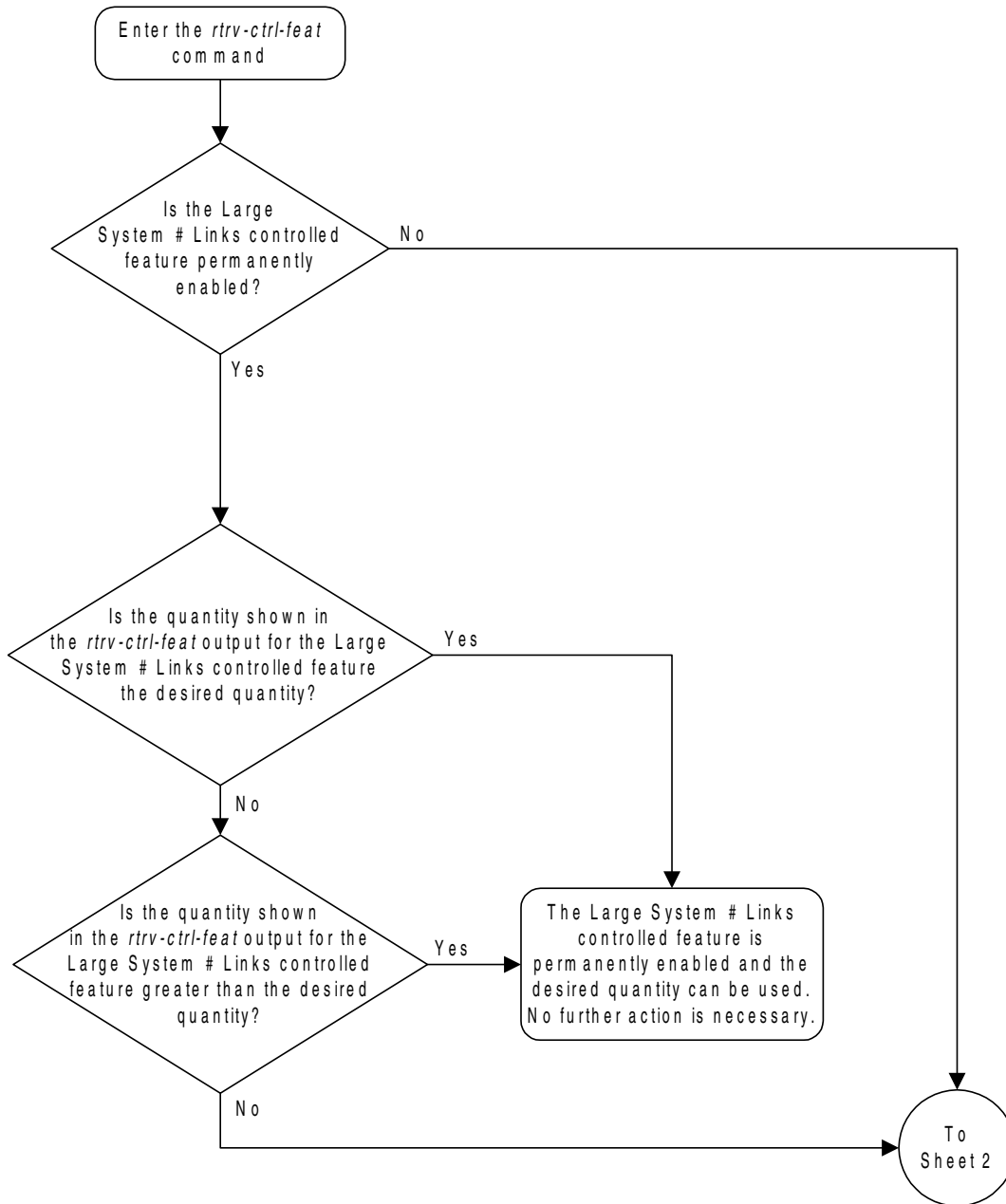
The following features have expired temporary keys:

Feature Name	Partnum
Zero entries found.	

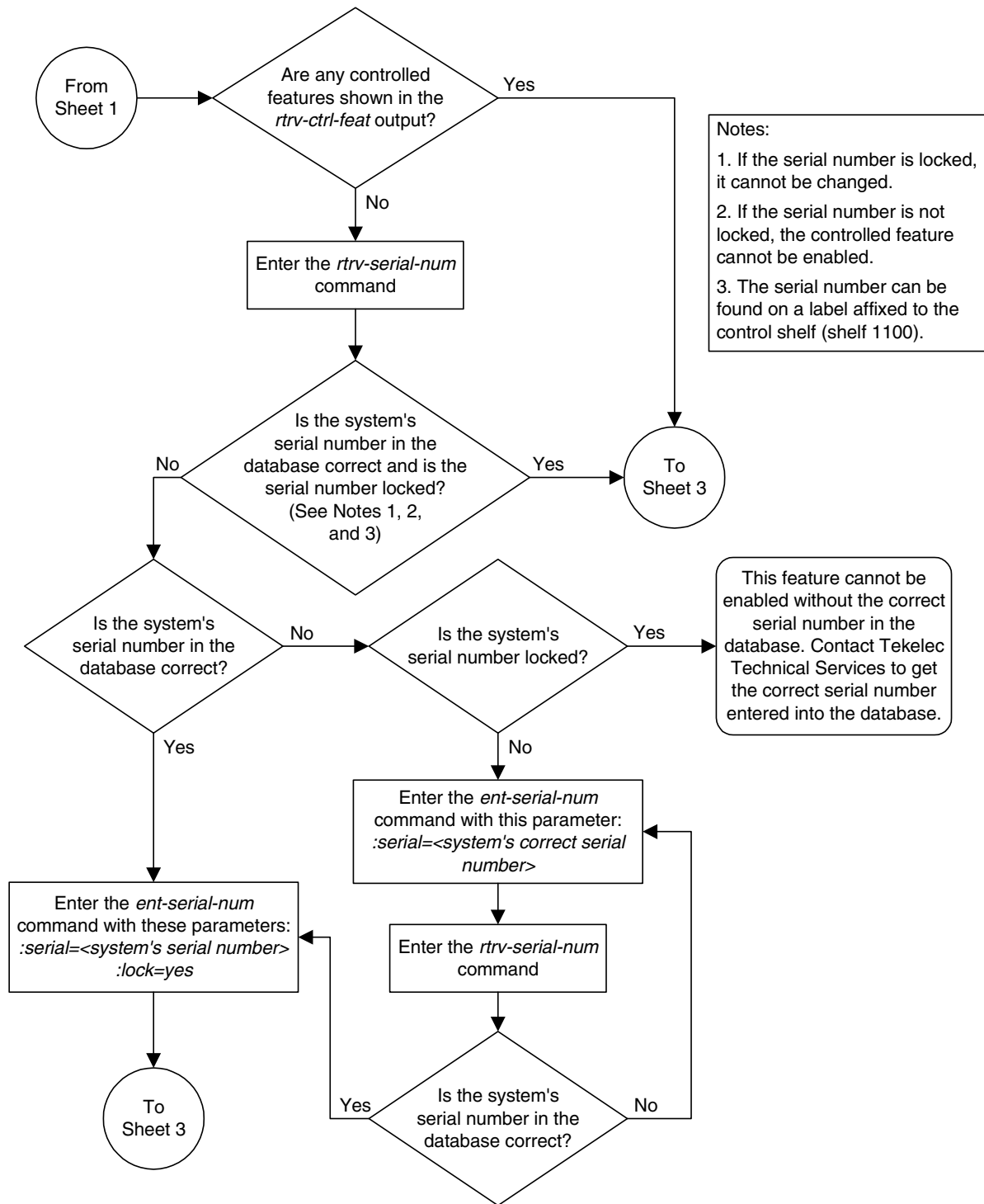
8. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

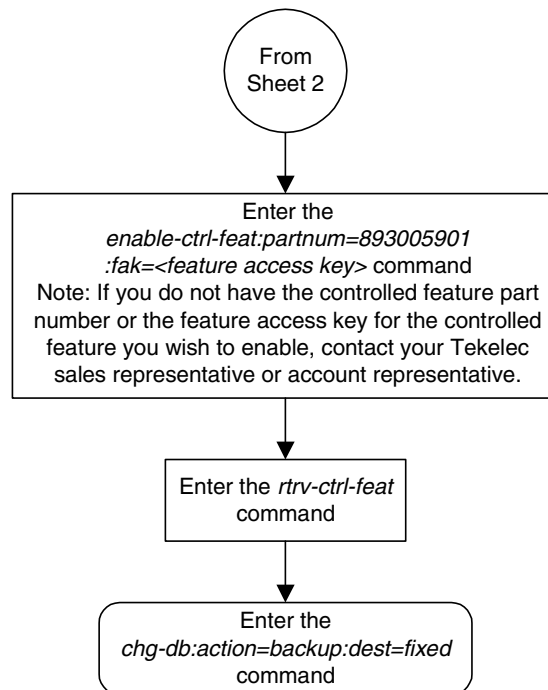
Flowchart 3-6. Enabling the Large System # Links Controlled Feature (Sheet 1 of 3)



Flowchart 3-6. Enabling the Large System # Links Controlled Feature
(Sheet 2 of 3)



Flowchart 3-6. Enabling the Large System # Links Controlled Feature
(Sheet 3 of 3)



Removing an IP Signaling Link

This procedure is used to remove an IP signaling link from the database using the `dlt-slk` command. The `dlt-slk` command uses these parameters.

- `:loc` – The card location of the IP card that the IP signaling link is assigned to.
- `:port` – The port on the card location specified in the `loc` parameter.
- `:force` – This parameter must be used to remove the last link in a linkset without having to remove all of the routes that referenced the linkset.

The `tfatcabmlq` parameter (TFA/TCA Broadcast Minimum Link Quantity), assigned to linksets, shows the minimum number of links in the given linkset (or in the combined link set in which it resides) that must be available for traffic. When the number of signaling links in the specified linkset is equal to or greater than the value of the `tfatcabmlq` parameter, the status of the routes that use the specified linkset is set to allowed and can carry traffic. Otherwise, these routes are restricted. The value of the `tfatcabmlq` parameter cannot exceed the total number of signaling links contained in the linkset.

The `dlt-slk` command makes sure that the number of signaling links assigned to a linkset is greater than or equal to the value of the `tfatcabmlq` parameter. If the number of signaling links associated with a linkset drops below the value of the `tfatcabmlq` parameter for that linkset, the `tfatcabmlq` value for that linkset is automatically decremented. The value of the `tfatcabmlq` parameter for a specified linkset can be verified using the `rtrv-ls:lsn=<linkset name>` command specifying the name of the linkset. The `tfatcabmlq` parameter value is shown in the `tfatcabmlq` field of the `rtrv-ls` command output.

Canceling the RTRV-SLK Command

Because the `rtrv-slk` command used in this procedure can output information for a long period of time, the `rtrv-slk` command can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-slk` command can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-slk` command was entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-slk` command was entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-slk` command was entered, from another terminal other than the terminal where the `rtrv-slk` command was entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current link configuration using the `rtrv-slk` command. This is an example of the possible output.

```

rlghncxa03w 04-12-19 21:16:37 GMT EAGLES5 31.6.0

LOC  PORT  LSN          SLC TYPE      L2T          L1          PCR  PCR
      SET  BPS      MODE TSET    ECM  N1  N2
1201  A    ls01          0  LIMDS0      1  56000  --- ---  BASIC ---  -----
1201  B    lsa1          0  LIMDS0      1  56000  --- ---  BASIC ---  -----
1202  B    ls02          0  LIMV35      2  64000  DTE ---  BASIC ---  -----
1203  A    ls03          0  LIMDS0      3  56000  --- ---  BASIC ---  -----
1203  B    lsa2          0  LIMDS0      1  56000  --- ---  BASIC ---  -----
1204  B    ls01          1  LIMDS0      1  56000  --- ---  BASIC ---  -----
1205  A    lsa3          0  LIMV35      4  64000  DCE ON   BASIC ---  -----
1206  A    ls02          1  LIMV35      2  64000  DTE ---  BASIC ---  -----
1207  A    lsn1207a     0  LIMDS0      1  56000  --- ---  BASIC ---  -----
1207  B    lsn1207b     0  LIMDS0      1  56000  --- ---  BASIC ---  -----
1208  B    ls03          1  LIMDS0      3  56000  --- ---  BASIC ---  -----
1212  A    ls04          0  LIMV35      4  64000  DTE ---  BASIC ---  -----
1213  B    ls05          0  LIMDS0      5  56000  --- ---  BASIC ---  -----
1214  A    lsn1214a     0  LIMV35      2  64000  DTE ---  PCR  76  3800
1214  B    lsa3          1  LIMV35      4  64000  DCE ON   BASIC ---  -----
1215  A    ls05          1  LIMDS0      5  56000  --- ---  BASIC ---  -----
1301  B    ls06          0  LIMV35      6  56000  DTE ---  BASIC ---  -----
1304  B    ls06          1  LIMV35      6  56000  DTE ---  BASIC ---  -----
1308  A    ls06          2  LIMV35      6  56000  DTE ---  BASIC ---  -----
1311  A    ls01          2  LIMDS0      1  56000  --- ---  BASIC ---  -----
1311  A1   ls05          2  LIMDS0      5  56000  --- ---  BASIC ---  -----
1311  B    ls03          2  LIMDS0      3  56000  --- ---  BASIC ---  -----
1311  B1   ls07          1  LIMDS0      7  56000  --- ---  BASIC ---  -----
1313  A    ls07          0  LIMDS0      7  56000  --- ---  BASIC ---  -----
1315  A    lsn5          0  LIMV35     11  64000  DTE OFF  BASIC ---  -----
1317  A    lsi7          0  LIMV35     11  64000  DTE OFF  BASIC ---  -----

LOC  PORT  LSN          SLC TYPE      LP          ATM          VCI  VPI  LL
      SET  BPS      TSEL
1302  A    atmansi0     0  LIMATM      3  1544000  EXTERNAL  35  15  0
1305  A    atmansi1     0  LIMATM      4  1544000  INTERNAL  100 20  2
1318  A    atmansi0     1  LIMATM      9  1544000  LINE      150 25  4

LOC  PORT  LSN          SLC TYPE      LP          ATM          VCI  VPI  CRC4  SI  SN
      SET  BPS      TSEL
2101  A    atmitu1     0  LIME1ATM    5  2.048M  LINE      150  2  ON    1  20
2105  A    atmitu1     1  LIME1ATM    5  2.048M  LINE      35  15  ON    2  15

LOC  PORT  LSN          SLC TYPE      IPLIML2
2202  A    lsnlp1      0  IPLIM      SAALTALI
2205  A    lsnip1      1  IPLIM      M2PA
2204  B    lsnlp2      0  IPLIM      M3UA
2213  A    lsnip5      0  IPLIMI     M2PA
2215  A    lsnlp2      1  IPLIM      M3UA

LOC  PORT  LSN          SLC TYPE
2207  A    lsnlp3      0  SS7IPGW
2211  A    lsnlp4      0  IPGWI

LOC  PORT  LSN          SLC TYPE      L2T          PCR  PCR  E1  E1
      SET  BPS      MODE N1  N2  LOC PORT TS
No Links Set Up.

```

```

LOC   PORT LSN           SLC TYPE           L2T           PCR   PCR   T1   T1
      SET  BPS           ECM   N1    N2    LOC  PORT TS
No Links Set Up.
SLK table is (31 of 500) 6% full

```

2. Any in-service IP connections on the signaling link being removed in this procedure must be placed out of service. Have the far-end node for the signaling link being removed perform these actions:

- Place the TALI sockets in the NEA-FEP state.
 - Place the M3UA or SUA associations in either the ASP-INACTIVE or ASP-DOWN state.
-

3. Display the IP link associated with the signaling link being removed the database by entering the **rtrv-ip-lnk** command with the location and port of the signaling link. For this example, enter these commands.

```
rtrv-ip-lnk:loc=2202:port=a
```

The following is an example of the possible output.

```

rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.6.0
LOC   PORT IPADDR           SUBMASK           DUPLEX SPEED MACTYPE AUTO
2202  A    192.003.001.010  255.255.255.128  HALF   10    802.3  NO

```

```
rtrv-ip-lnk:loc=2204:port=a
```

The following is an example of the possible output.

```

rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.6.0
LOC   PORT IPADDR           SUBMASK           DUPLEX SPEED MACTYPE AUTO
2204  A    192.001.001.010  255.255.255.128  HALF   10    802.3  NO

```

4. Display the IP host information associated with the IP link by entering the **rtrv-ip-host** command with the IP address shown in step 3. For this example, enter these commands.

```
rtrv-ip-host:ipaddr=192.001.001.010
```

The following is an example of the possible output.

```

rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.6.0
IPADDR           HOST
192.1.1.10       IPNODE1_2204
IP Host table is (10 of 512) 2% full

```

```
rtrv-ip-host:ipaddr=192.003.001.010
```

The following is an example of the possible output.

```

rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.6.0
IPADDR           HOST
192.3.1.10       IPNODE1_2202
IP Host table is (10 of 512) 2% full

```

5. Display the socket associated with the local host name shown in step 4 by entering the `rtrv-appl-sock` command. For this example, enter these commands.

```
rtrv-appl-sock:localhost=ipnode1_2202
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.6.0
SNAME KC_HLR1_2202
  LINK      A
  LHOST     IPNODE1_2202
  RHOST     KC_HLR2
  LPORT     7000          RPORT      7001
  SERVER    YES          DCMP5      1
  REXMIT    FIXED       RTT        60
  OPEN      YES          ALW        YES
```

```
IP Appl Sock/Assoc table is (4 of 4000) 1% full
```

```
rtrv-appl-sock:localhost=ipnode1_2204
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.6.0
```

```
IP Appl Sock/Assoc table is (4 of 4000) 1% full
```

NOTE: If the specified socket name is not in the database, the `rtrv-appl-sock` output shows no socket information as show above.

NOTE: If there is no socket shown in step 5, or the `open` and `alw` parameter values of the socket shown in step 5 are `no`, skip this step and go to step 7.

6. Change the `open` and `alw` parameter values in the socket shown in step 5 using the `chg-appl-sock` command with the `open=no` and `alw=no` parameters, as necessary.

For example, enter this command.

```
chg-appl-sock:sname=kc_hlr1_2202:open=no:alw=no
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.6.0
CHG-APPL-SOCK: MASP A - COMPLTD
```

7. Display the association associated with the local host name shown in step 5 that was not assigned to a socket by entering the `rtrv-assoc` command. For this example, enter this command.

```
rtrv-assoc:localhost=ipnode1_2204
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.6.0
ANAME ASSOC1
  PORT      A
  ADAPTER   M3UA          VER          M3UA RFC
```

```
LHOST      IPNODE1_2204
ALHOST     ---
RHOST      GW100.NC.TEKELEC.COM
LPORT      1030          RPORT      1030
ISTRMS     2            OSTRMS     2
RMODE      LIN          RMIN       120          RMAX       800
RTIMES     10          CWMIN      3000
OPEN       YES         ALW        YES
```

IP Appl Sock/Assoc table is (4 of 4000) 1% full

NOTE: If there is no association shown in step 7, or the `open` and `alw` parameter values of the association shown in step 7 are `no`, skip this step and go to step 9.

8. Change the value of the `open` and `alw` parameters to `no` by specifying the `chg-assoc` command with the `open=no` and `alw=no` parameters, as necessary. For this example, enter this command.

```
chg-assoc:aname=assoc1:open=no:alw=no
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.6.0
CHG-ASSOC: MASP A - COMPLTD;
```

9. Deactivate the link to be removed using the `dact-slk` command, using the output from step 1 to obtain the card location and port information of the signaling link to be removed. For this example, enter these commands.

```
dact-slk:loc=2202:port=a
```

```
dact-slk:loc=2204:port=a
```

When each of these command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-07 08:41:12 GMT EAGLE5 31.6.0
Deactivate Link message sent to card
```

10. Verify that the link is out of service - maintenance disabled (OOS-MT-DSBLD) using the `rept-stat-slk` command with the card location and port containing the signaling link. For this example, enter these commands.

```
rept-stat-slk:loc=2202:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-23 13:06:25 GMT EAGLE5 31.6.0
SLK      LSN      CLLI      PST      SST      AST
2202,A   ls05      ls05clli  OOS-MT   Unavail  ----
ALARM STATUS      = *    0235 REPT-LNK-MGTINH: local inhibited
UNAVAIL REASON    = LI
```

```
rept-stat-slk:loc=2204:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-23 13:06:25 GMT EAGLE5 31.6.0
SLK      LSN      CLLI      PST      SST      AST
2204,A   ls04      ls04clli  OOS-MT   Unavail  ----
ALARM STATUS      = *    0235 REPT-LNK-MGTINH: local inhibited
UNAVAIL REASON    = LI
```

11. If the signaling link to be removed is the last signaling link on a card, the card must be inhibited before the signaling link is removed. Before entering the **dlt-slk** command, enter the **rmv-card** command and specify the location of the card to be inhibited. The card location is shown in the output of **rept-stat-slk** command executed in step 10. If the signaling link to be removed is not the last signaling link on the card, go to step 12.

In the example used for this procedure, the signaling link is the last signaling link on the card and must be inhibited. Enter these commands.

```
rmv-card:loc=2202
```

```
rmv-card:loc=2204
```

When each of these command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-07 08:41:12 GMT EAGLE5 31.6.0
Card has been inhibited.
```

12. Remove the signaling link from the system using the **dlt-slk** command. If there is only one signaling link in the linkset, the **force=yes** parameter must be specified to remove the signaling link.

In the example used in this procedure, the signaling link is the last signaling link in the linkset. Enter these commands.

```
dlt-slk:loc=2202:port=a:force=yes
```

```
dlt-slk:loc=2204:port=a:force=yes
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-07 08:41:17 GMT EAGLE5 31.6.0
DLT-SLK: MASP A - COMPLTD
```

13. Verify the changes using the **rtrv-slk** command. This is an example of the possible output.

```
rlghncxa03w 04-12-19 21:16:37 GMT EAGLE5 31.6.0
```

LOC	PORT	LSN	SLC	TYPE	SET	BPS	L2T	L1	TSET	ECM	PCR	PCR
								MODE			N1	N2
1201	A	ls01	0	LIMDS0	1	56000		---	---	BASIC	---	-----
1201	B	lsa1	0	LIMDS0	1	56000		---	---	BASIC	---	-----
1202	B	ls02	0	LIMV35	2	64000		DTE	---	BASIC	---	-----
1203	A	ls03	0	LIMDS0	3	56000		---	---	BASIC	---	-----
1203	B	lsa2	0	LIMDS0	1	56000		---	---	BASIC	---	-----
1204	B	ls01	1	LIMDS0	1	56000		---	---	BASIC	---	-----
1205	A	lsa3	0	LIMV35	4	64000		DCE	ON	BASIC	---	-----
1206	A	ls02	1	LIMV35	2	64000		DTE	---	BASIC	---	-----
1207	A	lsn1207a	0	LIMDS0	1	56000		---	---	BASIC	---	-----
1207	B	lsn1207b	0	LIMDS0	1	56000		---	---	BASIC	---	-----
1208	B	ls03	1	LIMDS0	3	56000		---	---	BASIC	---	-----
1213	B	ls05	0	LIMDS0	5	56000		---	---	BASIC	---	-----
1214	A	lsn1214a	0	LIMV35	2	64000		DTE	---	PCR	76	3800
1214	B	lsa3	1	LIMV35	4	64000		DCE	ON	BASIC	---	-----
1215	A	ls05	1	LIMDS0	5	56000		---	---	BASIC	---	-----
1301	B	ls06	0	LIMV35	6	56000		DTE	---	BASIC	---	-----
1304	B	ls06	1	LIMV35	6	56000		DTE	---	BASIC	---	-----
1308	A	ls06	2	LIMV35	6	56000		DTE	---	BASIC	---	-----

IP7 Secure Gateway Configuration Procedures

```

1311 A   ls01      2  LIMDS0  1  56000  --- ---  BASIC --- -----
1311 A1  ls05      2  LIMDS0  5  56000  --- ---  BASIC --- -----
1311 B   ls03      2  LIMDS0  3  56000  --- ---  BASIC --- -----
1311 B1  ls07      1  LIMDS0  7  56000  --- ---  BASIC --- -----
1313 A   ls07      0  LIMDS0  7  56000  --- ---  BASIC --- -----
1315 A   lsn5      0  LIMV35 11  64000  DTE OFF  BASIC --- -----
1317 A   lsi7      0  LIMV35 11  64000  DTE OFF  BASIC --- -----

```

```

LOC  PORT LSN          SLC TYPE      LP          ATM
      SET BPS      TSEL          VCI  VPI  LL
1302 A   atmansi0    0  LIMATM  3  1544000  EXTERNAL 35  15  0
1305 A   atmansi1    0  LIMATM  4  1544000  INTERNAL 100 20  2
1318 A   atmansi0    1  LIMATM  9  1544000  LINE      150 25  4

```

```

LOC  PORT LSN          SLC TYPE      LP          ATM          E1ATM
      SET BPS      TSEL          VCI  VPI  CRC4 SI SN
2101 A   atmitul1    0  LIME1ATM 5  2.048M  LINE      150  2  ON  1 20
2105 A   atmitul1    1  LIME1ATM 5  2.048M  LINE      35  15  ON  2 15

```

```

LOC  PORT LSN          SLC TYPE      IPLIML2
      SET BPS      M2PA
2205 A   lsnip1      1  IPLIM  M2PA
2213 A   lsnip5      0  IPLIMI M2PA
2215 A   lsnlp2      1  IPLIM  M3UA

```

```

LOC  PORT LSN          SLC TYPE
      SET BPS
2207 A   lsnlp3      0  SS7IPGW
2211 A   lsnlp4      0  IPGWI

```

```

LOC  PORT LSN          SLC TYPE      L2T          PCR PCR  E1  E1
      SET BPS      ECM  N1  N2  LOC PORT TS

```

No Links Set up.

```

LOC  PORT LSN          SLC TYPE      L2T          PCR PCR  T1  T1
      SET BPS      ECM  N1  N2  LOC PORT TS

```

No Links Set up.

SLK table is (31 of 500) 6% full

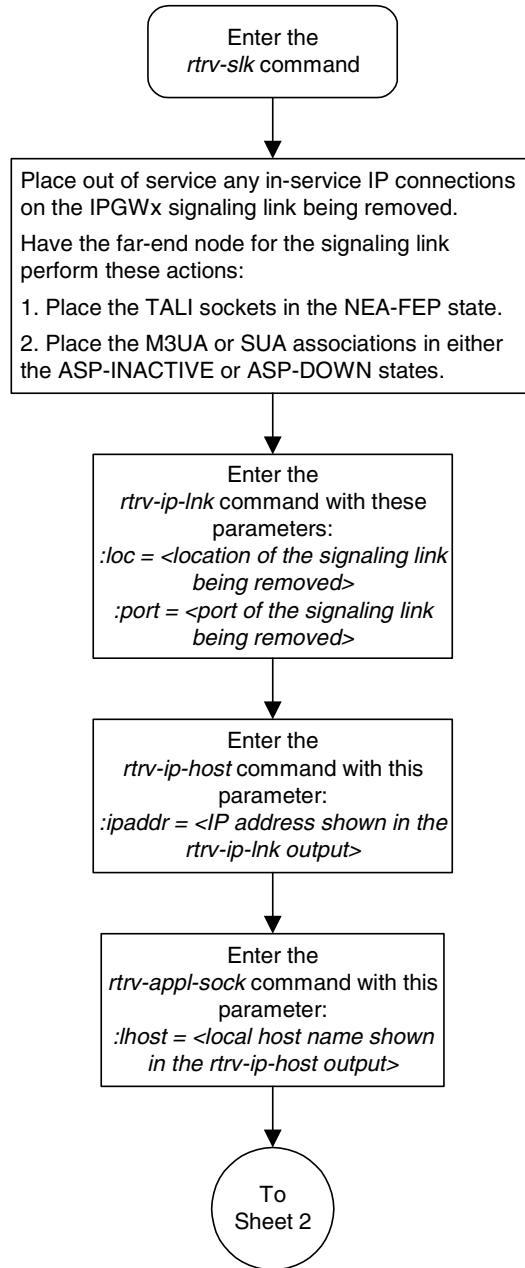
- Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```

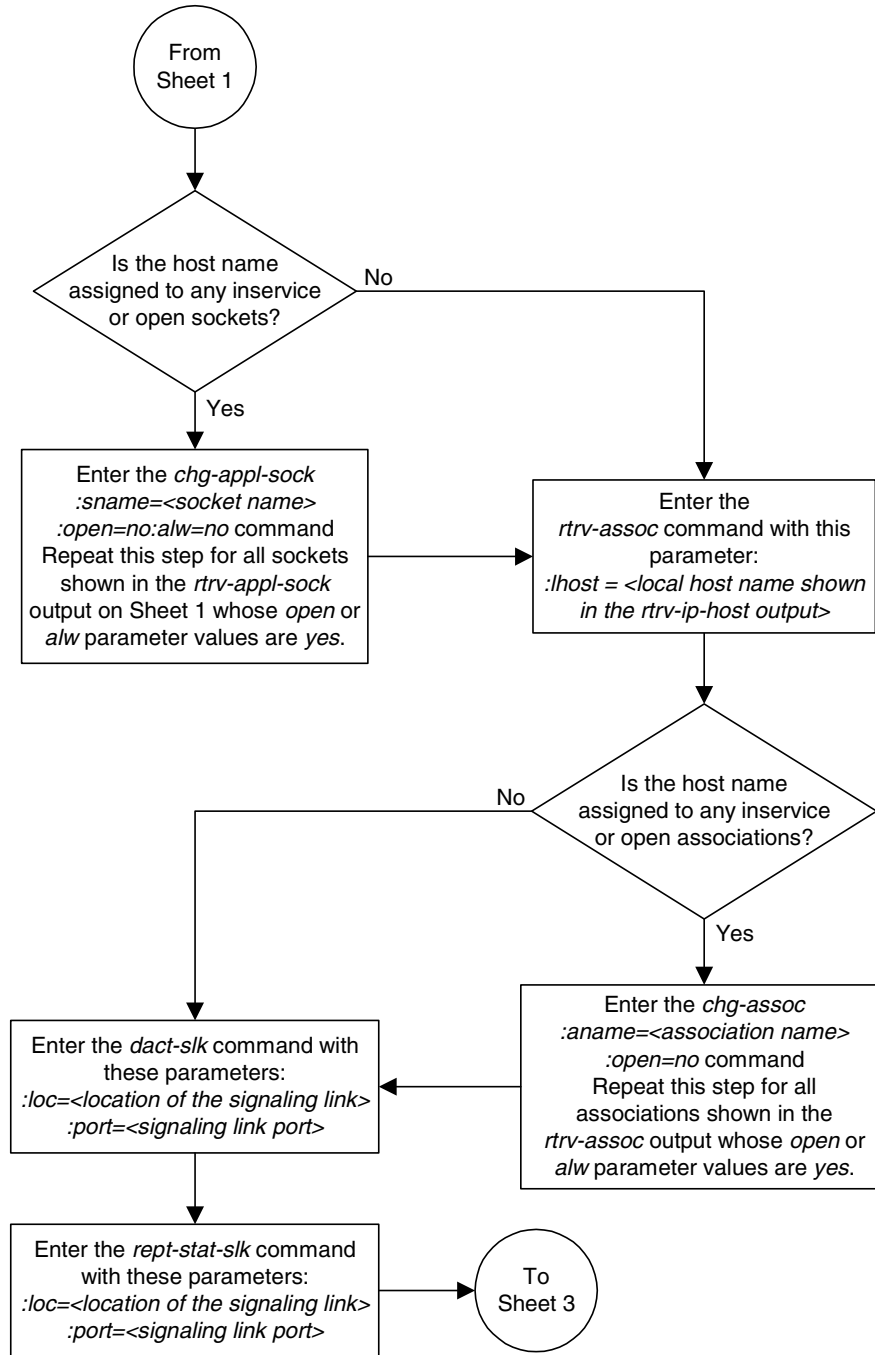
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.

```

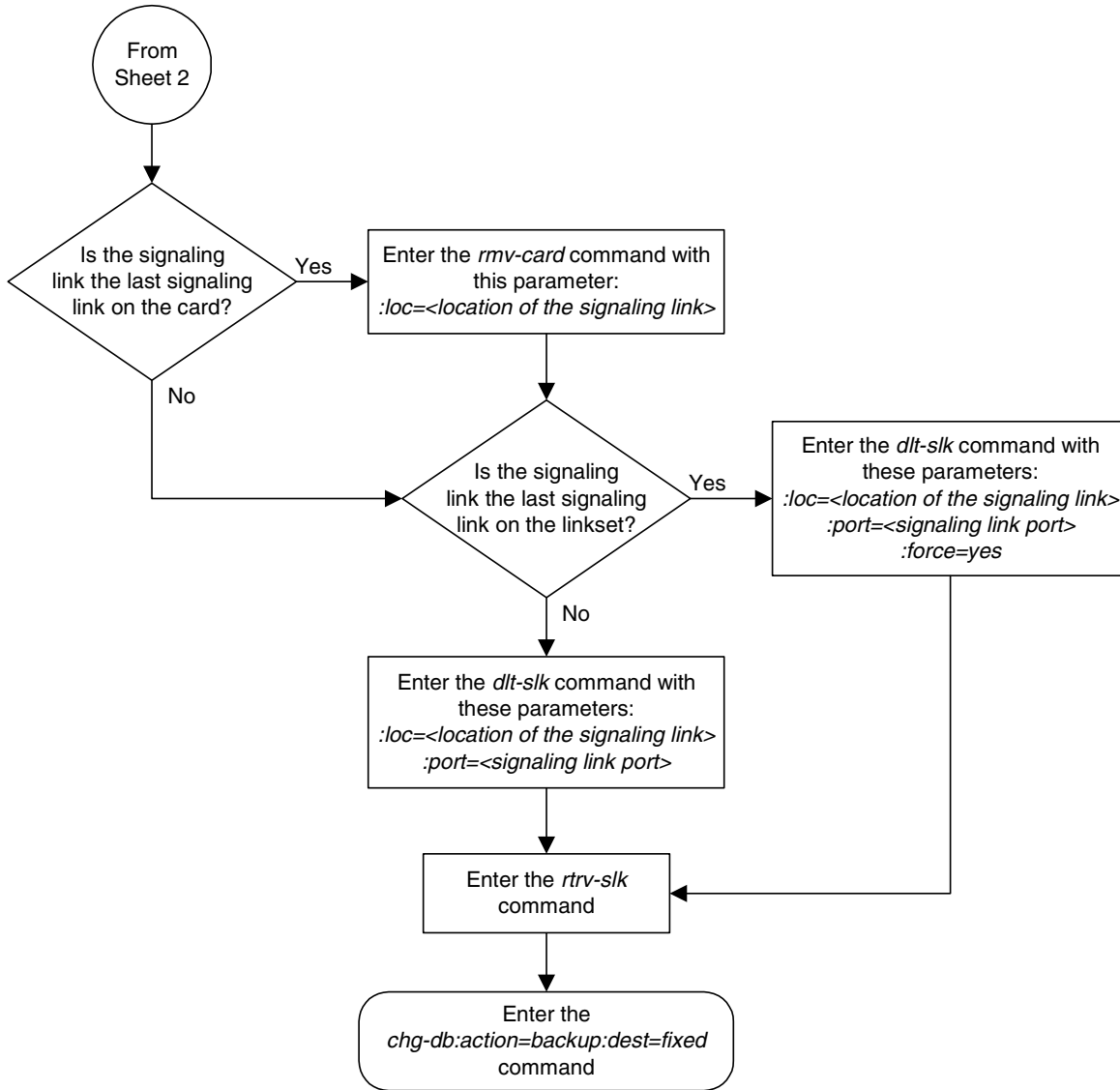
Flowchart 3-7. Removing an IP Signaling Link (Sheet 1 of 3)



Flowchart 3-7. Removing an IP Signaling Link (Sheet 2 of 3)



Flowchart 3-7. Removing an IP Signaling Link (Sheet 3 of 3)



Migrating IPLIMx M3UA Signaling Links to IPGWx M3UA Connections

To take advantage of the M3UA protocol generating application server notifications for IPGWx signaling links, this procedure describes how to migrate IPLIMx M3UA signaling links to IPGWx signaling links. The M3UA protocol does not generate application server notifications for IPLIMx signaling links.

An IPLIMx signaling link is a signaling link assigned to a card running either the IPLIM or IPLIMI applications. A linkset containing IPLIMx signaling links is an IPLIMx linkset.

An IPGWx signaling link is a signaling link assigned to a card running either the SS7IPGW or IPGWI applications. A linkset containing IPGWx signaling links is an IPGWx linkset.

To migrate IPLIMx signaling links to IPGWx signaling links, one IPLIMx signaling link in the linkset is removed. The IPLIMx card is removed from the database, and an IPGWx card is configured in the same card location. When the IPLIMx card is removed from the database, the IP card and IP link provisioning for that card is also removed from the database. The IP card and IP link provisioning is shown in the `rtrv-ip-card` and `rtrv-ip-lnk` command outputs. It is recommended to record the IP card and IP link provisioning information before removing the IPLIMx card from the database. This information will be provisioned for the IPGWx card after the IPGWx card is added to the database.

An IPGWx linkset is added to the database. An IPGWx signaling link, assigned to the IPGWx card added earlier, is added to the IPGWx linkset.

All routes using the IPLIMx linkset that was removed earlier are changed to use the IPGWx linkset. The relative cost value of these routes are not changed.

The IP card and IP link provisioning information for the IPLIMx card, recorded earlier, is provisioned for the IPGWx card using the `chg-ip-card` and the `chg-ip-lnk` commands.

The association and ASP that were used for the IPLIMx signaling link are not changed in this procedure and can continue to be used for the IPGWx signaling link. However, an association for an IPGWx signaling link must have the `port=a` parameter assigned to it. An IPGWx signaling link can only use port A. IPLIMx signaling links can use ports A through B3. If the `port` value for the association is anything but port A, the `port` value of the association must be changed to A.

An application server (AS) containing the IPGWx ASP is configured. The application server is assigned to an application routing key.

The IPGWx card and IPGWx signaling link are placed back into service.

Procedure

1. Display the current signaling link configuration using the `rtrv-slk` command. This is an example of the possible output.

```
rlghncxa03w 04-12-19 21:16:37 GMT EAGLE5 31.6.0
```

LOC	PORT	LSN	SLC	TYPE	SET	BPS	L2T	L1	MODE	TSET	ECM	PCR	N1	PCR	N2
1201	B	lsa1	0	LIMDS0	1	56000			---	---	BASIC	---			
1203	B	lsa2	0	LIMDS0	1	56000			---	---	BASIC	---			
1205	A	lsa3	0	LIMV35	3	64000		DCE	ON		BASIC	---			
1207	A	lsn1207a	0	LIMDS0	1	56000			---	---	BASIC	---			
1207	B	lsn1207b	0	LIMDS0	1	56000			---	---	BASIC	---			
1214	A	lsn1214a	0	LIMV35	2	64000		DTE	---		PCR	76	3800		
1214	B	lsa3	1	LIMV35	3	64000		DCE	ON		BASIC	---			

LOC	PORT	LSN	SLC	TYPE	LP	SET	BPS	ATM	TSEL	VCI	VPI	LL

LOC	PORT	LSN	SLC	TYPE	LP	SET	BPS	ATM	TSEL	VCI	VPI	CRC4	SI	SN

No Links Set up.

LOC	PORT	LSN	SLC	TYPE	IPLIML2
1203	A	e5e6a	0	IPLIM	M3UA
2204	B	e5e6a	1	IPLIM	M3UA
2215	A	e5e6a	2	IPLIM	M3UA

No Links Set up.

LOC	PORT	LSN	SLC	TYPE

No Links Set up.

LOC	PORT	LSN	SLC	TYPE	L2T	SET	BPS	ECM	PCR	N1	PCR	N2	E1	LOC	E1	PORT	TS

No Links Set up.

LOC	PORT	LSN	SLC	TYPE	L2T	SET	BPS	ECM	PCR	N1	PCR	N2	T1	LOC	T1	PORT	TS

No Links Set up.

SLK table is (7 of 500) 1% full.

M3UA IPLIMx signaling links are shown by the entry `M3UA` in the `IPLIML2` field of the `rtrv-slk` output. If no signaling links with this entry are shown in the `rtrv-slk` output, this procedure cannot be performed.

2. Choose one of the M3UA IPLIMx signaling links from step 1. Display the attributes of the card assigned to the M3UA IPLIMx signaling link by entering the **rtrv-ip-card** command and specifying the card location of the M3UA IPLIMx signaling link. For this example, enter this command.

rtrv-ip-card:loc=1203

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
  LOC 1203
    SRCHORDR LOCAL
    DNSA      150.1.1.1
    DNSB      -----
    DEFROUTER -----
    DOMAIN    -----
```

Record this information. This information will assigned to the IPGWx card in step 16 of this procedure

3. Display the IP link associated with the M3UA IPLIMx signaling link by entering the **rtrv-ip-lnk** command with the location of the signaling link. For this example, enter this command.

rtrv-ip-lnk:loc=1203

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.6.0
LOC  PORT IPADDR          SUBMASK          DUPLEX SPEED MACTYPE AUTO
1203  A    192.003.001.010  255.255.255.128  HALF   10    802.3  NO
```

Record this information. This information will assigned to the IPGWx card in step 17 of this procedure

4. Display the IP host name assigned to the IP address shown in step 3 by entering the **rtrv-ip-host** command with the IP address. For this example, enter this command.

rtrv-ip-host:ipaddr=193.3.1.10

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0

IPADDR          HOST
192.3.1.10      IPNODE1-1203

IP Host table is (10 of 512) 2% full
```

5. Display the association referencing the local host name that is associated with the M3UA IPLIMx signaling link by entering the `rtrv-assoc` command and specifying the local host name shown in the `rtrv-ip-host` output in step 4. For this example, enter this command.

```
rtrv-assoc: lhost="ipnode-1203"
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME swbel32
  PORT      A
  ADAPTER   M3UA          VER      M3UA RFC
  LHOST     ipnode1-1203
  ALHOST    ---
  RHOST     gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  LPORT     1030          RPORT   2345
  ISTRMS    2              OSTRMS  2
  RMODE     LIN           RMIN    120          RMAX    800
  RTIMES    10           CWMIN   3000
  OPEN      YES          ALW     YES
```

```
IP Appl Sock/Assoc table is (1 of 4000) 1% full
```

6. Any in-service IP connections on the IPLIMx M3UA signaling link used in this procedure must be placed out of service. The recommended method is to have the far end node place these IP connections out of service. Have the far-end node for the IPLIMx M3UA signaling link place the M3UA associations in either the ASP-INACTIVE or ASP-DOWN state.

NOTE: If you choose to perform this step, skip steps 7 and 8, and go to step 9.

NOTE: If the `open` and `alw` parameter values of the association shown in step 5 are `no`, skip this step and step 8, and go to step 9.

7. Change the value of the `alw` parameter to `no` by specifying the `chg-assoc` command with the `alw=no` parameter, as necessary. For this example, enter this command.

```
chg-assoc: aname=swbel32: alw=no
```

CAUTION: This command impacts network performance and should only be used during periods of low traffic.

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD
```

8. Change the value of the `open` parameter to `no` by specifying the `chg-assoc` command with the `open=no` parameter, as necessary. For this example, enter this command.

```
chg-assoc: aname=swbel32: open=no
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD
```



9. Deactivate the M3UA IPLIMx signaling link with the card location and port values shown in step 1 using the **dact-slk** command. For example, enter this command:

```
dact-slk:loc=1203:port=a
```



CAUTION: This command impacts network performance and should only be used during periods of low traffic.

After this command has successfully completed, this message appears.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
Deactivate Link message sent to card.
```

10. Inhibit the IPLIMx card using the **inh-card** command. For example, enter this command.

```
inh-card:loc=1203
```

This message should appear.

```
rlghncxa03w 04-06-28 21:18:37 GMT EAGLE5 31.10.0
Card has been inhibited.
```

11. Remove the M3UA IPLIMx signaling link from the database using the **dlt-slk** command. If there is only one signaling link in the linkset, the **force=yes** parameter must be specified to remove the signaling link.

For this example, enter these commands.

```
dlt-slk:loc=1203:port=a
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-07 08:41:17 GMT EAGLE5 31.6.0
DLT-SLK: MASP A - COMPLTD
```

12. Remove the IPLIMx card from the database using the **dlt-card** command. The **dlt-card** command has only one parameter, **loc**, which is the location of the card. For this example, enter this command.

```
dlt-card:loc=1203
```

When this command has successfully completed, this message appears.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
DLT-CARD: MASP A - COMPLTD
```

13. Add the IPGWx card into the same card location that was occupied by the IPLIMx card, removed in step 12, by performing the “Adding an IP Card” procedure on page 3-16.
-

14. Add the IPGWx linkset, by performing the “Configuring an IPGWx Linkset” procedure on page 3-40.
-

15. Add the IPGWx signaling link to the IPGWx card added in step 13 by performing the “Adding an IP Signaling Link” procedure on page 3-82.

16. Display the route containing the linkset displayed in step 1 by entering the **rtrv-rte** command with the linkset name shown in the LSN column in step 1. For this example, enter this command.

```
rtrv-rte:lsn=e5e6a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-07 11:43:04 GMT EAGLE5 31.6.0
LSN          DPC          RC
e5e6a       003-002-004    20
```

17. Add the necessary routes containing the IPGWx linkset added in step 14, by performing the “Adding a Route” procedure in the *Database Administration Manual - SS7*. The relative cost of these routes must be equal to the relative cost of the routes containing the original IPLIMx linkset.

18. Provision the IP card information recorded in step 2 to the IPGWx card added step 12 by performing the “Changing an IP Card” procedure on page 3-173.

19. Provision the IP link information recorded in step 3 for the IPGWx card added step 12 by performing the “Changing an IP Link” procedure on page 3-158.

NOTE: If the **port** parameter value of the association displayed in step 5 is **A**, skip this step and go to step 21.

20. Change the **port** parameter value of the association displayed in step 5 by entering the **chg-assoc** command with the association name displayed in step 5, and the **port=a** parameter. For this example, enter this command.

```
chg-assoc:aname=swbel32:port=a
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD
```

21. Display the ASPs in the database by entering the **rtrv-asp** command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP          ASSOCIATION          UAPS
asp1         swbel32              3
asp2         a2                   1
asp3         a3                   1
asp4         assoc1               10
asp5         assoc2               10
asp6         assoc3               10
asp7         assoc4               10
```

```
ASP Table is (7 of 4000) 1% full
```


22. Add the ASP shown in step 21 that is associated with the association shown in step 5 to an application server by performing the “Adding an Application Server” procedure on page 3-397.

23. Provision routing keys for routes provisioned in step 17 by performing the “Adding an Application Routing Key Containing an Application Server” procedure on page 3-240. The application server provisioned in step 22 must be assigned to these routing keys.

24. Place the IPGWx card added in step 13 using the **alw-card** command. For example, enter this command.

```
alw-card:loc=1203
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-06-28 21:21:37 GMT EAGLE5 31.10.0
Card has been allowed.
```

25. Activate the signaling link assigned to the IPGWx card using the **act-slk** command. For example, enter this command.

```
act-slk:loc=1203:port=a
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Activate Link message sent to card
```

26. Change the value of the **open** and **alw** parameters of the associations displayed in step 5 to **yes** by specifying the **chg-assoc** command with the **open=yes** and **alw=yes** parameters. For this example, enter this command.

```
chg-assoc:aname=swbel32:open=yes:alw=yes
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD
```

27. Have the far-end node for the signaling link shown in step 25 place the M3UA associations in the ASP-ACTIVE state.

28. Verify that the associations specified in step 26 are in service by entering the **rept-stat-assoc** command with the association names used in step 26. The association is in service if the value in the **PST** column is **IS-NR** and the value in the **SST** column is **ASP-ACTIVE**. For this example, enter this command.

```
rept-stat-assoc:aname=swbel32
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASSOCIATION      PST          SST
swbel32          IS-NR       ASP-ACTIVE
```

29. Verify that the ASPs (shown in step 21) associated with the associations changed in step 26 are in service by entering the **rept-stat-asp** command with the ASP names shown in step 21. The ASP is in service if the value in the **PST** column is **IS-NR** and the value in the **SST** column is **ASP-ACTIVE**. For this example, enter this command.

```
rept-stat-asp:aspname=asp1
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP          ASP ID          PST          SST
asp1        0x00000001     IS-NR       ASP-ACTIVE
```

30. Verify that the application server added in step 22 is in service by entering the **rept-stat-as** command with the application server name specified in step 22. The application server is in service if the value in the **PST** column is **IS-NR** and the value in the **SST** column is **ACTIVE**. For this example, enter this command.

```
rept-stat-as:asname=as1
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
AS          PST          SST
as1        IS-NR       ACTIVE
```

31. Verify that the routes added in step 17 are available by entering the **rept-stat-rte** command with the DPC of the routes that were added. The routes are available if the value in the **PST** column is **IS-NR**, the value in the **SST** column is **Allowed**, and the value in the **AST** column is **ACCESS**. For this example, enter this command.

```
rept-stat-rte:dPCA=001-004-000
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
DPCA          PST          SST          AST
001-004-000  IS-NR       Allowed     ACCESS
```

32. If either the associations, ASPs, application server, or routes are in service or available, go to step 33.

If either the associations, ASPs, application server, or routes are not in service or available, contact Tekelec Technical Services. See "Tekelec Technical Services" on page 1-8.

33. Verify that the IPGWx card is carrying traffic by entering the **msucount -1** pass command with the card location of the IP card added in step 13. For this example, enter this command.

```
pass:loc=1203:cmd="msucount -1"
```

The following is an example of the possible output.

IP7 Secure Gateway Configuration Procedures

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
PASS: Command sent to card

rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
MSUCOUNT: Command In Progress

rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
MSUCOUNT: MSU Count Report

-----
Link Measurements (Port A)
-----

Transmit Counts
-----
tx bytes:                927186
tx msus:                 35661
tx average rate (msus/second): 00441

Receive Counts
-----
rcv bytes:              775302
rcv msus:              29826
rcv average rate (msus/second): 00342

Reroute Counts
-----
msus sent to mate cards: 00000
msus received from mate cards: 00000

MGMT Primitive Totals
-----
MTPP primitives received 00000
MTPP primitives discarded 00000
MTPP primitives transmitted 00000
RKRP primitives received 00000
RKRP primitives discarded 00000
RKRP dynamic route key table updates 00000

Transmit Discard Counts
-----
discarded tx due to special adjpc msu: 00000
discarded tx due to discard all adjpc msu: 00000
discarded tx due to no ss7 rtbl entry: 00000
discarded tx due to no ss7 rtkey: 00001
discarded tx due to no conn avail to pc: 00000
discarded tx due to no conn avail to rtkey: 00001
discarded tx due to congested connection: 00000
discarded tx due to sccp msg type: 00000
discarded tx due to sccp class: 00001
discarded tx due to circular rte: 00000
discarded tx due to normalization error: 00000
discarded tx due to invalid traffic type: 00000
discarded tx due to M3UA conversion error: 00001
discarded tx due to SUA conversion error: 00000
discarded tx due to AS-Pending overflow: 00000
discarded tx due to AS timer Tr expiry: 00000
discarded tx due to reroute failure: 00000
```

```

Receive Discard Counts
-----
discarded rcv due to link state:          00000
discarded rcv due to sccp msg type:      00001
discarded rcv due to sccp class:         00003
discarded rcv due to sccp called party:  00004
discarded rcv due to sccp calling party: 00021
discarded rcv due to isup sio:           00011
discarded rcv due to normalization error: 00000
discarded rcv due to error in XSRV packet: 00000
discarded rcv due to M3UA PDU error:     00001
discarded rcv due to SUA PDU error:      00000
discarded rcv due to invalid rcontext    00000
    
```

```

Stored Transmit Discard Data
-----
83 01 05 05 0a 01 03 bf 09 80 03 08 0d 05 c3 07
01 05 05 05 c3 07 0a 01 03 08 e2 06 c7 04 13 10
    
```

```

Stored Receive Discard Data
-----
53 41 53 49 73 63 63 70 1a 00 09 01 03 08 0d 05
c3 05 0a 01 03 05 c3 05 01 05 05 08 e2 06 c7 04
    
```

END of Report

If the output of the **msucount -1** pass command shows that the IPGWx card is not carrying traffic, contact Tekelec Technical Services. See "Tekelec Technical Services" on page 1-8.

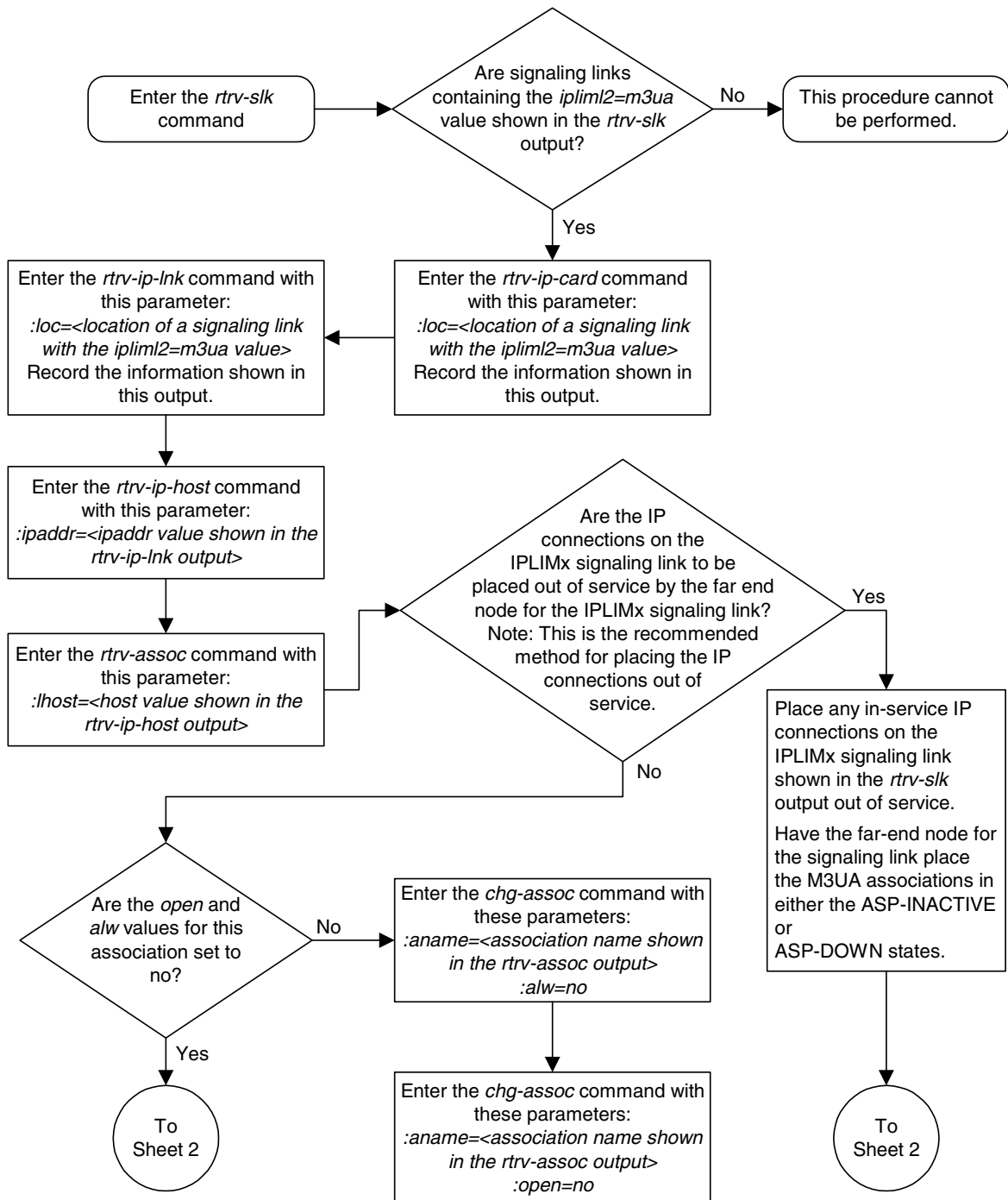
-
34. If other IPLIMx signaling links are to be migrated to IPGWx signaling links, repeat this procedure. If all the desired IPLIMx signaling links have been migrated to IPGWx signaling links, go to step 35.

-
35. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

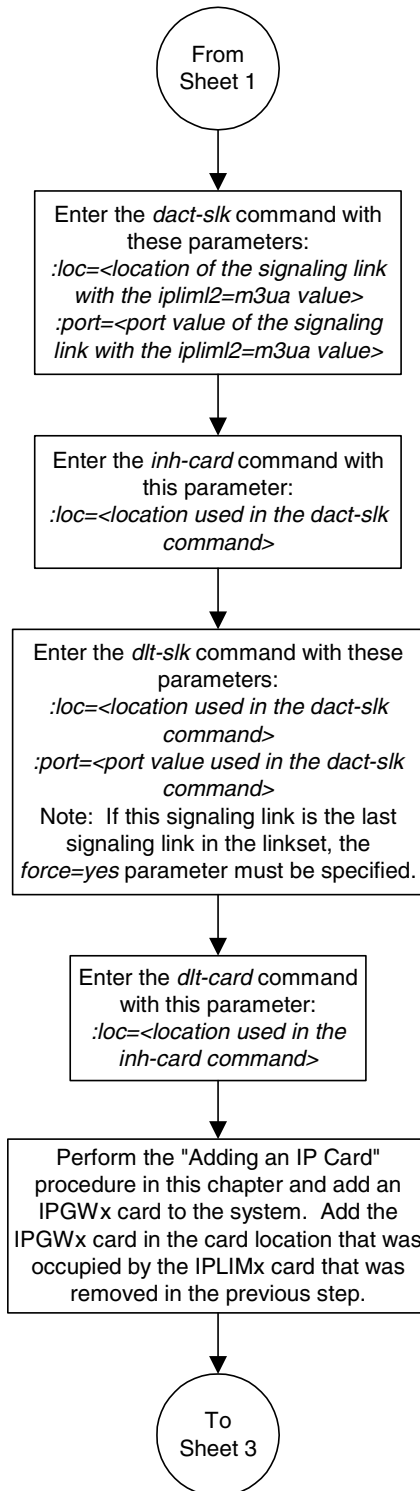
```

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

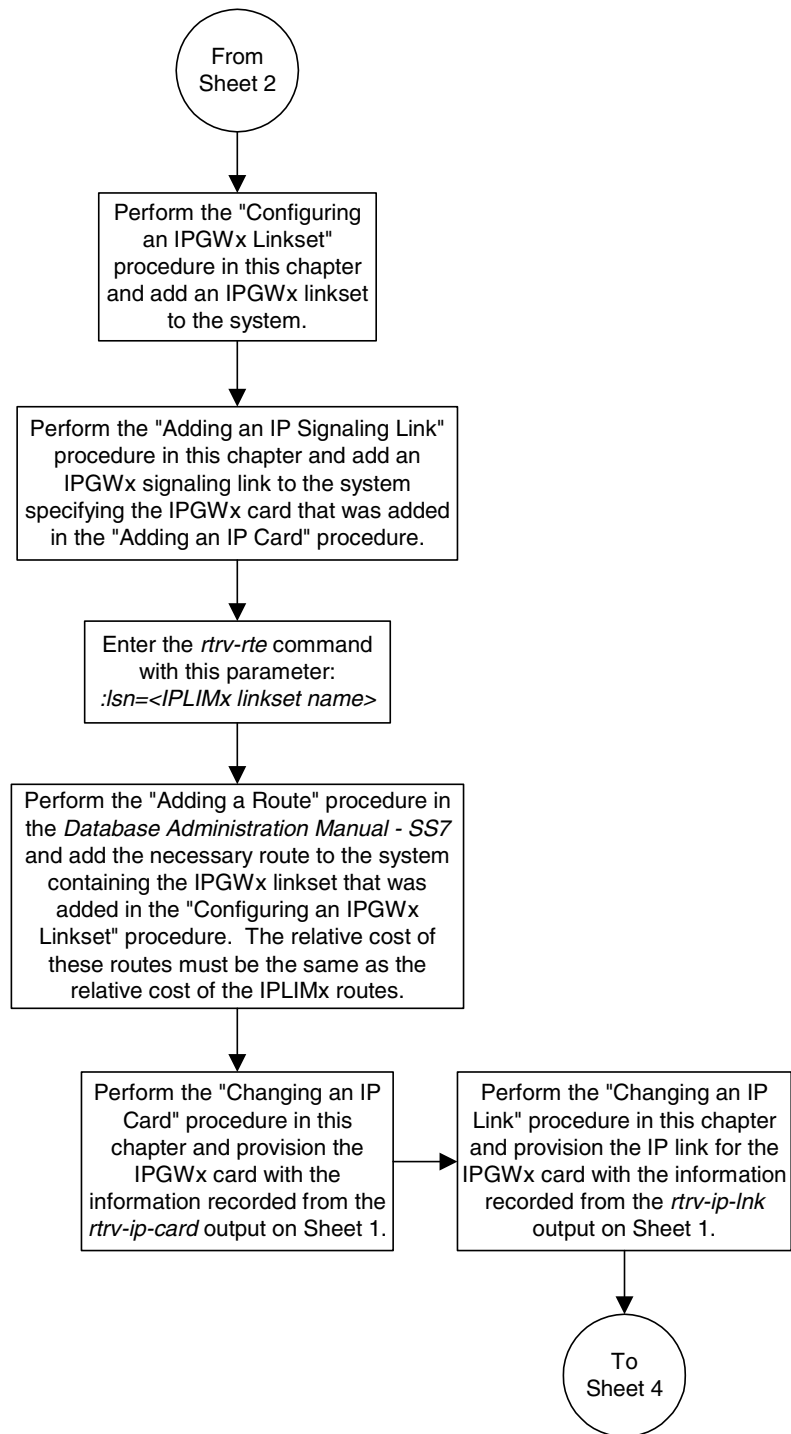
Flowchart 3-8. Migrating IPLIMx M3UA Signaling Links to IPGWx M3UA Connections (Sheet 1 of 6)



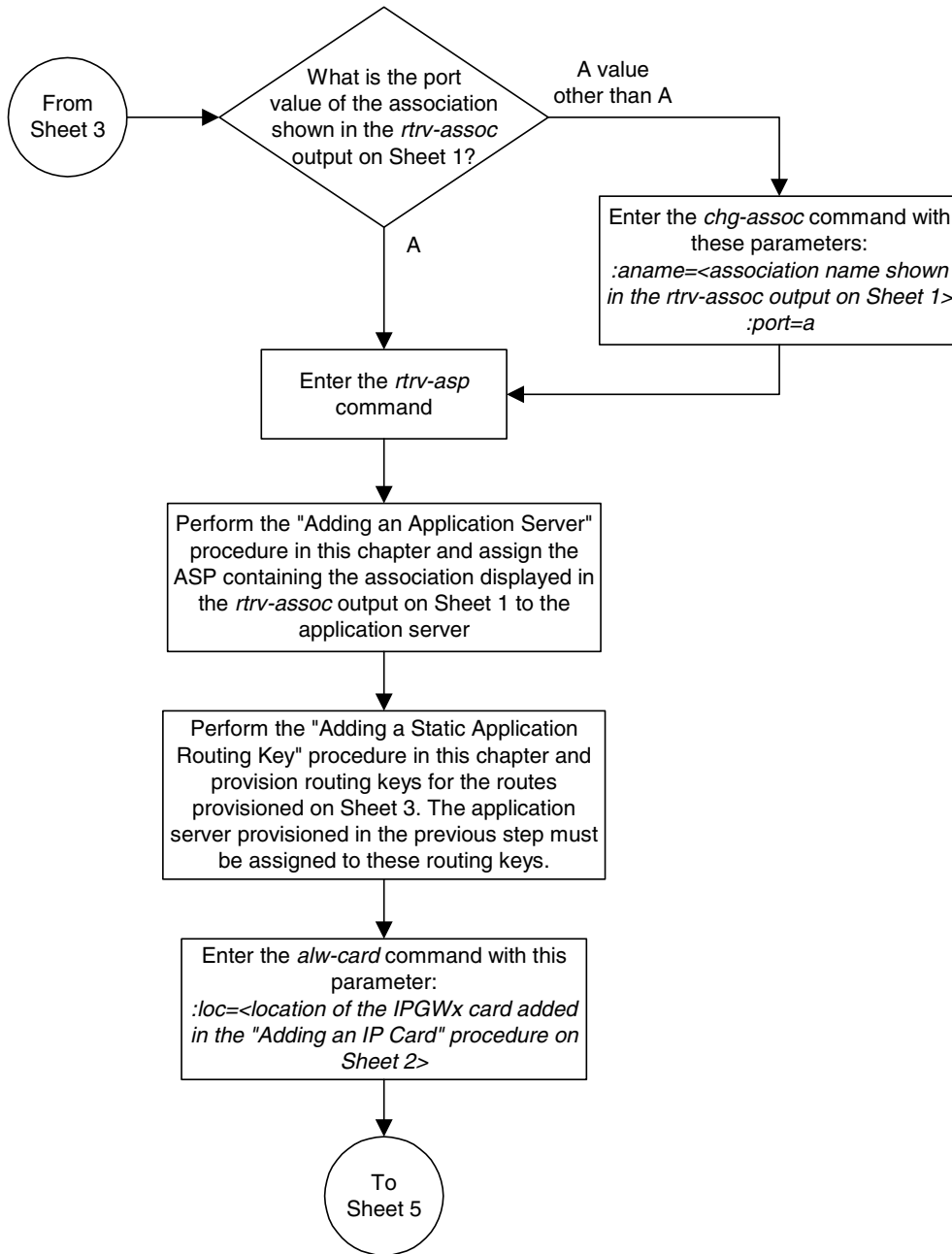
Flowchart 3-8. Migrating IPLIMx M3UA Signaling Links to IPGWx M3UA Connections (Sheet 2 of 6)



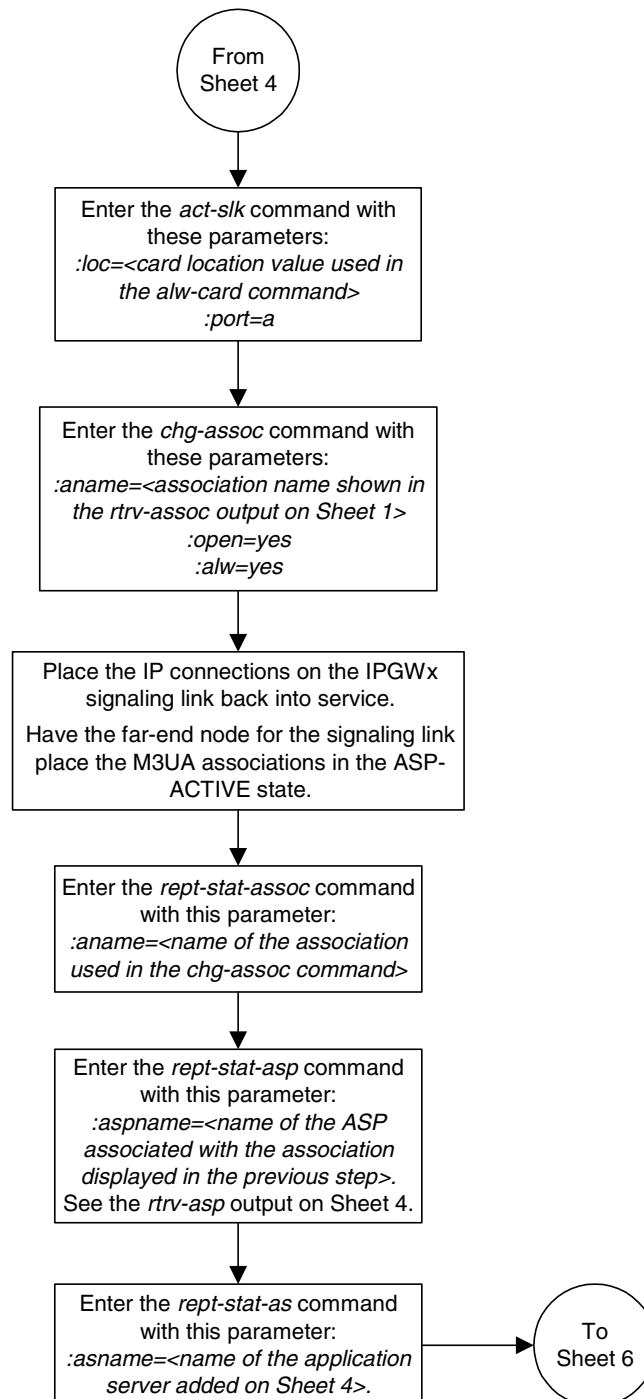
Flowchart 3-8. Migrating IPLIMx M3UA Signaling Links to IPGWx M3UA Connections (Sheet 3 of 6)



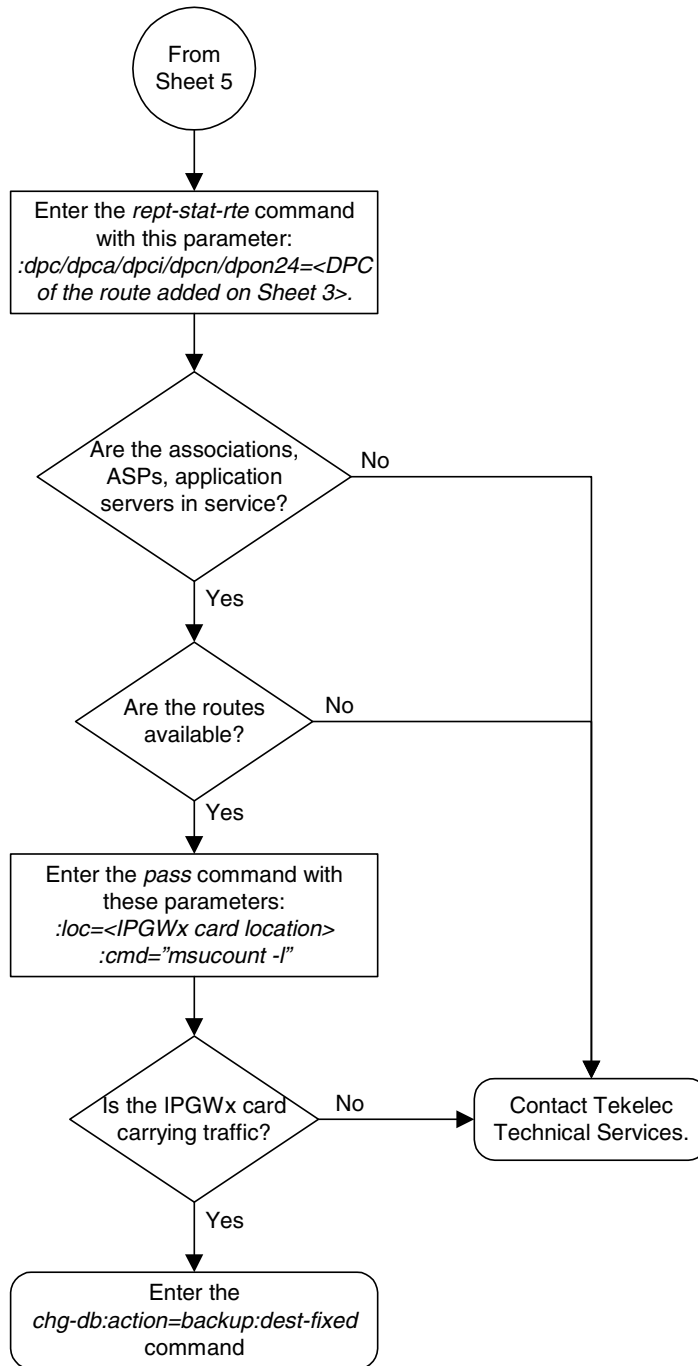
Flowchart 3-8. Migrating IPLIMx M3UA Signaling Links to IPGWx M3UA Connections (Sheet 4 of 6)



Flowchart 3-8. Migrating IPLIMx M3UA Signaling Links to IPGWx M3UA Connections (Sheet 5 of 6)



Flowchart 3-8. Migrating IPLIMx M3UA Signaling Links to IPGWx M3UA Connections (Sheet 6 of 6)



Changing the IP Protocol Option

Use this procedure to change the IP protocol option with the `chg-sg-opts:sync` command.

To change the `:sync` option, which has the values `tali` or `sassi`, the IP cards associated with the `ss7ipgw` or `ipgwi` application must be inhibited, and the signaling links assigned to this card must be deactivated.

Procedure

1. Display the current IP options in the database by entering the `rtrv-sg-opts` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SYNC:          TALI
SRKQ:          250
DRKQ:          750
SNMPCONT:     john doe 555-123-4567
GETCOMM:      public
SETCOMM:      private
TRAPCOMM:     public
INHFEPALM:    NO
SCTPCSUM:     crc32c
IPGWABATE:    NO
IPLIMABATE:   NO
IPTPSALMTHRESH: 80
```

To change the protocol option (synchronization code) for the card, the signaling link to the IP card and the card have to be inhibited.

2. Display the current IP parameters associated with card in the database by entering the `rtrv-ip-card` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
LOC 1201
  SRCHORDR  LOCAL
  DNSA      150.1.1.1
  DNSB      -----
  DEFROUTER -----
  DOMAIN    -----

LOC 1203
  SRCHORDR  LOCAL
  DNSA      192.1.1.40
  DNSB      -----
  DEFROUTER -----
  DOMAIN    NC.TEKELEC.COM

LOC 1205
  SRCHORDR  SRVONLY
  DNSA      192.1.1.40
  DNSB      -----
  DEFROUTER -----
  DOMAIN    NC.TEKELEC.COM
```

3. Display the signaling link associated with the card shown in step 2 using the **rtrv-slk** command specifying the card location. For this example, enter this command.

```
rtrv-slk:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-19 21:17:04 GMT EAGLE5 31.10.0
LOC  PORT LSN          SLC TYPE  IPLIML2
1201 A   nc001          0  IPLIM  SAALTALI
```

4. Verify the status of the signaling link shown in step 3 using the **rept-stat-slk** command. For example, enter this command.

```
rept-stat-slk:loc=1201:port=a
```

The output lists the signaling link assigned to this card:

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK   LSN          CLLI          PST          SST          AST
1201,A  nc001          ----- IS-NR          Avail          ----
Command Completed.
```

If the signaling link is in service-normal (IS-NR), go to step 5 to deactivate the signaling link. If the signaling link is out-of-service-maintenance disabled (OOS-MT-DSBLD), go to step 7 to verify the card status.

5. Deactivate the signaling link assigned to the IP card using the **dact-slk** command. For example, enter this command:

```
dact-slk:loc=1201:port=a
```



CAUTION: This command impacts network performance and should only be used during periods of low traffic.

After this command has successfully completed, this message appears.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
Deactivate Link message sent to card.
```

6. Verify the new link status using the **rept-stat-slk** command. For example, enter this command.

```
rept-stat-slk:loc=1201:port=a
```

The output displays the link status as OOS-MT-DSBLD and gives off a minor alarm:

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
SLK   LSN          CLLI          PST          SST          AST
1201,A  nc001          ----- OOS-MT-DSBLD AVAIL          ---
ALARM STATUS = * 0236 REPT-LKS:not aligned
UNAVAIL REASON = NA
Command Completed.
```

- Verify the status of the IP card to be inhibited using the **rept-stat-card** command. For example, enter this command.

```
rept-stat-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD VERSION      TYPE      APPL      PST      SST      AST
1201 114-000-000  DCM      IPLIM     IS-NR     Active   -----
ALARM STATUS      = No Alarms.
BPDCM GPL         = 002-102-000
IMT BUS A         = Conn
IMT BUS B         = Conn
SLK A PST         = IS-NR      LS=nc001  CLLI=-----
SCCP TVG RESULT   = 24 hr: -----, 5 min: -----
SLAN TVG RESULT   = 24 hr: -----, 5 min: -----
Command Completed.
```

If the IP card to be inhibited is in service-normal (IS-NR), go to step 8 to inhibit the IP card. If the IP card is out-of-service-maintenance disabled (OOS-MT-DSBLD), go to step 10 to change the IP options.

- Inhibit the IP card using the **inh-card** command. For example, enter this command.

```
inh-card:loc=1201
```

This message should appear.

```
rlghncxa03w 04-06-28 21:18:37 GMT EAGLE5 31.10.0
Card has been inhibited.
```

- Display the status of the IP card to verify that it is out-of-service maintenance-disabled (OOS-MT-DSBLD). Enter this command.

```
rept-stat-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD VERSION      TYPE      APPL      PST      SST      AST
1201 114-000-000  DCM      IPLIM     OOS-MT-DSBLD Manual   -----
ALARM STATUS      = No Alarms.
BPDCM GPL         = 002-102-000
IMT BUS A         = Conn
IMT BUS B         = Conn
SLK A PST         = IS-NR      LS=nc001  CLLI=-----
SCCP TVG RESULT   = 24 hr: -----, 5 min: -----
SLAN TVG RESULT   = 24 hr: -----, 5 min: -----
Command Completed.
```

10. Change the IP options in the database using the **chg-sg-opts** command. For this example, enter this command.

```
chg-sg-opts:sync=sassi
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
CHG-SG-OPTS: MASP A - COMPLTD
```

11. Verify the new IP options in the database using the **rtrv-sg-opts** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SYNC:          SASSI
SRKQ:          250
DRKQ:          750
SNMPCONT:     john doe 555-123-4567
GETCOMM:      public
SETCOMM:      private
TRAPCOMM:     public
INHFEPALM:    NO
SCTPCSUM:     crc32c
IPGWABATE:    NO
IPLIMABATE:   NO
IPTPSALMTHRESH: 80
```

NOTE: If step 8 was not performed, skip steps 12 and 13, and go to step 14.

12. Allow the IP card that was inhibited in step 8 using the **alw-card** command. For example, enter this command.

```
alw-card:loc=1201
```

This message should appear.

```
rlghncxa03w 04-06-28 21:21:37 GMT EAGLE5 31.10.0
Card has been allowed.
```

13. Verify the in-service normal (IS-NR) status of the IP card using the **rept-stat-card** command. For example, enter this command.

```
rept-stat-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD  VERSION      TYPE      APPL      PST          SST          AST
1201  114-000-000    DCM       IPLIM     IS-NR        Active       -----
  ALARM STATUS      = No Alarms.
  BPDCM GPL         = 002-102-000
  IMT BUS A         = Conn
  IMT BUS B         = Conn
  SLK A   PST       = IS-NR          LS=nc001  CLLI=-----
  SCCP TVG RESULT   = 24 hr: -----, 5 min: -----
  SLAN TVG RESULT   = 24 hr: -----, 5 min: -----
Command Completed.
```

NOTE: If step 5 was not performed, skip steps 14 and 15, and go to step 16.

14. Activate the signaling link from step 5 using the **act-slk** command. For example, enter this command.

```
act-slk:loc=1201:port=a
```

The link changes its state from OOS-MT-DSBLD (out-of-service maintenance-disabled) to IS-NR (in-service normal).

The output confirms the activation.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Activate Link message sent to card
```

15. Verify the in-service normal (IS-NR) status of the signaling link by using the **rept-stat-slk** command. For example, enter this command.

```
rept-stat-slk:loc=1201:port=a
```

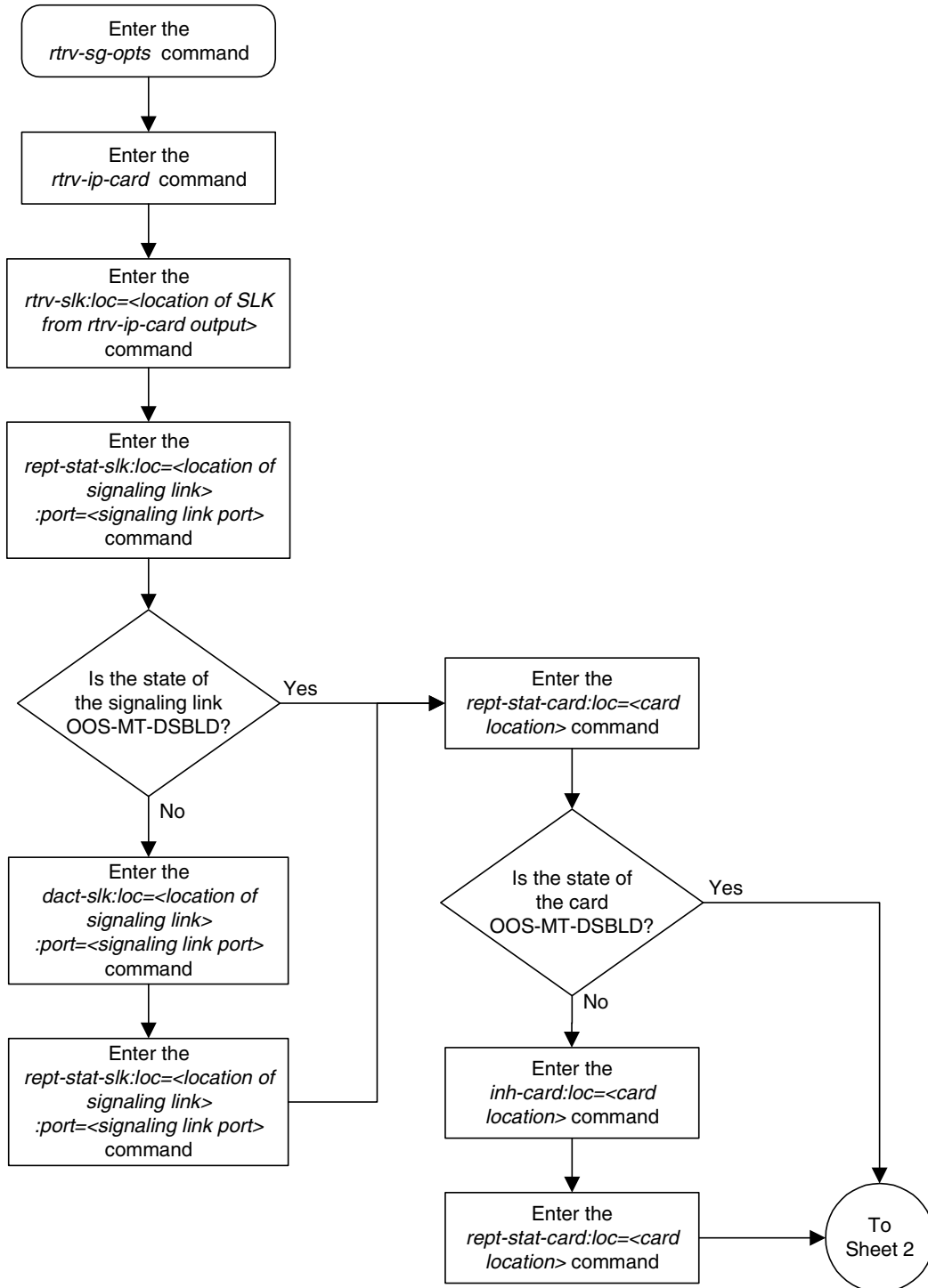
This message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1201,A   nc001     -----  IS-NR    Avail    ----
Command Completed.
```

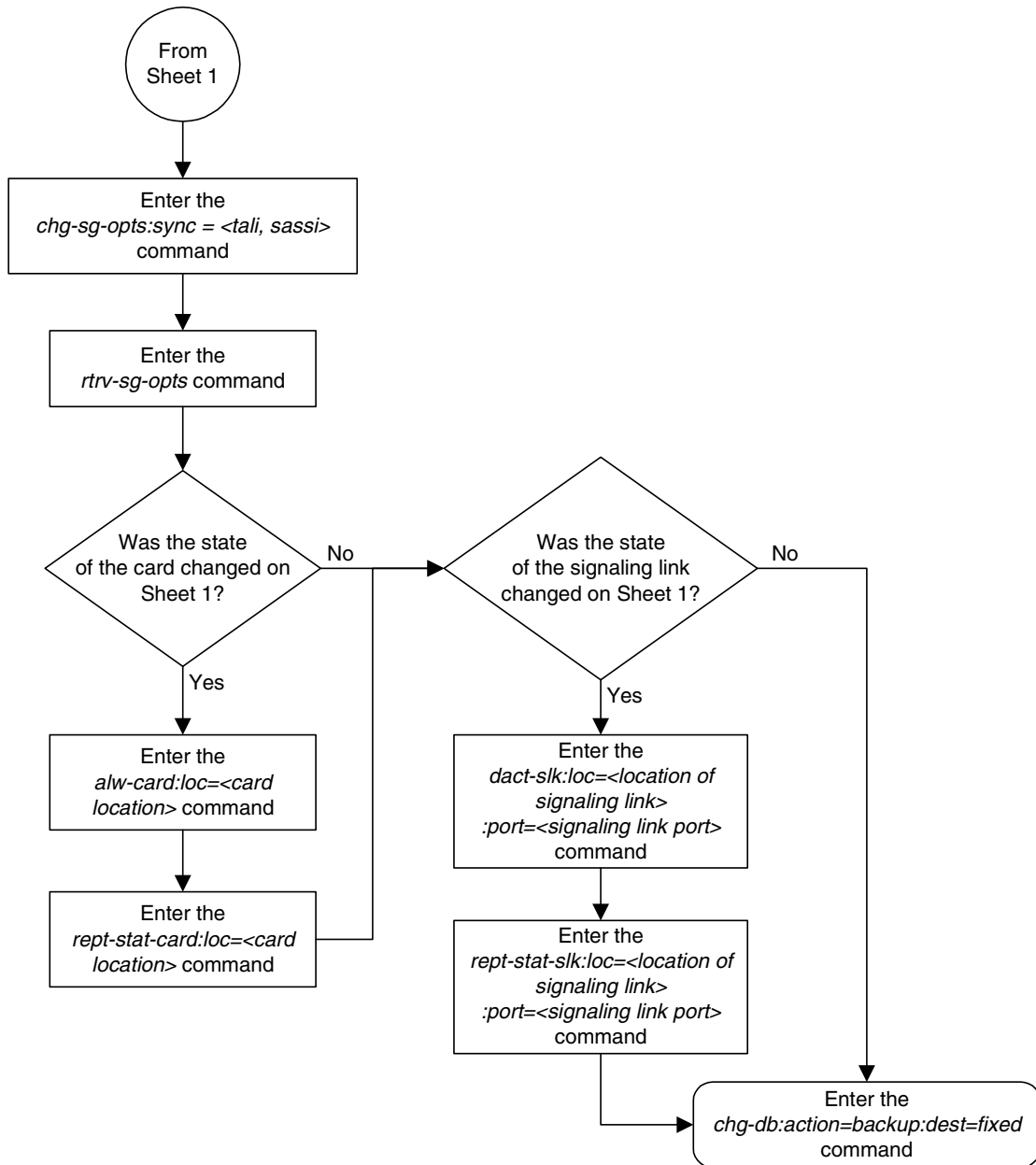
16. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-9. Changing the IP Protocol Option (Sheet 1 of 2)



Flowchart 3-9. Changing the IP Protocol Option (Sheet 2 of 2)



Changing IP Options other than SYNC and SCTPCSUM

Use this procedure to change the IP options defined by these parameters: **drkq**, **getcomm**, **setcomm**, **snmpcont**, **srkq**, **trapcomm**, **inhfepalm**, **ipgwabate**, **iplimabate**. These parameters do not require the IP card associated with an **ss7ipgw** or **ipgwi** application to be inhibited prior to configuration.

NOTE: The **chg-sg-opts** command also contains the **iptpsalmthresh** parameter, used to configure the IP TPS alarm threshold. This parameter is not used in this procedure. Perform the “Configuring the IP TPS Alarm Threshold” procedure on page 3-328 to configure the IP TPS alarm threshold with the **iptpsalmthresh** parameter.

:drkq – The dynamic routing key quantity used to specify the maximum number of dynamic routing key entries in the Routing Key table of each **ss7ipgw** and **ipgwi** card.

:getcomm – The community name used to validate SNMP *Get* and *GetNext* requests. This value applies to each IP card SNMP agent.

:setcomm – The community name used to validate SNMP *Set* requests. This value applies to each IP card SNMP agent.

:snmpcont – The system contact information for each IP card SNMP agent, used to define the *sysContact* object in the SNMP MIB II System Group.

:srkq – The static routing key quantity used to specify the maximum number of static routing key entries in the Routing Key table of each **ss7ipgw** and **ipgwi** card.

:trapcomm – The community name used when sending SNMP traps. This value applies to each IP card SNMP agent.

:inhfepalm – This parameter specifies whether or not major alarms for TALI sockets whose secondary state is NEA-FEP will be inhibited (suppressed). This value applies to all IPLIM and SS7IPGW cards in the system.

When this parameter is set to **no** (default), the NEA-FEP sockets are reported as OOS-MT and a major alarm (UAM 0084 - IP Connection Unavailable) is raised for that connection.

When this parameter is set to **yes**, all TALI sockets with a secondary status of NEA-FEP are reported as IS-NR and no socket alarm is raised. For IPLIM and IPLIMI cards, where each link consists of a single TALI socket, a link alarm will still be raised when the TALI socket's secondary status is NEA-FEP, regardless of the **inhfepalm** parameter value.

:ipgwabate – enables (**ipgwabate=yes**) or disables (**ipgwabate=no**) SS7 congestion abatement procedures for SS7IPGW signaling links (signaling links assigned to cards running the **ss7ipgw** application). The default value for this parameter is **no**.

:iplimabate – enables (**iplimabate=yes**) or disables (**iplimabate=no**) SS7 congestion abatement procedures for IPLIM signaling links (signaling links assigned to cards running the **iplim** application). The default value for this parameter is **no**.

The sum of the values specified for the **srkq** and **drkq** parameters must not be greater than:

- 1000 if there are any DCM cards (870-1945-xx) running the **ss7ipgw** or **ipgwi** application.
- 2500 if all cards that are running the **ss7ipgw** or **ipgwi** application are SSEDCCM cards (870-2732-xx).

Replacing an SSEDCCM card with a dual-slot DCM card when the sum of the values for the **srkq** and **drkq** parameters is greater than 1000 will result in the DCM card being auto-inhibited.

The value specified for the **srkq** parameter cannot be less than the current number of static entries in the Routing Key table.

The value that can be specified for the **srkq** parameter also depends on how many dynamic routing keys are actively registered. The value specified for the **srkq** parameter cannot exceed the lowest value determined by subtracting the number of dynamic entries on either an **ss7ipgw** or **ipgwi** card from:

- 1000 if there are any dual-slot DCM cards (870-1945-xx) running the **ss7ipgw** or **ipgwi** application
- 2500 if all cards that are running the **ss7ipgw** or **ipgwi** application are SSEDCCM cards (870-2732-xx).

For example, if one dual-slot DCM card has 200 dynamic entries and the other card has 300 dynamic entries, the value specified for **srkq** cannot exceed 700 (1000 - 300 = 700; 1000 - 200 = 800; 700 is the lower value).

If **d** is the current maximum number of actual dynamic routing keys on any card that is running the **ss7ipgw** or **ipgwi** application, then the sum of **d** and the **srkq** value cannot exceed:

- 1000 per card if there are any dual-slot DCM cards (870-1945-xx) running the **ss7ipgw** or **ipgwi** application
- 2500 per card if all cards that are running the **ss7ipgw** or **ipgwi** application are SSEDCCM cards (870-2732-xx).

Effectively this means that even if the **drkq** parameter value has been decreased to less than **d**, the **srkq** value cannot be increased until **d** has also decreased.

The Dynamic Routing Key feature must be on in order to enter the **drkq** parameter. If the current value of the **drkq** parameter is greater than 0, then the Dynamic Routing Key feature is on. If the current value of the **drkq** parameter is 0, enter the **rtrv-feat** command. The **DYNRTK** field in the **rtrv-feat** command output shows whether or not this feature is on.

The values of the **snmpcont**, **getcomm**, **setcomm**, and **trapcomm** parameters are a string of up to 32 characters that is not case sensitive. If the character string contains characters other than alphanumeric characters, the character string must be enclosed in single quotes.

Procedure

1. Display the current IP options in the database by entering the `rtrv-sg-opts` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
SYNC:          TALI
SRKQ:          250
DRKQ:          750
SNMPCONT:      john doe 555-123-4567
GETCOMM:       public
SETCOMM:       private
TRAPCOMM:      public
INHFEPALM:     NO
SCTPCSUM:      crc32c
IPGWABATE:     NO
IPLIMABATE:    NO
IPTPSALMTHRESH: 80
```

NOTE: If the current value of the `drkq` parameter is 0 and is not being changed, or if the current value of the `drkq` parameter is greater than 0, skip steps 2 and 3, and go to step 4.

2. Verify that the Dynamic Routing Key feature is on, by entering the `rtrv-feat` command. If the Dynamic Routing Key feature is on, the `DYNRTK` field should be set to `on`. For this example, the Dynamic Routing Key feature is off.

NOTE: The `rtrv-feat` command output contains other fields that are not used by this procedure. If you wish to see all the fields displayed by the `rtrv-feat` command, see the `rtrv-feat` command description in the *Commands Manual*.

NOTE: If the Dynamic Routing Key feature is on, skip step 3 and go to step 4.

3. Turn the Dynamic Routing Key feature on by entering this command.

```
chg-feat:dynrtk=on
```

NOTE: Once the Dynamic Routing Key feature is turned on with the `chg-feat` command, it cannot be turned off.

The Dynamic Routing Key feature must be purchased before you turn this feature on with the `chg-feat` command. If you are not sure if you have purchased the Dynamic Routing Key feature, contact your Tekelec Sales Representative or Account Representative.

When the `chg-feat` has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 11:43:04 GMT EAGLE5 31.10.0
CHG-FEAT: MASP A - COMPLTD
```

4. Change the IP options in the database using the **chg-sg-opts** command. For this example, enter this command.

```
chg-sg-opts:srkq=200:drkq=800
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:18:37 GMT EAGLE5 31.10.0  
CHG-SG-OPTS: MASP A - COMPLTD
```

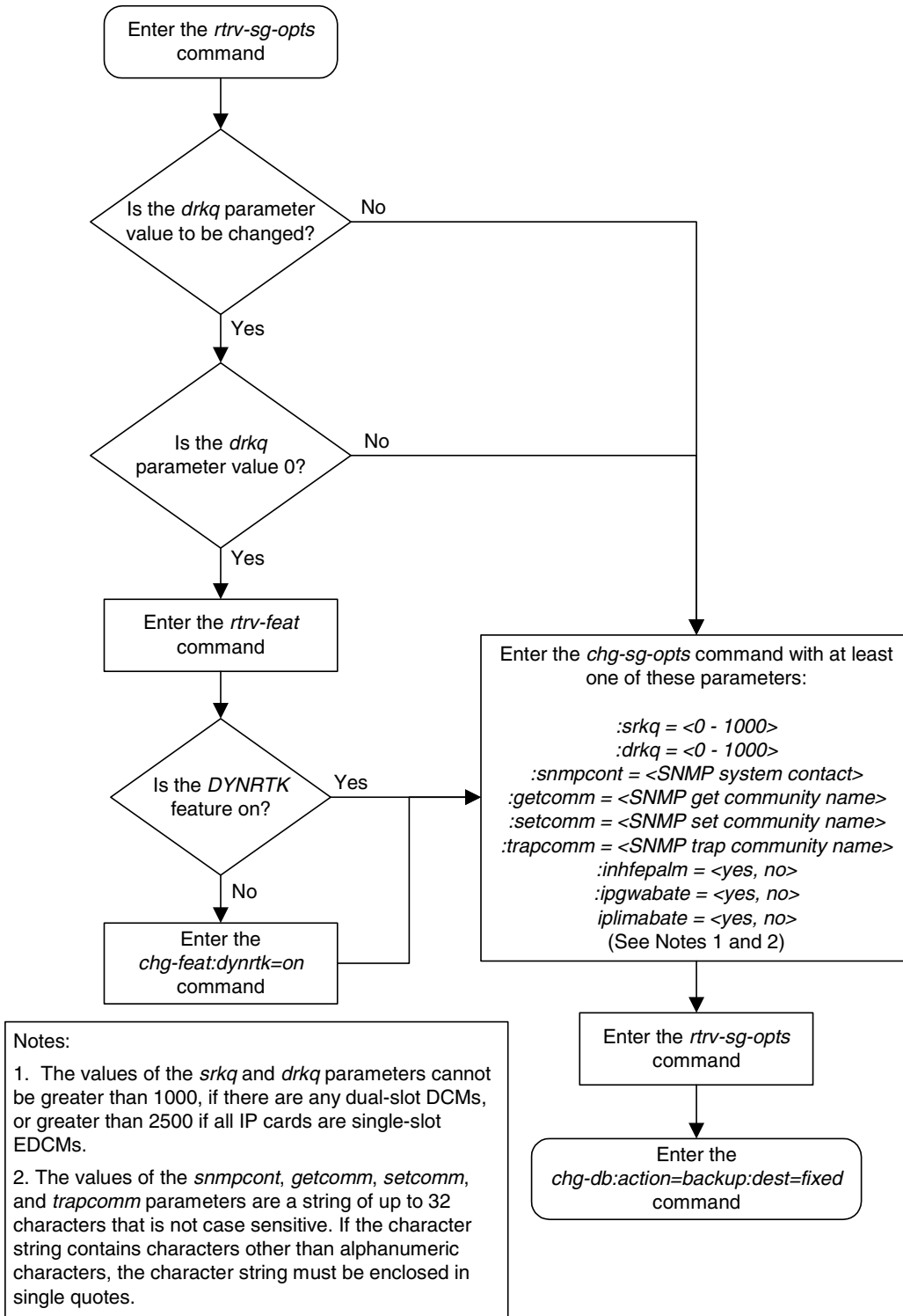
5. Verify the new IP options in the database by entering the **rtrv-sg-opts** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0  
SYNC:          TALI  
SRKQ:          200  
DRKQ:          800  
SNMPCONT:     john doe 555-123-4567  
GETCOMM:      public  
SETCOMM:      private  
TRAPCOMM:     public  
INHFEPALM:    NO  
SCTPCSUM:     crc32c  
IPGWABATE:    NO  
IPLIMABATE:   NO  
IPTPSALMTHRESH: 80
```

6. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-10. Changing an IP Option That Does Not Require Inhibiting the IP Card



Adding an IP Host

This procedure associates hostnames with IP addresses using the **ent-ip-host** command.

The **ent-ip-host** command uses the following parameters.

:host– The host name to be associated with the IP address. This parameter identifies the logical name assigned to the device with the IP address indicated. The host name can contain up to 60 characters (using only these characters: a-z, A-Z, 0-9, -, .) and is not case sensitive. The host name must begin with a letter. Host names containing a dash (-) must be enclosed in double quotes.

:ipaddr – The IP address to be associated with the hostname. The node's IP address. This is an IP address expressed in standard "dot notation." IP addresses consist of the system's network number and the machine's unique host number.

Procedure

1. Display the current IP host information in the database by entering the **rtrv-ip-host** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
```

IPADDR	HOST
192.1.1.10	IPNODE1-1201
192.1.1.12	IPNODE1-1203
192.1.1.14	IPNODE1-1205
192.1.1.20	IPNODE2-1201
192.1.1.22	IPNODE2-1203
192.1.1.24	IPNODE2-1205
192.1.1.32	KC-HLR2
192.1.1.50	DN-MS1
192.1.1.52	DN-MS2

```
IP Host table is (9 of 512) 2% full
```

2. Add IP host information to the database by entering the **ent-ip-host** command. For example, enter this command.

```
ent-ip-host:host="kc-hlr1":ipaddr=192.1.1.30
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:18:37 GMT EAGLE5 31.10.0
ENT-IP-HOST: MASP A - COMPLTD
```

3. Verify the new IP host information in the database by entering the **rtrv-ip-host** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
```

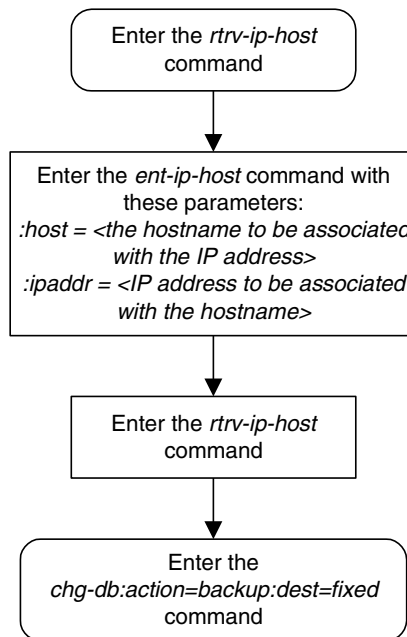
```
IPADDR          HOST
192.1.1.10      IPNODE1-1201
192.1.1.12      IPNODE1-1203
192.1.1.14      IPNODE1-1205
192.1.1.20      IPNODE2-1201
192.1.1.22      IPNODE2-1203
192.1.1.24      IPNODE2-1205
192.1.1.30      KC-HLR1
192.1.1.32      KC-HLR2
192.1.1.50      DN-MSC1
192.1.1.52      DN-MSC2
```

```
IP Host table is (10 of 512) 2% full
```

4. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-11. Adding an IP Host



Removing an IP Host

This procedure removes the association between a hostname and an IP address using the `dlt-ip-host` command.

The `dlt-ip-host` command uses the following parameters.

:host—Hostname. The hostname to be removed. This parameter identifies the logical name assigned to a device with an IP address.

Before an IP host can be removed, the associated IP address must not be referenced in the IP link table. This can be verified in the `rtrv-ip-lnk` output

Procedure

1. Display the current IP host information in the database by entering the `rtrv-ip-host` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
```

IPADDR	HOST
192.1.1.10	IPNODE1-1201
192.1.1.12	IPNODE1-1203
192.1.1.14	IPNODE1-1205
192.1.1.20	IPNODE2-1201
192.1.1.22	IPNODE2-1203
192.1.1.24	IPNODE2-1205
192.1.1.30	KC-HLR1
192.1.1.32	KC-HLR2
192.1.1.50	DN-MS1
192.1.1.52	DN-MS2
192.3.3.33	GW100.NC.TEKELEC.COM

```
IP Host table is (11 of 512) 2% full
```

2. Verify that the IP address of the IP host is not referenced in the IP link table by entering the `rtrv-ip-lnk` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
```

LOC	PORT	IPADDR	SUBMASK	DUPLEX	SPEED	MACTYPE	AUTO
1201	A	192.001.001.010	255.255.255.0	----	---	DIX	YES
1203	A	192.001.001.012	255.255.255.0	----	---	DIX	YES
1205	A	192.001.001.014	255.255.255.0	FULL	100	DIX	NO

3. If the IP address of the IP host is referenced in the IP link table, remove the reference by changing the IP address to 0.0.0.0 using the procedure “Changing an IP Link” on page 3-158.
-

4. Delete IP host information from the database by entering the `dlt-ip-host` command. For example, enter this command.

```
dlt-ip-host:host=gw100.nc.tekelec.com
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
DLT-IP-HOST: MASP A - COMPLTD
```

5. Verify the changed IP host information in the database by entering the `rtrv-ip-host` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:20:37 GMT EAGLE5 31.10.0
```

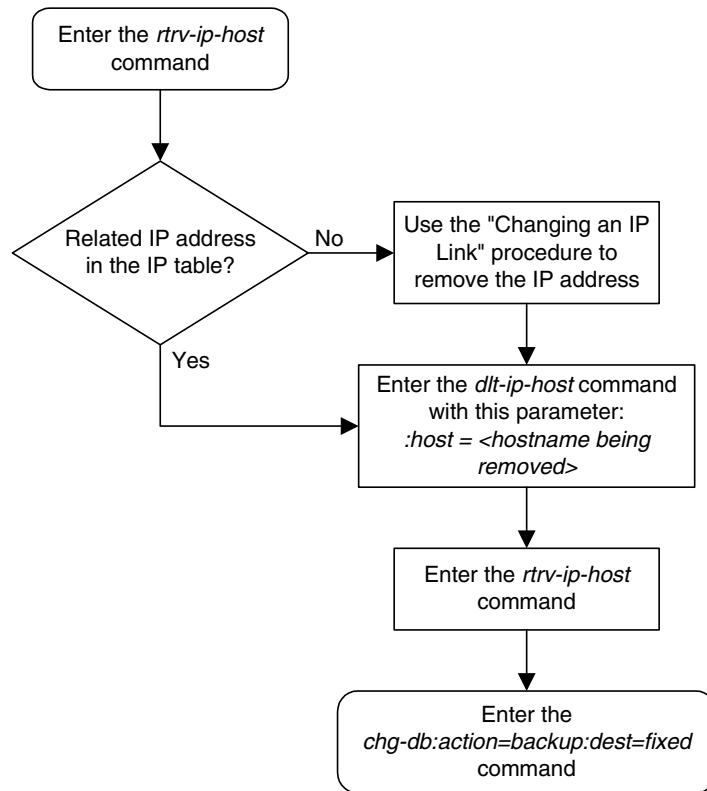
IPADDR	HOST
192.1.1.10	IPNODE1-1201
192.1.1.12	IPNODE1-1203
192.1.1.14	IPNODE1-1205
192.1.1.20	IPNODE2-1201
192.1.1.22	IPNODE2-1203
192.1.1.24	IPNODE2-1205
192.1.1.30	KC-HLR1
192.1.1.32	KC-HLR2
192.1.1.50	DN-MSC1
192.1.1.52	DN-MSC2

```
IP Host table is (10 of 512) 2% full
```

6. Back up the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-12. Removing an IP Host



Changing an IP Link

This procedure is used to change the link parameters for IP cards using the **chg-ip-lnk** command. These link parameters are used to configure the Ethernet hardware.

The **chg-ip-lnk** command uses the following parameters.

- :loc** – The card location of the IP card.
- :port** – The Ethernet interface on the IP card, A or B.
- :ipaddr** – IP address assigned to the Ethernet interface on the IP card. This is an IP address expressed in standard “dot notation.” IP addresses consist of the system’s network number and the machine’s unique host number.
- :submask** – The subnet mask of the IP interface. A subnet mask is an IP address with a restricted range of values. The bits in the mask must be a string of one’s followed by a string of zero’s. There must be at least two one’s in the mask, and the mask cannot be all one’s. See Table 3-15 on page 3-159 to assign the correct parameter values.
- :auto** – Tells hardware whether to automatically detect the **duplex** and **speed**.
- :duplex** – This is the mode of operation of the interface.
- :speed** – This is the bandwidth in megabits per second of the interface.
- :mactype** – This is the Media Access Control Type of the interface.

If the **ipaddr** parameter value is non-zero, the **ipaddr** value must be shown in the **rtrv-ip-host** output.

A zero **ipaddr** parameter value (0.0.0.0) indicates the IP card Ethernet interface to IP link association is disabled.

If the **defrouter** parameter of the **chg-ip-card** command contains an IP address for the card specified in this procedure, the network portion of one of the IP addresses assigned to the card in this procedure must match the network portion of the IP address specified by the **defrouter** parameter of the **chg-ip-card** command.

The network portion of the IP address is based on the class of the IP address (shown in Table 3-15 on page 3-159). If the IP address is a Class A IP address, the first field is the network portion of the IP address. If the IP address is a Class B IP address, the first two fields are the network portion of the IP address. If the IP address is a Class C IP address, the first three fields are the network portion of the IP address. For example, if the IP address is 193.5.207.150, a Class C IP address, the network portion of the IP address is 193.5.207.

If the **auto=yes** parameter is specified, then the **duplex** and **speed** parameters are not allowed.

The **loc** parameter value must be shown in the **rtrv-ip-card** output.

The IP card must be placed out of service.

If either the **ipaddr** or **submask** parameters are specified, then both parameters must be specified. If the **ipaddr** parameter value is zero (0.0.0.0), the **submask** parameter is not required.

If the IP card is a single-slot EDCM, the A or B interface can be used. The B interface cannot be used with the DCM.

The IP address and subnet mask values cannot be changed to an address representing a different network if:

- If the network interface specified by the **loc** and **port** parameters has a default router, **dnrsa**, or **dsnb** parameter values assigned to it, as shown in the **rtrv-ip-card** output.
- Any IP routes, shown in the **rtrv-ip-rte** output, reference the IP address for the network interface specified by the **loc** and **port** parameters.

The IP link cannot be changed if open sockets or associations reference the IP link being changed.

The network portion of the IP addresses assigned to the IP links on an IP card must be unique. For example, if IP links are assigned to IP card 1103, the network portion of the IP address for Ethernet interface A (**port=a**) must be different from the IP address for Ethernet interface B (**port=b**).

The **submask** parameter value is based upon the **ipaddr** setting. See Table 3-15 for the valid input values for the **submask** and **ipaddr** parameter combinations.

Table 3-15. Valid Subnet Mask Parameter Values

Network Class	IP Network Address Range	Valid Subnet Mask Values
A	1.0.0.0 to 127.0.0.0	255.0.0.0 (the default value for a class A IP address) 255.192.0.0 255.224.0.0 255.240.0.0 255.248.0.0 255.252.0.0 255.254.0.0 255.255.128.1

Table 3-15. Valid Subnet Mask Parameter Values (Continued)

A+B	131.0.0.0 to 191.255.0.0	255.255.0.0 (the default value for a class B IP address) 255.255.192.0 255.255.224.0 255.255.240.0 255.255.248.0 255.255.252.0 255.255.254.0 255.255.255.128
A+B+C	192.0.0.0 to 223.255.255.0	255.255.255.0 (the default value for a class C IP address) 255.255.255.192 255.255.255.224 255.255.255.240 255.255.255.248 255.255.255.252

Canceling the `RTRV-APPL-SOCK` and `RTRV-ASSOC` Commands

Because the `rtrv-appl-sock` and `rtrv-assoc` commands used in this procedure can output information for a long period of time, the `rtrv-appl-sock` and `rtrv-assoc` commands can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-appl-sock` and `rtrv-assoc` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-appl-sock` or `rtrv-assoc` commands was entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-appl-sock` or `rtrv-assoc` commands was entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-appl-sock` or `rtrv-assoc` commands were entered, from another terminal other than the terminal where the `rtrv-appl-sock` or `rtrv-assoc` commands were entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current link parameters associated with the IP card in the database by entering the **rtrv-ip-lnk** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.10.0
LOC  PORT  IPADDR          SUBMASK          DUPLEX  SPEED  MACTYPE  AUTO
1201  A     192.001.001.001 255.255.255.128  HALF   10     802.3    NO
1203  A     192.001.001.012 255.255.255.0   ----   ---    DIX      YES
1205  A     192.001.001.014 255.255.255.0   FULL   100    DIX      NO
```

2. If IP address information is being added or changed (not deleted) in the link parameters, verify that the IP address is present in the IP host table by using the **rtrv-ip-host** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

IPADDR          HOST
192.1.1.1       IPNODE1-1201
192.1.1.12      IPNODE1-1203
192.1.1.14      IPNODE1-1205
192.1.1.20      IPNODE2-1201
192.1.1.22      IPNODE2-1203
192.1.1.24      IPNODE2-1205
192.1.1.30      KC-HLR1
192.1.1.32      KC-HLR2
192.1.1.50      DN-MS1
192.1.1.52      DN-MS2
```

IP Host table is (10 of 512) 2% full

If the required IP address information is not shown in the **rtrv-ip-host** output, add the IP address information to the IP host table using the procedure "Adding an IP Host" on page 3-153.

3. To change IP link parameters, the signaling link to the IP card and the IP card have to be inhibited. Display the signaling link associated with the card shown in step 2 using the **rtrv-slk** command specifying the card location. For this example, enter this command.

```
rtrv-slk:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-19 21:17:04 GMT EAGLE5 31.10.0
LOC  PORT  LSN          SLC  TYPE  IPLIML2
1201  A     nc001        0    IPLIM  SAALTALI
```

- Retrieve the status of the signaling link assigned to the IP card to be changed using the `rept-stat-slk` command. For example, enter this command.

```
rept-stat-slk:loc=1201:port=a
```

The output lists the signaling link assigned to this card:

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1201,A   nc001     -----  IS-NR    Avail    ----
Command Completed.
```

If the signaling link is in service-normal (IS-NR), go to step 5 to deactivate the signaling link. If the signaling link is out-of-service-maintenance disabled (OOS-MT-DSBLD), go to step 7 to verify the IP card status.

- Deactivate the signaling link assigned to the IP card using the `rept-stat-slk` command. For example, enter this command.

```
dact-slk:loc=1201:port=a
```



CAUTION: This command impacts network performance and should only be used during periods of low traffic.

After this command has successfully completed, this message appears.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
Deactivate Link message sent to card.
```

- Verify the new link status using the `rept-stat-slk` command. For example, enter this command.

```
rept-stat-slk:loc=1201:port=a
```

The output displays the link status as OOS-MT-DSBLD and gives off a minor alarm:

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1201,A   nc001     -----  OOS-MT-DSBLD AVAIL    ---
ALARM STATUS = * 0236 REPT-LKS:not aligned
UNAVAIL REASON = NA
Command Completed.
```


- Verify the status of the IP card to be inhibited using the **rept-stat-card** command. For example, enter this command.

```
rept-stat-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD  VERSION      TYPE    APPL      PST          SST          AST
1201  114-000-000    DCM     IPLIM     IS-NR        Active       -----
ALARM STATUS      = No Alarms.
BPDCM GPL         = 002-102-000
IMT BUS A         = Conn
IMT BUS B         = Conn
SLK A   PST       = IS-NR          LS=nc001  CLLI=-----
SCCP TVG RESULT   = 24 hr: -----, 5 min: -----
SLAN TVG RESULT   = 24 hr: -----, 5 min: -----
Command Completed.
```

If the IP card to be inhibited is in service-normal (IS-NR), go to step 8 to inhibit the card. If the IP card is out-of-service-maintenance disabled (OOS-MT-DSBLD), go to step 10 to change the IP link parameters.

- Inhibit the IP card using the **inh-card** command. For example, enter this command.

```
inh-card:loc=1201
```

This message should appear.

```
rlghncxa03w 04-06-28 21:18:37 GMT EAGLE5 31.10.0
Card has been inhibited.
```

- Display the status of the IP card to verify that it is out-of-service maintenance-disabled (OOS-MT-DSBLD). Enter this command.

```
rept-stat-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD  VERSION      TYPE    APPL      PST          SST          AST
1201  114-000-000    DCM     IPLIM     OOS-MT-DSBLD Manual       -----
ALARM STATUS      = No Alarms.
BPDCM GPL         = 002-102-000
IMT BUS A         = Conn
IMT BUS B         = Conn
SLK A   PST       = IS-NR          LS=nc001  CLLI=-----
SCCP TVG RESULT   = 24 hr: -----, 5 min: -----
SLAN TVG RESULT   = 24 hr: -----, 5 min: -----
Command Completed.
```

NOTE: If the `ipaddr` or `submask` parameter values are not being changed, skip step 10 and go to step 11.

10. Display the attributes of the IP card assigned to the IP link being changed by entering the `rtrv-ip-card` command and specifying the card location of the IP link. For this example, enter this command.

```
rtrv-ip-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
  LOC 1201
    SRCHORDR  LOCAL
    DNSA      150.1.1.1
    DNSB      -----
    DEFROUTER -----
    DOMAIN    -----
```

If the `rtrv-ip-card` output shows an IP address for the default router (`DEFROUTER`) whose network portion matches the network portion of the IP address being changed, go to the “Changing an IP Card” procedure on page 3-173 and change the IP address of the default router to `0.0.0.0`.

11. Display any IP routes referencing the IP link being changed by entering the `rtrv-ip-rte` command and specifying the card location of the IP link. For this example, enter this command.

```
rtrv-ip-rte:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
LOC  DEST          SUBMASK          GTWY
1201 128.252.10.5    255.255.255.255 140.188.13.33
1201 128.252.0.0     255.255.0.0     140.188.13.34
1201 150.10.1.1      255.255.255.255 140.190.15.3

IP Route table is (5 of 1024) 1% full
```

If the `rtrv-ip-rte` output shows that the card has IP routes assigned to it, go to the “Removing an IP Route” procedure on page 3-188 and remove the IP routes from the database.

NOTE: If the required IP address information is not shown in the `rtrv-ip-host` output in step 2 and a new local host was added to the database for this procedure, skip steps 12 and 13, and go to step 14.

12. Display the application socket referencing the local host name that is associated with the IP link being changed by entering the `rtrv-appl-sock` command and specifying the local host name shown in the `rtrv-ip-host` output in step 2. For this example, enter this command.

```
rtrv-appl-sock:lhost="ipnode1-1201"
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.10.0
SNAME kchlr11201
PORT A
LHOST ipnode1-1201
RHOST kc-hlr1
LPORT 7000 RPORT 7000
SERVER YES DCMPS 1
REXMIT FIXED RTT 60
OPEN YES ALW NO
```

IP Appl Sock/Assoc table is (3 of 4000) 1% full

If the **rtrv-appl-sock** output shows that the **open** parameter is **yes**, go to the “Changing an Application Socket” procedure on page 3-205 and change the value of the **open** parameter to **no**.

NOTE: If an application socket was shown in the **rtrv-appl-sock** output in step 12, skip step 13 and go to step 14.

13. Display the association referencing the local host name that is associated with the IP link being changed by entering the **rtrv-assoc** command and specifying the local host name shown in the **rtrv-ip-host** output in step 2. For this example, enter this command.

rtrv-assoc:lhost="ipnode-1201"

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME swbel32
PORT A
ADAPTER M3UA VER M3UA RFC
LHOST ipnode1-1201
ALHOST ---
RHOST gw100.ncd-economic-development.southeastern-cooridor-ash.gov
LPORT 1030 RPORT 2345
ISTRMS 2 OSTRMS 2
RMODE LIN RMIN 120 RMAX 800
RTIMES 10 CWMIN 3000
OPEN YES ALW YES
```

IP Appl Sock/Assoc table is (1 of 4000) 1% full

If the **rtrv-assoc** output shows that the **open** parameter is **yes**, go to the “Changing an Association” procedure on page 3-350 and change the value of the **open** parameter to **no**.

14. Change the link parameters associated with the IP card in the database using the **chg-ip-lnk** command. For this example, enter this command.

```
chg-ip-lnk:loc=1201:port=a:ipaddr=192.1.1.10
:submask=255.255.255.0:auto=yes:mactype=dix
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:18:37 GMT EAGLE5 31.10.0
CHG-IP-LNK: MASP A - COMPLTD
```

15. Verify the new link parameters associated with the IP card that was changed in step 14 by entering the **rtrv-ip-lnk** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
LOC  PORT  IPADDR          SUBMASK          DUPLEX  SPEED  MACTYPE  AUTO
1201 A    192.001.001.010 255.255.255.0   ----   ---   DIX      YES
1203 A    192.001.001.012 255.255.255.0   ----   ---   DIX      YES
1205 A    192.001.001.014 255.255.255.0   FULL  100   DIX      NO
```

NOTE: If step 8 was not performed, skip steps 16 and 17, and go to step 18.

16. Allow the IP card that was inhibited in step 8 by using by using the **alw-card** command. For example, enter this command.

```
alw-card:loc=1201
```

This message should appear.

```
rlghncxa03w 04-06-28 21:20:37 GMT EAGLE5 31.10.0
Card has been allowed.
```

17. Verify the in-service normal (IS-NR) status of the IP card using the **rept-stat-card** command. For example, enter this command.

```
rept-stat-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD  VERSION  TYPE  APPL  PST          SST          AST
1201  114-000-000  DCM   IPLIM  IS-NR        Active       -----
ALARM STATUS      = No Alarms.
BPDCM GPL         = 002-102-000
IMT BUS A         = Conn
IMT BUS B         = Conn
SLK A   PST       = IS-NR      LS=nc001  CLLI=-----
SCCP TVG RESULT   = 24 hr: -----, 5 min: -----
SLAN TVG RESULT   = 24 hr: -----, 5 min: -----
Command Completed.
```

NOTE: If step 5 was not performed, skip steps 18 and 19, and go to step 20.

- 18 Activate the signaling link from step 5 using the `act-slk` command. For example, enter this command.

```
act-slk:loc=1201:port=a
```

The link changes its state from OOS-MT-DSBLD (out-of-service maintenance-disabled) to IS-NR (in-service normal).

The output confirms the activation.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Activate Link message sent to card
```

19. Verify the in-service normal (IS-NR) status of the signaling link using the `rept-stat-slk` command. For example, enter this command.

```
rept-stat-slk:loc=1201:port=a
```

This message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1201,A   nc001     ----- IS-NR      Avail     ----
Command Completed.
```

NOTE: If the `ipaddr` or `submask` values were not changed, skip steps 20 and 21, and go to step 22.

NOTE: If the IP address of the default router was not changed to 0.0.0.0 in step 10, skip step 20, and go to step 21.

20. Go to the “Changing an IP Card” procedure on page 3-173 and change the IP address of the default router to a non-zero value, where the network portion of the default router IP address matches the network portion of the IP link’s new IP address.
-

NOTE: If IP routes were not removed in step 11, skip step 21, and go to step 22.

21. Go to the “Adding an IP Route” procedure on page 3-183 and add the IP routes back into the database.
-

NOTE: If the `open` parameter value for either an application socket or an association was not changed in either steps 12 or 13, skip step 22, and go to step 23.

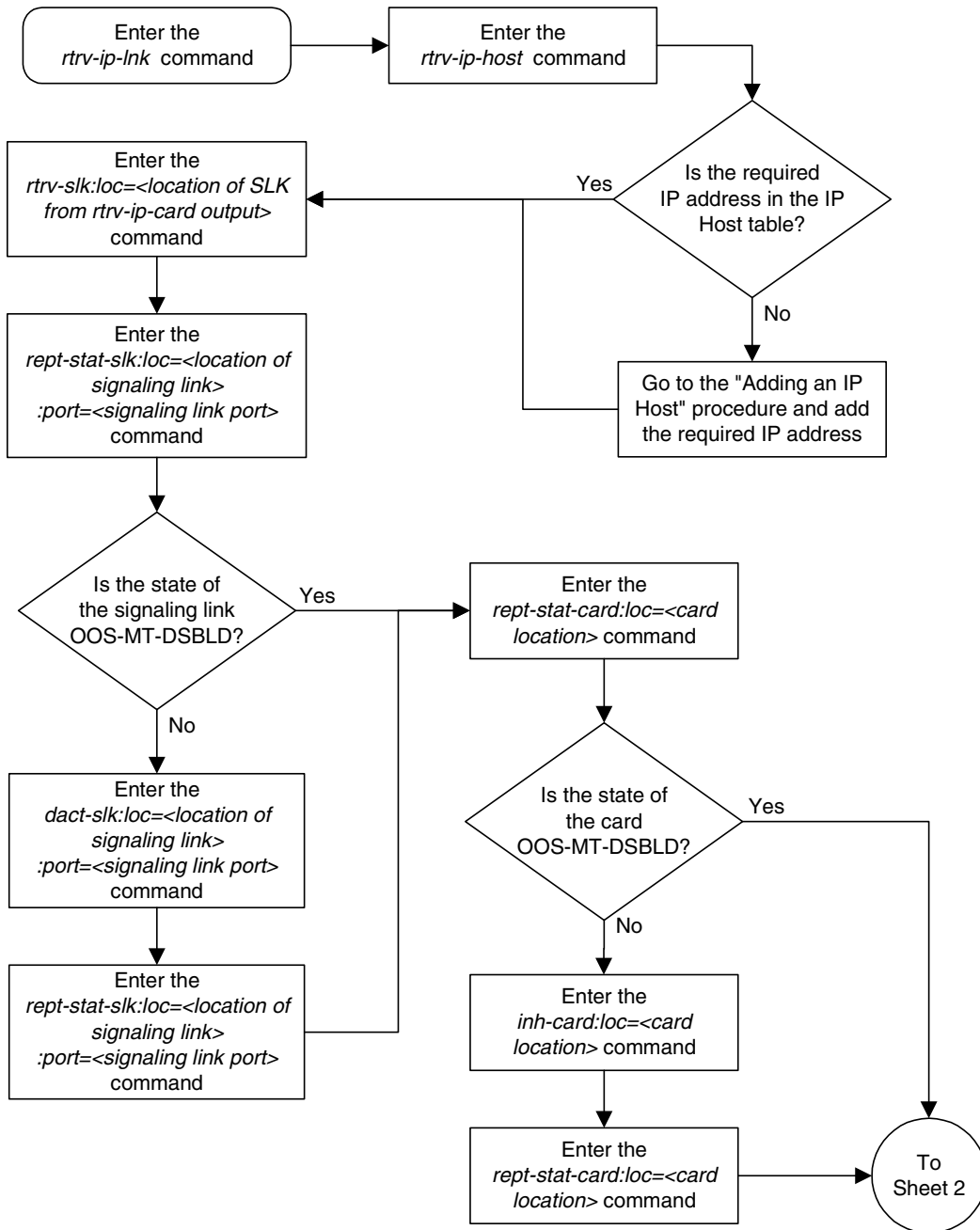
22. Go to one of these procedures and change the value of the `open` parameter either the application socket or the association to `yes`.
- For an application socket – “Changing an Application Socket” on page 3-205
 - For an association – “Changing an Association” on page 3-350
-

23. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

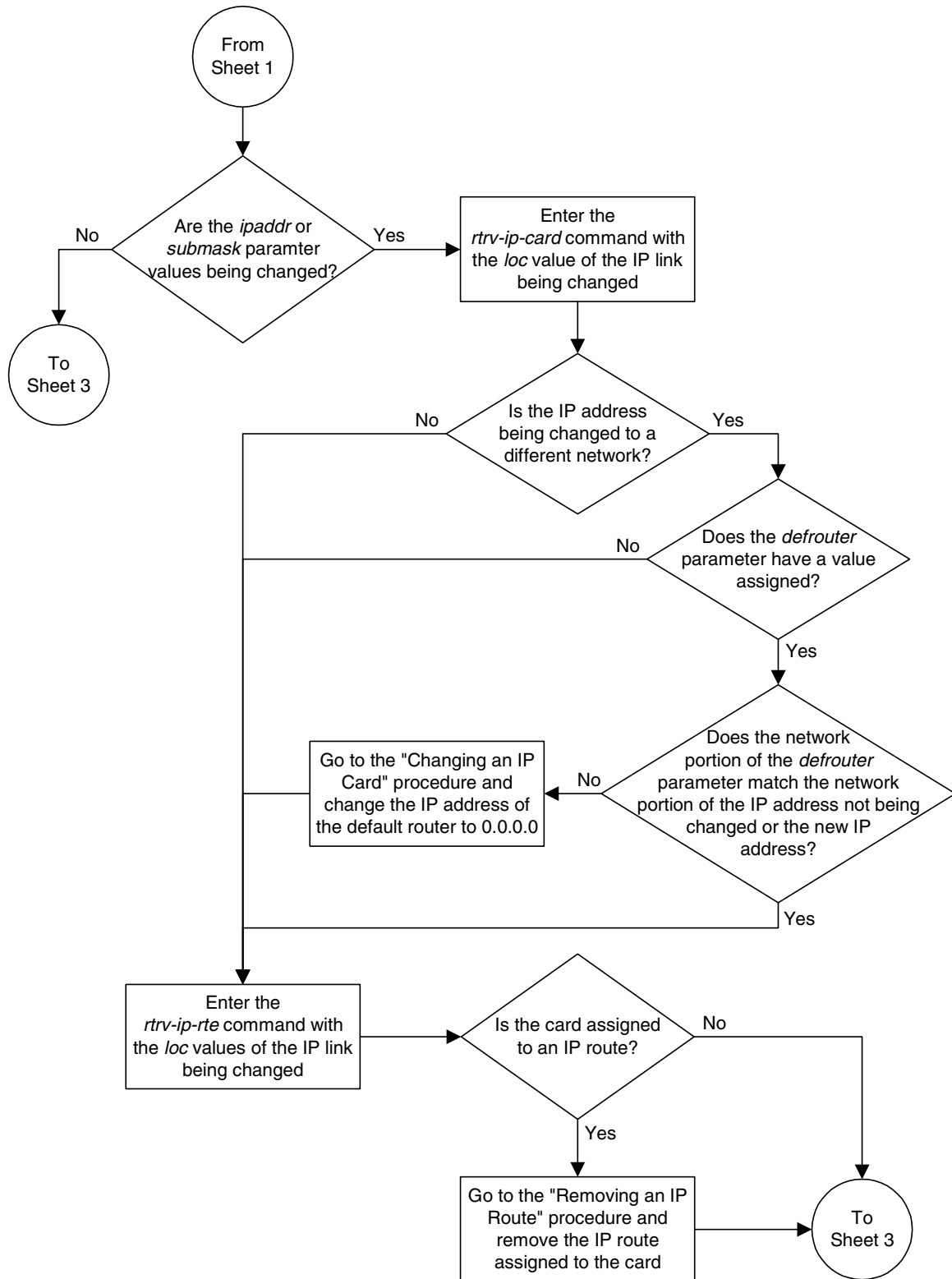
```

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

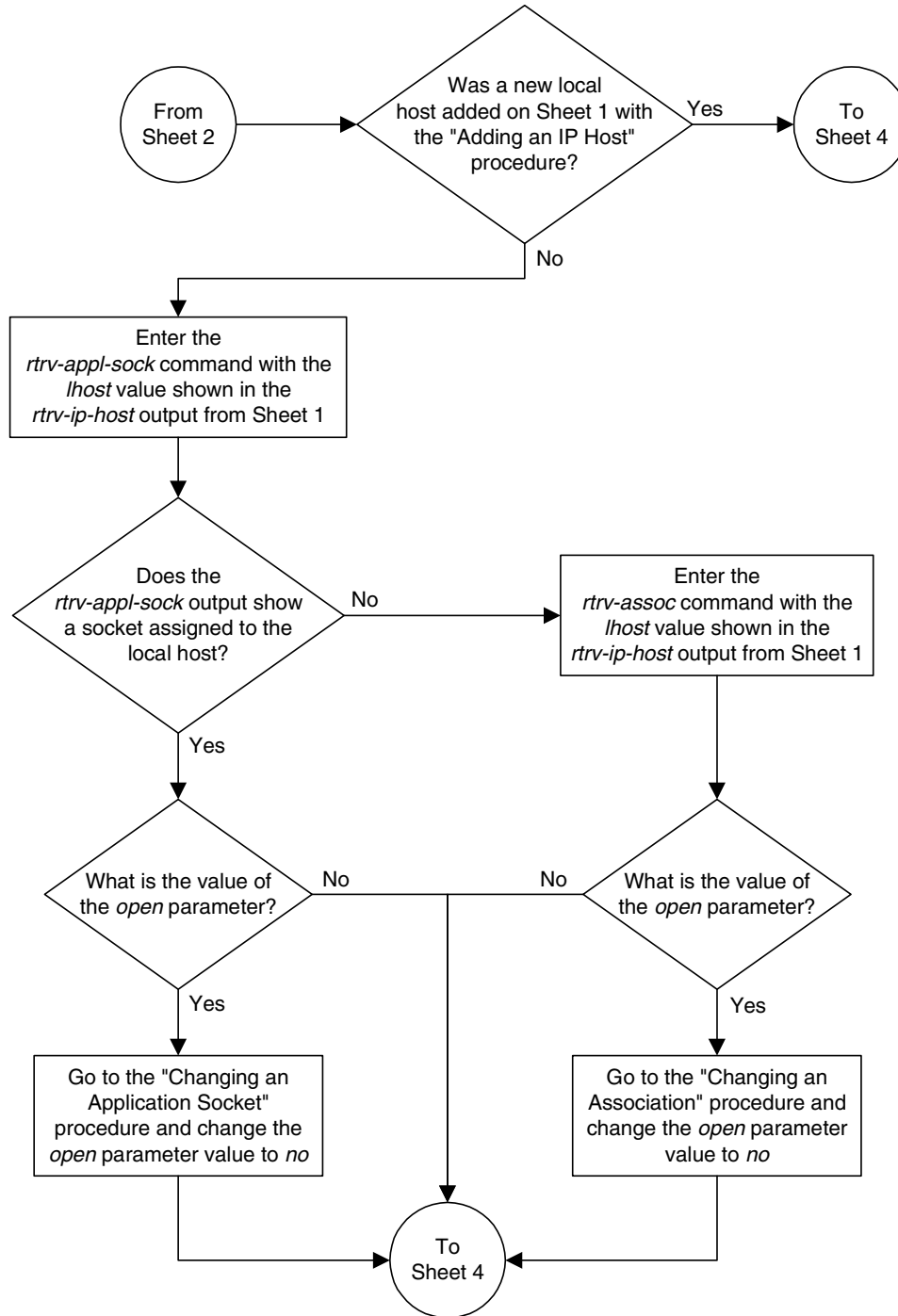
Flowchart 3-13. Changing an IP Link (Sheet 1 of 5)



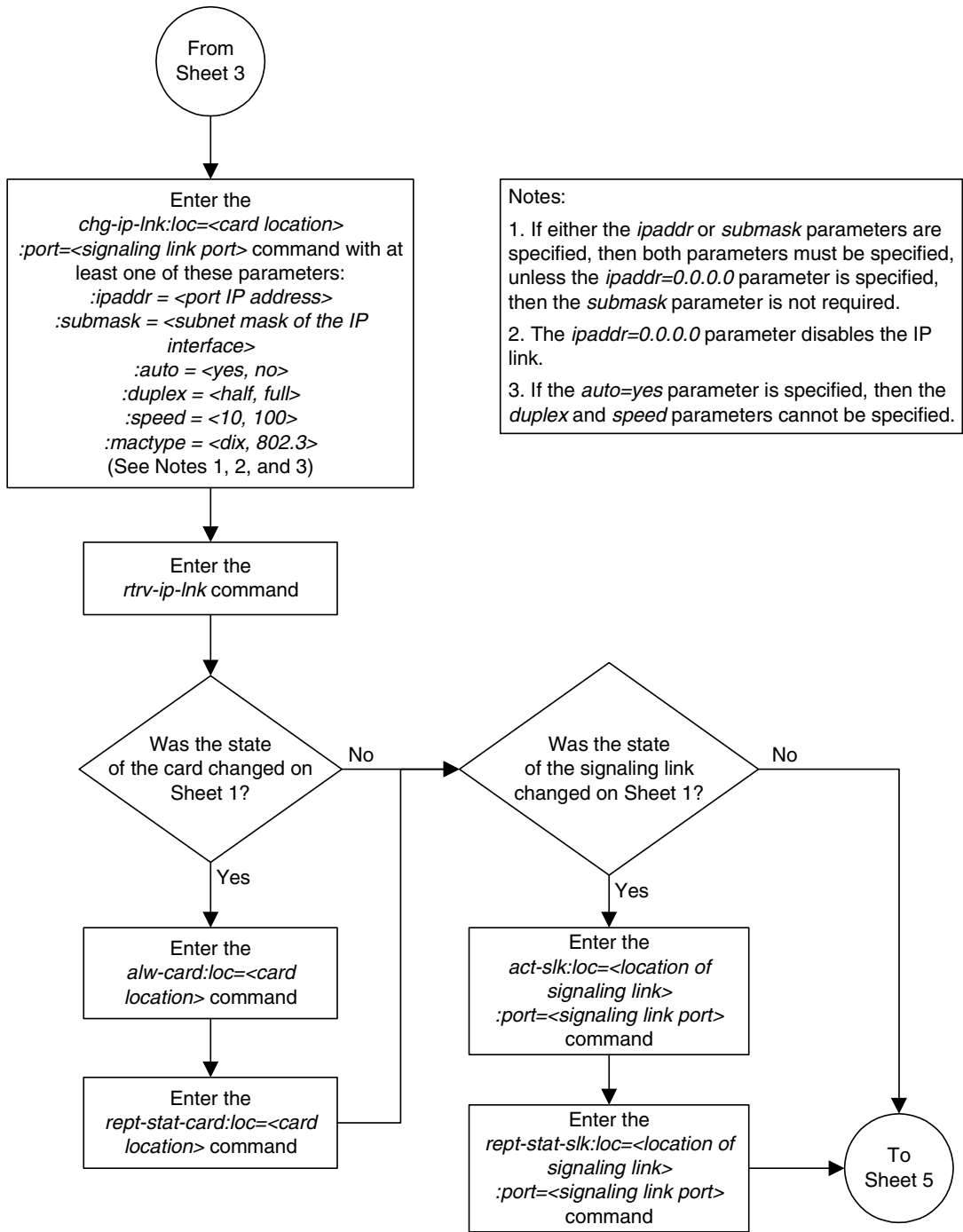
Flowchart 3-13. Changing an IP Link (Sheet 2 of 5)



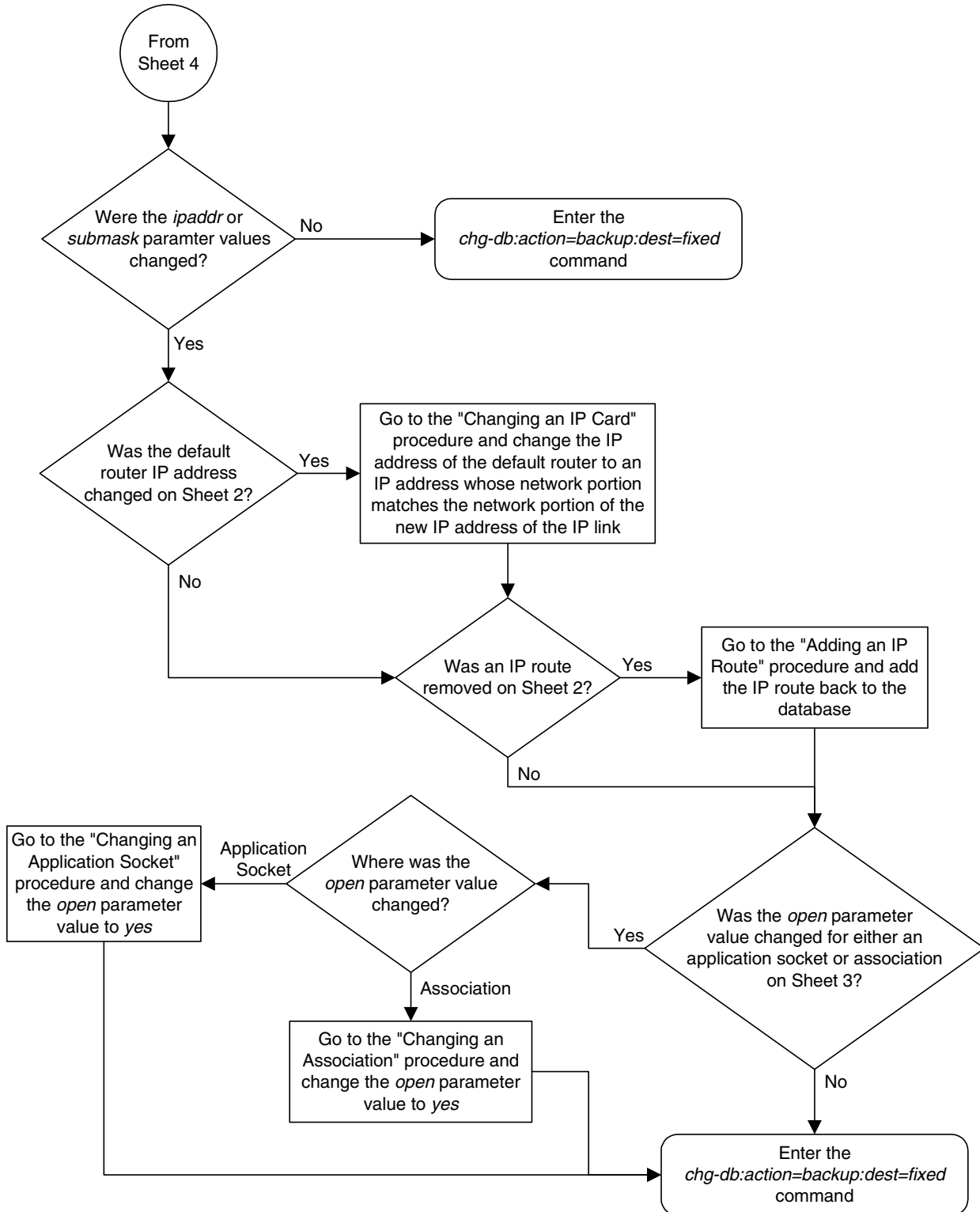
Flowchart 3-13. Changing an IP Link (Sheet 3 of 5)



Flowchart 3-13. Changing an IP Link (Sheet 4 of 5)



Flowchart 3-13. Changing an IP Link (Sheet 5 of 5)



Changing an IP Card

This procedure is used to change the IP stack parameters associated with an IP card in the database using the **chg-ip-card** command.

The **chg-ip-card** command uses the following parameters.

:loc – The card location of the IP card

:srchordr – Host Table Search Order

:dnrsa – Domain name server A's IP address. This is an IP address expressed in standard "dot notation." IP addresses consist of the system's network number and the machine's unique host number.

:dnrsb – Domain name server B's IP address. This is an IP address expressed in standard "dot notation." IP addresses consist of the system's network number and the machine's unique host number.

:domain – The domain name is used to construct a fully-qualified DNS name consisting of 120 characters or less. For example, a domain name can be **tekelec.com**, the hostname is **john.doe**. The fully-qualified DNS name would be **john.doe@tekelec.com**.

:defrouter – Default router IP address. This is an IP address expressed in standard "dot notation." IP addresses consist of the system's network number and the machine's unique host number.

:rstdomain – Reset Domain name. The parameter is used to reset the domain to a NULL value.

The IP card must be placed out of service.

The **rstdomain** parameter cannot be specified if the **domain** parameter is specified.

If the **defrouter** parameter is specified in this procedure, the network portion of one of the IP addresses assigned to the card, shown in the **rtrv-ip-lnk** output, must match the network portion of the IP address specified by the **defrouter** parameter.

The network portion of the IP address is based on the class of the IP address (shown in Table 3-15 on page 3-159). If the IP address is a Class A IP address, the first field is the network portion of the IP address. If the IP address is a Class B IP address, the first two fields are the network portion of the IP address. If the IP address is a Class C IP address, the first three fields are the network portion of the IP address. For example, if the IP address is 193.5.207.150, a Class C IP address, the network portion of the IP address is 193.5.207.

Specifying the IP address 0.0.0.0 for the **dnrsa** or **dnrsb** parameters, removes the IP address for Ethernet A (**dnrsa**) or Ethernet B (**dnrsb**).

When an IP card is entered into the database with the `ent-card` command, the IP stack parameters associated with this card are initially set with these default values:

- `:srchordr` – SRVR
- `:dnrsa` – No DNSA IP address is specified
- `:dnrsb` – No DNSB IP address is specified
- `:domain` – No domain name is specified
- `:defrouter` – No default router IP address is specified
- `:rstdomain` – No

The value of any optional parameter not specified with the `chg-ip-card` command is not changed.

The examples in this procedure are based on the sample network shown in Figure 3-3 on page 3-13 and Table 3-3 on page 3-15.

Procedure

1. Display the current IP parameters associated with card in the database by entering the `rtrv-ip-card` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
  LOC 1201
    SRCHORDR  LOCAL
    DNSA      150.1.1.1
    DNSB      -----
    DEFROUTER -----
    DOMAIN    -----

  LOC 1203
    SRCHORDR  LOCAL
    DNSA      192.1.1.40
    DNSB      -----
    DEFROUTER -----
    DOMAIN    NC.TEKELEC.COM

  LOC 1205
    SRCHORDR  SRVONLY
    DNSA      192.1.1.40
    DNSB      -----
    DEFROUTER -----
    DOMAIN    NC.TEKELEC.COM
```

To change the parameters of an IP card, the signaling link to the card and the card have to be inhibited.

2. Display the signaling link associated with the card shown in step 1 using the `rtrv-slk` command specifying the card location. For this example, enter this command.

```
rtrv-slk:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
LOC  PORT LSN          SLC TYPE  IPLIML2
1201 A   nc001          0  IPLIM  SAALTALI
```

3. Retrieve the status of the signaling link shown in step 2 using the `rept-stat-slk` command specifying the card location and signaling link port. For example, enter this command.

```
rept-stat-slk:loc=1201:port=a
```

The output lists the signaling link assigned to this card:

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK   LSN      CLLI      PST      SST      AST
1201,A nc001      ----- IS-NR      Avail     ----
Command Completed.
```

If the signaling link is in service-normal (IS-NR), go to step 4 to deactivate the signaling link. If the signaling link is out-of-service-maintenance disabled (OOS-MT-DSBLD), skip steps 4 and 5, and go to step 6 to verify the card status.

4. Deactivate the signaling link assigned to the IP card using the `rept-stat-slk` command. For example, enter this command.

```
dact-slk:loc=1201:port=a
```



CAUTION: This command impacts network performance and should only be used during periods of low traffic.

After this command has successfully completed, this message appears.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
Deactivate Link message sent to card.
```

5. Verify the new link status using the **rept-stat-slk** command. For example, enter this command.

```
rept-stat-slk:loc=1201:port=a
```

The output displays the link status as OOS-MT-DSBLD and gives off a minor alarm:

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1201,A   nc001      ----- OOS-MT-DSBLD AVAIL   ---
ALARM STATUS = * 0236 REPT-LKS:not aligned
UNAVAIL REASON = NA
Command Completed.
```

6. Verify the status of the IP card to be inhibited using the **rept-stat-card** command. For example, enter this command.

```
rept-stat-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD  VERSION  TYPE  APPL  PST      SST      AST
1201  114-000-000 DCM   IPLIM IS-NR     Active   -----
  ALARM STATUS      = No Alarms.
  BPDCM GPL         = 002-102-000
  IMT BUS A        = Conn
  IMT BUS B        = Conn
  SLK A   PST       = IS-NR      LS=nc001  CLLI=-----
  SCCP TVG RESULT  = 24 hr: -----, 5 min: -----
  SLAN TVG RESULT  = 24 hr: -----, 5 min: -----
Command Completed.
```

If the IP card to be inhibited is in service-normal (IS-NR), go to step 7 to inhibit the card. If the IP card is out-of-service-maintenance disabled (OOS-MT-DSBLD), skip steps 7 and 8, and go to step 9.

7. Inhibit the IP card using the **inh-card** command. For example, enter this command.

```
inh-card:loc=1201
```

This message should appear.

```
rlghncxa03w 04-06-28 21:18:37 GMT EAGLE5 31.10.0
Card has been inhibited.
```

8. Display the status of the IP card to verify that it is out-of-service maintenance-disabled (OOS-MT-DSBLD). Enter this command.

```
rept-stat-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD  VERSION      TYPE      APPL      PST          SST          AST
1201  114-000-000    DCM       IPLIM     OOS-MT-DSBLD Manual       -----
ALARM STATUS      = No Alarms.
BPDCM GPL         = 002-102-000
IMT BUS A         = Conn
IMT BUS B         = Conn
SLK A   PST       = IS-NR           LS=nc001  CLLI=-----
SCCP TVG RESULT  = 24 hr: -----, 5 min: -----
SLAN TVG RESULT  = 24 hr: -----, 5 min: -----
Command Completed.
```

NOTE: If the `defrouter` parameter is not specified in step 10, skip this step and go to step 10.

9. Verify that the IP address of either Ethernet A or B (the address whose network portion matches the network portion of the `defrouter` parameter value to be used in step 10) is in the IP link table by entering the `rtrv-ip-lnk` command with the card location specified in this procedure. For this example, enter this command.

```
rtrv-ip-lnk:loc=1201
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
LOC  PORT IPADDR      SUBMASK          DUPLEX SPEED MACTYPE AUTO
1201  A    192.001.001.010 255.255.255.0   ----  ---  DIX    YES
1201  B    -----          -----          ----  ---  DIX    YES
```

If the network portion of the IP address specified by the `defrouter` value does not match the network portions of either IP address displayed in this step, perform one of these actions:

- Choose another value for the `defrouter` parameter, making sure that the network portion of the new IP address matches the network portion of one of the IP addresses displayed in this step.
- Perform the “Changing an IP Link” procedure on page 3-158 and change one of the IP addresses shown in this step so that the network portion of the new IP address changed in the “Changing an IP Link” procedure matches the network portion of the IP address value for the `defrouter` parameter.

10. Change the IP stack parameters associated with an IP card in the database using the **chg-ip-card** command. For this example, enter this command.

```
chg-ip-card:loc=1201:srchordr=local:dnsa=192.1.1.40
:domain=nc.tekelec.com
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:20:37 GMT EAGLE5 31.10.0
CHG-IP-CARD: MASP A - COMPLTD
```

11. Verify the new IP parameters associated with the IP card that was changed in step 10 by entering the **rtrv-ip-card** command.

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:21:37 GMT EAGLE5 31.10.0
LOC 1201
  SRCHORDR  LOCAL
  DNSA      192.1.1.40
  DNSB      -----
  DEFROUTER -----
  DOMAIN    NC.TEKELEC.COM

LOC 1203
  SRCHORDR  LOCAL
  DNSA      192.1.1.40
  DNSB      -----
  DEFROUTER -----
  DOMAIN    NC.TEKELEC.COM

LOC 1205
  SRCHORDR  SRVROONLY
  DNSA      192.1.1.40
  DNSB      -----
  DEFROUTER -----
  DOMAIN    NC.TEKELEC.COM
```

NOTE: If step 7 was not performed, skip steps 12 and 13, and go to step 14.

12. Allow the IP card that was inhibited in step 7 by using the **alw-card** command. For example, enter this command.

```
alw-card:loc=1201
```

This message should appear.

```
rlghncxa03w 04-06-28 21:22:37 GMT EAGLE5 31.10.0
Card has been allowed.
```

13. Verify the in-service normal (IS-NR) status of the IP card using the **rept-stat-card** command. For example, enter this command.

```
rept-stat-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD  VERSION      TYPE      APPL      PST          SST          AST
1201  114-000-000    DCM       IPLIM     IS-NR        Active       -----
ALARM STATUS      = No Alarms.
BPDCM GPL         = 002-102-000
IMT BUS A         = Conn
IMT BUS B         = Conn
SLK A   PST        = IS-NR          LS=nc001  CLLI=-----
SCCP TVG RESULT   = 24 hr: -----, 5 min: -----
SLAN TVG RESULT   = 24 hr: -----, 5 min: -----
Command Completed.
```

NOTE: If step 4 was not performed, skip steps 14 and 15, and go to step 16.

14. Activate the signaling link from step 4 using the **act-slk** command. For example, enter this command.

```
act-slk:loc=1201:port=a
```

The link changes its state from OOS-MT-DSBLD (out-of-service maintenance-disabled) to IS-NR (in-service normal).

The output confirms the activation.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Activate Link message sent to card
```

15. Verify the in-service normal (IS-NR) status of the signaling link using the **rept-stat-slk** command. For example, enter this command.

```
rept-stat-slk:loc=1201:port=a
```

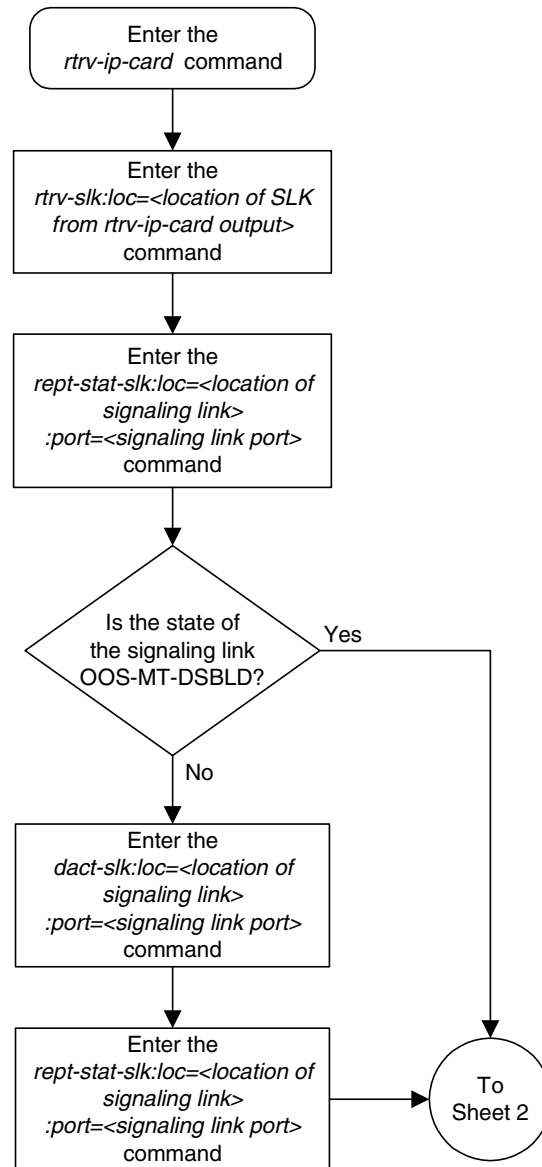
This message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK   LSN      CLLI      PST          SST          AST
1201,A nc001    -----  IS-NR        Avail       ----
Command Completed.
```

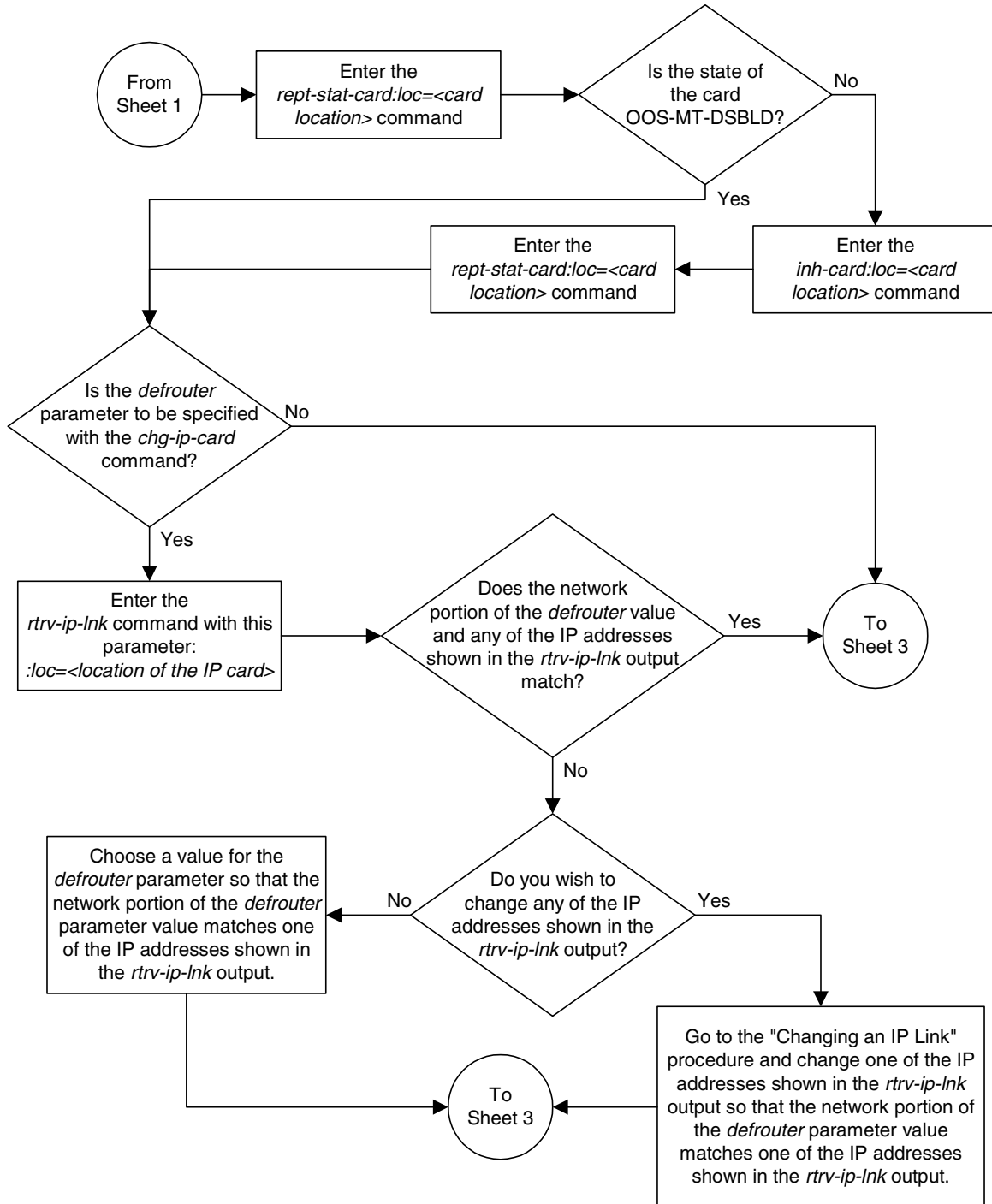
16. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

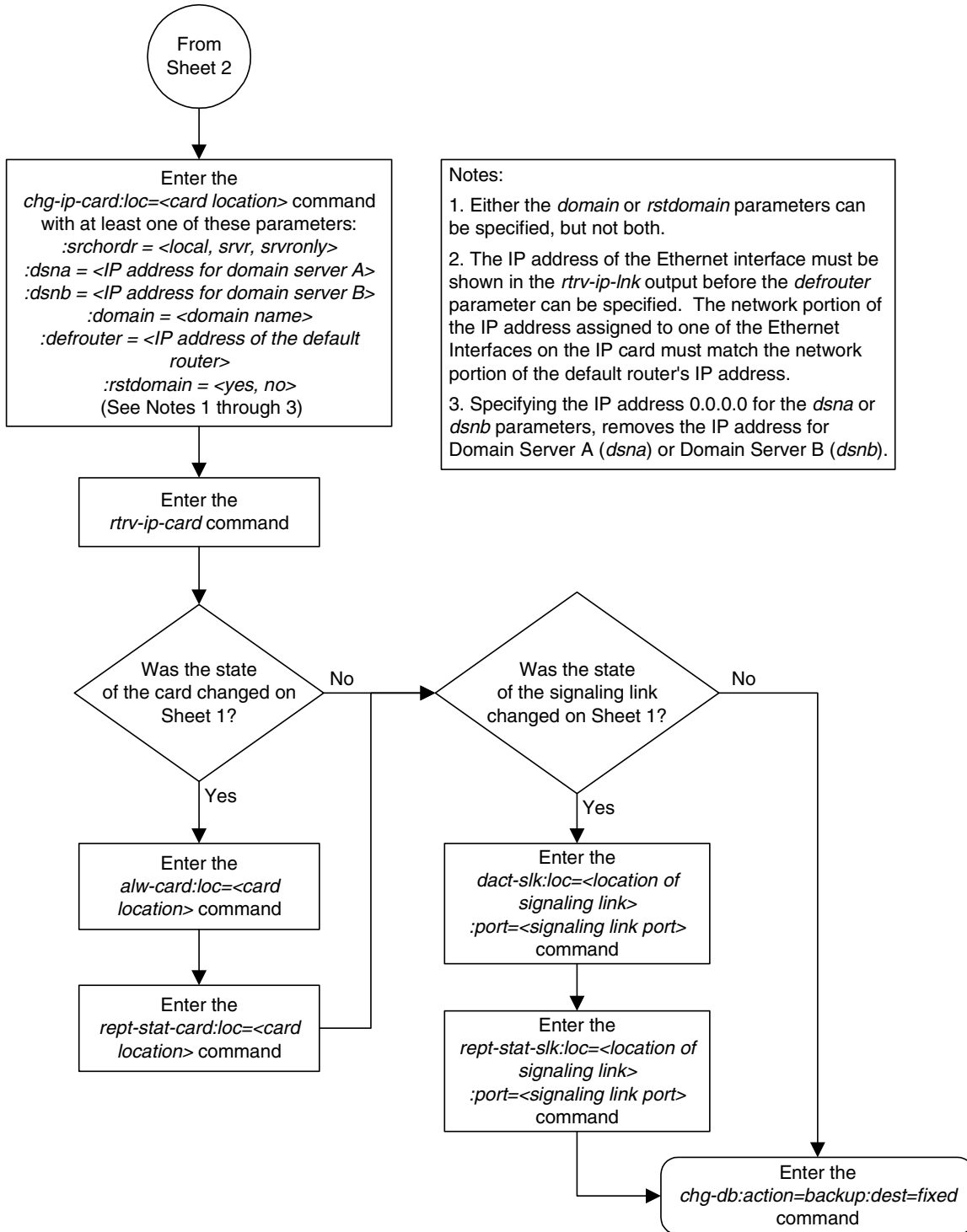
Flowchart 3-14. Changing an IP Card (Sheet 1 of 3)



Flowchart 3-14. Changing an IP Card (Sheet 2 of 3)



Flowchart 3-14. Changing an IP Card (Sheet 3 of 3)



Adding an IP Route

This procedure is used to add an IP route to the database using the `ent-ip-rte` command.

The `ent-ip-rte` command uses these parameters.

- `:loc` – The location of the IP card that the IP route will be assigned to.
- `:dest` – The IP address of the remote host or network.
- `:submask` – The subnet mask of the destination IP address.
- `:gtwy` – The IP address of the gateway or router that will send the IP data to its final destination.

There can be a maximum of 64 IP routes assigned to an IP card.

The system can contain a maximum of 1024 IP routes.

If the IP card specified by the `loc` parameter is a single-slot EDCM, the card may contain IP addresses for Ethernet A and B. If the IP card specified by the `loc` parameter is a DCM, the card can contain an IP address for Ethernet A only.

The network portion of the IP address value of the `gtwy` parameter must be the same as the network portion of the IP addresses shown for either the A or B interfaces in the `rtrv-ip-card` output.

The value of the `dest` and `gtwy` parameters cannot be 127.x.x.x (the loopback address), 0.0.0.0, or the IP addresses of the A or B interfaces on the IP card, and cannot be assigned to another IP card.

If the `dest` parameter value represents a host IP address, the value for the `submask` parameter must be 255.255.255.255. Otherwise, the `submask` parameter value identifies the network/host ID portions that must be entered when the `dest` parameter value represents a network address.

The submask is applied to the IP address which is being routed to see if it yields a route match. For example, if IP address 192.1.1.2 is being routed and the IP routing table contains these entries.

IP address	Submask	Gateway
191.1.0.0	255.255.0.0	192.168.110.250
192.0.0.0	255.0.0.0	192.168.110.251

IP routing occurs as follows:

1. The subnet mask of route 1 (255.255.0.0) is applied to the IP address being routed (192.1.1.2) with the resulting IP address of 192.1.0.0. IP address 192.1.0.0 does not match IP address 191.1.0.0 in the IP routing table, so the next route is chosen.
2. The subnet mask of route 2 (255.0.0.0) is applied to the IP address being routed (192.1.1.2) with the resulting IP address of 192.0.0.0 which matches the second route in the IP routing table, so this route is selected for routing this datagram.

See Table 3-16 for the valid input values for the **submask** and **dest** parameter combinations.

Table 3-16. Valid Subnet Mask Parameter Values

Network Class	IP Network Address Range	Valid Subnet Mask Values
A	1.0.0.0 to 127.0.0.0	255.0.0.0 (the default value for a class A IP address) 255.192.0.0 255.224.0.0 255.240.0.0 255.248.0.0 255.252.0.0 255.254.0.0 255.255.128.1
A+B	128.1.0.0 to 191.255.0.0	255.255.0.0 (the default value for a class B IP address) 255.255.192.0 255.255.224.0 255.255.240.0 255.255.248.0 255.255.252.0 255.255.254.0 255.255.255.128
A+B+C	192.0.0.0 to 223.255.255.0	255.255.255.0 (the default value for a class C IP address) 255.255.255.192 255.255.255.224 255.255.255.240 255.255.255.248 255.255.255.252

Procedure

1. Display the IP routes in the database with the **rtrv-ip-rte** command. This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLES 31.10.0
LOC  DEST          SUBMASK          GTWY
1301 128.252.10.5    255.255.255.255 140.188.13.33
1301 128.252.0.0     255.255.0.0      140.188.13.34
1301 150.10.1.1      255.255.255.255 140.190.15.3
1303 192.168.10.1    255.255.255.255 150.190.15.23
1303 192.168.0.0     255.255.255.0    150.190.15.24

IP Route table is (5 of 1024) 1% full
```

2. Display the IP cards in the database with the `rtrv-ip-card` command. This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
LOC 1212
  SRCHORDR  LOCAL
  DNSA      150.1.1.1
  DNSB      -----
  DEFROUTER 150.1.1.100
  DOMAIN    NC.TEKELEC.COM

LOC 1301
  SRCHORDR  SRVROONLY
  DNSA      140.188.13.10
  DNSB      140.190.15.28
  DEFROUTER -----
  DOMAIN    NC.TEKELEC.COM

LOC 1303
  SRCHORDR  LOCAL
  DNSA      150.190.15.1
  DNSB      -----
  DEFROUTER 150.190.15.25
  DOMAIN    NC.TEKELEC.COM
```

If the required IP card is not shown in the `rtrv-ip-card` output, perform the “Adding an IP Card” procedure on page 3-16 to add the card to the database.

Perform the “Changing an IP Card” procedure on page 3-173 and make sure that the network portion of the IP addresses assigned for the A or B interfaces of the IP card is the same as the network portion of the IP address that will be assigned to the `gtwy` parameter of the IP route

3. Add the IP route to the database using the `ent-ip-rte` command. For this example, enter this command.

```
ent-ip-rte:loc=1212:dest=132.10.175.20:submask=255.255.255.255
:gtwy=150.1.1.50
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
ENT-IP-RTE: MASP A - COMPLTD
```

4. Verify the changes using the `rtrv-ip-rte` command with the card location specified with the `ent-ip-rte` command in step 5. For this example, enter these commands.

```
rtrv-ip-rte:loc=1212
```

This is an example of the possible output.

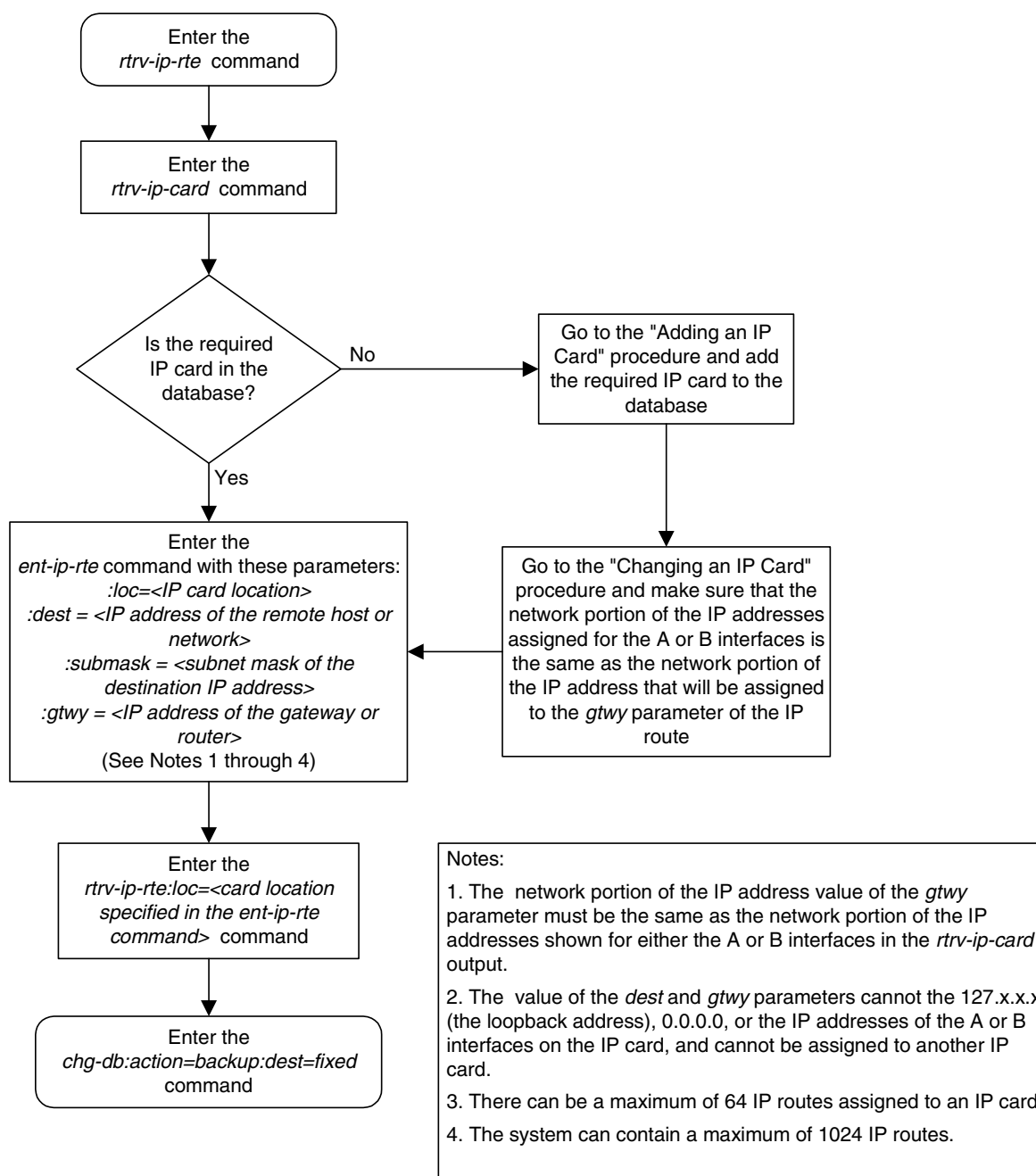
```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
LOC  DEST          SUBMASK          GTWY
1212 132.10.175.20    255.255.255.255 150.1.1.50

IP Route table is (6 of 1024) 1% full
```

5. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-15. Adding an IP Route



Removing an IP Route

This procedure is used to remove an IP route from the database using the `dlt-ip-rte` command.

The `dlt-ip-rte` command uses these parameters.

- `:loc` – The location of the IP card containing the IP route being removed.
- `:dest` – The IP address of the remote host or network assigned to the IP route being removed.
- `:force` – To remove the IP route, the IP card that the route is assigned to must be out of service, or the `force=yes` parameter must be specified with the `dlt-ip-rte` command. The `force=yes` parameter allows the IP route to be removed if the IP card is in service.



CAUTION: Removing an IP route while the IP card is still in service can result in losing the ability to route outbound IP traffic on the IP card. This can cause both TCP and SCTP sessions on the IP card to be lost.

Procedure

1. Display the IP routes in the database with the `rtrv-ip-rte` command. This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
LOC  DEST          SUBMASK          GTWY
1212 132.10.175.20    255.255.0.0      150.1.1.50
1301 128.252.10.5     255.255.255.255  140.188.13.33
1301 128.252.0.0     255.255.0.0      140.188.13.34
1301 150.10.1.1       255.255.255.255  140.190.15.3
1303 192.168.10.1     255.255.255.255  150.190.15.23
1303 192.168.0.0      255.255.255.0    150.190.15.24
```

```
IP Route table is (6 of 1024) 1% full
```

NOTE: If the IP card that the IP route is being assigned to is not shown in the `rtrv-ip-card` output in step 2, skip this step and go to step 4.

2. Verify the state of the IP card containing the IP route being removed by entering the `rept-stat-card` command and specifying the card location of the IP card. The IP card should be in the out-of-service maintenance-disabled (OOS-MT-DSBLD) in order to remove the IP route. If the IP card's state is out-of-service maintenance-disabled, the entry `OOS-MT-DSBLD` is shown in the `PST` column of the `rept-stat-card` output. For this example, enter this command.

```
rept-stat-card:loc=1301
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD  VERSION      TYPE      APPL      PST          SST          AST
1301  114-000-000    DCM       IPLIM     IS-NR        Active       -----
ALARM STATUS      = No Alarms.
BPDCM GPL         = 002-102-000
IMT BUS A         = Conn
IMT BUS B         = Conn
SLK A   PST        = IS-NR          LS=nc001  CLLI=-----
SCCP TVG RESULT   = 24 hr: -----, 5 min: -----
SLAN TVG RESULT   = 24 hr: -----, 5 min: -----
Command Completed.
```

NOTE: If the output of step 2 shows that the IP card's state is not `OOS-MT-DSBLD`, and you do not wish to change the state of the IP card, skip step 3 and go to step 4.

3. Change the IP card's state to `OOS-MT-DSBLD` using the `inh-card` command and specifying the card location of the IP card. For this example, enter these commands.

```
inh-card:loc=1301
```

When this command has successfully completed, this message appears.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
Card has been inhibited.
```

4. Remove the IP route from the database using the `dlt-ip-rte` command. If the state of the IP card is not `OOS-MT-DSBLD`, the `force=yes` parameter must be specified with the `dlt-ip-rte` command. For this example, enter this command.

```
dlt-ip-rte:loc=1301:dest=128.252.0.0
```



CAUTION: Removing an IP route while the IP card is still in service can result in losing the ability to route outbound IP traffic on the IP card. This can cause both TCP and SCTP sessions on the IP card to be lost.

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
DLT-IP-RTE: MASP A - COMPLTD
```

5. Verify the changes using the `rtrv-ip-rte` command. This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
LOC  DEST          SUBMASK          GTWY
1212 132.10.175.20    255.255.0.0     150.1.1.50
1301 128.252.10.5     255.255.255.255 140.188.13.33
1301 150.10.1.1       255.255.255.255 140.190.15.3
1303 192.168.10.1     255.255.255.255 150.190.15.23
1303 192.168.0.0      255.255.0.0     150.190.15.24
```

```
IP Route table is (5 of 1024) 1% full
```

NOTE: If the IP card containing the IP route that was removed from the database does not contain other IP routes, skip step 6 and go to step 7.

6. Place the IP card back into service by using the `alw-card` command. For example, enter this command.

```
alw-card:loc=1301
```

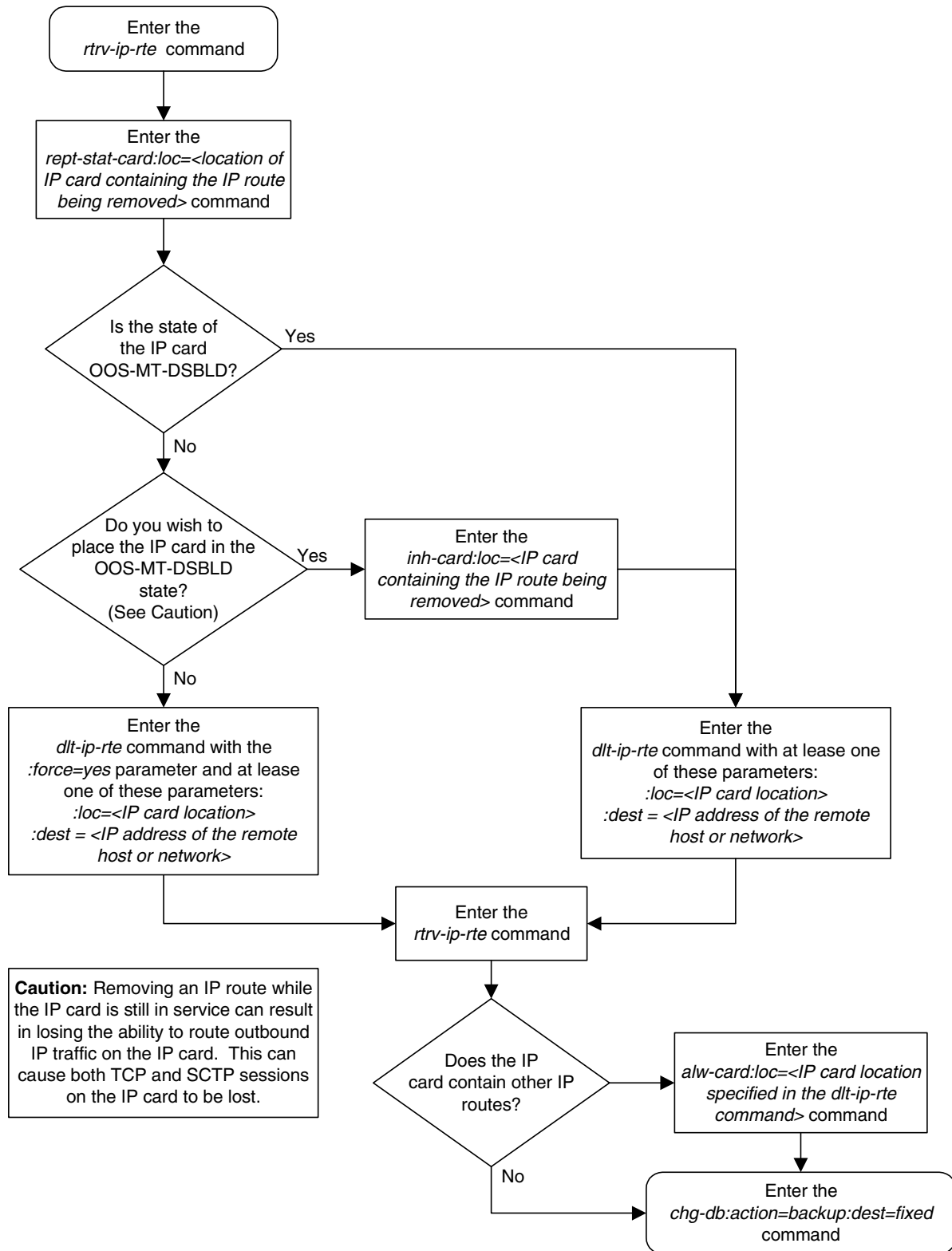
This message should appear.

```
rlghncxa03w 04-06-28 21:22:37 GMT EAGLE5 31.10.0
Card has been allowed.
```

7. Back up the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-16. Removing an IP Route



Adding an Application Socket

This procedure is used to add an application socket to the database using the `ent-appl-sock` command. The combination of local host, local TCP port, remote host and remote TCP port defines an application socket.

The `ent-appl-sock` command uses these parameters.

- :sname**— The name assigned to the socket. Valid socket names can contain up to 15 alphanumeric characters where the first character is a letter and the remaining characters are alphanumeric characters. The **sname** parameter value is not case-sensitive.
- :lhost** – Local Hostname. The logical name assigned to the local host device.
- :lport** – The TCP port number for the Local host.
- :rhost** – Remote Hostname. The logical name assigned to the remote host device.
- :rport** – The TCP port number of the remote host.
- :port** – The signaling link port on the IP card. If a signaling link port is not specified for a socket when it is entered, the socket defaults to the A port. If the card's application is `iplim` or `iplimi`, and the card is a dual-slot DCM, the values for the **port** parameter can be only **a** or **b**. If the card's application is `iplim` or `iplimi`, and the card is a single-slot EDCM, the values for the **port** parameter can be **a**, **a1**, **a2**, **a3**, **b**, **b1**, **b2**, or **b3**. If the IP card's application is `ss7ipgw` or `ipgwi`, only **port=a** can be specified.

For the `ss7ipgw` and `ipgwi` applications, there is a maximum of 50 connections (associations plus sockets) for each local host.

For the `iplim` and `iplimi` applications, each IP card can have one socket for each signaling link assigned to the card. Dual-slot DCMs can have a maximum of two sockets. Single-slot EDCMs can have a maximum of 8 sockets.

The system can contain a maximum of 4000 connections (associations plus sockets).

The socket name must be unique (not already used).

The socket table, which contains both the socket and association data, contains fields whose values are not assigned using the `ent-appl-sock` command. When a socket is added to the database, these fields receive their default values. If a different value is desired, the `chg-appl-sock` command must be used. These fields and their default values are:

<code>open=no</code>	<code>dcmps=10</code>
<code>alw=no</code>	<code>rexmit=fixed</code>
<code>server=yes</code>	<code>rtt=60</code>

The value of the **lhost** and **rhost** parameters is a text string of up to 60 characters, with the first character being a letter. The command line on the terminal can contain up to 150 characters. If the host name is too long to fit on the **ent-appl-sock** command line, go to the “Changing an Application Socket” procedure on page 3-205 to complete the entry of the host name.

The IP address of the local host (**lhost** parameter) must be shown in the **rtrv-ip-lnk** output.

The signaling link being assigned to the socket must be out of service. This state is shown in the **rept-stat-slk** output with the entries **OOS-MT** in the **PST** field and **Unavail** in the **SST** field.

If the card’s application is either IPLIM or IPLIMI:

- The **iplim12** parameter value of the signaling link assigned to the socket must be **saaltali**.
- The signaling link being assigned to the socket must be out of service. This state is shown in the **rept-stat-slk** output with the entries **OOS-MT** in the **PST** field and **Unavail** in the **SST** field.
- If the socket is being opened in this procedure with the **chg-appl-sock** command and the **open=yes** parameter, the signaling link assigned to the socket must be in the database and the **iplim12** parameter value of the signaling link assigned to the socket must be **saaltali**.

If the card’s application is either SS7IPGW or IPGWI, the signaling link being assigned to the socket must be in service. This state is shown in the **rept-stat-slk** output with the entries **IS-NR** in the **PST** field and **Avail** in the **SST** field.

The B Ethernet interface of the IP card can be used only if the IP card is a single-slot EDCM.

If the socket is being activated in this procedure with the **chg-appl-sock** command, the socket must contain values for the **lhost**, **lport**, **rhost**, and **rport** parameters.

Canceling the RTRV-APPL-SOCK Command

Because the `rtrv-appl-sock` command used in this procedure can output information for a long period of time, the `rtrv-appl-sock` command can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-appl-sock` command can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-appl-sock` command was entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-appl-sock` command was entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-appl-sock` command was entered, from another terminal other than the terminal where the `rtrv-appl-sock` command was entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current application socket information in the database by entering the `rtrv-appl-sock` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:14:37 GMT EAGLE5 31.10.0
SNAME kchlr11201
  PORT  A
  LHOST ipnode1-1201
  RHOST kc-hlr1
  LPORT 7000          RPORT 7000
  SERVER YES          DCMP5 1
  REXMIT FIXED        RTT 60
  OPEN  YES           ALW  NO

IP Appl Sock/Assoc table is (3 of 4000) 1% full
```

- Verify that the local host name to be assigned to the socket is in the database by using the **rtrv-ip-host** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
```

IPADDR	HOST
192.1.1.10	IPNODE1-1201
192.1.1.12	IPNODE1-1203
192.1.1.14	IPNODE1-1205
192.1.1.20	IPNODE2-1201
192.1.1.22	IPNODE2-1203
192.1.1.24	IPNODE2-1205
192.1.1.30	KC-HLR1
192.1.1.32	KC-HLR2
192.1.1.50	DN-MS1
192.1.1.52	DN-MS2

IP Host table is (10 of 512) 2% full

If the required hostname is not in the database, add the IP host name using the "Adding an IP Host" on page 3-153 procedure.

- Display the IP links in the database by entering the **rtrv-ip-lnk** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
```

LOC	PORT	IPADDR	SUBMASK	DUPLEX	SPEED	MACTYPE	AUTO
1201	A	192.001.001.010	255.255.255.0	----	---	DIX	YES
1203	A	192.001.001.012	255.255.255.0	----	---	DIX	YES
1205	A	192.001.001.014	255.255.255.0	FULL	100	DIX	NO

If the required IP link is not in the database, add the IP link using the "Changing an IP Link" on page 3-158 procedure.

- Display the application running on the IP card shown in step 3 using the **rept-stat-card** command specifying the location of the IP card. For this example, enter this command.

```
rept-stat-card:loc=1203
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
```

CARD	VERSION	TYPE	APPL	PST	SST	AST
1203	114-000-000	DCM	IPLIM	IS-NR	Active	-----
ALARM STATUS		= No Alarms.				
BPDCM GPL		= 002-102-000				
IMT BUS A		= Conn				
IMT BUS B		= Conn				
SLK A	PST	= IS-NR	LS=nc001	CLLI=-----		
SCCP TVG RESULT		= 24 hr: -----, 5 min: -----				
SLAN TVG RESULT		= 24 hr: -----, 5 min: -----				

Command Completed.

NOTE: If the card's application is SS7IPGW or IPGWI, shown in the **APPL** column in the **rept-stat-card** output in step 4, skip steps 5, 6, 7, and 8, and go to step 9.

5. Display the signaling link referenced by the IP link that will be assigned to the socket by entering the **rtrv-slk** command and specifying the location and port of the IP link. For this example, enter this command.

```
rtrv-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-19 21:17:04 GMT EAGLE5 31.10.0
LOC  PORT LSN          SLC TYPE   IPLIML2
1203 A    e5e6a          1  IPLIM    SAALTALI
```

When the IP card's application is either IPLIM or IPLIMI, the **ipliml2** parameter value for the signaling link assigned to the socket must be **saaltali**. If the **ipliml2** parameter is not **saaltali**, remove the signaling link using the "Removing an IP Signaling Link" procedure on page 3-115. Add the signaling link back into the database with the **ipliml2=saaltali** parameter, and without activating the signaling link, using the "Adding an IP Signaling Link" procedure on page 3-82.

NOTE: If the "Adding an IP Signaling Link" procedure on page 3-82 was not performed in step 5, skip steps 6, 7, and 8, and go to step 9.

6. Display the status of the signaling link shown in step 5 using the **rept-stat-slk** command specifying the card location and signaling link port. For example, enter this command.

```
rept-stat-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK   LSN      CLLI      PST      SST      AST
1203,A e5e6a    -----  IS-NR    Avail    ----
Command Completed.
```

NOTE: If the primary state (PST) of the signaling link is **oos-MT** and the secondary state (SST) is **Unavail**, skip steps 7 and 8, and go to step 9.

- 7 Deactivate the signaling link from step 6 using the **dact-slk** command. For example, enter this command.

```
dact-slk:loc=1203:port=a
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Deactivate Link message sent to card
```

8. Verify the status of the signaling link using the **rept-stat-slk** command. For example, enter this command.

```
rept-stat-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1203,A   e5e6a     -----  OOS-MT   Unavail  ----
Command Completed.
```

9. Add application socket information to the database by entering the **ent-appl-sock** command. For example, enter this command.

```
ent-appl-sock:sname=kchlr11203:lhost="ipnode-1203"
:lport=7005:rhost="kc-hlr1":rport=7005:port=a
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
ENT-APPL-SOCK: MASP A - COMPLTD
```

NOTE: If the socket added in step 9 is not being activated in this procedure, skip step 10 and go to step 11.

10. Activate the socket added in step 9 by entering the **chg-appl-sock** command with the socket name specified in step 9 and the **open=yes** and **alw=yes** parameters. For example, enter this command.

```
chg-appl-sock:sname=kchlr11203:open=yes:alw=yes
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
CHG-APPL-SOCK: MASP A - COMPLTD
```

NOTE: If the card's application is SS7IPGW or IPGWI, skip steps 11 and 12, and go to step 13.

11. Activate the signaling link assigned to the socket using the **act-slk** command. For example, enter this command.

```
act-slk:loc=1203:port=a
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Activate Link message sent to card
```

12. Verify the status of the signaling link using the **rept-stat-slk** command. For example, enter this command.

```
rept-stat-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1203,A   e5e6a     -----  IS-NR    Avail    ----
Command Completed.
```

13. Verify the new application socket information in the database by entering the **rtrv-appl-sock** command with the socket name specified in step 9. For this example, enter this command.

```
rtrv-appl-sock:sname=kchlr11203
```

The following is an example of the possible output.

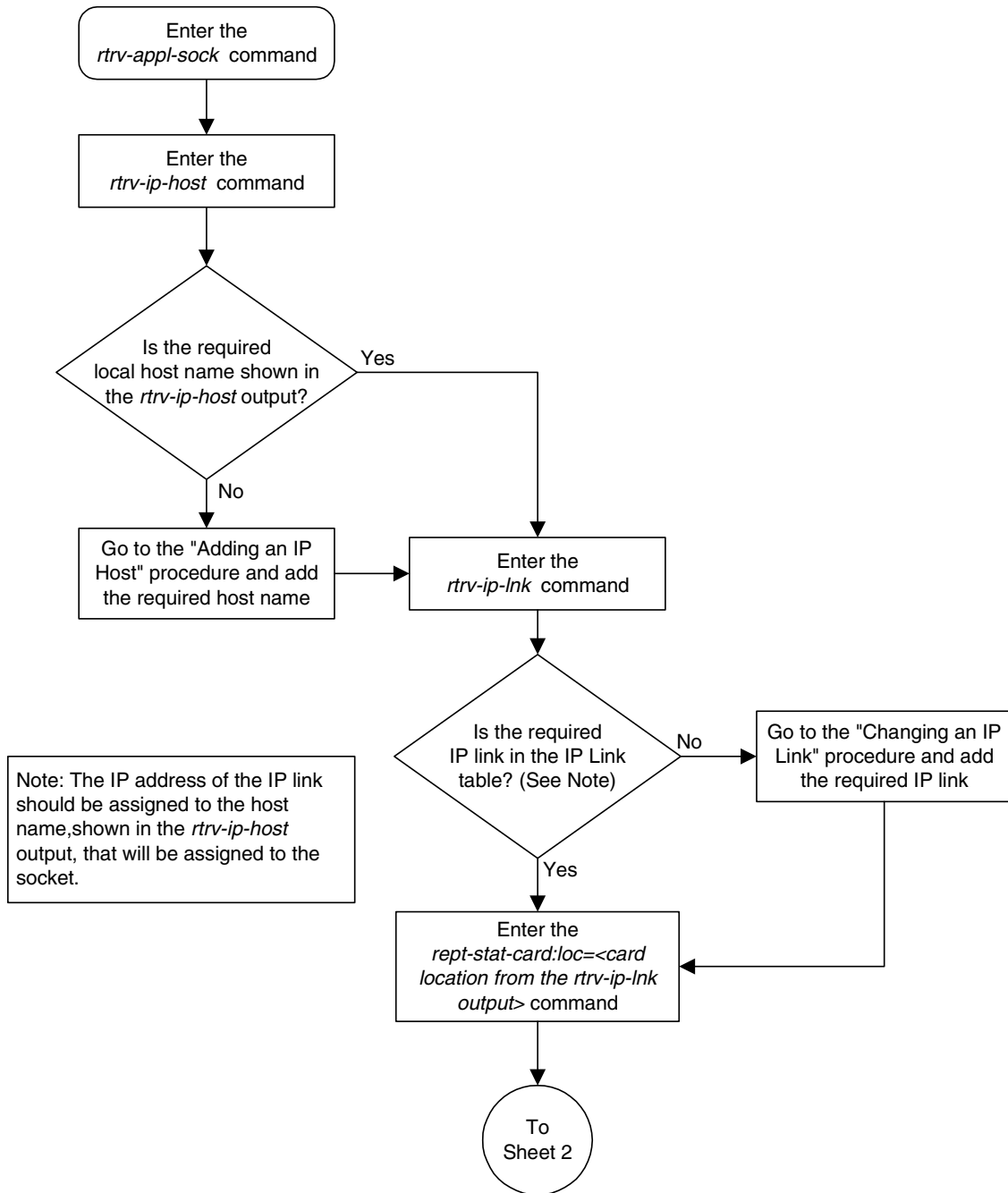
```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SNAME kchlr11203
  PORT  A
  LHOST ipnode1-1203
  RHOST kc-hlr1
  LPORT 7005      RPORT 7005
  SERVER YES      DCMP5 10
  REXMIT FIXED    RTT 60
  OPEN  YES      ALW  YES

IP Appl Sock/Assoc table is (3 of 4000) 1% full
```

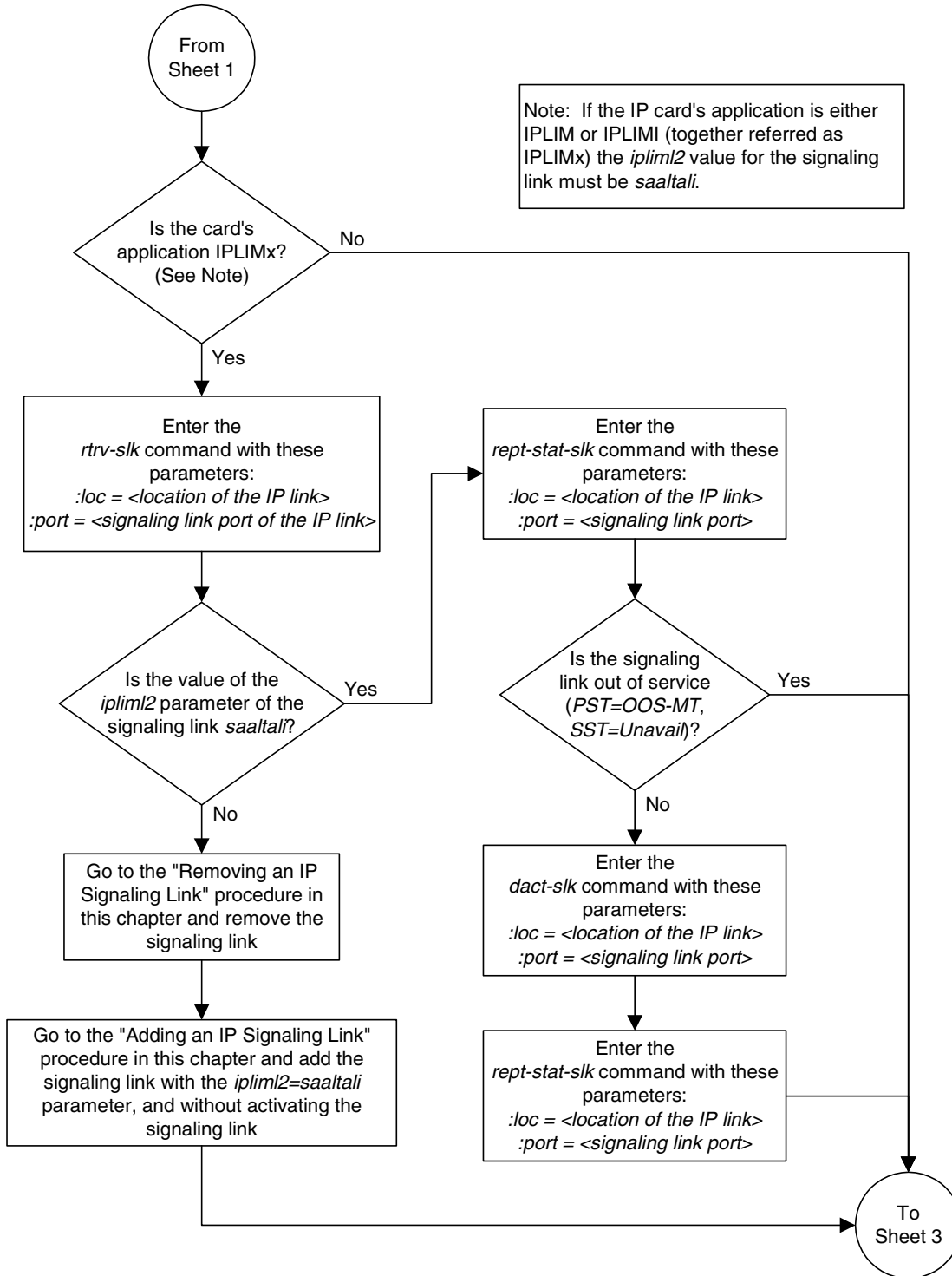
14. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

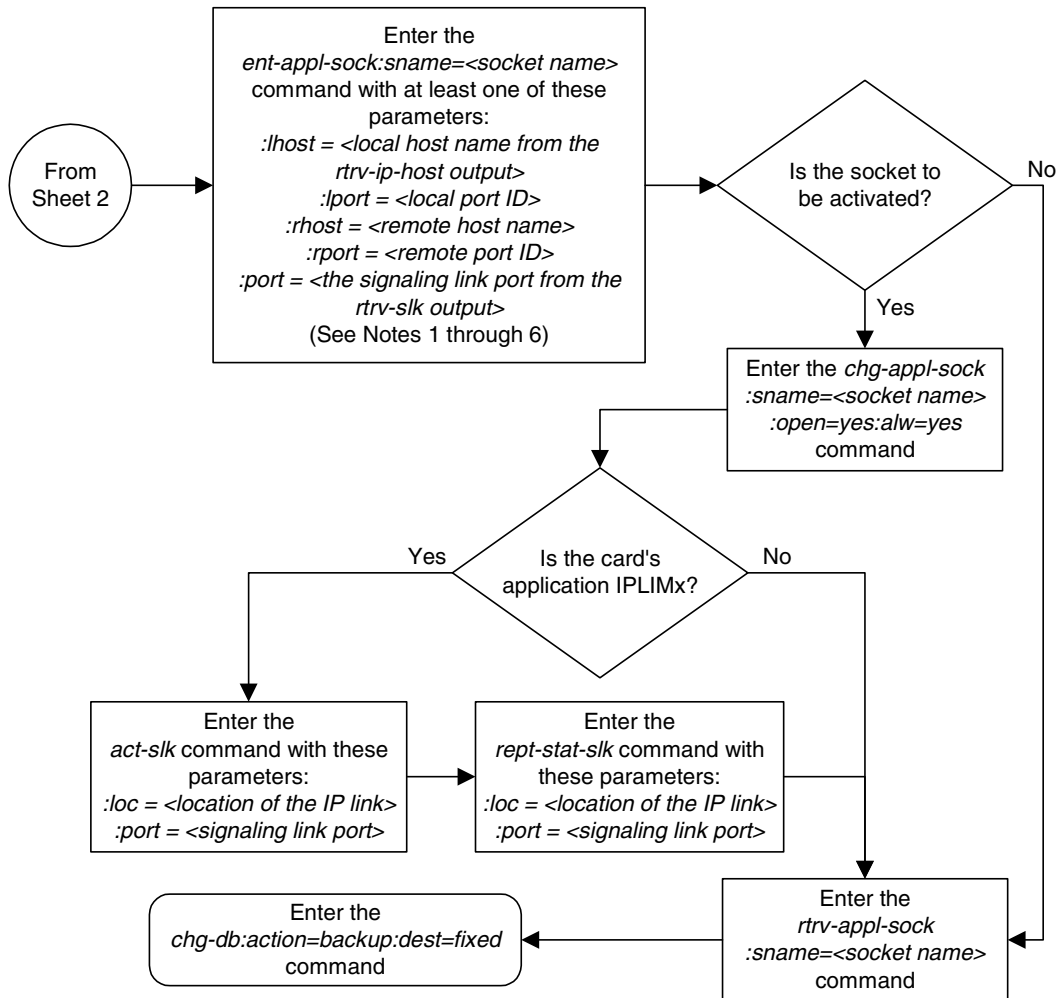
Flowchart 3-17. Adding an Application Socket (Sheet 1 of 3)



Flowchart 3-17. Adding an Application Socket (Sheet 2 of 3)



Flowchart 3-17. Adding an Application Socket (Sheet 3 of 3)



- Notes:
1. If the card containing the signaling link is a DCM, the B Ethernet interface cannot be used. Single-slot EDCMs can use the B Ethernet interface.
 2. Each local host on a card running either the *ss7ipgw* or *ipgwi* applications can contain a maximum of 50 connections (associations plus sockets).
 3. The system can contain a maximum of 4000 connections (associations plus sockets).
 4. Cards running either the *iplim* or *iplimi* applications can have only one connection for each signaling link port and a maximum of two connections for each card, if the card is a dual-slot DCM. If the card is a single-slot EDCM, the card may contain a maximum of eight connections.
 5. The value of the *lhost* and *rhost* parameters is a text string of up to 60 characters, with the first character being a letter. The command line on the terminal can contain up to 150 characters. If the host name is too long to fit on the *ent-appl-sock* command line, go to the "Changing an Application Socket" procedure to complete the entry of the host name.
 6. If the new socket is to be activated in this procedure with the *chg-appl-sock* command, the socket must contain values for the *lhost*, *rhost*, *lport*, and *rport* parameters.

Removing an Application Socket

This procedure is used to remove an application socket from the database using the `dlt-appl-sock` command.

The `dlt-appl-sock` command has only one parameter, `:sname` – the socket name being removed.

The `open` parameter must be set to `no` before the application socket can be removed. Use the `chg-appl-sock` command to change the value of the `open` parameter.

Canceling the RTRV-APPL-SOCK Command

Because the `rtrv-appl-sock` command used in this procedure can output information for a long period of time, the `rtrv-appl-sock` command can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-appl-sock` command can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-appl-sock` command was entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-appl-sock` command was entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-appl-sock` command was entered, from another terminal other than the terminal where the `rtrv-appl-sock` command was entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current application socket information in the database by entering the `rtrv-appl-sock` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
SNAME kchlr11201
  PORT  A
  LHOST ipnode1-1201
  RHOST kc-hlr1
  LPORT 7000          RPORT 7000
  SERVER YES          DCMPS 1
  REXMIT FIXED        RTT 60
  OPEN  YES           ALW  NO
```



```
SNAME kchlr11203
PORT A
LHOST ipnode1-1203
RHOST kc-hlr1
LPORT 7005          RPORT 7005
SERVER YES          DCMPS 10
REXMIT FIXED        RTT 60
OPEN NO             ALW NO
```

IP Appl Sock/Assoc table is (3 of 4000) 1% full

NOTE: If the application socket information shows the value of the open parameter in the socket being removed from the database is no, skip this step and go to step 3.

2. Change the open parameter value in the socket being removed from the database using the `chg-app1-sock` command with the `open=no` parameter.



CAUTION: Setting the open parameter value to no could cause traffic to be lost.

For example, enter this command.

```
chg-app1-sock:sname=kchlr11201:open=no
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
CHG-APPL-SOCK: MASP A - COMPLTD
```

3. Remove the application socket information from the database by entering the `dl1-app1-sock` command. For example, enter this command.

```
dl1-app1-sock:sname=kchlr11201
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
DLT-APPL-SOCK: MASP A - COMPLTD
```

4. Verify the new application socket information in the database by entering the `rtrv-app1-sock` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:18:37 GMT EAGLE5 31.10.0
SNAME kchlr11203
PORT A
LHOST ipnode1-1203
RHOST kc-hlr1
LPORT 7005          RPORT 7005
SERVER YES          DCMPS 10
REXMIT FIXED        RTT 60
OPEN NO             ALW NO
```

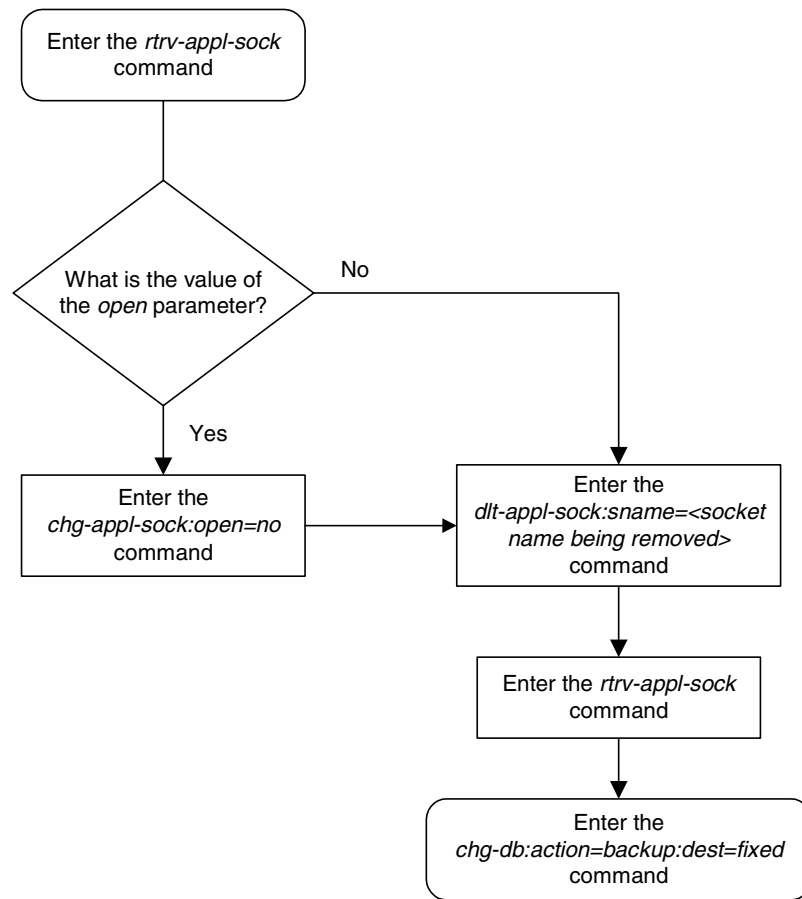
IP Appl Sock/Assoc table is (3 of 4000) 1% full

- Back up the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```

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

Flowchart 3-18. Removing an Application Socket



Changing an Application Socket

This procedure is used to change an application socket in the database using the **chg-appl-sock** command.

The **chg-appl-sock** command uses these parameters.

- :sname** – Socket Name.
- :lhost** – Local Hostname. The logical name assigned to the local host device.
- :lport** – The TCP port number for the Local host.
- :rhost** – Remote Hostname. The logical name assigned to the remote host device.
- :rport** – The TCP port number of the remote host.
- :port** – The signaling link port on the IP card. If the card's application is **iplim** or **iplimi**, and the card is a dual-slot DCM, the values for the **port** parameter can be only **a** or **b**. If the card's application is **iplim** or **iplimi**, and the card is a single-slot EDCM, the values for the **port** parameter can be **a**, **a1**, **a2**, **a3**, **b**, **b1**, **b2**, or **b3**. If the IP card's application is **ss7ipgw** or **ipgwi**, only **port=a** can be specified.
- :server** – Server Role. The role of the local socket in the Client/Server relationship.
- :open** – Socket State. Indicates to the connection manager software to open the socket if the socket is operational.
- :alw** – Connection State. Indicates to the connection manager software if the socket is allowed to carry SS7 traffic.
- :dcmps** – DCM Parameter Set. The DCM parameter set that will be used by the socket.
- :reemit** – Indicates the retransmission mode that the user wants the TCP stack to use for this socket.
- :rtt** – Indicates the measured or expected round trip time (RTT) of the socket in milliseconds.

For more information on the **reemit** and **rtt** parameters, go to the "Configuring IP Socket Retransmission Parameters" procedure on page 3-217.

The **open** parameter must be set to **no** before changes can be made to **server**, **lhost**, **lport**, **rhost**, **rport**, **rtt**, **reemit**, and **port** parameters.

The **open** parameter must be changed with a separate **chg-appl-sock** command. The **open** parameter can not be on a command line that has **server**, **lhost**, **lport**, **rhost**, and **rport** parameters.

At least one optional parameter is required.

For the **ss7ipgw** and **ipgwi** applications, there is a maximum of 50 connections (associations plus sockets) for each local host.

For the **iplim** and **iplimi** applications, each IP card can have one socket for each signaling link assigned to the card. Dual-slot DCMs can have a maximum of two sockets. Single-slot EDCM cards can have a maximum of eight sockets.

The system can contain a maximum of 4000 connections (associations plus sockets).

The value of the **lhost** and **rhost** parameters is a text string of up to 60 characters, with the first character being a letter.

The command input is limited to 150 characters, including the hostname.

To set the **open** parameter value to **yes**, the socket specified by the **sname** parameter must contain values for the **lhost**, **lport**, **rhost**, and **rport** parameters.

The **rtt** parameter cannot be specified with the **rexmit=bsd** parameter.

When the **rexmit=fixed** or **rexmit=mod** parameters are specified, the **rtt** parameter must be specified.

The IP address of the local host (**lhost** parameter) must be shown in the **rtrv-ip-lnk** output.

If the card's application is either IPLIM or IPLIMI:

- The **iplim12** parameter value of the signaling link assigned to the socket must be **saaltali**.
- The signaling link being assigned to the socket must be out of service. This state is shown in the **rept-stat-slk** output with the entries **OOS-MT** in the **PST** field and **Unavail** in the **SST** field.
- If the socket is being opened in this procedure with the **chg-appl-sock** command and the **open=yes** parameter, the signaling link assigned to the socket must be in the database and the **iplim12** parameter value of the signaling link assigned to the socket must be **saaltali**.

If the card's application is either SS7IPGW or IPGWI, the signaling link being assigned to the socket must be in service. This state is shown in the **rept-stat-slk** output with the entries **IS-NR** in the **PST** field and **Avail** in the **SST** field.

The B Ethernet interface of the IP card can be used only if the IP card is a single-slot EDCM.

If the socket being changed is a client socket, shown in the **rtrv-appl-sock** output with the entry **NO** in the **SERVER** field, the socket's **lhost** and **lport** values cannot match the values of any open socket.

If the socket being changed is a server socket, shown in the **rtrv-appl-sock** output with the entry **YES** in the **SERVER** field, the socket's **lhost** and **lport** values cannot match the values of any open client socket.

Canceling the RTRV-APPL-SOCK Command

Because the `rtrv-appl-sock` command used in this procedure can output information for a long period of time, the `rtrv-appl-sock` command can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-appl-sock` command can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-appl-sock` command was entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-appl-sock` command was entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-appl-sock` command was entered, from another terminal other than the terminal where the `rtrv-appl-sock` command was entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current application socket information in the database by entering the `rtrv-appl-sock` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
SNAME kchlr11201
  PORT  A
  LHOST ipnode1-1201
  RHOST kc-hlr1
  LPORT 7000          RPORT 7000
  SERVER YES          DCMP5 1
  REXMIT FIXED        RTT 60
  OPEN  YES           ALW  NO

SNAME kchlr11203
  PORT  A
  LHOST ipnode1-1203
  RHOST kc-hlr1
  LPORT 7005          RPORT 7005
  SERVER YES          DCMP5 10
  REXMIT FIXED        RTT 60
  OPEN  YES           ALW  NO

IP Appl Sock/Assoc table is (3 of 4000) 1% full
```

NOTE: To change the values of these parameters: `server`, `lhost`, `lport`, `rhost`, `rport`, `rtt`, `rexmit`, or `rport`, the value of the `open` parameter must be `no`. If the values of any of these parameters are being changed and the `open` parameter value for the socket being changed is `no`, skip this step and go to step 3.

NOTE: If only the values of the `alw`, `open`, or `dcmps` parameters are being changed, skip steps 2 through 9, and go to step 10.

2. Change the value of the `open` parameter to `no` using the `chg-appl-sock` command with the `open=no` parameter. For example, enter this command.

```
chg-appl-sock:sname=kchlr11201:open=no
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
CHG-APPL-SOCK: MASP A - COMPLTD
```

NOTE: If the local host name assigned to the socket is not being changed, skip this step and go to step 4.

3. Verify that the local host name to be assigned to the socket is in the database by using the `rtrv-ip-host` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

IPADDR          HOST
192.1.1.10      IPNODE1-1201
192.1.1.12      IPNODE1-1203
192.1.1.14      IPNODE1-1205
192.1.1.20      IPNODE2-1201
192.1.1.22      IPNODE2-1203
192.1.1.24      IPNODE2-1205
192.1.1.30      KC-HLR1
192.1.1.32      KC-HLR2
192.1.1.50      DN-MS1
192.1.1.52      DN-MS2
```

```
IP Host table is (10 of 512) 2% full
```

If the required hostname is not in the database, add the IP host name using the “Adding an IP Host” on page 3-153 procedure.

NOTE: If the `port` parameter value is not being changed, skip this step and go to step 5.

4. Display the IP links in the database by entering the `rtrv-ip-lnk` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
LOC  PORT IPADDR          SUBMASK          DUPLEX SPEED MACTYPE AUTO
1201  A    192.001.001.010      255.255.255.0    ----  ---  DIX    YES
1203  A    192.001.001.012      255.255.255.0    ----  ---  DIX    YES
1205  A    192.001.001.014      255.255.255.0    FULL  100  DIX    NO
```

If the required IP link is not in the database, add the IP link using the “Changing an IP Link” on page 3-158 procedure.

5. Display the application running on the IP card shown in step 4 using the `rept-stat-card` command specifying the location of the IP card. For this example, enter this command.

```
rept-stat-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD  VERSION  TYPE  APPL  PST  SST  AST
1201  114-000-000  DCM   IPLIM  IS-NR  Active  -----
ALARM STATUS      = No Alarms.
BPDCM GPL         = 002-102-000
IMT BUS A         = Conn
IMT BUS B         = Conn
SLK A  PST         = IS-NR      LS=nc001  CLLI=-----
SCCP TVG RESULT   = 24 hr: -----, 5 min: -----
SLAN TVG RESULT   = 24 hr: -----, 5 min: -----
Command Completed.
```

NOTE: If the card’s application is `SS7IPGW` or `IPGWI`, shown in the `APPL` column in the `rept-stat-card` output in step 5, skip steps 6, 7, 8, and 9, and go to step 10.

6. Display the signaling link referenced by the IP link that will be assigned to the socket by entering the `rtrv-slk` command and specifying the location and port of the IP link. For this example, enter this command.

```
rtrv-slk:loc=1201:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-19 21:17:04 GMT EAGLE5 31.10.0
LOC  PORT LSN          SLC TYPE  IPLIML2
1203  A    e5e6a         1  IPLIM  SAALTALI
```

When the IP card’s application is either `IPLIM` or `IPLIMI`, the `ipliml2` parameter value for the signaling link assigned to the socket must be `saaltali`. If the `ipliml2` parameter is not `saaltali`, remove the signaling link using the “Removing an IP Signaling Link” procedure on page 3-115. Add the signaling link back into the database with the `ipliml2=saaltali` parameter, and without activating the signaling link, using the “Adding an IP Signaling Link” procedure on page 3-82.

NOTE: If the “Adding an IP Signaling Link” procedure on page 3-82 was not performed in step 6, skip steps 7, 8, and 9, and go to step 10.

7. Display the status of the signaling link shown in step 6 using the **rept-stat-slk** command specifying the card location and signaling link port. For example, enter this command.

```
rept-stat-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1203,A   e5e6a     -----  IS-NR    Avail    ----
Command Completed.
```

NOTE: If the primary state (PST) of the signaling link is **OOS-MT** and the secondary state (SST) is **Unavail**, skip steps 8 and 9, and go to step 10.

8. Deactivate the signaling link from step 7 using the **act-slk** command. For example, enter this command.

```
dact-slk:loc=1203:port=a
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Deactivate Link message sent to card
```

9. Verify the status of the signaling link using the **rept-stat-slk** command. For example, enter this command.

```
rept-stat-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1203,A   e5e6a     -----  OOS-MT   Unavail  ----
Command Completed.
```

10. Change the application socket information in the database by using the **chg-appl-sock** command. For example, enter this command.

```
chg-appl-sock:sname=kchlr11201:rhost="kc-kc-kc":alw=yes
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
CHG-APPL-SOCK: MASP A - COMPLTD
```

NOTE: If step 2 was not performed in this procedure, skip step 11 and go to step 12.

11. Change the **open** parameter value back to **yes** by using the **chg-appl-sock** command. For example, enter this command.

```
chg-appl-sock:sname=kchlr11201:open=yes
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:18:37 GMT EAGLE5 31.10.0
CHG-APPL-SOCK: MASP A - COMPLTD
```

NOTE: If the card's application is SS7IPGW or IPGWI, skip steps 12 and 13, and go to step 14.

12. Activate the signaling link assigned to the socket using the **act-slk** command. For example, enter this command.

```
act-slk:loc=1203:port=a
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Activate Link message sent to card
```

13. Verify the status of the signaling link using the **rept-stat-slk** command. For example, enter this command.

```
rept-stat-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1203,A   e5e6a    -----  IS-NR    Avail    ----
Command Completed.
```

14. Verify the new application socket information in the database by entering the **rtrv-appl-sock** command with the socket name specified in step 10. For this example, enter this command.

```
rtrv-appl-sock:sname=kchlr11201
```

The following is an example of the possible output.

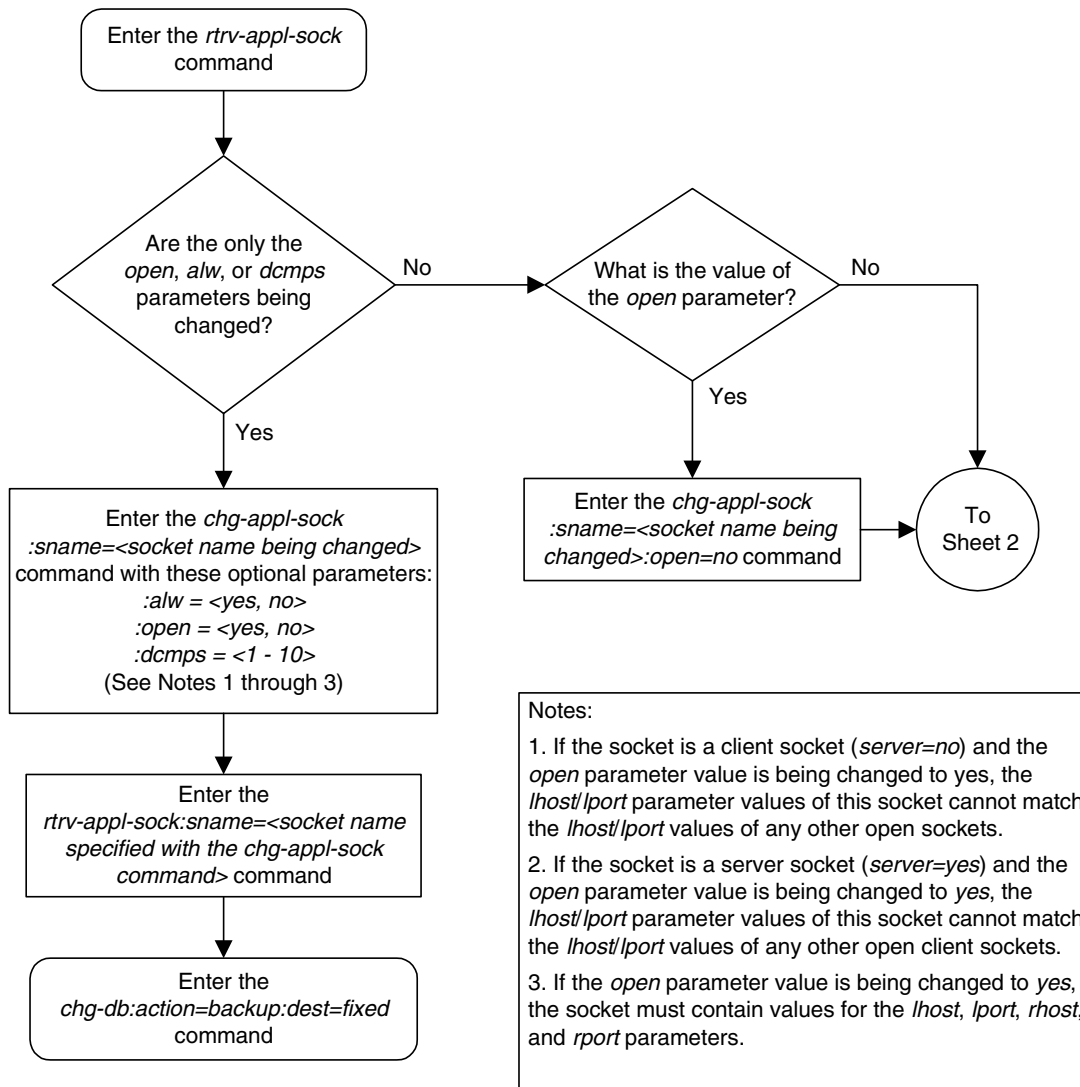
```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
SNAME kchlr11201
      PORT    A
      LHOST   ipnode1-1201
      RHOST   kc-kc-kc
      LPORT   7000      RPORT    7000
      SERVER  YES      DCMPS    1
      REXMIT  FIXED    RTT      60
      OPEN    YES      ALW      YES

IP Appl Sock/Assoc table is (3 of 4000) 1% full
```

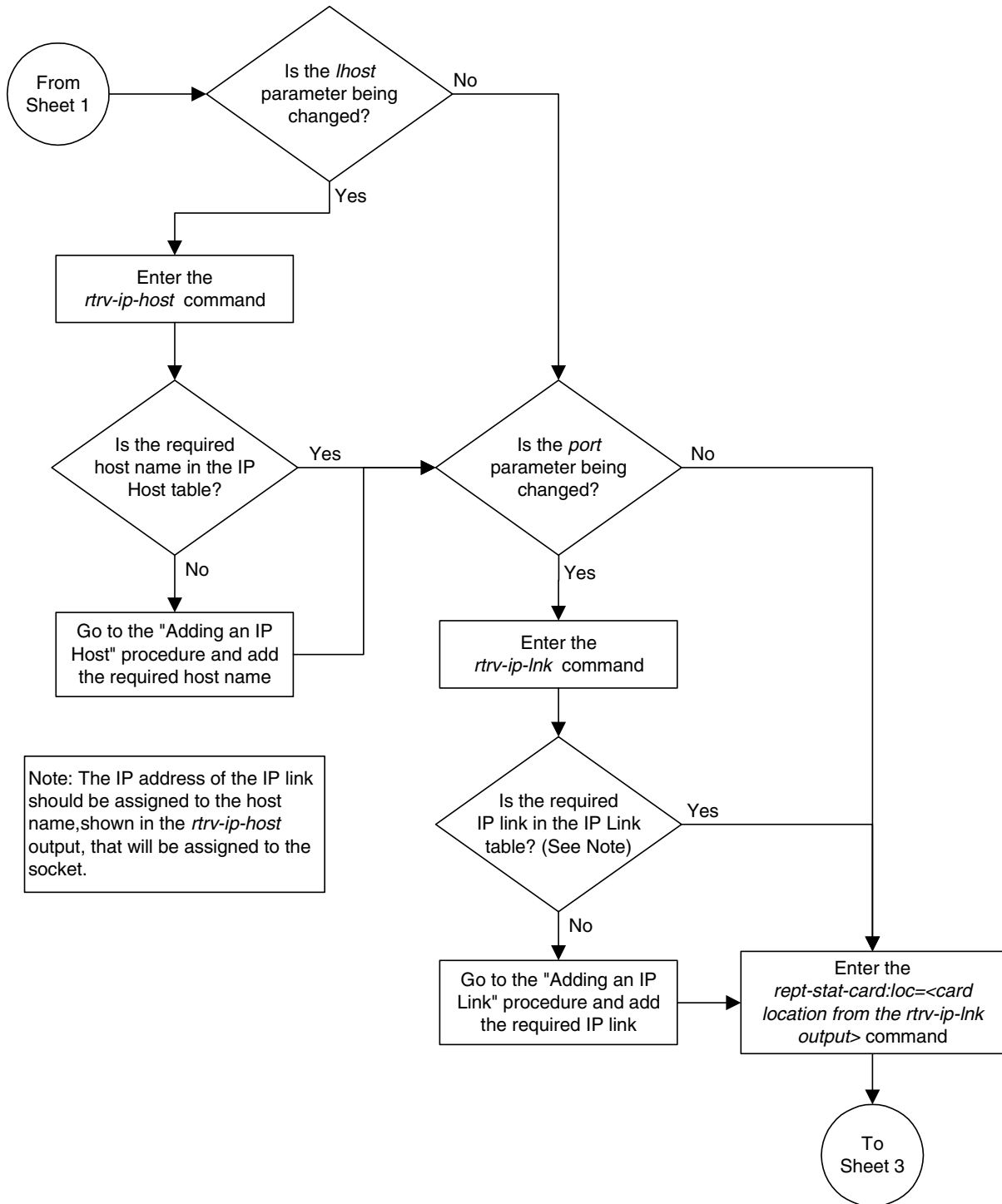
15. Back up the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

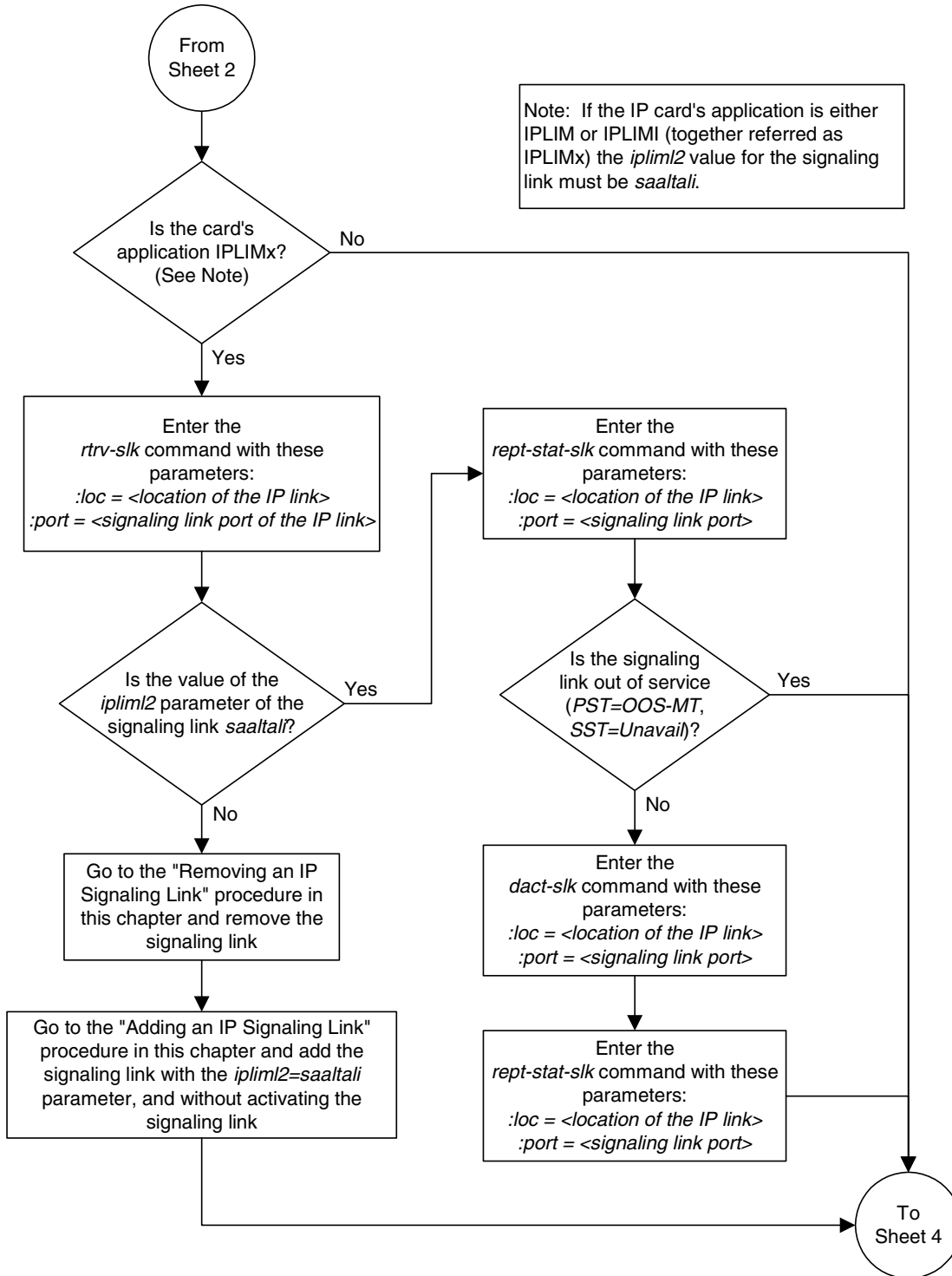
Flowchart 3-19. Changing an Application Socket (Sheet 1 of 5)



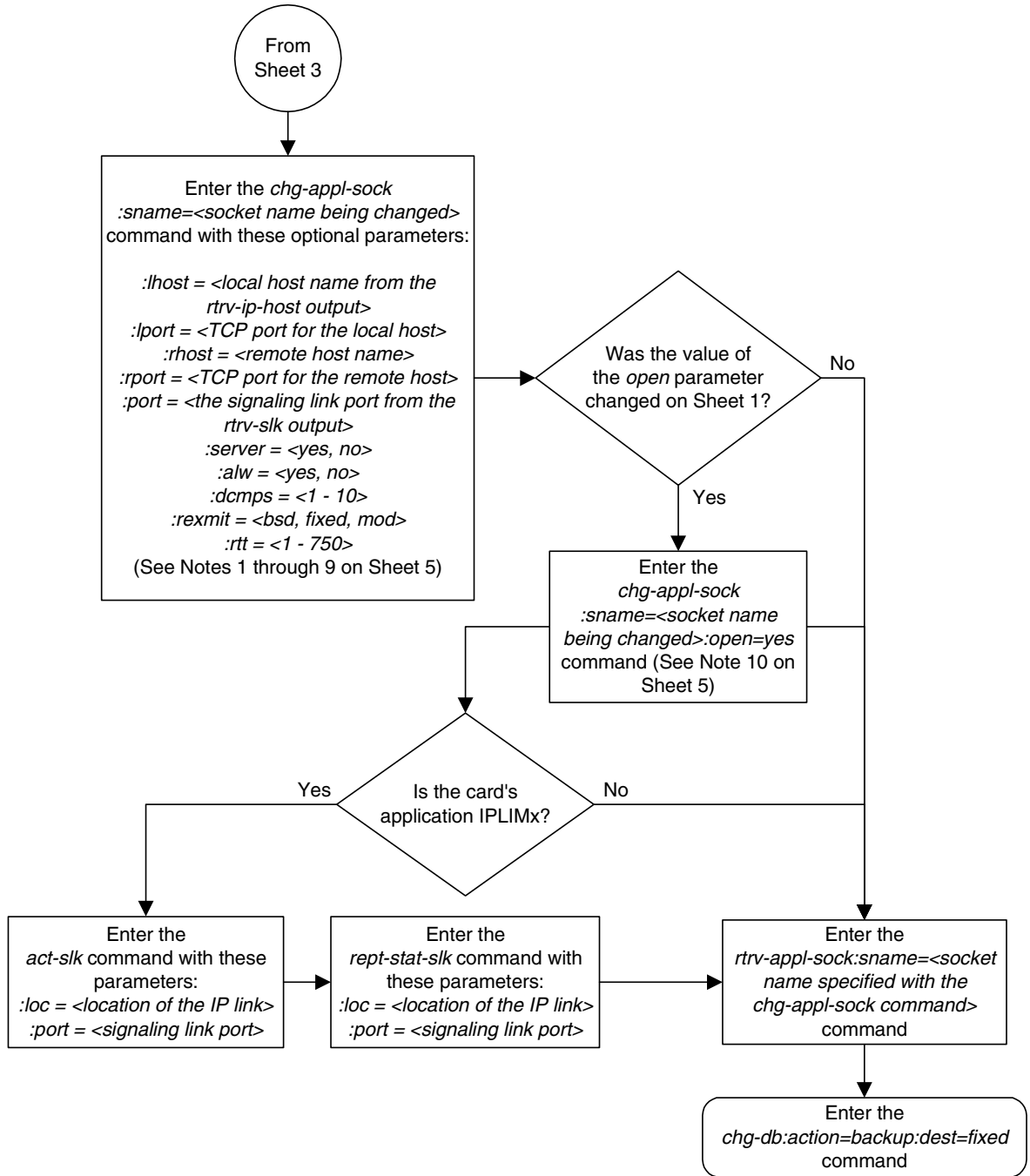
Flowchart 3-19. Changing an Application Socket (Sheet 2 of 5)



Flowchart 3-19. Changing an Application Socket (Sheet 3 of 5)



Flowchart 3-19. Changing an Application Socket (Sheet 4 of 5)



Flowchart 3-19. Changing an Application Socket (Sheet 5 of 5)

Notes:

1. If the card containing the signaling link is a DCM, the B Ethernet interface cannot be used. Single-slot EDCMs can use the B Ethernet interface.
2. Each local host on a card running either the *ss7ipgw* or *ipgwi* applications can contain a maximum of 50 connections (associations plus sockets).
3. The system can contain a maximum of 4000 connections (associations plus sockets).
4. Cards running either the *iplim* or *iplimi* applications can have only one connection for each signaling link port and a maximum of two connections for each card, if the card is a dual-slot DCM. If the card is a single-slot EDCM, the card may contain a maximum of eight connections.
5. The value of the *lhost* and *rhost* parameters is a text string of up to 60 characters, with the first character being a letter.
6. If the socket is a client socket (*server=no*) and the *open* parameter value is being changed to *yes*, the *lhost/lport* parameter values of this socket cannot match the *lhost/lport* values of any other open sockets.
7. If the socket is a server socket (*server=yes*) and the *open* parameter value is being changed to *yes*, the *lhost/lport* parameter values of this socket cannot match the *lhost/lport* values of any other open client sockets.
8. The *rtt* parameter cannot be specified with the *rexmit=bsd* parameter.
9. When the *rexmit=fixed* or *rexmit=mod* parameters are specified, the *rtt* parameter must be specified.
10. If the *open* parameter value is being changed to *yes*, the socket must contain values for the *lhost*, *lport*, *rhost*, and *rport* parameters.

Configuring IP Socket Retransmission Parameters

This procedure is used to configure the retransmission parameters for sockets using the **rexit** and **rtt** parameters of the **chg-appl-sock** command.

:rexit – Indicates the retransmission mode that the user wants the TCP stack to use for a socket. Possible values are **bsd** (standard), **fixed** (Tekelec version), or **mod** (combination of **bsd** and **fixed**). The default value is **fixed**.

:rtt – Indicates the measured or expected round trip time of the socket in milliseconds. Be aware that you are entering the round trip time, not the retransmission timeout that will be used for the socket. The initial retransmission timeout that is actually applied to the socket will be the next 125 millisecond increment above the entered round trip time. The default value is 60.

It is important to set the configured round trip time as accurately as possible. When the round trip time is configured too low, network congestion can occur, thus delaying (or preventing) the delivery of SS7 data, resulting in a negative impact on MSU throughput. If the round trip time is set too high, the TCP protocol layer may act unpredictably, resulting in the SS7 service being degraded. The MSU throughput would be lowered, possibly affecting the client application software. When the round trip time is configured correctly, the TCP network can deliver SS7 data in a timely manner with little or no network congestion.

The “Changing an Application Socket” procedure on page 3-205 is used to change the values of these parameters. In addition to using the “Changing an Application Socket” procedure, these pass commands are also used in this procedure.

- **ping** – tests for the presence of hosts on the network.
- **sockrtt** – displays the round trip time data
- **netstat -p tcp** – determines if retransmissions have occurred.

For more information of the **pass** commands, go to the *Commands Manual*.

The **rexit** and **rtt** parameter values are set using the data collected from the **pass** commands.

The **rtt** parameter cannot be specified with the **rexit=bsd** parameter.

When the **rexit=fixed** or **rexit=mod** parameters are specified, the **rtt** parameter must be specified.

Canceling the RTRV-APPL-SOCK Command

Because the `rtrv-appl-sock` command used in this procedure can output information for a long period of time, the `rtrv-appl-sock` command can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-appl-sock` command can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-appl-sock` command was entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-appl-sock` command was entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-appl-sock` command was entered, from another terminal other than the terminal where the `rtrv-appl-sock` command was entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current application socket information in the database by entering the `rtrv-appl-sock` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
SNAME kchlr11201
  PORT  A
  LHOST ipnode1-1201
  RHOST kc-hlr1
  LPORT 7000          RPORT 7000
  SERVER YES          DCMPS 1
  REXMIT FIXED        RTT 60
  OPEN  YES           ALW  NO

SNAME kchlr11203
  PORT  A
  LHOST ipnode1-1203
  RHOST kc-hlr1
  LPORT 7005          RPORT 7005
  SERVER YES          DCMPS 10
  REXMIT FIXED        RTT 60
  OPEN  YES           ALW  YES

IP Appl Sock/Assoc table is (3 of 4000) 1% full
```

2. Display the IP address assigned to the remote host that will be pinged in step 4 using the `rtrv-ip-host` command with the remote host name shown in step 1. For this example, enter this command.

```
rtrv-ip-host:host="kc-hlr1"
```

The following is an example of the possible output

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

IPADDR          HOST
192.1.1.30      kc-hlr1

IP Host table is (10 of 512) 2% full
```

3. Display the IP links assigned to the IP address shown in step 2 by entering the `rtrv-ip-lnk` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
LOC  PORT  IPADDR          SUBMASK          DUPLEX  SPEED  MACTYPE  AUTO
1201 A    192.001.001.030 255.255.255.0    ----   ---   DIX      YES
1203 A    192.001.001.012 255.255.255.0    ----   ---   DIX      YES
1205 A    192.001.001.014 255.255.255.0    FULL   100   DIX      NO
```

4. Using the outputs of steps 1 through 3 as a guide, enter the `pass:cmd="ping"` command specifying the card and the host name of the remote host. This command is entered several times to obtain the average round trip time. For this example, enter this command.

```
pass:loc=1201:cmd="ping kc-hlr1"
```

The following is an example of the possible output

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
PASS: Command sent to card

rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
PING command in progress

rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
PING kc-hlr1 (192.1.1.30): 56 data bytes
64 bytes from tekral.nc.tekelec.com (192.1.1.30): icmp_seq=0. time=5. ms
64 bytes from tekral.nc.tekelec.com (192.1.1.30): icmp_seq=1. time=9. ms
64 bytes from tekral.nc.tekelec.com (192.1.1.30): icmp_seq=2. time=14. ms
----tekral PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 5/9/14

PING command complete
```

5. Go to the "Changing an Application Socket" procedure on page 3-205 and change the retransmission parameters (`rtrt` and `rexmit`) of the socket based on the results of pinging the remote host in step 4.

6. A TALI monitor (MONI) message is sent to the remote host.
-

7. Enter the `pass:cmd="sockrtt"` command to display the round trip time data collected during the sending of the TALI monitor acknowledgement (MONA) message. For this example, enter this command.

```
pass:loc=1201:cmd="sockrtt kc-hlr1"
```

The following is an example of the possible output

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
PASS: Command sent to card

rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

SOCKRTT: Socket round-trip time report (in milliseconds)

Configured Traffic Round-Trip Time
Retransmission Mode           : MOD
Fixed Round Trip Time         : 250

Measured Normal Traffic Round-Trip Times

    Minimum round-trip time           : 5
    Maximum round-trip time           : 195
    Weighted Average round-trip time  : 10
    Last recorded round-trip time     : 10

Measured Congested Traffic Round-Trip Times

    Minimum round-trip time           : 0
    Maximum round-trip time           : 0
    Weighted Average round-trip time  : 0
    Last recorded round-trip time     : 0

rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
SOCKRTT command complete
```

8. Enter the `pass:cmd="netstat -p tcp"` command to determine if any retransmissions have occurred. For this example, enter this command.

```
pass:loc=1201:cmd="netstat -p tcp"
```

The following is an example of the possible output

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
PASS: Command sent to card

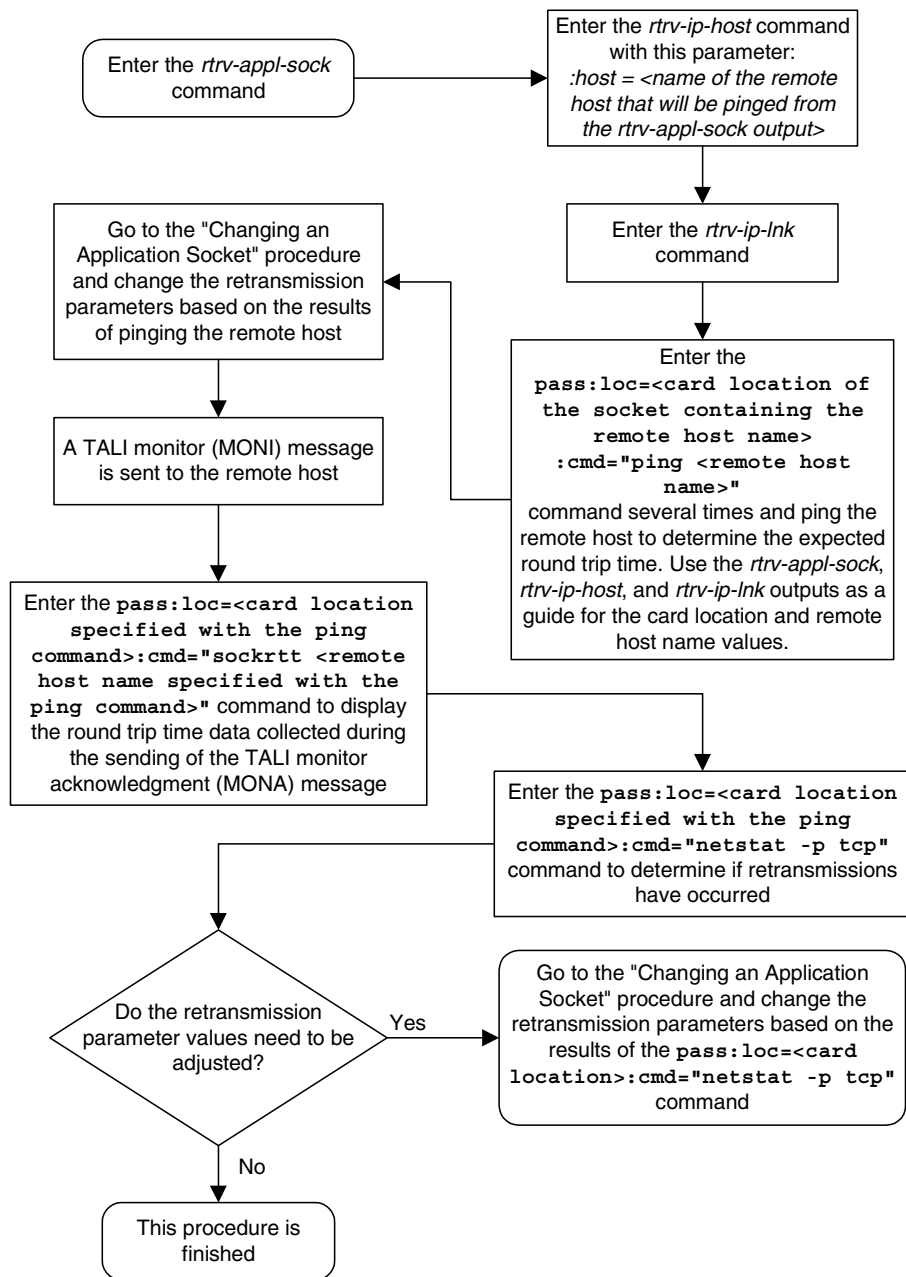
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
TCP:
  0 packet sent
    0 data packet (0 byte)
    0 data packet (0 byte) retransmitted
    0 ack-only packet (0 delayed)
    0 URG only packet
    0 window probe packet
    0 window update packet
    0 control packet
  0 packet received
    0 ack (for 0 byte)
    0 duplicate ack
    0 ack for unsent data
    0 packet (0 byte) received in-sequence
    0 completely duplicate packet (0 byte)
    0 packet with some dup. data (0 byte duped)
    0 out-of-order packet (0 byte)
    0 packet (0 byte) of data after window
    0 window probe
    0 window update packet
    0 packet received after close
    0 discarded for bad checksum
    0 discarded for bad header offset field
    0 discarded because packet too short
  0 connection request
  0 connection accept
  0 connection established (including accepts)
  0 connection closed (including 0 drop)
  0 embryonic connection dropped
  0 segment updated rtt (of 0 attempt)
  0 retransmit timeout
    0 connection dropped by rexmit timeout
  0 persist timeout
  0 keepalive timeout
    0 keepalive probe sent
    0 connection dropped by keepalive
  0 pcb cache lookup failed

rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
NETSTAT command complete
```

NOTE: If the results of the `pass:cmd="netstat -p tcp"` command show that the retransmission parameters do not need to be adjusted, do not perform this step. This procedure is finished.

9. Go to the "Changing an Application Socket" procedure on page 3-205 and adjust the retransmission parameter (`rtt` and `rexit`) values of the socket based on the results of the `pass:cmd="netstat -p tcp"` command entered in step 8.

Flowchart 3-20. Configuring IP Retransmission Parameters



Changing a DCM Parameter Set

This procedure is used to change a Database Communication Module Parameter Set in the database using the **chg-dcmps** command. Parameter sets are sets of generic timers and parameters that can be used by any IP application.

NOTE: For IP, timers one through four correspond to timers T1, T2, T3, T4 in the TALI state machine.

The **chg-dcmps** command uses these parameters.

- :set** – The set number, 1 to 9.
- :timer** – The timer number within the set, 1 to 10. Only timers 1 to 4 are used. Timers 5 through 10 are not used.
- :tvalue** – The value the timer will be set to.
- :parm** – The parameter number within the timer, 1 to 10. Only parameter numbers 1 through 3 are used. Parameter numbers 4 through 10 are not used.
- :pvalue** – The numerical value that **pvalue** will be set to if specified.
- :srcset** – The source set of the copy, 1 - 10.

The values of the **timer**, **tvalue**, **parm**, and **pvalue** parameters is shown in the **rtrv-dcmps** output. The output shows the values for the **tvalue** and **pvalue** in bits. The values for these parameters are entered as a decimal number. Table 3-17 shows the decimal equivalent for the bit values shown in the **rtrv-dcmps** output.

Table 3-17. DCMPS Values

Bit Value	Decimal Number Range
32	0 - 4294967295
8	0 - 255

While the value of the **pvalue** parameter when used with the **parm=3** parameter is 32 bits, or from 0 to 4294967295, only the first 6 bits (bits 0 - 5) are used. Bits 6-31 are reserved. This makes the decimal value of the **pvalue** parameter when used with the **parm=3** parameter from 0 to 63.

The value of the **pvalue** parameter when used with the **parm=2** parameter (enabling or disabling Nagle's Algorithm, TCP socket option) is either 0 (disabling Nagle's Algorithm) or 1 (enabling Nagle's Algorithm).

At least one of these parameters, **timer**, **parm**, or **srcset**, must be entered.

If the **srcset** parameter is specified, no other optional parameters can be entered.

If the **timer** parameter is specified, the **tvalue** parameter must be specified.

If the **parm** parameter is specified, the **pvalue** parameter must be specified.

NOTE: Set number 10 is a default parameter set and cannot be changed. In order to change the DCM parameters set for a socket using set number 10, use the `chg-appl-sock` command to change the DCM parameter set to a different set number, and then use the `chg-dcmps` command to modify the new set.

Canceling the `RTRV-DCMPS` Command

Because the `rtrv-dcmps` command used in this procedure can output information for a long period of time, the `rtrv-dcmps` command can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-dcmps` command can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-dcmps` command was entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-dcmps` command was entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-dcmps` command was entered, from another terminal other than the terminal where the `rtrv-dcmps` command was entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current DCM parameter set information in the database by entering the `rtrv-dcmps` command. For example, enter this command.

`rtrv-dcmps:set=1`

The following is an example of the possible output.

rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

SET	TIMER	TVALUE	PARM	PVALUE
1	1	4000	1	255
1	2	3000	2	1
1	3	3000	3	1
1	4	10000	4	0
1	5	0	5	0
1	6	0	6	0
1	7	0	7	0
1	8	0	8	0
1	9	0	9	0
1	10	0	10	0

TIMER 1: TALI T1 Timer, time (mS) between sending of TEST msgs by NE
TVALUE : Valid range = 32-bits

TIMER 2: TALI T2 Timer, time (mS) to wait for response to TEST msg
TVALUE : Valid range = 32-bits

TIMER 3: TALI T3 Timer, time (mS) to continue processing rcv'd service
msgs after NE is prohibited
TVALUE : Valid range = 32-bits

TIMER 4: TALI T4 Timer, time (mS) between sending of MONI msgs by NE
TVALUE: Valid range = 32-bits

PARM 1: Type of Service (TOS), IP header socket option
PVALUE: Valid range = lowest 8-bits

PARM 2: Nagle's Algorithm, TCP socket option
PVALUE: Valid range = lowest bit: 0 = Disable Nagle, 1 = Enable Nagle

PARM 3: Default SORP Flags socket option. Each bit is used as an
enabled/disabled flag for a particular socket option.
PVALUE: Valid range = 32-bits

BIT	BIT VALUE
0=Broadcast Phase MTPP Primitives;	0=Disabled , 1=Enabled
1=Response Method MTPP Primitives;	0=Disabled , 1=Enabled
2=SCCP with MTP;	0=Disabled , 1=Enabled
3=ISUP via MTP;	0=Disabled , 1=Enabled
4=Group Code in MTPP;	0=Disabled , 1=Enabled
5=Use XSRV;	0=Disabled , 1=Enabled
6-31=Reserved	

2. Change the DCM parameter set information in the database by using the **chg-dcmps** command. For example, enter this command.

```
chg-dcmps:set=1:timer=1:tvalue=500
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
CHG-DCMPS: MASP A - COMPLTD
```

3. Verify the new application socket information in the database by entering the **rtrv-dcmps** command. For example, enter this command.

```
rtrv-dcmps:set=1
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
SET  TIMER      TVALUE  PARM      PVALUE
 1      1          500      1          255
 1      2          3000     2           1
 1      3          3000     3           1
 1      4          10000    4           0
 1      5           0         5           0
 1      6           0         6           0
 1      7           0         7           0
 1      8           0         8           0
 1      9           0         9           0
 1     10           0        10           0
```

TIMER 1: TALI T1 Timer, time (mS) between sending of TEST msgs by NE
TVALUE : Valid range = 32-bits

TIMER 2: TALI T2 Timer, time (mS) to wait for response to TEST msg
TVALUE : Valid range = 32-bits

TIMER 3: TALI T3 Timer, time (mS) to continue processing rcv'd service
msgs after NE is prohibited
TVALUE : Valid range = 32-bits

TIMER 4: TALI T4 Timer, time (mS) between sending of MONI msgs by NE
TVALUE : Valid range = 32-bits

PARM 1: Type of Service (TOS), IP header socket option
PVALUE : Valid range = lowest 8-bits

PARM 2: Nagle's Algorithm, TCP socket option
PVALUE : Valid range = lowest bit: 0 = Disable Nagle, 1 = Enable Nagle

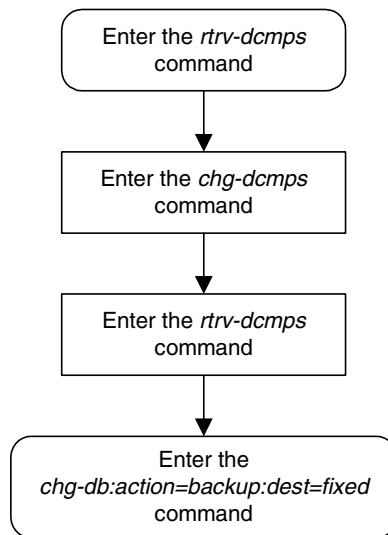
PARM 3: Default SORP Flags socket option. Each bit is used as an
enabled/disabled flag for a particular socket option.
PVALUE : Valid range = 32-bits

BIT	BIT VALUE
0=Broadcast Phase MTPP Primitives;	0=Disabled , 1=Enabled
1=Response Method MTPP Primitives;	0=Disabled , 1=Enabled
2=SCCP with MTP;	0=Disabled , 1=Enabled
3=ISUP via MTP;	0=Disabled , 1=Enabled
4=Group Code in MTPP;	0=Disabled , 1=Enabled
5=Use XSRV;	0=Disabled , 1=Enabled
6-31=Reserved	

4. Back up the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-21. Changing an DCM Parameter Set



Adding an Application Routing Key Containing a Socket

This procedure is used to add an application routing key containing a socket to the database, or add a socket to an existing routing key containing sockets using the `ent-appl-rtkey` command.

An application routing key defines a filter that checks the specified values in an incoming SS7 MSU to determine which, if any, socket or association receives the MSU. For more information about static routing keys, see “Understanding Routing for SS7IPGW and IPGWI Applications” on page 2-23.

The `ent-appl-rtkey` command uses these parameters.

:dpc/dpca/dpci/dpcn/dpcn24 – The destination point code value that is used to filter incoming MSUs. This parameter must not specify a cluster route.

:opc/opca/opci/opcn/opcn24 – The originating point code value that is used to filter incoming MSUs. This parameter must not specify a cluster route. This parameter is valid only when the `si` parameter value is set to 4, 5, or 13. This parameter is required if `si=4, 5, or 13` and `type=full`.

NOTE: See the “Point Code Formats” section in the *Database Administration Manual - SS7* for a definition of the point code types that are used on the system and for a definition of the different formats that can be used for ITU national point codes.

:si – The service indicator value that is used to filter incoming MSUs. The range of values for the service indicator parameter (`si`) can be a numerical value from 0 to 15, or for selected service indicator values, a text string can be used instead of numbers. Table 3-18 shows the text strings that can be used in place of numbers for the service indicator values.

Table 3-18. Service Indicator Text String Values

Service Indicator Value	Text String
0	snm
1	regtest
2	spltst
3	sccp
4	tup
5	isup
13	qbicc

:ssn – The subsystem value that is used to filter incoming MSUs. The `ssn` parameter is only valid when the `si` parameter value is set to 3 or `sccp`.

:sname – The name of the socket that will receive the incoming MSU if the filter key values (**dpc**, **si**, **ssn**) match the values in the incoming MSU.

:cics – The starting circuit identification code that is used to filter incoming MSUs. When specified with **cice**, **cics** identifies the start of the range of circuit identification codes. The **cics** parameter is valid only when the **si** parameter value is set to 4, 5, or 13. The **cics** is required if **si=4**, 5, or 13 and **type=full**.

:cice – The ending circuit identification code that is used to filter incoming MSUs. When specified with **cics**, **cice** identifies the end of the range of circuit identification codes. The **cice** parameter is valid only when the **si** parameter value is set to 4, 5, or 13. The **cice** is required if **si=4**, 5, or 13 and **type=full**.

:type – The routing key type – Identifies the type of application routing key that is being entered and used to route message signaling units (MSUs). One of three values, **full/partial/default**, can be specified for the type parameter (see Table 3-19 on page 3-230). If **type** is not explicitly specified, **type = full** is assumed.

The **ent-appl-rtkey** command also contains these parameters which cannot be used in this procedure.

:asname – The application server name

:rcontext – The routing context parameter.

These parameters and their use are discussed in more detail in the “Adding an Application Routing Key Containing an Application Server” procedure on page 3-240 procedure.

Application socket names are shown in the **rtrv-appl-sock** output.

A routing key can be associated with up to 16 socket names . There is a maximum of 1000 routing keys allowed per system (if there are any dual-slot DCM cards), or 2500 routing keys allowed per system (if all cards running the **ss7ipgw** or **ipgwi** application are SSEDCM cards). Each of routing key's socket or application server names must be uniquely named.

The number of static routing keys is limited by the **srkq** parameter that was specified on the **chg-sg-opts** command.

Routing keys are associated only with the **ss7ipgw** or **ipgwi** application.

Group codes are required for 14-bit ITU-N point codes (DPCN/OPCN) when the Duplicate Point Code feature is enabled.

The starting circuit identification code must be less than or equal to the ending circuit identification code.

The ISUP routing over IP feature must be on in order to enter a routing key with these parameters: **dpc**, **si**, **opc**, **cics**, and **cice**. The **IPISUP** field in the **rtrv-feat** command output shows whether or not this feature is on.

When a routing key is added to the database, the **pstncat** and **pstnid** parameter values are set to zero and the **norm** parameter is set to **no**. These values cannot be changed with the **ent-app1-rtkey** command. To change these values, go to the “Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key” procedure on page 3-307.

The parameter combinations used by the **ent-app1-rtkey** command are based on the type of routing key and the service indicator value in the routing key. The parameter combinations are shown in Table 3-19.

Table 3-19. Routing Key Parameter Combinations for Adding a Routing Key Containing a Socket

SI=3 (SCCP)		SI=4 (TUP), 5 (ISUP), 13 (QBICC)		Other SI Values		Default Routing Key
Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	
dpc ^{1, 2}	sname	dpc ^{1, 2}	sname	dpc ^{1, 2}	sname	sname
si=3 ⁴	type=partial	si=4, 5, 13 ⁴	type=partial	si=value other than 3, 4, 5, 13 ⁴	type=partial	type=default
ssn	dpc ^{1, 2, 3}	opc ^{1, 2}	dpc ^{1, 2, 3}	sname	dpc ^{1, 2, 3}	
type=full	si=3 ^{3, 4}	cics ^{5, 6, 7, 8, 9}	si=4, 5, 13 ^{3, 4}	type=full	si=value other than 3, 4, 5, 13 ^{3, 4}	
sname		cice ^{5, 6, 7, 8, 9}	opc ^{1, 2, 3}			
		type=full				
		sname				

Notes:

1. The **dpc** and **opc** parameters can be either an ANSI point code (**dpc_a**, **opc_a**), ITU-I point code (**dpc_i**, **opc_i**), 14-bit ITU-N point code (**dpc_n**, **opc_n**), or 24-bit ITU-N point code (**dpc_{n24}**, **opc_{n24}**). If the **dpc** and **opc** parameters are specified, the **dpc** and **opc** must be the same type of point code. For example, if the **dpc_a** parameter is specified, the OPC is specified with the **opc_a** parameter.
2. If the ITU National Duplicate Point Code feature is on, the values for the **dpc_n** and **opc_n** parameters must have group codes assigned to them. The field **ITUDUPPC** in the **rtv-feat** command output shows whether or not the ITU National Duplicate Point Code feature is on. If group codes are specified for ITU-N DPC and OPC, the groups codes must be the same.
3. These parameters are optional for partial routing keys, but at least one these parameters must be specified with the **ent-app1-rtkey** command.
4. Text strings can be used in place of some numerical service indicator values. See Table 3-18 on page 3-228 for a list of these text strings.

Table 3-19. Routing Key Parameter Combinations for Adding a Routing Key Containing a Socket (Continued)

SI=3 (SCCP)		SI=4 (TUP), 5 (ISUP), 13 (QBICC)		Other SI Values		Default Routing Key
Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	
5. When the service indicator parameter value equals 4 and an ANSI dpc is specified, the <code>opc</code> , <code>cics</code> , and <code>cice</code> parameters cannot be used. If the service indicator parameter value equals 4 and an ITU dpc is specified, the <code>opc</code> , <code>cics</code> , and <code>cice</code> parameters are required.						
6. If the service indicator parameter (<code>si</code>) value is 4, the values of the <code>cics</code> and <code>cice</code> parameters is from 0 to 4095.						
7. If the service indicator parameter (<code>si</code>) value is 5 and the point code in the routing key is either an ITU-I, 14-bit ITU-N, or 24-bit ITU-N point code, the values of the <code>cics</code> and <code>cice</code> parameters is from 0 to 4095. If the point code in the routing key is an ANSI point code, the values of the <code>cics</code> and <code>cice</code> parameters is from 0 to 16383.						
8. If the service indicator parameter value is 13, the values of the <code>cics</code> and <code>cice</code> parameters is from 0 to 4294967295.						
9. The CIC range, defined by the <code>cics</code> and <code>cice</code> parameters, cannot overlap the CIC range in an existing routing key.						

Canceling the `RTRV-APPL-SOCK` and `RTRV-APPL-RTKEY` Commands

Because the `rtrv-appl-sock` and `rtrv-appl-rtkey` commands used in this procedure can output information for a long period of time, the `rtrv-appl-sock` and `rtrv-appl-rtkey` commands can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-appl-sock` and `rtrv-appl-rtkey` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-appl-sock` or `rtrv-appl-rtkey` commands were entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-appl-sock` or `rtrv-appl-rtkey` commands were entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-appl-sock` and `rtrv-appl-rtkey` commands were entered, from another terminal other than the terminal where the `rtrv-appl-sock` or `rtrv-appl-rtkey` commands were entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current application routing key information in the database by entering the `rtrv-appl-rtkey` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC          SI SSN      OPC          CICS         CICE
  STATIC    123-234-123  5 ---      122-124-125  1            1000
  STATIC    123-234-123  5 ---      100-100-100  1001         5000
    1105     005-005-001  5 ---      010-010-001  1            500
    1105     005-005-001  5 ---      010-010-001  501         1000
    1107     006-006-001  5 ---      011-011-001  1            500
    1107     006-006-001  5 ---      011-011-001  501         1000

STATIC Route Key table is (7 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

NOTE: If the routing key will be assigned to a new DPC, skip this step and go to step 3.

NOTE: If a default routing key is being added in this procedure, and the `rtrv-appl-rtkey` output in step 1 shows default routing keys, enter the `rtrv-appl-rtkey` command with the `display=all` and `type=default` parameters. Then go to step 3. If the `rtrv-appl-rtkey` output in step 1 does not show any default routing keys, skip this step and go to step 3.

2. Display the specific routing key information for the routing key that the new routing key will be added to by entering the `rtrv-appl-rtkey` command with the `display=all` parameter and the DPC value shown in the `rtrv-appl-rtkey` output in step 1. For this example, enter this command.

```
rtrv-appl-rtkey:dpc=123-234-123:display=all
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC          SI SSN      OPC          CICS         CICE
  STATIC    123-234-123  5 ---      122-124-125  1            1000
  ATTR:PSTNCAT PSTNID NORM DUP
           0          0 N      -
  SNAMEs:socket31

  STATIC    123-234-123  5 ---      100-100-100  1            50
  ATTR:PSTNCAT PSTNID NORM DUP
           0          0 N      -
  SNAMEs:socket31

STATIC Route Key table is (7 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full
```

```

STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full

```

If this routing key has an application server assigned to it, another socket cannot be assigned to the routing key. Continue with this procedure at step 3 and add a new routing key with a new DPC and the desired socket.

3. Display the current application socket information in the database by entering the `rtrv-appl-sock` command. The following is an example of the possible output.

```

rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
SNAME socket31
  PORT  A
  LHOST ipnode1-1201
  RHOST kc-hlr1
  LPORT 7000          RPORT 7000
  SERVER YES          DCMPS 1
  REXMIT FIXED       RTT 60
  OPEN  YES          ALW  NO

SNAME kchlr11203
  PORT  A
  LHOST ipnode1-1203
  RHOST kc-hlr1
  LPORT 7005          RPORT 7005
  SERVER YES          DCMPS 10
  REXMIT FIXED       RTT 60
  OPEN  YES          ALW  YES

```

```
IP Appl Sock/Assoc table is (2 of 4000) 1% full
```

If the required socket is not in the database, go to the “Adding an Application Socket” procedure on page 3-192 to add the socket. Then go to step 4.

NOTE: If a default routing key is being added to the database, or if the SI value of the routing key being added is a value other than 4, 5, or 13, skip steps 4 and 5, and go to step 6.

4. Verify that the ISUP Routing over IP feature is on, by entering the `rtrv-feat` command. If the ISUP Routing over IP feature is on, the `IPISUP` field should be set to `on`. For this example, the ISUP Routing over IP feature is off.

NOTE: The `rtrv-feat` command output contains other fields that are not used by this procedure. If you wish to see all the fields displayed by the `rtrv-feat` command, see the `rtrv-feat` command description in the *Commands Manual*.

NOTE: If the ISUP Routing over IP feature is on, skip step 5 and go to step 6.

5. Turn the ISUP Routing over IP feature on by entering this command.

```
chg-feat:ipisup=on
```

NOTE: Once the ISUP Routing over IP feature is turned on with the `chg-feat` command, it cannot be turned off.

The ISUP Routing over IP feature must be purchased before you turn this feature on with the `chg-feat` command. If you are not sure if you have purchased the ISUP Routing over IP feature, contact your Tekelec Sales Representative or Account Representative.

When the `chg-feat` has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 11:43:04 GMT EAGLE5 31.10.0
CHG-FEAT: MASP A - COMPLTD
```

6. Add an application routing key entry to the database by entering the `ent-appl-rtkey` command. The parameters required for the `ent-appl-rtkey` command are determined by the type of routing key being added and the service indicator value in the routing key. See Table 3-19 on page 3-230 for the parameter combinations that can be used for the type of routing key being added to the database.

NOTE: If the DPC and OPC values are ITU-N point codes, these point codes must have group codes assigned to them if the ITU National Duplicate Point Code feature is on. The `ITUDUPPC` field in the `rtrv-feat` command executed in step 4 shows whether or not the ITU National Duplicate Point Code feature is on.

A socket can be added to an existing routing key if the `DPC` value specified in this procedure must be same as the `DPC` value shown in the existing routing key.

For this example, a full ISUP routing key is being added to the database. Enter this command.

```
ent-appl-rtkey:dpca=001-002-003:si=5:opca=100-100-100:cics=1
:cice=50:sname=socket5:type=full
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
ENT-APPL-RTKEY: MASP A - COMPLTD
```

- Verify the new application routing key information in the database by entering the `rtrv-appl-rtkey` command with the socket name (`sname`) specified in step 6 and the `display=all` parameter. For this example, enter this command.

```
rtrv-appl-rtkey:sname=socket5:display=all
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC          SI SSN OPCA          CICS          CICE
  STATIC 001-002-003 5 --- 100-100-100 1             50
  ATTR:PSTNCAT PSTNID NORM DUP
                0      0 N   -
  SNAME:socket5
```

```
STATIC Route Key table is ( 8 of 2000) 1% full
1105  Route Key table is ( 2 of 500) 1% full
1107  Route Key table is ( 2 of 500) 1% full
```

```
STATIC Route Key Socket Association table is (8 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

If a socket was assigned to the routing key added in this procedure and you wish to add other sockets to the routing key, repeat this procedure from step 3. If no other sockets are to be added to the routing key, go to step 8.

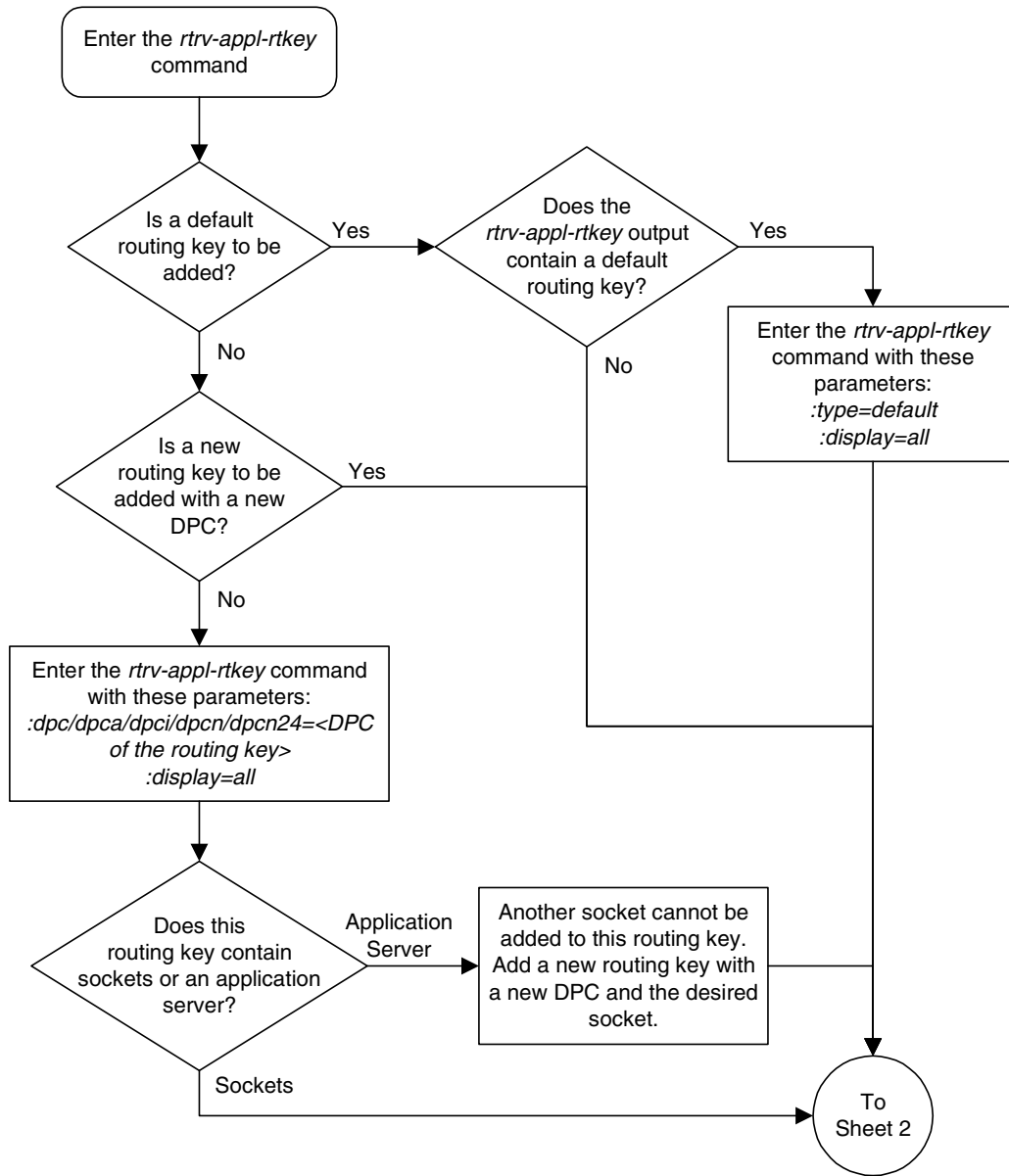
- If you wish to change the PSTN presentation information in the routing key that was added in step 6, go to the “Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key” procedure on page 3-307. Do not perform step 9.

If you do not wish to change the PSTN presentation information in the routing key, skip this step and go to step 9.

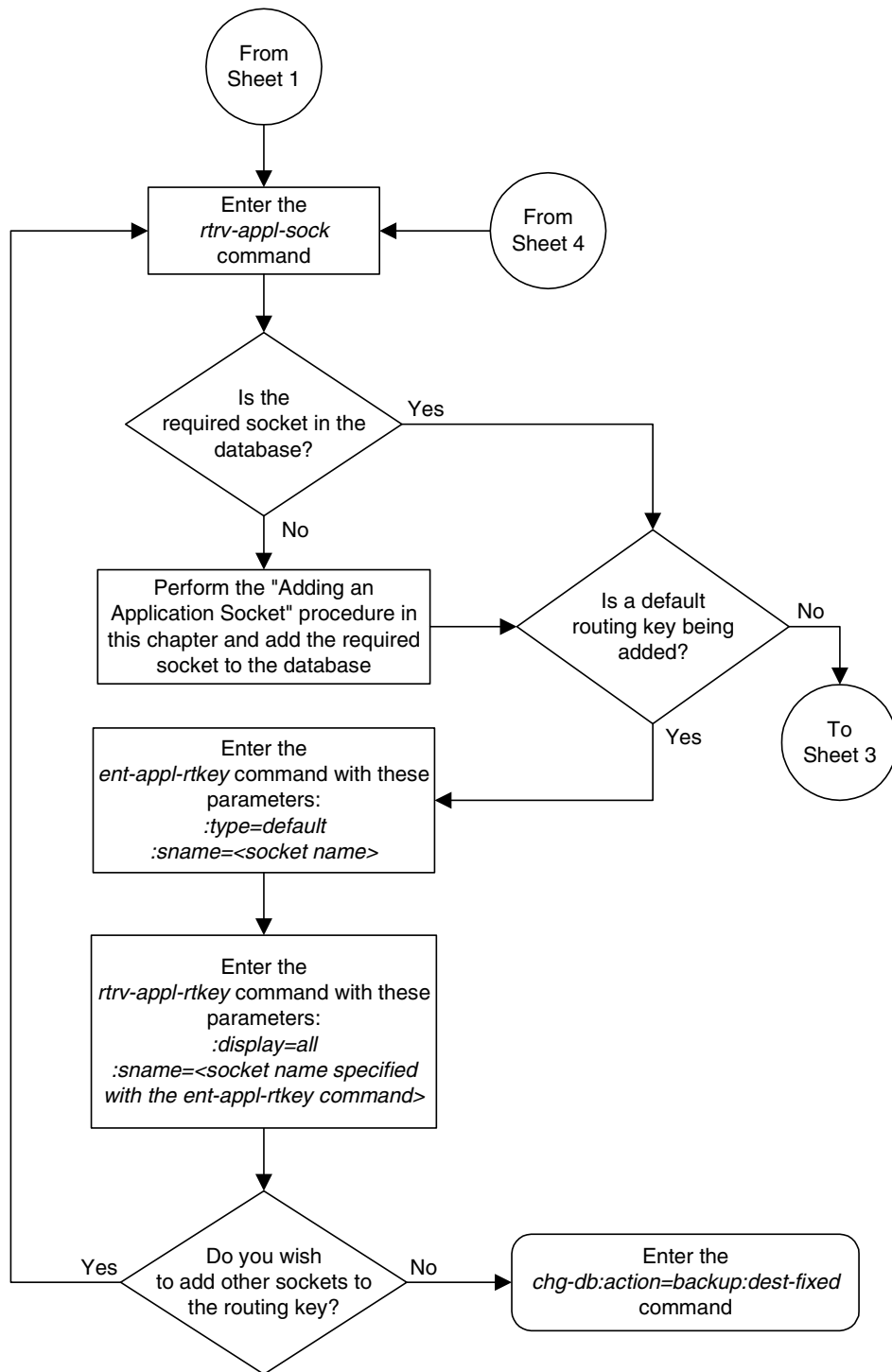
- Back up the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

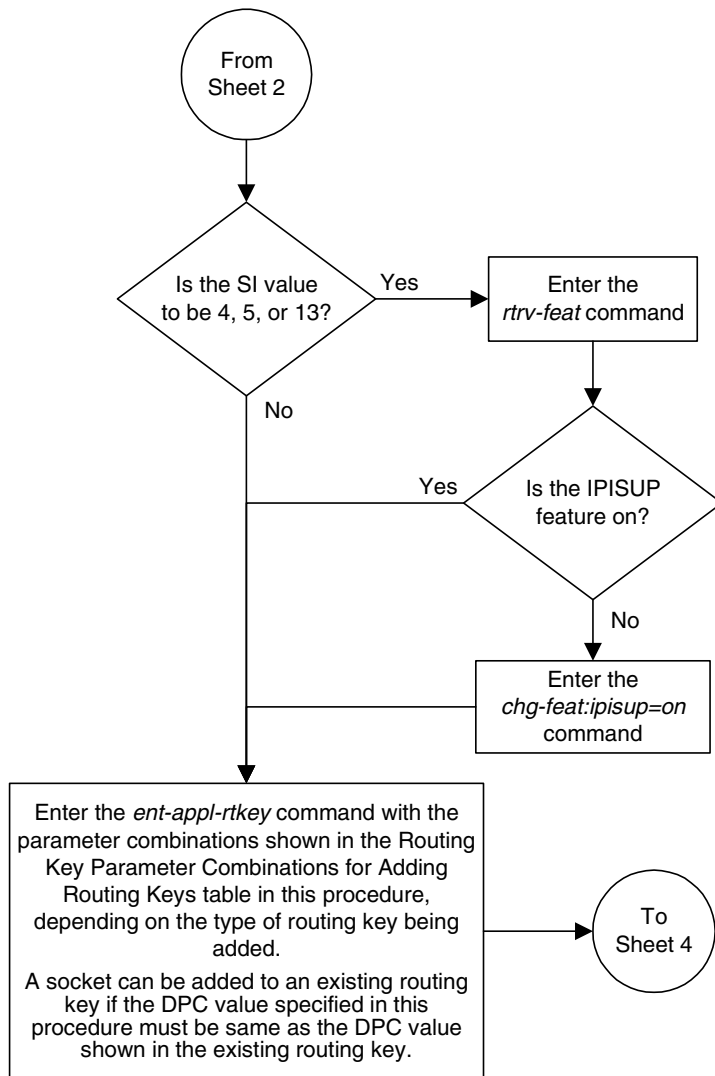
Flowchart 3-22. Adding an Application Routing Key Containing a Socket
(Sheet 1 of 4)



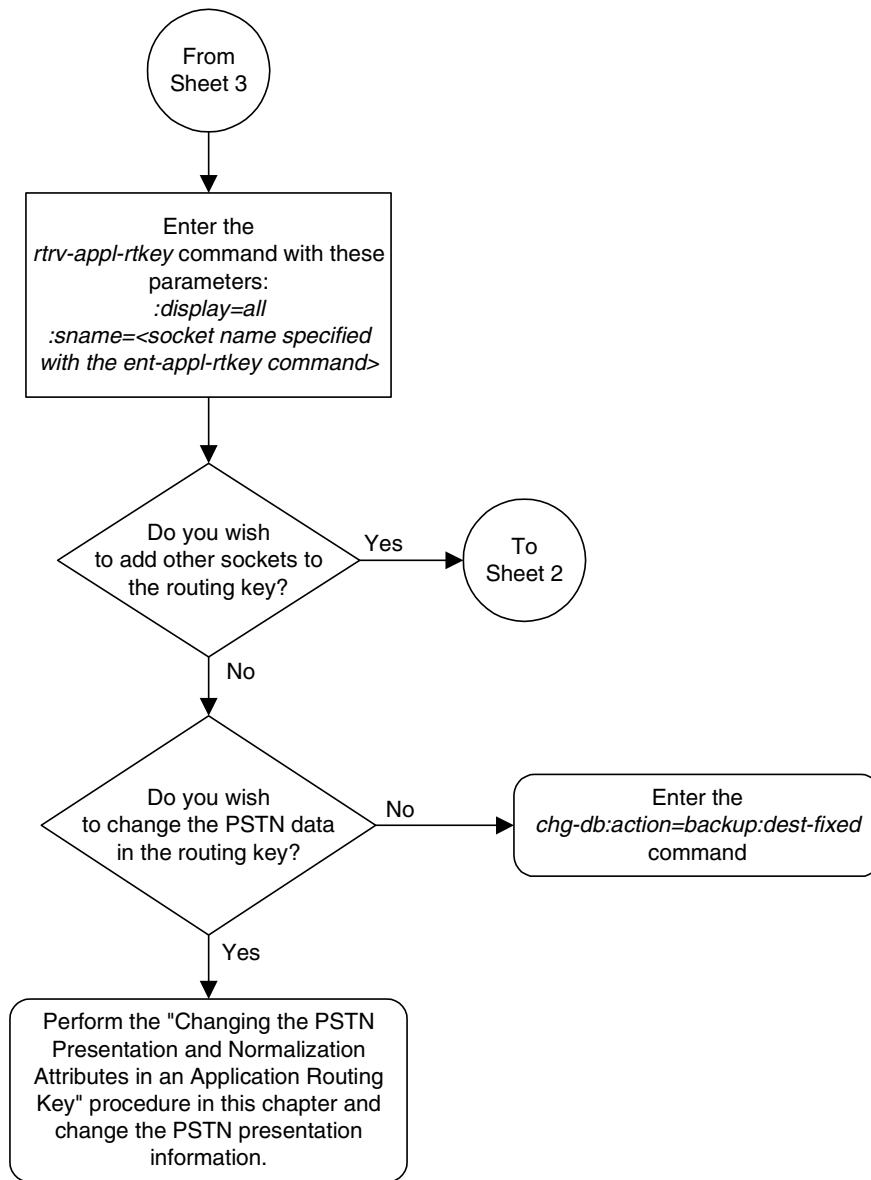
Flowchart 3-22. Adding an Application Routing Key Containing a Socket
(Sheet 2 of 4)



Flowchart 3-22. Adding an Application Routing Key Containing a Socket
(Sheet 3 of 4)



Flowchart 3-22. Adding an Application Routing Key Containing a Socket
(Sheet 4 of 4)



Adding an Application Routing Key Containing an Application Server

This procedure is used to add an application routing key containing an application server to the database using the `ent-app1-rtkey` command.

An application routing key defines a filter that checks the specified values in an incoming SS7 MSU to determine which, if any, socket or association receives the MSU. For more information about static routing keys, see “Understanding Routing for SS7IPGW and IPGWI Applications” on page 2-23.

The `ent-app1-rtkey` command uses these parameters.

`:dpc/dpca/dpci/dpcn/dpcn24` – The destination point code value that is used to filter incoming MSUs. This parameter must not specify a cluster route.

`:opc/opca/opci/opcn/opcn24` – The originating point code value that is used to filter incoming MSUs. This parameter must not specify a cluster route. This parameter is valid only when the `si` parameter value is set to 4, 5, or 13. This parameter is required if `si=4, 5, or 13` and `type=full`.

NOTE: See the “Point Code Formats” section in the *Database Administration Manual - SS7* for a definition of the point code types that are used on the system and for a definition of the different formats that can be used for ITU national point codes.

`:si` – The service indicator value that is used to filter incoming MSUs. The range of values for the service indicator parameter (`si`) can be a numerical value from 0 to 15, or for selected service indicator values, a text string can be used instead of numbers. Table 3-20 shows the text strings that can be used in place of numbers for the service indicator values.

Table 3-20. Service Indicator Text String Values

Service Indicator Value	Text String
0	snm
1	regtest
2	spltst
3	sccp
4	tup
5	isup
13	qbicc

:ssn – The subsystem value that is used to filter incoming MSUs. The **ssn** parameter is only valid when the **si** parameter value is set to 3 or **sccp**.

:cics – The starting circuit identification code that is used to filter incoming MSUs. When specified with **cice**, **cics** identifies the start of the range of circuit identification codes. The **cics** parameter is valid only when the **si** parameter value is set to 4, 5, or 13. The **cics** is required if **si=4, 5, or 13** and **type=full**.

:cice – The ending circuit identification code that is used to filter incoming MSUs. When specified with **cics**, **cice** identifies the end of the range of circuit identification codes. The **cice** parameter is valid only when the **si** parameter value is set to 4, 5, or 13. The **cice** is required if **si=4, 5, or 13** and **type=full**.

:type – The routing key type – Identifies the type of application routing key that is being entered and used to route message signaling units (MSUs). One of three values, **full/partial/default**, can be specified for the type parameter (see Table 3-21 on page 3-242). If **type** is not explicitly specified, **type = full** is assumed.

:asname – Application server (AS) name.

:rcontext – The routing context parameter, which has two functions:

- Provides an index of the application server traffic that the sending ASP is configured or registered to receive.
- Identifies the SS7 network context for the message. The routing context parameter implicitly defines the SS7 point code format used, the SS7 network indicator value, and the SCCP protocol type/variant/version used.

The **ent-appl-rtkey** command also contains the **sname** (socket name) parameters which cannot be used in this procedure. The **sname** parameter and its use is discussed in more detail in the “Adding an Application Routing Key Containing a Socket” procedure on page 3-228 procedure.

Application server names are shown in the **rtrv-as** output.

Only one application server can be assigned to a routing key. There is a maximum of 1000 routing keys allowed per system (if there are any dual-slot DCM cards), or 2500 routing keys allowed per system (if all cards running the **ss7ipgw** or **ipgwi** application are SSEDCCM cards). Each of routing key’s socket or application server names must be uniquely named.

The number of static routing keys is limited by the **srkq** parameter that was specified on the **chg-sg-opts** command.

Routing keys are associated only with the **ss7ipgw** or **ipgwi** application.

Group codes are required for 14-bit ITU-N point codes (DPCN/OPCN) when the Duplicate Point Code feature is enabled.

The starting circuit identification code must be less than or equal to the ending circuit identification code.

The ISUP routing over IP feature must be on in order to enter a routing key with these parameters: `dpc`, `si`, `opc`, `cics`, and `cice`. The `IPISUP` field in the `rtrv-feat` command output shows whether or not this feature is on.

The parameter combinations used by the `ent-app1-rtkey` command are based on the type of routing key and the service indicator value in the routing key. The parameter combinations are shown in Table 3-21.

Table 3-21. Routing Key Parameter Combinations for Adding a Routing Key Containing an Application Server

SI=3 (SCCP)		SI=4 (TUP), 5 (ISUP), 13 (QBICC)		Other SI Values		Default Routing Key
Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	
dpc ^{1, 2}	type=partial	dpc ^{1, 2}	type=partial	dpc ^{1, 2}	type=partial	type=default
si=3 ⁴	dpc ^{1, 2, 3}	si=4, 5, 13 ⁴	dpc ^{1, 2, 3}	si=value other than 3, 4, 5, 13 ⁴	dpc ^{1, 2, 3}	asname ¹⁰
ssn	si=3 ^{3, 4}	opc ^{1, 2}	si=4, 5, 13 ^{3, 4, 10}	type=full	si=value other than 3, 4, 5, 13 ^{3, 4, 10}	rcontext ¹⁰
type=full	asname ¹⁰	cics ^{5, 6, 7, 8, 9}	opc ^{1, 2, 3}	asname ¹⁰	asname ¹⁰	
asname ¹⁰	rcontext ¹⁰	cice ^{5, 6, 7, 8, 9}	asname ¹⁰	rcontext ¹⁰	rcontext ¹⁰	
rcontext ¹⁰		type=full	rcontext ¹⁰			
		asname ¹⁰				
		rcontext ¹⁰				

Notes:

1. The `dpc` and `opc` parameters can be either an ANSI point code (`dpca`, `opca`), ITU-I point code (`dpci`, `opci`), 14-bit ITU-N point code (`dpcn`, `opcn`), or 24-bit ITU-N point code (`dpcn24`, `opcn24`). If the `dpc` and `opc` parameters are specified, the `dpc` and `opc` must be the same type of point code. For example, if the `dpca` parameter is specified, the OPC is specified with the `opca` parameter.
2. If the ITU National Duplicate Point Code feature is on, the values for the `dpcn` and `opcn` parameters must have group codes assigned to them. The field `ITUDUPPC` in the `rtrv-feat` command output shows whether or not the ITU National Duplicate Point Code feature is on. If group codes are specified for ITU-N DPC and OPC, the groups codes must be the same.
3. These parameters are optional for partial routing keys, but at least one these parameters must be specified with the `ent-app1-rtkey` command.
4. Text strings can be used in place of some numerical service indicator values. See Table 3-20 on page 3-240 for a list of these text strings.

Table 3-21. Routing Key Parameter Combinations for Adding a Routing Key Containing an Application Server (Continued)

SI=3 (SCCP)		SI=4 (TUP), 5 (ISUP), 13 (QBICC)		Other SI Values		Default Routing Key
Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	
<p>5. When the service indicator parameter value equals 4 and an ANSI dpc is specified, the <code>opc</code>, <code>cics</code>, and <code>cice</code> parameters cannot be used. If the service indicator parameter value equals 4 and an ITU dpc is specified, the <code>opc</code>, <code>cics</code>, and <code>cice</code> parameters are required.</p> <p>6. If the service indicator parameter (<code>si</code>) value is 4, the values of the <code>cics</code> and <code>cice</code> parameters is from 0 to 4095.</p> <p>7. If the service indicator parameter (<code>si</code>) value is 5 and the point code in the routing key is either an ITU-I, 14-bit ITU-N, or 24-bit ITU-N point code, the values of the <code>cics</code> and <code>cice</code> parameters is from 0 to 4095. If the point code in the routing key is an ANSI point code, the values of the <code>cics</code> and <code>cice</code> parameters is from 0 to 16383.</p> <p>8. If the service indicator parameter value is 13, the values of the <code>cics</code> and <code>cice</code> parameters is from 0 to 4294967295.</p> <p>9. The CIC range, defined by the <code>cics</code> and <code>cice</code> parameters, cannot overlap the CIC range in an existing routing key.</p> <p>10. The following rules apply to using the <code>rcontext</code> parameter.</p> <ul style="list-style-type: none"> • The value of the <code>rcontext</code> parameter is from 0 to 4294967295. • The <code>rcontext</code> parameter is required for a routing key containing an SUA application server. • The <code>rcontext</code> parameter is optional for a routing key containing an M3UA application server. • The <code>rcontext</code> parameter value must be unique in the database. Multiple routing keys cannot have the same <code>rcontext</code> value assigned. • An application server can be assigned to a maximum of four routing keys containing <code>rcontext</code> parameter values. • If the application server being assigned to the new routing key is assigned to other routing keys that do not contain <code>rcontext</code> parameter values, the <code>rcontext</code> parameter cannot be assigned to the new routing key. • If the application server being assigned to the new routing key is assigned to other routing keys that contain <code>rcontext</code> parameter values, the <code>rcontext</code> parameter must be assigned to the new routing key. 						

Canceling the `RTRV-AS` and `RTRV-APPL-RTKEY` Commands

Because the `rtrv-as` and `rtrv-appl-rtkey` commands used in this procedure can output information for a long period of time, the `rtrv-as` and `rtrv-appl-rtkey` commands can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-as` and `rtrv-appl-rtkey` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-as` or `rtrv-appl-rtkey` commands were entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-as` or `rtrv-appl-rtkey` commands were entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-as` and `rtrv-appl-rtkey` commands were entered, from another terminal other than the terminal where the `rtrv-as` or `rtrv-appl-rtkey` commands were

entered. To enter the **canc-cmd:trm=<xx>** command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the **rtrv-secu-trm** command. The user's permissions can be verified with the **rtrv-user** or **rtrv-secu-user** commands.

For more information about the **canc-cmd** command, go to the *Commands Manual*.

Procedure

1. Display the current application routing key information in the database by entering the **rtrv-appl-rtkey** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC      SI SSN      OPC      CICS      CICE
  STATIC    123-234-123  5 ---      122-124-125  1          1000
  STATIC    123-234-123  5 ---      100-100-100 1001        5000
  1105      005-005-001  5 ---      010-010-001 1          500
  1105      005-005-001  5 ---      010-010-001 501        1000
  1107      006-006-001  5 ---      011-011-001 1          500
  1107      006-006-001  5 ---      011-011-001 501        1000

KEY:LOC      DPCI      SI SSN      OPC      CICS      CICE
  STATIC    2-100-7      6 ---      -----      -----      -----
  STATIC    3-137-6      6 ---      -----      -----      -----
  STATIC    4-035-7      5 ---      3-200-4      200          300
  STATIC    6-006-6      5 ---      1-002-3      150          175
  STATIC    6-006-7      6 ---      -----      -----      -----
  STATIC    6-006-8      3 170      -----      -----      -----
  STATIC    6-006-8      5 ---      1-002-3      75           100
  STATIC    6-024-7      5 ---      1-057-4      150          175
  STATIC    6-024-7      5 ---      2-175-5      150          175
  STATIC    7-008-7      6 ---      -----      -----      -----

KEY:LOC      DPC      SI SSN      OPC      CICS      CICE
  STATIC    DEFAULT KEY ** *** ***** ***** *****

STATIC Route Key table is (13 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (13 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

The database can contain only one default routing key. If the **rtrv-appl-rtkey** output contains a default routing key, a default routing key cannot be added in this procedure. Go to step 2 to add either a full or partial routing key with the desired application server.

2. Display the current application server information in the database by entering the `rtrv-as` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
      AS Name           Mode           ASP Names
      as1              LOADSHARE     asp1
                                      asp2
                                      asp3
                                      asp5
                                      asp6
      as2              OVERRIDE      asp7
      as3              LOADSHARE     asp8
                                      asp9
      as4              LOADSHARE     asp10
                                      asp11
      as5              LOADSHARE     asp12
                                      asp13
```

AS table is (5 of 250) 1% full.

If the required application server is not in the database, go to the “Adding an Application Server” procedure on page 3-397 to add the application server.

If the `rcontext` parameter will not be specified for the routing key, make sure that the `adapter` parameter value for the associations assigned to the new application server is **M3UA**.

If the `rcontext` parameter will be specified for the routing key, make sure that the `open` parameter value of the associations is set to `no`. The `adapter` parameter value of these associations can be either **SUA** or **M3UA**.

SUA associations, and their corresponding ASPs and application server, can be assigned to only these types of routing keys:

- Full routing key – DPC/SI=3/SSN
- Partial routing key – DPC/SI=3
- Partial routing key – DPC only
- Partial routing key – SI=3 only
- Default routing key.

After the new application server is added to the database, go to step 4.

3. Display the routing keys containing the application server being used in this procedure by entering the `rtrv-appl-rtkey` command with the application server name and the `display=all` parameter. For this example, enter these commands.

```
rtrv-appl-rtkey:asname=as3:display=all
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0

KEY:LOC      DPCI      SI SSN    OPCI      CICS      CICE
  STATIC    6-024-7    5 ---    1-057-4    150      175
  RCONTEXT:-
  ASNAME:as3
  ANAMES:assoc11      assoc12

KEY:LOC      DPCI      SI SSN    OPCI      CICS      CICE
  STATIC    2-100-7    6 ---    -----
  RCONTEXT:-
  ASNAME:as3
  ANAMES:assoc11      assoc12

STATIC Route Key table is (7 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

```
rtrv-appl-rtkey:asname=as4:display=all
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0

KEY:LOC      DPCI      SI SSN    OPCI      CICS      CICE
  STATIC    4-035-7    5 ---    3-200-4    200      300
  RCONTEXT:225
  ASNAME:as4
  ANAMES:assoc15      assoc16

KEY:LOC      DPCI      SI SSN    OPCI      CICS      CICE
  STATIC    3-137-6    6 ---    -----
  RCONTEXT:300
  ASNAME:as4
  ANAMES:assoc15      assoc16

KEY:LOC      DPC      SI SSN    OPC      CICS      CICE
  STATIC    DEFAULT KEY ** *** *****
  RCONTEXT:450
  ASNAME:as4
  ANAMES:assoc15      assoc16

STATIC Route Key table is (7 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

If the application server is not assigned to any routing keys, the **rcontext** parameter can be specified for the new routing key using this application server. Go to step 4.

If the application server is assigned to other routing keys, and the routing keys do not contain **rcontext** parameter values, the **rcontext** parameter cannot be specified for the new routing key being added in this procedure. If you wish to use the **rcontext** parameter for the new routing key, go to step 2 and choose another application server that is assigned to routing keys containing **rcontext** parameter values, or add a new application server to the database.

If you do not wish to use the **rcontext** parameter for the new routing key, go to step 7.

If the application server is assigned to other routing keys, and the routing keys contain **rcontext** parameter values, the **rcontext** parameter must be specified for the new routing key being added in this procedure. An application server can be assigned to a maximum of four routing keys containing **rcontext** parameter values. If the application server is assigned to four routing keys containing **rcontext** parameter values, the application server cannot be assigned to the new routing key being added in this procedure. Go to step 2 and choose another application server to assign to the routing key, or add a new application server to the database.

If the application server is assigned to less than four routing keys containing **rcontext** parameter values, the application server can be assigned to the new routing key being added in this procedure. Go to step 4.

-
4. Display the application server processes (ASPs) assigned to the application server shown in step 2, or added in step 2, using the **rtrv-asp** command and specifying the ASP name shown in step 2, or added in step 2,. For this example, enter these commands.

```
rtrv-asp:aspname=asp8
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP          ASSOCIATION          UAPS
asp8         assoc11          10
```

```
ASP Table is (3 of 4000) 1% full
```

```
rtrv-asp:aspname=asp9
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP          ASSOCIATION          UAPS
asp9         assoc12          10
```

```
ASP Table is (3 of 4000) 1% full
```

```
rtrv-asp:aspname=asp10
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP                ASSOCIATION                UAPS
asp10              assoc15                      10
```

```
ASP Table is (3 of 4000) 1% full
```

```
rtrv-asp:aspname=asp11
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP                ASSOCIATION                UAPS
asp11              assoc16                      10
```

```
ASP Table is (3 of 4000) 1% full
```

```
rtrv-asp:aspname=asp20
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP                ASSOCIATION                UAPS
asp20              assoc20                      10
```

```
ASP Table is (3 of 4000) 1% full
```

Repeat this step for each ASP assigned to the desired application server name shown in step 2 to display the association assigned to each ASP that is assigned to the application server.

-
5. Display the association assigned to the ASPs displayed in step 4, to verify the **open** parameter value of the association, using the **rtrv-assoc** command with the association names shown in step 4. For this example, enter these commands.

```
rtrv-assoc:aname=assoc11
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc11
  PORT      A
  ADAPTER   M3UA          VER          M3UA RFC
  LHOST     gw110.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030              RPORT       1030
  ISTRMS    2                OSTRMS      2
  RMODE     LIN          RMIN         120          RMAX         800
  RTIMES    10            CWMIN        3000
  OPEN      YES          ALW          YES
```

IP Appl Sock table is (10 of 4000) 1% full

rtrv-assoc:aname=assoc12

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc12
  PORT      A
  ADAPTER   M3UA          VER      M3UA RFC
  LHOST     gw200.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     2564          RPORT    1030
  ISTRMS    2             OSTRMS   2
  RMODE     LIN           RMIN     120          RMAX     800
  RTIMES    10           CWMIN    3000
  OPEN      YES          ALW      YES
IP Appl Sock table is (10 of 4000) 1% full
```

rtrv-assoc:aname=assoc15

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc15
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw150.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1500          RPORT    1030
  ISTRMS    2             OSTRMS   2
  RMODE     LIN           RMIN     120          RMAX     800
  RTIMES    10           CWMIN    3000
  OPEN      YES          ALW      YES
IP Appl Sock table is (4 of 4000) 1% full
```

rtrv-assoc:aname=assoc16

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc16
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw160.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     3571          RPORT    1030
  ISTRMS    2             OSTRMS   2
  RMODE     LIN           RMIN     120          RMAX     800
  RTIMES    10           CWMIN    3000
  OPEN      YES          ALW      YES
IP Appl Sock table is (4 of 4000) 1% full
```

```
rtrv-assoc:aname=assoc20
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc20
  PORT      A
  ADAPTER   SUA          VER          SUA RFC
  LHOST     gw180.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     2080          RPORT     1030
  ISTRMS    2              OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES          ALW       YES
IP Appl Sock table is (4 of 4000) 1% full
```

Repeat this step for each association name displayed in step 4 to verify the **open** parameter of each association assigned to the application server.

NOTE: If the **rcontext** parameter is not being specified in this procedure, skip step 6 and go to step 7.

NOTE: If the **open** parameter value for all the associations assigned to the application server is **no** (shown in step 5 or assigned to the new application server added in step 2), skip step 6 and go to step 7.

6. Change the value of the **open** parameter to **no** by specifying the **chg-assoc** command with the **open=no** parameter. For this example, enter this command.

```
chg-assoc:aname=assoc11:open=no
chg-assoc:aname=assoc12:open=no
chg-assoc:aname=assoc15:open=no
chg-assoc:aname=assoc16:open=no
chg-assoc:aname=assoc20:open=no
```

When each of these commands have successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD
```



CAUTION: The IP connections using the associations specified in this step will not be able to carry any traffic when the **open** parameter is changed to **no**.

Repeat this step for all the associations assigned to the application server that have the **open=yes** parameter value.

NOTE: If a default routing key is being added to the database, or if the SI value of the routing key being added is a value other than 4, 5, or 13, skip steps 7 and 8, and go to step 9.

7. Verify that the ISUP Routing over IP feature is on, by entering the `rtrv-feat` command. If the ISUP Routing over IP feature is on, the `IPISUP` field should be set to `on`. For this example, the ISUP Routing over IP feature is off.

NOTE: The `rtrv-feat` command output contains other fields that are not used by this procedure. If you wish to see all the fields displayed by the `rtrv-feat` command, see the `rtrv-feat` command description in the *Commands Manual*.

NOTE: If the ISUP Routing over IP feature is on, skip step 8 and go to step 9.

8. Turn the ISUP Routing over IP feature on by entering this command.

```
chg-feat:ipisup=on
```

NOTE: Once the ISUP Routing over IP feature is turned on with the `chg-feat` command, it cannot be turned off.

The ISUP Routing over IP feature must be purchased before you turn this feature on with the `chg-feat` command. If you are not sure if you have purchased the ISUP Routing over IP feature, contact your Tekelec Sales Representative or Account Representative.

When the `chg-feat` has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 11:43:04 GMT EAGLE5 31.10.0
CHG-FEAT: MASP A - COMPLTD
```

9. Add an application routing key entry to the database by entering the `ent-appl-rtkey` command. The parameters required for the `ent-appl-rtkey` command are determined by the type of routing key being added and the service indicator value in the routing key. See Table 3-21 on page 3-242 for the parameter combinations that can be used for the type of routing key being added to the database.

For this example, enter these commands.

```
ent-appl-rtkey:dpci=3-009-3:si=5:opci=4-100-3:cics=100
:cice=500:asname=as3:type=full

ent-appl-rtkey:dpci=4-200-3:si=5:opci=5-135-7:cics=1000
:cice=2000:asname=as4:type=full:rcontext=1000

ent-appl-rtkey:dpci=1-050-2:si=5:opci=6-077-7:cics=200
:cice=300:asname=as20:type=full:rcontext=2000
```

When each of these commands have successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
ENT-APPL-RTKEY: MASP A - COMPLTD
```

10. Verify the new application routing key information in the database by entering the `rtrv-appl-rtkey` command with the routing key parameters specified in step 9 (`dpc`, `si`, `opc`, `cics`, `cice`, `ssn`, `asname`, `type`, and `rcontext`, as applicable) with the `display=all` parameter. For this example, enter these commands.

```
rtrv-appl-rtkey:dpci=3-009-3:si=5:opci=4-100-3:cics=100
:cice=500:asname=as3:type=full:display=all
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0

KEY:LOC      DPCI      SI SSN OPCI      CICS      CICE
  STATIC    3-009-3   5 --- 4-100-3   100       500
          RCONTEXT:-
          ASNAME:as3
          ANAMES:assoc11      assoc12
```

```
STATIC Route Key table is (12 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full
```

```
STATIC Route Key Socket Association table is (12 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

```
rtrv-appl-rtkey:dpci=4-200-3:si=5:opci=5-135-7:cics=1000
:cice=2000:asname=as4:type=full:rcontext=1000:display=all
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0

KEY:LOC      DPCI      SI SSN OPCI      CICS      CICE
  STATIC    4-200-3   5 --- 5-135-7   1000     2000
          RCONTEXT:1000
          ASNAME:as4
          ANAMES:assoc15      assoc16
```

```
STATIC Route Key table is (12 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full
```

```
STATIC Route Key Socket Association table is (12 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

```
rtrv-appl-rtkey:dpci=1-050-2:si=5:opci=6-077-7:cics=200
:cice=300:asname=as20:type=full:rcontext=2000:display=all
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

```
KEY:LOC      DPCI      SI SSN OPCI      CICS      CICE
  STATIC    1-050-2    5 --- 6-077-7    200      300
          RCONTEXT:2000
          ASNAME:as20
          ANAMES:assoc20
```

```
STATIC Route Key table is (12 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full
```

```
STATIC Route Key Socket Association table is (12 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

NOTE: If the **open** parameter value of the associations assigned to the routing key added in this procedure was not changed (step 6 was not performed), skip this step and go to step 12.

11. Change the value of the **open** parameter of the associations that were changed in step 6 to **yes** by specifying the **chg-assoc** command with the **open=yes** parameter. For this example, enter these commands.

```
chg-assoc:aname=assoc11:open=yes
chg-assoc:aname=assoc12:open=yes
chg-assoc:aname=assoc15:open=yes
chg-assoc:aname=assoc16:open=yes
chg-assoc:aname=assoc20:open=yes
```

When each of these commands have successfully completed, this message should appear.

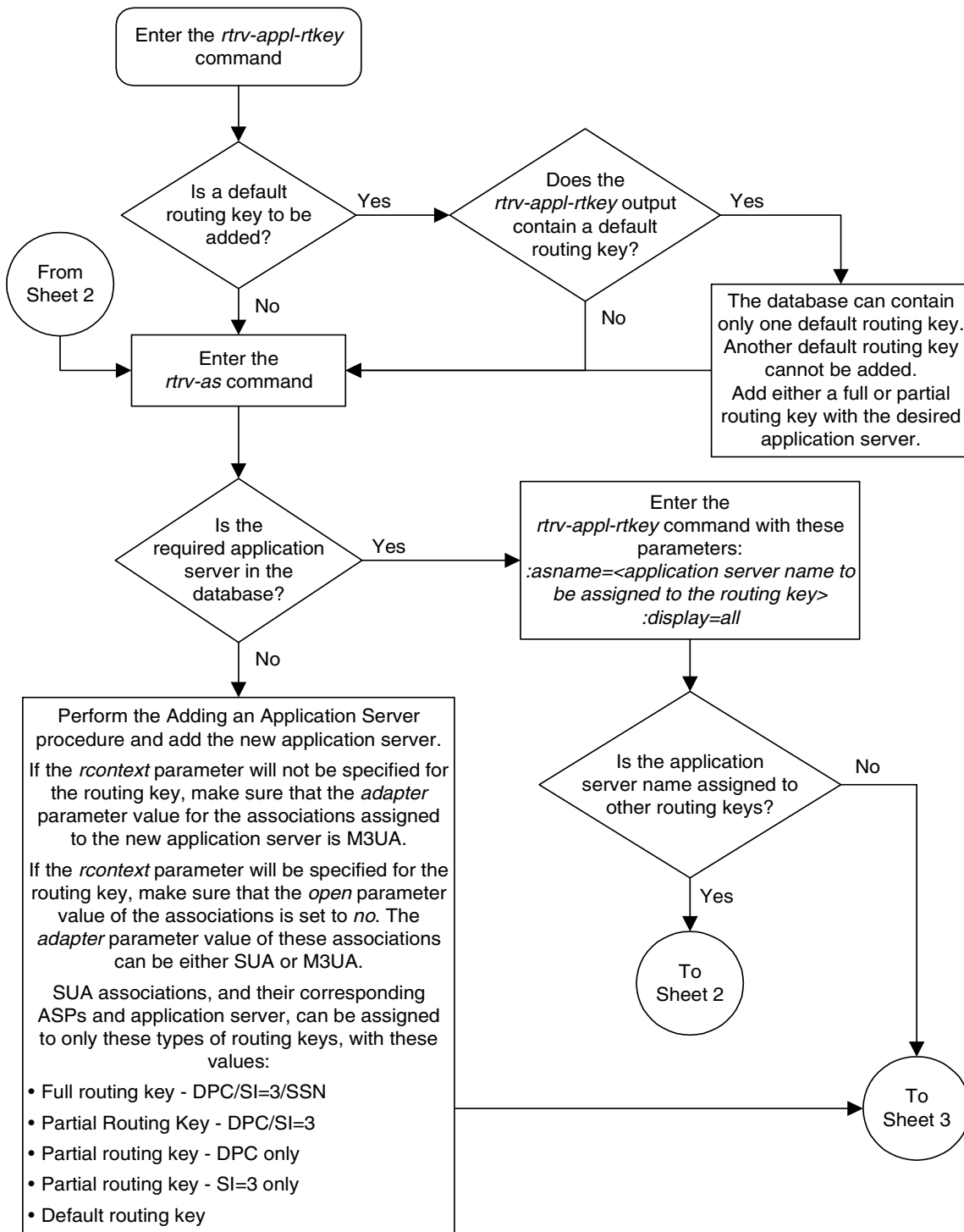
```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

Repeat this step for all the associations that were changed in step 6.

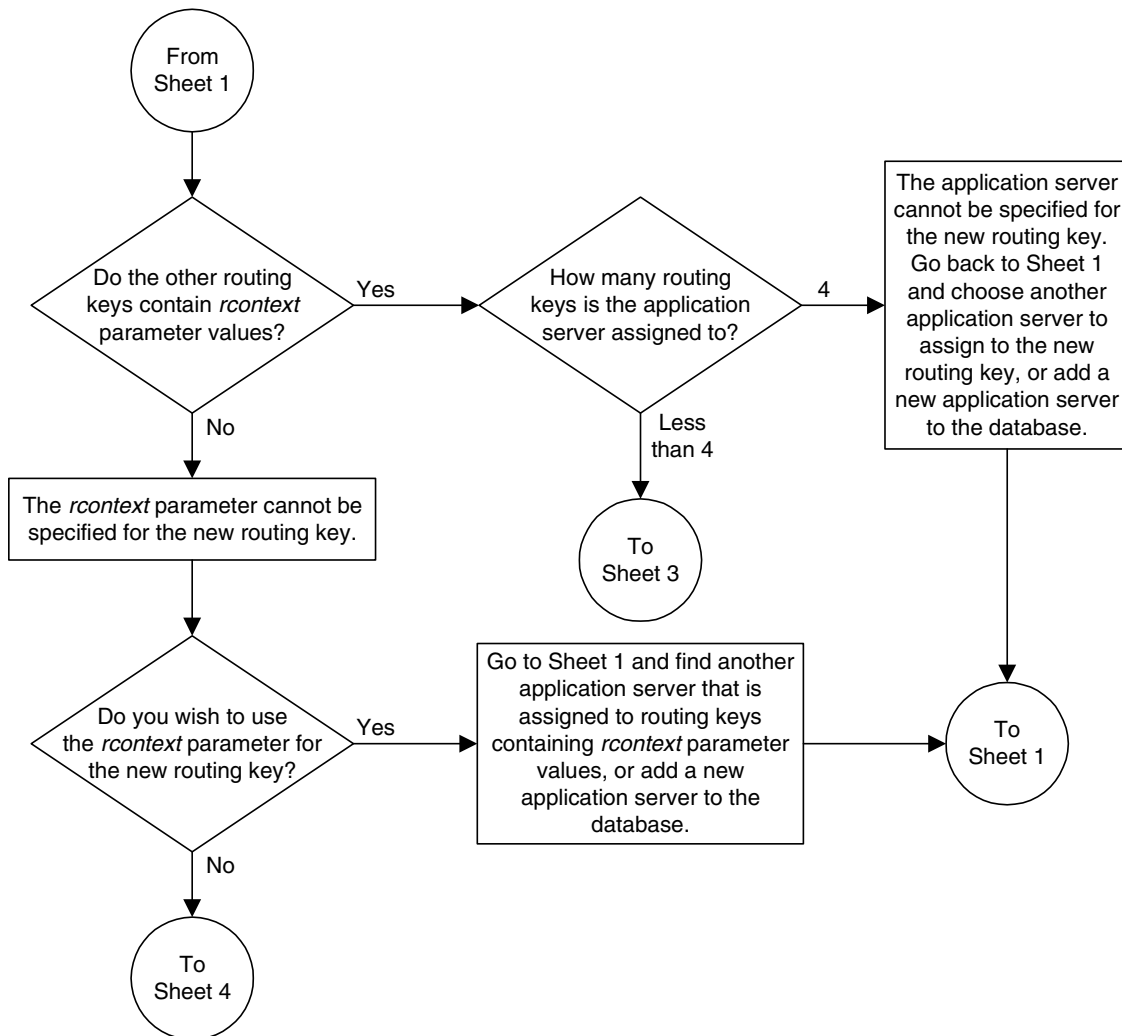
12. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

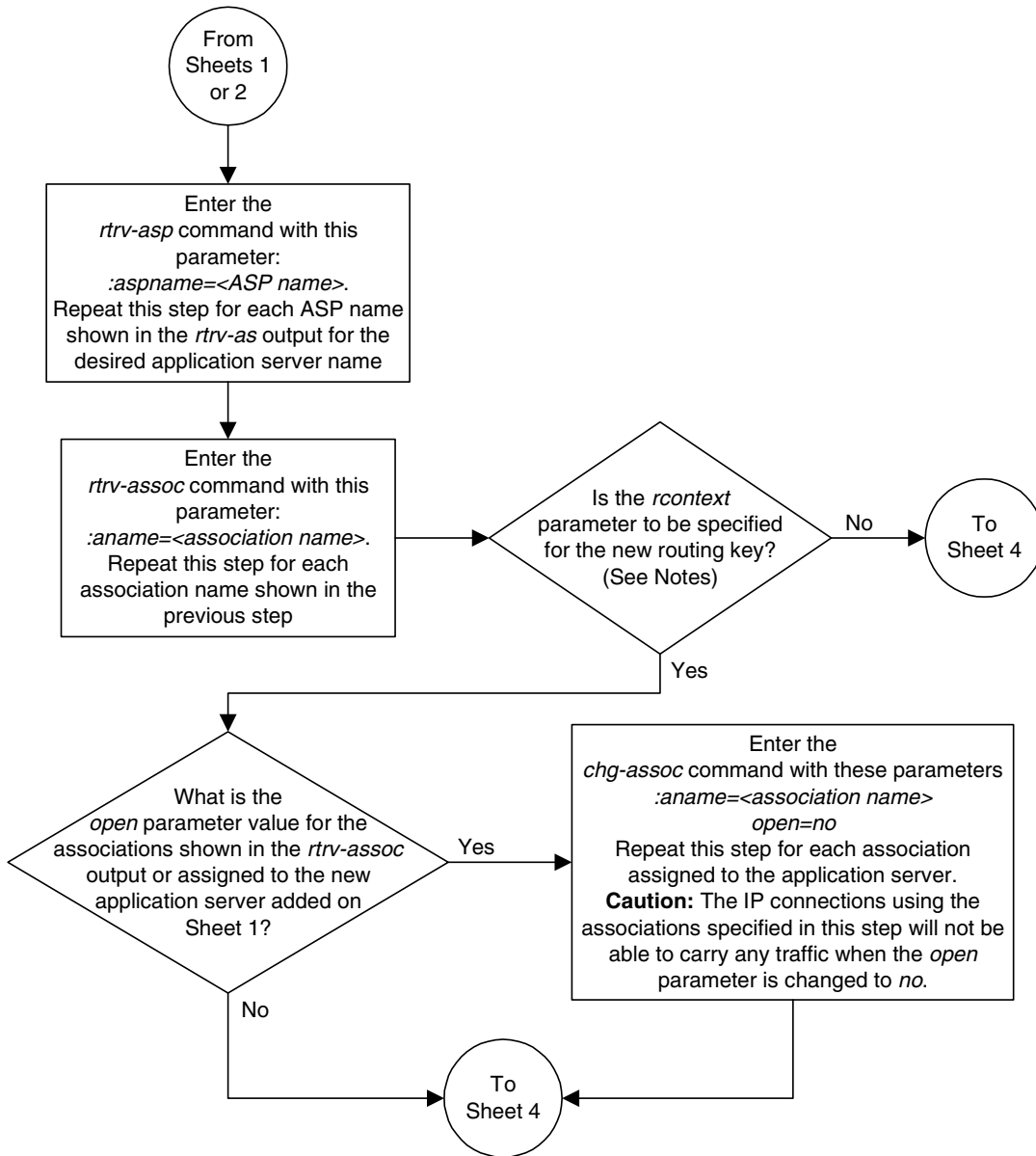
Flowchart 3-23. Adding an Application Routing Key Containing an Application Server (Sheet 1 of 4)



Flowchart 3-23. Adding an Application Routing Key Containing an Application Server (Sheet 2 of 4)



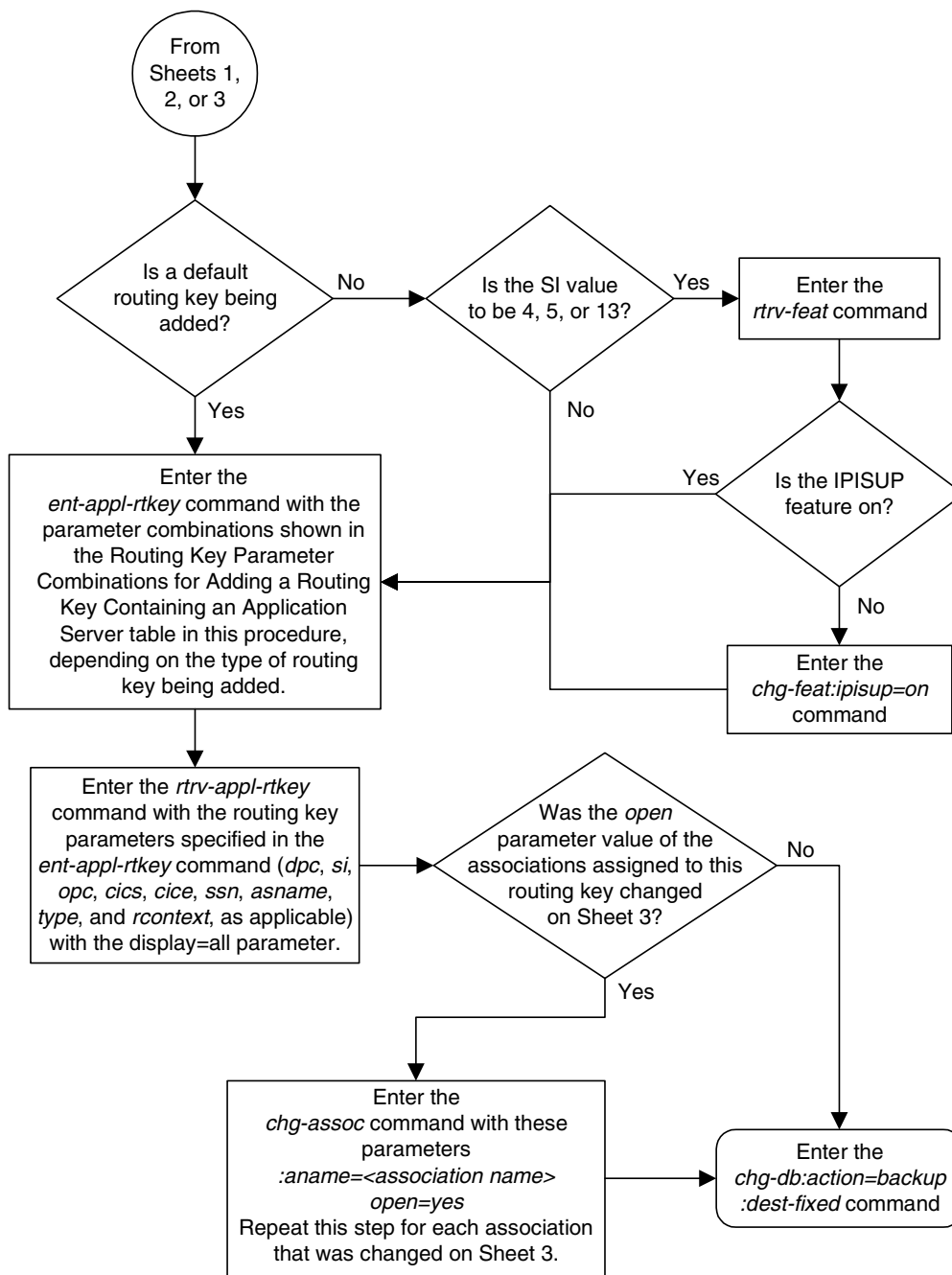
Flowchart 3-23. Adding an Application Routing Key Containing an Application Server (Sheet 3 of 4)



Notes:

1. If the *adapter* parameter value for the application server is SUA, and a new application server is specified for the routing key, the *rcontext* parameter is required.
2. If the *adapter* parameter value for the application server is M3UA, and a new application server is specified for the routing key, the *rcontext* parameter is optional.
3. If the application server is assigned to other routing keys, and those routing keys contain routing context values (no more than 3 routing keys), the *rcontext* parameter must be specified for this routing key.
4. If the application server is assigned to other routing keys, and those routing keys do not contain routing context values, the *rcontext* parameter cannot be specified for this routing key.

Flowchart 3-23. Adding an Application Routing Key Containing an Application Server (Sheet 4 of 4)



Removing an Application Routing Key

This procedure is used to remove a static or dynamic application routing key from the database using the `dlr-app1-rtkey` command. For more information about static and dynamic routing keys, see “Understanding Routing for SS7IPGW and IPGW Applications” on page 2-23.

The `dlr-app1-rtkey` command uses these parameters.

:dpc/dpca/dpci/dpcn/dpca24 – The destination point code value that is used to filter incoming MSUs.

:opc/opca/opci/opcn/opcn24 – The originating point code value that is used to filter incoming MSUs. This parameter must not specify a cluster route. This parameter must not specify a cluster route. This parameter is only valid when the `si` parameter value is set to 4, 5, or 13. This parameter is required if `si=4, 5, or 13` and `type=full`.

NOTE: See the “Point Code Formats” section in the *Database Administration Manual - SS7* for a definition of the point code types that are used on the system and for a definition of the different formats that can be used for ITU national point codes.

:si – The service indicator value that is used to filter incoming MSUs. The range of values for the service indicator parameter (`si`) can be a numerical value from 0 to 15, or for selected service indicator values, a text string can be used instead of numbers. Table 3-22 shows the text strings that can be used in place of numbers for the service indicator values.

Table 3-22. Service Indicator Text String Values

Service Indicator Value	Text String
0	snm
1	regtest
2	spltst
3	sccp
4	tup
5	isup
13	qbicc

:ssn – The subsystem value that is used to filter incoming MSUs. The `ssn` parameter is only valid when the `si` parameter value is set to 3 or `sccp`.

:sname – The name of the socket that will receive the incoming MSU.

:cics – The starting circuit identification code that is used to filter incoming MSUs. Specify with `cice` to delete routing keys with the circuit identification

code or range of circuit identification codes. The **cics** parameter is only valid when the **si** parameter value is set to **4**, **5**, or **13**. The **cics** is required if **si=4**, **5**, or **13** and **type=full**.

:cice - The ending circuit identification code that is used to filter incoming MSUs. Specify with **cics** to delete routing keys with the circuit identification code or range of circuit identification codes. The **cice** parameter is only valid when the **si** parameter value is set to **4**, **5**, or **13**. The **cics** is required if **si=4**, **5**, or **13** and **type=full**.

:loc - Card location that indicates from which **ss7ipgw** or **ipgwi** card to delete a dynamic routing key entry. If this parameter is not specified, a static entry is deleted.

:type - Identifies the type of application routing key that is being deleted. One of three values, **type = full/partial/default**. If **type** is not explicitly specified, **type = full** is assumed.

:asname - Application server (AS) name.

The parameter combinations used by the **dlt-app1-rtkey** command are based on the type of routing key and the service indicator value in the routing key. The parameter combinations are shown in Table 3-23 on page 3-260.

Table 3-23. Routing Key Parameter Combinations for Removing Routing Keys

SI=3 (SCCP)		SI=4 (TUP), 5 (ISUP), 13 (QBICC)		Other SI Values		Default Routing Key ¹
Full Routing Key ¹	Partial Routing Key ¹	Full Routing Key ¹	Partial Routing Key ¹	Full Routing Key ¹	Partial Routing Key ¹	
dpc	sname	dpc	sname	dpc	sname	sname
si=3 ¹	type=partial	si=4, 5, 13 ¹	type=partial	si=value other than 3, 4, 5, 13 ¹	type=partial	type=default
ssn	dpc ²	opc	dpc ²	sname	dpc ²	asname
type=full	si=3 ^{1, 2}	cics	si=4, 5, 13 ^{1, 2}	type=full	si=value other than 3, 4, 5, 13 ^{1, 2}	loc ³
sname	asname	cice	opc ²	asname	asname	
asname	loc ³	type=full	asname	loc ³	loc ³	
loc ³		sname	loc ³			
		asname				
		loc ³				

Notes:

1. The values for these parameters must be entered exactly as shown in the `rtrv-appl-rtkey` command output for the routing key being removed. However, text strings can be used in place of some numerical service indicator values. See Table 3-22 on page 3-258 for a list of these text strings.
2. These parameters are optional for partial routing keys, but at least one these parameters must be specified with the `dlt-appl-rtkey` command.
3. If the `loc` parameter is not specified, a static entry that matches the other specified parameters is deleted.

Canceling the RTRV-APPL-RTKEY Command

Because the `rtrv-appl-rtkey` command used in this procedure can output information for a long period of time, the `rtrv-appl-rtkey` command can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-appl-rtkey` command can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-appl-rtkey` command was entered.
- Enter the `cancel-cmd` without the `trm` parameter at the terminal where the `rtrv-appl-rtkey` command was entered.
- Enter the `cancel-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-appl-rtkey` commands were entered, from another terminal other than the terminal where the `rtrv-appl-rtkey` command was entered. To enter the `cancel-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can

be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `cancl-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current application routing key information in the database by entering the `rtrv-appl-rtkey` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC      SI SSN      OPC      CICS      CICE
  STATIC    123-234-123  5 ---      122-124-125  1          1000
  STATIC    123-234-123  5 ---      100-100-100 1001        5000
    1105     005-005-001  5 ---      010-010-001  1           500
    1105     005-005-001  5 ---      010-010-001 501         1000
    1107     006-006-001  5 ---      011-011-001  1           500
    1107     006-006-001  5 ---      011-011-001 501         1000

KEY:LOC      DPCI      SI SSN      OPCI      CICS      CICE
  STATIC    6-006-6     3 170 -----
  STATIC    6-006-7     6 --- -----
  STATIC    6-006-6     5 ---      1-002-3     150         175
  STATIC    6-006-6     5 ---      1-002-3     75          100

KEY:LOC      DPC      SI SSN      OPC      CICS      CICE
  STATIC    DEFAULT KEY ** *** ***** ***** *****

STATIC Route Key table is (7 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

2. Display the specific routing key information for the routing key being removed from the database by entering the `rtrv-appl-rtkey` command with the `display=all` parameter and the `DPC`, `SI`, `SSN`, `OPC`, `CICS`, or `CICE` values shown in the `rtrv-appl-rtkey` output in step 1 for the routing key being removed. For this example, enter these commands.

```
rtrv-appl-rtkey:dPCA=006-006-001:si=5:cics=501:cice=1000
:display=all
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC      SI SSN    OPC      CICS      CICE
    1107    006-006-001  5 ---    011-011-001  501      1000
          ATTR:PSTNCAT PSTNID NORM DUP
                   0      0 N    -
          SNAMEs:socket31
```

```
STATIC Route Key table is (7 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full
```

```
STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

```
rtrv-appl-rtkey:dpci=6-006-6:si=3:ssn=170:display=all
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
KEY:LOC      DPCI      SI SSN    OPC      CICS      CICE
    STATIC    6-006-6    3 170  -----  -----  -----
          RCONTEXT:-
          ASNAME:as2
          ANAMES:assoc1
```

```
STATIC Route Key table is (7 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full
```

```
STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

NOTE: If an application server is not assigned to the routing key, or if the routing key containing an application server shown in step 2 does not contain a routing context value (`rcontext` parameter value), skip steps 3 and 4, and go to step 5.

3. Display the association assigned to the routing key by entering the `rtrv-assoc` parameter with the association name shown in step 2. For this example, enter this command.

```
rtrv-assoc:aname=assoc1
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc1
  PORT      A
  ADAPTER   M3UA          VER          M3UA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030          RPORT     1030
  ISTRMS    2            OSTRMS    2
  RMODE     LIN           RMIN      120          RMAX      800
  RTIMES    10           CWMIN    3000
  OPEN      YES          ALW        YES
IP Appl Sock table is (7 of 4000) 1% full
```

Repeat this step for all the associations shown in step 2.

NOTE: If the `open` parameter value of all the associations shown in step 3 is `no`, skip step 4 and go to step 5.

4. Change the `open` parameter value of the association to `no` by using the `chg-assoc` command. For example, enter this command.

```
chg-assoc:aname=assoc1:open=no
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:18:37 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD
```



CAUTION: The IP connections using the associations specified in this step will not be able to carry any traffic when the `open` parameter is changed to `no`.

Repeat this step for all the associations shown in step 3 that contain the `open=yes` parameter value.

-
5. Remove application routing key information from the database by entering the `dlt-appl-rtkey` command. The parameters required for the `dlt-appl-rtkey` command are determined by the type of routing key being added and the service indicator value in the routing key. See Table 3-23 on page 3-260 for the parameter combinations that can be used for the type of routing key being added to the database. For example, enter these commands.

```
dlt-appl-rtkey:dpca=006-006-001:loc=1107:si=5:cics=501
:cice=1000:sname=socket31
```

```
dlt-appl-rtkey:dpca=6-006-6:si=3:ssn=170:asname=as2
```

When each of these commands have successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
DLT-APPL-RTKEY: MASP A - COMPLTD
```

- Verify the changes by entering the `rtrv-appl-rtkey` command with the routing key parameters specified in step 5 (`dpc`, `si`, `opc`, `cics`, `cice`, `ssn`, `asname`, `sname`, `type`, and `loc`, as applicable). For this example, enter these commands.

```
rtrv-appl-rtkey:dPCA=006-006-001:loc=1107:si=5:cics=501
:cice=1000
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

STATIC Route Key table is (6 of 2000) 1% full
1105 Route Key table is (2 of 500) 1% full
1107 Route Key table is (1 of 500) 1% full

STATIC Route Key Socket Association table is (6 of 32000) 1% full
1105 Route Key Socket Association table is (2 of 8000) 1% full
1107 Route Key Socket Association table is (1 of 8000) 1% full
```

```
rtrv-appl-rtkey:dpci=6-006-6:si=3:ssn=170:asname=as2
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

STATIC Route Key table is (6 of 2000) 1% full
1105 Route Key table is (2 of 500) 1% full
1107 Route Key table is (1 of 500) 1% full

STATIC Route Key Socket Association table is (6 of 32000) 1% full
1105 Route Key Socket Association table is (2 of 8000) 1% full
1107 Route Key Socket Association table is (1 of 8000) 1% full
```

NOTE: If step 4 was not performed, skip step 7 and go to step 8.

- Change the `open` parameter value of the associations that were changed in step 4 to `yes` by using the `chg-assoc` command. For example, enter this command.

```
chg-assoc:aname=assoc1:open=yes
```

When this command has successfully completed, the following message should appear.

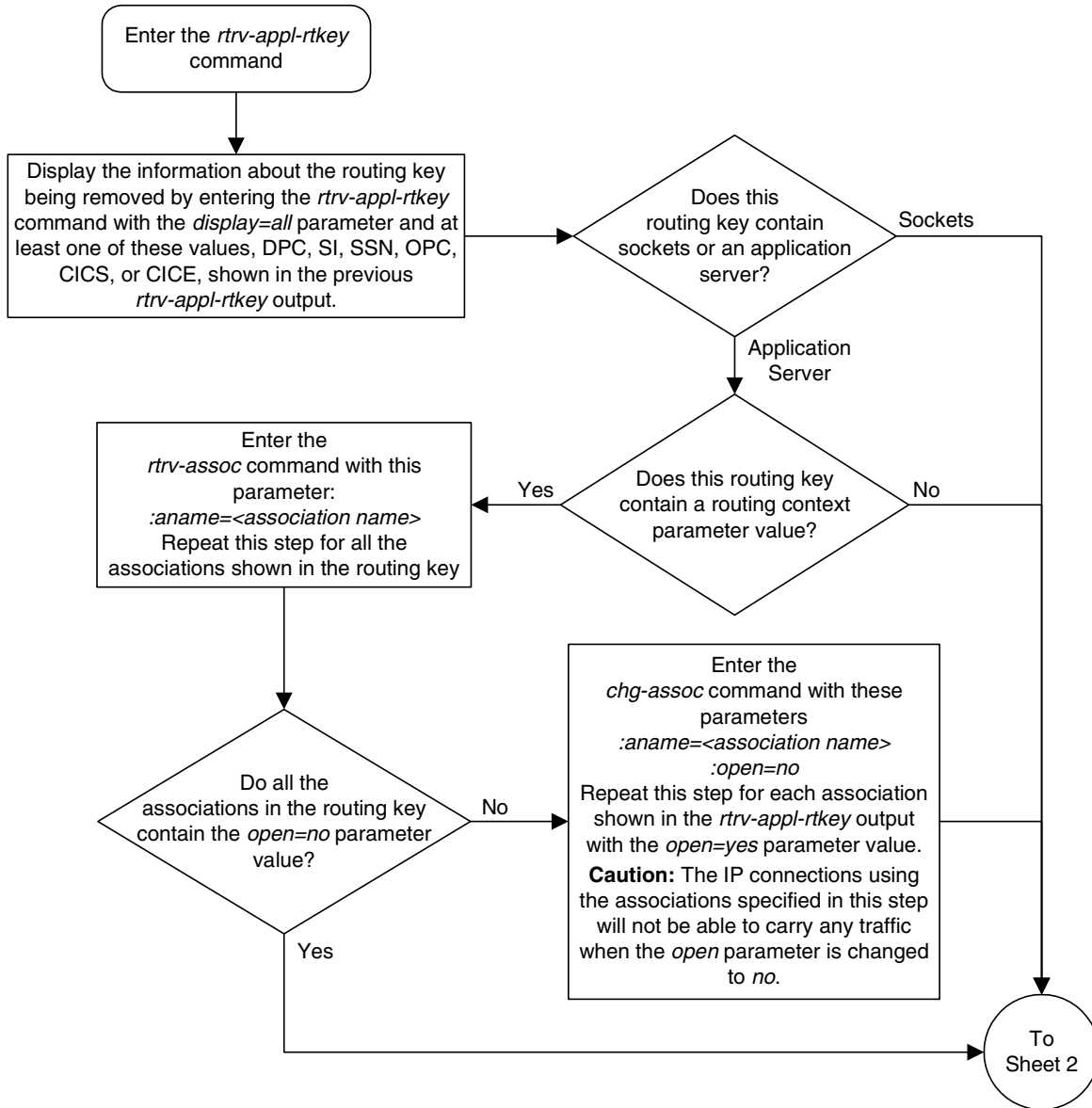
```
rlghncxa03w 04-12-28 21:18:37 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD
```

Repeat this step for all the associations that were changed in step 4.

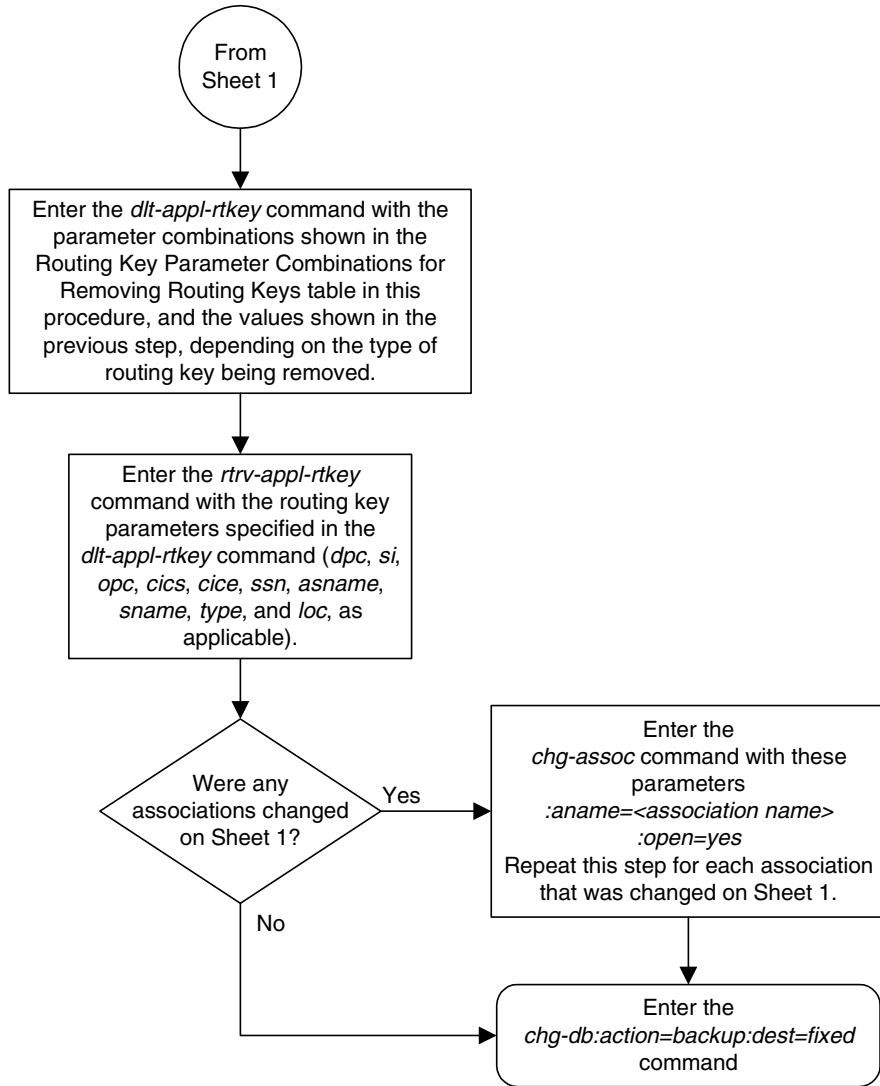
- Back up the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-24. Removing an Application Routing Key (Sheet 1 of 2)



Flowchart 3-24. Removing an Application Routing Key (Sheet 2 of 2)



Replacing the IP Connections in an Existing Application Routing Key with a Single Socket

Performing this procedure replaces all the IP connections assigned to an existing application routing key with a single socket. The IP connections can be sockets (defined by the `sname` parameter in the `rtrv-app1-rtkey` output), or an application server (defined by the `asname` parameter in the `rtrv-app1-rtkey` output). The `chg-app1-rtkey` and these parameters are used in this procedure.

NOTE: If the routing key has any sockets assigned to it, the new socket name (defined by the `nsname` parameter) replaces all the existing socket names. If you still wish to use some of the old socket names that were assigned to the routing key, perform the “Adding an Application Routing Key Containing a Socket” procedure on page 3-228 to add these socket names to the routing key.

`:dpc/dpca/dpci/dpcn/dpcn24` – Destination point code value that is used to filter incoming MSUs.

`:opc/opca/opci/opcn/opcn24` – The originating point code value that is used to filter incoming MSUs. This value must not specify a cluster route.

NOTE: See the “Point Code Formats” section in the *Database Administration Manual - SS7* for a definition of the point code types that are used on the system and for a definition of the different formats that can be used for ITU national point codes.

`:si` – The service indicator value that is used to filter incoming MSUs. The range of values for the service indicator parameter (`si`) can be a numerical value from 0 to 15, or for selected service indicator values, a text string can be used instead of numbers. Table 3-24 shows the text strings that can be used in place of numbers for the service indicator values.

Table 3-24. Service Indicator Text String Values

Service Indicator Value	Text String
0	snm
1	regtest
2	spltst
3	sccp
4	tup
5	isup
13	qbicc

`:ssn` – The subsystem number value that is used to filter incoming MSUs.

:nsname – The name of the new socket that will receive the incoming MSU. The new socket name replaces all of the existing IP connections assigned to the routing key.

:cics - Starting circuit identification code that is used to filter incoming MSUs. Specify with **cice** to identify the routing key to be changed.

:cice - Ending circuit identification code that is used to filter incoming MSUs. Specify with **cics** to identify the routing key to be changed.

:type - Key type. Identifies the type of application routing key that will be changed. One of three values, **type = full/partial/default**. If **type** is not explicitly specified, **type = full** is assumed.

The **chg-app1-rtkey** command contains other parameters that are not used in this procedure.

:ncics - New starting circuit identification code that is used to filter incoming MSUs.

:ncice - New ending circuit identification code that is used to filter incoming MSUs.

:split - The circuit identification code value where the specified range of the routing key specified by the **cics** and **cice** values is to be split into two entries.

:pstncat – The PSTN category assigned to the routing key.

:pstnid – The PSTN ID assigned to the routing key.

:norm – Specifies whether the ISUP Normalization process is enabled or disabled for MSUs using the routing key.

:nasname – The name of the new application server that will receive the incoming MSU.

:rcontext – The routing context parameter.

See the “Changing the CIC values in an Existing Application Routing Key” procedure on page 3-275 for changing a routing key using the **ncics**, **ncice**, and **split** parameters.

See the “Changing the Routing Context Value in an Existing Application Routing Key” procedure on page 3-283 for changing the routing context parameter value in an existing routing key.

See the “Replacing the IP Connections in an Existing Application Routing Key with an Application Server” procedure on page 3-293 for details about using the **nasname** parameter.

See the “Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key” procedure on page 3-307 for changing a routing key using the **pstncat**, **pstnid**, and **norm** parameters.

Rules for Replacing the IP Connections in an Existing Application Routing Key with a Single Socket

The parameter combinations used by the `chg-app1-rtkey` command to assign a new socket name to a routing key are shown in Table 3-25.

Table 3-25. Routing Key Parameter Combinations for Replacing the IP Connections in an Existing Application Routing Key with a Single Socket

SI=3 (SCCP)		SI=4 (TUP), 5 (ISUP), 13 (QBICC)		Other SI Values		Default Routing Key
Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	
nsname ^{3, 4}	nsname ^{3, 4}	nsname ^{3, 4}	nsname ^{3, 4}	nsname ^{3, 4}	nsname ^{3, 4}	nsname ^{3, 4}
dpc ¹	type=partial	dpc ¹	type=partial	dpc ¹	type=partial	type=default
si=3 ¹	dpc ^{1, 2}	si=4, 5, 13 ¹	dpc ^{1, 2}	si=value other than 3, 4, 5, 13 ¹	dpc ^{1, 2}	
ssn ¹	si=3 ^{1, 2}	opc ¹	si=4, 5, 13 ^{1, 2}	type=full	si=value other than 3, 4, 5, 13 ^{1, 2}	
type=full		cics ¹	opc ^{1, 2}			
		cice ¹				
		type=full				

Notes:

1. The values for these parameters must be entered exactly as shown in the `rtrv-app1-rtkey` command output for the routing key being changed. However, text strings can be used in place of some numerical service indicator values. See Table 3-24 on page 3-267 for a list of these text strings. The text string must correspond to the numerical value shown in the routing key being changed.
2. These parameters are optional for partial routing keys, but at least one these parameters must be specified with the `chg-app1-rtkey` command.
3. Changing the socket name for a routing key that has any socket names assigned to it replaces all the socket names in the routing key with the new socket name. Perform the "Adding an Application Routing Key Containing a Socket" procedure on page 3-228 to add any of the old socket names to the routing key.
4. A socket name cannot be assigned to a routing key containing a routing context (`rcontext`) parameter value.

Canceling the RTRV-APPL-SOCK and RTRV-APPL-RTKEY Commands

Because the `rtrv-appl-sock` and `rtrv-appl-rtkey` commands used in this procedure can output information for a long period of time, the `rtrv-appl-sock` and `rtrv-appl-rtkey` commands can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-appl-sock` and `rtrv-appl-rtkey` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-appl-sock` or `rtrv-appl-rtkey` commands were entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-appl-sock` or `rtrv-appl-rtkey` commands were entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-appl-sock` or `rtrv-appl-rtkey` commands were entered, from another terminal other than the terminal where the `rtrv-appl-sock` or `rtrv-appl-rtkey` commands were entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current application routing key information in the database by entering the `rtrv-appl-rtkey` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC          SI SSN OPC          CICS          CICE
  STATIC 123-234-123 5 --- 122-124-125    1            1000
  STATIC 123-234-123 5 --- 100-100-100    1              50
    1105 005-005-001 5 --- 010-010-001    1              500
    1105 005-005-001 5 --- 010-010-001 501            1000
    1107 006-006-001 5 --- 011-011-001    1              500
    1107 006-006-001 5 --- 011-011-001 501            1000

1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (2 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

2. Display the specific routing key information for the routing key being changed by entering the `rtrv-appl-rtkey` command with the `display=all` parameter and the `DPC`, `SI`, `SSN`, `OPC`, `CICS`, or `CICE` values shown in the `rtrv-appl-rtkey` output in step 1 for the routing key being changed. For this example, enter this command.

```
rtrv-appl-rtkey:dpc=006-006-001:cics=501:cice=1000:display=all
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

```
KEY:LOC      DPC          SI SSN OPC          CICS      CICE
  STATIC 123-234-123  5 --- 122-124-125  1        1000
```

```
ATTR:PSTNCAT PSTNID NORM DUP
           0      0 N  -
SNAMES:kchlr11201
```

```
STATIC Route Key table is (2 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full
```

```
STATIC Route Key Socket Association table is (2 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

If the routing key contains a socket name, go to step 3.

A socket cannot be assigned to a routing key that contains a routing context value. If the routing key displayed in this step contains a routing context parameter value, this procedure cannot be performed.

If the routing key contains an application server, but the routing key does not contain a routing context value, go to step 3.

3. Display the current application socket information in the database by entering the `rtrv-appl-sock` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
SNAME kchlr11201
  PORT  A
  LHOST ipnode1-1201
  RHOST kc-hlr1
  LPORT 7000          RPORT 7000
  SERVER YES          DCMP5 1
  REXMIT FIXED       RTT 60
  OPEN  YES          ALW  NO

SNAME socket2
  PORT  A
  LHOST ipnode1-1203
  RHOST kc-hlr1
  LPORT 7005          RPORT 7005
  SERVER YES          DCMP5 10
  REXMIT FIXED       RTT 60
  OPEN  YES          ALW  YES
```

IP Appl Sock/Assoc table is (3 of 4000) 1% full

If the required socket is not in the database, go to the “Adding an Application Socket” procedure on page 3-192 to add the socket.

4. Assign the new socket name to the routing key by entering the `chg-appl-rtkey` command. Go to the Rules for Replacing the IP Connections in an Existing Application Routing Key with a Single Socket section on page 3-269 to determine the required parameter combination.

For this example, enter this command.

```
chg-appl-rtkey:dpca=123-234-123:si=5:opca=122-124-125:cics=1
:cice=1000:nname=socket2
```

NOTE: If the routing key has any sockets assigned to it, the new socket name (defined by the `nname` parameter) replaces all the existing socket names. If you still wish to use some of the old socket names that were assigned to the routing key, perform the “Adding an Application Routing Key Containing a Socket” procedure on page 3-228 to add these socket names to the routing key.

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
CHG-APPL-RTKEY: MASP A - COMPLTD
```

5. Display the changes by entering the **rtrv-appl-rtkey** command with the socket name of the routing key specified in step 4 and the **display=all** parameter. For this example, enter this command.

```
rtrv-appl-rtkey:sname=socket2:display=all
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
KEY:LOC      DPC          SI SSN OPCA      CICS      CICE
      STATIC 123-234-123 5 --- 122-124-125   1         1000
      ATTR:PSTNCAT PSTNID NORM DUP
              0      0 N   -
      SNAMEs:socket2

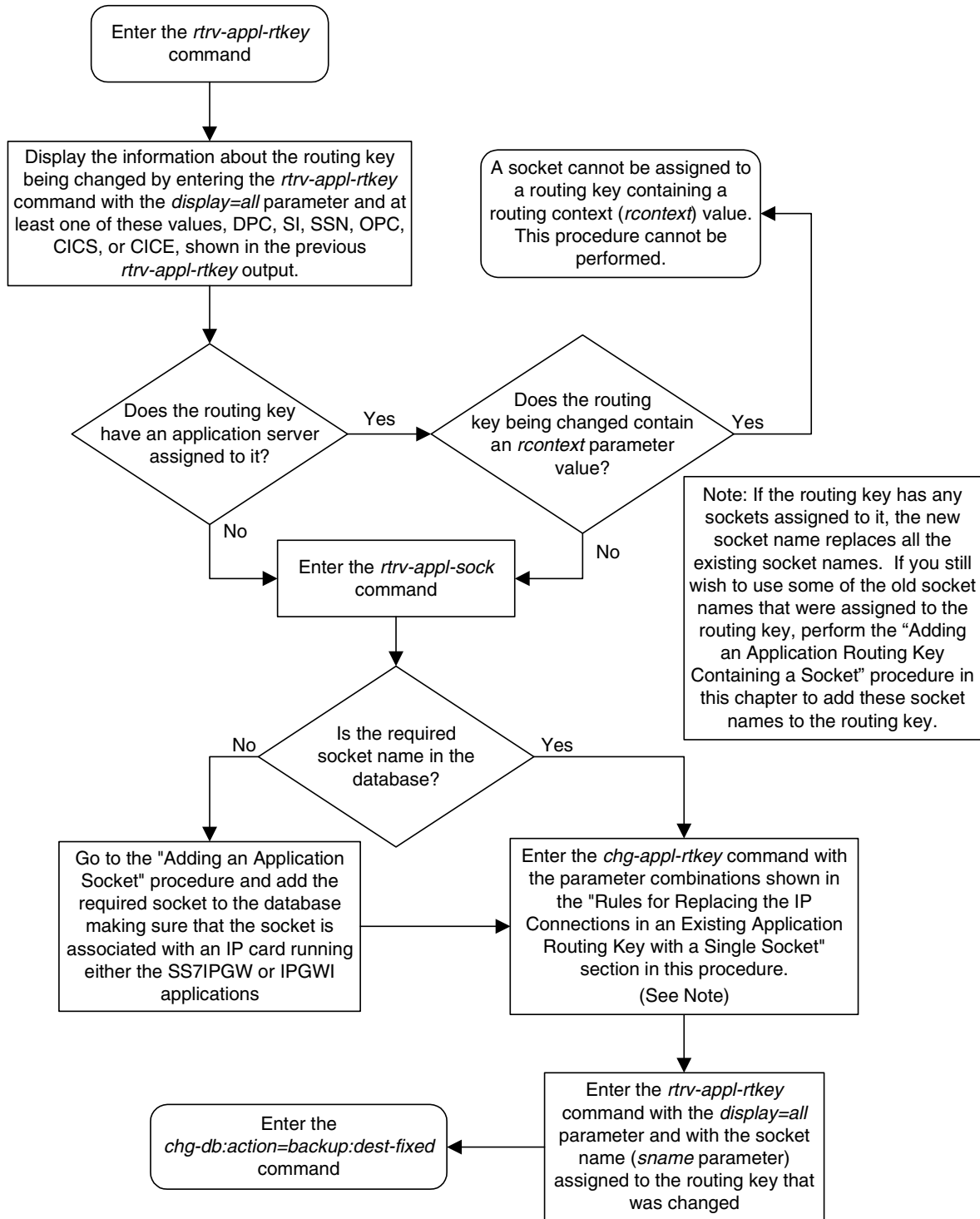
STATIC Route Key table is (2 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (2 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

6. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-25. Replacing the IP Connections in an Existing Application Routing Key with a Single Socket



Changing the CIC values in an Existing Application Routing Key

This procedure is used to change the CIC values in an existing application routing key using the `chg-app1-rtkey` command. These parameters are used in this procedure.

`:dpc/dpca/dpci/dpcn/dpcn24` – Destination point code value that is used to filter incoming MSUs.

`:opc/opca/opci/opcn/opcn24` – The originating point code value that is used to filter incoming MSUs. This value must not specify a cluster route.

NOTE: See the “Point Code Formats” section in the *Database Administration Manual - SS7* for a definition of the point code types that are used on the system and for a definition of the different formats that can be used for ITU national point codes.

`:si` – The service indicator value that is used to filter incoming MSUs. The range of values for the service indicator parameter (`si`) can be a numerical value from 0 to 15, or for selected service indicator values, a text string can be used instead of numbers. Table 3-26 shows the text strings that can be used in place of numbers for the service indicator values.

Table 3-26. Service Indicator Text String Values

Service Indicator Value	Text String
4	tup
5	isup
13	qbicc

`:cics` - Starting circuit identification code that is used to filter incoming MSUs. Specify with `cice` to identify the routing key to be changed.

`:cice` - Ending circuit identification code that is used to filter incoming MSUs. Specify with `cics` to identify the routing key to be changed.

`:ncics` - New starting circuit identification code that is used to filter incoming MSUs. Specify the `ncics` parameter and/or the `ncice` parameter to change the range of circuit identification codes assigned to the routing key.

`:ncice` - New ending circuit identification code that is used to filter incoming MSUs. Specify the `ncice` parameter and/or the `ncics` parameter to change the range of circuit identification codes assigned to the routing key.

`:split` - The circuit identification code value where the specified range of CIC values for the routing key specified by the `cics` and `cice` values is to be split into two routing keys. The CIC values in one routing key range from the `cics` value of the original routing key to a value equal to one less than the `split` value. The CIC values in the other routing key range from the `split`

value to the **cice** value of the original routing key. All other parameters in both routing keys remain the same as in the original routing key. The range of CIC values cannot be split if the routing key contains a routing context parameter value.

:type - Key type. Identifies the type of application routing key that will be changed. One of three values, **type = full/partial/default**. If **type** is not explicitly specified, **type = full** is assumed. Only the **type=full** parameter can be used in this procedure.

The **chg-appl-rtkey** command contains other parameters that are not used in this procedure.

:nsname – The name of the new socket that will receive the incoming MSU. The new socket name replaces all of the existing socket associations for the routing key.

:ssn – The subsystem number value that is used to filter incoming MSUs. See the “Adding an Application Routing Key Containing a Socket” procedure on page 3-228 for more information on using the **ssn** parameter with a routing key.

:pstncat – The PSTN category assigned to the routing key.

:pstnid – The PSTN ID assigned to the routing key.

:norm – Specifies whether the ISUP Normalization process is enabled or disabled for MSUs using the routing key.

:nasname – The name of the new application server that will receive the incoming MSU.

:rcontext – The routing context parameter.

See the “Replacing the IP Connections in an Existing Application Routing Key with a Single Socket” procedure on page 3-267 for details about using the **nsname** parameter.

See the “Changing the Routing Context Value in an Existing Application Routing Key” procedure on page 3-283 for changing the routing context parameter value in an existing routing key.

See the “Replacing the IP Connections in an Existing Application Routing Key with an Application Server” procedure on page 3-293 for details about using the **nasname** parameter.

See the “Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key” procedure on page 3-307 for changing a routing key using the **pstncat**, **pstnid**, and **norm** parameters.

Rules for Changing the Range of CIC Values in an Existing Routing Key

The parameter combinations used by the `chg-app1-rtkey` command to change the range of CIC values in the routing key are shown in Table 3-27.

Table 3-27. Routing Key Parameter Combinations for Changing the Range of CIC Values in an Existing Routing Key

SI=4 (TUP)	SI=5 (ISUP)		SI=13 (QBICC)
dpci/dpcn/dpcn24=<the DPC assigned to the routing key> ¹	dpc/dpca=<the DPC assigned to the routing key> ¹	dpci/dpcn/dpcn24=<the DPC assigned to the routing key> ¹	dpc/dpca/dpci/dpcn/dpcn24=<the DPC assigned to the routing key> ¹
si=4 ¹	si=5 ¹	si=5 ¹	si=13 ¹
opci/opcn/opcn24=<the OPC assigned to the routing key> ¹	opc/opca=<the OPC assigned to the routing key> ¹	opci/opcn/opcn24=<the OPC assigned to the routing key> ¹	opc/opca/opci/opcn/opcn24=<the OPC assigned to the routing key> ¹
cics=<the CICS value assigned to the routing key> ^{1, 3}	cics=<the CICS value assigned to the routing key> ^{1, 3}	cics=<the CICS value assigned to the routing key> ^{1, 3}	cics=<the CICS value assigned to the routing key> ^{1, 3}
cice=<the CICE value assigned to the routing key> ^{1, 3}	cice=<the CICE value assigned to the routing key> ^{1, 3}	cice=<the CICE value assigned to the routing key> ^{1, 3}	cice=<the CICE value assigned to the routing key> ^{1, 3}
type=full	type=full	type=full	type=full
ncics=<0 to 4095> ^{3, 4}	ncics=<0 to 16383> ^{3, 4}	ncics=<0 to 4095> ^{3, 4}	ncics=<0 to 4294967295> ^{3, 4}
ncice=<0 to 4095> ^{3, 4}	ncice=<0 to 16383> ^{3, 4}	ncice=<0 to 4095> ^{3, 4}	ncice=<0 to 4294967295> ^{3, 4}
<p>1. The values for these parameters must be entered exactly as shown in the <code>rtrv-app1-rtkey</code> command output for the routing key being changed. However, text strings can be used in place of some numerical service indicator values. See Table 3-26 on page 3-275 for a list of these text strings. The text string must correspond to the numerical value shown in the routing key being changed.</p> <p>2. The <code>dpc</code> and <code>opc</code> must be the same type of point code. For example, if the <code>dpca</code> parameter is specified, the OPC is specified with the <code>opca</code> parameter.</p> <p>3. The <code>cics</code> and <code>cice</code> parameters must be specified and either the <code>ncics</code> or <code>ncice</code> parameters, or both, must be specified. If both the <code>ncics</code> and <code>ncice</code> parameters are specified, the value of the <code>ncics</code> parameter must be less than the value of the <code>ncice</code> parameter. If the <code>ncics</code> parameter is not specified, the value of the <code>ncice</code> parameter must be greater than or equal to the <code>cics</code> parameter value. If the <code>ncice</code> parameter is not specified, the value of the <code>ncics</code> parameter must be less than or equal to the <code>cice</code> parameter value.</p> <p>4. The new CIC range cannot overlap the CIC range in an existing routing key.</p>			

Rules for Splitting the Range of CIC Values in an Existing Routing Key

The parameter combinations used by the `chg-app1-rtkey` command to split the range of CIC values in the routing key are shown in Table 3-28.

Splitting the range of CIC values creates two routing keys. The CIC values in one routing key ranges from the `cics` value of the original routing key to a value equal to one less than the `split` value. The CIC values in the other routing key ranges from the `split` value to the `cice` value of the original routing key. All other parameters in both routing keys remain the same as in the original routing key. The range of CIC values cannot be split if the routing key contains a routing context parameter value.

Table 3-28. Routing Key Parameter Combinations for Splitting the Range of CIC Values in an Existing Routing Key

SI=4 (TUP)	SI=5 (ISUP)		SI=13 (QBICC)
dpci/dpcn/dpcn24=<the DPC assigned to the routing key> ¹	dpc/dpca=<the DPC assigned to the routing key> ¹	dpci/dpcn/dpcn24=<the DPC assigned to the routing key> ¹	dpc/dpca/dpci/dpcn/dpcn24=<the DPC assigned to the routing key> ¹
si=4 ¹	si=5 ¹	si=5 ¹	si=13 ¹
opci/opcn/opcn24=<the OPC assigned to the routing key> ¹	opc/opca=<the OPC assigned to the routing key> ¹	opci/opcn/opcn24=<the OPC assigned to the routing key> ¹	opc/opca/opci/opcn/opcn24=<the OPC assigned to the routing key> ¹
cics=<the CICS value assigned to the routing key> ¹	cics=<the CICS value assigned to the routing key> ¹	cics=<the CICS value assigned to the routing key> ¹	cics=<the CICS value assigned to the routing key> ¹
cice=<the CICE value assigned to the routing key> ¹	cice=<the CICE value assigned to the routing key> ¹	cice=<the CICE value assigned to the routing key> ¹	cice=<the CICE value assigned to the routing key> ¹
type=full	type=full	type=full	type=full
split=<0 to 4095> ³	split=<0 to 16383> ³	split=<0 to 4095> ³	split=<0 to 4294967295> ³
<p>1. The values for these parameters must be entered exactly as shown in the <code>rtrv-app1-rtkey</code> command output for the routing key being changed. However, text strings can be used in place of some numerical service indicator values. See Table 3-26 on page 3-275 for a list of these text strings. The text string must correspond to the numerical value shown in the routing key being changed.</p> <p>2. The <code>dpc</code> and <code>opc</code> must be the same type of point code. For example, if the <code>dpca</code> parameter is specified, the OPC is specified with the <code>opca</code> parameter.</p> <p>4. The <code>split</code> parameter value must be greater than the <code>cics</code> parameter value and less than the <code>cice</code> parameter value.</p>			

Canceling the RTRV-APPL-SOCK, RTRV-AS, and RTRV-APPL-RTKEY Commands

Because the `rtrv-appl-sock`, `rtrv-as`, and `rtrv-appl-rtkey` commands used in this procedure can output information for a long period of time, the `rtrv-appl-sock`, `rtrv-as`, and `rtrv-appl-rtkey` commands can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-appl-sock`, `rtrv-as`, and `rtrv-appl-rtkey` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-appl-sock`, `rtrv-as`, or `rtrv-appl-rtkey` commands were entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-appl-sock`, `rtrv-as`, or `rtrv-appl-rtkey` commands were entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-appl-sock`, `rtrv-as`, or `rtrv-appl-rtkey` commands were entered, from another terminal other than the terminal where the `rtrv-appl-sock`, `rtrv-as`, or `rtrv-appl-rtkey` commands were entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current application routing key information in the database by entering the `rtrv-appl-rtkey` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC          SI SSN OPC          CICS      CICE
  STATIC 123-234-123 5 --- 122-124-125    1        1000
  STATIC 123-234-123 5 --- 100-100-100    1           50
    1105 005-005-001 5 --- 010-010-001    1           500
    1105 005-005-001 5 --- 010-010-001   501        1000
    1107 006-006-001 5 --- 011-011-001    1           500
    1107 006-006-001 5 --- 011-011-001   501        1000

STATIC Route Key table is (2 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (2 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

2. Display the specific routing key information for the routing key being changed by entering the `rtrv-appl-rtkey` command with the `display=all` parameter and the `DPC`, `SI`, `OPC`, `CICS`, or `CICE` values shown in the `rtrv-appl-rtkey` output in step 1 for the routing key being changed. The service indicator value for the routing key to be used in this procedure is either 4, 5, or 13. For this example, enter this command.

```
rtrv-appl-rtkey:dpc=123-234-123:si=5:opc=122-124-125:cics=1
:cice=1000:display=all
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC          SI SSN OPC          CICS      CICE
      STATIC 123-234-123  5 --- 122-124-125    1         1000

      ATTR:PSTNCAT PSTNID NORM DUP
              0      0 N  -
      SNAMEs:kchlr11201

STATIC Route Key table is (2 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (2 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

3. Change the CIC values of the routing key by entering the `chg-appl-rtkey` command. The parameters required for the `chg-appl-rtkey` command are determined by the type of change being made to the routing key. Go to one of these sections to determine the required parameter combination.

- “Rules for Changing the Range of CIC Values in an Existing Routing Key” on page 3-277
- “Rules for Splitting the Range of CIC Values in an Existing Routing Key” on page 3-278

NOTE: If the routing key contains a routing context value, the range of CIC values cannot be split.

To change the range of CIC values for this example, enter this command.

```
chg-appl-rtkey:dpca=123-234-123:si=5:opca=122-124-125:cics=1
:cice=1000:ncice=2000
```

To split the range of CIC values for this example, enter this command.

```
chg-appl-rtkey:dpca=123-234-123:si=5:opca=122-124-125:cics=1
:cice=1000:split=500
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
CHG-APPL-RTKEY: MASP A - COMPLTD
```

4. Display the new application routing key information in the database by entering the **rtrv-appl-rtkey** command with the socket name or application server name of the routing key specified in step 6 and the **display=all** parameter. For this example, enter this command.

```
rtrv-appl-rtkey:sname=socket2:display=all
```

If the range of CIC values was changed, this is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
KEY:LOC      DPC          SI SSN OPCA          CICS          CICE
  STATIC 123-234-123 5 --- 122-124-125 1          2000

  ATTR:PSTNCAT PSTNID NORM DUP
                0      0 N   -
  SNAMEs:socket2

STATIC Route Key table is (2 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (2 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

If the range of CIC values was split, this is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
KEY:LOC      DPC          SI SSN OPCA          CICS          CICE
  STATIC 123-234-123 5 --- 122-124-125 1          499

  ATTR:PSTNCAT PSTNID NORM DUP
                0      0 N   -
  SNAMEs:socket2

KEY:LOC      DPC          SI SSN OPCA          CICS          CICE
  STATIC 123-234-123 5 --- 122-124-125 500        1000

  ATTR:PSTNCAT PSTNID NORM DUP
                0      0 N   -
  SNAMEs:socket2

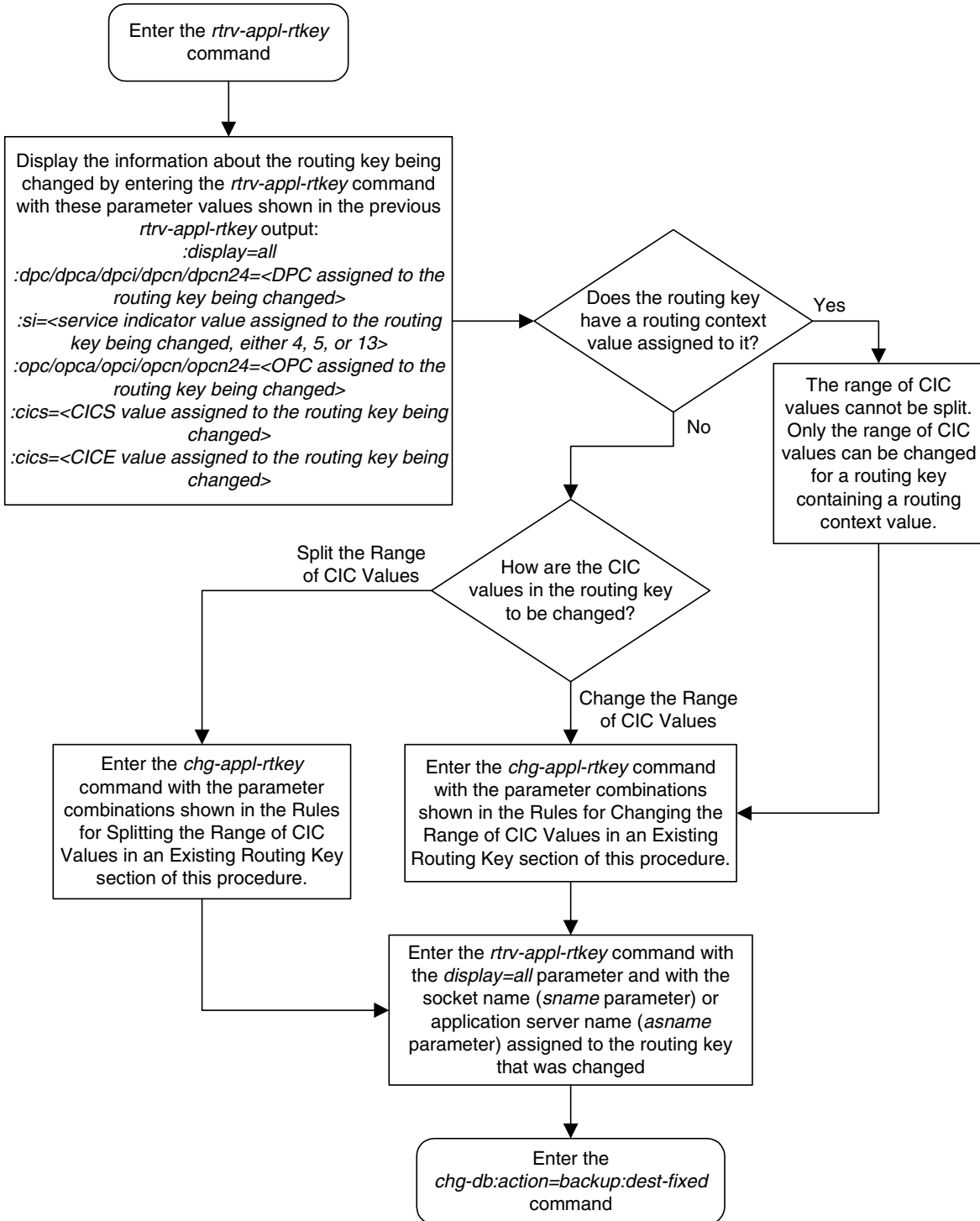
STATIC Route Key table is (3 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (2 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

5. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-26. Changing the CIC values in an Existing Application Routing Key



Changing the Routing Context Value in an Existing Application Routing Key

This procedure is used to change the routing context value in an existing application routing key using the `chg-app1-rtkey` command. These parameters are used in this procedure.

:dpc/dpca/dpci/dpcn/dpcn24 – Destination point code value that is used to filter incoming MSUs.

:opc/opca/opci/opcn/opcn24 - The originating point code value that is used to filter incoming MSUs. This value must not specify a cluster route.

NOTE: See the “Point Code Formats” section in the *Database Administration Manual - SS7* for a definition of the point code types that are used on the system and for a definition of the different formats that can be used for ITU national point codes.

:si – The service indicator value that is used to filter incoming MSUs. The range of values for the service indicator parameter (**si**) can be a numerical value from 0 to 15, or for selected service indicator values, a text string can be used instead of numbers. Table 3-29 shows the text strings that can be used in place of numbers for the service indicator values.

Table 3-29. Service Indicator Text String Values

Service Indicator Value	Text String	Service Indicator Value	Text String
0	snm	3	sccp
1	regtest	4	tup
2	spltst	5	isup
		13	qbicc

:ssn – The subsystem number value that is used to filter incoming MSUs.

:cics - Starting circuit identification code that is used to filter incoming MSUs.

:cice - Ending circuit identification code that is used to filter incoming MSUs.

:type - Key type. Identifies the type of application routing key that will be changed. One of three values, **type = full/partial/default**. If **type** is not explicitly specified, **type = full** is assumed.

:rcontext – The routing context parameter, which has two functions:

- Provides an index of the application server traffic that the sending ASP is configured or registered to receive.
- Identifies the SS7 network context for the message. The routing context parameter implicitly defines the SS7 point code format used, the SS7 network indicator value, and the SCCP protocol type/variant/version used.

The **chg-appl-rtkey** command contains other parameters that are not used in this procedure.

:nsname – The new name of the new socket that will receive the incoming MSU.

:ncics - New starting circuit identification code that is used to filter incoming MSUs.

:ncice - New ending circuit identification code that is used to filter incoming MSUs.

:split - The circuit identification code value where the specified range of the routing key specified by the **cics** and **cice** values is to be split into two entries.

:pstncat – The PSTN category assigned to the routing key.

:pstnid – The PSTN ID assigned to the routing key.

:norm – Specifies whether the ISUP Normalization process is enabled or disabled for MSUs using the routing key.

:nasname – The new name of the new application server that will receive the incoming MSU.

See the “Replacing the IP Connections in an Existing Application Routing Key with a Single Socket” procedure on page 3-267 for details about using the **nsname** parameter.

See the “Changing the CIC values in an Existing Application Routing Key” procedure on page 3-275 for changing a routing key using the **ncics**, **ncice**, and **split** parameters.

See the “Replacing the IP Connections in an Existing Application Routing Key with an Application Server” procedure on page 3-293 for details about using the **nasname** parameter.

See the “Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key” procedure on page 3-307 for changing a routing key using the **pstncat**, **pstnid**, and **norm** parameters.

Rules for Changing the Routing Context Value in an Existing Application Routing Key

The parameter combinations used by the `chg-appl-rtkey` command to change the routing context value in an existing application routing key are shown in Table 3-30.

Table 3-30. Routing Key Parameter Combinations for Changing the Routing Context Value in an Existing Application Routing Key

SI=3 (SCCP)		SI=4 (TUP), 5 (ISUP), 13 (QBICC)		Other SI Values		Default Routing Key
Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	
dpc ¹	type=partial	dpc ¹	type=partial	dpc ¹	type=partial	type=default
si=3 ¹	dpc ^{1, 2}	si=4, 5, 13	dpc ^{1, 2}	si=value other than 3, 4, 5, 13 ¹	dpc ^{1, 2}	rcontext ⁴
ssn ¹	si=3 ^{1, 2}	opc ¹	si=4, 5, 13 ^{1, 2}	type=full	si=value other than 3, 4, 5, 13 ^{1, 2}	
type=full	rcontext ³	cics	opc ²	rcontext ³	rcontext ³	
rcontext ³		cice	rcontext ³			
		type=full				
		rcontext ⁴				

Notes:

- The values for these parameters must be entered exactly as shown in the `rtrv-appl-rtkey` command output for the routing key being changed. However, text strings can be used in place of some numerical service indicator values. See Table 3-29 on page 3-283 for a list of these text strings. The text string must correspond to the numerical value shown in the routing key being changed.
- These parameters are optional for partial routing keys, but at least one these parameters must be specified with the `chg-appl-rtkey` command.
- The following rules apply to using the `rcontext` parameter.
 - The value of the `rcontext` parameter is from 0 to 4294967295.
 - The `rcontext` parameter is required for a routing key containing an SUA application server.
 - The `rcontext` parameter is optional for a routing key containing an M3UA application server.
 - The `rcontext` parameter value must be unique in the database. Multiple routing keys cannot have the same `rcontext` value assigned.
 - An application server can be assigned to a maximum of four routing keys containing `rcontext` parameter values.
 - If the application server being assigned to the new routing key is assigned to other routing keys that do not contain `rcontext` parameter values, the `rcontext` parameter cannot be assigned to the new routing key.
 - If the application server being assigned to the new routing key is assigned to other routing keys that contain `rcontext` parameter values, the `rcontext` parameter must be assigned to the new routing key.

Canceling the RTRV-APPL-SOCK, RTRV-AS, and RTRV-APPL-RTKEY Commands

Because the `rtrv-appl-sock`, `rtrv-as`, and `rtrv-appl-rtkey` commands used in this procedure can output information for a long period of time, the `rtrv-appl-sock`, `rtrv-as`, and `rtrv-appl-rtkey` commands can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-appl-sock`, `rtrv-as`, and `rtrv-appl-rtkey` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-appl-sock`, `rtrv-as`, or `rtrv-appl-rtkey` commands were entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-appl-sock`, `rtrv-as`, or `rtrv-appl-rtkey` commands were entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-appl-sock`, `rtrv-as`, or `rtrv-appl-rtkey` commands were entered, from another terminal other than the terminal where the `rtrv-appl-sock`, `rtrv-as`, or `rtrv-appl-rtkey` commands were entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current application routing key information in the database by entering the `rtrv-appl-rtkey` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC          SI SSN OPC          CICS          CICE
  STATIC 123-234-123 5 --- 122-124-125 1          1000
  STATIC 123-234-123 5 --- 100-100-100 1           50
    1105 005-005-001 5 --- 010-010-001 1           500
    1105 005-005-001 5 --- 010-010-001 501        1000
    1107 006-006-001 5 --- 011-011-001 1           500
    1107 006-006-001 5 --- 011-011-001 501        1000

KEY:LOC      DPCI          SI SSN OPC          CICS          CICE
  STATIC 6-006-6    3 170 -----
  STATIC 6-006-7    6 --- -----
  STATIC 6-006-6    5 --- 1-002-3    150          175
  STATIC 6-006-6    5 --- 1-002-3    75           100

KEY:LOC      DPC          SI SSN OPC          CICS          CICE
  STATIC DEFAULT KEY ** *** ***** ***** *****

STATIC Route Key table is (7 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full
```

```
STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

2. Display the specific routing key information for the routing key being changed by entering the **rtrv-appl-rtkey** command with the **display=all** parameter and the **DPC**, **SI**, **SSN**, **OPC**, **CICS**, or **CICE** values shown in the **rtrv-appl-rtkey** output in step 1 for the routing key being changed. For this example, enter this command.

```
rtrv-appl-rtkey:dpci=6-006-6:si=5:opci=1-002-3:cics=75
:cice=100:display=all
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

```
KEY:LOC      DPC          SI SSN OPC          CICS      CICE
  STATIC 6-006-6      5 --- 1-002-3      75        100
```

```
RCONTEXT:310
ASNAME:as2
ANAMES:assoc1
```

```
STATIC Route Key table is (7 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full
```

```
STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

If the routing key displayed in this step contains socket names, a routing context value cannot be assigned to the routing key. This procedure cannot be performed.

If the routing key contains an application server and a routing context value, skip step 3 and go to step 4.

If the routing key contains an application server and does not contain a routing context value, go to step 3.

3. Display these routing keys by entering the `rtrv-appl-rtkey` command with the application server name and the `display=all` parameter. For this example, enter this command.

```
rtrv-appl-rtkey:asname=as2:display=all
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
```

```
KEY:LOC      DPCI      SI SSN    OPCI      CICS      CICE
  STATIC    6-006-6   3 170  -----
           RCONTEXT:89
           ASNAME:as2
           ANAMES:assoc1

KEY:LOC      DPCI      SI SSN    OPCI      CICS      CICE
  STATIC    6-006-7   6 ---  -----
           RCONTEXT:55
           ASNAME:as2
           ANAMES:assoc1

KEY:LOC      DPCI      SI SSN    OPCI      CICS      CICE
  STATIC    6-006-6   5 ---  1-002-3  150      175
           RCONTEXT:7
           ASNAME:as2
           ANAMES:assoc1

KEY:LOC      DPCI      SI SSN    OPCI      CICS      CICE
  STATIC    6-006-6   5 ---  1-002-3  75       100
           RCONTEXT:310
           ASNAME:as2
           ANAMES:assoc1
```

```
STATIC Route Key table is (7 of 2000) 1% full
1105 Route Key table is (2 of 500) 1% full
1107 Route Key table is (2 of 500) 1% full
```

```
STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105 Route Key Socket Association table is (2 of 8000) 1% full
1107 Route Key Socket Association table is (2 of 8000) 1% full
```

If the routing keys displayed in this step do not contain `rcontext` parameter values, the `rcontext` parameter cannot be specified for the routing key being changed in this procedure.

If you wish to change the routing context value of another routing key, go back to step 2 and select another routing key.

If you do not wish to change the routing context value of another routing key, this procedure cannot be performed.

4. Display the association displayed in the `rtrv-appl-rtkey` output in step 2, using the `rtrv-assoc` command with the association name shown in step 2.

```
rtrv-assoc:aname=assoc1
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc1
PORT      A
ADAPTER   M3UA          VER      M3UA RFC
LHOST     gw105.nc.tekelec.com
ALHOST    ---
RHOST     gw100.nc.tekelec.com
LPORT     1030             RPORT    1030
ISTRMS    2                OSTRMS   2
RMODE     LIN          RMIN     120          RMAX     800
RTIMES    10             CWMIN    3000
OPEN      YES         ALW      YES
IP Appl Sock table is (4 of 4000) 1% full
```

Repeat this step for each association name displayed in step 2.

NOTE: If the `open` parameter value for all the associations assigned to the application server is `no` (shown in step 4), skip step 5 and go to step 6.

5. Change the value of the `open` parameter to `no` by specifying the `chg-assoc` command with the `open=no` parameter. For this example, enter this command.

```
chg-assoc:aname=assoc1:open=no
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```



CAUTION: The IP connections using the associations specified in this step will not be able to carry any traffic when the `open` parameter is changed to `no`.

Repeat this step for all the associations assigned to the application server that have the `open=yes` parameter value.

6. Change application routing key information to the database by entering the `chg-appl-rtkey` command. Go to the Rules for Changing the Routing Context Value in an Existing Application Routing Key section on page 3-285 to determine the required parameter combination.

For this example, enter this command.

```
chg-appl-rtkey:dpci=6-006-6:si=5:opci=1-002-3:cics=75
:cice=100:rcontext=5280
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
CHG-APPL-RTKEY: MASP A - COMPLTD
```

7. Display the new application routing key information in the database by entering the **rtrv-appl-rtkey** command with the application server name of the routing key and the routing context value specified in step 6 and the **display=all** parameter. For this example, enter this command.

```
rtrv-appl-rtkey:asname=asname=as2:rcontext=5280:display=all
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC          SI SSN OPC          CICS          CICE
      STATIC 6-006-6      5 --- 1-002-3      75            100

      RCONTEXT:5280
      ASNAME:as2
      ANAMES:assoc1

STATIC Route Key table is (7 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

NOTE: If step 5 was not performed in this procedure, skip this step and go to step 9.

8. Change the value of the **open** parameter of the associations that were changed in step 5 to **yes** by specifying the **chg-assoc** command with the **open=yes** parameter. For this example, enter this command.

```
chg-assoc:aname=assoc1:open=yes
```

When this command has successfully completed, this message should appear.

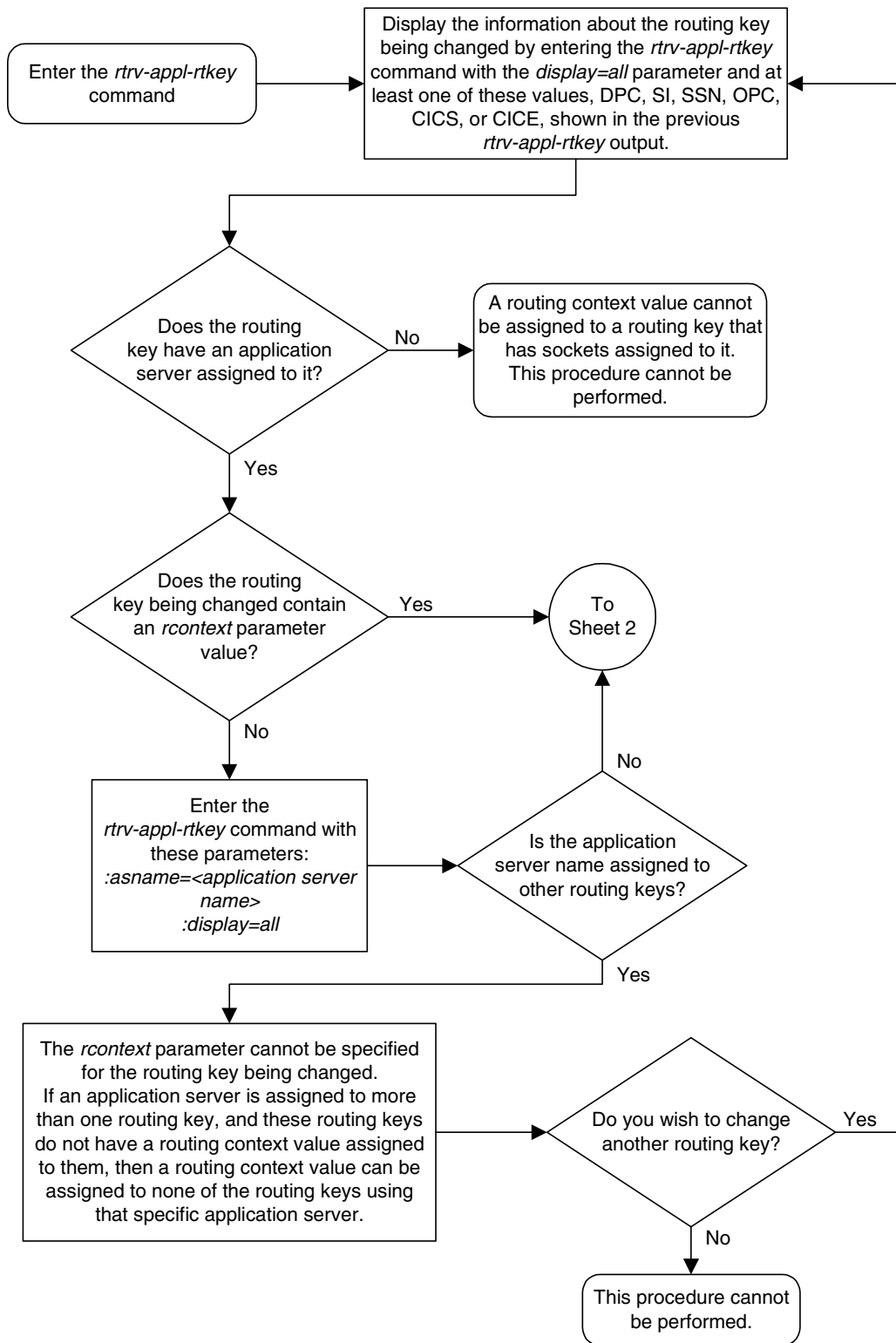
```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

Repeat this step for all the associations that were changed in step 5.

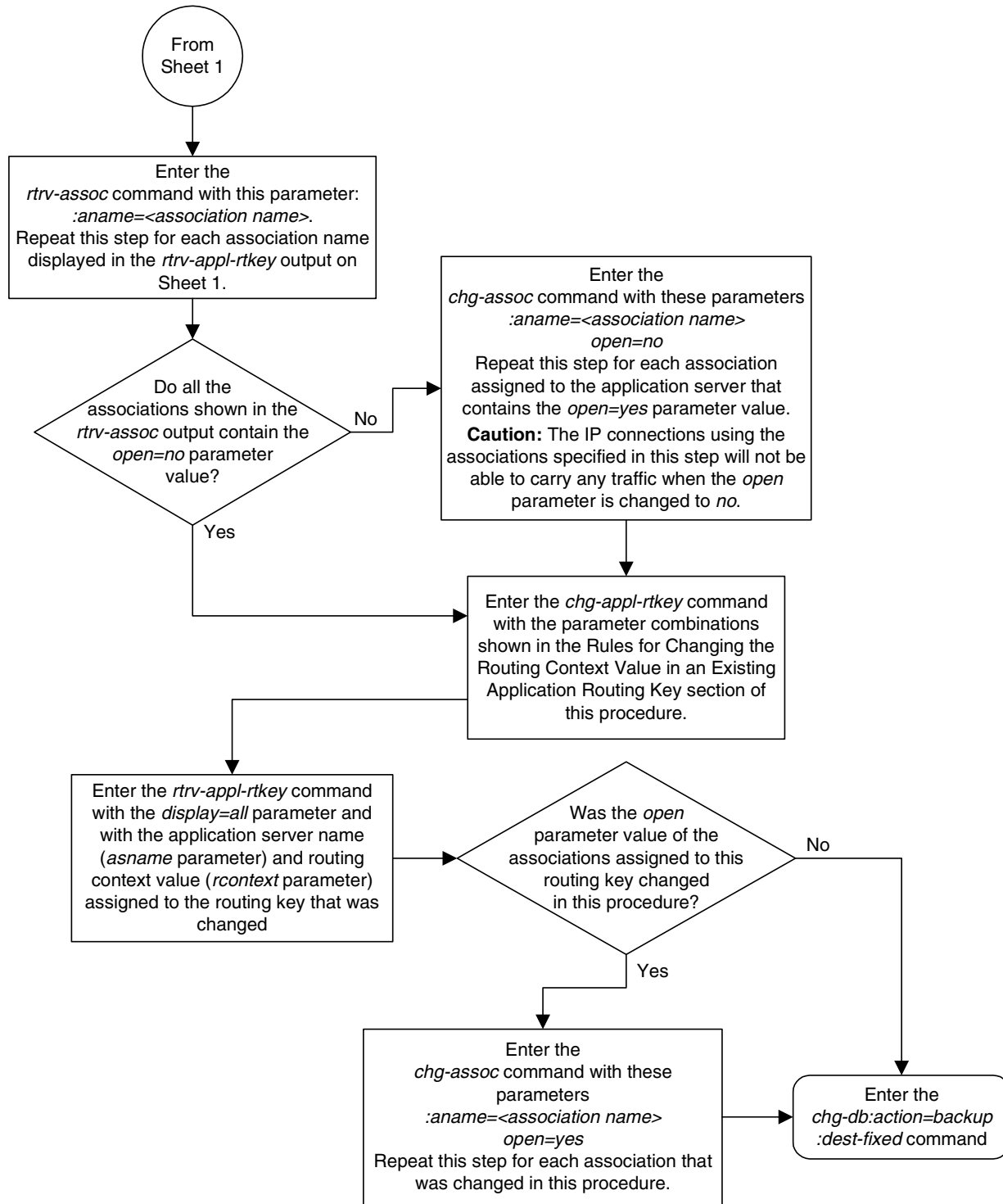
-
9. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-27. Changing the Routing Context Value in an Existing Application Routing Key (Sheet 1 of 2)



Flowchart 3-27. Changing the Routing Context Value in an Existing Application Routing Key (Sheet 2 of 2)



Replacing the IP Connections in an Existing Application Routing Key with an Application Server

Performing this procedure replaces all the IP connections assigned to an existing application routing key with an application server. The IP connections can be sockets (defined by the **sname** parameter in the **rtrv-appl-rtkey** output), or an application server (defined by the **asname** parameter in the **rtrv-appl-rtkey** output). The **chg-appl-rtkey** and these parameters are used in this procedure.

This procedure is used assign a new application server name to an existing application routing key using the **chg-appl-rtkey** command. These parameters are used in this procedure.

The **chg-appl-rtkey** command uses these parameters.

:dpc/dpca/dpci/dpcn/dpcn24 – Destination point code value that is used to filter incoming MSUs.

:opc/opca/opci/opcn/opcn24 - The originating point code value that is used to filter incoming MSUs. This value must not specify a cluster route.

NOTE: See the “Point Code Formats” section in the *Database Administration Manual - SS7* for a definition of the point code types that are used on the system and for a definition of the different formats that can be used for ITU national point codes.

:si – The service indicator value that is used to filter incoming MSUs. The range of values for the service indicator parameter (**si**) can be a numerical value from 0 to 15, or for selected service indicator values, a text string can be used instead of numbers. Table 3-24 shows the text strings that can be used in place of numbers for the service indicator values.

Table 3-31. Service Indicator Text String Values

Service Indicator Value	Text String
0	snm
1	regtest
2	spltst
3	sccp
4	tup
5	isup
13	qbicc

:ssn – The subsystem number value that is used to filter incoming MSUs.

:nasname – The name of the new application server that will receive the incoming MSU. The new application server name replaces all of the existing application server associations for the routing key.

:cics - Starting circuit identification code that is used to filter incoming MSUs. Specify with **cice** to identify the routing key to be changed.

:cice - Ending circuit identification code that is used to filter incoming MSUs. Specify with **cics** to identify the routing key to be changed.

The **chg-appl-rtkey** command contains other parameters that are not used in this procedure.

:nsname – The name of the new socket that will receive the incoming MSU. The new socket name replaces all of the existing socket associations for the routing key.

:ncics - New starting circuit identification code that is used to filter incoming MSUs.

:ncice - New ending circuit identification code that is used to filter incoming MSUs.

:split - The circuit identification code value where the specified range of the routing key specified by the **cics** and **cice** values is to be split into two entries.

:pstncat – The PSTN category assigned to the routing key.

:pstnid – The PSTN ID assigned to the routing key.

:norm – Specifies whether the ISUP Normalization process is enabled or disabled for MSUs using the routing key.

:rcontext – The routing context parameter.

See the “Replacing the IP Connections in an Existing Application Routing Key with a Single Socket” procedure on page 3-267 for details about using the **nsname** parameter.

See the “Changing the CIC values in an Existing Application Routing Key” procedure on page 3-275 for changing a routing key using the **ncics**, **ncice**, and **split** parameters.

See the “Changing the Routing Context Value in an Existing Application Routing Key” procedure on page 3-283 for changing the routing context parameter value in an existing routing key.

See the “Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key” procedure on page 3-307 for changing a routing key using the **pstncat**, **pstnid**, and **norm** parameters.

Rules for Replacing the IP Connections in an Existing Application Routing Key with an Application Server

The parameter combinations used by the **chg-app1-rtkey** command to assign a new application server name to a routing key are shown in Table 3-32.

Table 3-32. Routing Key Parameter Combinations for Replacing the IP Connections in an Existing Application Routing Key with an Application Server

SI=3 (SCCP)		SI=4 (TUP), 5 (ISUP), 13 (QBICC)		Other SI Values		Default Routing Key
Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	Full Routing Key	Partial Routing Key	
nasname ^{3, 4, 5}	nasname ^{3, 4, 5}	nasname ^{3, 4, 5}	nasname ^{3, 4, 5}	nasname ^{3, 4, 5}	nasname ^{3, 4, 5}	nasname ^{3, 4, 5}
dpc ¹	type=partial	dpc ¹	type=partial	dpc ¹	type=partial	type=default
si=3 ¹	dpc ^{1, 2}	si=4, 5, 13 ¹	dpc ^{1, 2}	si=value other than 3, 4, 5, 13 ¹	dpc ^{1, 2}	
ssn ¹	si=3 ^{1, 2}	opc ¹	si=4, 5, 13 ^{1, 2}	type=full	si=value other than 3, 4, 5, 13 ^{1, 2}	
type=full		cics ¹	opc ^{1, 2}			
		cice ¹				
		type=full				

Notes:

1. The values for these parameters must be entered exactly as shown in the **rttrv-app1-rtkey** command output for the routing key being changed. However, text strings can be used in place of some numerical service indicator values. See Table 3-31 on page 3-293 for a list of these text strings. The text string must correspond to the numerical value shown in the routing key being changed.
2. These parameters are optional for partial routing keys, but at least one these parameters must be specified with the **chg-app1-rtkey** command.
3. An application server cannot be assigned to a routing key if that application server is assigned to four routing keys containing routing context values.
4. If the routing key being changed does not contain a routing context value, the **adapter** parameter value for the associations assigned to the new application server must be M3UA. If the routing key being changed does contain a routing context value, the **adapter** parameter value of these associations can be either SUA or M3UA.
5. SUA associations, and their corresponding ASPs and application server, can be assigned to only these types of routing keys, with these values:
 - Full routing key - DPC/SI=3/SSN
 - Partial Routing Key - DPC/SI=3
 - Partial routing key - DPC only
 - Partial routing key - SI=3 only
 - Default routing key

Canceling the RTRV-AS and RTRV-APPL-RTKEY Commands

Because the `rtrv-as` and `rtrv-appl-rtkey` commands used in this procedure can output information for a long period of time, the `rtrv-as` and `rtrv-appl-rtkey` commands can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-as` and `rtrv-appl-rtkey` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-as` or `rtrv-appl-rtkey` commands were entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-as` or `rtrv-appl-rtkey` commands were entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-as` or `rtrv-appl-rtkey` commands were entered, from another terminal other than the terminal where the `rtrv-as` or `rtrv-appl-rtkey` commands were entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current application routing key information in the database by entering the `rtrv-appl-rtkey` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC          SI SSN OPC          CICS      CICE
  STATIC 123-234-123 5 --- 122-124-125 1          1000
  STATIC 123-234-123 5 --- 100-100-100 1           50
    1105 005-005-001 5 --- 010-010-001 1           500
    1105 005-005-001 5 --- 010-010-001 501        1000
    1107 006-006-001 5 --- 011-011-001 1           500
    1107 006-006-001 5 --- 011-011-001 501        1000

KEY:LOC      DPCI          SI SSN OPC          CICS      CICE
  STATIC 6-006-6    3 170 -----
  STATIC 6-006-7    6 --- -----
  STATIC 6-006-6    5 --- 1-002-3    150        175
  STATIC 6-006-6    5 --- 1-002-3    75         100

KEY:LOC      DPC          SI SSN OPC          CICS      CICE
  STATIC DEFAULT KEY ** *** ***** ***** *****

STATIC Route Key table is (7 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full
```

```

STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
    
```

2. Display the specific routing key information for the routing key being changed by entering the `rtrv-appl-rtkey` command with the `display=all` parameter and the `DPC`, `SI`, `SSN`, `OPC`, `CICS`, or `CICE` values shown in the `rtrv-appl-rtkey` output in step 1 for the routing key being changed. For this example, enter this command.

```

rtrv-appl-rtkey:dpci=6-006-6:si=5:opci=1-002-3:cics=75
:cice=100:display=all
    
```

This is an example of the possible output.

```

rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
    
```

KEY:LOC	DPC	SI	SSN	OPC	CICS	CICE
STATIC	6-006-6	5	---	1-002-3	75	100

```

RCONTEXT:310
ASNAME:as2
ANAMES:assoc1
    
```

```

STATIC Route Key table is (7 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full
    
```

```

STATIC Route Key Socket Association table is (8 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
    
```

3. Display the current application server information in the database by entering the `rtrv-as` command. The following is an example of the possible output.

```

rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
    
```

AS Name	Mode	ASP Names
as1	LOADSHARE	asp1 asp2 asp3 asp5 asp6
as2	OVERRIDE	asp7
as3	OVERRIDE	asp8

```

AS table is (3 of 250) 1% full.
    
```

If the required application server is not in the database, go to the “Adding an Application Server” procedure on page 3-397 to add the application server.

If the routing key being changed does not contain a routing context value, make sure that the `adapter` parameter value for the associations assigned to the new application server is `M3UA`.

If the routing key being changed contains a routing context value, make sure that the `adapter` parameter value for the associations assigned to the new application server can be either `SUA` or `M3UA`.

SUA associations, and their corresponding ASPs and application server, can be assigned to only these types of routing keys:

- Full routing key – DPC/SI=3/SSN
- Partial routing key – DPC/SI=3
- Partial routing key – DPC only
- Partial routing key – SI=3 only
- Default routing key.

If the application server will not be assigned to one of these types of routing keys, the **adapter** parameter value of the associations assigned to the application server must be **M3UA**.

After the new application server is added to the database, go to step 10.

-
4. Display these routing keys by entering the **rtrv-appl-rtkey** command with the application server name and the **display=all** parameter. For this example, enter this command.

```
rtrv-appl-rtkey:asname=as2:display=all
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
```

```
KEY:LOC      DPCI      SI SSN    OPCI      CICS      CICE
  STATIC    6-006-6   3 170 -----
             RCONTEXT:89
             ASNAME:as2
             ANAMES:assoc1
```

```
KEY:LOC      DPCI      SI SSN    OPCI      CICS      CICE
  STATIC    6-006-7   6 --- -----
             RCONTEXT:55
             ASNAME:as2
             ANAMES:assoc1
```

```
KEY:LOC      DPCI      SI SSN    OPCI      CICS      CICE
  STATIC    6-006-6   5 --- 1-002-3 150      175
             RCONTEXT:7
             ASNAME:as2
             ANAMES:assoc1
```

```
KEY:LOC      DPCI      SI SSN    OPCI      CICS      CICE
  STATIC    6-006-6   5 --- 1-002-3 75       100
             RCONTEXT:310
             ASNAME:as2
             ANAMES:assoc1
```

```
STATIC Route Key table is (7 of 2000) 1% full
1105 Route Key table is (2 of 500) 1% full
1107 Route Key table is (2 of 500) 1% full
```

```
STATIC Route Key Socket Association table is (7 of 32000) 1% full
```



```
1105 Route Key Socket Association table is (2 of 8000) 1% full
1107 Route Key Socket Association table is (2 of 8000) 1% full
```

If the application server is not assigned to any routing keys, go to step 10.

If the application server is assigned to four routing keys containing routing context values, the application server cannot be assigned to the routing key being changed in this procedure. Go to step 3 and choose another application server to assign to the routing key.

If the application server is assigned to less than four routing keys containing routing context values, the application server can be assigned to the routing key being changed in this procedure. Go to step 5.

5. Display the association displayed in the `rtrv-appl-rtkey` output in step 2, using the `rtrv-assoc` command with the association name shown in either step 2.

```
rtrv-assoc:aname=assoc1
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc1
  PORT      A
  ADAPTER   M3UA          VER      M3UA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030          RPORT    1030
  ISTRMS    2             OSTRMS   2
  RMODE     LIN          RMIN     120          RMAX     800
  RTIMES    10          CWMIN    3000
  OPEN      YES        ALW      YES
IP Appl Sock table is (8 of 4000) 1% full
```

Repeat this step for each association name displayed in step 2.

NOTE: If the `open` parameter value for all the associations assigned to the application server is `no` (shown in step 5), skip step 6 and go to step 7.

6. Change the value of the `open` parameter to `no` by specifying the `chg-assoc` command with the `open=no` parameter. For this example, enter this command.

```
chg-assoc:aname=assoc1:open=no
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```



CAUTION: The IP connections using the associations specified in this step will not be able to carry any traffic when the `open` parameter is changed to `no`.

Repeat this step for all the associations assigned to the application server that have the `open=yes` parameter value.

7. Display the application server processes (ASPs) assigned to the new application server being assigned to the routing key (shown in step 3) using the `rtrv-asp` command and specifying the ASP name shown in step 3. For this example, enter this command.

```
rtrv-asp:aspname=asp8
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP          ASSOCIATION          UAPS
asp8         assoc8                          10
```

ASP Table is (3 of 4000) 1% full

Repeat this step for each ASP assigned to the desired application server name shown in step 3.

8. Display the association assigned to the ASP displayed in step 7, using the `rtrv-assoc` command with the association name shown in either step 7.

```
rtrv-assoc:aname=assoc8
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc8
PORT      A
ADAPTER   M3UA          VER          M3UA RFC
LHOST     gw801.nc.tekelec.com
ALHOST    ---
RHOST     gw100.nc.tekelec.com
LPORT     2000             RPORT        1030
ISTRMS    2                OSTRMS        2
RMODE     LIN              RMIN          120           RMAX          800
RTIMES    10               CWMIN         3000
OPEN      YES            ALW           YES
```

IP Appl Sock table is (4 of 4000) 1% full

Repeat this step for each association name displayed in step 7.

NOTE: If the `open` parameter value for all the associations assigned to the application server is `no` (shown in step 8), skip step 9 and go to step 10.

9. Change the value of the `open` parameter to `no` by specifying the `chg-assoc` command with the `open=no` parameter. For this example, enter this command.

```
chg-assoc:aname=assoc8:open=no
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

CAUTION: The IP connections using the associations specified in this step will not be able to carry any traffic when the `open` parameter is changed to `no`.

Repeat this step for all the associations assigned to the application server that have the `open=yes` parameter value.



10. Assign the new application server name to the routing key by entering the **chg-app1-rtkey** command. Go to the Rules for Replacing the IP Connections in an Existing Application Routing Key with an Application Server section on page 3-295 to determine the required parameter combination.

For this example, enter this command.

```
chg-app1-rtkey:dpci=6-006-6:si=5:opci=1-002-3:cics=75
:cice=100:nasname=as3
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
CHG-APPL-RTKEY: MASP A - COMPLTD
```

11. Display the new application routing key information in the database by entering the **rtrv-app1-rtkey** command with the socket name or application server name of the routing key specified in step 10 and the **display=all** parameter. For this example, enter this command.

```
rtrv-app1-rtkey:aname=as3:display=all
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
KEY:LOC      DPC          SI  SSN  OPCA      CICS      CICE
      STATIC 6-006-6      5  ---  1-002-3   75        100

      RCONTEXT:310
      ASNAME:as3
      ANAMES:assoc8

STATIC Route Key table is (7 of 2000) 1% full
1105 Route Key table is (2 of 500) 1% full
1107 Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (7 of 32000) 1% full
1105 Route Key Socket Association table is (2 of 8000) 1% full
1107 Route Key Socket Association table is (2 of 8000) 1% full
```

NOTE: If the **open** parameter value of the associations assigned to the routing key changed in this procedure was not changed (step 9 was not performed), skip this step and go to step 13.

12. Change the value of the **open** parameter of the associations that were changed in steps 6 and 9 to **yes** by specifying the **chg-assoc** command with the **open=yes** parameter. For this example, enter these commands.

```
chg-assoc:aname=assoc1:open=yes
```

```
chg-assoc:aname=assoc8:open=yes
```

When each of these commands have successfully completed, this message should appear.

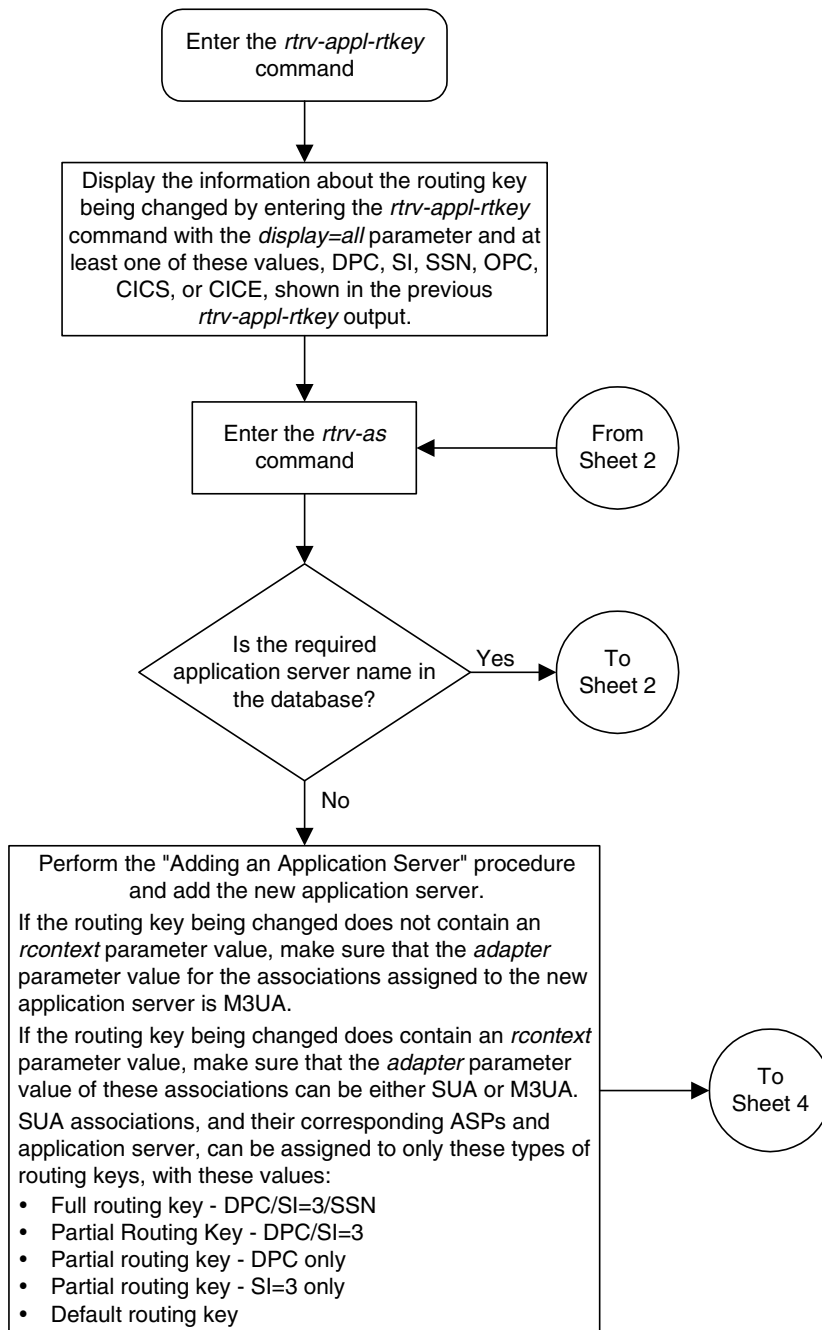
```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

Repeat this step for all the associations that were changed in steps 6 and 9.

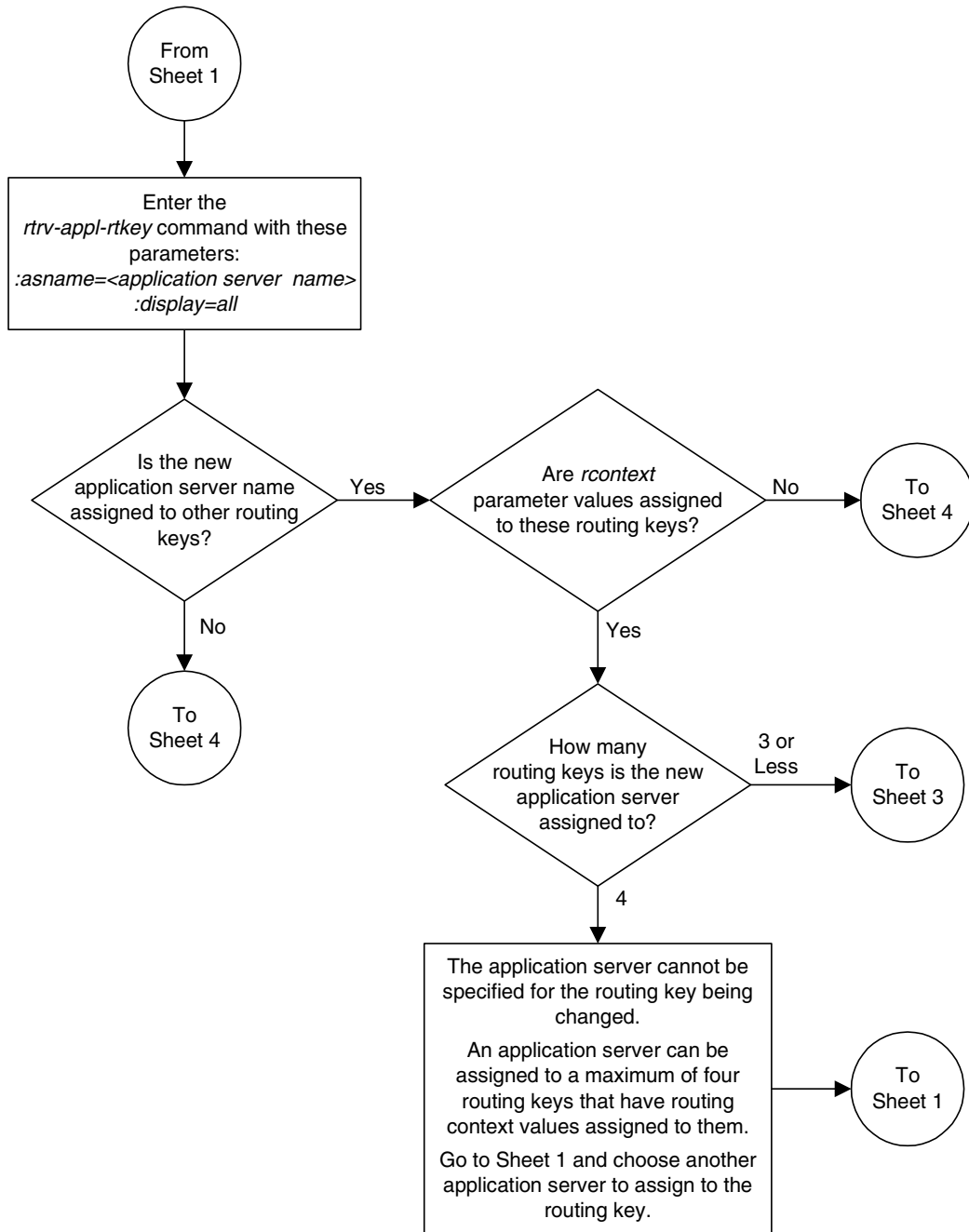
13. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

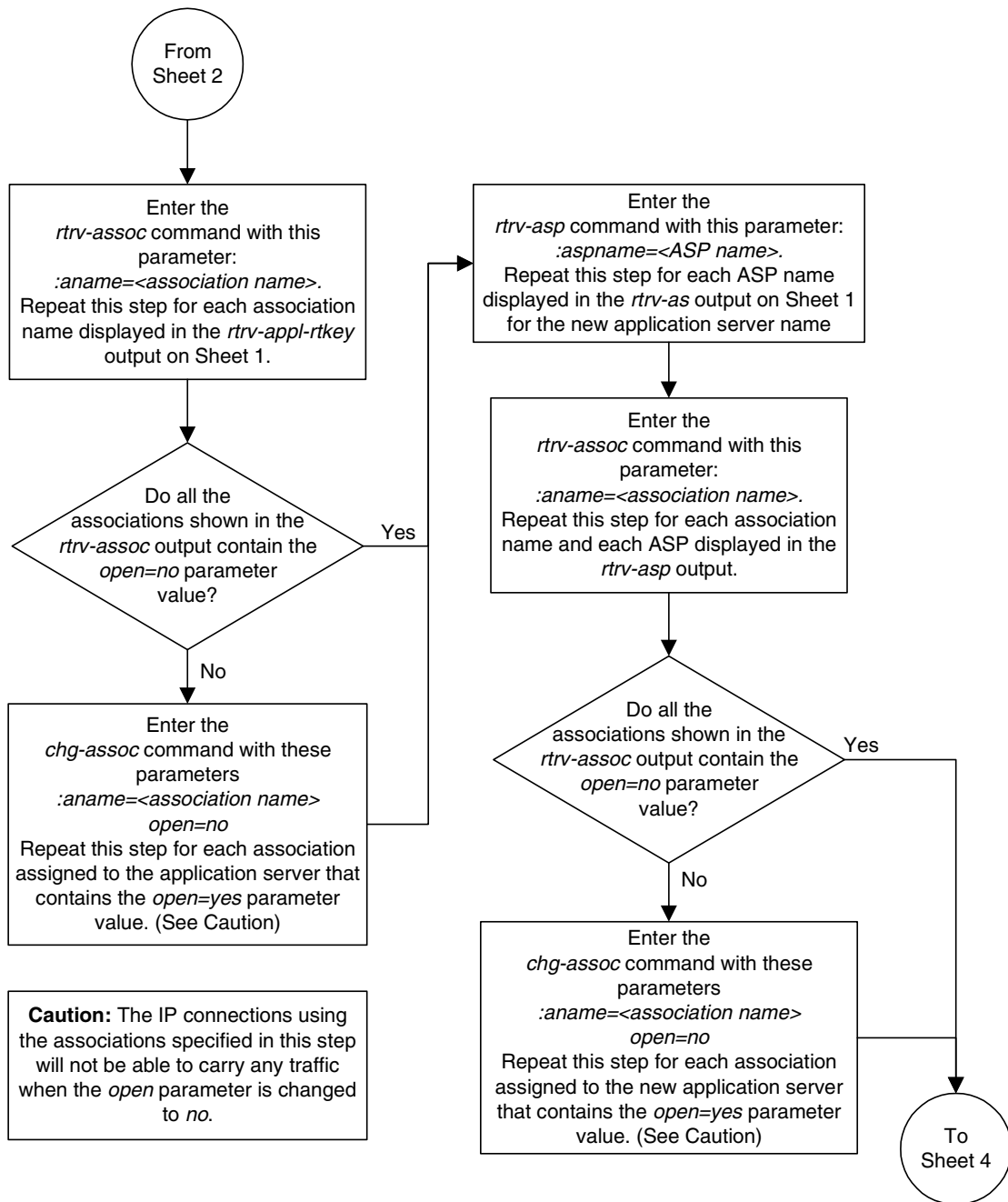
Flowchart 3-28. Assigning a New Application Server Name to an Existing Application Routing Key (Sheet 1 of 4)

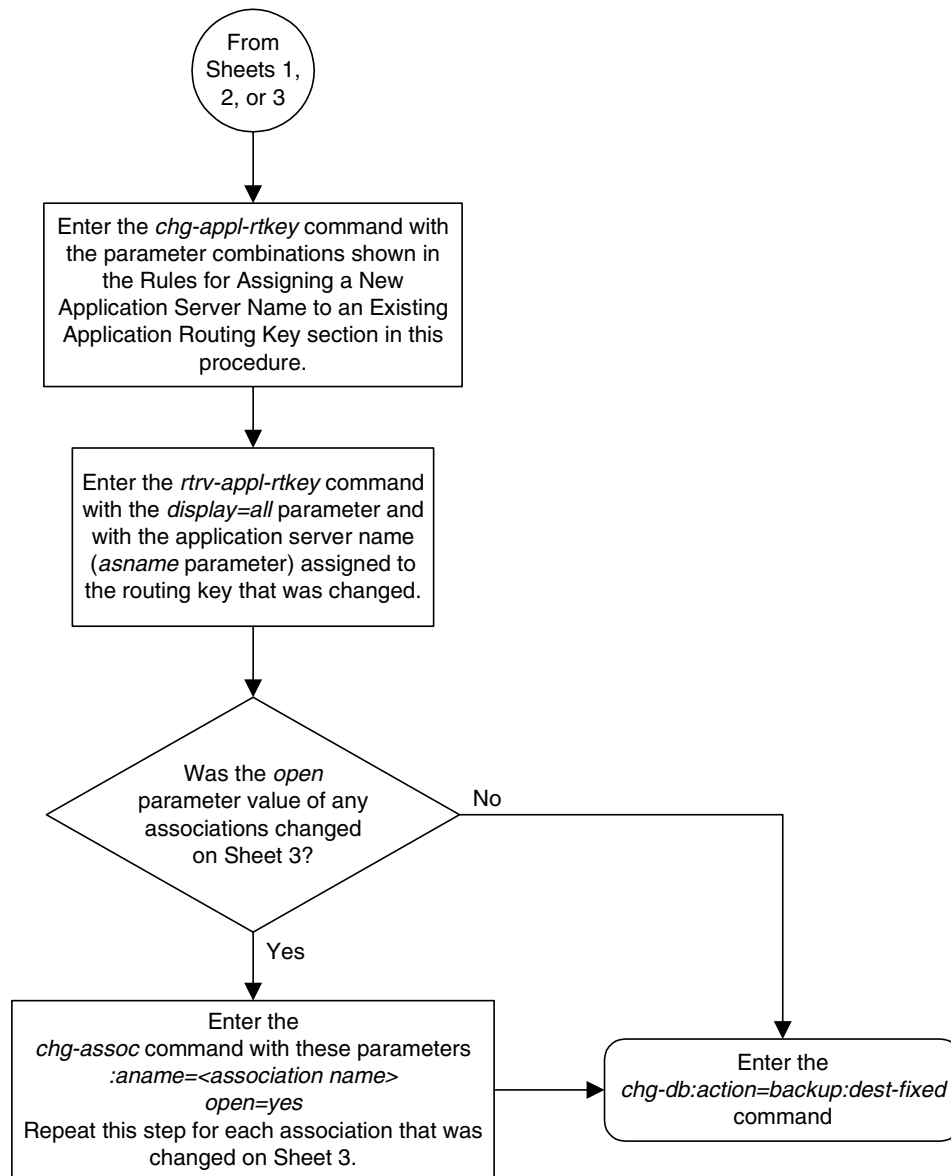


Flowchart 3-28. Assigning a New Application Server Name to an Existing Application Routing Key (Sheet 2 of 4)



Flowchart 3-28. Assigning a New Application Server Name to an Existing Application Routing Key (Sheet 3 of 4)



Flowchart 3-28. Assigning a New Application Server Name to an Existing Application Routing Key (Sheet 4 of 4)

Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key

This procedure is used for the `ss7ipgw` and `ipgwi` applications to change the PSTN (public switched telephone network) presentation and normalization settings in an application routing key using the `chg-appl-rtkey` command with these parameters.

- `:pstncat` – The PSTN category assigned to the routing key.
- `:pstnid` – The PSTN ID assigned to the routing key.
- `:norm` – Specifies whether the ISUP Normalization process is enabled or disabled for MSUs using the routing key.

The PSTN presentation information is a 32-bit value indicating the format of the MTP-3 data portion of a MSU while it exists in a public switched telephone network. It consists of a PSTN category and PSTN ID value which identifies the protocol that is used to encode or decode the data in the MTP-3 portion of MSUs. The PSTN category is used to identify a logical partitioning of groups of PSTN IDs. The PSTN ID uniquely identifies a presentation within a given PSTN category.

The `pstncat`, `pstnid`, and `norm` values are used to identify the PSTN presentation and normalization attributes for the routing key. These values allow the system to convey the PSTN format information to IP devices and control the normalization process for MSUs using the routing key.

Table 4-1 on page 4-3 shows the PSTN presentation information used by these parameters and supported by the system. The values shown in the PSTN Category and PSTN ID columns in Table 4-1 are used as the values for the `pstncat` and `pstnid` parameters of the `chg-appl-rtkey` command.

The information in Table 4-1 is also shown in the output of the `rtrv-pstn-pres` command. The values in the `PSTNCAT Value(s)` and `Valid PSTNID Value(s) in PSTNCAT` columns in the following output example are the values that can be used by the `pstncat` and `pstnid` parameters of the `chg-appl-rtkey` command.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0

PSTNCAT      PSTNID      PSTNDESC
00001        00001      ITU Q.767
00001        00002      ETSI V3
00001        00003      UK PNO-ISC7
00001        00004      GERMAN ISUP
00001        00020      MEXICO
04096        01000      User Defined 4096/1000
```

These parameters are also used by the `chg-appl-rtkey` command to change the PSTN presentation and normalization settings in the routing key.

`:dpc/dpca/dpci/dpcn/dpcn24` – Destination point code value that is used to filter incoming MSUs.

NOTE: See the “Point Code Formats” section in the *Database Administration Manual - SS7* for a definition of the point code types that are used on the system and for a definition of the different formats that can be used for ITU national point codes.

`:si` – The service indicator value that is used to filter incoming MSUs. The range of values for the service indicator parameter (`si`) can be a numerical value from 0 to 15, or for selected service indicator values, a text string can be used instead of numbers. Table 3-33 shows the text strings that can be used in place of numbers for the service indicator values.

Table 3-33. Service Indicator Text String Values

Service Indicator Value	Text String
0	snm
1	regtest
2	spltst
3	sccp
4	tup
5	isup
13	qbicc

`:opc/opca/opci/opcn/opcn24` - The originating point code value that is used to filter incoming MSUs. This value must not specify a cluster route.

NOTE: See the “Point Code Formats” section in the *Database Administration Manual - SS7* for a definition of the point code types that are used on the system and for a definition of the different formats that can be used for ITU national point codes.

`:cics` - Starting circuit identification code that is used to filter incoming MSUs. Specify with `cice` to identify the routing key to be changed.

`:cice` - Ending circuit identification code that is used to filter incoming MSUs. Specify with `cics` to identify the routing key to be changed.

`:type` - Key type. Identifies the type of application routing key that will be changed. If the `type` parameter is not explicitly specified, `type = full` is assumed.

`:ssn` – The subsystem number value that is used to filter incoming MSUs.

The **chg-appl-rtkey** command also contains these parameters, but these parameters cannot be used when changing the PSTN presentation information in the routing key. For more information on these parameters, see the “Replacing the IP Connections in an Existing Application Routing Key with a Single Socket” procedure on page 3-267.

:nsname – The name of the new socket that will receive the incoming MSU.

:ncics – New starting circuit identification code that is used to filter incoming MSUs.

:ncice – New ending circuit identification code that is used to filter incoming MSUs.

:split – The circuit identification code value where the specified range of the routing key specified by the **cics** and **cice** values is to be split into two entries.

:nasname – The name of the new application server that will receive the incoming MSU.

:rcontext – The routing context value assigned to the routing key.

The **pstnid=0** parameter can be specified only with the **pstncat=0** parameter.

The values 2 through 4095 for the **pstncat** parameter are reserved and cannot be used.

If the value of the **pstncat** parameter is from 4096 to 65536, the value of the **pstnid** parameter can be from 0 to 65535.

The **norm=no** parameter can be specified for all values of the **pstncat** parameter. The **pstncat=1** and the **pstnid=<1,2,3, or 4>** parameters are specified with the **norm=no** parameter, ISUP normalization will not be performed on MSUs using the routing key.

The **pstncat=1** parameter may only be used with 14-bit ITU-N, 24-bit ITU-N, or ITU-I point codes and when the value of the service indicator parameter is 5. The value of the **pstnid** parameter specified with the **pstncat=1** parameter can range from 1 to 32.

The **norm=yes** parameter can be specified only under these conditions:

- The value of the **pstncat** parameter must be 1
- The value of the **pstnid** parameter values can range from 1 to 32.
- The ISUP Normalization controlled feature must be enabled and its status must be on.
- The value of the service indicator parameter in the routing key must be 5.
- The point code in the routing key must be either an ITU-I, 14-bit ITU-N, or 24-bit ITU-N point code.
- The controlled feature associated with the **pstnid** parameter values 1 to 32 must be enabled and its status must be on.

The **rtrv-ctrl-feat** command shows whether or not the controlled features are enabled. If any of the required controlled features are not enabled, enter the **enable-ctrl-feat** command with the feature part number and the feature access key for the required controlled feature. The status of these controlled features is set to **on** with the **chg-ctrl-feat** command.

NOTE: If you do not have the part number or the feature access key for the required controlled feature, contact your Tekelec sales representative or account representative.

Table 4-1 on page 4-3 also shows the part numbers of the controlled features used in this procedure. The Quantity Control feature allows a customer to provision a specified quantity of user-defined variants within the PSTN categories 4096 - 65535. Each Quantity Control Feature is associated with a specific quantity of variants. To provision user-defined variants, it is necessary to purchase the appropriate Feature Access Keys from Tekelec. Variants enabled using the Quantity Control feature do not have associated PSTN Presentation values.

The part number for user-defined variants is 893-0100-nn, where nn is a number ranging from 01 to 20. Use part number 893-0100-01 to order one new variant, 893-0100-05 to order five new variants, and so on.

The values of the **dpc**, **opc**, **si**, **cics**, and **cice** parameters specified in this procedure must match the values in the routing key that is being changed in this procedure.

If the ITU National Duplicate Point Code feature is on, the values for the **dpcn** and **opcn** parameters must have group codes assigned to them. The field **ITUDUPPC** in the **rtrv-feat** command output shows whether or not the ITU National Duplicate Point Code feature is on. If group codes are specified for ITU-N DPC and OPC, the groups codes must be the same.

Canceling the RTRV-APPL-RTKEY Command

Because the `rtrv-appl-rtkey` command used in this procedure can output information for a long period of time, the `rtrv-appl-rtkey` command can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-appl-rtkey` command can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-appl-rtkey` command was entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-appl-rtkey` command was entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-appl-rtkey` command was entered, from another terminal other than the terminal where the `rtrv-appl-rtkey` command was entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current application routing key information in the database by entering the `rtrv-appl-rtkey` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC          SI SSN OPC          CICS          CICE
  STATIC 123-234-123 5 --- 122-124-125      1           1000
  STATIC 123-234-123 5 --- 100-100-100       1             50
    1105 005-005-001 5 --- 010-010-001       1             500
  1105 005-005-001 5 --- 010-010-001     501          1000
  1107 006-006-001 5 --- 011-011-001       1             500
  1107 006-006-001 5 --- 011-011-001     501          1000

STATIC Route Key table is (2 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (2 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

2. Display the current values of the **pstncat**, **pstnid**, and **norm** parameters of the routing key by entering the **rtrv-appl-rtkey** command with the DPC of the routing key shown in step 1 and the **display=all** parameter. For this example, enter this command.

```
rtrv-appl-rtkey:dpcn=12323-de:display=all
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC          SI SSN OPCA          CICS      CICE
      STATIC 12323-DE    5 --- 12212-DE    1         1000
      ATTR:PSTNCAT PSTNID NORM DUP
              0      0 N  -
      SNAMEs:socket6

STATIC Route Key table is (2 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (2 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

NOTE: If the value of the **norm** parameter is being set to **no**, skip steps 3 and 4, and go to step 5.

3. Verify that the ISUP Normalization controlled feature is enabled and activated by entering the **rtrv-crt1-feat** command. If the ISUP Normalization controlled feature is enabled, the ISUP Normalization controlled feature name should be shown in the **Feature Name** field of the output, and the status of the ISUP Normalization controlled feature, in the **status** field, should be set to **on**. The following is an example of the possible output

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
The following features have been permanently enabled:

Feature Name          Partnum    Status    Quantity
IPGWx Signaling TPS  893012814 on        20000
ISUP Normalization   893000201 on        ----
ETSI v3 Normalization 893000601 on        ----

The following features have been temporarily enabled:

Feature Name          Partnum    Status    Quantity    Trial Period Left
Zero entries found.

The following features have expired temporary keys:

Feature Name          Partnum
Zero entries found.
```

If the ISUP Normalization controlled feature is not enabled and turned on, go to the “Enabling Controlled Features” procedure on page 6-2 and to “Turning On and Off Controlled Features” procedure on page 6-10 to enable and turn on the ISUP Normalization controlled feature.

4. Display the PSTN presentation information supported by the system by entering the `rtrv-pstn-pres` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
PSTNCAT PSTNID PSTNDESC
00001 00001 ITU Q.767
00001 00002 ETSI V3
00001 00003 UK PNO-ISC7
00001 00004 GERMAN ISUP
04096 01000 User Defined 4096/1000
```

ISUP Variant table is (6 of 21) 29% full

NOTE: An * will be displayed next to the PSTN Category for entries that are no longer usable. These are entries that are disabled because their temporary feature key expired.

The output of the `rtrv-pstn-pres` command shows the values in the **PSTNCAT Value(s)** and **Valid PSTNID Value(s)** in **PSTNCAT** columns that can be used by the `pstncat` and `pstnid` parameters of the `chg-appl-rtkey` command

If the value of the `norm` parameter is being set to `yes`, and the `rtrv-ctrl-feat` output in step 3 shows that the controlled feature that corresponds to the PSTNID parameter value being specified in this procedure is not enabled and turned on, go to the “Enabling Controlled Features” procedure on page 6-2 and to “Turning On and Off Controlled Features” procedure on page 6-10 to enable and turn on the required controlled feature.

Table 4-1 on page 4-3 shows the part numbers of the controlled features and the `pstnid` parameter values that can be used in this procedure.

NOTE: If 14-bit ITU-N point codes (`dpcn`, `opcn`) are not being specified for the routing key, skip step 5 and go to step 6.

5. Verify whether or not the ITU National Duplicate Point Code feature is on, by entering the `rtrv-feat` command. If the ITU National Duplicate Point Code feature is on, the `ITUDUPPC` field will be set to `on`.

NOTE: The `rtrv-feat` command output contains other fields that are not used by this procedure. If you wish to see all the fields displayed by the `rtrv-feat` command, see the `rtrv-feat` command description in the *Commands Manual*.

6. Change PSTN presentation information in the routing key by entering the **chg-appl-rtkey** command with the **pstncat**, **pstnid**, and **norm** parameters.

```
chg-appl-rtkey:dpcn=12323-de:si=5:opc=12212-de:cics=1
:cice=1000:pstncat=1:pstnid=2:norm=yes
```

NOTE: If the DPC and OPC values are ITU-N point codes, these point codes must have group codes assigned to them if the ITU National Duplicate Point Code feature is on. The **ITUDUPPC** field in the **rtrv-feat** command executed in step 5 shows whether or not the ITU National Duplicate Point Code feature is on.

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
CHG-APPL-RTKEY: MASP A - COMPLTD
```

7. Verify the new values of the **pstncat**, **pstnid**, and **norm** parameters that were changed in step 6 by entering the **rtrv-appl-rtkey** command with the DPC of the routing key specified in step 6 and the **display=all** parameter. For this example, enter this command.

```
rtrv-appl-rtkey:dpcn=12323-de:display=all
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0

KEY:LOC      DPC          SI SSN OPCA          CICS          CICE
      STATIC 12323-DE    5 --- 12212-DE    1             1000
      ATTR:PSTNCAT PSTNID NORM DUP
              1         2 Y   -
      SNAMEs: socket6

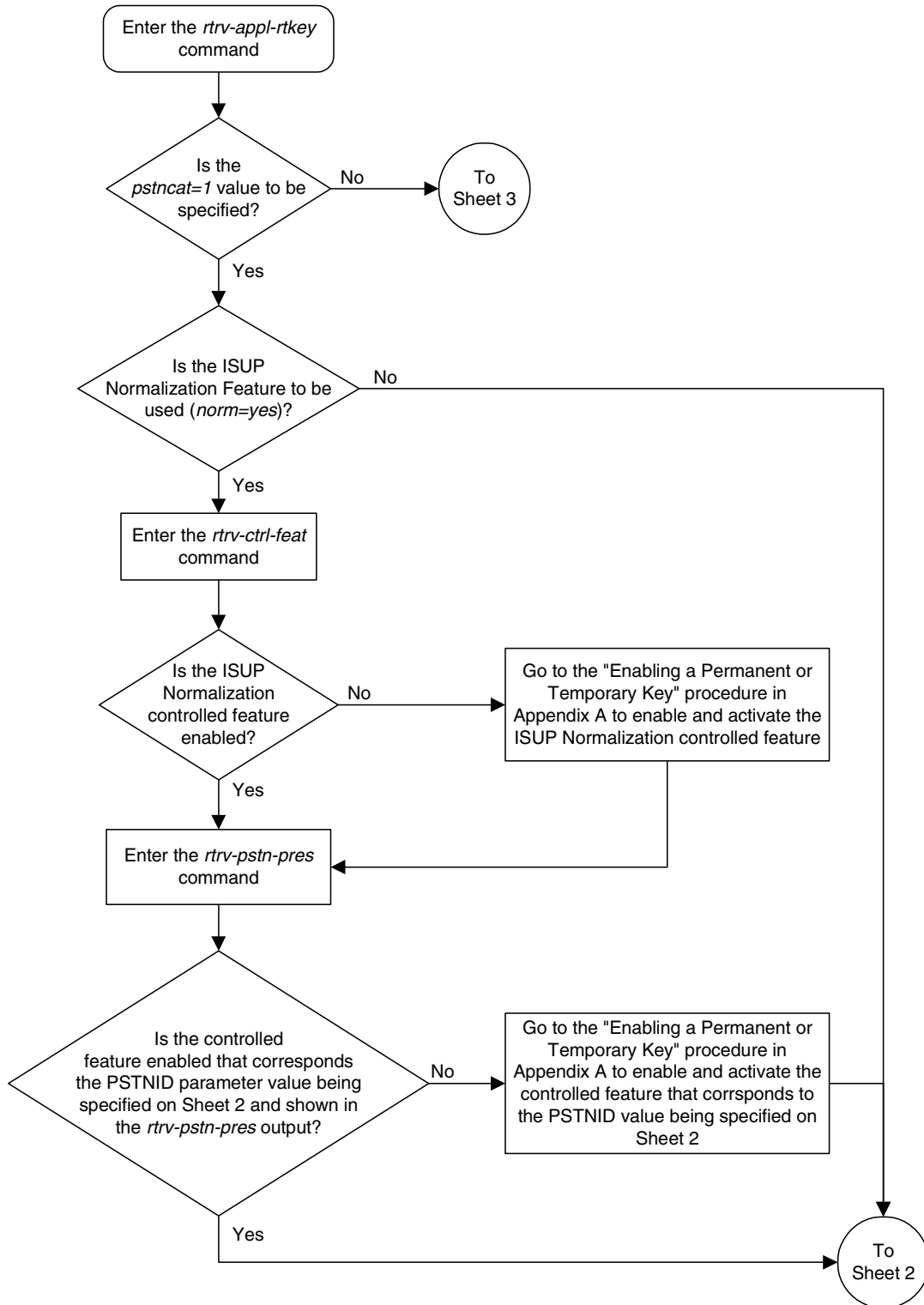
STATIC Route Key table is (2 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full

STATIC Route Key Socket Association table is (2 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

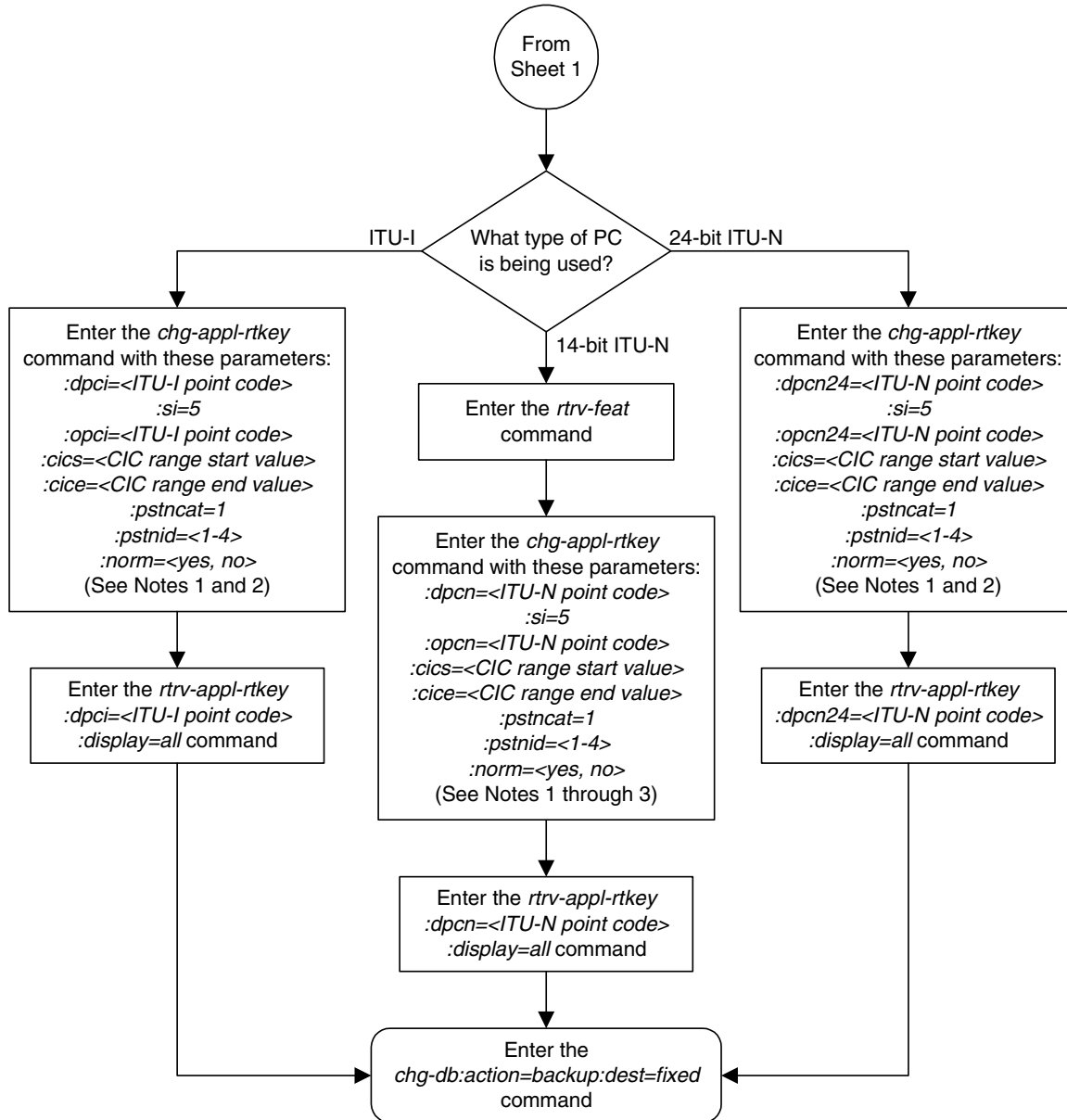
8. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-29. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key (Sheet 1 of 6)



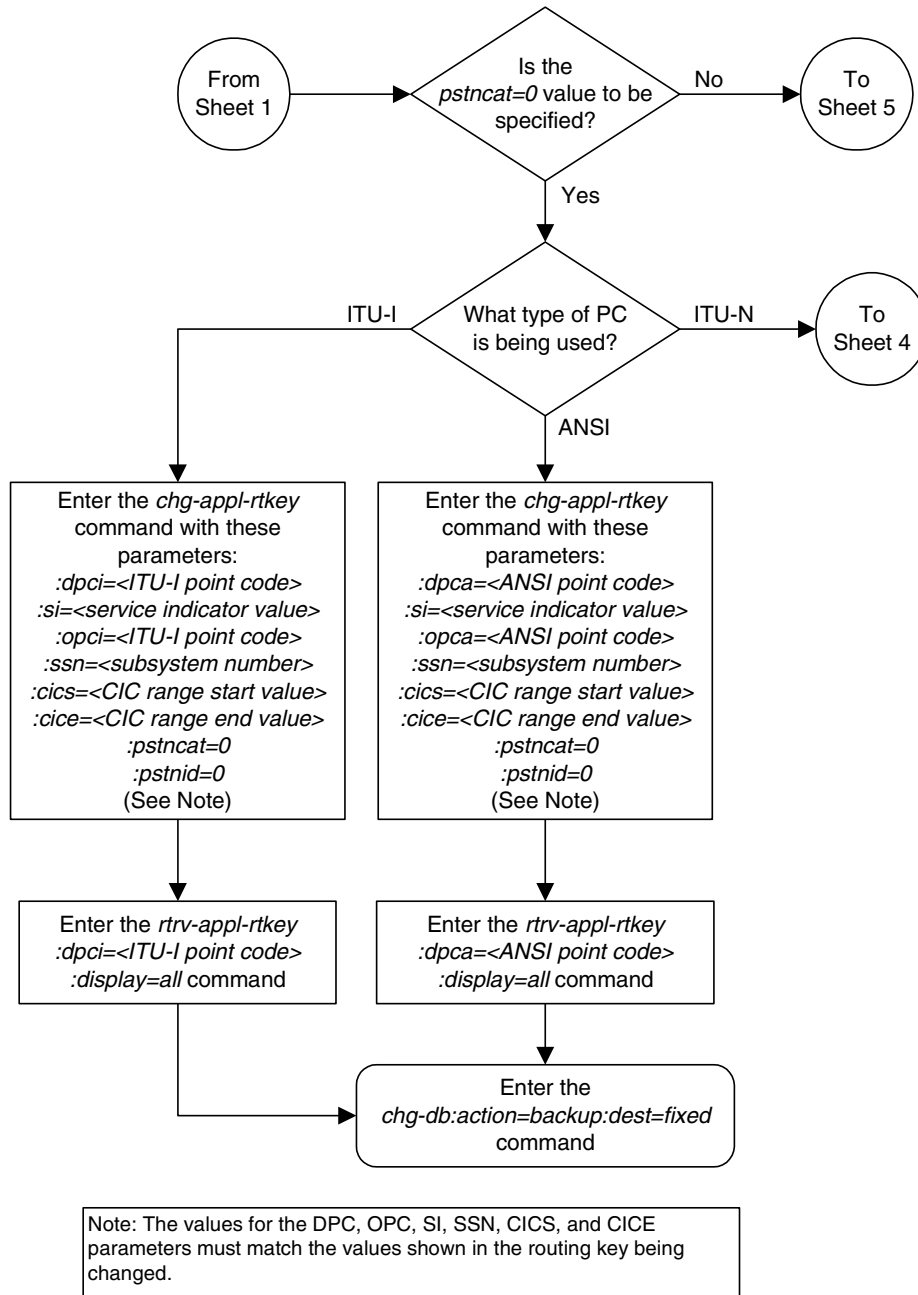
Flowchart 3-29. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key (Sheet 2 of 6)



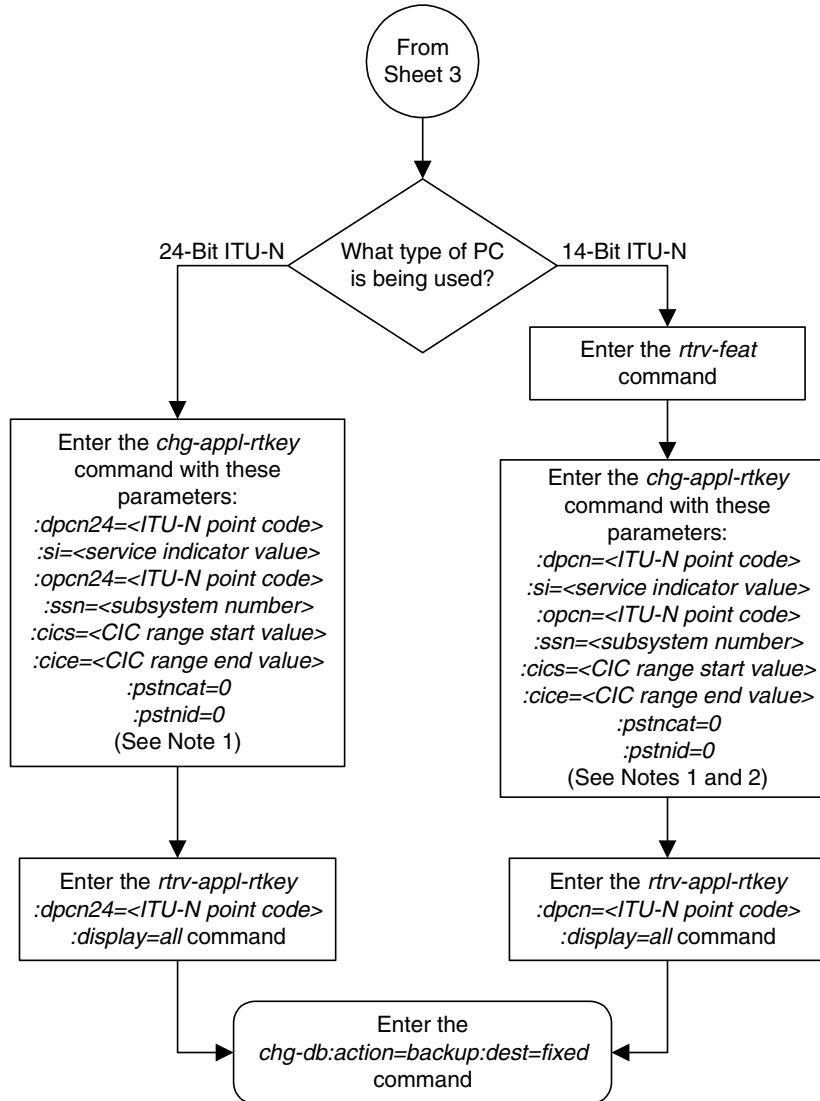
Notes:

1. The *norm=yes* parameter is only required if the ISUP Normalization feature is to be used for the MSUs using the routing key.
2. The values for the DPC, OPC, SI, CICS, and CICE parameters must match the values shown in the routing key being changed.
3. If the Duplicate Point Code feature is on, the DPCN and OPCN values must have a group code assigned to the point code. If both the DPCN and OPCN parameters are specified, the group codes must be the same. The ITUDUPPC field in the *rtvr-feat* command shows whether or not this feature is on.

Flowchart 3-29. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key (Sheet 3 of 6)

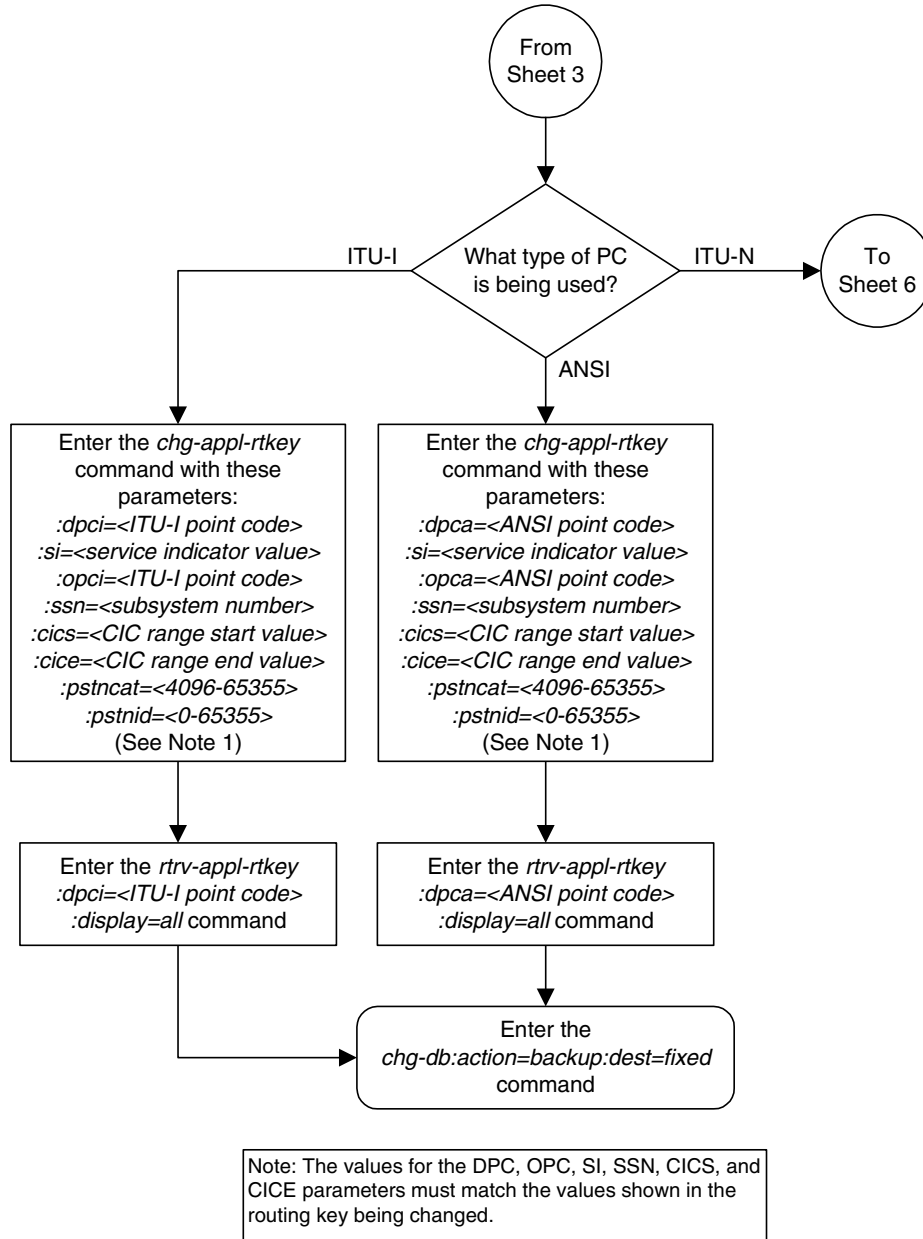


Flowchart 3-29. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key (Sheet 4 of 6)

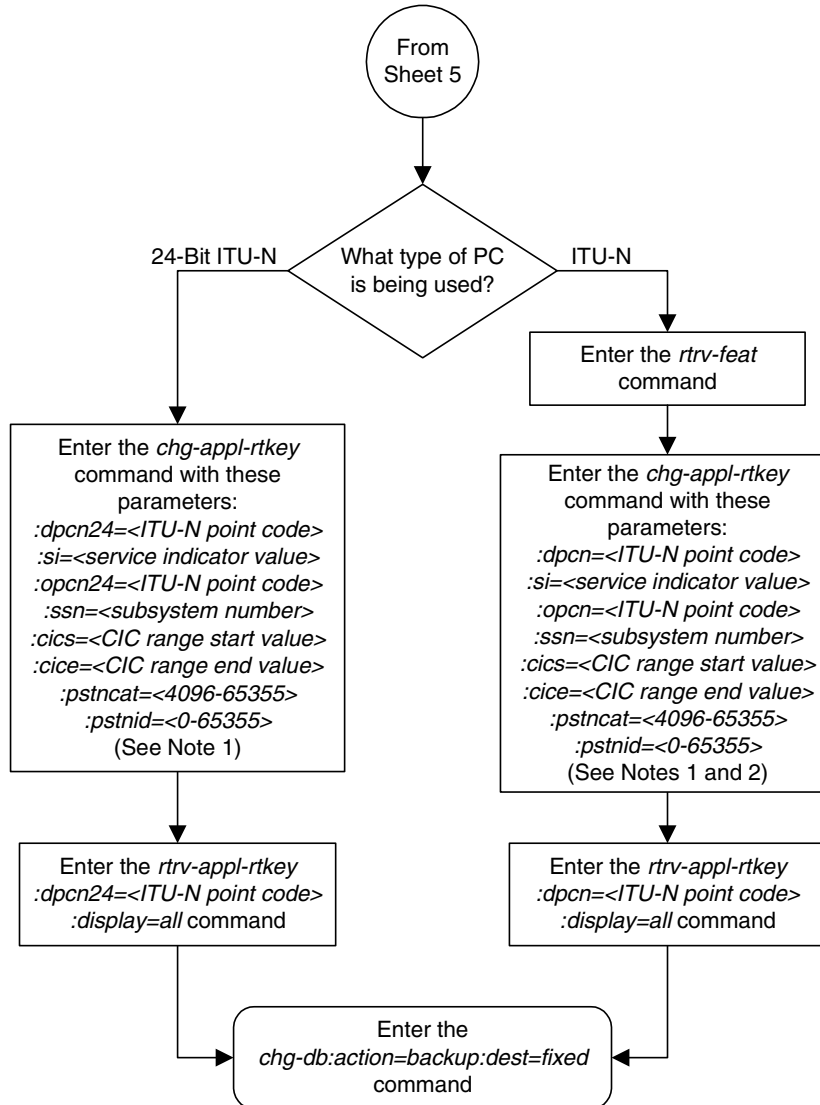


Notes:
 1. The values for the DPC, OPC, SI, SSN, CICS, and CICE parameters must match the values shown in the routing key being changed.
 2. If the Duplicate Point Code feature is on, the DPCN and OPCN values must have a group code assigned to the point code. If both the DPCN and OPCN parameters are specified, the group codes must be the same. The ITUDUPPC field in the *rtvr-feat* command shows whether or not this feature is on.

Flowchart 3-29. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key (Sheet 5 of 6)



Flowchart 3-29. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key (Sheet 6 of 6)



Notes:
 1. The values for the DPC, OPC, SI, SSN, CICS, and CICE parameters must match the values shown in the routing key being changed.
 2. If the Duplicate Point Code feature is on, the DPCN and OPCN values must have a group code assigned to the point code. If both the DPCN and OPCN parameters are specified, the group codes must be the same. The ITUDUPPC field in the *rtrv-feat* command shows whether or not this feature is on.

Increasing the System-Wide IPGWx Signaling TPS

This procedure is used with **IPGWx** applications (IP cards running either the **ss7ipgw** or **ipgwi** applications) and increases the system-wide IP transactions per second (TPS), using the **enable-ctrl-feat** command.

The system is shipped with a default TPS rate of 200 transactions per second.

The **enable-ctrl-feat** command uses these parameters.

:partnum – The Tekelec-issued part number associated with the controlled feature. The part number is a 9-digit number, not including dashes; the first three digits must be 893 (that is, 893xxxxxx, where x is a numeric value). Table 3-34 on page 3-322 shows the part numbers that can be used with this procedure.

:fak – The feature access key obtained from the Tekelec Customer Service department. The feature access key contains 13 alphanumeric characters and is not case sensitive.

NOTE: The number of system IP transactions per second cannot be enabled with a temporary feature access key.

NOTE: If you do not have the feature access key, you can obtain it from your Tekelec Sales Representative or Account Representative.

The **enable-ctrl-feat** command requires that the database contain a valid serial number for the system, and that this serial number is locked. This can be verified with the **rtrv-serial-num** command. The system is shipped with a serial number in the database, but the serial number is not locked. The serial number can be changed, if necessary, and locked once the system is on-site, by using the **ent-serial-num** command. The **ent-serial-num** command uses these parameters.

:serial – The serial number assigned to the system. The serial number is not case sensitive.

:lock – Specifies whether or not the serial number is locked. This parameter has only one value, **yes**, which locks the serial number. Once the serial number is locked, it cannot be changed.

NOTE: To enter and lock the system's serial number, the ent-serial-num command must be entered twice, once to add the correct serial number to the database with the serial parameter, then again with the serial and the lock=yes parameters to lock the serial number. You should verify that the serial number in the database is correct before locking the serial number. The serial number can be found on a label affixed to the control shelf (shelf 1100).

The TPS rate specified in this procedure must be greater than the current TPS rate.

Table 3-34. System-Wide IPGWx Signaling TPS Part Numbers

Part Number	IPGWx System IP TPS	Part Number	IPGWx System IP TPS	Part Number	IPGWx System IP TPS
893-0128-01	200	893-0128-21	34,000	893-0128-41	74,000
893-0128-02	400	893-0128-22	36,000	893-0128-42	76,000
893-0128-03	600	893-0128-23	38,000	893-0128-43	78,000
893-0128-04	1,000	893-0128-24	40,000	893-0128-44	80,000
893-0128-05	2,000	893-0128-25	42,000	893-0128-45	82,000
893-0128-06	4,000	893-0128-26	44,000	893-0128-46	84,000
893-0128-07	6,000	893-0128-27	46,000	893-0128-47	86,000
893-0128-08	8,000	893-0128-28	48,000	893-0128-48	88,000
893-0128-09	10,000	893-0128-29	50,000	893-0128-49	90,000
893-0128-10	12,000	893-0128-30	52,000	893-0128-50	92,000
893-0128-11	14,000	893-0128-31	54,000	893-0128-51	94,000
893-0128-12	16,000	893-0128-32	56,000	893-0128-52	96,000
893-0128-13	18,000	893-0128-33	58,000	893-0128-53	98,000
893-0128-14	20,000	893-0128-34	60,000	893-0128-54	100,000
893-0128-15	22,000	893-0128-35	62,000	893-0128-55	102,000
893-0128-16	24,000	893-0128-36	64,000	893-0128-56	104,000
893-0128-17	26,000	893-0128-37	66,000	893-0128-57	106,000
893-0128-18	28,000	893-0128-38	68,000	893-0128-58	108,000
893-0128-19	30,000	893-0128-39	70,000	893-0128-59	110,000
893-0128-20	32,000	893-0128-40	72,000	893-0128-60	112,000

Procedure

1. Display enabled controlled feature information in the database by entering the `rtrv-ctrl-feat` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
The following features have been permanently enabled:
```

Feature Name	Partnum	Status	Quantity
IPGWx Signaling TPS	893012801	on	200
ISUP Normalization	893000201	on	----
ETSI v3 Normalization	893000601	on	----

```
The following features have been temporarily enabled:
```

Feature Name	Partnum	Status	Quantity	Trial Period Left
Zero entries found.				

```
The following features have expired temporary keys:
```

Feature Name	Partnum
Zero entries found.	

NOTE: If the `rtrv-ctrl-feat` output in step 1 shows any controlled features are enabled, or if the IPGWx Signaling TPS quantity is greater than 200, skip steps 2 through 5, and go to step 6.

2. Display the serial number in the database with the `rtrv-serial-num` command. This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
System serial number = nt00001231
```

```
System serial number is not locked.
```

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
Command Completed
```

NOTE: If the serial number is correct and locked, skip steps 3, 4, and 5, and go to step 6. If the serial number is correct but not locked, skip steps 3 and 4, and go to step 5. If the serial number is not correct, but is locked, this feature cannot be enabled and the remainder of this procedure cannot be performed. Contact Tekelec Technical Services to get an incorrect and locked serial number changed. See "Tekelec Technical Services" on page 1-8. The serial number can be found on a label affixed to the control shelf (shelf 1100).

3. Enter the correct serial number into the database using the `ent-serial-num` command with the `serial` parameter.

For this example, enter this command.

```
ent-serial-num:serial=<system's correct serial number>
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 03-02-28 21:15:37 GMT Rel 30.0.0
ENT-SERIAL-NUM: MASP A - COMPLTD
```

- Verify that the serial number entered into step 3 was entered correctly using the **rtrv-serial-num** command. This is an example of the possible output.

```
rlghncxa03w 03-02-28 21:15:37 GMT Rel 30.0.0
System serial number = nt00001231
```

System serial number is not locked.

```
rlghncxa03w 03-02-28 21:15:37 GMT Rel 30.0.0
Command Completed
```

If the serial number was not entered correctly, repeat steps 3 and 4 and re-enter the correct serial number.

- Lock the serial number in the database by entering the **ent-serial-num** command with the serial number shown in step 2, if the serial number shown in step 2 is correct, or with the serial number shown in step 4, if the serial number was changed in step 3, and with the **lock=yes** parameter.

For this example, enter this command.

```
ent-serial-num:serial=<system's serial number>:lock=yes
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 03-02-28 21:15:37 GMT Rel 30.0.0
ENT-SERIAL-NUM: MASP A - COMPLTD
```

- Increase the system-wide IP transactions per second (TPS) by entering the **enable-ctrl-feat** command with the part number corresponding to the desired quantity (without the dashes), shown in Table 3-34 on page 3-322, and the feature access key for the desired quantity. For example, enter this command.

```
enable-ctrl-feat:partnum=893012814:fak=<feature access key>
```

NOTE: The number of system IP transactions per second cannot be enabled with a temporary feature access key.

NOTE: If you do not have the feature access key, you can obtain it from your Tekelec Sales Representative or Account Representative.

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
ENABLE-CTRL-FEAT: MASP A - COMPLTD
```

7. Verify the new feature information in the database by entering the **rtrv-ctrl-feat** command with the part number specified in step 6. For this example, enter this command.

```
rtrv-ctrl-feat:partnum=893012814
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
```

The following features have been permanently enabled:

Feature Name	Partnum	Status	Quantity
IPGWx Signaling TPS	893012814	on	20000

The following features have been temporarily enabled:

Feature Name	Partnum	Status	Quantity	Trial Period Left
Zero entries found.				

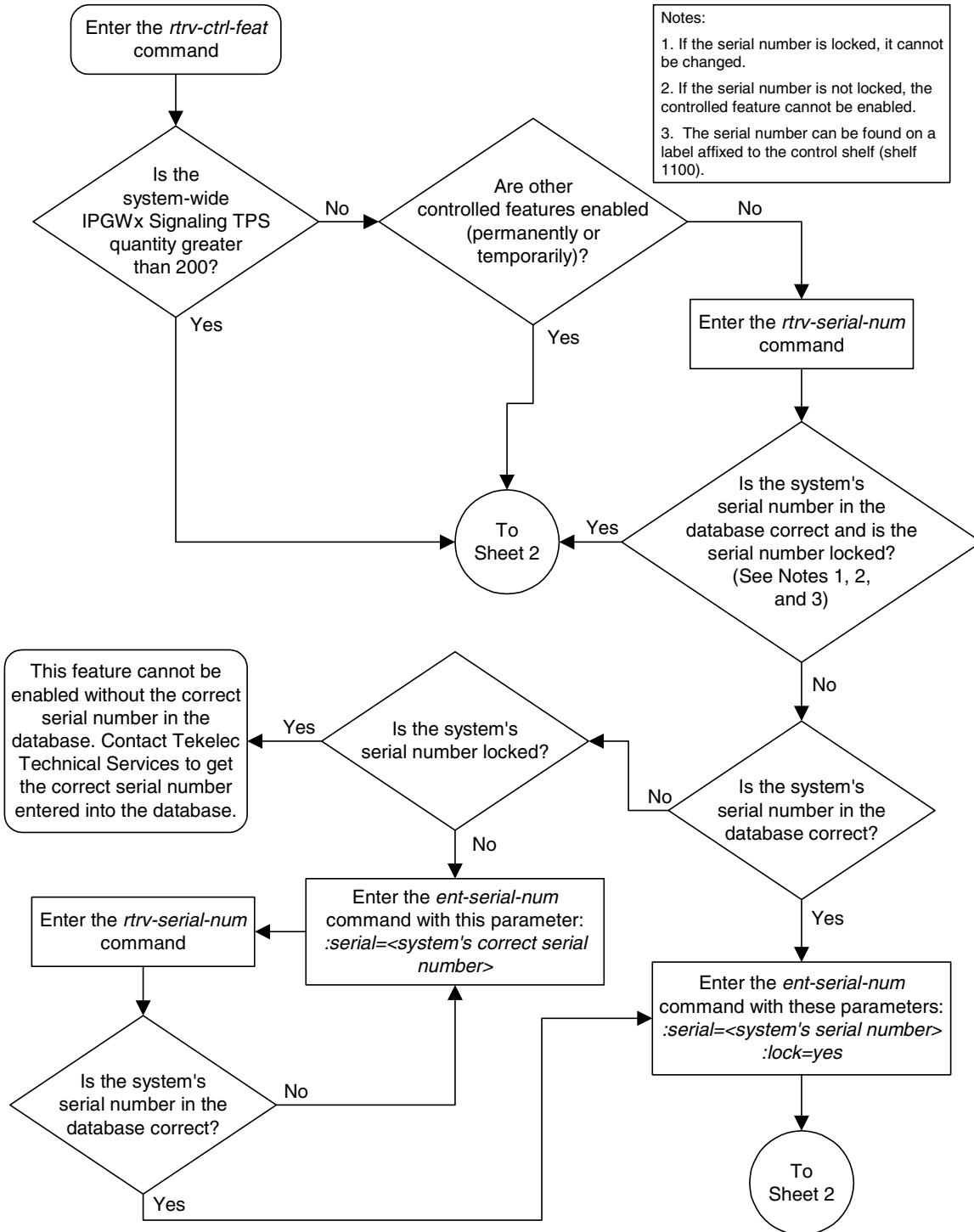
The following features have expired temporary keys:

Feature Name	Partnum
Zero entries found.	

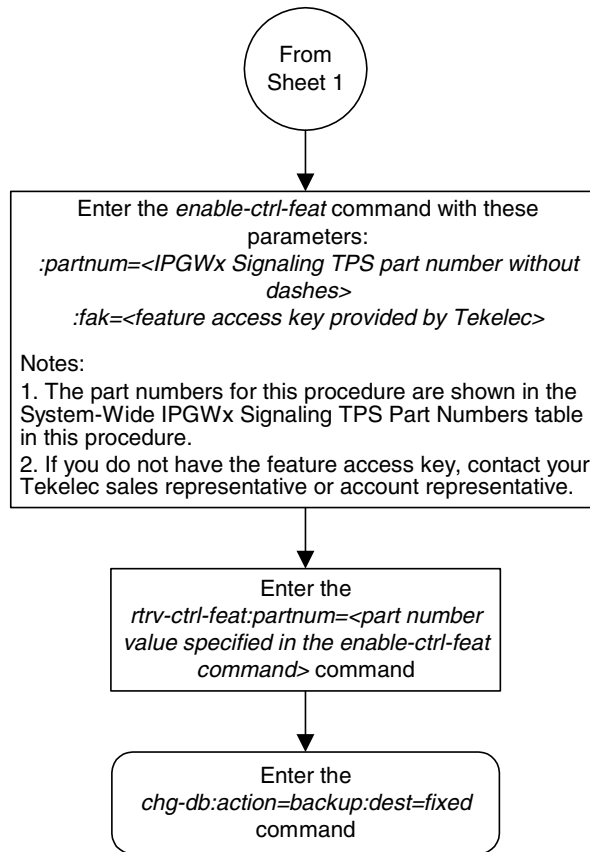
-
8. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-30. Increasing the IPGWx Signaling TPS (Sheet 1 of 2)



Flowchart 3-30. Increasing the IPGWx Signaling TPS (Sheet 1 of 2)



Configuring the IP TPS Alarm Threshold

The IP TPS alarm threshold is the percentage of the IPGWx signaling TPS at which an alarm is raised. This threshold is set with the `iptpsalmthresh` parameter of the `chg-stpopts` command. The values for the `iptpsalmthresh` parameter are from 10 to 100 percent, with the system default value of 80 percent. The value of the IP TPS alarm threshold is shown in the `IPTPSALMTHRESH` field of the `rtrv-sg-opts` command output.

When this threshold is exceeded, UAM 0114, System IP TPS Threshold exceeded, is generated. UAM 0114 is automatically cleared when the percentage of the IPGWx signaling TPS calculated by the system falls below the value of the `iptpsalmthresh` parameter value. UAM 0117, System IP TPS normal, is generated when UAM 0114 is cleared.



CAUTION: UAM 0114 is also generated if the IP TPS alarm threshold is set to a percentage that is less than the current percentage of the IPGWx signaling TPS calculated by the system. If UAM 0114 is not automatically cleared after performing this procedure, perform the alarm clearing procedure for UAM 0114 in the *Maintenance Manual*.

Procedure

1. Display the current IP options in the database by entering the `rtrv-sg-opts` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SYNC:          TALI
SRKQ:          250
DRKQ:          750
SNMPCONT:     john doe 555-123-4567
GETCOMM:      public
SETCOMM:      private
TRAPCOMM:     public
INHFEPALM:    NO
SCTPCSUM:     crc32c
IPGWABATE:    NO
IPLIMABATE:   NO
IPTPSALMTHRESH: 80
```

2. Change the IP TPS alarm threshold using the `chg-sg-opts` command and the `iptpsalmthresh` parameter. For this example, enter this command.

```
chg-sg-opts:iptpsalmthresh=90
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
CHG-SG-OPTS: MASP A - COMPLTD
```



CAUTION: UAM 0114 is generated if the IP TPS alarm threshold is set to a percentage that is less than the current percentage of the IPGWx signaling TPS calculated by the system. If UAM 0114 is not automatically cleared after performing this procedure, perform the alarm clearing procedure for UAM 0114 in the *Maintenance Manual*.

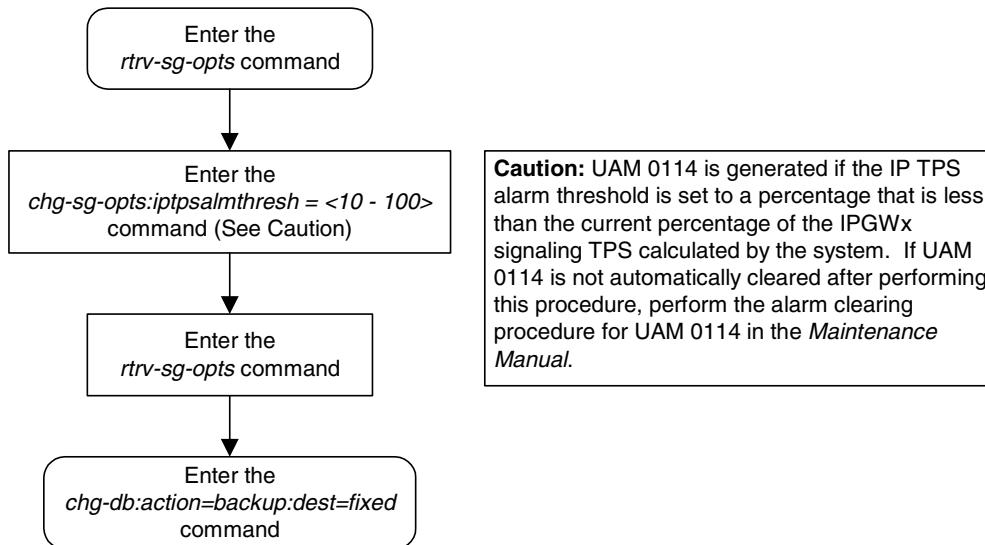
-
3. Verify the new IP options in the database using the `rtrv-sg-opts` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SYNC:          SASSI
SRKQ:          250
DRKQ:          750
SNMPCONT:      john doe 555-123-4567
GETCOMM:       public
SETCOMM:       private
TRAPCOMM:      public
INHFEPALM:    NO
SCTPCSUM:      crc32c
IPGWABATE:     NO
IPLIMABATE:    NO
IPTPSALMTHRESH: 90
```

-
4. Back up the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-31. Configuring the IP TPS Alarm Threshold



IETF Adapter Layer Configuration

To provision the IETF Adapter layer, associations, application server processes, and application servers must be configured in the database, in this order:

1. Associations
2. Application server processes (ASP)
3. Application servers (AS).

NOTE: The M3UA and M2PA adapter layers on cards running either the IPLIM or IPLIMI applications (IPLIMx cards) does not support application servers. Application servers cannot be provisioned for ASPs containing associations assigned to IPLIMx cards. The M2PA adapter layer does not support ASPs, thus ASPs cannot be provisioned for associations using the M2PA adapter layer assigned to IPLIMx cards. The M3UA adapter layer on cards running either the SS7IPGW or IPGWI applications (IPGWx cards) does support application servers. Application servers can be provisioned for ASPs containing associations assigned to IPGWx cards.

The application server is then assigned to a routing key. The following procedures show the steps necessary to provision the associations, application server processes, and application servers.

These procedures use a variety of commands. If more information on these commands is needed, go to the *Commands Manual* to find the required information.

Adding an Association

This procedure is used to configure SCTP associations in the socket table using the **ent-assoc** command. The combination of a local host, local SCTP port, remote host and remote SCTP port defines an association.

The **ent-assoc** command uses these parameters:

- :aname** – The name assigned to the association. Valid association names can contain up to 15 alphanumeric characters where the first character is a letter and the remaining characters are alphanumeric characters. The **aname** parameter value is not case-sensitive.
- :lhost** – Local Hostname. The logical name assigned to the local host device.
- :lport** – The SCTP port number for the local host.
- :rhost** – Remote Hostname. The logical name assigned to the remote host device.
- :rport** – The SCTP port number for the remote host.
- :port** – The signaling link port on the IP card. If a signaling link port is not specified for a socket when it is entered, the socket defaults to the A port. If the card's application is **iplim** or **iplimi**, and the card is a dual-slot DCM, the values for the **port** parameter can be only **a** or **b**. If the card's application is **iplim** or **iplimi**, and the card is a single-slot EDCM, the values for the **port** parameter can be **a**, **a1**, **a2**, **a3**, **b**, **b1**, **b2**, or **b3**. If the IP card's application is **ss7ipgw** or **ipgwi**, only **port=a** can be specified.
- :adapter** – The adapter layer for this association.
- :alhost** – The alternate local host name.
- :m2patset** – The M2PA timer set assigned to the association. The **m2patset** parameter can be specified only with the **adatper=m2pa** parameter. If the **adapter=m2pa** parameter is specified, and the **m2patset** parameter is not specified with the **ent-assoc** command, the default value for the **m2patset** parameter (1 - M2PA timer set 1) is assigned to the association.

The socket table, which contains both the socket and association data, contains fields whose values are not assigned using the **ent-assoc** command. When an association is added to the database, these fields receive their default values. If a different value is desired, the **chg-assoc** command must be used. These fields and their default values are:

```

open=no           rtimes=10
alw=no           cwmin=3000
adapter=m3ua     ver=rfc
rmode=lin       istrms=2
rmin=120        ostrms=2
rmax=800

```

The value of the **lhost**, **rhost**, or **alhost** parameters is a text string of up to 60 characters, with the first character being a letter. The command line on the terminal can contain up to 150 characters. If the host names are too long to fit on the **ent-assoc** command line, go to the “Changing an Association” procedure on page 3-350 to complete the entry of the host names.

Each local host on a card running either the **ss7ipgw** or **ipgwi** applications can contain a maximum of 50 connections (associations plus sockets).

The system can contain a maximum of 4000 connections (associations plus sockets).

For the **iplim** and **iplimi** applications, the IP card can one association for each signaling link on the card. The dual-slot DCM can contain only two signaling links, resulting in a maximum of two associations on these cards. The single-slot EDCM can contain a maximum of eight signaling links, resulting in a maximum of eight associations for this card.

The B Ethernet interface of the IP card can be used only if the IP card is a single-slot EDCM.

If the association is to be activated in this procedure, with the **chg-assoc** command, the association must contain values for the **lhost**, **lport**, **rhost**, **rport** parameters.

If the card’s application is either IPLIM or IPLIMI:

- The **iplim12** parameter value of the signaling link assigned to the association must be **m3ua** or **m2pa**. The **adapter** parameter value of the association must match the **iplim12** parameter value.
- The signaling link being assigned to the association must be out of service. This state is shown in the **rept-stat-slk** output with the entries **OOS-MT** in the **PST** field and **Unavail** in the **SST** field.
- If the association is being opened in this procedure with the **chg-assoc** command and the **open=yes** parameter, the signaling link assigned to the association must be in the database and the **iplim12** parameter value of the signaling link assigned to the association must be **m3ua** or **m2pa**.

If the card’s application is either SS7IPGW or IPGWI, the signaling link being assigned to the association must be in service. This state is shown in the **rept-stat-slk** output with the entries **IS-NR** in the **PST** field and **Avail** in the **SST** field.

Uni-homed endpoints are associations configured with the **lhost** parameter only. The **lhost** parameter value represents an IP address that corresponds to either the A or B network interface of the IP card. Multi-homed endpoints are associations configured with both the **lhost** and **alhost** parameters. The **lhost** parameter value represents an IP address corresponding to one of the network interfaces (A or B) of the IP card while the **alhost** parameter value represents an IP address corresponding to the other network interface of the same IP card.

Canceling the RTRV-ASSOC Command

Because the `rtrv-assoc` command used in this procedure can output information for a long period of time, the `rtrv-assoc` command can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-assoc` command can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-assoc` command was entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-assoc` command was entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-assoc` command was entered, from another terminal other than the terminal where the `rtrv-assoc` command was entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the associations in the database using the `rtrv-assoc` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLES 31.10.0
ANAME swbel32
  PORT      A
  ADAPTER   M3UA          VER      M3UA RFC
  LHOST     ipnode1-1201
  ALHOST    ---
  RHOST     gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  LPORT     1030          RPORT    2345
  ISTRMS    2            OSTRMS   2
  RMODE     LIN           RMIN     120          RMAX     800
  RTIMES    10           CWMIN    3000
  OPEN      YES          ALW      YES

ANAME a2
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030          RPORT    2345
  ISTRMS    2            OSTRMS   2
  RMODE     LIN           RMIN     120          RMAX     800
  RTIMES    10           CWMIN    3000
  OPEN      YES          ALW      YES
```

```

ANAME a3
  PORT      A
  ADAPTER   SUA          VER          SUA RFC
  LHOST     gw106.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030         RPORT      2346
  ISTRMS    2           OSTRMS     2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES         ALW        YES
IP Appl Sock table is (3 of 4000) 1% full

```

2. Verify that the local host name to be assigned to the association is in the database by using the `rtrv-ip-host` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
```

```

IPADDR      HOST
192.1.1.10  IPNODE1-1201
192.1.1.12  IPNODE1-1203
192.1.1.14  IPNODE1-1205
192.1.1.20  IPNODE2-1201
192.1.1.22  IPNODE2-1203
192.1.1.24  IPNODE2-1205
192.1.1.30  KC-HLR1
192.1.1.32  KC-HLR2
192.1.1.50  DN-MS1
192.1.1.52  DN-MS2

```

```
IP Host table is (10 of 512) 2% full
```

If the required hostname is not in the database, add the IP host name using the “Adding an IP Host” on page 3-153 procedure.

3. Display the IP links in the database by entering the `rtrv-ip-lnk` command. The following is an example of the possible output.

```

rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
LOC  PORT  IPADDR      SUBMASK      DUPLEX  SPEED  MACTYPE  AUTO
1201  A     192.001.001.010  255.255.255.0  ----   ---   DIX      YES
1203  A     192.001.001.012  255.255.255.0  ----   ---   DIX      YES
1205  A     192.001.001.014  255.255.255.0  FULL   100   DIX      NO

```

If the required IP link is not in the database, add the IP link using the “Changing an IP Link” on page 3-158 procedure.

- Display the application running on the IP card shown in step 3 using the **rept-stat-card** command specifying the location of the IP card. For this example, enter this command.

```
rept-stat-card:loc=1203
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD VERSION      TYPE      APPL      PST      SST      AST
1203  114-000-000  DCM      IPLIM     IS-NR    Active   -----
  ALARM STATUS    = No Alarms.
  BPDCM GPL      = 002-102-000
  IMT BUS A      = Conn
  IMT BUS B      = Conn
  SLK A  PST     = IS-NR      LS=nc001  CLLI=-----
  SCCP TVG RESULT = 24 hr: -----, 5 min: -----
  SLAN TVG RESULT = 24 hr: -----, 5 min: -----
Command Completed.
```

NOTE: If the card's application is **SS7IPGW** or **IPGWI**, shown in the **APPL** column in the **rept-stat-card** output in step 4, skip steps 5, 6, 7, and 8, and go to step 9.

- Display the signaling link referenced by the IP link that will be assigned to the association by entering the **rtrv-slk** command and specifying the location and port of the IP link. For this example, enter this command.

```
rtrv-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-19 21:17:04 GMT EAGLE5 31.10.0
LOC  PORT LSN      SLC TYPE  IPLIML2
1203 A    e5e6a      1  IPLIM  M3UA
```

When the IP card's application is either **IPLIM** or **IPLIMI**, the **ipliml2** parameter value for the signaling link assigned to the association must be **m3ua** or **m2pa**, and must match the value of the **adapter** parameter specified in step 10. If the **ipliml2** parameter is not **m3ua** or **m2pa**, remove the signaling link using the "Removing an IP Signaling Link" procedure on page 3-115. Add the signaling link back into the database with either the **ipliml2=m3ua** or **ipliml2=m2pa** parameter, and without activating the signaling link, using the "Adding an IP Signaling Link" procedure on page 3-82.

NOTE: If the “Adding an IP Signaling Link” procedure on page 3-82 was not performed in step 5, skip steps 6, 7, and 8, and go to step 9.

6. Display the status of the signaling link shown in step 5 using the `rept-stat-slk` command specifying the card location and signaling link port. For example, enter this command.

```
rept-stat-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1203,A   e5e6a     -----  IS-NR    Avail    ----
Command Completed.
```

NOTE: If the primary state (PST) of the signaling link is `OOS-MT` and the secondary state (SST) is `Unavail`, skip steps 7 and 8, and go to step 9.

7. Deactivate the signaling link from step 6 using the `dact-slk` command. For example, enter this command.

```
dact-slk:loc=1203:port=a
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Deactivate Link message sent to card
```

8. Verify the status of the signaling link using the `rept-stat-slk` command. For example, enter this command.

```
rept-stat-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1203,A   e5e6a     -----  OOS-MT   Unavail  ----
Command Completed.
```

NOTE: If the `adapter=m2pa` parameter will not be specified with the `ent-assoc` command in step 10, skip step 9 and go to step 10.

9. Verify the values of the M2PA timer set you wish to assign to the association by entering the `rtrv-m2pa-tset` command. This is an example of the possible output.

NOTE: If the `m2patset` parameter will not be specified with the `ent-assoc` command, the M2PA timer set 1 will be assigned to the association.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

```
M2PA Timers (in msec)
```

TSET	T1	T3	T4N	T4E	T5	T6	T7	T16	T17	T18
1	10000	10000	10000	500	1000	3000	1200	200	250	1000
2	10000	10000	10000	500	1000	3000	1200	200	250	1000

```

3      10000 10000 10000 500 1000 3000 1200 200 250 1000
4      10000 10000 10000 500 1000 3000 1200 200 250 1000
5      10000 10000 10000 500 1000 3000 1200 200 250 1000
6      10000 10000 10000 500 1000 3000 1200 200 250 1000
7      10000 10000 10000 500 1000 3000 1200 200 250 1000
8      10000 10000 10000 500 1000 3000 1200 200 250 1000
9      10000 10000 10000 500 1000 3000 1200 200 250 1000
10     10000 10000 10000 500 1000 3000 1200 200 250 1000
11     10000 10000 10000 500 1000 3000 1200 200 250 1000
12     10000 10000 10000 500 1000 3000 1200 200 250 1000
13     10000 10000 10000 500 1000 3000 1200 200 250 1000
14     10000 10000 10000 500 1000 3000 1200 200 250 1000
15     10000 10000 10000 500 1000 3000 1200 200 250 1000
16     10000 10000 10000 500 1000 3000 1200 200 250 1000
17     10000 10000 10000 500 1000 3000 1200 200 250 1000
18     10000 10000 10000 500 1000 3000 1200 200 250 1000
19     10000 10000 10000 500 1000 3000 1200 200 250 1000
20     10000 10000 10000 500 1000 3000 1200 200 250 1000

```

If the M2PA timer set you wish to assign to the association does not contain the desired values, go to the “Changing an M2PA Timer Set” procedure on page 3-379 and changed the desired timer values.



CAUTION: Changing an M2PA timer set may affect the performance of any associations using the timer set being changed.

-
10. Add the association using the `ent-assoc` command. For this example, enter this command.

```
ent-assoc:aname=assoc1:lhost=gw105.nc.tekelec.com:lport=1030:
rhost=gw100.nc.tekelec.com:rport=1030:adapter=m3ua
```

NOTE: See Flowchart 3-32 on page 3-344 (Sheet 5) for the rules that apply to the `ent-assoc` command.

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ENT-ASSOC: MASP A - COMPLTD
```

NOTE: If the association added in step 9 is not being activated in this procedure, skip step 10 and go to step 11.

11. Activate the association added in step 9 by entering the `chg-assoc` command with the association name specified in step 9 and the `open=yes` and `alw=yes` parameters. For example, enter this command.

```
chg-assoc:aname=assoc1:open=yes:alw=yes
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD
```

NOTE: If the card's application is SS7IPGW or IPGWI, skip steps 11 and 12, and go to step 13.

- 12 Activate the signaling link assigned to the association using the **act-slk** command. For example, enter this command.

```
act-slk:loc=1203:port=a
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Activate Link message sent to card
```

13. Verify the status of the signaling link using the **rept-stat-slk** command. For example, enter this command.

```
rept-stat-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1203,A   e5e6a     -----  IS-NR    Avail    ----
Command Completed.
```

14. Verify the changes using the **rtrv-assoc** command specifying the association name specified in step 9. For this example, enter this command.

```
rtrv-assoc:aname=assoc1
```

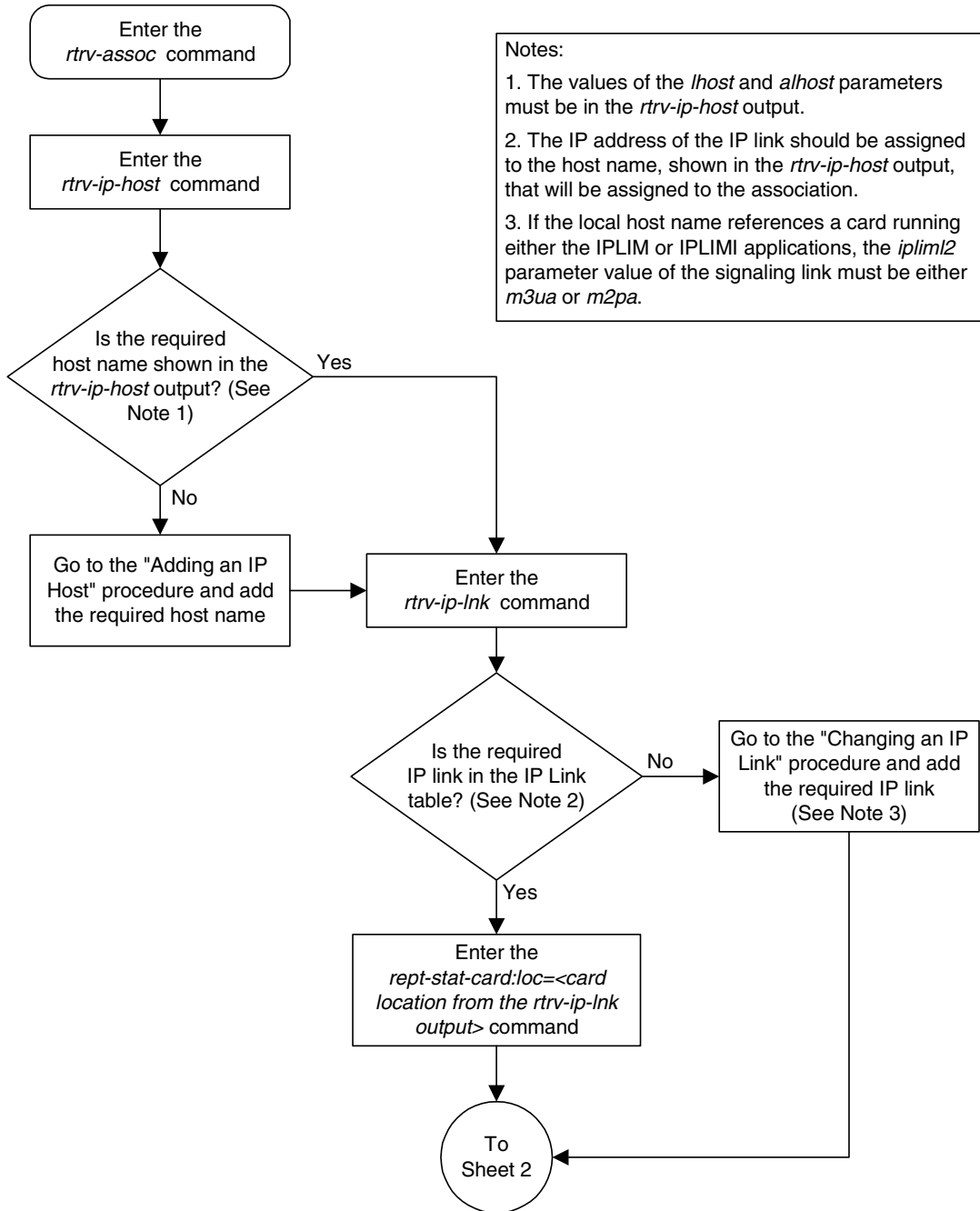
This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc1
PORT      A
ADAPTER   M3UA      VER        M3UA RFC
LHOST     gw105.nc.tekelec.com
ALHOST    ---
RHOST     gw100.nc.tekelec.com
LPORT     1030      RPORT      1030
ISTRMS    2          OSTRMS     2
RMODE     LIN        RMIN       120        RMAX       800
RTIMES    10        CWMIN      3000
OPEN      NO         ALW        NO
IP Appl Sock table is (4 of 4000) 1% full
```

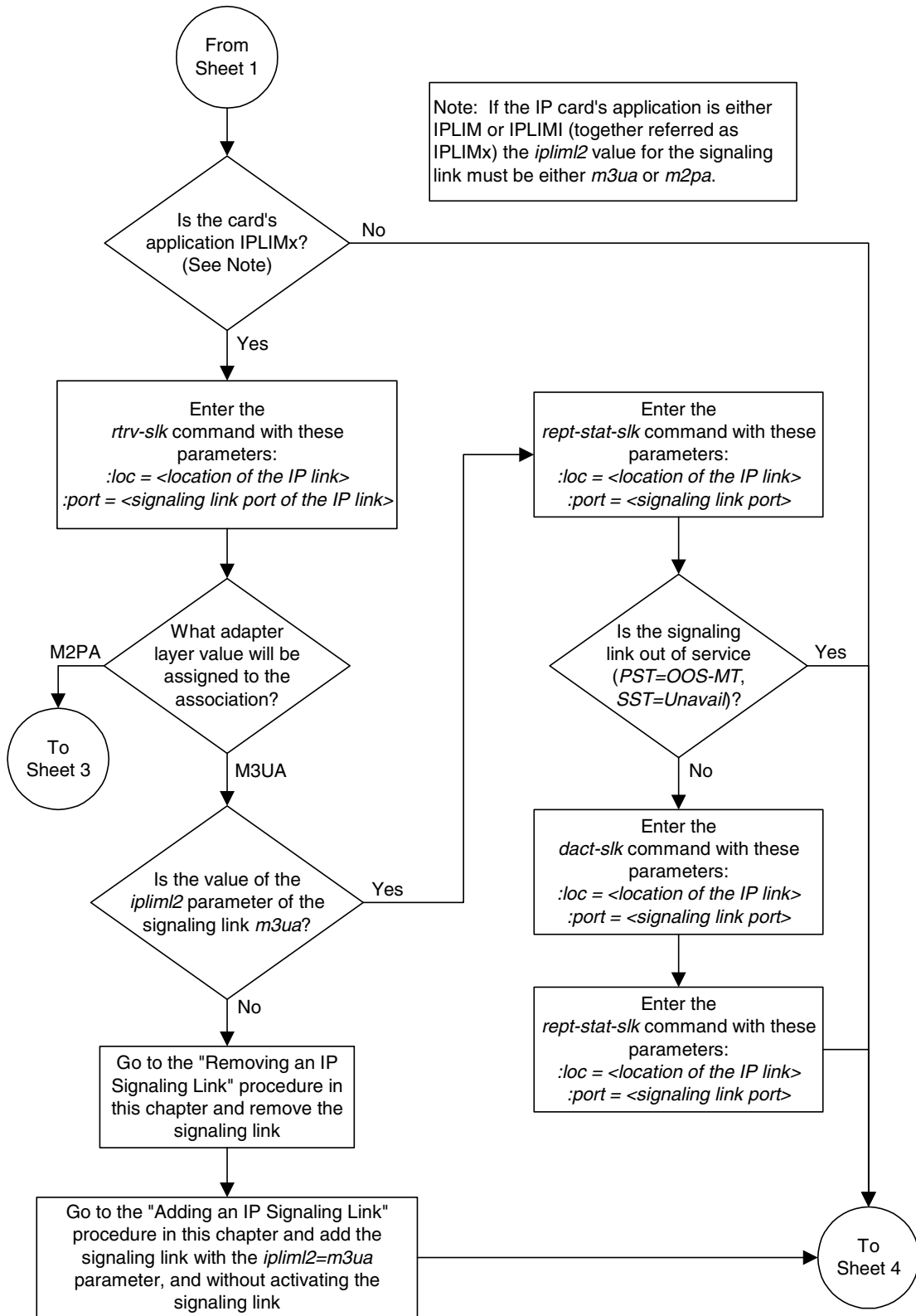
15. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

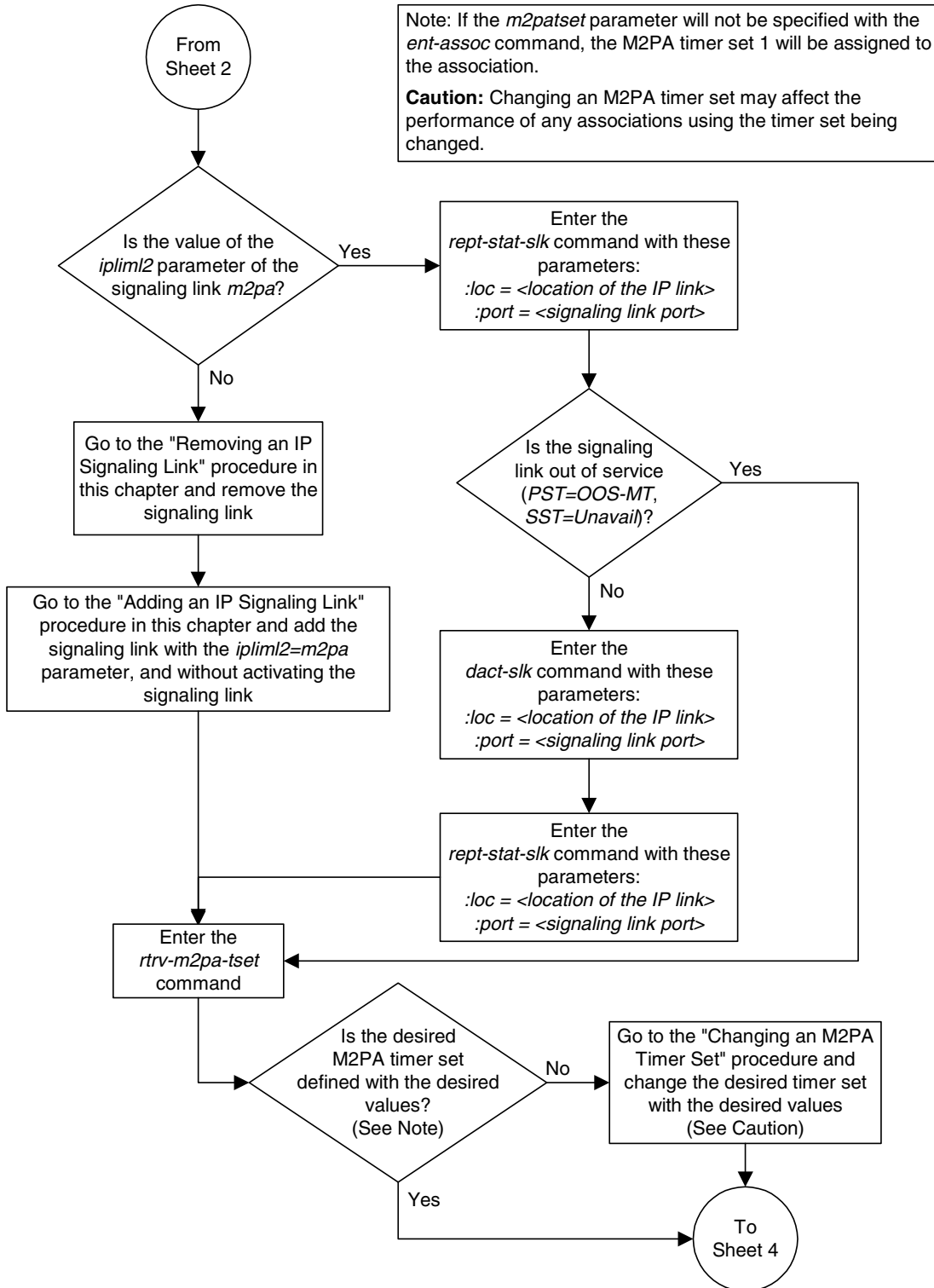
Flowchart 3-32. Adding an Association (Sheet 1 of 5)



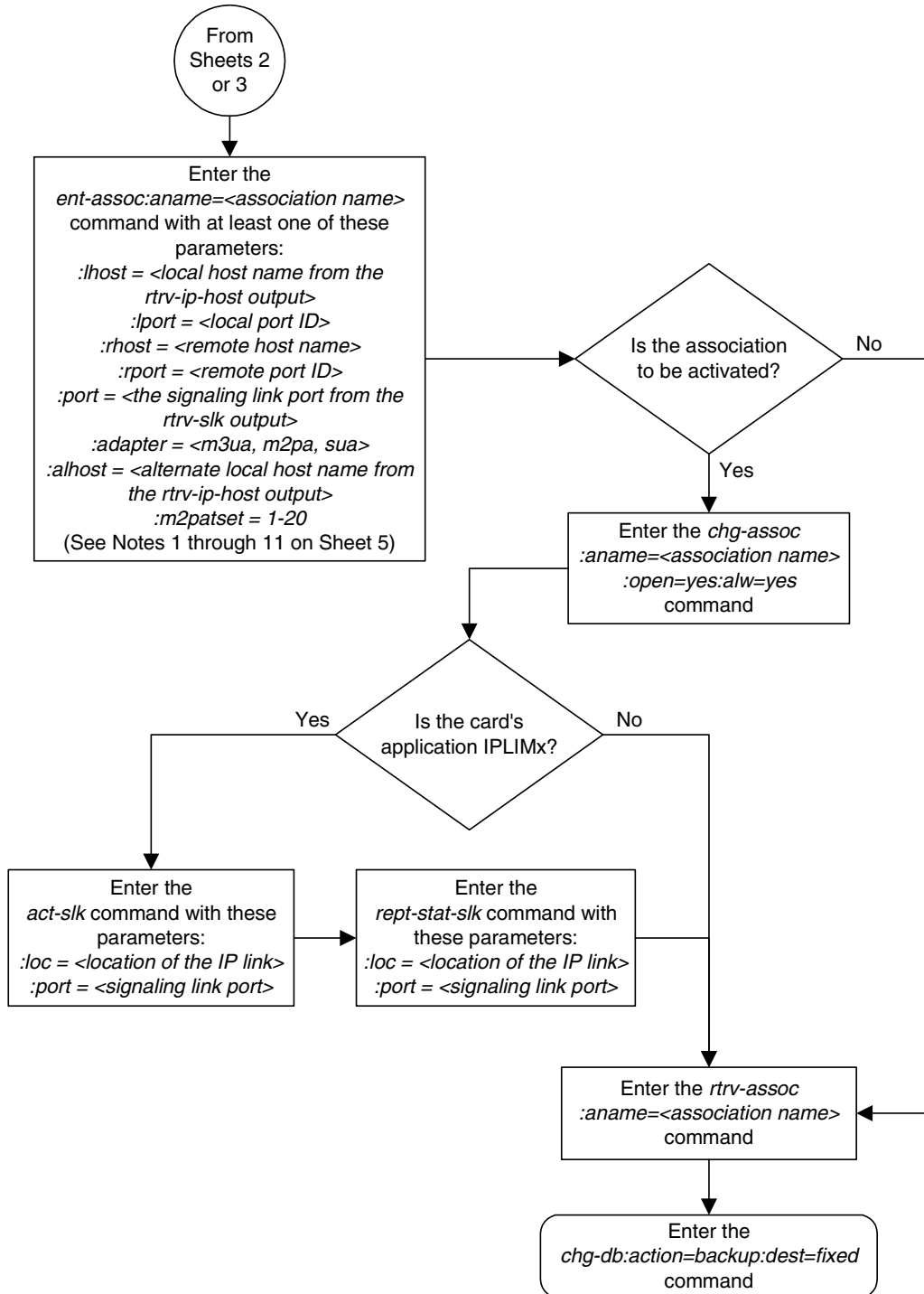
Flowchart 3-32. Adding an Association (Sheet 2 of 5)



Flowchart 3-32. Adding an Association (Sheet 3 of 5)



Flowchart 3-32. Adding an Association (Sheet 4 of 5)



Flowchart 3-32. Adding an Association (Sheet 5 of 5)

Notes:

1. If the card containing the signaling link is a DCM, the B Ethernet interface cannot be used. Single-slot EDCMs can use the B Ethernet interface.
2. If the card's application is either *iplim* or *iplimi*, the *adapter* parameter value must be either *m3ua* or *m2pa*. The value of the *adapter* parameter must match the value of the *ipliml2* parameter of the signaling link being assigned to the association. For example, if the value of the signaling link's *ipliml2* parameter is *m3ua*, then the *adapter=m3ua* parameter must be specified for the association. If the value of the signaling link's *ipliml2* parameter is *m2pa*, then the *adapter=m2pa* parameter must be specified for the association.
3. Each local host on a card running either the *ss7ipgw* or *ipgwi* applications can contain a maximum of 50 connections (associations plus sockets).
4. The system can contain a maximum of 4000 connections (associations plus sockets).
5. Cards running either the *iplim* or *iplimi* applications can have only one connection for each signaling link port and a maximum of two connections for each card, if the card is a dual-slot DCM. If the card is a single-slot EDCM, the card may contain a maximum of eight connections.
6. The value of the *lhost*, *rhost*, or *alhost* parameters is a text string of up to 60 characters, with the first character being a letter. The command line on the terminal can contain up to 150 characters. If the host names are too long to fit on the *ent-assoc* command line, go to the "Changing an Association" procedure in this chapter to complete the entry of the host names.
7. If the new association is to be activated in this procedure with the *chg-assoc* command, the association must contain values for the *lhost*, *rhost*, *lport*, and *rport* parameters.
8. If the *lhost* and *alhost* are specified, the *lhost* parameter value represents the IP address corresponding to one of the network interfaces (A or B) on the IP card while the *alhost* parameter value represents the IP address corresponding to the other network interface of the same IP card.
9. Card's running either *ss7ipgw* or *ipgwi* applications can have only the values *m3ua* or *sua* for the *adapter* parameter.
10. The default value for the *adapter* parameter is *m3ua*.
11. The *m2patset* parameter can be specified only with the *adapter=m2pa* parameter.
12. The *m2patset* parameter value defaults to M2PA timer set 1 (*m2patset=1*) if the *m2patset* parameter is not specified.

Removing an Association

This procedure is used to remove an association from the database using the `dlt-assoc` command.

The `dlt-assoc` command uses one parameter, `aname`, the name of the association being removed from the database. The association being removed must be in the database.

The `open` parameter must be set to `no` before the association can be removed. Use the `chg-assoc` command to change the value of the `open` parameter.

The association being removed from the database cannot be assigned to an ASP. This can be verified with the `rtrv-asp` command. If the association has an ASP assigned to it, go to the "Removing an Application Server Process" procedure on page 3-387 and remove the ASP assignment to the association.

Canceling the RTRV-ASSOC and RTRV-ASP Commands

Because the `rtrv-assoc` and `rtrv-asp` commands used in this procedure can output information for a long period of time, the `rtrv-assoc` and `rtrv-asp` commands can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-assoc` and `rtrv-asp` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-assoc` or `rtrv-asp` commands were entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-assoc` or `rtrv-asp` commands were entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-assoc` or `rtrv-asp` commands were entered, from another terminal other than the terminal where the `rtrv-assoc` or `rtrv-asp` commands were entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the associations in the database using the `rtrv-assoc` command. This is an example of possible output.

```

rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME swbel32
  PORT      A
  ADAPTER   M3UA          VER      M3UA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  LPORT     1030          RPORT     2345
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES         ALW       YES

ANAME a2
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030          RPORT     2345
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES         ALW       YES

ANAME a3
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw106.nc.tekelec.com
  LPORT     1030          RPORT     2346
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES         ALW       YES

ANAME assoc1
  PORT      A
  ADAPTER   M3UA          VER      M3UA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030          RPORT     1030
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES         ALW       YES
IP Appl Sock table is (4 of 4000) 1% full

```

2. Display the ASPs referencing the association being removed from the database using the `rtrv-asp` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP          ASSOCIATION          UAPS
asp1        swbe132          1
asp2        a2                1
asp3        a3                1
asp4        assoc1         10
```

ASP Table is (4 of 4000) 1% full

If the association is assigned to an ASP, go to the “Removing an Application Server Process” procedure on page 3-387 and remove the ASP from the database.

NOTE: If the value of the `open` parameter for the association being removed from the database (shown in step 1) is `no`, skip this step and go to step 4.

3. Change the value of the `open` parameter to `no` by specifying the `chg-assoc` command with the `open=no` parameter. For this example, enter this command.

chg-assoc:aname=assoc1:open=no

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

4. Remove the association from the database using the `dlt-assoc` command. For this example, enter this command.

dlt-assoc:aname=assoc1

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
DLT-ASSOC: MASP A - COMPLTD
```

5. Verify the changes using the **rtrv-assoc** command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME swbel32
  PORT      A
  ADAPTER   M3UA          VER      M3UA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  LPORT     1030          RPORT    2345
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES         ALW       YES

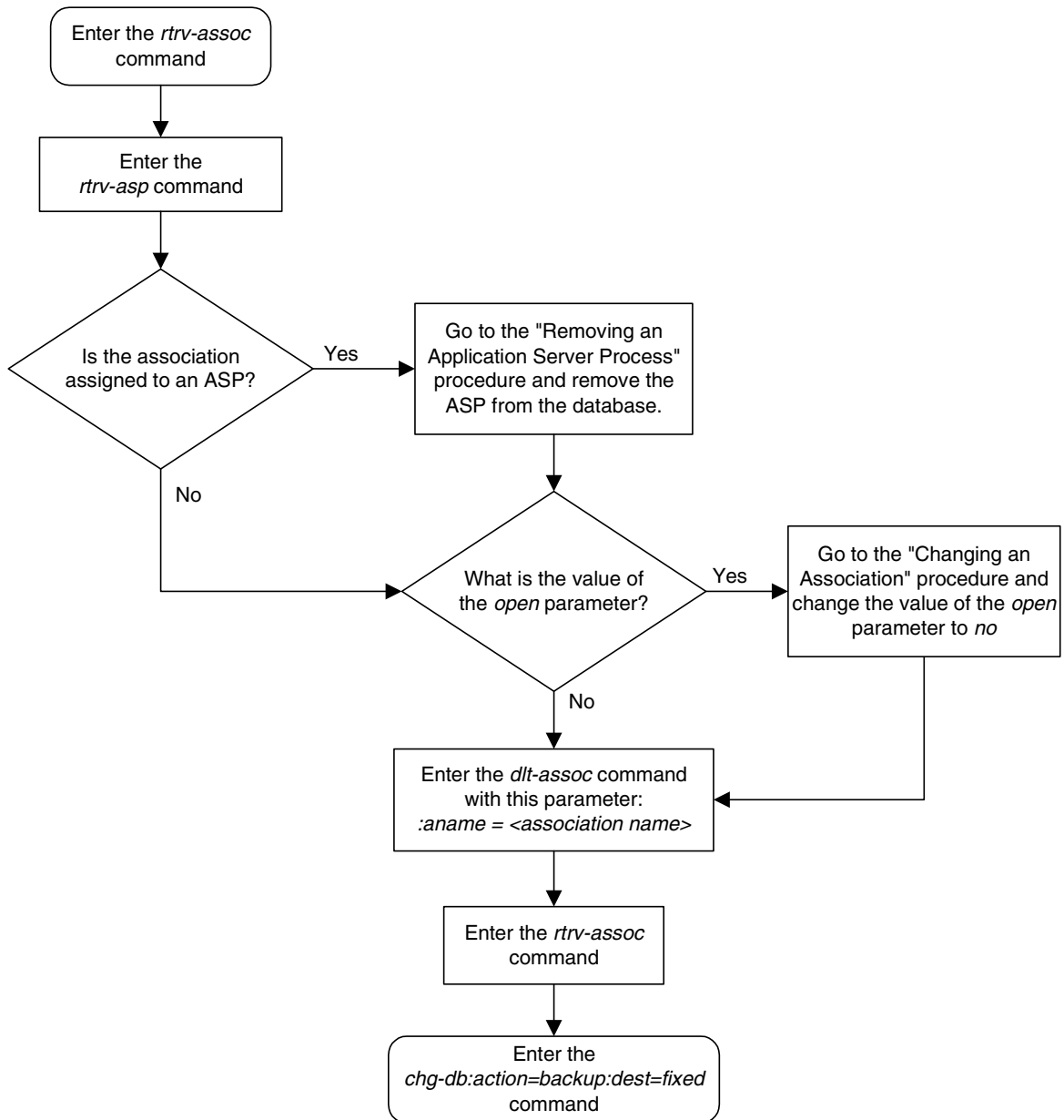
ANAME a2
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030          RPORT    2345
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES         ALW       YES

ANAME a3
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw106.nc.tekelec.com
  LPORT     1030          RPORT    2346
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES         ALW       YES
IP Appl Sock table is (3 of 4000) 1% full
```

6. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-33. Removing an Association



Changing an Association

This procedure is used to change the values of the attributes of the SCTP associations in the database using the **chg-assoc** command.

The **chg-assoc** command uses these parameters:

- :aname** – The name assigned to the association. Valid association names can contain up to 15 alphanumeric characters where the first character is a letter and the remaining characters are alphanumeric characters. The **aname** parameter value is not case-sensitive.
- :lhost** – The host name for the local host, **lhost** can be any string of characters starting with a letter and comprising these characters ['a'..'z', 'A'..'Z', '0'..'9', '-', '.']. Hostnames are not case-sensitive and can contain up to 60 characters. The default value of this optional parameter is empty (null string).
- :lport** – The SCTP port number for the local host.
- :rhost** – The host name for the remote host, **rhost** can be any string of characters starting with a letter and comprising these characters ['a'..'z', 'A'..'Z', '0'..'9', '-', '.']. Hostnames are not case-sensitive and can contain up to 60 characters. The default value of this optional parameter is empty (null string).
- :rport** – The SCTP port number for the remote host.
- :port** – The signaling link port on the IP card. If the card's application is **iplim** or **iplimi**, and the card is a dual-slot DCM, the values for the **port** parameter can be only **a** or **b**. If the card's application is **iplim** or **iplimi**, and the card is a single-slot EDCM, the values for the **port** parameter can be **a**, **a1**, **a2**, **a3**, **b**, **b1**, **b2**, or **b3**. If the IP card's application is **ss7ipgw** or **ipgwi**, only **port=a** can be specified.
- :adapter** – The adapter layer for this association, either **m3ua**, **m2pa**, or **sua**.
- :open** – The connection state for this association. Valid values are **yes** or **no**. When the **open=yes** parameter is specified, the connection manager opens the association if the association is operational. When the **open=no** parameter is specified, the connection manager will not open the association.
- :alw** – The connection state for this association. Valid values are **yes** or **no**. When the **alw=yes** parameter is specified, the connection manager allows the association to carry SS7 traffic. When the **alw=no** parameter is specified, the connection manager prohibits the association from carrying SS7 traffic.
- :rmode** – The retransmission policy used when packet loss is detected. The values are **rfc** or **lin**.
 - **rfc** – Standard RFC 2960 algorithm in the retransmission delay doubles after each retransmission. The RFC 2960 standard for congestion control is also used.

- **lin** – Tekelec's linear retransmission policy where each retransmission timeout value is the same as the initial transmission timeout and only the slow start algorithm is used for congestion control.

:rmin – The minimum value of the calculated retransmission timeout in milliseconds, from 10 - 1000.

:rmax – The maximum value of the calculated retransmission timeout in milliseconds, from 10 - 1000.

:rtimes – The number of times a data retransmission will occur before closing the association from 3 - 12.

:cwmn – The minimum size in bytes of the association's congestion window and the initial size in bytes of the congestion window, from 1500 - 196608.

The **rmode**, **rmin**, **rmax**, **rtimes**, and **cwmn** parameters are used to configure the SCTP retransmission controls for an association, in addition to other commands. Go to the "Configuring SCTP Retransmission Control for an Association" procedure on page 3-370 to configure the SCTP retransmission controls for an association.

:ver – The version of M3UA that should be used with this association. The values for this parameter are either **db** (for the draft 8 version) or **rfc** (for the RFC version).

:istrms – The number of inbound streams (1 or 2) advertised by the SCTP layer for the association.

:ostrms – The number of outbound streams (1 or 2) advertised by the SCTP layer for the association.

:m2patset – The M2PA timer set assigned to the association. The **m2patset** parameter can be specified only with the **adaper=m2pa** parameter, or if the association already has the **adapter=m2pa** parameter assigned and the **adapter** parameter value is not being changed. If the **adapter** parameter value is being changed to **m2pa**, and the **m2patset** parameter is not specified, the default value for the **m2patset** parameter (1 - M2PA timer set 1) is assigned to the association. If the **adapter** parameter value for the association is **m2pa**, is not being changed, and the **m2patset** parameter is not specified with the **chg-assoc** command, the **m2patset** parameter value is not changed.

If the value of the **open** parameter is **yes**, only the value of the **alw** parameter can be changed. To change the values of other parameters, the value of the **open** parameter must be **no**.

To set the **open** parameter value to **yes**, the association specified by the **aname** parameter must contain values for the **lhost**, **lport**, **rhost**, and **rport** parameters. The **lhost** parameter value must have a signaling link assigned to it.

At least one optional parameter is required.

The command input is limited to 150 characters, including the hostnames.

Each local host on a card running either the **ss7ipgw** or **ipgwi** applications can contain a maximum of 50 connections (associations plus sockets).

The system can contain a maximum of 4000 connections (associations plus sockets).

For the **iplim** and **iplimi** applications, the IP card can one association for each signaling link on the card. The dual-slot DCM can contain only two signaling links, resulting in a maximum of two associations on these cards. The single-slot EDCM can contain a maximum of eight signaling links, resulting in a maximum of eight associations for this card.

The B Ethernet interface of the IP card can be used only if the IP card is a single-slot EDCM.

The adapter parameter value cannot be changed if the association is assigned to an ASP. This can be verified with the **rtrv-asp** command. If the association has an ASP assigned to it, go to the “Removing an Application Server Process” procedure on page 3-387 and remove the ASP assignment to the association.

The value of the **rmin** parameter must be less than or equal to the **rmax** parameter value.

For associations assigned to the **ss7ipgw** or **ipgwi** applications, the value of the **cwmin** parameter must be less than or equal to 16384.

If the card’s application is either IPLIM or IPLIMI:

- The **iplim12** parameter value of the signaling link assigned to the association must be **m3ua** or **m2pa**. The **adapter** parameter value of the association must match the **iplim12** parameter value.
- The signaling link being assigned to the association must be out of service. This state is shown in the **rept-stat-slk** output with the entries **OOS-MT** in the **PST** field and **Unavail** in the **SST** field.
- If the association is being opened in this procedure with the **chg-assoc** command and the **open=yes** parameter, the signaling link assigned to the association must be in the database and the **iplim12** parameter value of the signaling link assigned to the association must be **m3ua** or **m2pa**.

If the card’s application is either SS7IPGW or IPGWI, the signaling link being assigned to the association must be in service. This state is shown in the **rept-stat-slk** output with the entries **IS-NR** in the **PST** field and **Avail** in the **SST** field.

Uni-homed endpoints are associations configured with the **lhost** parameter only. The **lhost** parameter value represents an IP address that corresponds to either the A or B network interface of the IP card. Multi-homed endpoints are associations configured with both the **lhost** and **alhost** parameters. The **lhost** parameter value represents an IP address corresponding to one of the network interfaces (A or B) of the IP card while the **alhost** parameter value represents an IP address corresponding to the other network interface of the same IP card.

The `ver` parameter cannot be specified for SUA or M2PA connections.

The `alhost=none` parameter removes the alternate local host from the specified association, which also removes the multi-homed endpoint capability.

Canceling the RTRV-ASSOC and RTRV-ASP Commands

Because the `rtrv-assoc` and `rtrv-asp` commands used in this procedure can output information for a long period of time, the `rtrv-assoc` and `rtrv-asp` commands can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-assoc` and `rtrv-asp` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-assoc` or `rtrv-asp` commands were entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-assoc` or `rtrv-asp` commands were entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-assoc` or `rtrv-asp` commands were entered, from another terminal other than the terminal where the `rtrv-assoc` or `rtrv-asp` commands were entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the associations in the database using the `rtrv-assoc` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME swbel32
      PORT      A
ADAPTER  M3UA          VER      M3UA RFC
LHOST    gw105.nc.tekelec.com
ALHOST   ---
RHOST    gw100.ncd-economic-development.southeastern-cooridor-ash.gov
LPORTR   1030          RPORT   2345
ISTRMS   2           OSTRMS   2
RMODE    LIN          RMIN     120          RMAX     800
RTIMES   10          CWMIN    3000
OPEN     YES          ALW      YES
```

```

ANAME a2
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030         RPORT    2345
  ISTRMS    2           OSTRMS   2
  RMODE     LIN          RMIN     120          RMAX     800
  RTIMES    10          CWMIN    3000
  OPEN      YES         ALW      YES

ANAME a3
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw106.nc.tekelec.com
  LPORT     1030         RPORT    2346
  ISTRMS    2           OSTRMS   2
  RMODE     LIN          RMIN     120          RMAX     800
  RTIMES    10          CWMIN    3000
  OPEN      YES         ALW      YES

ANAME assoc1
  PORT      A
  ADAPTER   M3UA         VER      M3UA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030         RPORT    1030
  ISTRMS    2           OSTRMS   2
  RMODE     LIN          RMIN     120          RMAX     800
  RTIMES    10          CWMIN    3000
  OPEN      YES         ALW      YES
IP Appl Sock table is (4 of 4000) 1% full

```

NOTE: To change the values of these parameters: `lhost`, `lport`, `rhost`, `rport`, `port`, `adapter`, `rmode`, `rmin`, `rmax`, `rtimes`, `cwmin`, `ver`, `istrms`, or `ostrms`, the value of the `open` parameter must be `no`. If the values of any of these parameters are being changed and the `open` parameter value for the association being changed is `no`, skip this step and go to step 3.

NOTE: If only the values of the `alw` or `open` parameters are being changed, skip steps 2 through 10, and go to step 11.

2. Change the value of the `open` parameter to `no` by specifying the `chg-assoc` command with the `open=no` parameter. For this example, enter this command.

```
chg-assoc:aname=assoc1:open=no
```

When this command has successfully completed, this message should appear.

```

rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;

```

NOTE: If the local host name assigned to the association is not being changed, skip this step and step 4 and go to step 5.

3. Verify that the local host name to be assigned to the association is in the database by using the `rtrv-ip-host` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
```

IPADDR	HOST
192.1.1.10	IPNODE1-1201
192.1.1.12	IPNODE1-1203
192.1.1.14	IPNODE1-1205
192.1.1.20	IPNODE2-1201
192.1.1.22	IPNODE2-1203
192.1.1.24	IPNODE2-1205
192.1.1.30	KC-HLR1
192.1.1.32	KC-HLR2
192.1.1.50	DN-MS1
192.1.1.52	DN-MS2

```
IP Host table is (10 of 512) 2% full
```

If the required hostname is not in the database, add the IP host name using the “Adding an IP Host” on page 3-153 procedure.

4. Display the IP links in the database by entering the `rtrv-ip-lnk` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
```

LOC	PORT	IPADDR	SUBMASK	DUPLEX	SPEED	MACTYPE	AUTO
1201	A	192.001.001.010	255.255.255.0	----	---	DIX	YES
1203	A	192.001.001.012	255.255.255.0	----	---	DIX	YES
1205	A	192.001.001.014	255.255.255.0	FULL	100	DIX	NO

If the required IP link, one references the local host shown or added in step 3, is not in the database, add the IP link using the “Changing an IP Link” on page 3-158 procedure.

NOTE: If the `port` parameter value is not being changed, skip this step and go to step 5.

5. Display the signaling link associated with the association being changed using the `rtrv-slk` command and specifying the card location shown in step 4, and the new `port` parameter value for the association. The card location should reference the local host assigned to the association. The `rtrv-ip-lnk` output shows the card location associated with the IP address that is associated with the local host in step 3. If the `rtrv-ip-lnk` command was not executed in step 4, execute it now to get the card location and the IP address. To display the signaling link for this example, enter this command.

```
rtrv-slk:loc=1203:port=a
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-19 21:17:04 GMT EAGLE5 31.10.0
LOC  PORT LSN          SLC TYPE   IPLIML2
1203 A    e5e6a          1  IPLIM    M3UA
```

If the required signaling link is not in the database, add the signaling link using the “Adding an IP Signaling Link” procedure on page 3-82 without activating the signaling link. If the application of the card containing the signaling link is IPLIM or IPLIMI, the `ipliml2=m3ua` or `ipliml2=m2pa` parameter must be specified for the signaling link. The value of the `ipliml2` parameter must be the same as the association’s `adapter` parameter.

NOTE: If the `adapter` parameter value is not being changed, skip this step and go to step 7.

6. Display the ASPs referencing the association being removed from the database using the `rtrv-asp` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP          ASSOCIATION          UAPS
asp1        swbel32              1
asp2        a2                   1
asp3        a3                   1
asp4        assoc1               10
```

```
ASP Table is (4 of 4000) 1% full
```

If the association is assigned to an ASP, go to the “Removing an Application Server Process” procedure on page 3-387 and remove the ASP from the database.

7. Display the application running on the IP card shown in step 4 using the **rept-stat-card** command specifying the location of the IP card. For this example, enter this command.

```
rept-stat-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD VERSION      TYPE  APPL    PST          SST          AST
1201 114-000-000  DCM   IPLIM    IS-NR        Active       -----
  ALARM STATUS    = No Alarms.
  BPDCM GPL       = 002-102-000
  IMT BUS A      = Conn
  IMT BUS B      = Conn
  SLK A  PST      = IS-NR          LS=nc001  CLLI=-----
  SCCP TVG RESULT = 24 hr: -----, 5 min: -----
  SLAN TVG RESULT = 24 hr: -----, 5 min: -----
Command Completed.
```

NOTE: If the card's application is SS7IPGW or IPGWI, shown in the **APPL** column in the **rept-stat-card** output in step 7, or if a new signaling link was added in step 5, skip steps 8, 9, 10, and 11, and go to step 12.

8. Display the signaling link that will be assigned to the association by entering the **rtrv-slk** command and specifying the location and port of the signaling link. For this example, enter this command.

```
rtrv-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-19 21:17:04 GMT EAGLE5 31.10.0
LOC  PORT LSN          SLC TYPE  IPLIML2
1203 A  e5e6a             1  IPLIM    M3UA
```

When the IP card's application is either IPLIM or IPLIMI, the **iplim12** parameter value for the signaling link assigned to the association must be **m3ua** or **m2pa**. If the **iplim12** parameter is not **m3ua** or **m2pa**, remove the signaling link using the "Removing an IP Signaling Link" procedure on page 3-115. Add the signaling link back into the database with either the **iplim12=m3ua** or **iplim12=m2pa** parameter, and without activating the signaling link, using the "Adding an IP Signaling Link" procedure on page 3-82.

NOTE: If the “Adding an IP Signaling Link” procedure on page 3-82 was not performed in step 8, skip steps 9, 10, and 11, and go to step 12.

9. Display the status of the signaling link shown in step 8 using the `rept-stat-slk` command specifying the card location and signaling link port. For example, enter this command.

```
rept-stat-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1203,A  e5e6a      -----  IS-NR    Avail    ----
Command Completed.
```

NOTE: If the primary state (PST) of the signaling link is `oos-MT` and the secondary state (SST) is `Unavail`, skip steps 10 and 11, and go to step 12.

- 10 Deactivate the signaling link from step 9 using the `dact-slk` command. For example, enter this command.

```
dact-slk:loc=1203:port=a
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Deactivate Link message sent to card
```

11. Verify the status of the signaling link using the `rept-stat-slk` command. For example, enter this command.

```
rept-stat-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1203,A  e5e6a      -----  OOS-MT   Unavail  ----
Command Completed.
```

NOTE: If the `adapter=m2pa` parameter will not be specified with the `chg-assoc` command in step 13, or if the current value of the `adapter` parameter is not `m2pa`, skip step 12 and go to step 13.

12. Verify the values of the M2PA timer set you wish to assign to the association by entering the `rtrv-m2pa-tset` command. This is an example of the possible output.

NOTE: If the `m2patset` parameter will not be specified with the `chg-assoc` command, and the `adapter` parameter value is being changed to `m2pa`, the M2PA timer set 1 will be assigned to the association.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

M2PA Timers (in msec)

TSET	T1	T3	T4N	T4E	T5	T6	T7	T16	T17	T18
1	10000	10000	10000	500	1000	3000	1200	200	250	1000
2	10000	10000	10000	500	1000	3000	1200	200	250	1000
3	10000	10000	10000	500	1000	3000	1200	200	250	1000
4	10000	10000	10000	500	1000	3000	1200	200	250	1000
5	10000	10000	10000	500	1000	3000	1200	200	250	1000
6	10000	10000	10000	500	1000	3000	1200	200	250	1000
7	10000	10000	10000	500	1000	3000	1200	200	250	1000
8	10000	10000	10000	500	1000	3000	1200	200	250	1000
9	10000	10000	10000	500	1000	3000	1200	200	250	1000
10	10000	10000	10000	500	1000	3000	1200	200	250	1000
11	10000	10000	10000	500	1000	3000	1200	200	250	1000
12	10000	10000	10000	500	1000	3000	1200	200	250	1000
13	10000	10000	10000	500	1000	3000	1200	200	250	1000
14	10000	10000	10000	500	1000	3000	1200	200	250	1000
15	10000	10000	10000	500	1000	3000	1200	200	250	1000
16	10000	10000	10000	500	1000	3000	1200	200	250	1000
17	10000	10000	10000	500	1000	3000	1200	200	250	1000
18	10000	10000	10000	500	1000	3000	1200	200	250	1000
19	10000	10000	10000	500	1000	3000	1200	200	250	1000
20	10000	10000	10000	500	1000	3000	1200	200	250	1000

If the M2PA timer set you wish to assign to the association does not contain the desired values, go to the "Changing an M2PA Timer Set" procedure on page 3-379 and changed the desired timer values.



CAUTION: Changing an M2PA timer set may affect the performance of any associations using the timer set being changed.

13. Change the association using the `chg-assoc` command. For this example, enter this command.

```
chg-assoc:aname=assoc1:rhost=gw200.nc-tekelec.com:rport=2048
```

NOTE: See Flowchart 3-34 on page 3-369 (Sheet 9) for the rules that apply to the `chg-assoc` command.

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

NOTE: If the value of the **open** parameter was not changed in step 2, skip this step and go to step 15.

14. Change the value of the **open** parameter to **yes** by specifying the **chg-assoc** command with the **open=yes** parameter. For this example, enter this command.

```
chg-assoc:aname=assoc1:open=yes
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

NOTE: If the card's application is **SS7IPGW** or **IPGWI**, skip steps 15 and 16, and go to step 17.

15. Activate the signaling link assigned to the association using the **act-slk** command. For example, enter this command.

```
act-slk:loc=1203:port=a
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Activate Link message sent to card
```

16. Verify the status of the signaling link using the **rept-stat-slk** command. For example, enter this command.

```
rept-stat-slk:loc=1203:port=a
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1203,A   e5e6a      -----  IS-NR      Avail     ----
Command Completed.
```

17. Verify the changes using the **rtrv-assoc** command specifying the association name specified in step 13. For this example, enter this command.

```
rtrv-assoc:aname=assoc1
```

This is an example of possible output.

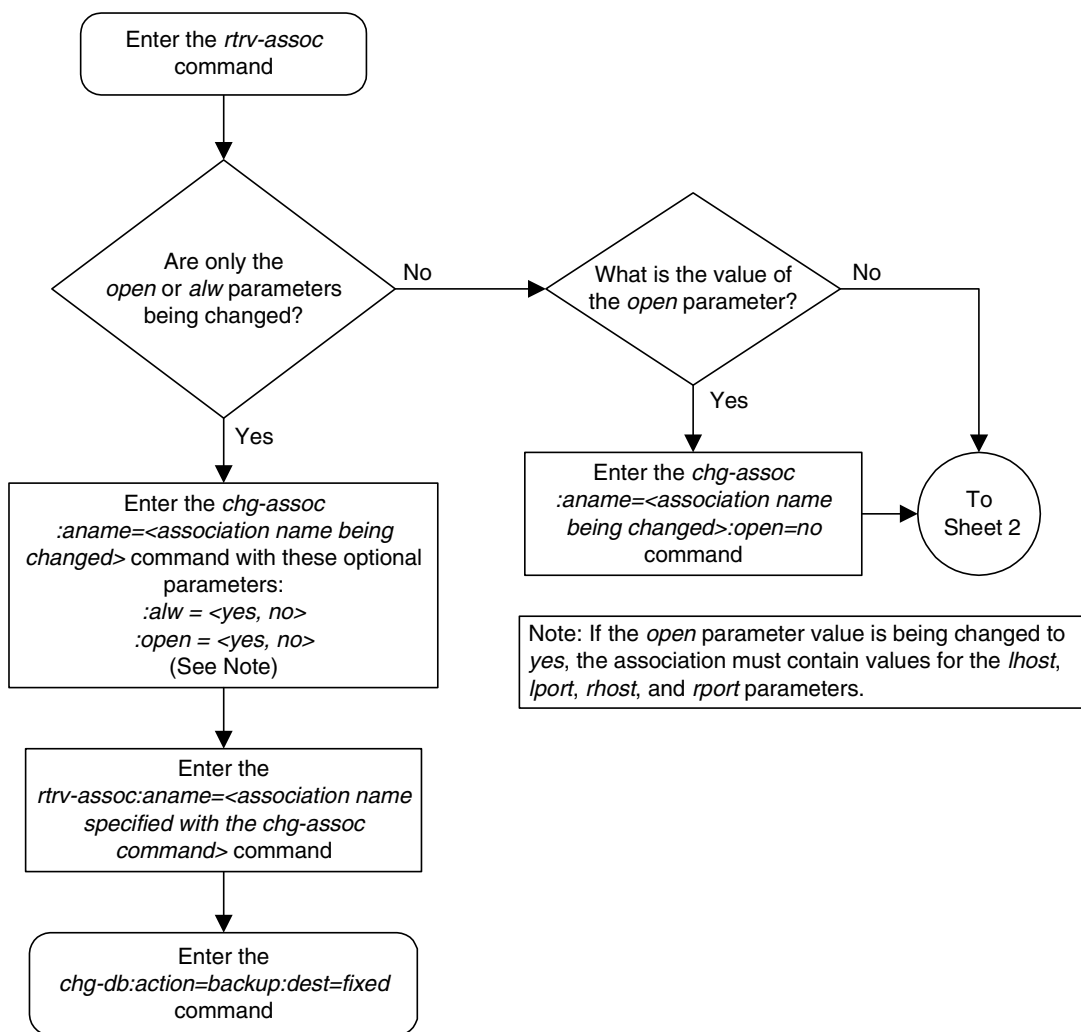
```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc1
  PORT      A
  ADAPTER   M3UA      VER      M3UA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw200.nc.tekelec.com
  LPORT     1030      RPORT    2048
  ISTRMS    2          OSTRMS   2
  RMODE     LIN        RMIN     120      RMAX     800
  RTIMES    10        CWMIN    3000
  OPEN      NO         ALW      NO
IP Appl Sock table is (4 of 4000) 1% full
```

18. Back up the new changes, using the `chg-db:action=backup:dest=fixed` command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

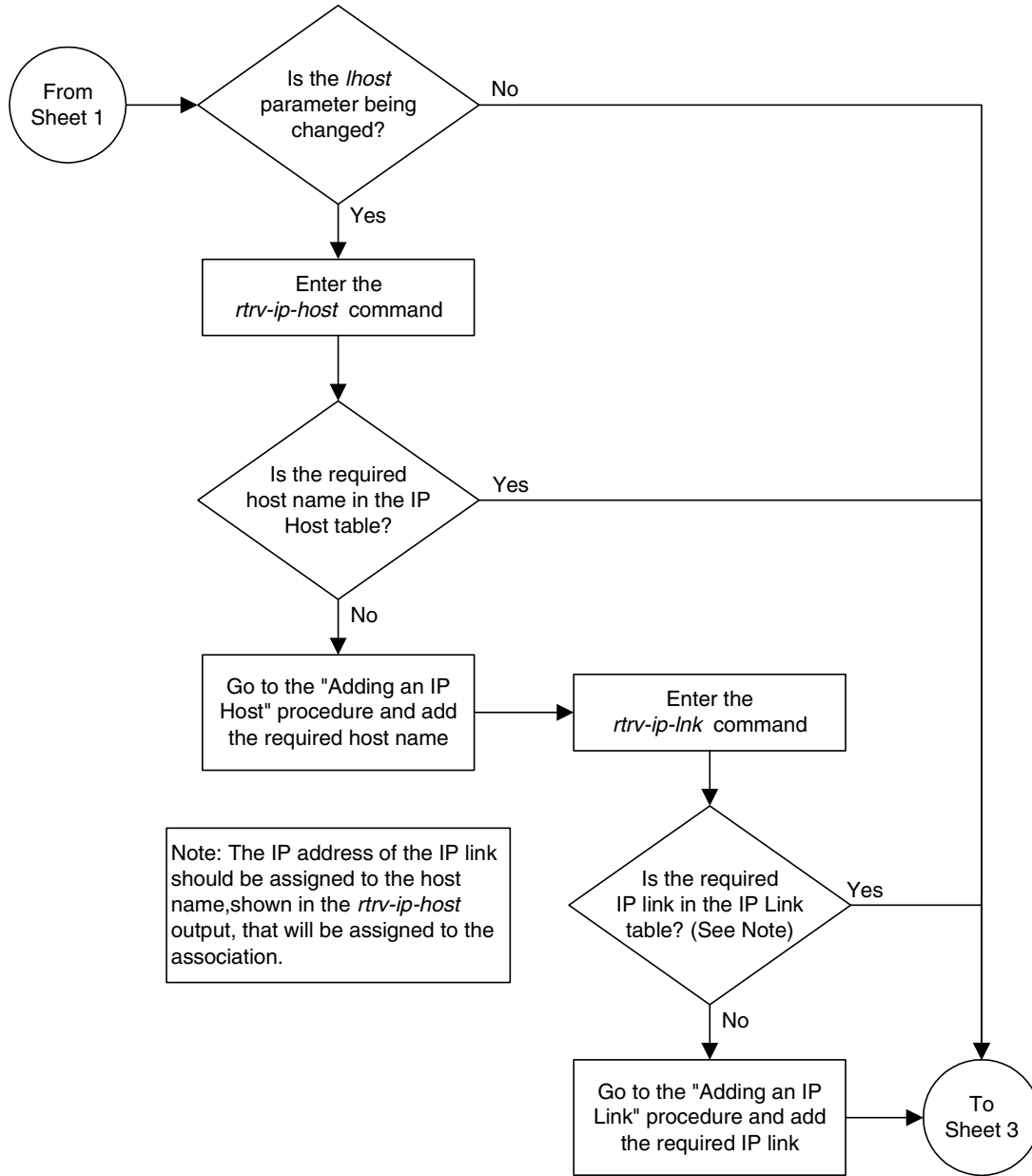
```

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

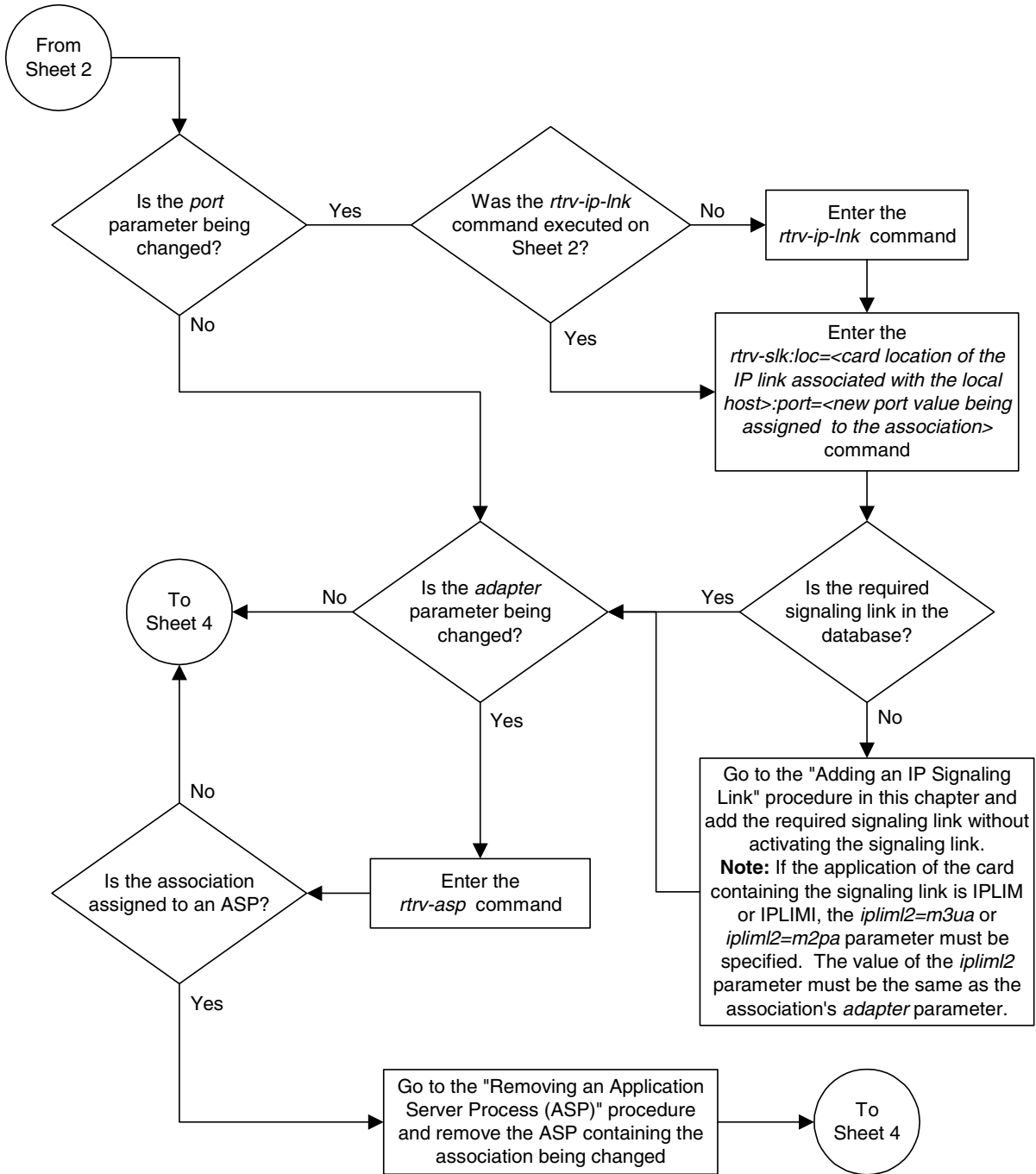
Flowchart 3-34. Changing an Association (Sheet 1 of 9)



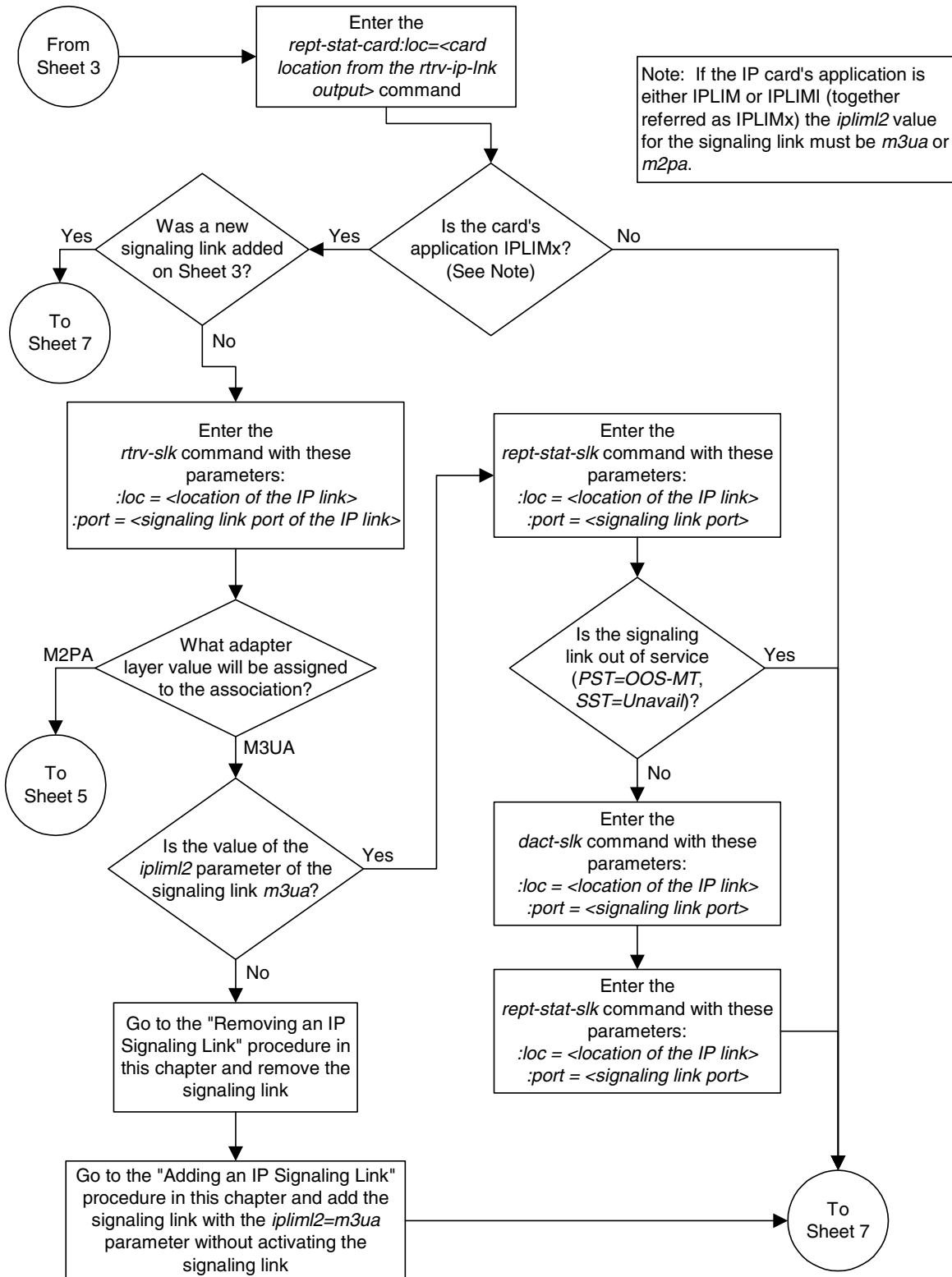
Flowchart 3-34. Changing an Association (Sheet 2 of 9)



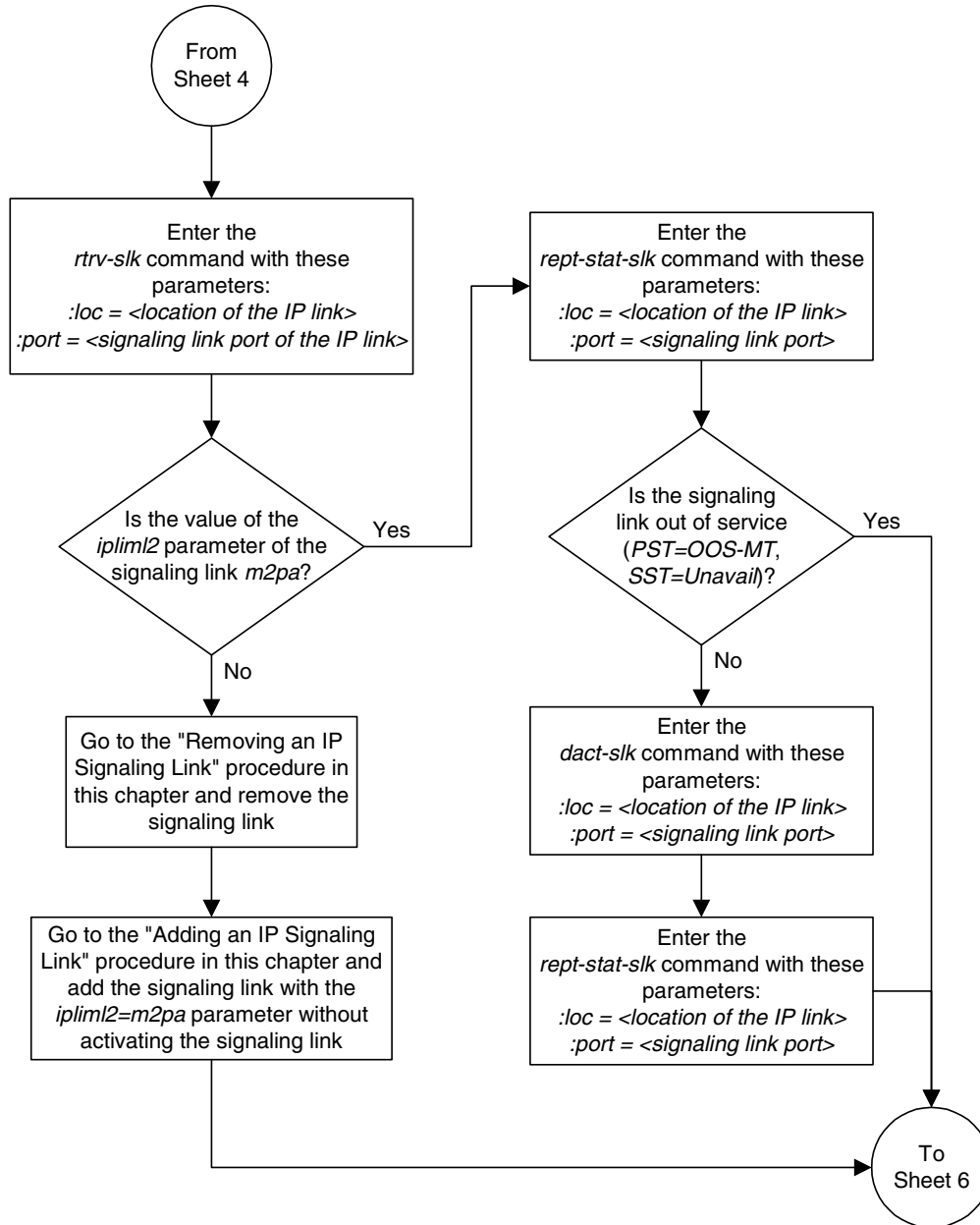
Flowchart 3-34. Changing an Association (Sheet 3 of 9)



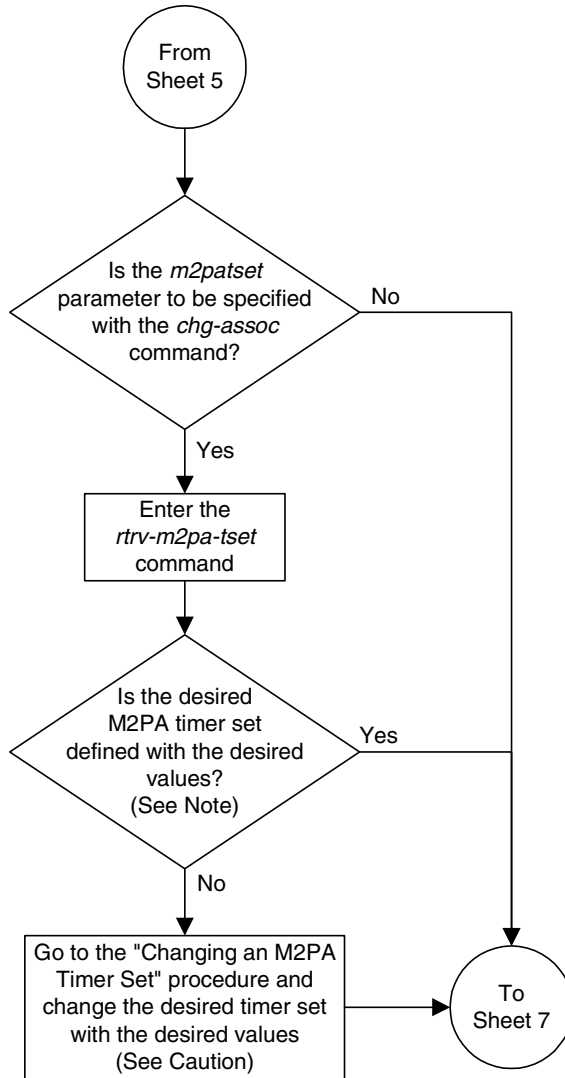
Flowchart 3-34. Changing an Association (Sheet 4 of 9)



Flowchart 3-34. Changing an Association (Sheet 5 of 9)



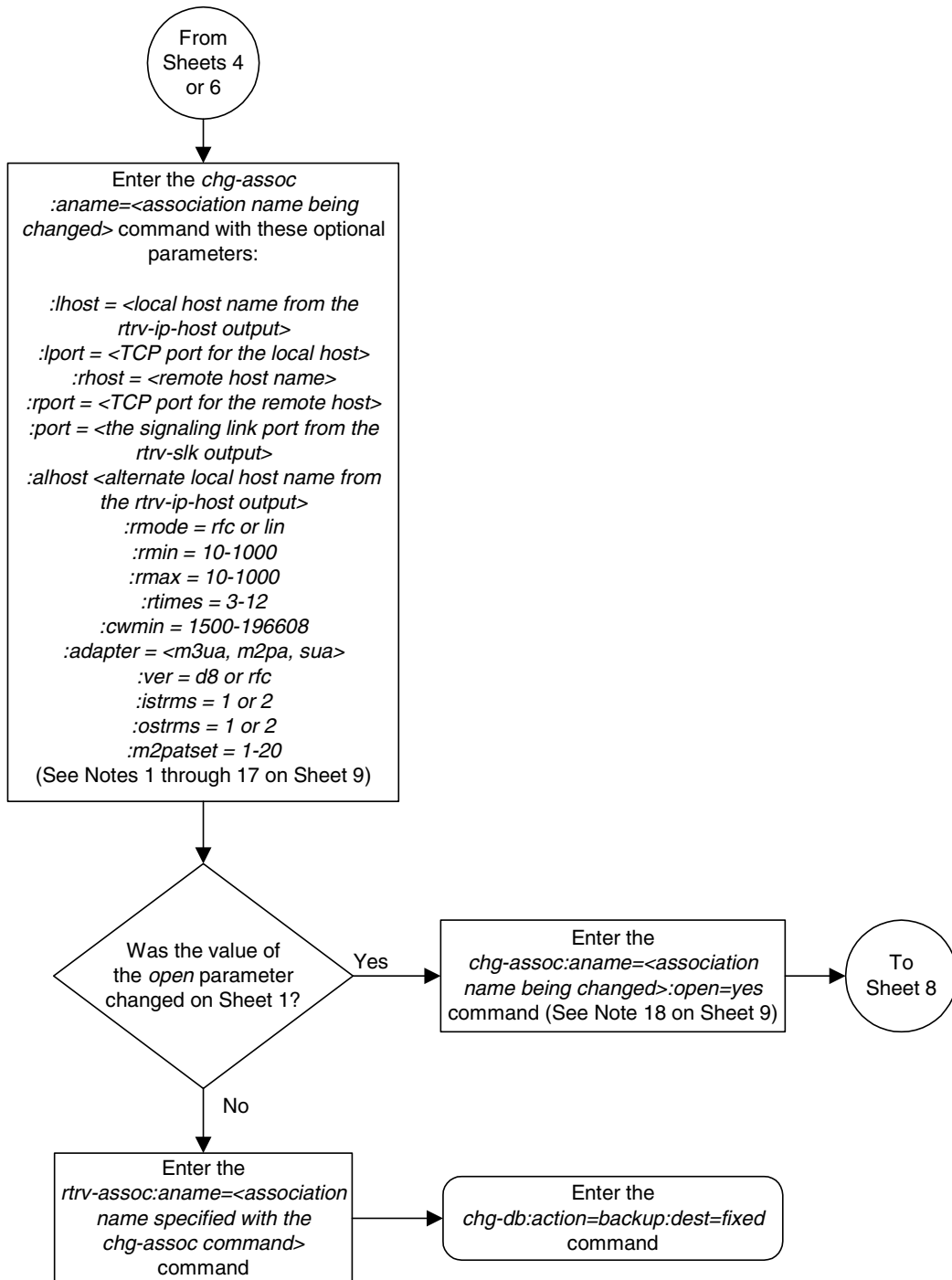
Flowchart 3-34. Changing an Association (Sheet 6 of 9)



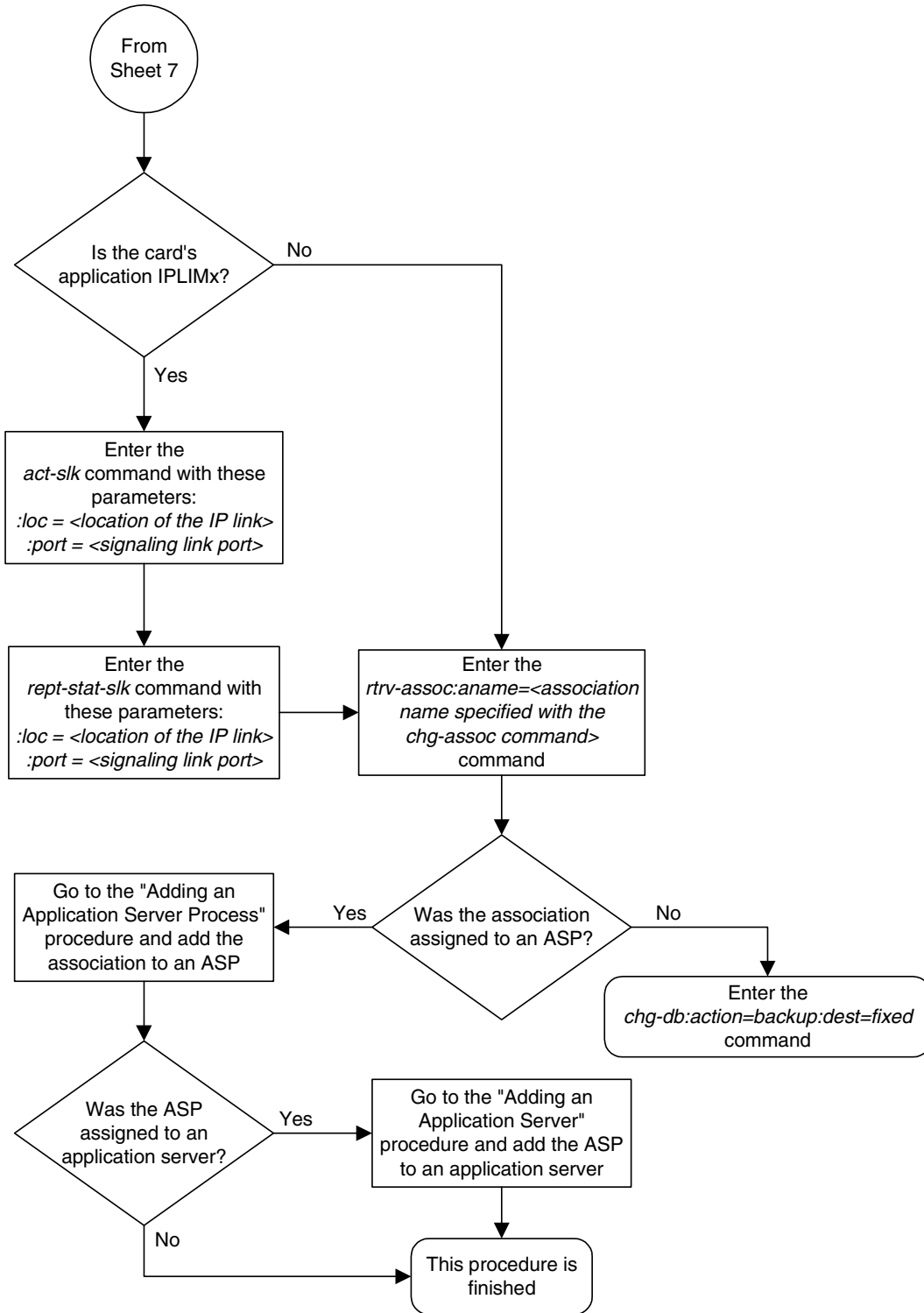
Note: If the *m2patset* parameter will not be specified with the *chg-assoc* command, and the *adapter* parameter value is being changed to *m2pa*, the M2PA timer set 1 will be assigned to the association.

Caution: Changing an M2PA timer set may affect the performance of any associations using the timer set being changed.

Flowchart 3-34. Changing an Association (Sheet 7 of 9)



Flowchart 3-34. Changing an Association (Sheet 8 of 9)



Flowchart 3-34. Changing an Association (Sheet 9 of 9)

Notes:

1. If any optional parameters are not specified with the *chg-assoc* command, those values are not changed.
2. If the card containing the signaling link is a DCM, the B Ethernet interface cannot be used. Single-slot EDCMs can use the B Ethernet interface.
3. Each local host on a card running either the *ss7ipgw* or *ipgwi* applications can contain a maximum of 50 connections (associations plus sockets).
4. The system can contain a maximum of 4000 connections (associations plus sockets).
5. Cards running either the *iplim* or *iplimi* applications can have only one connection for each signaling link port and a maximum of two connections for each card, if the card is a dual-slot DCM. If the card is a single-slot EDCM, the card may contain a maximum of eight connections.
6. The value of the *lhost* and *rhost* parameters is a text string of up to 60 characters, with the first character being a letter. The command input is limited to 150 characters, including the hostnames
7. If the card's application is either *iplim* or *iplimi*, the *adapter* parameter value must be either *m3ua* or *m2pa*. The value of the *adapter* parameter must match the value of the *ipliml2* parameter of the signaling link assigned to the card. For example, if the value of the signaling link's *ipliml2* parameter is *m3ua*, the value of the adapter parameter must be *m3ua*. If the current value of the *adapter* parameter is not *m3ua*, then the *adapter=m3ua* parameter must be specified with the *chg-assoc* command. If the value of the signaling link's *ipliml2* parameter is *m2pa*, the value of the *adapter* parameter must be *m2pa*. If the current value of the *adapter* parameter is not *m2pa*, then the *adapter=m2pa* parameter must be specified with the *chg-assoc* command.
8. Specifying the *lhost* parameter only creates a uni-homed endpoint. The network portion of the endpoint's IP address must be the same as the network portion of the IP address assigned to either the A or B network interface of the IP card.
9. Specifying the *lhost* and *alhost* parameters creates a multi-homed endpoint. The network portion of the IP address associated with the *lhost* parameter must be the same as the network portion of the IP address assigned to one of the network interfaces (A or B) of the IP card, and the network portion of the IP address associated with the *alhost* parameter must be the same as the network portion of the IP address assigned to the other network interface on the IP card.
10. The *alhost=none* parameter removes the alternate local host from the specified association, which also removes the multi-homed endpoint capability.
11. If the value of the *open* parameter is *yes*, only the value of the *alw* parameter can be changed. To change the values of other parameters, the value of the *open* parameter must be *no*.
12. The value of the *rmin* parameter must be less than or equal to the *rmax* parameter value.
13. For associations assigned to the *ss7ipgw* or *ipgwi* applications, the value of the *cwmin* parameter must be less than or equal to 16384.
14. The *ver* parameter cannot be specified for SUA or M2PA connections.
15. Cards running either *ss7ipgw* or *ipgwi* applications can have only the values *m3ua* or *sua* for the *adapter* parameter.
16. The *m2patset* parameter can be specified only with the *adapter=m2pa* parameter, or if the current *adapter* parameter value for the association is *m2pa*.
17. If the *mp2atset* parameter is not specified with the *chg-assoc* command, and the *adapter* parameter value is being changed to *m2pa*, the *m2patset* parameter value defaults to M2PA timer set 1 (*m2patset=1*).
18. If the *open* parameter value is being changed to *yes*, the association must contain values for the *lhost*, *lport*, *rhost*, and *rport* parameters. The *lhost* parameter value must have a signaling link assigned to it.

Configuring SCTP Retransmission Control for an Association

This procedure is used to gather the information required to configure the retransmission parameters for associations. If any assistance is needed to configure the retransmission parameters for associations, contact Tekelec Technical Services. See “Tekelec Technical Services” on page 1-8.

The retransmission parameters are configured using the **rmode**, **rmin**, **rmax**, **rtimes**, and **cwmin** parameters of the **chg-assoc** command.

:rmode – The retransmission mode used when packet loss is detected. The values are **rfc** or **lin**.

- **rfc** – Standard RFC 2960 algorithm in the retransmission delay doubles after each retransmission. The RFC 2960 standard for congestion control is also used.
- **lin** – Tekelec's linear retransmission mode where each retransmission timeout value is the same as the initial transmission timeout and only the slow start algorithm is used for congestion control.

:rmin – The minimum value of the calculated retransmission timeout in milliseconds.

:rmax – The maximum value of the calculated retransmission timeout in milliseconds.

NOTE: The **rmin** and **rmax** parameter values form a range of retransmission values. The value of the **rmin** parameter must be less than or equal to the **rmax** parameter value.

:rtimes – The number of times a data retransmission occurs before closing the association.

:cwmin – The minimum size in bytes of the association's congestion window and the initial size in bytes of the congestion window.

For associations assigned to the **ss7ipgw** or **ipgwi** applications, the value of the **cwmin** parameter must be less than or equal to 16384.

The “Changing an Association” procedure on page 3-350 is used to change the values of these parameters. In addition to using the “Changing an Association” procedure, these pass commands are also used in this procedure.

- **ping** – tests for the presence of hosts on the network.
- **assocrtt** – displays the SCTP round trip times for a specified association. Minimum, maximum, and average times are kept for each open association. The Retransmission Mode (RFC or LIN) and the configured Minimum and Maximum Retransmission Timeout limits are also displayed.
- **sctp -g sctp** – provides a summary list of all SCTP instances.

- **sctp -g pgs** – displays the pgs for a specific association. A specific association is specified using the **-p** and **-i** options.

For more information on the **pass** commands, see the *Commands Manual*.

The **chg-assoc** command contains other optional parameters that can be used to configure an association. These parameters are not shown here because they are not necessary for configuring the SCTP retransmission parameters. These parameters are explained in more detail in the “Changing an Association” procedure on page 3-350, or in the **chg-assoc** command description in the *Commands Manual*.

Canceling the RTRV-ASSOC Command

Because the **rtrv-assoc** command used in this procedure can output information for a long period of time, the **rtrv-assoc** command can be canceled and the output to the terminal stopped. There are three ways that the **rtrv-assoc** command can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the **rtrv-assoc** command was entered.
- Enter the **canc-cmd** without the **trm** parameter at the terminal where the **rtrv-assoc** command was entered.
- Enter the **canc-cmd:trm=<xx>**, where **<xx>** is the terminal where the **rtrv-assoc** command was entered, from another terminal other than the terminal where the **rtrv-assoc** command was entered. To enter the **canc-cmd:trm=<xx>** command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the **rtrv-secu-trm** command. The user's permissions can be verified with the **rtrv-user** or **rtrv-secu-user** commands.

For more information about the **canc-cmd** command, go to the *Commands Manual*.

Procedure

1. Display the associations in the database using the `rtrv-assoc` command. This is an example of possible output.

```

rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME swbel32
  PORT      A
  ADAPTER   M3UA          VER      M3UA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  LPORT     1030          RPORT     2345
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES          ALW       YES

ANAME a2
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030          RPORT     2345
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES          ALW       YES

ANAME a3
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw106.nc.tekelec.com
  LPORT     1030          RPORT     2346
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES          ALW       YES

ANAME assoc1
  PORT      A
  ADAPTER   M3UA          VER      M3UA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030          RPORT     1030
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000
  OPEN      YES          ALW       YES
IP Appl Sock table is (4 of 4000) 1% full

```

2. Display the IP address assigned to the local host that will be pinged in step 4 using the `rtrv-ip-host` command with the local host name shown in step 1. For this example, enter this command.

```
rtrv-ip-host:host=gw105.nc.tekelec.com
```

The following is an example of the possible output

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
```

```
IPADDR          HOST
192.1.1.30      GW100.NC.TEKELEC.COM
```

```
IP Host table is (10 of 512) 2% full
```

3. Display the card location assigned to the IP address of the local host shown in step 2 by entering the `rtrv-ip-lnk` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
```

```
LOC  PORT  IPADDR          SUBMASK          DUPLEX  SPEED  MACTYPE  AUTO
1201  A     192.001.001.030 255.255.255.0    ----   ---   DIX      YES
1203  A     192.001.001.012 255.255.255.0    ----   ---   DIX      YES
1205  A     192.001.001.014 255.255.255.0    FULL   100   DIX      NO
```

4. Using the outputs of steps 1 and 3 as a guide, enter the `ping` pass command specifying the card location of the local host, shown in step 3, and the name of the remote host assigned to the association being changed, shown in step 1. This command is entered several times to obtain the average round trip time. For this example, enter this command.

```
pass:loc=1201:cmd="ping gw100.nc.tekelec.com"
```

The following is an example of the possible output

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
```

```
PASS: Command sent to card
```

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
```

```
PING command in progress
```

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
```

```
PING GW100.NC.TEKELEC.COM (192.1.1.30): 56 data bytes
```

```
64 bytes from tekral.nc.tekelec.com (192.1.1.30): icmp_seq=0. time=5. ms
```

```
64 bytes from tekral.nc.tekelec.com (192.1.1.30): icmp_seq=1. time=9. ms
```

```
64 bytes from tekral.nc.tekelec.com (192.1.1.30): icmp_seq=2. time=14. ms
```

```
----tekral PING Statistics----
```

```
3 packets transmitted, 3 packets received, 0% packet loss
```

```
round-trip (ms)  min/avg/max = 5/9/14
```

```
PING command complete
```

NOTE: If the SCTP retransmission parameters are not to be changed, do not perform steps 5 through 9. This procedure is finished.

5. Go to the "Changing an Association" procedure on page 3-350 and change the retransmission parameters of the association based on the results of pinging the remote host.
-

6. Enter the **assocrtt** pass command to display the round trip time data collected after an association is established when an SCTP INIT message is sent and an acknowledgement is received.

The **assocrtt** command is entered with the card location from step 4 (the card location assigned to the association being changed), and the name of the association being changed. This association must contain the local host name used in step 2. For this example, enter this command.

```
pass:loc=1201:cmd="assocrtt assoc1"
```

The following is an example of the possible output

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
PASS: Command sent to card

rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
ASSOCRTT: Association round-trip time report (in milliseconds)

Retransmission Configuration
  Retransmission Mode           : LIN
  Minimum RTO                   : 120
  Maximum RTO                   : 800

Traffic Round-Trip Times
  Minimum round-trip time       : 5
  Maximum round-trip time       : 120
  Weighted Average round-trip time : 10
  Last recorded round-trip time  : 10

Measured Congested Traffic Round-Trip Times
  Minimum round-trip time       : 0
  Maximum round-trip time       : 0
  Weighted Average round-trip time : 0
  Last recorded round-trip time  : 0

;
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
ASSOCRTT command complete
```

7. Enter the **sctp -g sctp** pass command, specifying the card location from step 6, to display the SCTP instance information of each association on the card. For this example, enter this command.

```
pass:loc=1201:cmd="sctp -g sctp"
```

The following is an example of the possible output

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
PASS: Command sent to card

rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
Local   Local IP      Num of
Port    Address          Assoc
-----
7001    192.168.110.35   1
2222    192.168.110.12   3
         192.168.112.12

rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

SCTP command complete
```

- Enter the `sctp -g sctp -p <local port number>` pass command to display the association IDs. The association ID value (shown in the **Assoc ID** column of the output of this command) is used in the step 9 and identifies the association being changed.

The local port number is in the **Local Port** column displayed in step 7. Specify the card location used in step 7. For this example, enter this command.

pass:loc=1201:cmd="sctp -g sctp -p 2222"

The following is an example of the possible output

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
Local IP          Num of
Port   Address      Assoc
2222   192.168.110.12   3
        192.168.112.12

Assoc   Local   Primary      Remote
ID      IP Address  Port   Address      Port
  1     192.168.110.12  2222  192.168.112.4  5555
        192.168.112.12
  2     192.168.110.12  2222  192.168.112.4  6666
        192.168.112.12
  3     192.168.110.12  2222  192.168.112.4  7777
        192.168.112.12

        no.of inqueued msgs = 0
                max mtu = 1500
                max init times = 8
                max send times = 10
        max size reassembly = 1048576
        default rwnd value = 16384
                pre-open streams = 1
        ip datagram counter = 2781

Timer Values:          seconds      millisecs
      INIT              1              0
      RECV              0              200
      SEND              1              0
      SHUTDOWN          0              300
      HEARTBEAT         0              500
      PMTU              600             0

;

rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

SCTP command complete
```

9. Enter the `sctp -g peps -p <local port number> -i <association ID>` pass command to determine if retransmissions have occurred. The local port number is in the local port value specified for the `-p` option of the `sctp -g sctp` pass command performed in step 8. The association ID is the number shown in the `Assoc ID` column in step 8 identifying the association being changed. Specify the card location used in step 7. For this example, enter this command.

```
pass:loc=1201:cmd="sctp -g peps -p 2222 -i 2"
```

The following is an example of the possible output

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
PASS: Command sent to card

rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
      ip datagrams rcvd = 155402
      ip datagrams with data chunks rcvd = 120844
          data chunks rcvd = 367908
          data chunks read = 367900
              dup tsns rcvd = 8
                  sacks rcvd = 38734
              gap ack blocks rcvd = 3
          heartbeat requests rcvd = 135
          heartbeat acks rcvd = 52
          heartbeat requests sent = 52
          ip datagrams sent = 129254
      ip datagrams with data chunks sent = 73084
          data chunks sent = 396330
      retransmit data chunks sent = 135
          sacks sent = 64872
          Send Failed = 0
      retransmit timer count = 0
      consecutive retransmit timeouts = 0
      RTT between RMIN and RMAX inclusive = 6
          RTT greater than RMAX = 0
          fast retransmit count = 135
          recv timer count = 0
          heartbeat timer count = 244

          none left tosend = 0
          none left rwnd gate = 5
          none left cwnd gate = 8

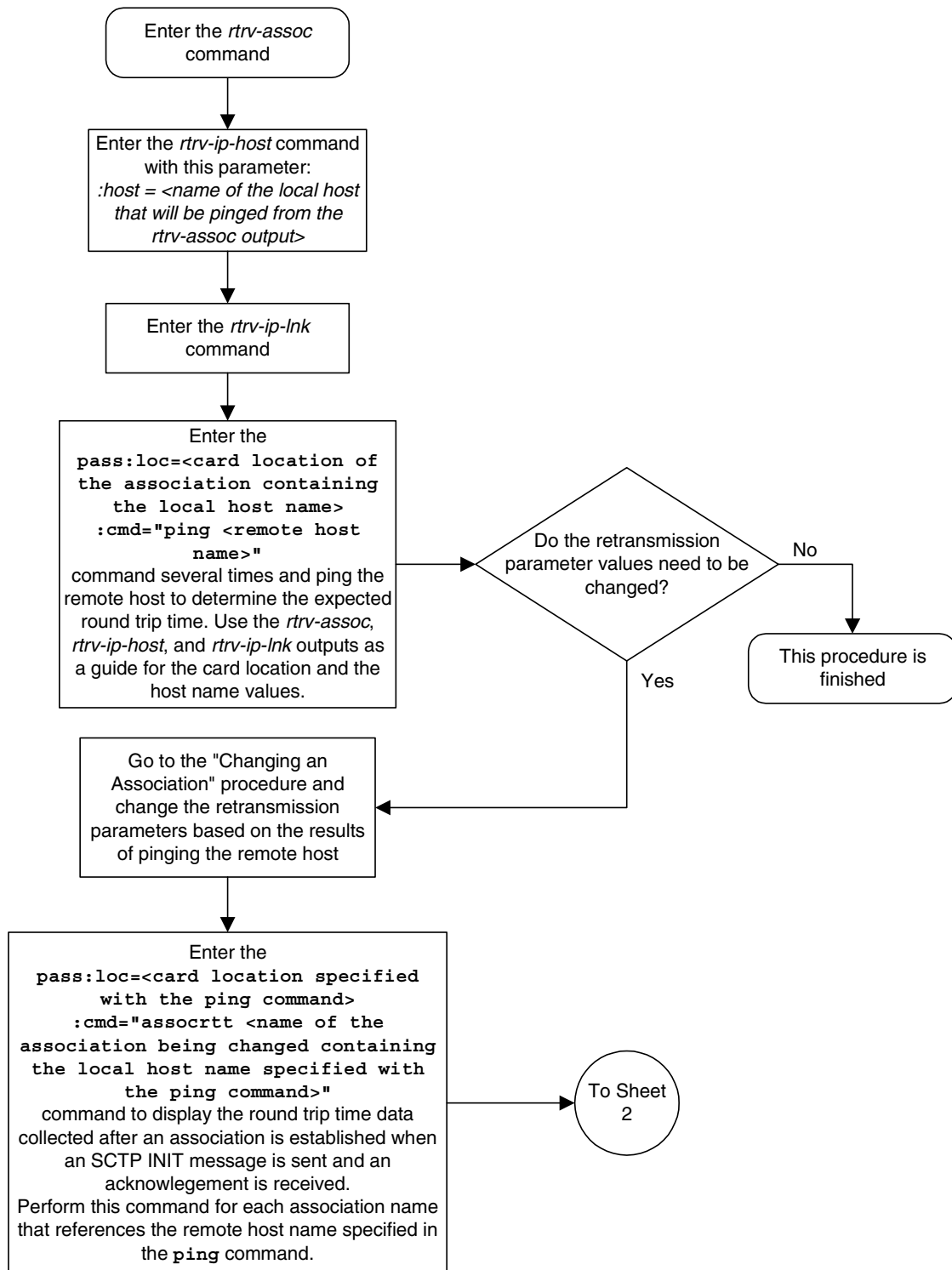
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

SCTP command complete
```

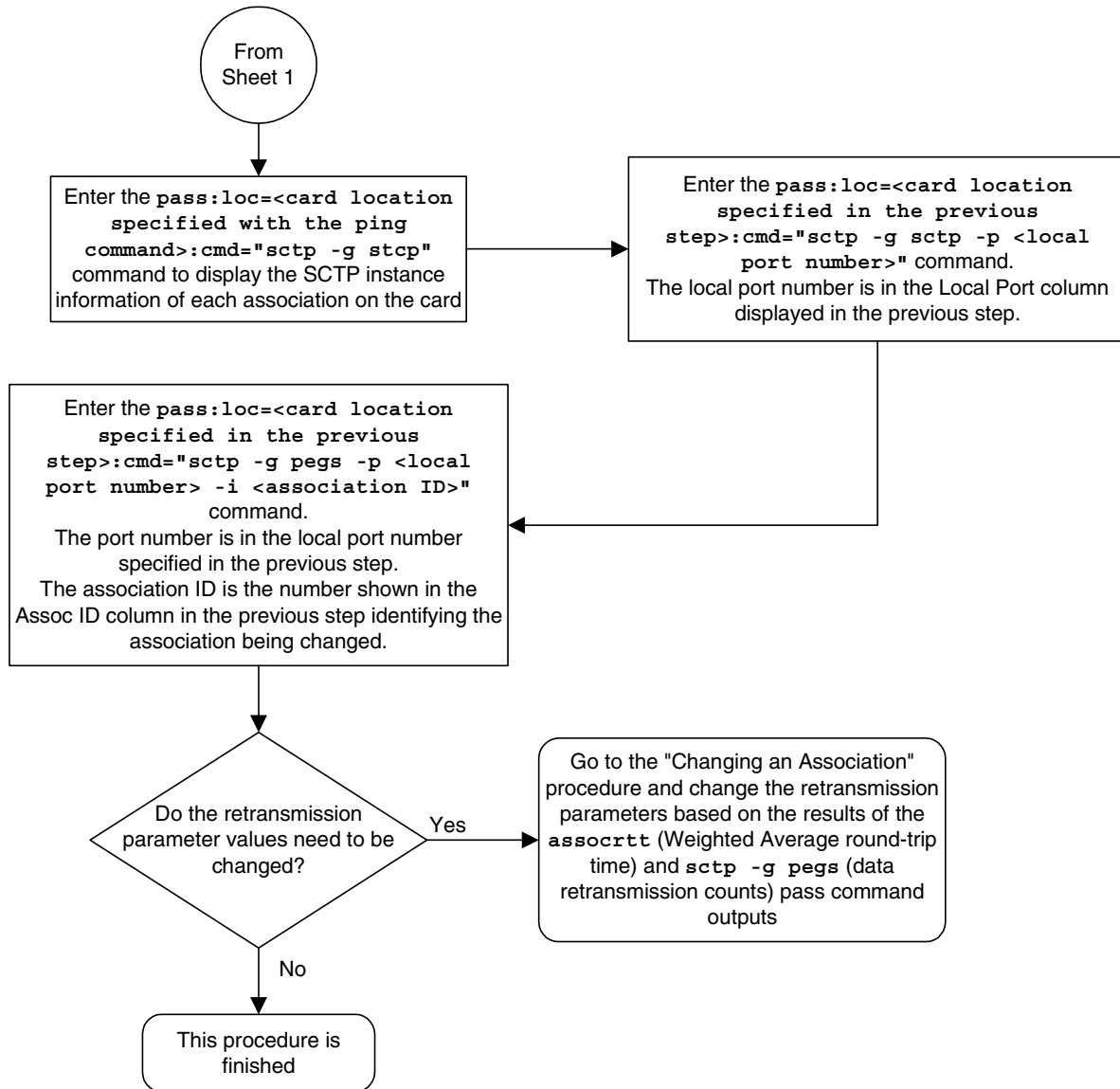
NOTE: The **Weighted Average round-trip time** shown in the `assocrtt` pass command output in step 6, and the data retransmission counts shown in the `sctp -g peps` pass command output in step 9 are used as a guide to determine the appropriate values for the `rmode`, `rmin`, `rmax`, and `rtimes` parameters. If the retransmission parameters do not have to be adjusted, do not perform this step. This procedure is finished.

10. Go to the “Changing an Association” procedure on page 3-350 and change the retransmission parameters of the association based on the results of the outputs of steps 6 and 9.
-

Flowchart 3-35. Configuring an Association for SCTP Retransmission Control (Sheet 1 of 2)



Flowchart 3-35. Configuring an Association for SCTP Retransmission Control (Sheet 2 of 2)



Changing an M2PA Timer Set

This procedure is used to change the values of the M2PA timers in an M2PA timer set using the `chg-m2pa-tset` command. The M2PA timers are used to control the behavior of the signaling link assigned to an M2PA association (an association containing the M2PA adapter layer - `adapter=m2pa`) during signaling link alignment and proving, and during times of transmit congestion.

The system contains 20 M2PA timer sets. One of these timer sets is assigned to an M2PA association using the `m2patset` parameter of either the `ent-assoc` or `chg-assoc` command. If the `m2patset` parameter is not specified with the `ent-assoc` command, or with the `chg-assoc` command if the adapter layer for that association is being changed to M2PA, timer set 1 is automatically assigned to the association.



CAUTION: Changing an M2PA timer set may affect the performance of any associations using the timer set being changed.

The `chg-m2pa-tset` command uses these parameters.

:tset – The M2PA timer set being changed, 1 - 20.

:srctset – The timer values in an existing M2PA timer set can be copied to another M2PA timer set, specified by the `tset` parameter. The `srctset` parameter specifies the timer set that is to be copied. If the `srctset` parameter is specified, no other timer values can be specified. The `srctset` parameter value cannot be the timer set specified by the `tset` parameter.

:t1 – Alignment Timer – The amount of time the M2PA adapter layer waits to receive a Link Status Alignment message from the peer, from 1000 to 60000 milliseconds. The system default value is 10000 milliseconds.

:t3 – Ready Timer – The amount of time after proving the M2PA adapter layer waits to receive a Link Status Ready message from the peer, 1000 to 60000 milliseconds. The system default value is 10000 milliseconds.

:t4e – Proving Timer (Emergency) – The amount of time the M2PA adapter layer generates Link Status Proving messages during emergency proving, from 400 to 600 milliseconds. The system default value is 500 milliseconds.

:t4n – Proving Timer (Normal) – The amount of time the M2PA adapter layer generates Link Status Proving messages during normal proving, from 1000 to 60000 milliseconds. The system default value is 10000 milliseconds.

:t5 – Busy Rate Timer – The amount of time between sending Link Status Busy messages while the link is in-service, from 100 milliseconds to 10000 milliseconds. The system default value is 1000 milliseconds.

:t6 – Remote Congestion Timer – The amount of time that a congested link will remain in service, from 1000 to 6000 milliseconds. The system default value is 3000 milliseconds.

: **t7** – Excess Delay in Acknowledgement Timer – The maximum amount of time that may pass between when a user data message is transmitted and an acknowledgement for that message is received from the peer, from 200 milliseconds to 2000 milliseconds. If this timer expires, the link is taken out of service. The system default value is 1200 milliseconds.

: **t16** – Proving Rate Timer – The amount of time between sending Link Status Proving messages while the T4N or T4E timer is running, from 50 milliseconds to 400 milliseconds. The system default value is 200 milliseconds.

: **t17** – Ready Rate Timer – The amount of time between sending Link Status Ready messages while the T3 timer is running, from 100 milliseconds to 500 milliseconds. The system default value is 250 milliseconds.

: **t18** – Processor Outage Rate Timer – The amount of time between sending Link Status Processor Outage messages while the link is in-service, from 100 milliseconds to 10000 milliseconds. The system default value is 1000 milliseconds.

The value of any timer parameter not specified with the **chg-m2pa-tset** command is not changed.

Procedure

1. Display the M2PA timer sets in the database by entering the **rtrv-m2pa-tset** command. This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

```
M2PA Timers (in msec)
```

TSET	T1	T3	T4N	T4E	T5	T6	T7	T16	T17	T18
1	10000	10000	10000	500	1000	3000	1200	200	250	1000
2	10000	10000	10000	500	1000	3000	1200	200	250	1000
3	10000	10000	10000	500	1000	3000	1200	200	250	1000
4	10000	10000	10000	500	1000	3000	1200	200	250	1000
5	10000	10000	10000	500	1000	3000	1200	200	250	1000
6	10000	10000	10000	500	1000	3000	1200	200	250	1000
7	10000	10000	10000	500	1000	3000	1200	200	250	1000
8	10000	10000	10000	500	1000	3000	1200	200	250	1000
9	10000	10000	10000	500	1000	3000	1200	200	250	1000
10	10000	10000	10000	500	1000	3000	1200	200	250	1000
11	10000	10000	10000	500	1000	3000	1200	200	250	1000
12	10000	10000	10000	500	1000	3000	1200	200	250	1000
13	10000	10000	10000	500	1000	3000	1200	200	250	1000
14	10000	10000	10000	500	1000	3000	1200	200	250	1000
15	10000	10000	10000	500	1000	3000	1200	200	250	1000
16	10000	10000	10000	500	1000	3000	1200	200	250	1000
17	10000	10000	10000	500	1000	3000	1200	200	250	1000
18	10000	10000	10000	500	1000	3000	1200	200	250	1000
19	10000	10000	10000	500	1000	3000	1200	200	250	1000
20	10000	10000	10000	500	1000	3000	1200	200	250	1000

2. Change the desired timer set with the **chg-m2pa-tset** command. To change a specific timer set, enter the **chg-m2pa-tset** command with the **tset** parameter and the timer parameters you wish to change. For this example, enter this command.

```
chg-m2pa-tset:tset=1:t1=27500:t3=3850:t4e=450:t4n=4859:t5=5700
:t6=3750:t7=1150:t16=250:t17=375:t18=8750
```

To copy an M2PA timer set to another timer set, enter the **chg-m2pa-tset** command with the **tset** and **srctset** parameters. For this example, copying timer set 1 to timer set 9, enter this command.

```
chg-m2pa-tset:tset=9:srctset=1
```

When the **chg-m2pa-tset** command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
CHG-M2PA-TSET: MASP A - COMPLTD
```

3. Verify the changes by entering the **rtrv-m2pa-tset** command specifying the timer set specified in step 2. For this example, enter these commands.

```
rtrv-m2pa-tset:tset=1
```

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

M2PA Timers (in msec)

TSET	T1	T3	T4N	T4E	T5	T6	T7	T16	T17	T18
1	27500	3850	450	4859	5700	3750	1150	250	375	8750

```
rtrv-m2pa-tset:tset=9
```

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

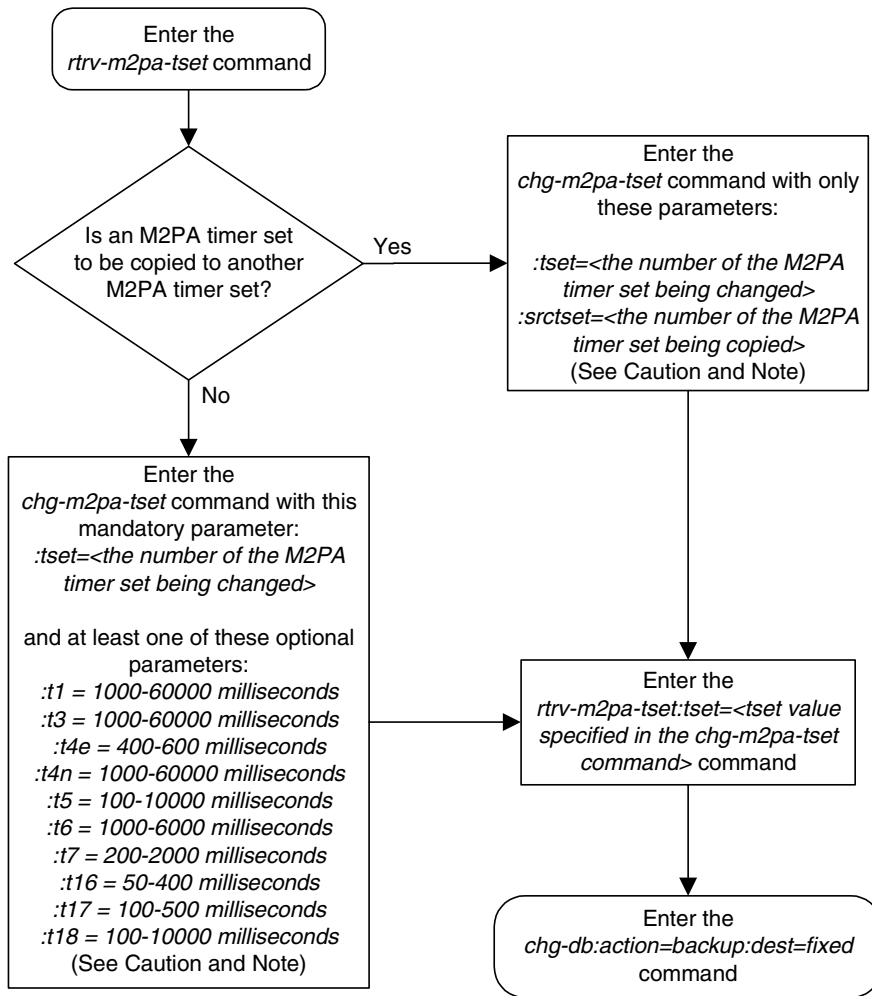
M2PA Timers (in msec)

TSET	T1	T3	T4N	T4E	T5	T6	T7	T16	T17	T18
9	27500	3850	450	4859	5700	3750	1150	250	375	8750

4. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-36. Changing an M2PA Timer Set



Note: Either the timer parameters (*t1*, *t3*, *t4e*, *t4n*, *t5*, *t6*, *t7*, *t16*, *t17*, *t18*) or the *srctset* parameter must be specified with the *chg-m2pa-tset* command. Both the timer parameters and the *srctset* parameter cannot be specified with the *chg-m2pa-tset* command.

Caution: Changing an M2PA timer set may affect the performance of any associations using the timer set being changed.

Adding an Application Server Process

This procedure is used to create an ASP (application server process) and assign an SCTP association to it using the **ent-asp** command. The **ent-asp** command uses these parameters:

:aspname - The name assigned to the ASP. Valid association names can contain up to 15 alphanumeric characters where the first character is a letter and the remaining characters are alphanumeric characters. The **aspname** parameter value is not case-sensitive.

:aname - The name assigned to the association. Valid association names can contain up to 15 alphanumeric characters where the first character is a letter and the remaining characters are alphanumeric characters. The **aname** parameter value is not case-sensitive.

An association containing the **adapter=m2pa** value cannot be assigned to an ASP. The association cannot be assigned to an existing ASP.

The UA parameter set value for the ASP cannot be assigned in this procedure. It can be changed after the ASP has been added to the database. When an ASP is added to the database, the UA parameter set value is defaulted to 10. Go to the "Changing an Application Server" procedure on page 3-412 to change the UA parameter set value.

Canceling the RTRV-ASP and RTRV-ASSOC Commands

Because the **rtrv-asp** and **rtrv-assoc** commands used in this procedure can output information for a long period of time, the **rtrv-asp** and **rtrv-assoc** commands can be canceled and the output to the terminal stopped. There are three ways that the **rtrv-asp** and **rtrv-assoc** commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the **rtrv-asp** or **rtrv-assoc** commands were entered.
- Enter the **canc-cmd** without the **trm** parameter at the terminal where the **rtrv-asp** or **rtrv-assoc** commands were entered.
- Enter the **canc-cmd:trm=<xx>**, where **<xx>** is the terminal where the **rtrv-asp** or **rtrv-assoc** commands were entered, from another terminal other than the terminal where the **rtrv-asp** or **rtrv-assoc** commands were entered. To enter the **canc-cmd:trm=<xx>** command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the **rtrv-secu-trm** command. The user's permissions can be verified with the **rtrv-user** or **rtrv-secu-user** commands.

For more information about the **canc-cmd** command, go to the *Commands Manual*.

Procedure

1. Display the application server processes in the database using the `rtrv-asp` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP                ASSOCIATION                UAPS
asp1                swbel32                    1
asp2                a2                        1
asp3                a3                        1

ASP Table is (3 of 4000) 1% full
```

2. Display the associations in the database using the `rtrv-assoc` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME swbel32
  PORT      A
  ADAPTER   M3UA          VER      M3UA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  LPORT     1030          RPORT    2345
  ISTRMS    2              OSTRMS   2
  RMODE     LIN          RMIN     120          RMAX     800
  RTIMES    10          CWMIN    3000
  OPEN      YES          ALW      YES

ANAME a2
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030          RPORT    2345
  ISTRMS    2              OSTRMS   2
  RMODE     LIN          RMIN     120          RMAX     800
  RTIMES    10          CWMIN    3000
  OPEN      YES          ALW      YES

ANAME a3
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw106.nc.tekelec.com
  LPORT     1030          RPORT    2346
  ISTRMS    2              OSTRMS   2
  RMODE     LIN          RMIN     120          RMAX     800
  RTIMES    10          CWMIN    3000
  OPEN      YES          ALW      YES
```

```

ANAME assoc1
PORT A
ADAPTER M3UA VER M3UA RFC
LHOST gw105.nc.tekelec.com
ALHOST ---
RHOST gw100.nc.tekelec.com
LPORT 1030 RPORT 1030
ISTRMS 2 OSTRMS 2
RMODE LIN RMIN 120 RMAX 800
RTIMES 10 CWMIN 3000
OPEN YES ALW YES
IP Appl Sock table is (4 of 4000) 1% full

```

If the association that is to be added to the ASP is not shown in the **rtrv-assoc** output, go to the “Adding an Association” procedure on page 3-332 and add the required association to the database.

3. Add the application server process to the database using the **ent-asp** command. For this example, enter this command.

```
ent-asp:aspname=asp4:aname=assoc1
```

When this command has successfully completed, this message should appear.

```

rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ENT-ASP: MASP A - COMPLTD

```

4. Verify the changes using the **rtrv-asp** command. This is an example of possible output.

```

rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP ASSOCIATION UAPS
asp1 swbel32 1
asp2 a2 1
asp3 a3 1
asp4 assoc1 10
ASP Table is (4 of 4000) 1% full

```

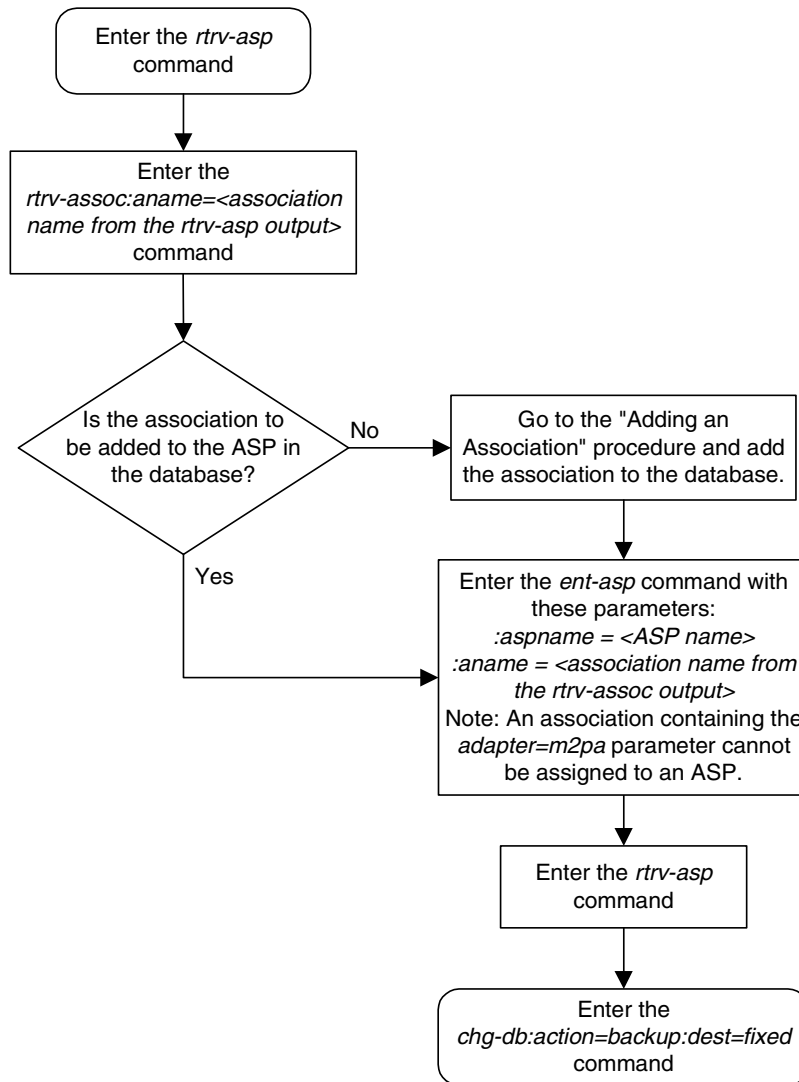
5. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```

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

```

Flowchart 3-37. Adding an Application Server Process



Removing an Application Server Process

This procedure is used to remove an ASP (application server process) from the database using the `dlt-asp` command.

The `dlt-asp` command uses one parameter, `aspname`, the name of the ASP being removed from the database. The ASP being removed must be in the database.

The ASP being removed from the database cannot be assigned to an application server (AS). This can be verified with the `rtrv-as` command. If the ASP has an application server assigned to it, go to the "Removing an Application Server" procedure on page 3-407 and remove the application server assignment to the ASP.

Canceling the RTRV-ASP and RTRV-AS Commands

Because the `rtrv-asp` and `rtrv-as` commands used in this procedure can output information for a long period of time, the `rtrv-asp` and `rtrv-as` commands can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-asp` and `rtrv-as` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-asp` or `rtrv-as` commands was entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-asp` or `rtrv-as` commands was entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-asp` or `rtrv-as` commands was entered, from another terminal other than the terminal where the `rtrv-asp` or `rtrv-as` commands was entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the application server processes in the database using the `rtrv-asp` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP                ASSOCIATION                UAPS
asp1                swbel32                    1
asp2                a2                        1
asp3                a3                        1
asp4                assoc1                    10
asp5                assoc2                    10
asp6                assoc3                    10
asp7                assoc4                    10
```

```
ASP Table is (7 of 4000) 1% full
```

2. Display the application servers in the database using the `rtrv-as` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
      AS Name           Mode           ASP Names
      as1                LOADSHARE      asp1
                                           asp2
                                           asp3
                                           asp5
                                           asp6
      as2                OVERRIDE       asp7
```

AS table is (2 of 250) 1% full.

If the ASP is assigned to an application server, go to the “Removing an Application Server” procedure on page 3-407 and remove the ASP from the application server.

3. Remove the application server from the database using the `dlt-asp` command. For this example, enter this command.

```
dlt-asp:aspname=asp5
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
DLT-ASP: MASP A - COMPLTD
```

4. Verify the changes using the `rtrv-asp` command. This is an example of possible output.

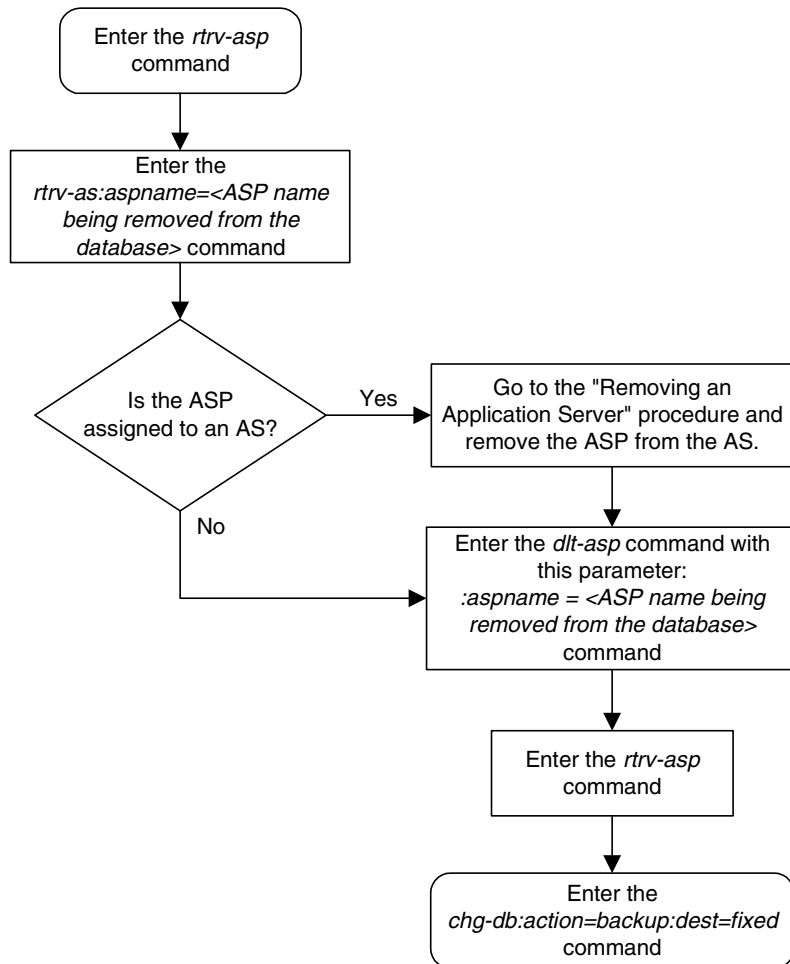
```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP           ASSOCIATION           UAPS
asp1          swbel32                1
asp2          a2                     1
asp3          a3                     1
asp4          assoc1                 10
asp6          assoc3                 10
asp7          assoc4                 10
```

ASP Table is (6 of 4000) 1% full

5. Back up the new changes, using the `chg-db:action=backup:dest=fixed` command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-38. Removing an Application Server Process



Changing an Application Server Process

This procedure is used to change the UA parameter set assigned to an ASP (application server process) using the **chg-asp** command.

The **chg-asp** command uses these parameters:

- **:aspname** - The name assigned to the ASP.
- **:uaps** - The UA parameter set value being assigned to the ASP.

This procedure can be performed only with ASPs containing M3UA associations.

The **open** parameter of the association assigned to the ASP must be set to **no** before the ASP can be changed. This can be verified with the **rtrv-assoc** command.

Application servers can contain up to 16 ASPs. All associations assigned to ASPs in an application server with the **open** parameter set to **yes** must have the same UA parameter set assigned to their ASPs.

Canceling the RTRV-ASP and RTRV-ASSOC Commands

Because the **rtrv-asp** and **rtrv-assoc** commands used in this procedure can output information for a long period of time, the **rtrv-asp** and **rtrv-assoc** commands can be canceled and the output to the terminal stopped. There are three ways that the **rtrv-asp** and **rtrv-assoc** commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the **rtrv-asp** or **rtrv-assoc** commands were entered.
- Enter the **canc-cmd** without the **trm** parameter at the terminal where the **rtrv-asp** or **rtrv-assoc** commands were entered.
- Enter the **canc-cmd:trm=<xx>**, where **<xx>** is the terminal where the **rtrv-asp** or **rtrv-assoc** commands were entered, from another terminal other than the terminal where the **rtrv-asp** or **rtrv-assoc** commands were entered. To enter the **canc-cmd:trm=<xx>** command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the **rtrv-secu-trm** command. The user's permissions can be verified with the **rtrv-user** or **rtrv-secu-user** commands.

For more information about the **canc-cmd** command, go to the *Commands Manual*.

Procedure

1. Display the application server processes in the database using the **rtrv-asp** command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP          ASSOCIATION          UAPS
asp1         swbel32             1
asp2         a2                  1
asp3         a3                  1
asp4         assoc1              10
asp5         assoc2              10
asp6         assoc3              10
asp7         assoc4              10

ASP Table is (7 of 4000) 1% full
```

2. Display the association assigned to the ASP that is being changed using the **rtrv-assoc** command and specifying the name of the association. For this example, enter this command.

```
rtrv-assoc:aname=swbel32
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME swbel32
PORT   A
ADAPTER M3UA          VER          M3UA RFC
LHOST  gw105.nc.tekelec.com
ALHOST ---
RHOST  gw100.ncd-economic-development.southeastern-cooridor-ash.gov
LPORT  1030           RPORT        2345
ISTRMS 2           OSTRMS        2
RMODE  LIN          RMIN          120          RMAX          800
RTIMES 10          CWMIN         3000
OPEN   YES         ALW           YES

IP Appl Sock table is (4 of 4000) 1% full
```

If the association is not an M3UA association (containing the value **M3UA** for the **adapter** parameter), choose another ASP and repeat this step. When an M3UA association is found, go to step 3.

If no M3UA associations are found, this procedure cannot be performed and is finished.

3. Verify if the ASP being changed is assigned to an application server by entering the **rtrv-as** command with the name of the ASP being changed. For this example, enter this command.

```
rtrv-as:aspname=asp1
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
AS Name          Mode          ASP Names

AS table is (3 of 250) 1% full.
```

This example shows that ASP1 is not assigned to an application server.

NOTE: If you do not wish to verify the values in the UA parameter set, skip this step and go to step 5.

4. Display the values in the UA parameter set by entering the **rtrv-uaps** command and specifying the desired UA parameter set number, from 1 to 10. For this example, enter this command.

rtrv-uaps:set=3

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
SET  TIMER      TVALUE  PARM    PVALUE
3     1           10      1       255
3     2           3000   2       0
3     3           0       3       0
3     4           0       4       0
3     5           0       5       0
3     6           0       6       0
3     7           0       7       0
3     8           0       8       0
3     9           0       9       0
3    10          0       10      0
```

TIMER 1: AS Recovery Timer (ms) T(r), min time AS msgs are queued, SS7IPGW and IPGWI applications enforce 10-2000(ms).
TVALUE : Valid range = 32-bits

TIMER 2: False IP Connection Congestion Timer, max time an association can be congested before failing due to false congestion. SS7IPGW and IPGWI applications enforce 0-30000(ms).
TVALUE : Valid range = 32-bits

PARM 1: ASP SNM options. Each bit is used as an enabled/disabled flag for a particular ASP SNM option.
PVALUE : Valid range = 32-bits

BIT	BIT VALUE
0=Broadcast	0=Disabled , 1=Enabled
1=Response Method	0=Disabled , 1=Enabled
2-5=Reserved	
6=Broadcast Congestion Status Change	0=Disabled , 1=Enabled
7-31=Reserved	

PARM 2: ASP/AS Notification options. Each bit is used an enabled/disabled flag for a particular ASP/AS Notification option.
PVALUE : Valid range = 32-bits

BIT	BIT VALUE
0=ASP Active Notifications	0=Disabled , 1=Enabled
1=ASP Inactive Notifications	0=Disabled , 1=Enabled
2=ASP AS State Query	0=Disabled , 1=Enabled
3-31=Reserved	

PARM 3: AS/ASP validations. Each bit is used to control a particular AS/ASP validation method.
PVALUE : Valid range = 32-bits

BIT	BIT VALUE
0=Strict ASP-ID checking	0=Disabled , 1=Enabled
1-31=Reserved	

If you wish to use the values shown in the UA parameter set, go to step 5.

If you do not wish to use the values shown in the UA parameter set, either go to the “Changing a UA Parameter Set” procedure on page 3-451 and change the values in this UA parameter set, or choose another UA parameter set and repeat this step.

5. If the value of the **open** parameter for the association shown in step 2 is **no**, skip this step and go to step 6.

If the value of the **open** parameter for the association shown in step 2 is **yes**, go to the “Changing an Association” procedure on page 3-350 and change the value of the **open** parameter to **no**.

6. Change the UA parameter set value assigned to the ASP using the **chg-asp** command, with the selected ASP name and the UA parameter set value used in step 4. For this example, enter this command.

```
chg-asp:aspname=asp1:uaps=3
```

NOTE: All associations assigned to ASPs in an application server with the open parameter set to yes must have the same UA parameter set assigned to their ASPs.

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASP: MASP A - COMPLTD
```

7. Verify the changes using the **rtrv-asp** command with the ASP name used in step 6. For this example, enter this command.

```
rtrv-asp:aspname=asp1
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP                ASSOCIATION                UAPS
asp1                swbel32                3

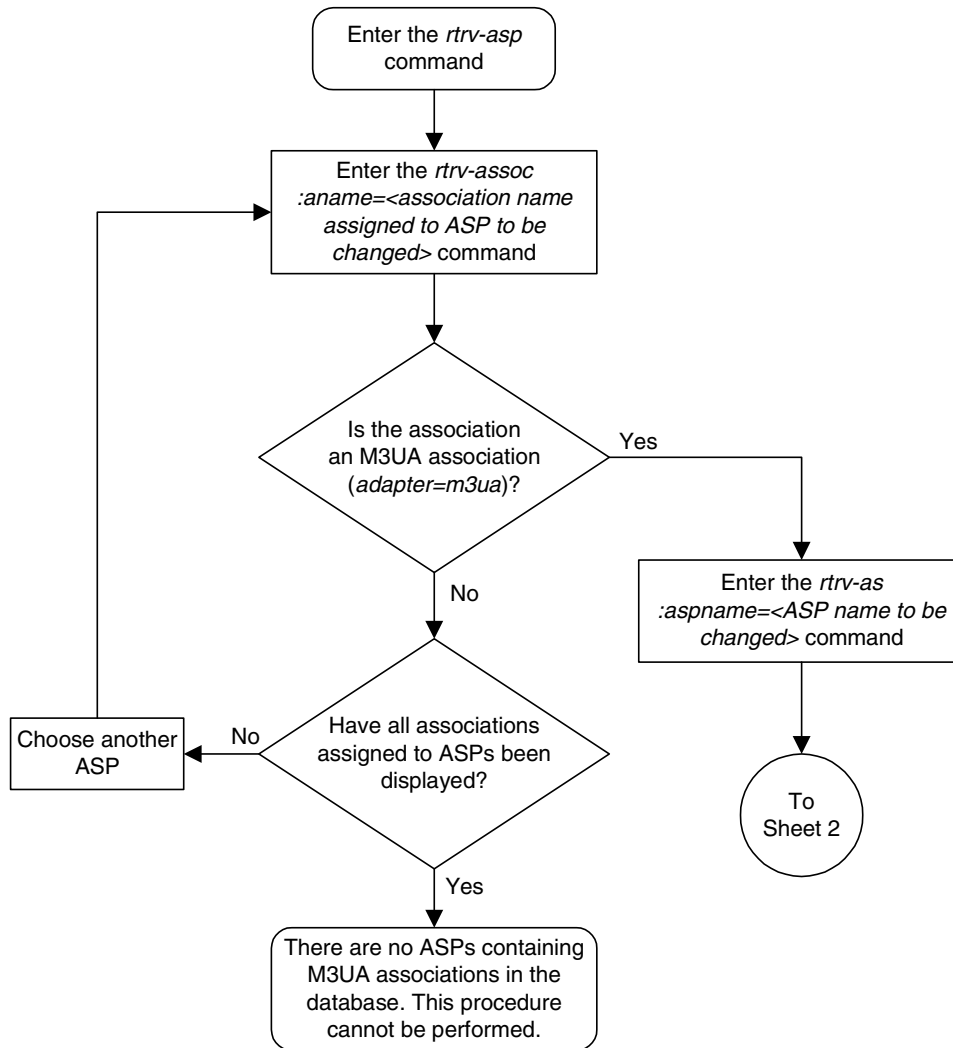
ASP Table is (7 of 4000) 1% full
```

8. Go to the “Changing an Association” procedure on page 3-350 and change the value of the **open** parameter to **yes**.

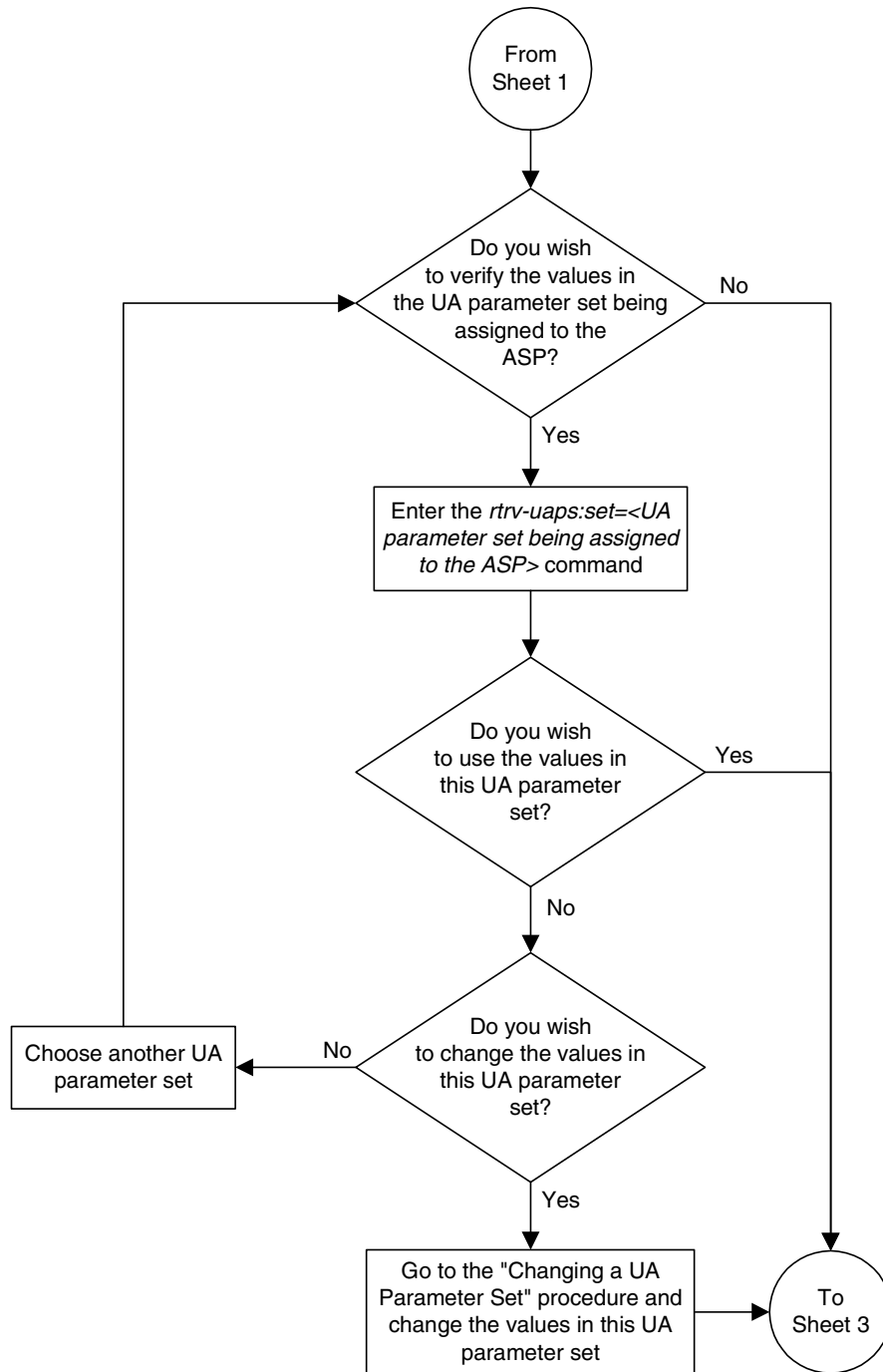
9. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

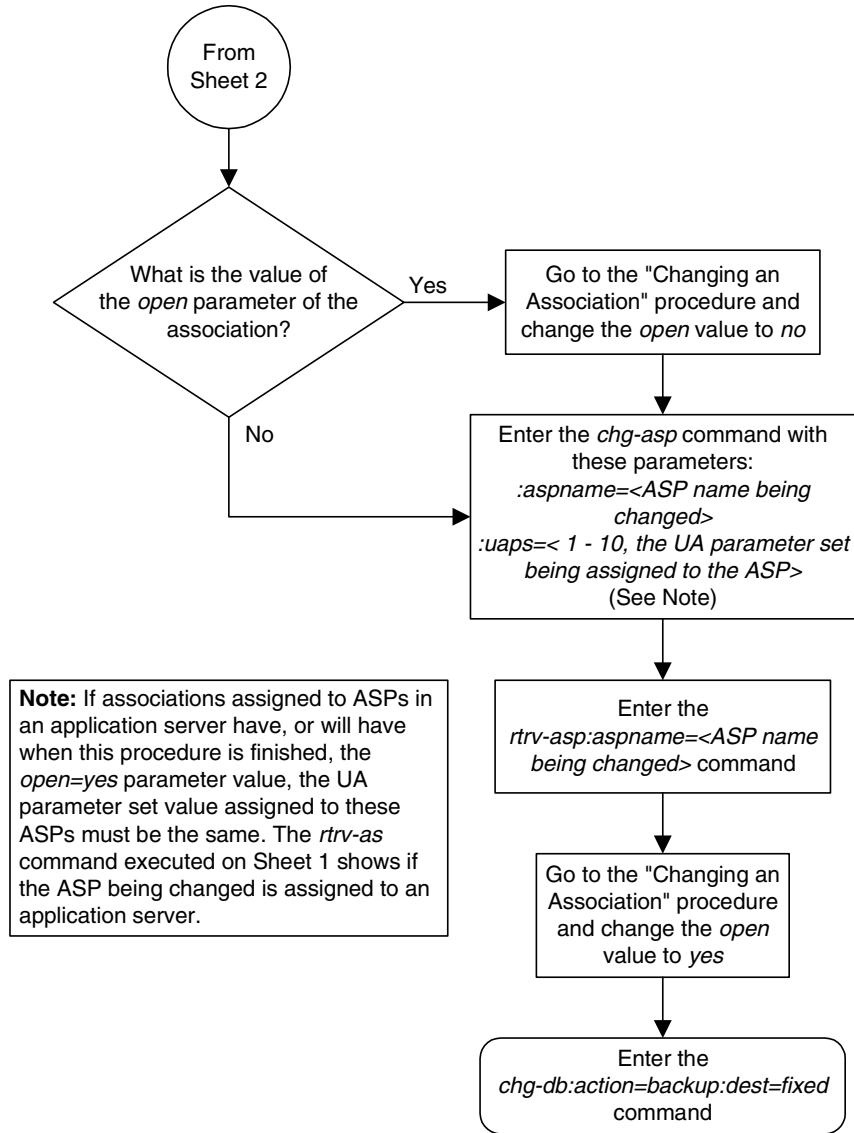
Flowchart 3-39. Changing an Application Server Process (Sheet 1 of 3)



Flowchart 3-39. Changing an Application Server Process (Sheet 2 of 3)



Flowchart 3-39. Changing an Application Server Process (Sheet 3 of 3)



Adding an Application Server

This procedure is used to create an application server and associate an application server process (ASP) with it using the **ent-as** command.

The **ent-as** command uses these parameters:

:asname – The application server name containing up to 15 alphanumeric characters, with the first character being an alphabetic character. Application server names are not case sensitive.

:aspname – The application server process name containing up to 15 alphanumeric characters, with the first character being an alphabetic character. Application server process names are not case sensitive.

The **open** parameter of the association assigned to the application server process must be set to **no** before the application server can be added to the database. This can be verified with the **rtrv-assoc** command.

The adapter type of the application server processes assigned to the application server must be the same. This can be verified in the **ADAPTER** field in the **rtrv-assoc** output.

The application of the IP signaling link referenced by the **lhost** parameter value in the association assigned to the application server process must be either **SS7IPGW** or **IPGWI**. This can be verified in the **APPL** field in the **rept-stat-card** output.

The **UA** parameter set values of the ASPs assigned to the application servers must be the same before the **open** parameter of the association assigned to the application server process is set to **yes**. The **UA** parameter set values are shown in the **UAPS** field of the **rtrv-asp** output. Before changing the **open** parameter value of the association assigned to the ASP being added to the application server to **yes**, verify the **UA** parameter set values of the ASPs in the application server. If the **UA** parameter set values are different, go to the “Changing an Application Server Process” procedure on page 3-390 and change the **UA** parameter set value of the ASP being added to the application server to match the **UA** parameter set values of the other ASPs in the application server.

Canceling the RTRV-ASP, RTRV-AS, and RTRV-ASSOC Commands

Because the **rtrv-asp**, **rtrv-as**, and **rtrv-assoc** commands used in this procedure can output information for a long period of time, the **rtrv-asp**, **rtrv-as**, and **rtrv-assoc** commands can be canceled and the output to the terminal stopped. There are three ways that the **rtrv-asp**, **rtrv-as**, and **rtrv-assoc** commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the **rtrv-asp**, **rtrv-as**, or **rtrv-assoc** commands were entered.
- Enter the **canc-cmd** without the **trm** parameter at the terminal where the **rtrv-asp**, **rtrv-as**, or **rtrv-assoc** commands were entered.

- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-asp`, `rtrv-as`, or `rtrv-assoc` commands were entered, from another terminal other than the terminal where the `rtrv-asp`, `rtrv-as`, or `rtrv-assoc` commands were entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the application servers in the database using the `rtrv-as` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
      AS Name           Mode           ASP Names
      as1                LOADSHARE      asp1
                                           asp2
                                           asp3
                                           asp5
                                           asp6
      as2                OVERRIDE      asp7

AS table is (2 of 250) 1% full.
```

2. Display the application server processes in the database using the `rtrv-asp` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP           ASSOCIATION           UAPS
asp1          swbel32                1
asp2          a2                     1
asp3          a3                     1
asp4          assoc1                 10
asp5          assoc2                 10
asp6          assoc3                 10
asp7          assoc4                 10

ASP Table is (7 of 4000) 1% full
```

If the ASP being added to the application server is not shown in the `rtrv-asp` output, go to the "Adding an Application Server Process" procedure on page 3-383 and add the ASP to the database following the rules shown on Sheet 5 of the "Adding an Application Server" flowchart on page 3-406.

NOTE: If the ASP was added to the database in step 2, skip steps 3 through 8, and go to step 9.

3. Display the associations in the database using the `rtrv-assoc` command and specifying the association name shown in the `rtrv-asp` output. For this example, enter this command.

```
rtrv-assoc:aname=assoc1
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc1
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030          RPORT    1030
  ISTRMS    2          OSTRMS   2
  RMODE     LIN          RMIN     120          RMAX      800
  RTIMES    10          CWMIN    3000
  OPEN      YES          ALW      YES
IP Appl Sock table is (7 of 4000) 1% full
```

NOTE: If the ASP is being assigned to a new application server, skip step 4 and go to step 5.

4. The `adapter` parameter value of all the associations assigned to an application server must be the same. Display the associations assigned to the application server by entering the `rtrv-assoc` command with the association name of each association assigned to the application server. The association names are shown in the `rtrv-asp` output in step 2. The ASP names assigned to the application server are shown in the `rtrv-as` output in step 1. For this example, enter this command.

```
rtrv-assoc:aname=assoc4
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
ANAME assoc4
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     dn-msc1
  ALHOST    ---
  RHOST     remotehost2
  LPORT     2345          RPORT    1025
  ISTRMS    2          OSTRMS   2
  RMODE     LIN          RMIN     120          RMAX      800
  RTIMES    10          CWMIN    3000
  OPEN      YES          ALW      YES
IP Appl Sock table is (7 of 4000) 1% full
```

If the `adapter` parameter value of associations shown in steps 3 and 4 are the same, go to step 5.

If the `adapter` parameter value of associations shown in steps 3 and 4 are not the same, you can select another ASP to add to the application server or you can add a new application server to the database.

To add new application server, go to the “Adding an Application Server Process” procedure on page 3-383 and add the ASP to the database following the rules shown on Sheet 5 of the “Adding an Application Server” flowchart on page 3-406.

To select another ASP to add to the application server, select the ASP from the `rtrv-asp` output in step 2, then verify the adapter parameter value of the association in step 3.

5. Display the IP address assigned to the `lhost` parameter value shown in step 3 using the `rtrv-ip-host` command and specifying the `host` parameter. For this example, enter this command.

```
rtrv-ip-host:host=gw105.nc.tekelec.com
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0

IPADDR          HOST
192.1.1.10      GW105.NC.TEKELEC.COM

IP Host table is (10 of 512) 2% full
```

6. Display the IP links in the database by entering the `rtrv-ip-lnk` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
LOC  PORT IPADDR          SUBMASK          DUPLEX  SPEED  MACTYPE  AUTO
1201 A    192.001.001.010    255.255.255.0    ----   ---   DIX      YES
1203 A    192.001.001.012    255.255.255.0    ----   ---   DIX      YES
1205 A    192.001.001.014    255.255.255.0    FULL   100   DIX      NO
```

7. Display the card type of the IP card shown in step 3 using the `rept-stat-card` command specifying the location of the IP card from the `rtrv-ip-lnk` output in step 6 corresponding to the IP address shown in the `rtrv-ip-host` output in step 5.

```
rept-stat-card:loc=1201
```

This is an example of the possible output.

```
rlghncxa03w 04-12-27 17:00:36 GMT EAGLE5 31.10.0
CARD  VERSION  TYPE  APPL  PST  SST  AST
1201  114-000-000  DCM   SS7IPGW  IS-NR  Active  -----
ALARM STATUS      = No Alarms.
BPDCM GPL         = 002-102-000
IMT BUS A         = Conn
IMT BUS B         = Conn
SLK A  PST         = IS-NR      LS=nc001  CLLI=-----
SCCP TVG RESULT   = 24 hr: -----, 5 min: -----
SLAN TVG RESULT   = 24 hr: -----, 5 min: -----
Command Completed.
```

If the card's application is IPLIM or IPLIMI, shown in the APPL column in the `rept-stat-card` output, either go back to step 3 and display another association corresponding to another ASP (shown in step 2) that is not

assigned to an application server (shown in step 1), or go to the “Adding an Application Server Process” procedure on page 3-383 and add the ASP to the database following the rules shown on Sheet 5 of the “Adding an Application Server” flowchart on page 3-406. Application servers are not supported on cards running the IPLIM or IPLIMI applications.

NOTE: If the value of the `open` parameter shown in step 3 is `no`, skip this step and go to step 9.

8. Change the value of the `open` parameter to `no` by specifying the `chg-assoc` command with the `open=no` parameter. For this example, enter this command.

```
chg-assoc:aname=assoc1:open=no
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

9. Add the application server to the database using the `ent-as` command. For this example, enter this command

```
ent-as:asname=as3:aspname=asp4
```

This is an example of possible inputs and outputs:

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ENT-AS: MASP A - COMPLTD;
```

10. Verify the changes using the `rtrv-as` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
```

AS Name	Mode	ASP Names
as1	LOADSHARE	asp1 asp2 asp3 asp5 asp6
as2	OVERRIDE	asp7
as3	LOADSHARE	asp4

AS table is (3 of 250) 1% full.

NOTE: If the application server process specified in step 9 was added as a result of the actions in either steps 2, 4, or 7, or does not contain an M3UA association, skip this step and go to step 12.

11. Verify that the UAPS parameter value of the ASP specified in step 8 is the same as the UAPS parameter values of the other ASPs assigned to the application server. The ASPs assigned to the application server are shown in the `rtrv-as` output in step 10, and the UAPS parameter values are shown in the `rtrv-asp` output in step 2. If the UAPS values are not the same, go to the “Changing an Application Server Process” procedure on page 3-390 and change the UAPS value of the ASP that was specified in step 9.
-

12. Change the value of the **open** parameter to **yes** by specifying the **chg-assoc** command with the **open=yes** parameter. For this example, enter this command.

chg-assoc:aname=assoc1:open=yes

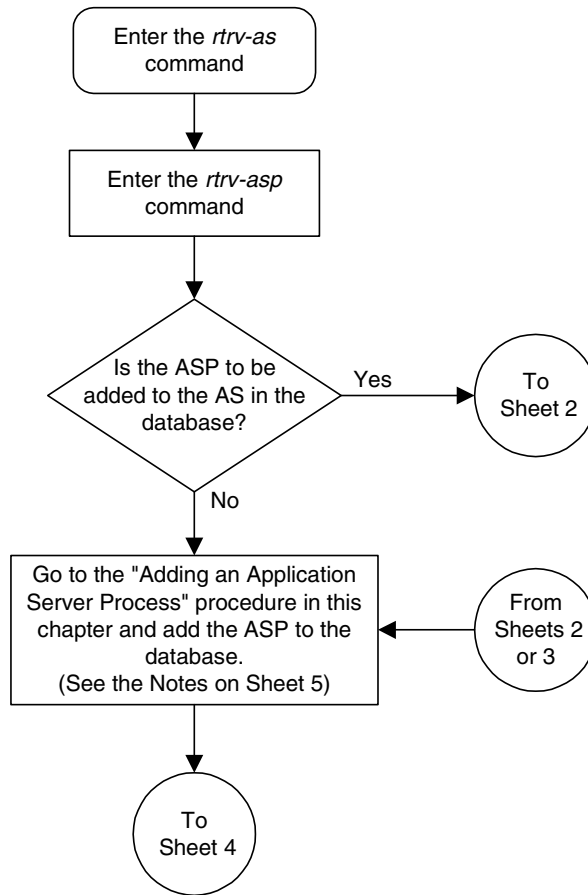
When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

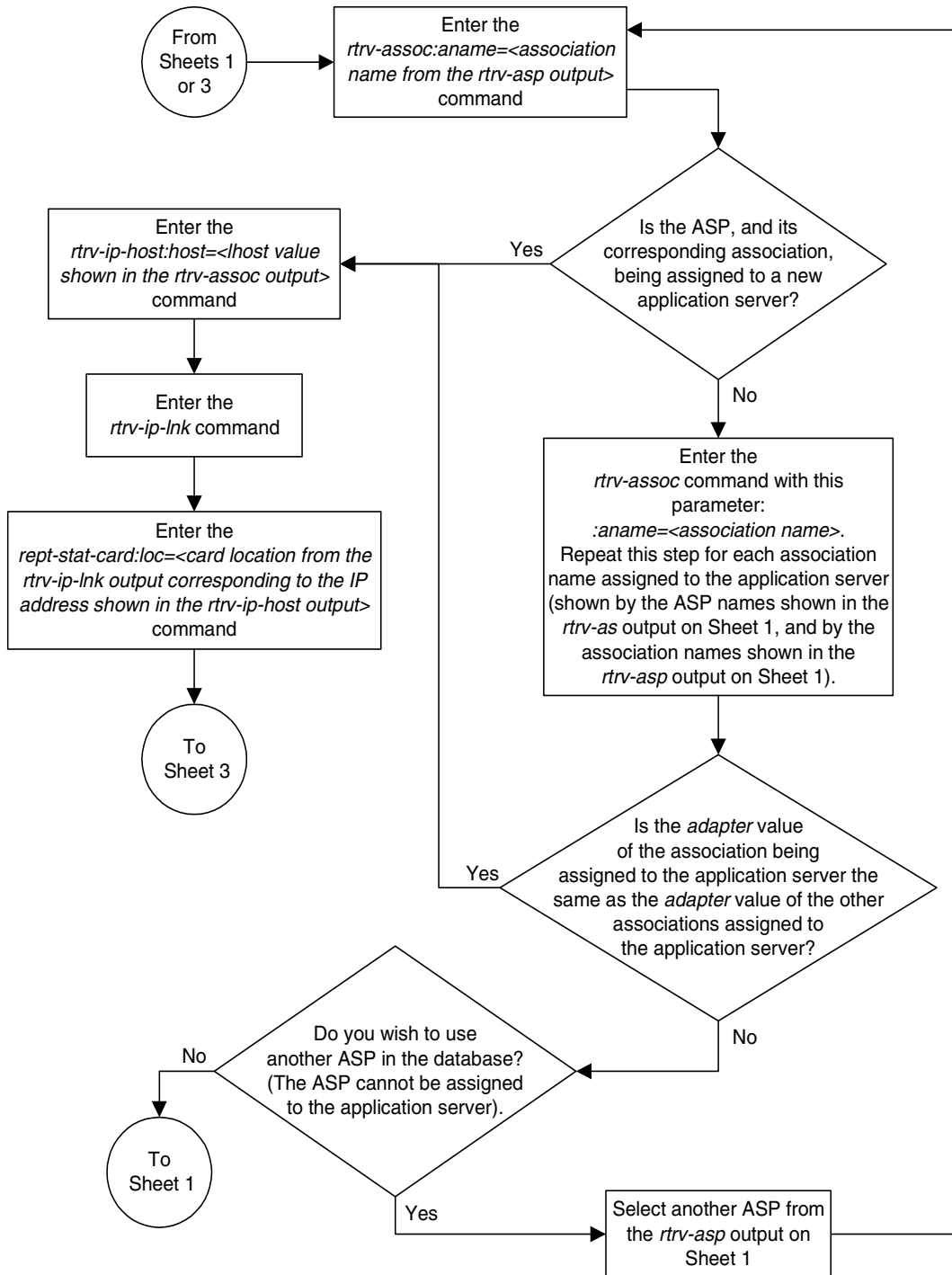
13. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

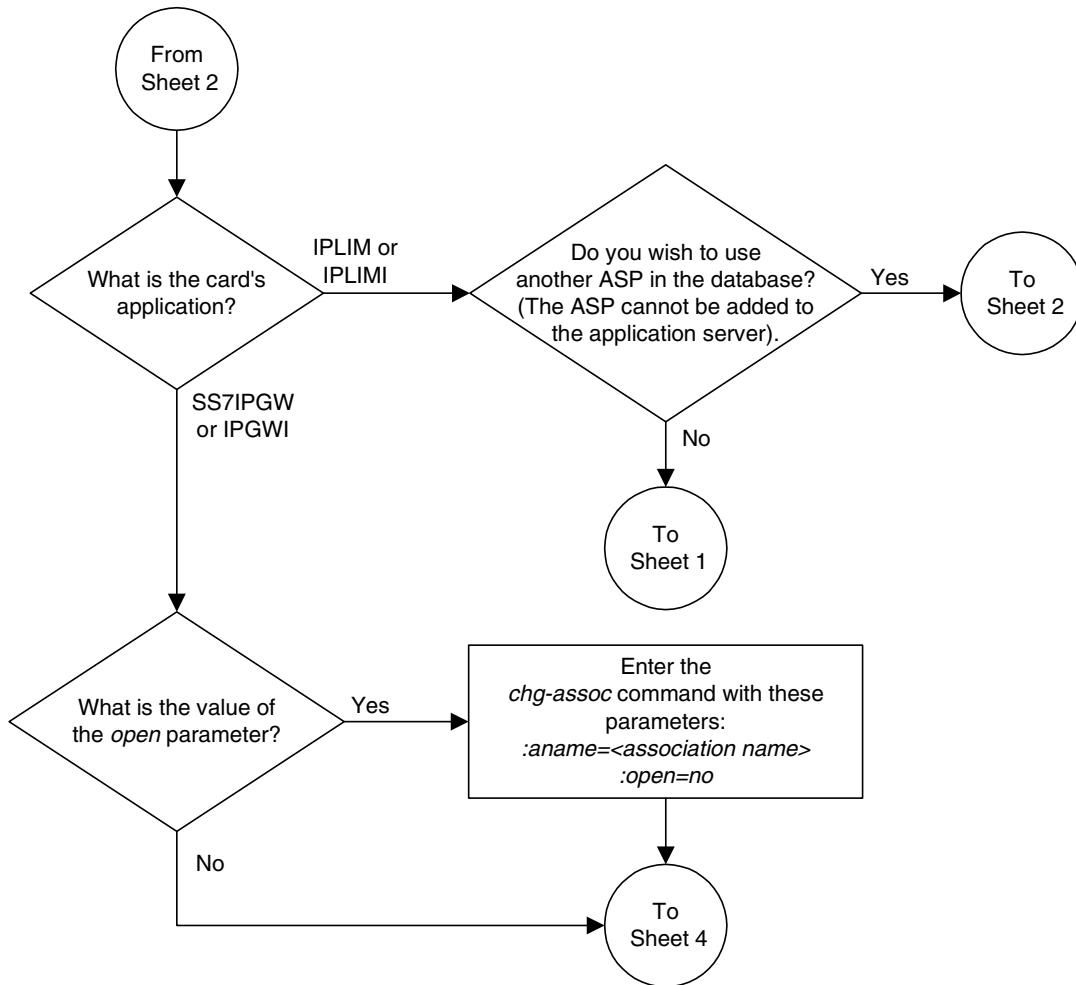
Flowchart 3-40. Adding an Application Server (Sheet 1 of 5)



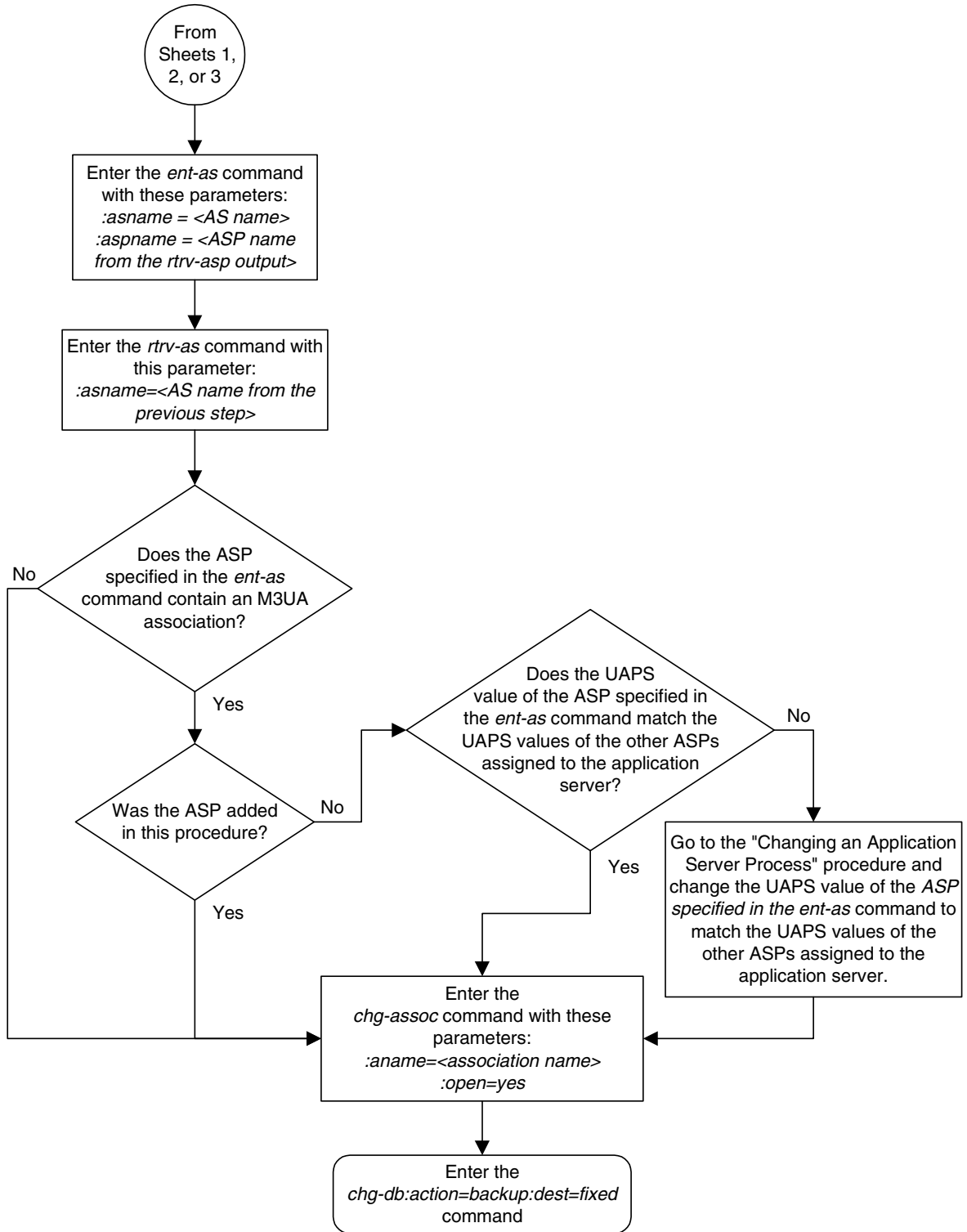
Flowchart 3-40. Adding an Application Server (Sheet 2 of 5)



Flowchart 3-40. Adding an Application Server (Sheet 3 of 5)



Flowchart 3-40. Adding an Application Server (Sheet 4 of 5)



Flowchart 3-40. Adding an Application Server (Sheet 5 of 5)

Notes:

1. If a new application server is being added in this procedure, and this application server will be assigned to a routing key containing a *rcontext* parameter value, the *adapter* parameter value for the association assigned to this application server can be either M3UA or SUA.
2. If a new application server is being added in this procedure, and this application server will be assigned to a routing key that does not contain a *rcontext* parameter value, the *adapter* parameter value for the association assigned to this application server must be M3UA.
3. If an ASP is being assigned to an existing application server, the *adapter* parameter value of the association assigned to the ASP must be the same as the *adapter* parameter value of the other associations/ASP's assigned to the application server.
4. SUA associations, and their corresponding ASP's and application server, can be assigned to only these types of routing keys:
 - Full routing key – DPC/SI=3/SSN
 - Partial routing key – DPC/SI=3
 - Partial routing key – DPC only
 - Partial routing key – SI=3 only
 - Default routing key.The routing key containing the application server with the SUA associations must have an *rcontext* value assigned to it.
If the new application server will not be assigned to one of these types of routing keys, the *adapter* parameter value of the associations assigned to the application server must be M3UA.
5. The value of the *open* parameter of the association is *no*.
6. The application of the card containing the signaling link assigned to the association is either SS7IPGW or IPGWI.
7. If the association assigned to this ASP is an M3UA association, the UA parameter set value of the ASP containing the M3UA association must be the same as the other ASP's in the application server. If the UA parameter set assigned to the other ASP's in the application server is not UA parameter set 10, the UA parameter assignment of the ASP being added must be changed using the "Changing an Application Server Process" procedure.

Removing an Application Server

This procedure is used to remove an ASP from an application server using the **dlt-as** command. If the ASP is the last ASP assigned to the application server, the application server is removed from the database.

The **dlt-as** command uses these parameters:

:asname – The application server name containing up to 15 alphanumeric characters, with the first character being an alphabetic character. Application server names are not case sensitive.

:aspname – The application server process name containing up to 15 alphanumeric characters, with the first character being an alphabetic character. Application server process names are not case sensitive.

The ASP name and application server name combination must be in the database.

The **open** parameter value in the association assigned to the ASP specified in the **dlt-as** command must be **no**. This can be verified with the **rtrv-assoc** command. Use the **chg-assoc** command to change the value of the **open** parameter.

Canceling the RTRV-ASP, RTRV-AS, and RTRV-ASSOC Commands

Because the **rtrv-asp**, **rtrv-as**, and **rtrv-assoc** commands used in this procedure can output information for a long period of time, the **rtrv-asp**, **rtrv-as**, and **rtrv-assoc** commands can be canceled and the output to the terminal stopped. There are three ways that the **rtrv-asp**, **rtrv-as**, and **rtrv-assoc** commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the **rtrv-asp**, **rtrv-as**, or **rtrv-assoc** commands were entered.
- Enter the **canc-cmd** without the **trm** parameter at the terminal where the **rtrv-asp**, **rtrv-as**, or **rtrv-assoc** commands were entered.
- Enter the **canc-cmd:trm=<xx>**, where **<xx>** is the terminal where the **rtrv-asp**, **rtrv-as**, or **rtrv-assoc** commands were entered, from another terminal other than the terminal where the **rtrv-asp**, **rtrv-as**, or **rtrv-assoc** commands were entered. To enter the **canc-cmd:trm=<xx>** command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the **rtrv-secu-trm** command. The user's permissions can be verified with the **rtrv-user** or **rtrv-secu-user** commands.

For more information about the **canc-cmd** command, go to the *Commands Manual*.

Procedure

1. Display the application servers in the database using the `rtrv-as` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
      AS Name          Mode          ASP Names
      as1              LOADSHARE    asp1
                                      asp2
                                      asp3
                                      asp5
                                      asp6
      as2              OVERRIDE     asp7
      as3              LOADSHARE    asp4

AS table is (3 of 250) 1% full.
```

2. Display the application server processes in the database using the `rtrv-asp` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP          ASSOCIATION          UAPS
ASP1        swbel32                1
ASP2        a2                    1
ASP3        a3                    1
ASP4        assoc1               10
ASP5        assoc2               10
ASP6        assoc3               10
ASP7        assoc4               10

ASP Table is (7 of 4000) 1% full
```

3. Display the associations in the database using the `rtrv-assoc` command and specifying the association name shown in the `rtrv-asp` output in step 2. For this example, enter this command.

```
rtrv-assoc:aname=assoc1
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc1
  PORT      A
  ADAPTER   M3UA          VER          M3UA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.nc.tekelec.com
  LPORT     1030          RPORT       1030
  ISTRMS    2              OSTRMS      2
  RMODE     LIN          RMIN        120          RMAX        800
  RTIMES    10          CWMIN       3000
  OPEN      YES          ALW         YES
IP Appl Sock table is (4 of 4000) 1% full
```

NOTE: If the value of the open parameter shown in step 3 is no, skip this step and go to step 5.

4. Change the value of the **open** parameter to **no** by specifying the **chg-assoc** command with the **open=no** parameter. For this example, enter this command.

```
chg-assoc:aname=assoc1:open=no
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

5. Remove the application server from the database using the **dlt-as** command. For this example, enter this command.

```
dlt-as:asname=as3:aspname=asp4
```

NOTE: If the ASP being removed from the application server is the last ASP assigned to the application server, the application server is removed from the database.

This is an example of possible inputs and outputs:

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ENT-AS: MASP A - COMPLTD;
```

6. Verify the changes using the **rtrv-as** command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
AS Name      Mode      ASP Names
      as1      LOADSHARE  asp1
                                           asp2
                                           asp3
                                           asp5
                                           asp6
      as2      OVERRIDE  asp7

AS table is (2 of 250) 1% full.
```

NOTE: If the value of the open parameter was not changed in step 4, skip this step and go to step 8.

7. Change the value of the **open** parameter to **yes** by specifying the **chg-assoc** command with the **open=yes** parameter. For this example, enter this command.

```
chg-assoc:aname=assoc1:open=yes
```

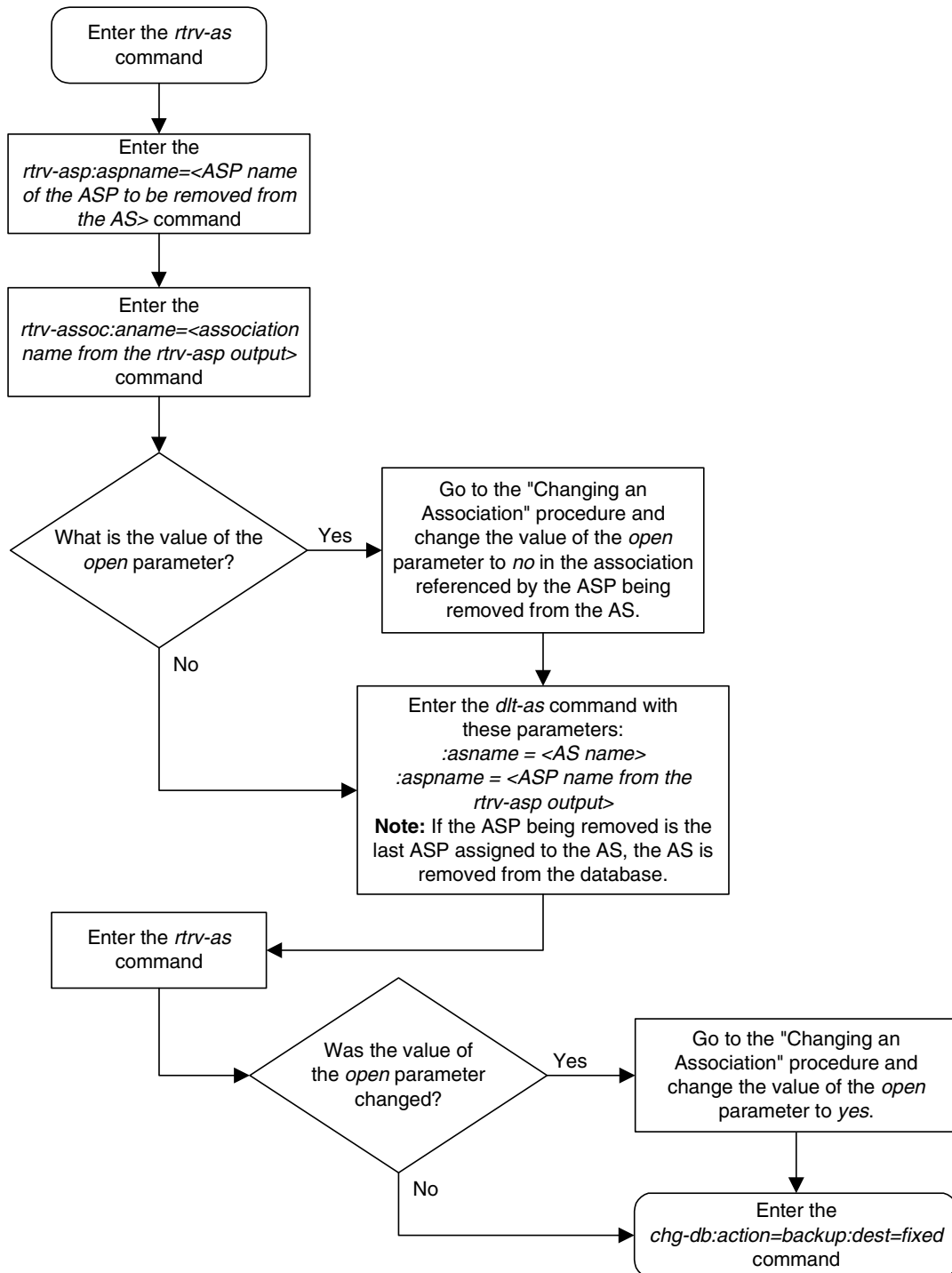
When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

8. Back up the new changes, using the `chg-db:action=backup:dest=fixed` command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-41. Removing an Application Server



Changing an Application Server

This procedure is used to change the characteristics of an existing application server using the **chg-as** command.

The **chg-as** command uses these parameters:

:asname – The application server name containing up to 15 alphanumeric characters, with the first character being an alphabetic character. Application server names are not case sensitive.

:mode – The traffic mode assigned to the application server, either **loadshare** or **override**.

The **open** parameter of the all associations assigned to the application server must be set to **no** before the application server can be changed. This can be verified with the **rtrv-assoc** command.

The ASPs assigned to the application server cannot be changed with this procedure. To change an ASP assigned to the application server, go to the “Removing an Application Server” procedure on page 3-407 and remove the ASP from the application server, then go to the “Adding an Application Server” procedure on page 3-397 and add the new ASP to the application server.

Canceling the RTRV-ASP, RTRV-AS, and RTRV-ASSOC Commands

Because the **rtrv-asp**, **rtrv-as**, and **rtrv-assoc** commands used in this procedure can output information for a long period of time, the **rtrv-asp**, **rtrv-as**, and **rtrv-assoc** commands can be canceled and the output to the terminal stopped. There are three ways that the **rtrv-asp**, **rtrv-as**, and **rtrv-assoc** commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the **rtrv-asp**, **rtrv-as**, or **rtrv-assoc** commands were entered.
- Enter the **cancel-cmd** without the **trm** parameter at the terminal where the **rtrv-asp**, **rtrv-as**, or **rtrv-assoc** commands were entered.
- Enter the **cancel-cmd:trm=<xx>**, where **<xx>** is the terminal where the **rtrv-asp**, **rtrv-as**, or **rtrv-assoc** commands were entered, from another terminal other than the terminal where the **rtrv-asp**, **rtrv-as**, or **rtrv-assoc** commands were entered. To enter the **cancel-cmd:trm=<xx>** command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the **rtrv-secu-trm** command. The user's permissions can be verified with the **rtrv-user** or **rtrv-secu-user** commands.

For more information about the **cancel-cmd** command, go to the *Commands Manual*.

Procedure

1. Display the application servers in the database using the **rtrv-as** command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
      AS Name           Mode           ASP Names
      as1              LOADSHARE    asp1
                                      asp2
                                      asp3
                                      asp5
                                      asp6
      as2              OVERRIDE     asp7

AS table is (2 of 250) 1% full.
```

2. Display the application server processes assigned to the application server in the database using the **rtrv-asp** command and specifying the name of the application server process shown in step 1. For this example, enter this command.

rtrv-asp:aspname=asp1

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP           ASSOCIATION           UAPS
asp1         swbel32                1

ASP Table is (7 of 4000) 1% full
```

3. Display the association assigned to the ASP shown in step 2 using the **rtrv-assoc** command and specifying the association name shown in the **rtrv-asp** output in step 2. For this example, enter this command.

rtrv-assoc:aname=swbel32

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME swbel32
  PORT      A
  ADAPTER   M3UA           VER           M3UA RFC
  LHOST     gw105.nc.tekelec.com
  ALHOST    ---
  RHOST     gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  LPORT     1030           RPORT         2345
  ISTRMS    2              OSTRMS        2
  RMODE     LIN           RMIN          120           RMAX          800
  RTIMES    10           CWMIN         3000
  OPEN      YES           ALW           YES

IP Appl Sock table is (4 of 4000) 1% full
```

NOTE: If the value of the `open` parameter shown in step 3 is `no`, skip this step and go to step 5.

- Change the value of the `open` parameter to `no` by specifying the `chg-assoc` command with the `open=no` parameter. For this example, enter this command.

```
chg-assoc:aname=swbel132:open=no
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD
```

NOTE: If all the ASPs and associations assigned to the application server been displayed, skip this step and go to step 6.

- Repeat steps 2 through 4 for all ASPs assigned to the application server being changed.
-

- Change the application server in the database using the `chg-as` command. For this example, enter this command

```
chg-as:aname=as1:mode=override
```

This is an example of possible inputs and outputs:

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-AS: MASP A - COMPLTD;
```

- Verify the changes using the `rtrv-as` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
      AS Name           Mode           ASP Names
      as1                LOADSHARE     asp1
                                           asp2
                                           asp3
                                           asp5
                                           asp6
      as2                OVERRIDE      asp7
AS table is (2 of 250) 1% full
```

NOTE: If the value of the `open` parameter was not changed in step 4, skip this step and go to step 9.

- Change the value of the `open` parameter to `yes` by specifying the `chg-assoc` command with the `open=yes` parameter. For this example, enter this command.

```
chg-assoc:aname=swbel132:open=yes
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

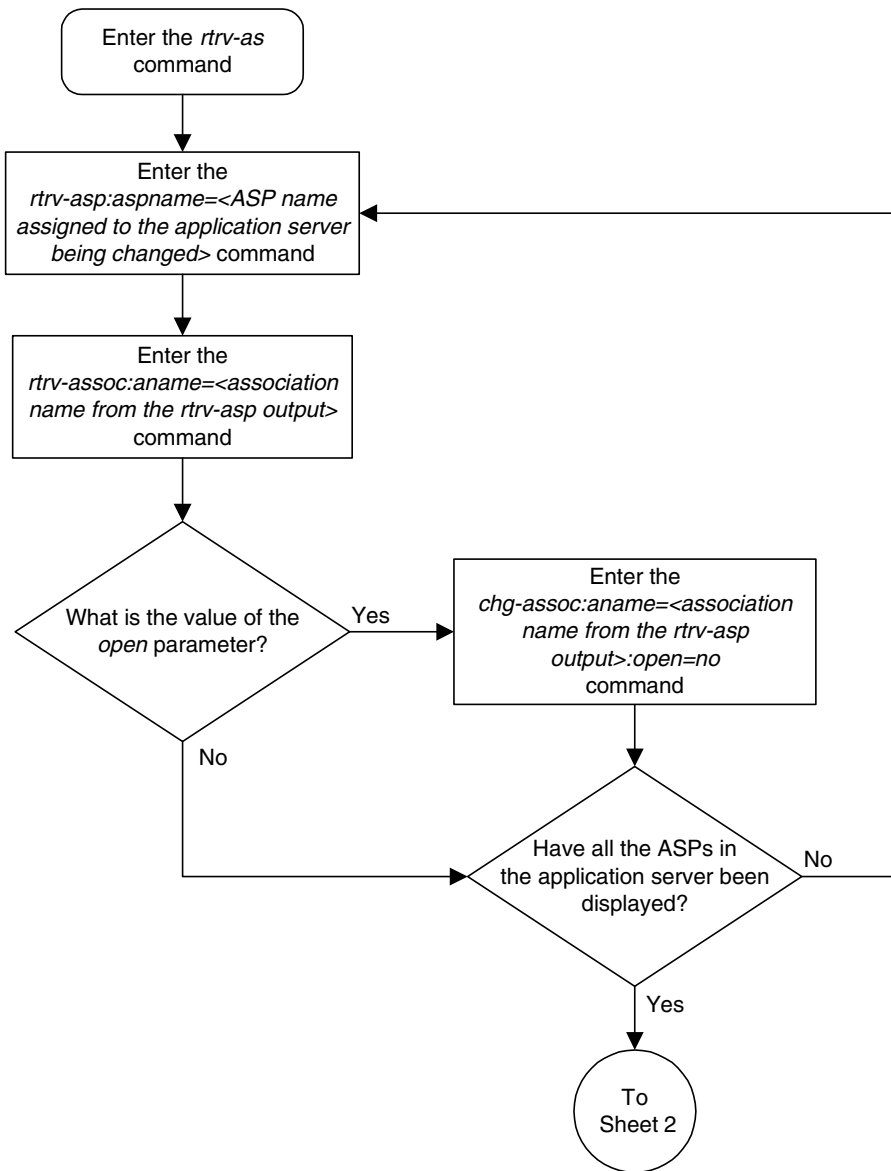
Repeat this step for all associations that were changed in step 4.

9. Back up the new changes, using the `chg-db:action=backup:dest=fixed` command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

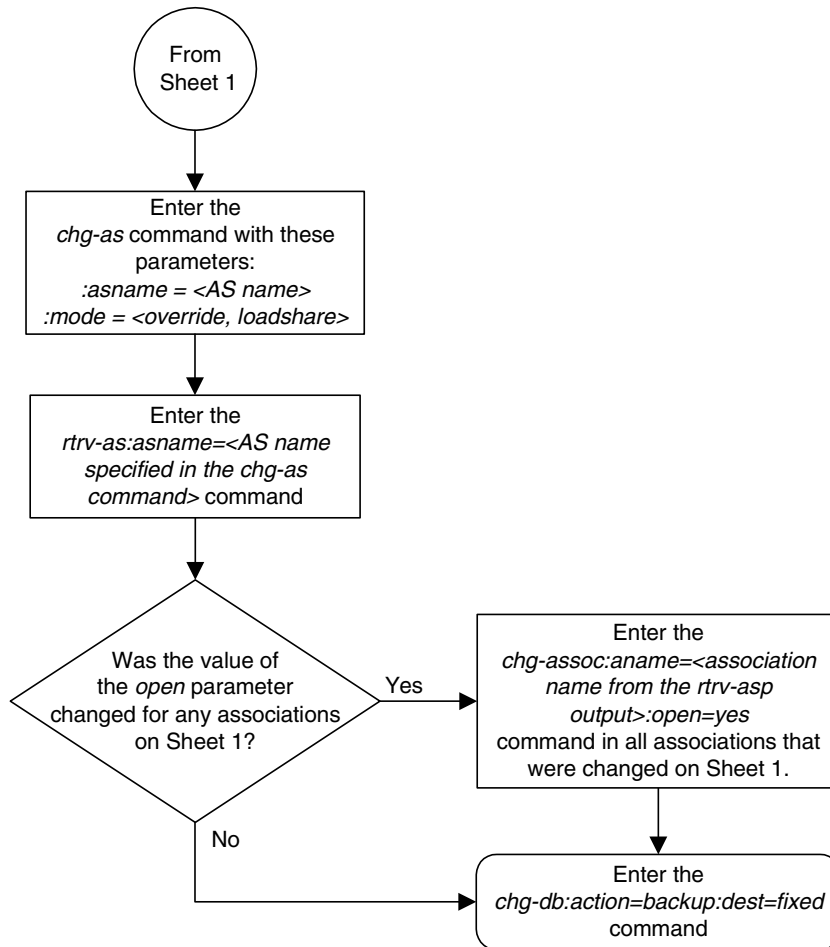
```

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

Flowchart 3-42. Changing an Application Server (Sheet 1 of 2)



Flowchart 3-42. Changing an Application Server (Sheet 2 of 2)



Adding a Network Appearance

The network appearance field identifies the SS7 network context for the message, for the purpose of logically separating the signaling traffic between the SGP (signaling gateway process) and the ASP (application server process) over a common SCTP (stream control transmission protocol) association. This field is contained in the DATA, DUNA, DAVA, DRST, DAUD, SCON, and DUPU messages.

The network appearance is provisioned in the database using the `ent-na` command with these parameters.

`:na` – the 32-bit value of the network appearance, from 0 to 4294967295.

`:type` – the network type of the network appearance, `ansi`, `itui`, `itun`, `itun24`.

`:gc` – the specific ITU-N group code associated with the network appearance.

The `gc` parameter can be specified only with the `type=itun` parameter.

The `gc` parameter must be specified with the `type=itun` parameter if the ITU Duplicate Point Code feature is on. If the ITU Duplicate Point Code feature is off, the `gc` parameter cannot be specified.

The `gc` parameter value must be shown in the `rtrv-spc` output.

Procedure

1. Display the network appearances in the database with the `rtrv-na` command. This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
TYPE GC NA
ANSI -- 100
ITUN FR 4000000000
ITUN GE 1000000000
```

NOTE: If the `gc` parameter is not being specified in this procedure, skip this step and go to step 3.

2. Display the secondary point codes in the database with the `rtrv-spc` command. This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
SPC (Secondary Point Codes)

SPCA
001-010-010
002-010-010
003-010-010

SPC-I
1-253-5
2-254-6
```

```
3-255-7
```

```
SPC-N
10-01-11-1-fr
13-02-12-0-ge
13-02-12-0-uk
```

```
SPC-N24
none
```

```
Secondary Point Code table is (9 of 40) 23% full
```

If you wish to specify a value for the **gc** parameter in step 3, and the **rtrv-spc** output does not show any ITU-N point codes with group code values, go to the "Adding a Secondary Point Code" procedure in the *Database Administration Manual - SS7* to turn the ITU Duplicate Point Code feature on, and add a secondary point code to the database with the desired group code value.

-
3. Add the network appearance to the database with the **ent-na** command. If the **gc** parameter is specified with the **ent-na** command, the **gc** parameter value must be assigned to an ITU-N point code (SPC-N) shown in the **rtrv-spc** output in step 2. For this example, enter these commands.

```
ent-na:na=1000:type=itui
ent-na:na=3:type=itun24
ent-na:na=150000:type=itun:gc=uk
```

When each of these commands have successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ENT-NA: MASP A - COMPLTD
```

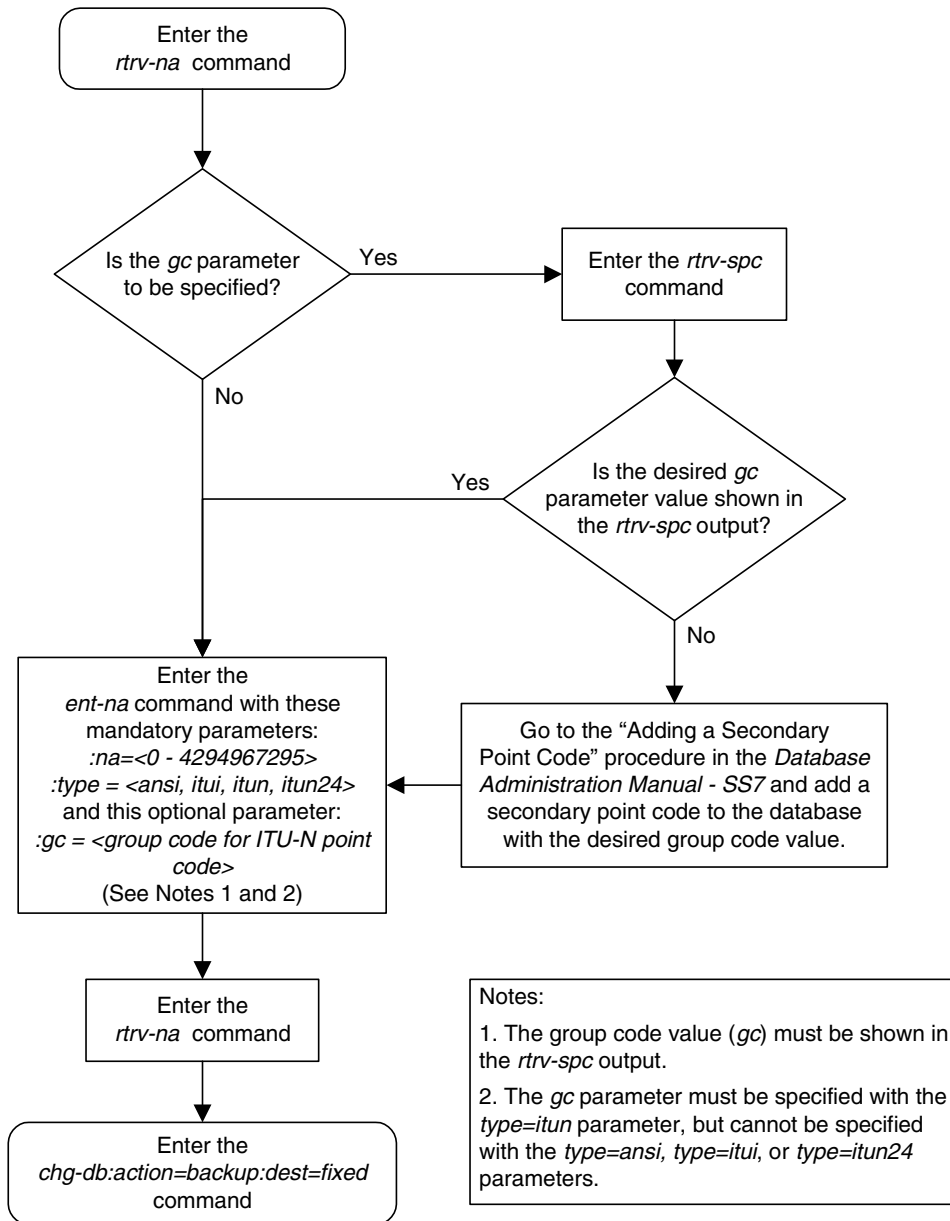
-
4. Verify the changes using the **rtrv-na** command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
TYPE      GC      NA
ANSI      --      100
ITUI      --      1000
ITUN      UK      150000
ITUN      FR      4000000000
ITUN      GE      10000000000
ITUN24    --      3
```

-
5. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-43. Adding a Network Appearance



Removing a Network Appearance

This procedure removes the network appearance from the database using the `dlt-na` command with these parameters.

`:na` – the 32-bit value of the network appearance, from 0 to 4294967295.

`:type` – the network type of the network appearance, `ansi`, `itui`, `itun`, `itun24`.

`:gc` – the specific ITU-N group code associated with the network appearance.

Specifying the `gc` parameter removes the specific network appearance containing the `na` and `gc` parameter values.

Specifying the `type=itun` parameter without the `gc` parameter removes all ITU-N network appearances containing the specified `na` parameter value.

Procedure

1. Display the network appearances in the database with the `rtrv-na` command. This is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
TYPE      GC          NA
ANSI      --          100
ITUI      --          1000
ITUN      UK          150000
ITUN      FR          4000000000
ITUN      GE          1000000000
ITUN24    --           3
```

2. Remove the network appearance from the database with the `dlt-na` command. For this example, enter these commands.

```
dlt-na:na=100:type=ansi
```

```
dlt-na:na=4000000000:type=itun:gc=fr
```

When each of these commands have successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
DLT-NA:  MASP A - COMPLTD
```

3. Verify the changes using the `rtrv-na` command. This is an example of possible output.

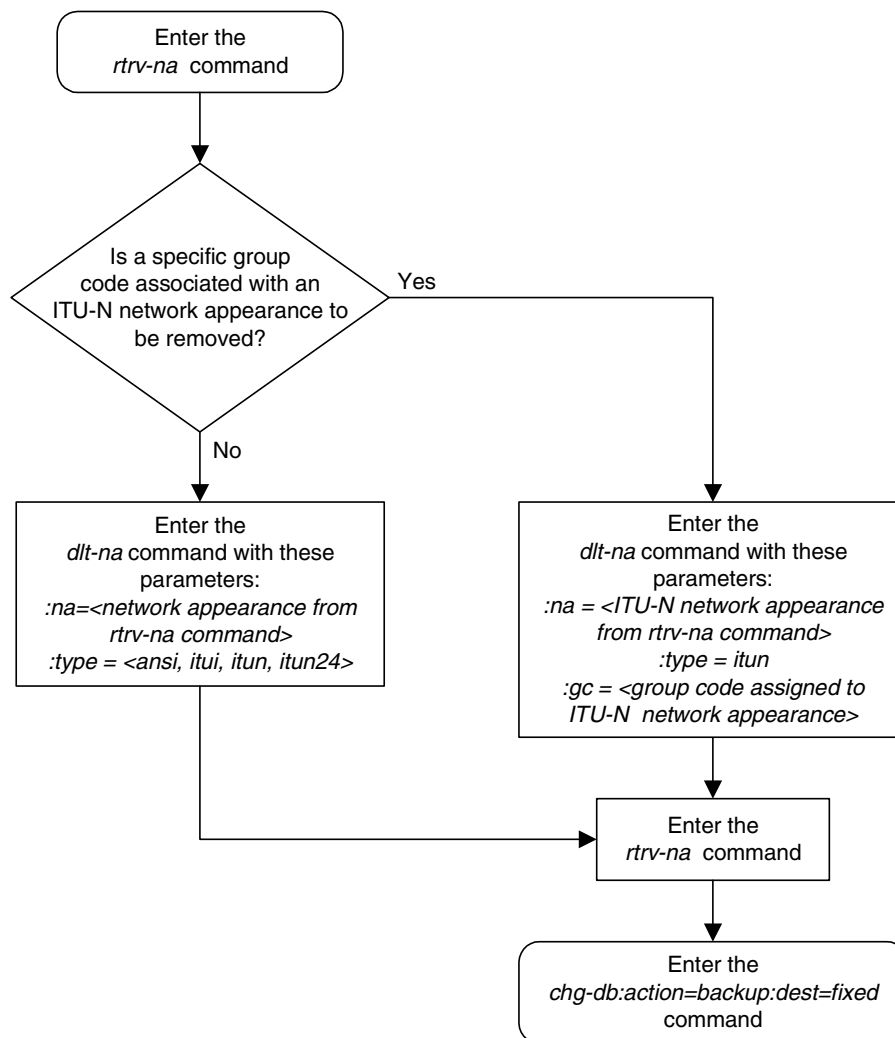
```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
TYPE      GC          NA
ITUI      --          1000
ITUN      UK          150000
ITUN      GE          1000000000
ITUN24    --           3
```

4. Back up the new changes, using the `chg-db:action=backup:dest=fixed` command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```

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

Flowchart 3-44. Removing a Network Appearance



Changing the SCTP Checksum Algorithm Option

Use this procedure to change the SCTP checksum algorithm, either Adler-32 or CRC-32c, applied to traffic on SCTP associations. The `sctpchecksum` parameter of the `chg-sg-opts` command is used to change this option. This option is a system-wide option that applies to associations assigned to IP cards running the IPLIM, IPLIMI, SS7IPGW, and IPGWI applications.

Once the SCTP checksum option has been changed, the associations on each IP card need to be reset by changing the `open` parameter value for each association to `no`, then back to `yes`. This ensures that the associations on the IP card are using the new SCTP checksum algorithm.

Canceling the `RTRV-ASSOC` Command

Because the `rtrv-assoc` command used in this procedure can output information for a long period of time, the `rtrv-assoc` command can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-assoc` command can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-assoc` command was entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-assoc` command was entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-assoc` command was entered, from another terminal other than the terminal where the `rtrv-assoc` command was entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the current IP options in the database by entering the `rtrv-sg-opts` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SYNC:          TALI
SRKQ:          250
DRKQ:          750
SNMPCONT:     john doe 555-123-4567
GETCOMM:      public
SETCOMM:      private
TRAPCOMM:     public
INHFEPALM:    NO
SCTPCSUM:     adler32
IPGWABATE:    NO
IPLIMABATE:   NO
IPTPSALMTHRESH: 80
```

2. Display the cards in the system by entering the `rtrv-card` command. This is an example of the possible output.

```
rlghncxa03w 04-12-15 16:34:56 GMT EAGLE5 31.10.0
CARD  TYPE      APPL  LSET NAME  PORT SLC  LSET NAME  PORT SLC
1101  TSM           SCCP  -----  --  --  -----  --  --
1102  TSM           GLS   -----  --  --  -----  --  --
1103  ACMENET      STPLAN -----  --  --  -----  --  --
1104  ACMENET      STPLAN -----  --  --  -----  --  --
1113  GSPM         EOAM  -----  --  --  -----  --  --
1114  TDM-A
1115  GSPM         EOAM  -----  --  --  -----  --  --
1116  TDM-B
1117  MDAL
1201  LIMDS0       SS7ANSI lsn1      A    0    lsn2      B    1
-----  --  --  -----  --  --
-----  --  --  -----  --  --
-----  --  --  -----  --  --
1202  DCM          IPLIM  ipnode2   A    1    -----  --  --
-----  --  --  -----  --  --
-----  --  --  -----  --  --
-----  --  --  -----  --  --
1203  LIMV35       SS7ANSI lsn2      A    0    lsn1      B    1
1204  LIMATM       ATMANSI atmgwy    A    0    -----  --  --
1205  DCM          IPLIM  ipnode1   A    0    ipnode3   B    1
-----  --  --  -----  --  --
-----  --  --  -----  --  --
-----  --  --  -----  --  --
1207  DCM          IPLIM  ipnode2   A    0    -----  --  --
-----  --  --  -----  --  --
-----  --  --  -----  --  --
-----  --  --  -----  --  --
1303  DCM          IPLIM  ipnode3   A    0    ipnode1   B    1
-----  --  --  -----  --  --
-----  --  --  -----  --  --
-----  --  --  -----  --  --
1305  DCM          IPLIM  ipnode4   A    0    -----  --  --
-----  --  --  -----  --  --
-----  --  --  -----  --  --
-----  --  --  -----  --  --
```

```

1308   DCM      IPLIM      -----   --  --   ipnode3      B   2
                                     ipnode1      A1  2   -----   --  --
                                     -----   --  --   ipnode4      B2  1
                                     -----   --  --   -----   --  --
1315   DCM      SS7IPGW   ipgtwy1      A   --   -----   --  --
1317   DCM      IPGWI     ipgtwy2      A   --   -----   --  --

```

Record the card location, shown in the **LOC** column, and signaling link port, shown in the **PORT** column, information for all cards running the IPLIM, IPLIMI, SS7IPGW, and IPGWI applications.

NOTE: If no cards running the IPLIM or IPLIMI applications are shown in the `rtrv-card` output in step 2, skip steps 3 through 16 and go to step 17.

3. Change the SCTP checksum option in the database using the `chg-sg-opts` command. For this example, enter this command.

```
chg-sg-opts:sctpcsum=crc32c
```

When this command has successfully completed, the following message should appear.

```

rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
CHG-SG-OPTS: MASP A - COMPLTD

```

4. Verify that the SCTP checksum algorithm was changed using the `rtrv-sg-opts` command. The SCTP checksum algorithm option value is shown in the **SCTPCSUM** parameter. The following is an example of the possible output.

```

rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SYNC:          TALI
SRKQ:          250
DRKQ:          750
SNMPCONT:      john doe 555-123-4567
GETCOMM:       public
SETCOMM:       private
TRAPCOMM:      public
INHFEPPALM:   NO
SCTPCSUM:      crc32c
IPGWABATE:     NO
IPLIMABATE:    NO
IPTPSALMTHRESH: 80

```

5. Select one of the IP cards shown in the `rtrv-card` output in step 2 running the IPLIM or IPLIMI applications. Place the signaling links on this card out of service using the `dact-slk` command. For this example, enter these commands.

```
dact-slk:loc=1308:port=a1
```

```
dact-slk:loc=1308:port=b
```

```
dact-slk:loc=1308:port=b2
```

When these commands have successfully completed, this message appears.

```

rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
Deactivate Link message sent to card

```

6. Display the IP addresses of the IP links in the database by entering the **rtrv-ip-lnk** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
LOC  PORT  IPADDR          SUBMASK          DUPLEX  SPEED  MACTYPE  AUTO  MCAST
-----
1202  A    192.001.001.010 255.255.255.0   HALF    10     DIX      NO   NO
1202  B    -----          -----          HALF    10     DIX      NO   NO
1205  A    192.001.001.012 255.255.255.0   HALF    10     DIX      NO   NO
1205  B    -----          -----          HALF    10     DIX      NO   NO
1207  A    192.001.001.014 255.255.255.0   HALF    10     DIX      NO   NO
1207  B    -----          -----          HALF    10     DIX      NO   NO
1303  A    192.001.001.020 255.255.255.0   HALF    10     DIX      NO   NO
1303  B    -----          -----          HALF    10     DIX      NO   NO
1305  A    192.001.001.022 255.255.255.0   HALF    10     DIX      NO   NO
1305  B    -----          -----          HALF    10     DIX      NO   NO
1308  A    192.001.001.024 255.255.255.0   HALF    10     DIX      NO   NO
1308  B    -----          -----          HALF    10     DIX      NO   NO
1315  A    192.001.001.050 255.255.255.0   HALF    10     DIX      NO   NO
1315  B    -----          -----          HALF    10     DIX      NO   NO
1317  A    192.001.001.052 255.255.255.0   HALF    10     DIX      NO   NO
1317  B    -----          -----          HALF    10     DIX      NO   NO
```

IP-LNK table is (16 of 512) 3% full.

7. Display the current IP host information in the database by entering the **rtrv-ip-host** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
IPADDR          HOST
192.1.1.10      IPNODE1-1201
192.1.1.12      IPNODE1-1203
192.1.1.14      IPNODE1-1205
192.1.1.20      IPNODE2-1201
192.1.1.22      IPNODE2-1203
192.1.1.24      IPNODE2-1205
192.1.1.32      KC-HLR2
192.1.1.50      DN-MS1
192.1.1.52      DN-MS2
```

IP Host table is (9 of 512) 2% full

8. Display the associations assigned to the IP card specified in step 5, using the **rtrv-assoc** command with the local host name of the associations assigned to the IP card. To find the local host name of the association, the card location of the IP card is assigned to an IP address in the IP link table (**rtrv-ip-lnk** output). The IP address is assigned to a hostname in the IP host table (**rtrv-ip-host** output).

For this example, the local host name of associations assigned to the IP card 1308 (the card specified in step 5) is IPNODE2-1205. Enter this command.

```
rtrv-assoc:lhost=ipnode2-1205
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME assoc2
  PORT      A1
  ADAPTER   MP2A
  LHOST     ipnode2-1205
  ALHOST    ---
  RHOST     remotehost2
  LPORT     2187          RPORT     1025
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000          M2PATSET  5
  OPEN      YES         ALW        YES

rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
ANAME assoc4
  PORT      B
  ADAPTER   MP2A
  LHOST     ipnode2-1205
  ALHOST    ---
  RHOST     remotehost1
  LPORT     3290          RPORT     1025
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000          M2PATSET  5
  OPEN      YES         ALW        YES

ANAME assoc5
  PORT      B2
  ADAPTER   MP2A
  LHOST     ipnode2-1205
  ALHOST    ---
  RHOST     remotehost1
  LPORT     1057          RPORT     1025
  ISTRMS    2            OSTRMS    2
  RMODE     LIN          RMIN      120          RMAX      800
  RTIMES    10          CWMIN     3000          M2PATSET  5
  OPEN      YES         ALW        YES

IP Appl Sock/Assoc table is (9 of 4000) 1% full
```

9. Change the value of the **open** parameter of the associations shown in step 8 to **no** by specifying the **chg-assoc** command with the **open=no** parameter. For this example, enter this command.

```
chg-assoc : aname=assoc2 : open=no
```

```
chg-assoc : aname=assoc4 : open=no
```

```
chg-assoc : aname=assoc5 : open=no
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```


10. Change the value of the **open** parameter of the associations changed in step 9 to **yes** by specifying the **chg-assoc** command with the **open=yes** parameter. For this example, enter this command.

```
chg-assoc:aname=assoc2:open=yes
chg-assoc:aname=assoc4:open=yes
chg-assoc:aname=assoc5:open=yes
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

11. Verify that the IP card is using the new SCTP checksum algorithm by entering the **sctp -g csum** pass command with the location of the IP card. For this example, enter this command.

```
pass:loc=1308:cmd="sctp -g csum"
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
PASS: Command sent to card
```

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
```

```
Checksum Algorithm is crc32c
```

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
```

```
SCTP command complete
```

If the IP card is not using the new SCTP checksum algorithm, contact Tekelec Technical Services. See "Tekelec Technical Services" on page 1-8.

12. Put the signaling links that were placed out of service in step 5 back into service using the **act-slk** command. For example, enter this command.

```
act-slk:loc=1308:port=a1
act-slk:loc=1308:port=b
act-slk:loc=1308:port=b2
```

When these commands have successfully completed, this message appears.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Activate Link message sent to card
```

13. Verify the in-service normal (IS-NR) status of the signaling link by using the **rept-stat-slk** command and specifying the card location and port values specified in step 12. For example, enter these commands.

```
rept-stat-slk:loc=1308:port=a1
```

This message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1308,A1  ipnode1  -----  IS-NR    Avail    ----
Command Completed.
```

```
rept-stat-slk:loc=1308:port=b
```

This message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1308,B  ipnode3  -----  IS-NR    Avail    ----
Command Completed.
```

```
rept-stat-slk:loc=1308:port=b2
```

This message should appear.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1308,B2 ipnode4  -----  IS-NR    Avail    ----
Command Completed.
```

14. Enter the `netstat -p sctp` pass command with the card location of the IP card to determine if any errors have occurred. For this example, enter this command.

```
pass:loc=1308:cmd="netstat -p sctp"
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0

SCTP:
  0 ip packets sent
    0 ip packets sent with data chunk
    0 control chunks (excludes retransmissions)
    0 ordered data chunks (excludes retransmissions)
    0 unordered data chunks (excludes retransmissions)
    0 user messages fragmented due to MTU
    0 retransmit data chunks sent
    0 sacks sent
    0 send failed
  0 ip packets received
    0 ip packets received with data chunk
    0 control chunks (excludes duplicates)
    0 ordered data chunks (excludes duplicates)
    0 unordered data chunks (excludes duplicates)
    0 user messages reassembled
    0 data chunks read
    0 duplicate tsns received
    0 sacks received
    0 gap ack blocks received
    0 out of the blue
    0 with invalid checksum
  0 connections established
    0 by upper layer
    0 by remote endpoint
  0 connections terminated
    0 ungracefully
    0 gracefully
  0 associations supported
  0 associations dropped due to retransmits
  0 consecutive retransmit timeouts
  0 retransmit timer count
  0 fast retransmit count
  0 heartbeat requests received
  0 heartbeat acks received
```

IP⁷ Secure Gateway Configuration Procedures

```
0 heartbeat requests sent
0 milliseconds cookie life at 4-way start-up handshake
0 retransmission attempts are allowed at start-up phase
```

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

```
NETSTAT command complete
```

If errors are shown in the pass command output, contact Tekelec Technical Services. See "Tekelec Technical Services" on page 1-8.

-
- 15.** Repeat steps 5 through 14 to update the other IP cards in the system running the IPLIM and IPLIMI applications with the new SCTP checksum algorithm.

Once all the IP cards running the IPLIM and IPLIMI applications have been updated, and if the **rtrv-card** output in step 2 does not show any cards running the SS7IPGW or IPGWI applications, this procedure is finished after the database is backed up in step 16.

If the **rtrv-card** output in step 2 shows cards running the SS7IPGW or IPGWI applications, skip step 16 and go to step 17.

-
- 16.** Back up the database by entering the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

-
- 17.** At the IP near end node, stop all traffic to one of the IP cards running the SS7IPGW or IPGWI applications on the IP⁷ Secure Gateway.

-
- 18.** At the IP⁷ Secure Gateway, enter the **msucount -1** pass command with the card location of the IP card selected in step 17. For this example, enter this command.

```
pass:loc=1315:cmd="msucount -1"
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
PASS: Command sent to card
```

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
MSUCOUNT: Command In Progress
```

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

```
MSUCOUNT: MSU Count Report
```

```
-----
Link Measurements (Port A)
```

```

-----
Transmit Counts
-----
tx bytes:                927186
tx msus:                  35661
tx average rate (msus/second): 00441

Receive Counts
-----
rcv bytes:                775302
rcv msus:                  29826
rcv average rate (msus/second): 00342

Reroute Counts
-----
msus sent to mate cards: 00000
msus received from mate cards: 00000

MGMT Primitive Totals
-----
MTPP primitives received      00000
MTPP primitives discarded     00000
MTPP primitives transmitted   00000
RKRK primitives received      00000
RKRK primitives discarded     00000
RKRK dynamic route key table updates 00000

Transmit Discard Counts
-----
discarded tx due to special adjpc msu: 00000
discarded tx due to discard all adjpc msu: 00000
discarded tx due to no ss7 rtbl entry: 00000
discarded tx due to no ss7 rtkey: 00001
discarded tx due to no conn avail to pc: 00000
discarded tx due to no conn avail to rtkey:00001
discarded tx due to congested connection: 00000
discarded tx due to sccp msg type: 00000
discarded tx due to sccp class: 00001
discarded tx due to circular rte: 00000
discarded tx due to normalization error: 00000
discarded tx due to invalid traffic type: 00000
discarded tx due to M3UA conversion error: 00001
discarded tx due to SUA conversion error: 00000
discarded tx due to AS-Pending overflow: 00000
discarded tx due to AS timer Tr expiry: 00000
discarded tx due to reroute failure: 00000

Receive Discard Counts
-----
discarded rcv due to link state: 00000
discarded rcv due to sccp msg type: 00001
discarded rcv due to sccp class: 00003
discarded rcv due to sccp called party: 00004
discarded rcv due to sccp calling party: 00021
discarded rcv due to isup sio: 00011
discarded rcv due to normalization error: 00000
discarded rcv due to error in XSRV packet: 00000
discarded rcv due to M3UA PDU error: 00001
discarded rcv due to SUA PDU error: 00000
discarded rcv due to invalid rcontext 00000

```

IP7 Secure Gateway Configuration Procedures

```
Stored Transmit Discard Data
-----
83 01 05 05 0a 01 03 bf 09 80 03 08 0d 05 c3 07
01 05 05 05 c3 07 0a 01 03 08 e2 06 c7 04 13 10
```

```
Stored Receive Discard Data
-----
53 41 53 49 73 63 63 70 1a 00 09 01 03 08 0d 05
c3 05 0a 01 03 05 c3 05 01 05 05 08 e2 06 c7 04
```

END of Report

-
- 19.** Display the IP addresses of the IP links in the database by entering the **rtrv-ip-lnk** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
LOC   PORT IPADDR          SUBMASK          DUPLEX  SPEED  MACTYPE AUTO  MCAST
-----
1202  A    192.001.001.010  255.255.255.0   HALF    10    DIX    NO   NO
1202  B    -----
1205  A    192.001.001.012  255.255.255.0   HALF    10    DIX    NO   NO
1205  B    -----
1207  A    192.001.001.014  255.255.255.0   HALF    10    DIX    NO   NO
1207  B    -----
1303  A    192.001.001.020  255.255.255.0   HALF    10    DIX    NO   NO
1303  B    -----
1305  A    192.001.001.022  255.255.255.0   HALF    10    DIX    NO   NO
1305  B    -----
1308  A    192.001.001.024  255.255.255.0   HALF    10    DIX    NO   NO
1308  B    -----
1315  A    192.001.001.050  255.255.255.0   HALF    10    DIX    NO   NO
1315  B    -----
1317  A    192.001.001.052  255.255.255.0   HALF    10    DIX    NO   NO
1317  B    -----
```

IP-LNK table is (16 of 512) 3% full.

-
- 20.** Display the current IP host information in the database by entering the **rtrv-ip-host** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
IPADDR          HOST
192.1.1.10      IPNODE1-1201
192.1.1.12      IPNODE1-1203
192.1.1.14      IPNODE1-1205
192.1.1.20      IPNODE2-1201
192.1.1.22      IPNODE2-1203
192.1.1.24      IPNODE2-1205
192.1.1.32      KC-HLR2
192.1.1.50      DN-MS1
192.1.1.52      DN-MS2
```

IP Host table is (9 of 512) 2% full

21. Display the associations assigned to the IP card specified in step 18, using the `rtrv-assoc` command with the local host name of the associations assigned to the IP card. To find the local host name of the association, the card location of the IP card is assigned to an IP address in the IP link table (`rtrv-ip-lnk` output). The IP address is assigned to a hostname in the IP host table (`rtrv-ip-host` output).

For this example, the local host name of associations assigned to the IP card 1315 (the card specified in step 18) is DN-MSCL. Enter this command.

```
rtrv-assoc: lhost=dn-mscl
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
ANAME assoc3
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     dn-mscl
  ALHOST    ---
  RHOST     remotehost2
  LPORT     2345          RPORT    1025
  ISTRMS    2            OSTRMS   2
  RMODE     LIN          RMIN     120          RMAX     800
  RTIMES    10          CWMIN    3000
  OPEN      YES          ALW      YES

ANAME assoc6
  PORT      A
  ADAPTER   SUA          VER      SUA RFC
  LHOST     dn-mscl
  ALHOST    host3
  RHOST     remotehost2
  LPORT     4156          RPORT    1025
  ISTRMS    2            OSTRMS   2
  RMODE     LIN          RMIN     120          RMAX     800
  RTIMES    10          CWMIN    3000
  OPEN      YES          ALW      YES

IP Appl Sock/Assoc table is (9 of 4000) 1% full
```

22. At the IP⁷ Secure Gateway, enter the `msucount -s` pass command with the card location specified in step 18 and the association names shown in step 21. For this example, enter this command.

```
pass:loc=1315:cmd="msucount -s assoc3"
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
PASS: Command sent to card
```

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
MSUCOUNT: Command In Progress
```

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
```

```
MSUCOUNT: MSU Count Report
```

```
-----
Socket Name Measurements
-----
```

```
Transmit Counts
-----
```

```
tx bytes:                320294
tx msus:                  12319
```

```
Transmit Discard Counts
-----
```

```
discarded tx due to sccp msg type:    00000
discarded tx due to sccp class:       00000
discarded tx due to normalization error: 00000
discarded tx due to invalid traffic type: 00000
discarded tx due to M3UA conversion error: 00000
discarded tx due to SUA conversion error: 00001
```

```
Receive Counts
-----
```

```
rcv bytes:                167681
rcv msus:                  06451
```

```
Receive Discard Counts
-----
```

```
discarded rcv due to link state:      00000
discarded rcv due to sccp msg type:   00000
discarded rcv due to sccp class:      00000
discarded rcv due to sccp called party: 00000
discarded rcv due to sccp calling party: 00003
discarded rcv due to isup sio:        00004
discarded rcv due to normalization error: 00000
discarded rcv due to error in XSRV packet: 00000
discarded rcv due to M3UA PDU error:  00000
discarded rcv due to SUA PDU error:   00001
```

```
Stored Transmit Discard Data
-----
```

```
no stored transmit discard data
```

```
Stored Receive Discard Data
-----
```

```
53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00
```

```
53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
```

```

05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00
53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00
53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00
53 41 53 49 73 63 63 70 17 00 09 80 03 08 0a 05
c3 05 0a 01 03 02 c1 05 08 e2 06 c7 04 00 00 00
53 41 53 49 73 63 63 70 17 00 09 80 03 08 0a 05
c3 05 0a 01 03 02 c1 05 08 e2 06 c7 04 00 00 00
53 41 53 49 73 63 63 70 17 00 09 80 03 08 0a 05
c3 05 0a 01 03 02 c1 05 08 e2 06 c7 04 00 00 00

```

END of Report

pass:loc=1315:cmd="msucount -s assoc6"

The following is an example of the possible output.

```

rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
PASS: Command sent to card

```

```

rlgh
ncxa03w 04-06-28 21:17:37 GMT EAGLE5 31.10.0
MSUCOUNT: Command In Progress

```

```

rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0

```

MSUCOUNT: MSU Count Report

```

-----
Socket Name Measurements
-----

```

Transmit Counts

```

-----
tx bytes:                               320294
tx msus:                                 12319

```

Transmit Discard Counts

```

-----
discarded tx due to sccp msg type:       00000
discarded tx due to sccp class:          00000
discarded tx due to normalization error: 00000
discarded tx due to invalid traffic type: 00000
discarded tx due to M3UA conversion error: 00000
discarded tx due to SUA conversion error: 00001

```

Receive Counts

```

-----
rcv bytes:                               167681
rcv msus:                                 06451

```

Receive Discard Counts

```

-----
discarded rcv due to link state:         00000
discarded rcv due to sccp msg type:      00000

```


IP⁷ Secure Gateway Configuration Procedures

```
discarded rcv due to sccp class:          00000
discarded rcv due to sccp called party:   00000
discarded rcv due to sccp calling party:  00003
discarded rcv due to isup sio:           00004
discarded rcv due to normalization error: 00000
discarded rcv due to error in XSRV packet: 00000
discarded rcv due to M3UA PDU error:      00000
discarded rcv due to SUA PDU error:       00001
```

Stored Transmit Discard Data

no stored transmit discard data

Stored Receive Discard Data

53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00

53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00

53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00

53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00

53 41 53 49 73 63 63 70 17 00 09 80 03 08 0a 05
c3 05 0a 01 03 02 c1 05 08 e2 06 c7 04 00 00 00

53 41 53 49 73 63 63 70 17 00 09 80 03 08 0a 05
c3 05 0a 01 03 02 c1 05 08 e2 06 c7 04 00 00 00

53 41 53 49 73 63 63 70 17 00 09 80 03 08 0a 05
c3 05 0a 01 03 02 c1 05 08 e2 06 c7 04 00 00 00

END of Report

-
23. At the IP near end node, disconnect all the associations attached to the IP card specified in step 22.

-
24. At the IP⁷ Secure Gateway, place the signaling link on this IP card out of service using the **dact-slk** command. For this example, enter this command.

```
dact-slk:loc=1315:port=a
```

When this command has successfully completed, this message appears.

```
rlghncxa03w 04-12-12 09:12:36 GMT EAGLE5 31.10.0
Deactivate Link message sent to card
```

NOTE: If the `chg-sg-opts` command was executed in step 3, skip steps 25 and 26, and go to step 27.

25. Change the SCTP checksum option in the database using the `chg-sg-opts` command. For this example, enter this command.

```
chg-sg-opts:sctpcsum=crc32c
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:19:37 GMT EAGLE5 31.10.0
CHG-SG-OPTS: MASP A - COMPLTD
```

26. Verify that the SCTP checksum algorithm was changed using the `rtrv-sg-opts` command. The SCTP checksum algorithm option value is shown in the `SCTPCSUM` parameter. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SYNC:          TALI
SRKQ:          250
DRKQ:          750
SNMPCONT:      john doe 555-123-4567
GETCOMM:       public
SETCOMM:       private
TRAPCOMM:      public
INHFEPALM:    NO
SCTPCSUM:      crc32c
IPGWABATE:     NO
IPLIMABATE:    NO
IPTPSALMTHRESH: 80
```

27. Change the value of the `open` parameter of the associations shown in step 21 to `no` by specifying the `chg-assoc` command with the `open=no` parameter. For this example, enter this command.

```
chg-assoc:aname=assoc3:open=no
```

```
chg-assoc:aname=assoc6:open=no
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

28. Change the value of the `open` parameter of the associations changed in step 27 to `yes` by specifying the `chg-assoc` command with the `open=yes` parameter. For this example, enter this command.

```
chg-assoc:aname=assoc3:open=yes
```

```
chg-assoc:aname=assoc6:open=yes
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-ASSOC: MASP A - COMPLTD;
```

29. Verify that the IP card is using the new SCTP checksum algorithm by entering the **sctp -g csum** pass command with the location of the IP card. For this example, enter this command.

```
pass:loc=1315:cmd="sctp -g csum"
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
PASS: Command sent to card
;

rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0

Checksum Algorithm is crc32c
;

rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0

SCTP command complete
```

If the IP card is not using the new SCTP checksum algorithm, contact Tekelec Technical Services. See "Tekelec Technical Services" on page 1-8.

-
30. At the IP near end node, configure all the associations attached to the IP card specified in step 29 to use the SCTP checksum algorithm.

-
31. Put the signaling link that was placed out of service in step 24 back into service using the **act-slk** command. For example, enter this command.

```
act-slk:loc=1315:port=a
```

When this command has successfully completed, this message appears.

```
rlghncxa03w 04-12-07 11:11:28 GMT EAGLE5 31.10.0
Activate Link message sent to card
```

-
32. Verify the in-service normal (IS-NR) status of the signaling link by using the **rept-stat-slk** command and specifying the card location and port value specified in step 31. For example, enter this command.

```
rept-stat-slk:loc=1315:port=a
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
SLK      LSN      CLLI      PST      SST      AST
1315,A   ipgtwy1  -----  IS-NR    Avail    ----
Command Completed.
```

-
33. At the IP near end node, connect one of the associations attached to the IP card specified in step 31.
-

34. At the IP⁷ Secure Gateway, enter the **rept-stat-assoc** command specifying the association names specified with the **chg-assoc** command in steps 27 and 28 to verify that the association is established with the IP near end node. For this example, enter this command.

```
rept-stat-assoc:aname=assoc3
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
ASSOCIATION      PST          SST
assoc3           IS-NR       -----
Command Completed.
```

```
rept-stat-assoc:aname=assoc6
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
ASSOCIATION      PST          SST
assoc6           IS-NR       -----
Command Completed.
```

35. Enter the **netstat -p sctp** pass command with the card location of the IP card to determine if any errors have occurred. For this example, enter this command.

```
pass:loc=1315:cmd="netstat -p sctp"
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0

SCTP:
  0 ip packets sent
    0 ip packets sent with data chunk
    0 control chunks (excludes retransmissions)
    0 ordered data chunks (excludes retransmissions)
    0 unordered data chunks (excludes retransmissions)
    0 user messages fragmented due to MTU
    0 retransmit data chunks sent
    0 sacks sent
    0 send failed
  0 ip packets received
    0 ip packets received with data chunk
    0 control chunks (excludes duplicates)
    0 ordered data chunks (excludes duplicates)
    0 unordered data chunks (excludes duplicates)
    0 user messages reassembled
    0 data chunks read
    0 duplicate tsns received
    0 sacks received
    0 gap ack blocks received
    0 out of the blue
    0 with invalid checksum
  0 connections established
    0 by upper layer
    0 by remote endpoint
  0 connections terminated
    0 ungracefully
    0 gracefully
  0 associations supported
```

IP⁷ Secure Gateway Configuration Procedures

```
0 associations dropped due to retransmits
0 consecutive retransmit timeouts
0 retransmit timer count
0 fast retransmit count
0 heartbeat requests received
0 heartbeat acks received
0 heartbeat requests sent
0 milliseconds cookie life at 4-way start-up handshake
0 retransmission attempts are allowed at start-up phase
```

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

```
NETSTAT command complete
```

If errors are shown in the pass command output, contact Tekelec Technical Services. See "Tekelec Technical Services" on page 1-8.

36. At the IP near end node, connect all the other associations attached to the IP card specified in step 35.

37. At the IP near end node, activate one of the associations attached to the IP card specified in step 35.

38. At the IP⁷ Secure Gateway, enter the `msucount -1` pass command with the card location of the IP card specified in step 35. For this example, enter this command.

```
pass:loc=1315:cmd="msucount -1"
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
PASS: Command sent to card
```

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
MSUCOUNT: Command In Progress
```

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

```
MSUCOUNT: MSU Count Report
```

```
-----
Link Measurements (Port A)
-----
```

```
Transmit Counts
```

```
-----
tx bytes:                927186
tx msus:                  35661
tx average rate (msus/second): 00441
```

```
Receive Counts
```

```
-----
rcv bytes:                775302
rcv msus:                  29826
rcv average rate (msus/second): 00342
```

Reroute Counts

```
-----
msus sent to mate cards:          00000
msus received from mate cards:    00000
```

MGMT Primitive Totals

```
-----
MTPP primitives received          00000
MTPP primitives discarded         00000
MTPP primitives transmitted       00000
RKRK primitives received          00000
RKRK primitives discarded         00000
RKRK dynamic route key table updates 00000
```

Transmit Discard Counts

```
-----
discarded tx due to special adjpc msu: 00000
discarded tx due to discard all adjpc msu: 00000
discarded tx due to no ss7 rtbl entry: 00000
discarded tx due to no ss7 rtkey: 00001
discarded tx due to no conn avail to pc: 00000
discarded tx due to no conn avail to rtkey:00001
discarded tx due to congested connection: 00000
discarded tx due to sccp msg type: 00000
discarded tx due to sccp class: 00001
discarded tx due to circular rte: 00000
discarded tx due to normalization error: 00000
discarded tx due to invalid traffic type: 00000
discarded tx due to M3UA conversion error: 00001
discarded tx due to SUA conversion error: 00000
discarded tx due to AS-Pending overflow: 00000
discarded tx due to AS timer Tr expiry: 00000
discarded tx due to reroute failure: 00000
```

Receive Discard Counts

```
-----
discarded rcv due to link state: 00000
discarded rcv due to sccp msg type: 00001
discarded rcv due to sccp class: 00003
discarded rcv due to sccp called party: 00004
discarded rcv due to sccp calling party: 00021
discarded rcv due to isup sio: 00011
discarded rcv due to normalization error: 00000
discarded rcv due to error in XSRV packet: 00000
discarded rcv due to M3UA PDU error: 00001
discarded rcv due to SUA PDU error: 00000
discarded rcv due to invalid rcontext 00000
```

Stored Transmit Discard Data

```
-----
83 01 05 05 0a 01 03 bf 09 80 03 08 0d 05 c3 07
01 05 05 05 c3 07 0a 01 03 08 e2 06 c7 04 13 10
```

Stored Receive Discard Data

```
-----
53 41 53 49 73 63 63 70 1a 00 09 01 03 08 0d 05
c3 05 0a 01 03 05 c3 05 01 05 05 08 e2 06 c7 04
```

END of Report

39. At the IP⁷ Secure Gateway, enter the `msucount -s` pass command with the card location specified in step 38 and the association names shown in step 34. For this example, enter this command.

```
pass:loc=1315:cmd="msucount -s assoc3"
```

The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
PASS: Command sent to card
```

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
MSUCOUNT: Command In Progress
```

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
```

```
MSUCOUNT: MSU Count Report
```

```
-----
Socket Name Measurements
-----
```

```
Transmit Counts
```

```
-----
tx bytes:                320294
tx msus:                  12319
```

```
Transmit Discard Counts
```

```
-----
discarded tx due to sccp msg type:    00000
discarded tx due to sccp class:      00000
discarded tx due to normalization error: 00000
discarded tx due to invalid traffic type: 00000
discarded tx due to M3UA conversion error: 00000
discarded tx due to SUA conversion error: 00001
```

```
Receive Counts
```

```
-----
rcv bytes:                167681
rcv msus:                  06451
```

```
Receive Discard Counts
```

```
-----
discarded rcv due to link state:      00000
discarded rcv due to sccp msg type:   00000
discarded rcv due to sccp class:     00000
discarded rcv due to sccp called party: 00000
discarded rcv due to sccp calling party: 00003
discarded rcv due to isup sio:       00004
discarded rcv due to normalization error: 00000
discarded rcv due to error in XSRV packet: 00000
discarded rcv due to M3UA PDU error:  00000
discarded rcv due to SUA PDU error:   00001
```

```
Stored Transmit Discard Data
```

```
-----
no stored transmit discard data
```

```
Stored Receive Discard Data
```

```
-----
53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
```

```

05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00
53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00
53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00
53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00
53 41 53 49 73 63 63 70 17 00 09 80 03 08 0a 05
c3 05 0a 01 03 02 c1 05 08 e2 06 c7 04 00 00 00
53 41 53 49 73 63 63 70 17 00 09 80 03 08 0a 05
c3 05 0a 01 03 02 c1 05 08 e2 06 c7 04 00 00 00
53 41 53 49 73 63 63 70 17 00 09 80 03 08 0a 05
c3 05 0a 01 03 02 c1 05 08 e2 06 c7 04 00 00 00

```

END of Report

pass:loc=1315:cmd="msucount -s assoc6"

The following is an example of the possible output.

```

rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
PASS: Command sent to card

```

```

rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
MSUCOUNT: Command In Progress

```

```

rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0

```

MSUCOUNT: MSU Count Report

```

-----
Socket Name Measurements
-----
Transmit Counts
-----
tx bytes:                               320294
tx msus:                                 12319
Transmit Discard Counts
-----
discarded tx due to sccp msg type:       00000
discarded tx due to sccp class:          00000
discarded tx due to normalization error: 00000
discarded tx due to invalid traffic type: 00000
discarded tx due to M3UA conversion error: 00000
discarded tx due to SUA conversion error: 00001
Receive Counts
-----
rcv bytes:                               167681
rcv msus:                                 06451
Receive Discard Counts
-----
discarded rcv due to link state:         00000
discarded rcv due to sccp msg type:     00000

```


IP7 Secure Gateway Configuration Procedures

```
discarded rcv due to sccp class:          00000
discarded rcv due to sccp called party:   00000
discarded rcv due to sccp calling party:  00003
discarded rcv due to isup sio:           00004
discarded rcv due to normalization error: 00000
discarded rcv due to error in XSRV packet: 00000
discarded rcv due to M3UA PDU error:      00000
discarded rcv due to SUA PDU error:       00001
```

Stored Transmit Discard Data

no stored transmit discard data

Stored Receive Discard Data

```
53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00
53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00
53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00
53 41 53 49 69 73 6f 74 11 00 87 0a 01 03 01 05
05 00 01 02 03 04 05 06 07 08 09 00 00 00 00 00
53 41 53 49 73 63 63 70 17 00 09 80 03 08 0a 05
c3 05 0a 01 03 02 c1 05 08 e2 06 c7 04 00 00 00
53 41 53 49 73 63 63 70 17 00 09 80 03 08 0a 05
c3 05 0a 01 03 02 c1 05 08 e2 06 c7 04 00 00 00
53 41 53 49 73 63 63 70 17 00 09 80 03 08 0a 05
c3 05 0a 01 03 02 c1 05 08 e2 06 c7 04 00 00 00
```

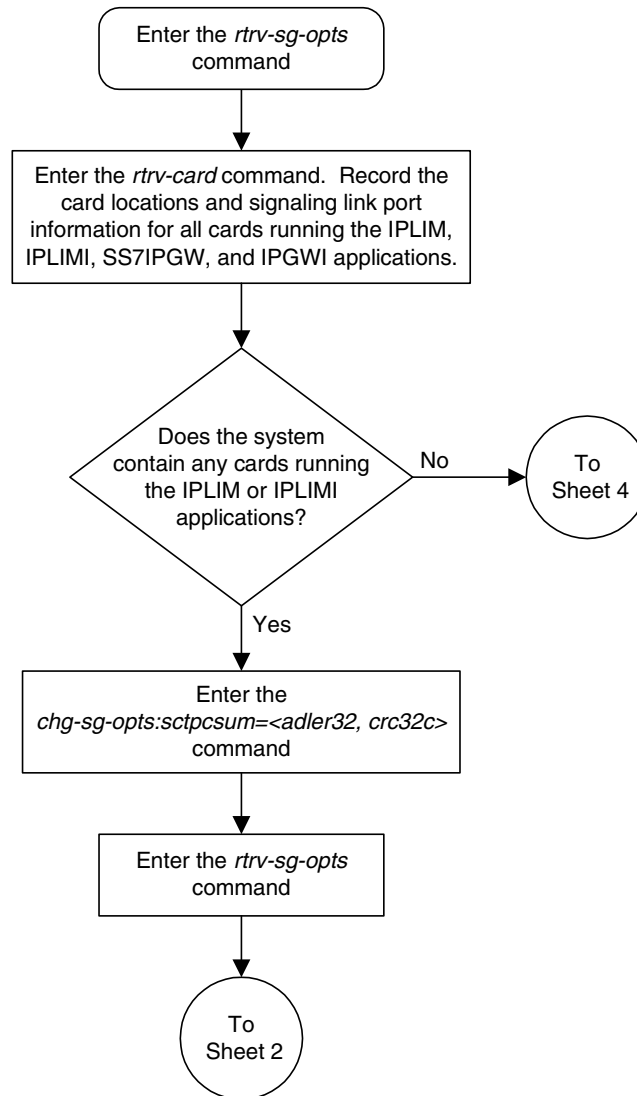
END of Report

If the outputs of the pass commands in steps 38 and 39 show that traffic is not flowing over the association, contact Tekelec Technical Services. See "Tekelec Technical Services" on page 1-8.

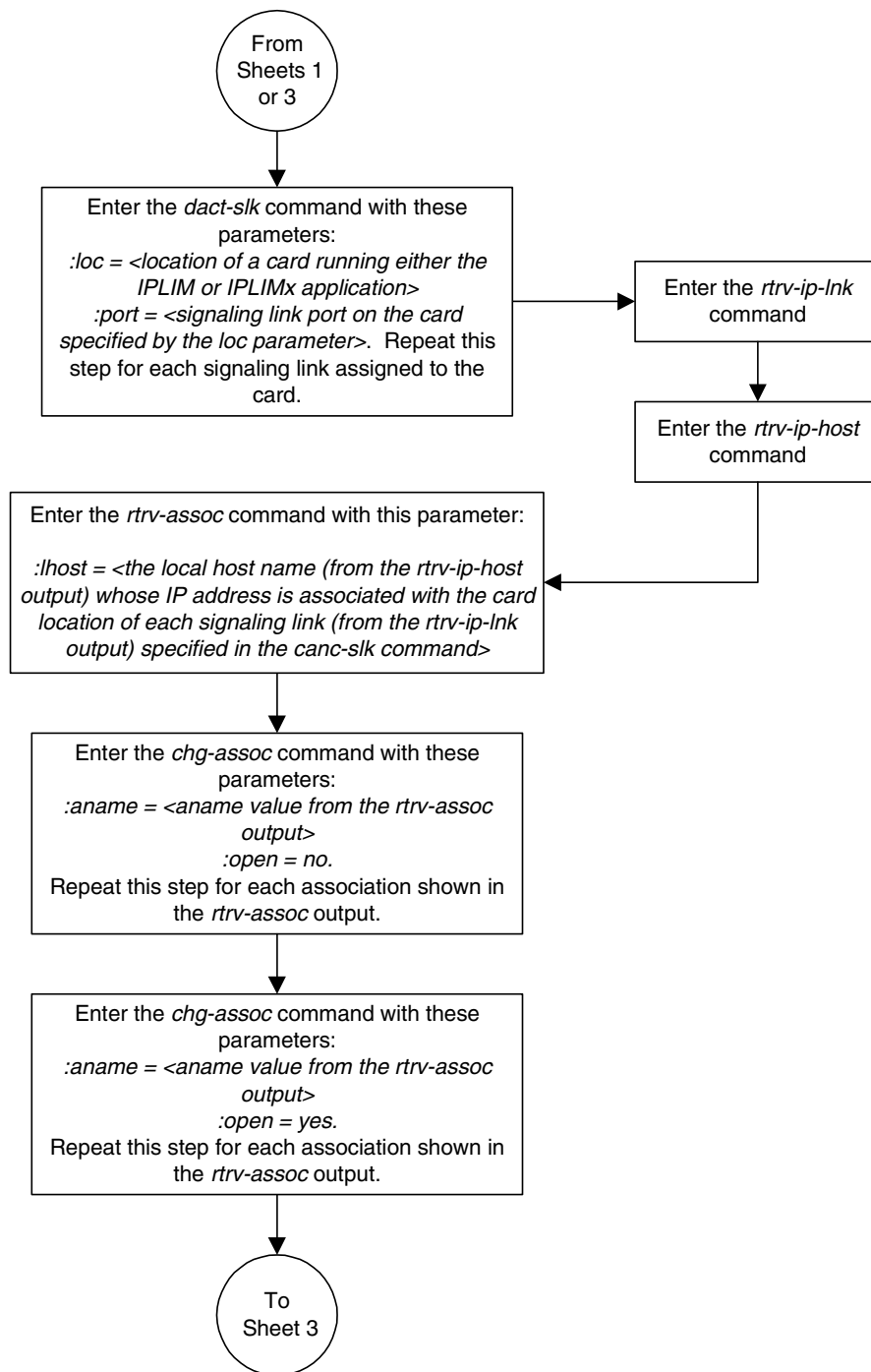
-
40. At the IP near end node, activate all the other associations attached to the IP card specified in step 39.
-
41. Repeat steps 17 through 40 to update the other IP cards in the system running the SS7IPGW and IPGWI applications with the new SCTP checksum algorithm.
-
42. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

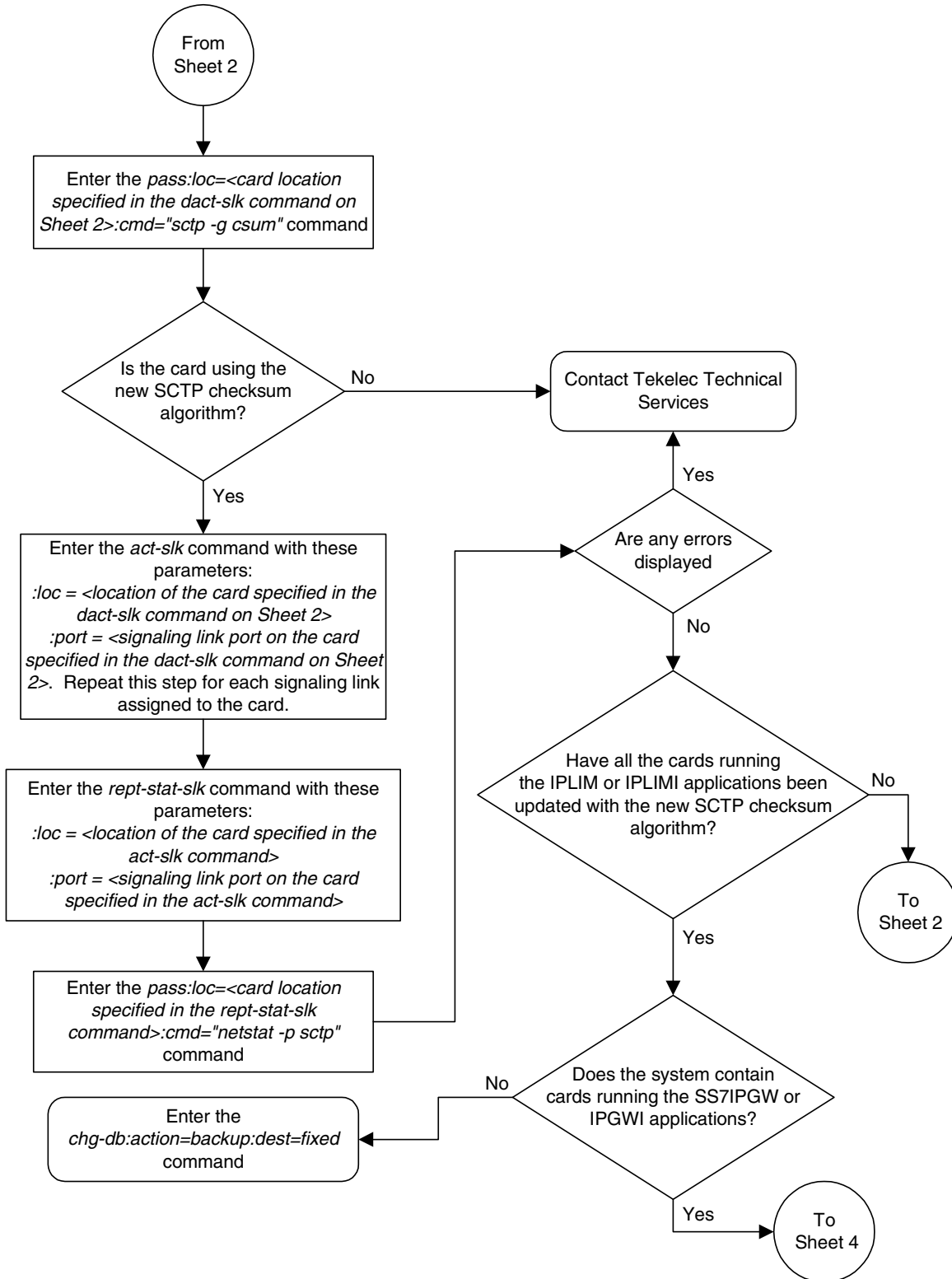
Flowchart 3-45. Changing the SCTP Checksum Option (Sheet 1 of 7)



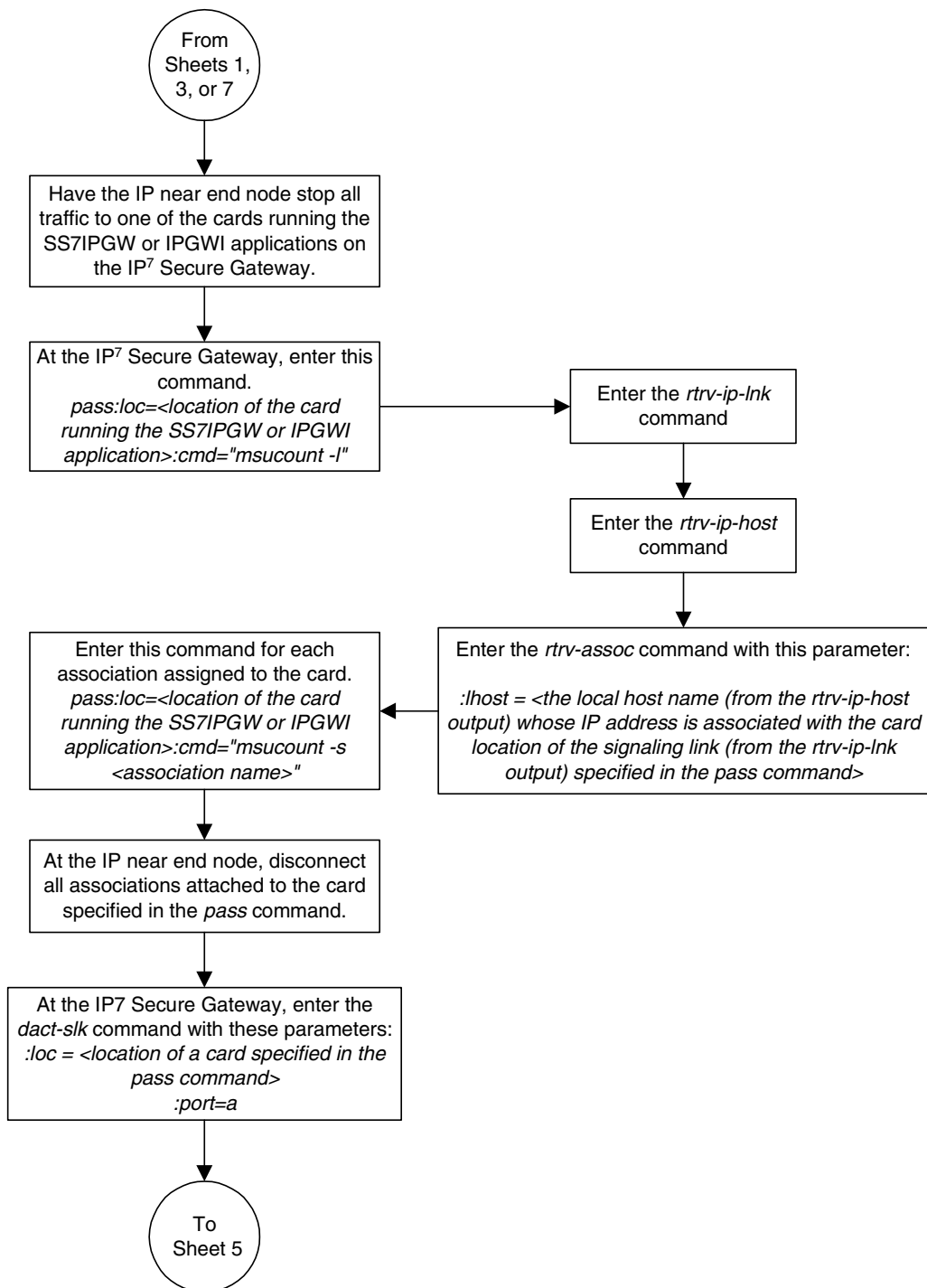
Flowchart 3-45. Changing the SCTP Checksum Option (Sheet 2 of 7)



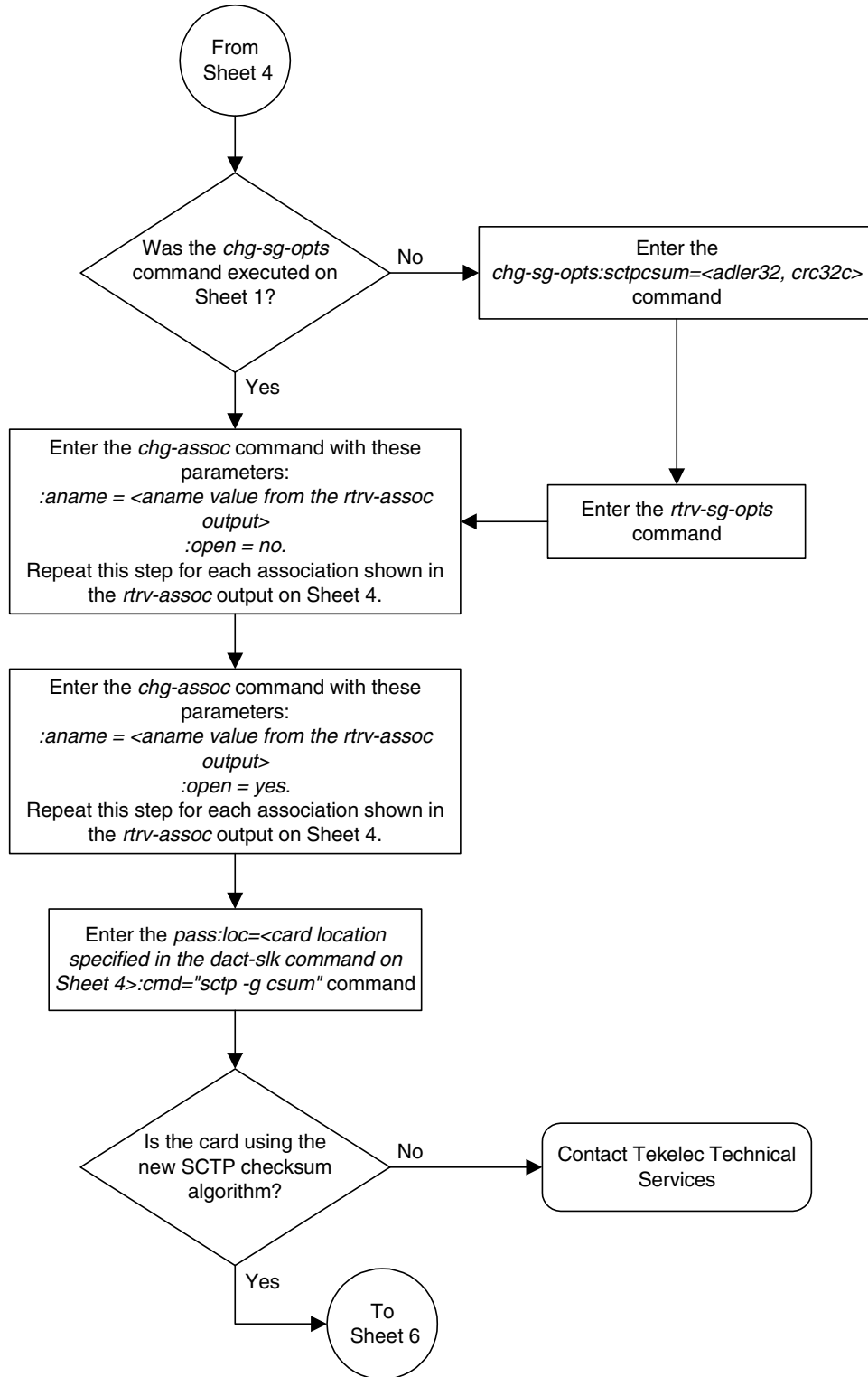
Flowchart 3-45. Changing the SCTP Checksum Option (Sheet 3 of 7)



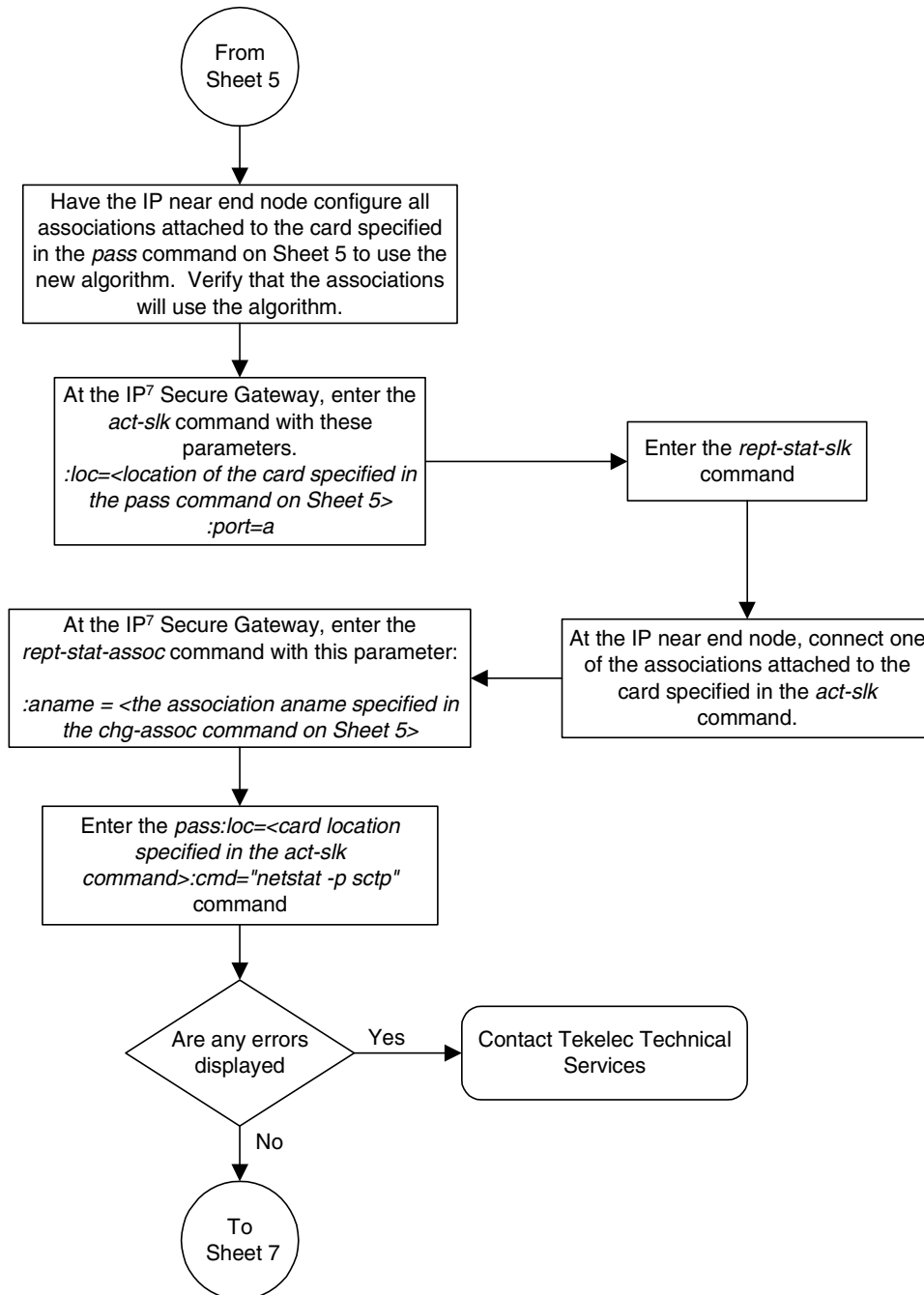
Flowchart 3-45. Changing the SCTP Checksum Option (Sheet 4 of 7)



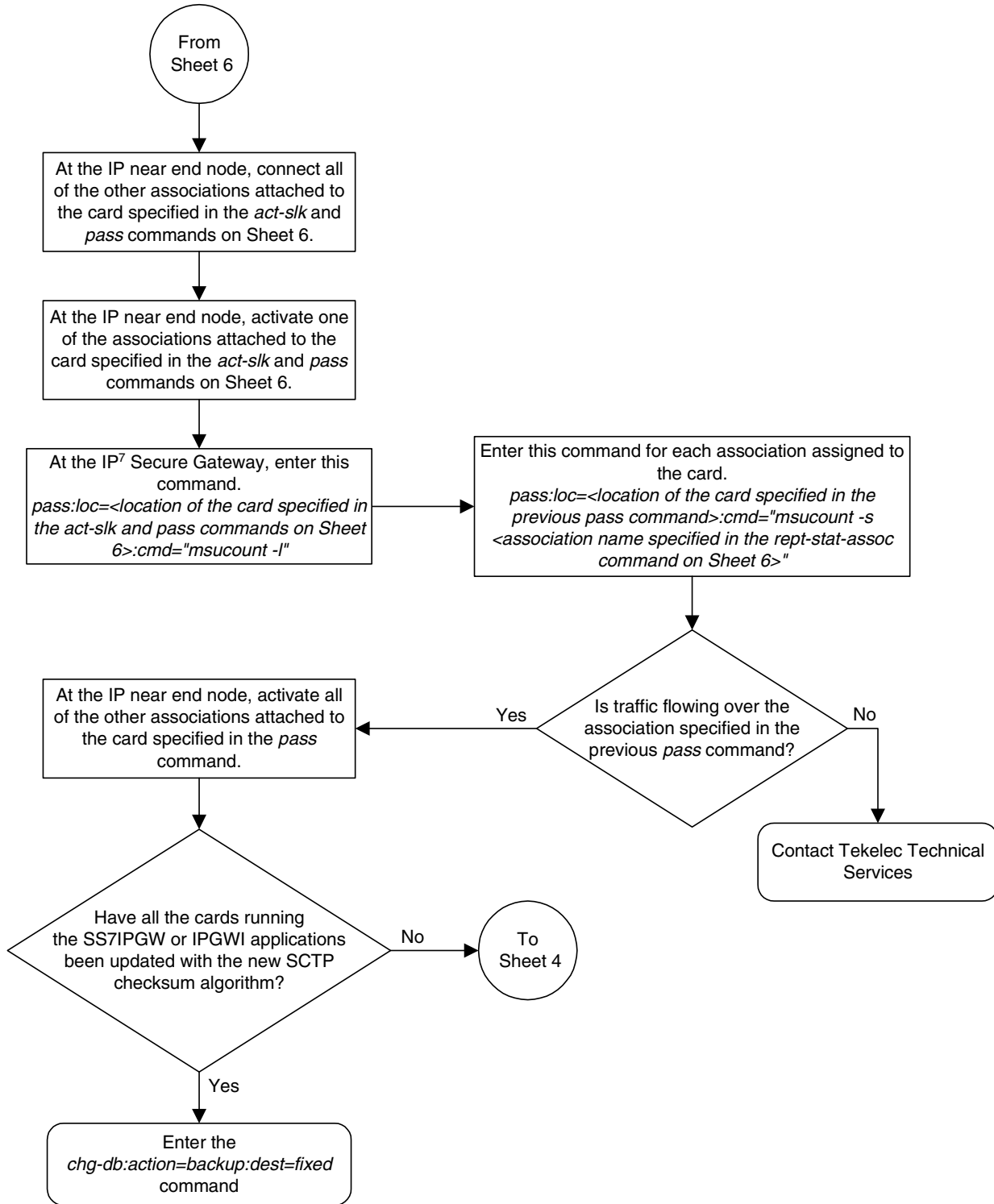
Flowchart 3-45. Changing the SCTP Checksum Option (Sheet 5 of 7)



Flowchart 3-45. Changing the SCTP Checksum Option (Sheet 6 of 7)



Flowchart 3-45. Changing the SCTP Checksum Option (Sheet 7 of 7)



Changing a UA Parameter Set

Use this procedure to change the values in a UA (user adapter) parameter set using the **chg-uaps** command. The **chg-uaps** command uses these parameters:

:set – the UA parameter set being changed, from 1 - 9

:scrsset – the source UA parameter set used to copy the values from one UA parameter set to another, from 1 to 10.

:timer – the timer being changed, from 1 to 10. Currently, there are 2 timers defined:

- Timer 1 – The AS Recovery Timer – the maximum amount of time messages are queued when an application server transitions from the AS-Active state to the AS-Pending state.
- Timer 2 – The False IP Connection Congestion Timer – the maximum amount of time (in milliseconds) that an association is allowed to remain congested before failing due to false connection congestion.

:tvalue – the value of the timer specified by the **timer** parameter:

- The value of timer 1 is from 10 to 2000 milliseconds. The system default value is 10 milliseconds.
- The value of timer 2 is from 0 to 30,000 milliseconds. The system default value is 3,000 milliseconds.

:parm – the UA parameters, from 1 to 10. Currently, only three UA parameters are defined:

- 1 – Controlling ASP SNM Behavior
- 2 – Controlling ASP/Application Server State Notification Behavior
- 3 – Controlling Validation Procedures

:pvalue – the value of the UA parameters, which is dependent on the **parm** parameter value. The value of the **pvalue** parameter is a bit-mapped value, requiring a 0 in the specific bit position to disable the item, or a 1 in the specific bit position to enable the item. The value of the **pvalue** parameter is a 32-bit number. Any bits not specified in the following lists are not used.

- If the **parm** value is 1, the bits used by the **pvalue** parameter are:
 - 0 – Broadcast – controls broadcast phase SNM TFPs, TFRs and TFAs that are sent when a destination's status changes. If this flag is set, SNM TFPs/TFRs/TFAs are replicated to all associations/sockets that meet the Multicast SNM Criteria and have this enabled. The default is to enable all broadcast phase messages.
 - 1 – Response Method – controls the sending of an SNM TFC/UPU as a reply to a message received on an association/socket for an unavailable destination. The SNM TFC/UPU is replicated to all

associations/sockets that have this capability and meet the Response SNM Criteria. The default is to allow the response to be sent.

- 6 – Broadcast Congestion Status Change – controls the sending of unsolicited congestion status changes by an ASP. Unsolicited congestion status messages (TFCs generated when a destination's congestion status changes) are replicated to all ASPs who have this capability and meet the Multicast SNM Criteria. The default is to generate no unsolicited congestion status changes.

Table 3-35 shows the values can be entered for the **pvalue** parameter if the **parm** value is 1. The **pvalue** parameter value can be entered as a hexadecimal or a decimal number.

Table 3-35. Valid PVALUE Parameter Values if PARM=1

Bits Enabled	Bits Disabled	Hexadecimal Value	Decimal Value
None	Bit 0 - Broadcast Bit 1 - Response Method Bit 6 - Broadcast Congestion Status Change	h'0	0
Bit 0 - Broadcast	Bit 1 - Response Method Bit 6 - Broadcast Congestion Status Change	h'1	1
Bit 1 - Response Method	Bit 0 - Broadcast Bit 6 - Broadcast Congestion Status Change	h'2	2
Bit 0 - Broadcast Bit 1 - Response Method	Bit 6 - Broadcast Congestion Status Change	h'3*	3*
Bit 6 - Broadcast Congestion Status Change	Bit 0 - Broadcast Bit 1 - Response Method	h'40	64
Bit 6 - Broadcast Congestion Status Change Bit 0 - Broadcast	Bit 1 - Response Method	h'41	65
Bit 6 - Broadcast Congestion Status Change Bit 1 - Response Method	Bit 0 - Broadcast	h'42	66
Bit 0 - Broadcast Bit 1 - Response Method Bit 6 - Broadcast Congestion Status Change	None	h'43	67
* The system default value			

- If the **parm** value is 2, the bits used by the **pvalue** parameter are:
 - 0 – ASP Active Notifications – controls the sending of ASP-Active notifications. If this value is specified, an ASP-Default notification is sent when an ASP transitions to the ASP-ACTIVE state. The default is not to send ASP-Active notifications.

- 1 – ASP Inactive Notifications – controls the sending of ASP-Inactive notifications. If this value is specified, an ASP-Inactive notification is sent when an ASP transitions to the ASP-INACTIVE state. The default is not to send ASP-Inactive notifications.

NOTE: To see the ASP activations and inactivations, bits 0 and 1 of the **pvalue** parameter value need to be enabled. See Table 3-36 on page 3-453.

- 2 – ASP AS State Query – controls the sending of ASP/AS State notifications on request by an ASP. If this value is specified, the system responds with ASP and AS state notifications if the remote ASP sends ASP-UP or ASP-INACTIVE, while the local ASP is in the ASP-INACTIVE state, or the remote ASP sends an ASP-ACTIVE notification while the local ASP is in the ASP-ACTIVE state. The default is not to send ASP/AS state notifications.

Table 3-36 shows the values can be entered for the **pvalue** parameter if the **parm** value is 2. The **pvalue** parameter value can be entered as a hexadecimal or a decimal number.

Table 3-36. Valid PVALUE Parameter Values if PARM=2

Bits Enabled	Bits Disabled	Hexadecimal Value	Decimal Value
None	Bit 0 - ASP Activate Notifications Bit 1 - ASP Inactivate Notifications Bit 2 - ASP AS State Query	h'0*	0*
Bit 0 - ASP Activate Notifications	Bit 1 - ASP Inactivate Notifications Bit 2 - ASP AS State Query	h'1	1
Bit 1 - ASP Inactivate Notifications	Bit 0 - ASP Activate Notifications Bit 2 - ASP AS State Query	h'2	2
Bit 0 - ASP Activate Notifications Bit 1 - ASP Inactivate Notifications	Bit 2 - ASP AS State Query	h'3	3
Bit 2 - ASP AS State Query	Bit 0 - ASP Activate Notifications Bit 1 - ASP Inactivate Notifications	h'4	4
Bit 0 - ASP Activate Notifications Bit 2 - ASP AS State Query	Bit 1 - ASP Inactivate Notifications	h'5	5
Bit 1 - ASP Inactivate Notifications Bit 2 - ASP AS State Query	Bit 0 - ASP Activate Notifications	h'6	6
Bit 0 - ASP Activate Notifications Bit 1 - ASP Inactivate Notifications Bit 2 - ASP AS State Query	None	h'7	7
* The system default value			

- Table 3-37 shows the values can be entered for the **pvalue** parameter if the **parm** value is 3. If the **parm** value is 3, the bit used by the **pvalue** parameter is 0 (Strict/Relaxed ASP-ID Checking). If this value is 1, the mode is strict and the ASP ID is validated. If this value is 0, the mode is relaxed and no validation occurs. The **pvalue** parameter value can be entered as a hexadecimal or a decimal number.

Table 3-37. Valid PVALUE Parameter Values if PARM=3

Bits Enabled	Bits Disabled	Hexadecimal Value	Decimal Value
None	Bit 0 - Relaxed ASP-ID Checking	h'0*	0*
Bit 0 - Strict ASP-ID Checking	None	h'1	1
* The system default value			

UA parameter set 10 contains the default values for the UA parameter sets and cannot be changed.

The **set** and **scrset** parameter values cannot be the same.

If the **scrset** parameter is specified, no other optional parameter may be specified.

The **timer** and **tvalue** parameters must be specified together. If one is specified, the other must be specified.

The **parm** and **pvalue** parameters must be specified together. If one is specified, the other must be specified.

The **open** parameter value of all associations assigned to the ASPs using the UA parameter set being changed must be set to **no** before the UA parameter set values can be changed.

Canceling the `RTRV-UAPS` and `RTRV-ASSOC` Commands

Because the `rtrv-uaps` and `rtrv-assoc` commands used in this procedure can output information for a long period of time, the `rtrv-uaps` and `rtrv-assoc` commands can be canceled and the output to the terminal stopped. There are three ways that the `rtrv-uaps` and `rtrv-assoc` commands can be canceled.

- Press the **F9** function key on the keyboard at the terminal where the `rtrv-uaps` or `rtrv-assoc` commands were entered.
- Enter the `canc-cmd` without the `trm` parameter at the terminal where the `rtrv-uaps` or `rtrv-assoc` commands were entered.
- Enter the `canc-cmd:trm=<xx>`, where `<xx>` is the terminal where the `rtrv-uaps` or `rtrv-assoc` commands were entered, from another terminal other than the terminal where the `rtrv-uaps` or `rtrv-assoc` commands were entered. To enter the `canc-cmd:trm=<xx>` command, the terminal must allow Security Administration commands to be entered from it and the user must be allowed to enter Security Administration commands. The terminal's permissions can be verified with the `rtrv-secu-trm` command. The user's permissions can be verified with the `rtrv-user` or `rtrv-secu-user` commands.

For more information about the `canc-cmd` command, go to the *Commands Manual*.

Procedure

1. Display the values in the UA parameter set being changed by entering the `rtrv-uaps` command and specifying the desired UA parameter set number, from 1 to 9. For this example, enter this command.

```
rtrv-uaps:set=3
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
SET  TIMER      TVALUE  PARM      PVALUE
 3      1          10      1          3
 3      2         3000    2          0
 3      3           0      3          0
 3      4           0      4          0
 3      5           0      5          0
 3      6           0      6          0
 3      7           0      7          0
 3      8           0      8          0
 3      9           0      9          0
 3     10           0     10          0
```

TIMER 1: AS Recovery Timer (ms) T(r), min time AS msgs are queued, SS7IPGW and IPGWI applications enforce 10-2000(ms).

TVALUE : Valid range = 32-bits

TIMER 2: False IP Connection Congestion Timer, max time an association can be congested before failing due to false congestion. SS7IPGW and IPGWI applications enforce 0-30000(ms).

TVALUE : Valid range = 32-bits

PARM 1: ASP SNM options. Each bit is used as an enabled/disabled flag for a particular ASP SNM option.

PVALUE : Valid range = 32-bits

BIT	BIT VALUE
0=Broadcast	0=Disabled , 1=Enabled
1=Response Method	0=Disabled , 1=Enabled
2-5=Reserved	
6=Broadcast Congestion Status Change	0=Disabled , 1=Enabled
7-31=Reserved	

PARM 2: ASP/AS Notification options. Each bit is used an enabled/disabled flag for a particular ASP/AS Notification option.

PVALUE : Valid range = 32-bits

BIT	BIT VALUE
0=ASP Active Notifications	0=Disabled , 1=Enabled
1=ASP Inactive Notifications	0=Disabled , 1=Enabled
2=ASP AS State Query	0=Disabled , 1=Enabled
3-31=Reserved	

PARM 3: AS/ASP validations. Each bit is used to control a particular AS/ASP validation method.

PVALUE : Valid range = 32-bits

BIT	BIT VALUE
0=Strict ASP-ID checking	0=Disabled , 1=Enabled
1-31=Reserved	

2. Display the application server processes in the database using the `rtrv-asp` command. This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ASP          ASSOCIATION          UAPS
asp1        swbel32                3
asp2        a2                    1
asp3        a3                    1
asp4        assoc1                10
asp5        assoc2                10
asp6        assoc3                10
asp7        assoc4                10
```

ASP Table is (7 of 4000) 1% full

3. Display the associations assigned to the ASPs that are using the UA parameter set being changed using the `rtrv-assoc` command and specifying the name of the association. For this example, enter this command.

`rtrv-assoc:aname=swbel32`

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
ANAME swbel32
PORT      A
ADAPTER   M3UA          VER          M3UA RFC
LHOST     gw105.nc.tekelec.com
ALHOST    ---
RHOST     gw100.ncd-economic-development.southeastern-cooridor-ash.gov
LPORT     1030          RPORT        2345
ISTRMS    2             OSTRMS       2
RMODE     LIN           RMIN         120          RMAX         800
RTIMES    10           CWMIN        3000
OPEN      YES          ALW          YES
```

IP Appl Sock table is (4 of 4000) 1% full

If the value of the **open** parameter for the association shown in this step is **no**, no action is necessary for this association.

If the value of the **open** parameter for the association shown in this step is **yes**, go to the “Changing an Association” procedure on page 3-350 and change the value of the **open** parameter to **no**.

Repeat this step for all associations assigned to ASPs using the UA parameter set being changed.

- Change the UA parameter set values using the **chg-uaps** command with the UA parameter set value used in step 1. If the **parm** and **pvalue** parameters are being specified, see Table 3-35 on page 3-452, Table 3-36 on page 3-453, or Table 3-37 on page 3-454 for the valid values of the **pvalue** parameter. For this example, enter this command.

```
chg-uaps:set=3:timer=1:tvalue=200:parm=2:pvalue=1
```

The value of the **pvalue** parameter can be entered as either a decimal value or a hexadecimal value. This example shows the **pvalue** parameter value of the **chg-uaps** command being entered as a decimal value. To specify the value of the **pvalue** parameter in the example used in this step as a hexadecimal value, specify the **pvalue=h'1** parameter.

```
chg-uaps:set=3:timer=1:tvalue=200:parm=2:pvalue=h'1
```

When this command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
CHG-UAPS: MASP A - COMPLTD
```

- Verify the changes using the **rtrv-uaps** command with the UA parameter set name used in step 4. For this example, enter this command.

```
rtrv-uaps:set=3
```

This is an example of possible output.

```
rlghncxa03w 04-12-28 09:12:36 GMT EAGLE5 31.10.0
SET  TIMER      TVALUE  PARM    PVALUE
 3      1          200     1        3
 3      2          3000    2         1
 3      3           0       3         0
 3      4           0       4         0
 3      5           0       5         0
 3      6           0       6         0
 3      7           0       7         0
 3      8           0       8         0
 3      9           0       9         0
 3     10           0      10         0
```

TIMER 1: AS Recovery Timer (ms) T(r), min time AS msgs are queued, SS7IPGW and IPGWI applications enforce 10-2000(ms).

TVALUE : Valid range = 32-bits

TIMER 2: False IP Connection Congestion Timer, max time an association can be congested before failing due to false congestion. SS7IPGW and IPGWI applications enforce 0-30000(ms).

TVALUE : Valid range = 32-bits

PARM 1: ASP SNM options. Each bit is used as an enabled/disabled flag for a particular ASP SNM option.

PVALUE : Valid range = 32-bits

BIT	BIT VALUE
0=Broadcast	0=Disabled , 1=Enabled
1=Response Method	0=Disabled , 1=Enabled
2-5=Reserved	
6=Broadcast Congestion Status Change	0=Disabled , 1=Enabled
7-31=Reserved	

IP7 Secure Gateway Configuration Procedures

PARAM 2: ASP/AS Notification options. Each bit is used as an enabled/disabled flag for a particular ASP/AS Notification option.

PVALUE : Valid range = 32-bits

BIT	BIT VALUE
0=ASP Active Notifications	0=Disabled , 1=Enabled
1=ASP Inactive Notifications	0=Disabled , 1=Enabled
2=ASP AS State Query	0=Disabled , 1=Enabled
3-31=Reserved	

PARAM 3: AS/ASP validations. Each bit is used to control a particular AS/ASP validation method.

PVALUE : Valid range = 32-bits

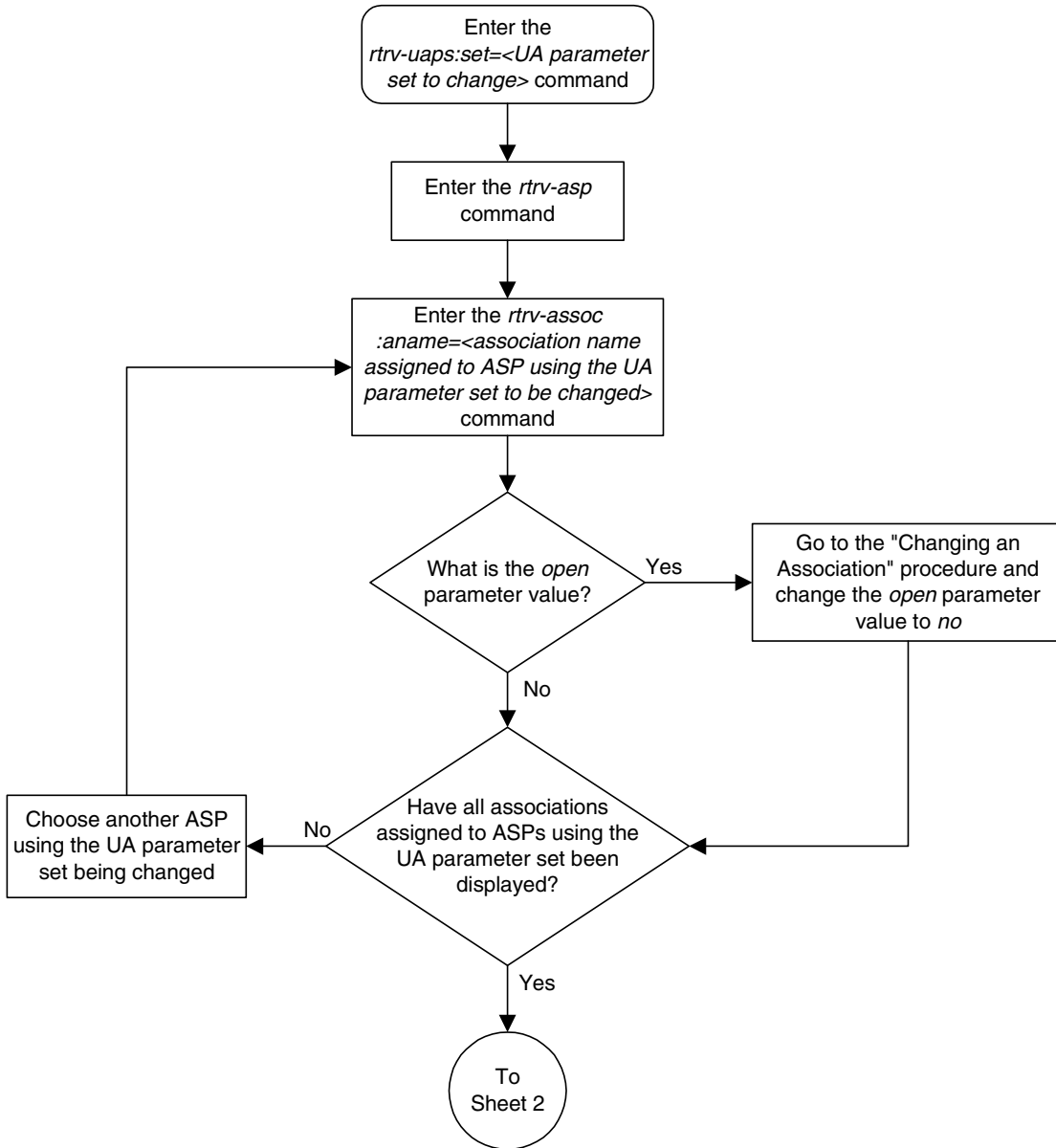
BIT	BIT VALUE
0=Strict ASP-ID checking	0=Disabled , 1=Enabled
1-31=Reserved	

-
6. If the **open** parameter value of any associations assigned to ASPs using the UA parameter set was changed to **no** in step 3, go to the "Changing an Association" procedure on page 3-350 and change the value of the **open** parameter in these associations to **yes**.

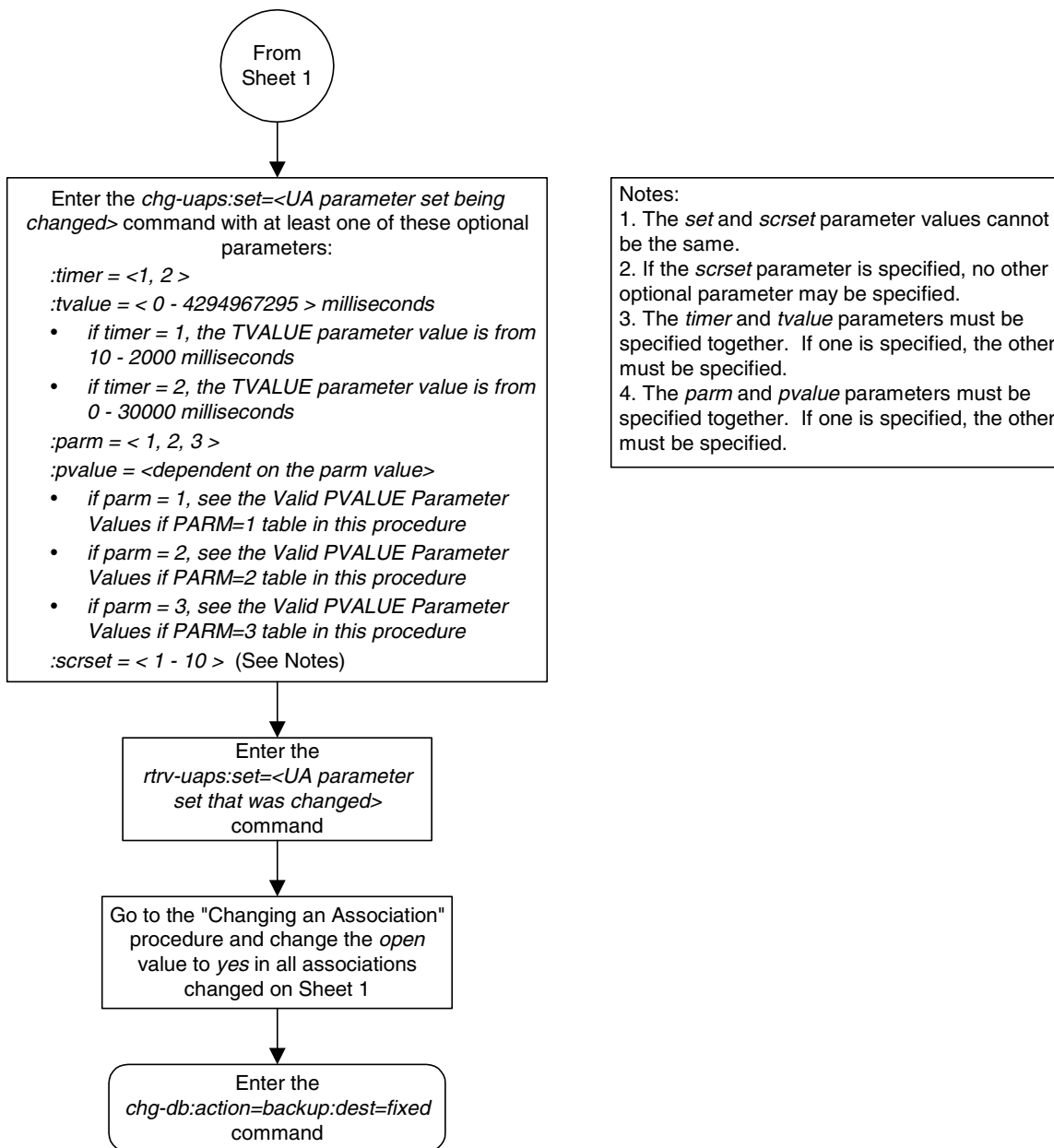
-
7. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 3-46. Changing a UA Parameter Set (Sheet 1 of 2)



Flowchart 3-46. Changing a UA Parameter Set (Sheet 2 of 2)



4

ISUP Variant Table Provisioning

Overview	4-2
Adding New ISUP PSTN Presentation Values.....	4-6
Changing ISUP Presentation Values.....	4-11
Removing ISUP Presentation Values	4-13
Changing ISUP Variant Table Entries.....	4-17
Copying ISUP Variant Table Entries	4-26

Overview

ISUP Normalization is Tekelec's process of converting/translating different customized versions of the ISUP protocol into one standard protocol (Normalized ISUP) for transmission to an IP device. This process also includes the reverse scenario, receiving Normalized ISUP messages from an IP device and denormalizing the message into customized versions.

IP⁷ Secure Gateway supports end-user ISUP Normalization Administration. It is now possible to use the Eagle's commands to achieve the following:

- Define and display new PSTN Presentation values for user-defined variants
- Provision a variant database starting from scratch
- Provision a variant database by copying another variants database
- Define the ISUP message types for a variant
- Define the ISUP parameters for a variant and the minimum length that is valid for each parameter
- Define the optional ISUP parameters supported for each ISUP message type
- Define the mandatory-fixed and mandatory-variable parameters that are supported for each ISUP message type and the order they appear in the message
- Assign a "conversion action" to ISUP messages and message/parameter combinations within a specific variant that require special software treatment
- Display the variant database

Prior implementations of the ISUP Normalization feature kept the ISUP data in hard-coded software tables. Changing ISUP parameters could only be achieved by means of a software revision. The disk-resident ISUP variant table eliminates this problem and increases flexibility and maintainability. This table include an entry in the variant's ISUP database table for each variant. When the **ent-pstn-pres** command is used to define a PSTN value, the first available entry in the ISUP variant database table is automatically allocated. The table entry is initialized to default values.

The ETSI V3 variant database is treated differently from other variants. It is automatically configured by the system during an upgrade or new installation. You will not have to enter the **ent-pstn-pres** command to define it. You cannot modify or delete the table entry for this variant, except to change the descriptive text.

The ISUP variant table supports a maximum of 21 entries, one of which is always the ETSI V3 variant. This allows for 20 entries for Tekelec-defined or user-defined ISUP variants.

ISUP Variant Table Provisioning

The normalization process occurs in the following steps:

1. The system receives a variant ISUP message from a PSTN.
2. The routing key variant database tables are accessed and provide the following information:
 - Indicates the message is to be routed to an IP device
 - Contains the PSTN Presentation value identifying the variant
 - Contains a “normalization flag” indicating the message is to be normalized
3. The software accesses database tables for the variant. The software performs some minor syntax validation on the received message and then constructs a normalized ISUP message.
4. The normalized message is sent in a TALI packet across an IPGWI connection to a far-end IP device.

The normalization function is performed entirely on the IPGWI card in the system. Everything presented to the MGCs that are using this feature is in normalized ISUP format. Everything that is presented to the MTP3 portion of the IPGWI card (to be routed back to a DS0 link towards the PSTN) is in the format for a specific ISUP variant. Each DS0 LIM (or any LIM in the system other than the IPGWI) receives MSUs from the PSTN wire and from the IMT in the same ISUP variant format. The DS0 LIMS do not know how to perform ISUP Normalization, and do not even know that it is occurring on the IPGWI cards.

The ISUP Normalization feature supports the normalization of the ISUP variants shown in Table 4-1.

Table 4-1. ISUP Variants Supported by this Feature

ISUP Variant	Part No.	PSTN Category	PSTN ID
ISUP Normalization	893000201	1	*
ITU Q.767 Normalization	893000501	1	1
ESTI V3 Normalization	893000601	1	2
UK PNO-ISC7 Normalization	893000401	1	3
German ISUP Normalization	893000301	1	4
French ISUP Normalization	893-0007-01	1	5
Sweden ISUP Normalization	893-0008-01	1	6
Belgium ISUP Normalization	893-0009-01	1	7
Netherlands ISUP Normalization	893-0010-01	1	8

Table 4-1. ISUP Variants Supported by this Feature (Continued)

ISUP Variant	Part No.	PSTN Category	PSTN ID
Switzerland ISUP Normalization	893-0011-01	1	9
Austria ISUP Normalization	893-0012-01	1	10
Italy ISUP Normalization	893-0013-01	1	11
Ireland ISUP Normalization	893-0014-01	1	12
India ISUP Normalization	893-0015-01	1	13
Malaysia ISUP Normalization	893-0016-01	1	14
Vietnam ISUP Normalization	893-0017-01	1	15
South Africa ISUP Normalization	893-0018-01	1	16
Argentina ISUP Normalization	893-0019-01	1	17
Chile ISUP Normalization	893-0020-01	1	18
Venezuela ISUP Normalization	893-0021-01	1	19
Mexico ISUP Normalization	893-0022-01	1	20
Brazil ISUP Normalization	893-0023-01	1	21
Spain ISUP Normalization	893-0024-01	1	22
Colombia ISUP Normalization	893-0025-01	1	23
Peru ISUP Normalization	893-0026-01	1	24
Hong Kong ISUP Normalization	893-0027-01	1	25
China ISUP Normalization	893-0028-01	1	26
Japan ISUP Normalization	893-0029-01	1	27
Korea ISUP Normalization	893-0030-01	1	28
Taiwan ISUP Normalization	893-0031-01	1	29
Philippines ISUP Normalization	893-0032-01	1	30
Singapore ISUP Normalization	893-0033-01	1	31
Australia ISUP Normalization	893-0034-01	1	32
Reserved for future definition by Tekelec		2 through 4095	
Available for user-defined categories		4095 through 65535	

ISUP Variant Table Provisioning

The Quantity Control feature allows a customer to provision a specified quantity of user-defined variants within the PSTN categories 4096 - 65535. Each Quantity Control Feature is associated with a specific quantity of variants. To provision user-defined variants, it is necessary to purchase the appropriate Feature Access Keys from Tekelec. Variants enabled using the Quantity Control feature do not have associated PSTN Presentation values.

The part number for user-defined variants is 893-0100-nn, where nn is a number ranging from 01 to 20. Use part number 893-0100-01 to order one new variant, 893-0100-05 to order five new variants, and so on.

Adding New ISUP PSTN Presentation Values

This procedure is used to add a new ISUP presentation value to the ISUP variant table, using the **ent-pstn-pres** command.

The PSTN Presentation value, consisting of a PSTN Category and PSTN ID, is used by the system to uniquely define an ISUP variant. The assignment of a new PSTN value also creates a new entry in the ISUP variant table. The new PSTN value must be unique.

This procedure may be used to define values within the Tekelec-defined range (PSTN Category 0-4095) as long as these control features are enabled:

- the controlled feature for the new PSTN category
- ISUP Normalization control feature

This command may be used to define values within the user-defined range (PSTN Category 4096-65535) as long as these control features are enabled:

- the controlled feature for the new PSTN category
- ISUP Normalization control feature
- ISUP Normalization Quantity control feature, to make sure that the quantity of user-defined PSTN categories is not exceeded.

The **ent-pstn-pres** command uses these parameters:

:pstncat - The PSTN Category identifying the new variant being defined is mandatory. Valid values for this parameter range from 0 to 65535.

:pstnid - The PSTN ID identifying the new variant being defined is mandatory. Valid values for this parameter range from 0 to 65535.

:pstndesc - The PSTN Description, a text description of the PSTN Presentation value, is optional. It should be used to describe the variant associated with the PSTN. This field is displayed by the **rtrv-pstn-pres** command and it has no other purpose. This alphanumeric string 0-31 characters in length is delimited with quotation marks.

Valid **pstncat** and **pstnid** parameter values are listed in Table 4-1 on page 4-3.

Procedure

1. Display the current value of the ISUP PSTNs using the `rtrv-pstn-pres` command. This is an example of possible output:

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
PSTNCAT PSTNID PSTNDESC
00001 00001 ITU Q.767
00001 00002 ETSI V3
00001 00003 UK PNO-ISC7
00001 00004 GERMAN ISUP
00001* 00020 Mexico
04096 01000 User Defined 4096/1000
```

ISUP Variant table is (6 of 21) 29% full

NOTE: An * will be displayed next to the PSTN Category for entries that are no longer usable. These are entries that are disabled because their temporary feature key expired.

2. Display enabled controlled feature information in the database by entering the `rtrv-ctrl-feat` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
The following features have been permanently enabled:
```

Feature Name	Partnum	Status	Quantity
IPGWx Signaling TPS	893012814	on	20000
ISUP Normalization	893000201	on	----
ETSI v3 Normalization	893000601	on	----

The following features have been temporarily enabled:

Feature Name	Partnum	Status	Quantity	Trial Period Left
Zero entries found.				

The following features have expired temporary keys:

Feature Name	Partnum
Zero entries found.	

If the ISUP Normalization control feature, the controlled feature for the new PSTN category, and if a user-defined PSTN category is being changed, or the ISUP Normalization Quantity control feature have not been enabled and turned on, go to the “Enabling Controlled Features” procedure on page 6-2 and to “Turning On and Off Controlled Features” procedure on page 6-10 to enable and turn on these controlled features.

3. Enter the desired new ISUP PSTN using the `ent-pstn-pres` command. For this example, enter this command.

```
ent-pstn-pres:pstncat=5000:pstnid=1
:pstndesc="Mexican ISUP v1.8"
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.10.0
ENT-PSTN-PRES: MASP A - COMPLTD
```

4. Verify that the new ISUP PSTN has been added to the database using the `rtrv-pstn-pres` command. This is an example of possible output:

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
PSTNCAT PSTNID PSTNDESC
00001 00001 ITU Q.767
00001 00002 ETSI V3
00001 00003 UK PNO-ISC7
00001 00004 GERMAN ISUP
00001* 00020 Mexico
04096 01000 User Defined 4096/1000
05000 00001 Mexican ISUP v1.8
```

ISUP Variant table is (7 of 21) 33% full

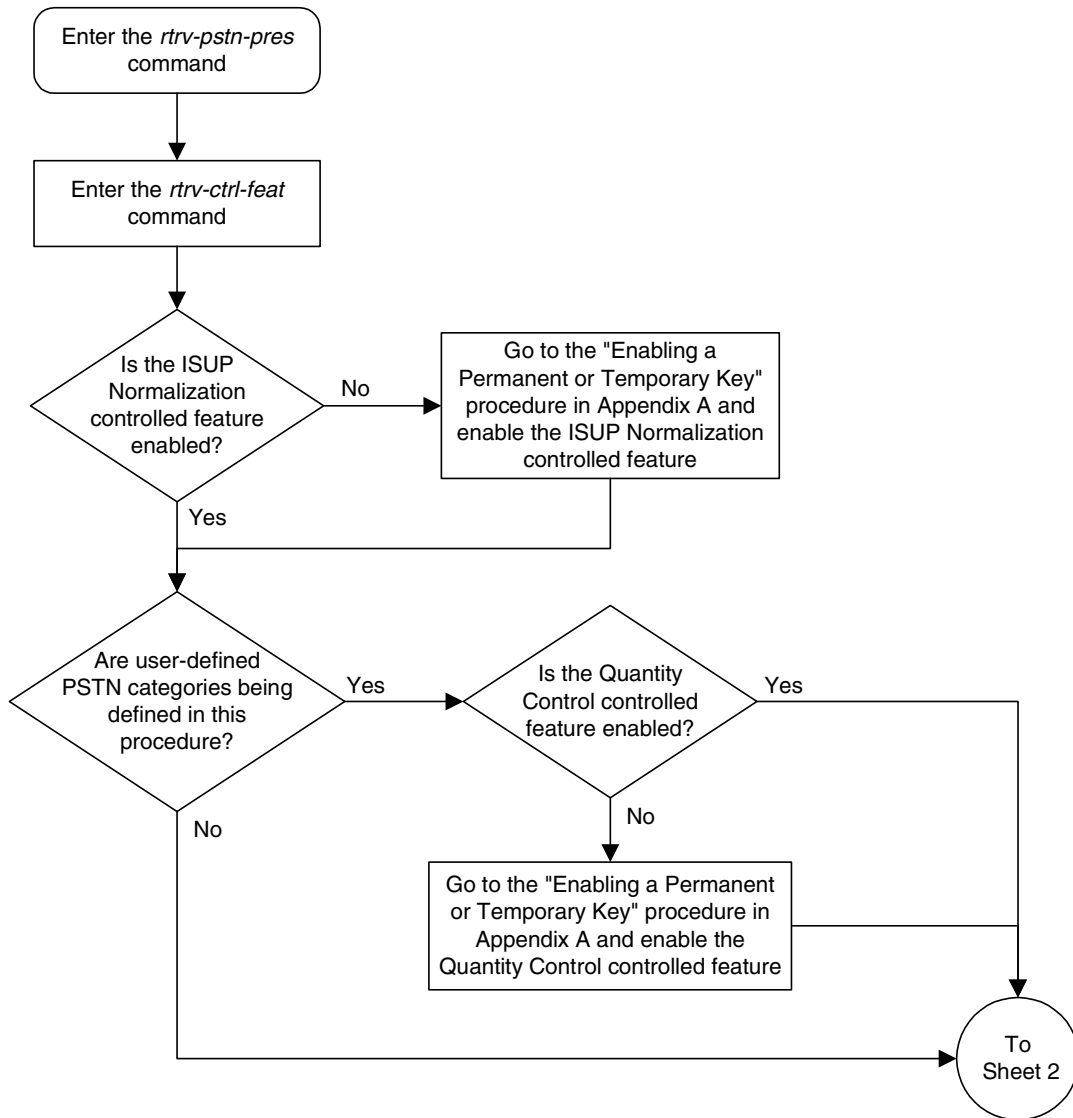
NOTE: An * will be displayed next to the PSTN Category for entries that are no longer usable. These are entries that are disabled because their temporary feature key expired.

5. Back up the new changes, using the `chg-db:action=backup:dest=fixed` command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

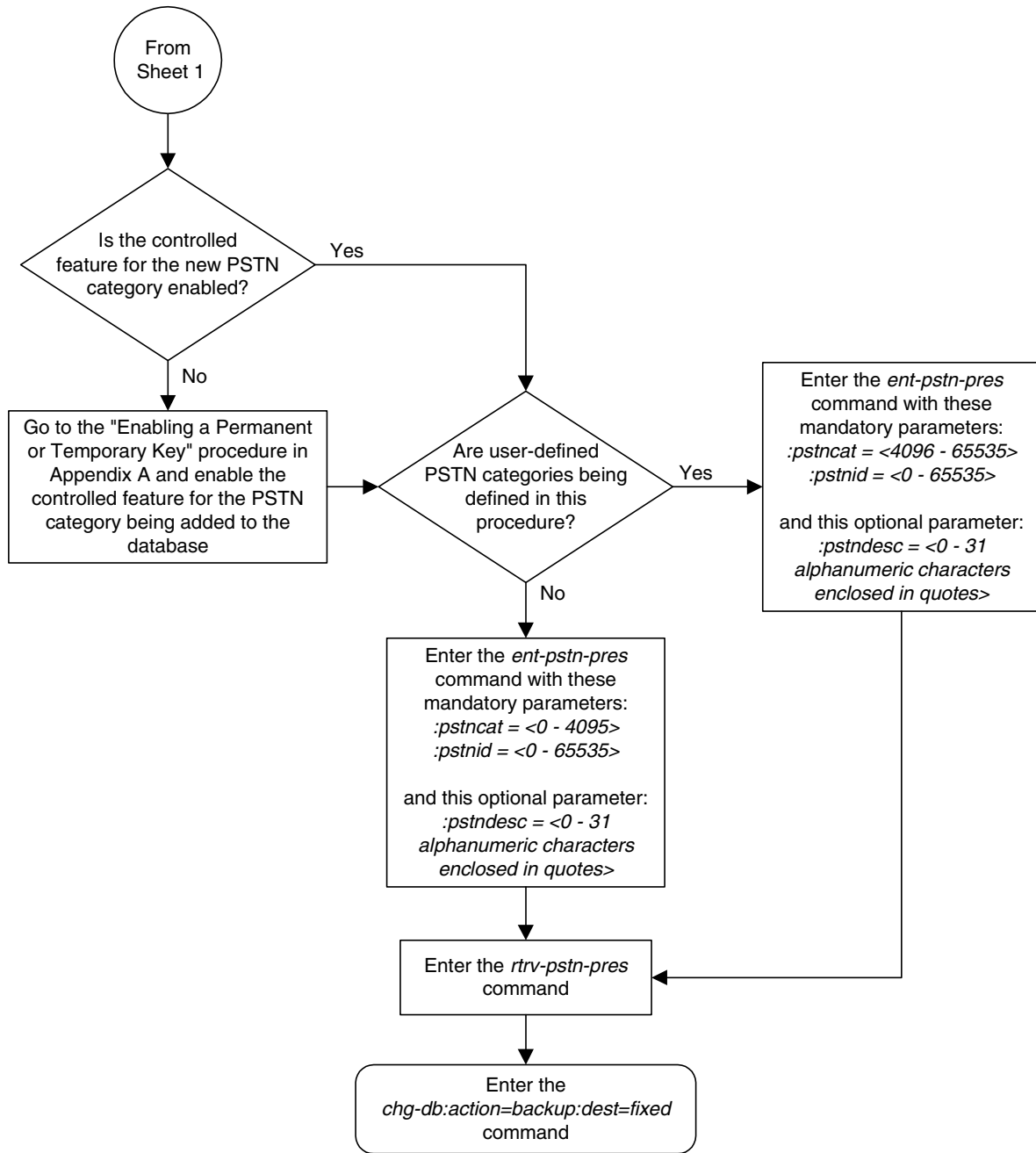
```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

ISUP Variant Table Provisioning

Flowchart 4-1. Adding ISUP PSTN Presentation Value (Sheet 1 of 2)



Flowchart 4-1. Adding ISUP PSTN Presentation Value (Sheet 2 of 2)



Changing ISUP Presentation Values

This procedure is used to change the description for a previously defined PSTN presentation value in the ISUP Variant Table, using the `chg-pstn-pres` command. The description of the PSTN presentation value is shown in the `PSTNDESC` column in the `rtrv-pstn-pres` output.

The `chg-pstn-pres` command uses these parameters:

- :pstncat** - The PSTN Category identifying the variant being changed is mandatory. Valid values for this parameter range from 0 to 65535.
- :pstnid** - The PSTN ID identifying the variant being changed is mandatory. Valid values for this parameter range from 0 to 65535.
- :pstndesc** - The PSTN Description, a text description of the PSTN Presentation value, is mandatory. It should be used to describe the variant associated with the PSTN. This field is displayed by the `rtrv-pstn-pres` command and it has no other purpose. This alphanumeric string 0 -31 characters in length is delimited with quotation marks.

Procedure

1. Display the current value of the ISUP PSTNs using the `rtrv-pstn-pres` command. This is an example of possible output:

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
PSTNCAT PSTNID PSTNDESC
00001 00001 ITU Q.767
00001 00002 ETSI V3
00001 00003 UK PNO-ISC7
00001 00004 GERMAN ISUP
00001* 00020 Mexico
04096 01000 User Defined 4096/1000
05000 00001 Mexican ISUP v1.8
```

ISUP Variant table is (7 of 21) 33% full

NOTE: An * will be displayed next to the PSTN Category for entries that are no longer usable. These are entries that are disabled because their temporary feature key expired.

2. Change the PSTN descriptive text using the `chg-pstn-pres` command. For this example, enter this command.

```
chg-pstn-pres:pstncat=4096:pstnid=1000
:pstndesc="French ISUP v5.7"
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.10.0
CHG-PSTN-PRES: MASP A - COMPLTD
```

3. Verify the changes using the `rtrv-pstn-pres` command. This is an example of possible output:

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
PSTNCAT PSTNID PSTNDESC
00001 00001 ITU Q.767
00001 00002 ETSI V3
00001 00003 UK PNO-ISC7
00001 00004 GERMAN ISUP
00001* 00020 Mexico
04096 01000 French ISUP v5.7
05000 00001 Mexican ISUP v1.8
```

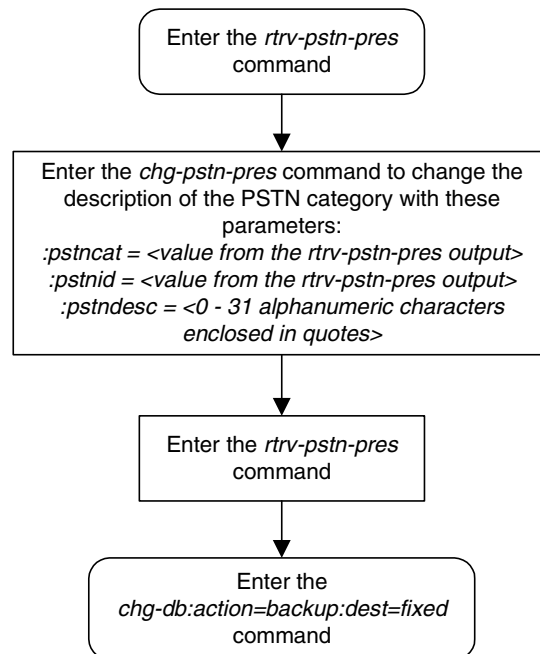
ISUP Variant table is (7 of 21) 33% full

NOTE: An * will be displayed next to the PSTN Category for entries that are no longer usable. These are entries that are disabled because their temporary feature key expired.

4. Back up the new changes, using the `chg-db:action=backup:dest=fixed` command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 4-2. Changing ISUP PSTN Presentation Value



Removing ISUP Presentation Values

This procedure is used to remove a previously defined ISUP presentation value from the ISUP variant table, using the `dlt-pstn-pres` command.

The PSTN Presentation value, consisting of a PSTN Category and PSTN ID, is used by the system to uniquely define an ISUP variant.

This command will also cause all the ISUP parameters provisioned for the variant with the `chg-isupvar-attrib` command to be deleted.

NOTE: Deleting the PSTN Presentation value may cause a loss of traffic if any routing keys are using that PSTN value. Use caution when performing this action. To display the routing keys that are using the PSTN value being removed from the database, enter the `rtrv-appl-rtkey` command with the `pstncat` and `pstnid` parameters.

NOTE: You cannot delete the PSTN Present value with Category=1, ID=2 (the ETSI V3 ISUP variant).

The `dlt-pstn-pres` command uses these parameters:

:pstncat - The PSTN Category identifying the variant being deleted is mandatory. Valid values for this parameter range from 0 to 65535.

:pstnid - The PSTN ID identifying the variant being deleted is mandatory. Valid values for this parameter range from 0 to 65535.

:force - You will need to set `force=yes` when deleting the PSTN presentation value.

Procedure

1. Display the current value of the ISUP PSTNs using the `rtrv-pstn-pres` command. This is an example of possible output:

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.10.0
PSTNCAT PSTNID PSTNDESC
00001 00001 ITU Q.767
00001 00002 ETSI V3
00001 00003 UK PNO-ISC7
00001 00004 GERMAN ISUP
00001* 00020 Mexico
04096 01000 French ISUP v5.7
05000 00001 Mexican ISUP v1.8
```

ISUP Variant table is (7 of 21) 33% full

NOTE: An * will be displayed next to the PSTN Category for entries that are no longer usable. These are entries that are disabled because their temporary feature key expired.

2. Display any routing keys that are using the PSTN value being removed from the database using the `rtrv-appl-rtkey` command with the `pstncat` and `pstnid` parameter values associated with the PSTN value being removed from the database, and the `display=all` parameter. For this example, enter this command.

```
rtrv-appl-rtkey:pstncat=04096:pstnid=01000:display=all
```

This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
```

```
KEY:LOC      DPC          SI SSN OPCA          CICS      CICE
      STATIC 12323-DE    5 --- 12212-DE    1          1000
      ATTR:PSTNCAT PSTNID NORM DUP
              4096  1000 Y    -
      SNAMEs:socket6
```

```
STATIC Route Key table is (2 of 2000) 1% full
1105  Route Key table is (2 of 500) 1% full
1107  Route Key table is (2 of 500) 1% full
```

```
STATIC Route Key Socket Association table is (2 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

If there is a routing key using the PSTN information being removed from the database, go to the “Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key” procedure on page 3-307 and change the routing keys so that they do not reference the PSTN value.

-
3. Remove the ISUP PSTN value from the database using the `dlr-pstn-pres` command with the `pstncat`, `pstnid`, and `force=yes` parameters. For this example, enter this command.

```
dlr-pstn-pres:pstncat=04096:pstnid=01000:force=yes
```

NOTE: The ISUP variant ETSI V3 (PSTNCAT=1, PSTNID=2) cannot be removed from the database.

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.10.0
DLR-PSTN-PRES: MASP A - COMPLTD
```

ISUP Variant Table Provisioning

4. Verify the changes using the `rtrv-pstn-pres` command. This is an example of possible output:

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
PSTNCAT PSTNID PSTNDESC
00001 00001 ITU Q.767
00001 00002 ETSI V3
00001 00003 UK PNO-ISC7
00001 00004 GERMAN ISUP
00001* 00020 Mexico
05000 00001 Mexican ISUP v1.8
```

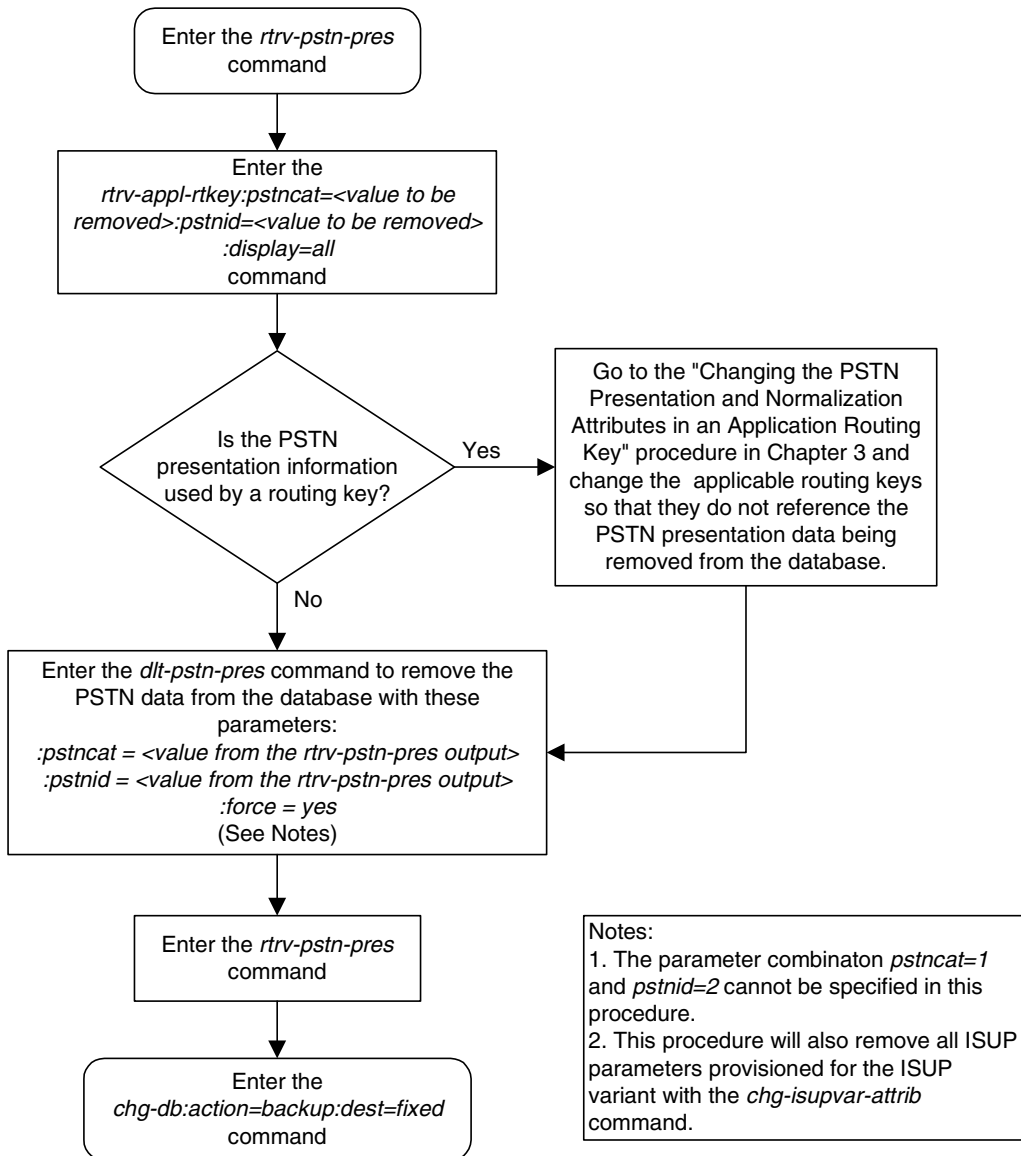
ISUP Variant table is (7 of 21) 33% full

NOTE: An * will be displayed next to the PSTN Category for entries that are no longer usable. These are entries that are disabled because their temporary feature key expired.

5. Back up the new changes, using the `chg-db:action=backup:dest=fixed` command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 4-3. Removing ISUP PSTN Presentation Value



Changing ISUP Variant Table Entries

This procedure is used to add a new ISUP presentation value to the ISUP variant table, using the `chg-isupvar-attr` command.

An ISUP variant table entry exists for each variant defined in the system. Each entry contains ISUP message and parameter data specific to the ISUP protocol used by that variant. A variant is uniquely defined by its PSTN Presentation value, consisting of a PSTN Category and PSTN ID.

The `pstncat` and `pstnid` parameters identify the ISUP variant table entry to be changed. Use the `rtrv-pstn-pres` command to display the only allowed values for the PSTN Category and ID. This procedure may be used to change any Tekelec-defined or user-defined variants that are displayed by `rtrv-pstn-pres`.

You can make the following changes to ISUP variant table entries.

- All the ISUP messages and parameters for the variant can be provisioned as defined or not defined. All the ISUP messages and parameters default to not defined until set to defined by this command.
- All the ISUP parameters for specific messages in the variant can be provisioned as supported or not supported. All the ISUP parameters default to not supported until set to supported by this command.
- The minimum valid parameter length can be specified for each defined ISUP parameter.
- All the ISUP messages that are provisioned as defined can also have a message conversion action assigned.
- All the ISUP parameters that are provisioned as supported can also have a parameter conversion action assigned.
- All the ISUP parameters that are provisioned as supported, can also be assigned as optional, mandatory-fixed (MF), or mandatory-variable (MV).
- If assigned as MF or MV, the numerical order the parameter appears in the message must be specified.

NOTE: You cannot change the attributes for the ETSI V3 ISUP variant (PSTN Category=1, PSTN ID=2).

The PSTN presentation value, consisting of a PSTN category and PSTN ID, is used by the system to uniquely define an ISUP variant. The assignment of a new PSTN value also creates a new entry in the ISUP variant table. The new PSTN value must be unique.

This procedure may be used to change values within the Tekelec-defined range (PSTN Category 0-4095) as long as these control features are enabled:

- the controlled feature for the new PSTN category
- ISUP Normalization control feature

This procedure may be used to change values within the user-defined range (PSTN Category 4096-65535) as long as these control features are enabled:

- the controlled feature for the new PSTN category
- ISUP Normalization control feature
- ISUP Normalization Quantity control feature, to make sure that the quantity of user-defined PSTN categories is not exceeded.

The `chg-isupvar-attrib` command uses these parameters:

:pstncat - The PSTN category identifying the new variant being defined. Valid values for this parameter range from 0 to 65535.

:pstnid - The PSTN ID identifying the new variant being defined. Valid values for this parameter range from 0 to 65535.

:msgcode - The ISUP message type code. This parameter is used to identify a specific ISUP message that is going to have its attributes changed. Valid values are 0-255 (h'00 - h'FF).

:parmcode - The ISUP parameter code. This parameter is used to identify a specific ISUP parameter that is going to have its attributes changed. When specified with the `msgcode` parameter, the `parmcode` parameter identifies a parameter within the `msgcode` parameter that is going to have its attributes changed. Valid values are 0-255 (h'00 - h'FF).

:attrib - The attribute being assigned to a message or parameter. This parameter can have values of `defined`, `notdefined`, `supp`, or `notsupp`.

- `defined` – the message or parameter is defined in the variant.
- `notdefined` – the message or parameter is not defined in the variant.
- `supp` – the parameter is supported in the specified message in the variant.
- `notsupp` – the parameter is not supported in the specified message in the variant.

:minlen - The minimum parameter length. This parameter has valid values of 0-255 (h'00 - h'FF). It is used for validating that the length of the received parameter is at least as long as the `minlen` parameter value.

:parmtyp - The type of ISUP parameter, and has valid values of `opt`, `mf`, or `mv`.

- `opt` – The parameter may appear in the Optional part of the ISUP message. This is the default and it does not have to be specified unless the parameter needs to be changed from either `mf` or `mv` to optional.
- `mf` – The parameter must appear in the Mandatory Fixed part of the ISUP message.
- `mv` – The parameter must appear in the Mandatory Variable part of the ISUP message.

ISUP Variant Table Provisioning

:order - The order in which the mandatory parameters appear in the message. Valid values are from 1 to 7.

:action - The message or parameter conversion action the software will follow when a message is received with the specified **msgcode** parameter value or the **msgcode/parmcode** parameter combination. Valid values are **none**, **convert**, and **passthru**.

- **none** – The software will follow its normal conversion rules. No special conversions will occur. This is the default.
- **convert** – The software will invoke a special conversion routine that is available in the system for the specified **msgcode** parameter value or **msgcode/parmcode** parameter combination.
- **passthru**, for the **msgcode** parameter, – The specified message code should be passed through unconverted using the raw MTP3 transfer method.
- **passthru**, for the **msgcode/parmcode** parameter combination, – The parameter code, when encountered in message code, should be passed through to the normalized section of the message (ignoring the **defined** or **supp** attributes of the normalized specification).

:force – Used to allow the ISUP Message Type Code to be changed to **notdefined**. This parameter has values of **yes** and **no**.

Table 4-2 on page 4-20 shows the parameter combinations that can be used with the **chg-isupvar-attrib** command.

Table 4-2. CHG-ISUPVAR-ATTRIB Parameter Combinations

Parameter Combination 1	Parameter Combination 2	Parameter Combination 3	Parameter Combination 4	Parameter Combination 5
pstncat = 0-65535 ¹ pstnid = 0-65535 ¹ msgcode = 0-255 attrib = defined action = none, convert, passthru ^{6,7}	pstncat = 0-65535 ¹ pstnid = 0-65535 ¹ msgcode = 0-255 attrib = notdefined force ³	pstncat = 0-65535 ¹ pstnid = 0-65535 ¹ parmcode = 0-255 attrib = defined minlen = 0-255 ²	pstncat = 0-65535 ¹ pstnid = 0-65535 ¹ parmcode = 0-255 attrib = notdefined	pstncat = 0-65535 ¹ pstnid = 0-65535 ¹ msgcode = 0-255 parmcode = 0-255 attrib = supp action = none, convert, passthru ^{6,7}
Parameter Combination 6	Parameter Combination 7	Parameter Combination 8	Parameter Combination 9	
pstncat = 0-65535 ¹ pstnid = 0-65535 ¹ msgcode = 0-255 parmcode = 0-255 attrib = supp parmtyp = opt ⁴ action = none, convert, passthru ^{6,7}	pstncat = 0-65535 ¹ pstnid = 0-65535 ¹ msgcode = 0-255 parmcode = 0-255 attrib = supp parmtyp = mf ⁵ order = 1-7 action = none, convert, passthru ^{6,7}	pstncat = 0-65535 ¹ pstnid = 0-65535 ¹ msgcode = 0-255 parmcode = 0-255 attrib = supp parmtyp = mv ⁵ order = 1-7 action = none, convert, passthru ^{6,7}	pstncat = 0-65535 ¹ pstnid = 0-65535 ¹ msgcode = 0-255 parmcode = 0-255 attrib = notsupp	
<p>Notes:</p> <ol style="list-style-type: none"> 1. The parameter combination pstncat=1 and pstnid=2 cannot be specified with the chg-isupvar-attrib command. 2. The minlen=0 parameter is valid only for the parmcode=0 (EOP) parameter. Otherwise, the values for this parameter are from 1 to 255. 3. Changing an ISUP Message Type Code to notdefined will clear all the associated parameter data. In this case, the force=yes parameter is required. Changing an ISUP Message Type Code to notdefined is destructive and will clear all the associated parameter data for that ISUP Message Type Code. 4. The opt value is the default value for the parmtyp parameter and it does not have to be specified unless the parameter value needs to be changed from mf or mv to opt. 5. The parmtyp parameter may be changed as long as the change does not violate the rules of the order parameter. The mf parameters must be specified in an ordered list starting with 1. The mv parameters must be specified in a different ordered list starting with 1. There can be no gaps in order number. A mf or mv parameter cannot be removed from a list (that is, changing parmtyp parameter value, or changing the attrib parameter value to notsupp) unless all parameters with a higher order number are deleted first. 6. The none value is the only valid value for the action parameter when the parmcode=0 parameter is specified. 7. The action parameter can be specified for user-defined variants, however the system will ignore the convert value. There will be no supported conversion action. 				

ISUP Variant Table Provisioning

Procedure

1. Display the current value of the ISUP supported parameters for all the variants using the `rtrv-isupvar-attr` command. This is an example of possible output.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.10.0
```

```
PSTNCAT PSTNID
```

```
00001 00001
```

MSGCODE	PARMCODE	TYPE	ORDER	ACTION
01h	---	---	-	NONE
	45h	MF	1	NONE
	00h	OPT	-	NONE
	40h	OPT	-	NONE

MSGCODE	PARMCODE	TYPE	ORDER	ACTION
0Ah	---	---	-	CONVERT
	45h	MF	1	NONE
	4Ch	MV	1	NONE
	00h	OPT	-	NONE
	56h	OPT	-	PASSTHRU

MSGCODE	PARMCODE	TYPE	ORDER	ACTION
0Bh	---	---	-	NONE
	45h	MF	1	NONE
	71h	MF	2	NONE
	00h	OPT	-	NONE
	72h	OPT	-	CONVERT

```
PSTNCAT PSTNID
```

```
00001 00002
```

MSGCODE	PARMCODE	TYPE	ORDER	ACTION
01h	---	---	-	NONE
	45h	MF	1	NONE
	00h	OPT	-	NONE
	40h	OPT	-	NONE

MSGCODE	PARMCODE	TYPE	ORDER	ACTION
0Ah	---	---	-	NONE
	45h	MF	1	NONE
	4Ch	MV	1	NONE
	00h	OPT	-	NONE
	10h	OPT	-	NONE
	56h	OPT	-	NONE

```
PSTNCAT PSTNID
```

```
04097 00001
```

MSGCODE	PARMCODE	TYPE	ORDER	ACTION
01h	---	---	-	NONE
	45h	MF	1	NONE
	00h	OPT	-	NONE
	40h	OPT	-	PASSTHRU

MSGCODE	PARMCODE	TYPE	ORDER	ACTION
0Ah	---	---	-	CONVERT
	45h	MF	1	NONE
	4Ch	MV	1	NONE
	00h	OPT	-	NONE
	56h	OPT	-	CONVERT

```
ISUP Variant table is (5 of 20) 25% full
```

2. Display enabled controlled feature information in the database by entering the `rtrv-ctrl-feat` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
The following features have been permanently enabled:
```

Feature Name	Partnum	Status	Quantity
IPGWx Signaling TPS	893012814	on	20000
ISUP Normalization	893000201	on	----
ETSI v3 Normalization	893000601	on	----

The following features have been temporarily enabled:

Feature Name	Partnum	Status	Quantity	Trial Period	Left
Zero entries found.					

The following features have expired temporary keys:

Feature Name	Partnum
Zero entries found.	

If the ISUP Normalization control feature, the controlled feature for the new PSTN category, and if a user-defined PSTN category is being changed, or the ISUP Normalization Quantity control feature have not been enabled and turned on, go to the “Enabling Controlled Features” procedure on page 6-2 and to “Turning On and Off Controlled Features” procedure on page 6-10 to enable and turn on these controlled features.

3. Enter the desired new values of the ISUP supported parameters using the `chg-isupvar-attrib` command and using one of the parameter combinations shown in Table 4-2 on page 4-20. For this example, enter this command.

```
chg-isupvar-attrib:pstncat=4097:pstnid=1:msgcode=10
:parmcode=100:attrib=supp:parmtyp=mv:order=1:action=passthru
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.10.0
CHG-ISUPVAR-ATTRIB: MASP A - COMPLTD
```

ISUP Variant Table Provisioning

4. Verify the changes using the `rtrv-isupvar-attrib` command with the `pstncat` and `pstnid` values used in step 3. For this example, enter this command.

```
rtrv-isupvar-attrib:pstncat=4097:pstnid=1
```

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.10.0
PSTNCAT PSTNID
04097 00001
```

MSGCODE	PARMCODE	TYPE	ORDER	ACTION
01h	---	---	-	NONE
	45h	MF	1	NONE
	00h	OPT	-	NONE
	40h	OPT	-	PASSTHRU

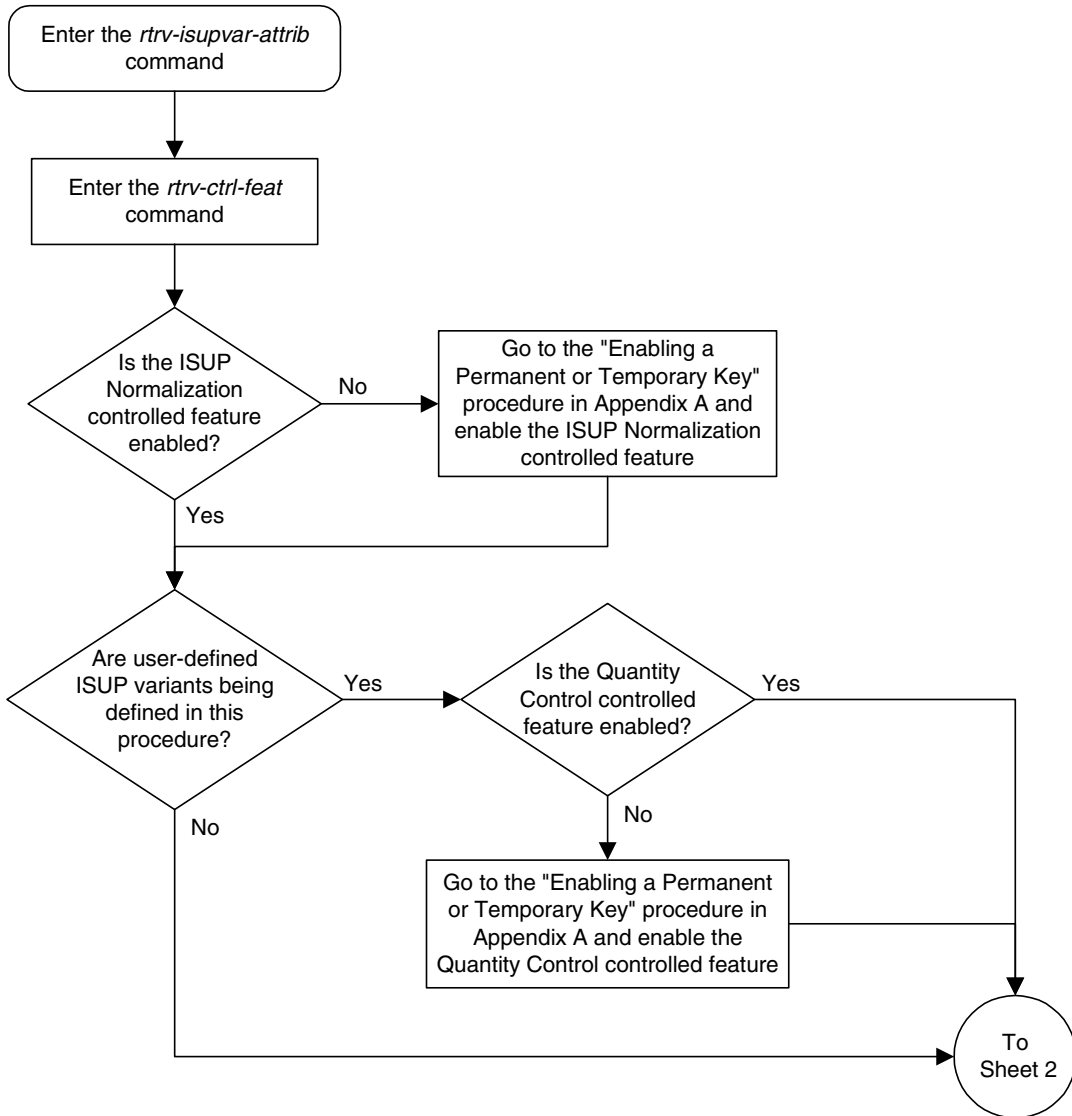
MSGCODE	PARMCODE	TYPE	ORDER	ACTION
0Ah	---	---	-	CONVERT
	45h	MF	1	NONE
	4Ch	MV	1	NONE
	00h	OPT	-	NONE
	56h	OPT	-	CONVERT
	64h	MV	1	PASSTHRU

```
ISUP Variant table is (5 of 20) 25% full
```

5. Back up the new changes, using the `chg-db:action=backup:dest=fixed` command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

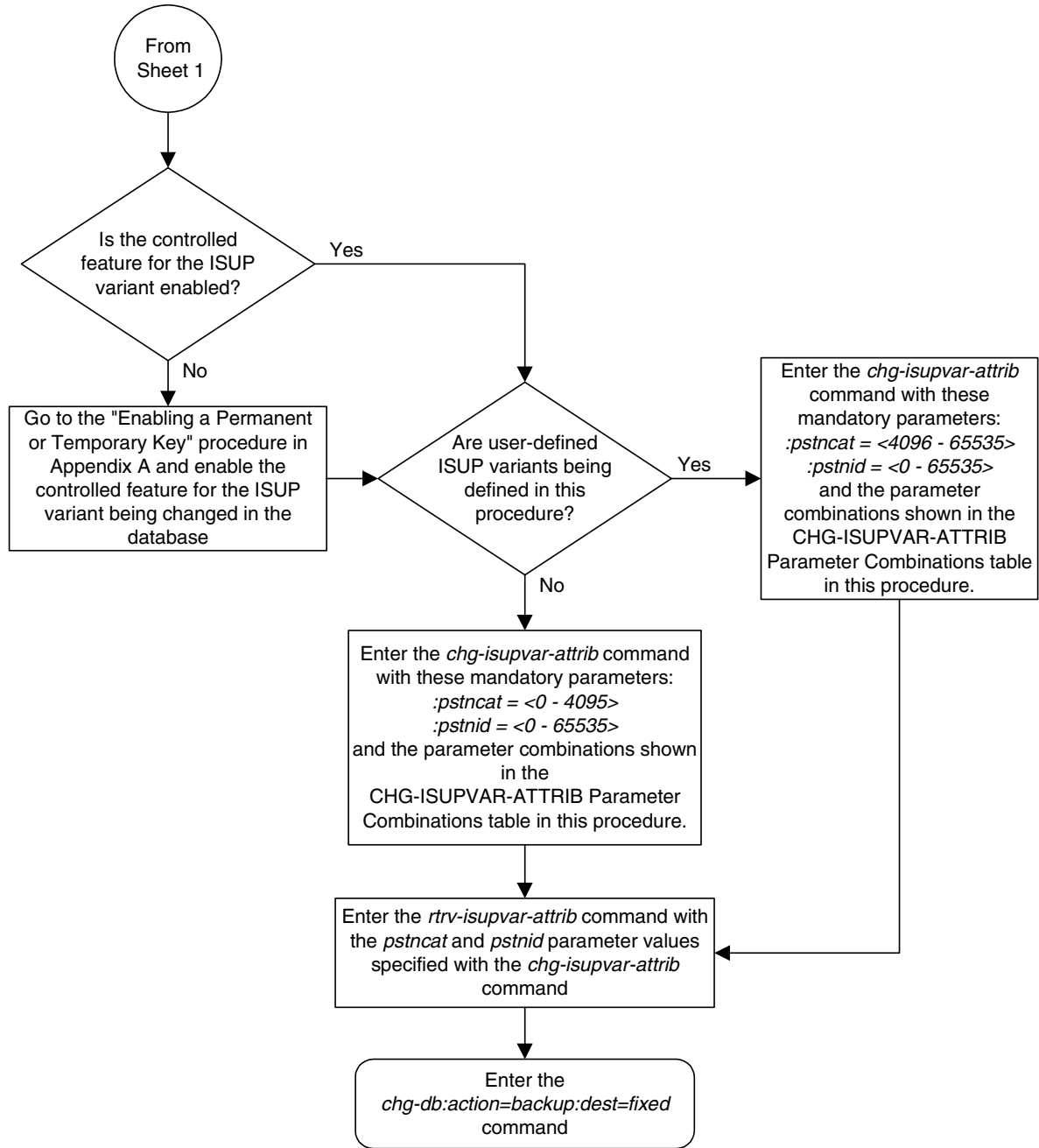
```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

Flowchart 4-4. Changing ISUP Attribute Values (Sheet 1 of 2)



ISUP Variant Table Provisioning

Flowchart 4-4. Changing ISUP Attribute Values (Sheet 2 of 2)



Copying ISUP Variant Table Entries

The `copy-isupvar-attr` command is used to copy one ISUP variant table entry to another ISUP variant table entry.

This command provides you with an easy way to provision a new ISUP variant table entry by copying all the data from another entry. You can then change the entry with the `chg-isupvar-attr` command.

An ISUP variant table entry exists for each variant defined in the system. Each entry contains ISUP message and parameter data specific to the ISUP protocol used by that variant. A variant is uniquely defined by its PSTN presentation value, consisting of a PSTN category and PSTN ID.

The PSTN presentation is used to identify both the source and destination table entries. Both entries must be previously defined PSTN presentation values, that is, either a Tekelec-defined PSTN or a user-defined PSTN entered into the database by the `ent-pstn-pres` commands. Use the `rtrv-pstn-pres` command to display the only allowed values for the source and destination PSTNs.

Tekelec-defined PSTNs (PSTN Category 0-4095) require that these control features are enabled:

- The controlled feature for the PSTN category
- ISUP Normalization control feature

User-defined PSTNs (PSTN Category 4096-65535) require that these control features are enabled:

- The controlled feature for the PSTN category
- ISUP Normalization control feature
- ISUP Normalization Quantity control feature, to make sure that the quantity of user-defined PSTN categories is not exceeded.

NOTE: The destination PSTN cannot be the ETSI V3 ISUP variant (PSTNCAT=1, PSTNID=2).

The `copy-isupvar-attr` command uses these parameters:

:pstncat – The source variant table entry being copied. Valid values for this parameter range from 0 to 65535.

:pstnid – The source variant table entry being copied. Valid values for this parameter range from 0 to 65535.

:dpstncat – The destination variant table entry where the source variant table is being copied. Valid values for this parameter range from 0 to 65535.

:dpstnid – The destination variant table entry where the source variant table is being copied. Valid values for this parameter range from 0 to 65535.

ISUP Variant Table Provisioning

Procedure

1. Display the current value of the ISUP supported parameters for all the variants using the `rtrv-isupvar-attr` command. This is an example of possible output:

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
PSTNCAT PSTNID
00001 00001

  MSGCODE  PARMCODE  TYPE  ORDER  ACTION
  01h      ---      ---   -      NONE
           45h      MF     1      NONE
           00h      OPT    -      NONE
           40h      OPT    -      NONE

  MSGCODE  PARMCODE  TYPE  ORDER  ACTION
  0Ah      ---      ---   -      CONVERT
           45h      MF     1      NONE
           4Ch      MV     1      NONE
           00h      -      -      NONE
           56h      -      -      PASSTHRU

  MSGCODE  PARMCODE  TYPE  ORDER  ACTION
  0Bh      ---      ---   -      NONE
           45h      MF     1      NONE
           71h      MF     2      NONE
           00h      OPT    -      NONE
           72h      OPT    -      CONVERT

PSTNCAT PSTNID
00001 00002

  MSGCODE  PARMCODE  TYPE  ORDER  ACTION
  01h      ---      ---   -      NONE
           45h      MF     1      NONE
           00h      OPT    -      NONE
           40h      OPT    -      NONE

  MSGCODE  PARMCODE  TYPE  ORDER  ACTION
  0Ah      ---      ---   -      NONE
           45h      MF     1      NONE
           4Ch      MV     1      NONE
           00h      OPT    -      NONE
           10h      OPT    -      NONE
           56h      OPT    -      NONE

PSTNCAT PSTNID
04097 00001

  MSGCODE  PARMCODE  TYPE  ORDER  ACTION
  01h      ---      ---   -      NONE
           45h      MF     1      NONE
           00h      OPT    -      NONE
           40h      OPT    -      PASSTHRU

  MSGCODE  PARMCODE  TYPE  ORDER  ACTION
  0Ah      ---      ---   -      CONVERT
           45h      MF     1      NONE
           4Ch      MV     1      NONE
           00h      OPT    -      NONE
           56h      OPT    -      CONVERT

ISUP Variant table is (5 of 20) 25% full
```

2. Display enabled controlled feature information in the database by entering the **rtrv-ctrl-feat** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
The following features have been permanently enabled:
```

Feature Name	Partnum	Status	Quantity
IPGWx Signaling TPS	893012814	on	20000
ISUP Normalization	893000201	on	----
ETSI v3 Normalization	893000601	on	----

The following features have been temporarily enabled:

Feature Name	Partnum	Status	Quantity	Trial Period Left
Zero entries found.				

The following features have expired temporary keys:

Feature Name	Partnum
Zero entries found.	

If the ISUP Normalization control feature, the controlled feature for the new PSTN category, and if a user-defined PSTN category is being changed, or the ISUP Normalization Quantity control feature have not been enabled and turned on, go to the "Enabling Controlled Features" procedure on page 6-2 and to "Turning On and Off Controlled Features" procedure on page 6-10 to enable and turn on these controlled features.

3. Copy an ISUP PSTN value using the **copy-isupvar-attrib** command. For this example, enter this command.

```
copy-isupvar-attrib:pstncat=1:pstnid=2:dpstncat=1:dpstnid=20
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-10 11:43:04 GMT EAGLE5 31.10.0
COPY-ISUPVAR-ATTRIB: MASP A - COMPLTD
```


ISUP Variant Table Provisioning

4. Verify the changes using the `rtrv-isupvar-attrib` command with the `pstncat` and `pstnid` parameters. Use the `dpstncat` and `dpstnid` parameter values used in step 3 for the values of the `pstncat` and `pstnid` parameters. For this example, enter this command.

```
rtrv-isupvar-attrib:pstncat=1:pstnid=20
```

This is an example of the possible output.

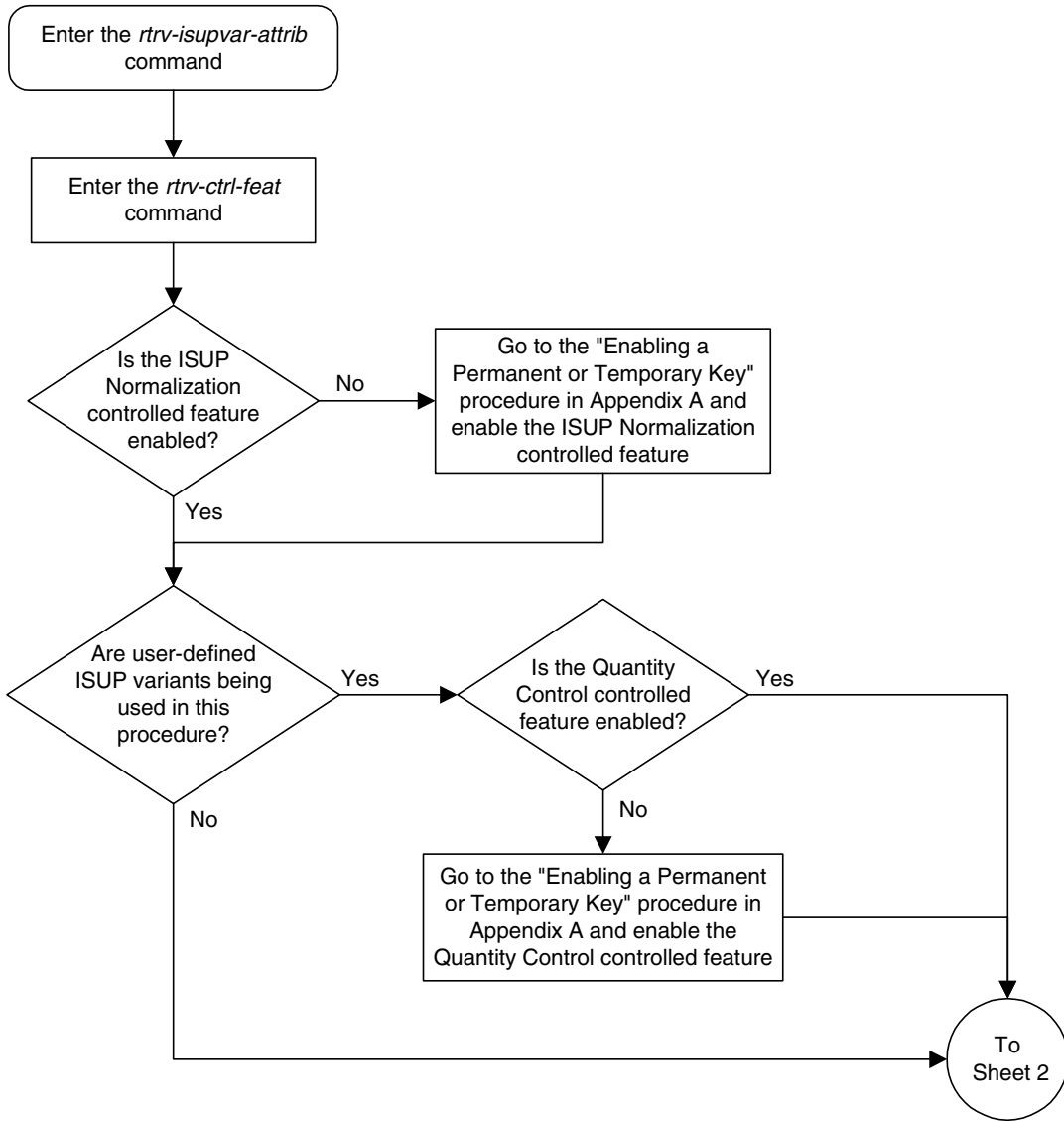
```
PSTNCAT  PSTNID
00001    00020

  MSGCODE  PARMCODE  TYPE  ORDER  ACTION
    01h     ---      ---   -      NONE
          45h      MF    1      NONE
          00h      OPT   -      NONE
          40h      OPT   -      NONE
  MSGCODE  PARMCODE  TYPE  ORDER  ACTION
  0Ah      ---      ---   -      NONE
          45h      MF    1      NONE
          4Ch      MV    1      NONE
          00h      OPT   -      NONE
          10h      OPT   -      NONE
          56h      OPT   -      NONE
```

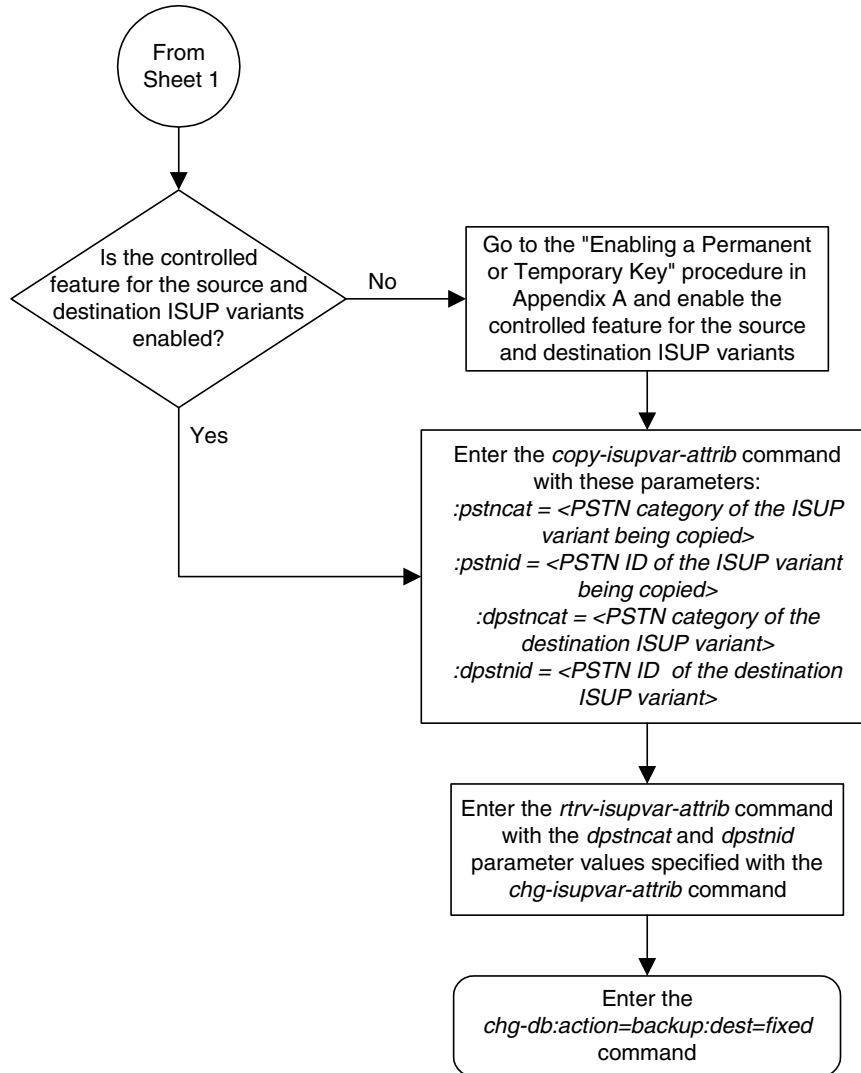
5. Back up the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 4-5. Copying ISUP Attribute Values (Sheet 1 of 2)



Flowchart 4-5. Copying ISUP Attribute Values (Sheet 2 of 2)



5

End Office Support

Overview	5-2
Internal Point Code	5-4
Adding an End Node Internal Point Code	5-14
Removing an End Node Internal Point Code.....	5-18

Overview

End Office Support enables the system to share its true point code (TPC) with an IP-based node without the need for a separate point code for the IP node. When the End Office Support feature is in use, the system shares a point code for up to three network types with attached IP network elements.

The system product lets you take advantage of next generation network technology by migrating existing signaling end points from the PSTN to the IP network. The fact that the system is a signaling transfer point and has its own point code, however, can present a significant network management issue. This feature provides the means to perform the migration without obtaining a new point code or reconfiguring the network to interface with both the system and an IP end office node.

This feature defines a new administered element, the "Remote Application," and alters the system's behavior with respect to its true point codes (or self-IDs). The vast majority of the system's STP features are unaffected by End Office Support.

Characteristics of this feature include:

- The system allows a set of IP network elements to share its true point code.
- The system allows messages destined to its true point code and having SI>=3 to be forwarded to an IP network element.
- The system enables IP networks elements sharing its true point code to participate in network management.
- The system supports ANSI, ITU national and international end office nodes.
- The system implements the MTP procedures required for an end office node.
- The End Office Support feature does not reduce the rated TPS of any system application.

The Remote Application Table contains fields for assigning each user part to an end office node. The default value is 'not assigned'.

New Remote Application Table commands provide for adding, deleting, and retrieving user-part assignments:

- **ent-rmt-appl**
- **dlt-rmt-appl**
- **rtrv-rmt-appl**

The user parts SI=0, SI=1, and SI=2 cannot be assigned to an end office node. The SNM case is a special case in that UPU's may be forwarded, even though SI=0 cannot be assigned to a remote application. All other SNMs are processed as destined to the system rather than the EO Node. This often results in a multicast throughout the system that updates the routing tables on all cards. An EO Node can receive these messages via replication performed by MTPP.

End Office Support

Each SS7-based application that receives a message destined to a TSPC checks the user-part assignment within the Remote Application Table. If the user-part is assigned and $SI \geq 3$, then the message is forwarded to the appropriate application, otherwise it is processed as though destined to the system.

To assign a remote application for the SCCP ($SI=3$) user part, you must also specify a subsystem number. The Remote Application Table maintains a record of assignments for all possible subsystems (256). Subsystems are either assigned or not assigned.

NOTE: SSN=0 is normally an invalid value. This feature makes use of SSN=0 for the purpose of forwarding certain MSUs to the EO Node.

- Received SCCP Messages that indicate route-on-global-title are treated as having $SSN=0$ for remote application assignment. If a remote application is assigned to $SSN=0$, then the message is forwarded, otherwise it is distributed to the local SCCP application. In previous releases, this would occur only for mis-configured networks. Messages indicating route-on-global-title and intended for the system, not the EO Node, should be sent to the system's capability point code.
- Received SCCP Messages that lack a Called Party SS are treated as having $SSN=0$ for remote application assignment. If a remote application is assigned to $SSN=0$, then the message is forwarded, otherwise it is distributed to the local SCCP application.
- Received SCCP Messages having a Called Party SS equal to SCMG ($SSN=1$) are processed and terminated by the system, and if $SSN=1$ has a remote application assigned, the MSU is also replicated and forwarded to the EO Node.
- Received SSCP Messages having a Called Party SSN not equal to 0 or SCMG (1) and for which a remote application is assigned are forwarded to the end office node. Messages received for unassigned subsystems are distributed to the local SCCP application.
- The EO Node cannot share SCCP subsystems (other than SCMG) with the system. If the EO Node assigns a given subsystem, such as LNP, then the subsystem local to the system cannot receive messages. Remote applications take priority over local applications.

Internal Point Code

To route SS7 messages to the IP address without adding another external point code, the End Office feature uses an internal point code (IPC). This point code is private to the system, and the PSTN has no awareness of it. Its sole purpose is to allow messages destined to the End Office Node to be routed from the inbound LIM to the IPGWx card (a card running either the SS7IPGW or IPGWI applications). An IPC must be entered as a destination and must be assigned for each network type having an end office node. This point code is also used internally by the system in order to route inbound messages to the outbound IPGWx card. The system can have up to three IPCs, one for ANSI, one for ITU International, and one for ITU National networks.

Table 5-1 displays a sample Remote Application Table. The Network Type and SI are used to index into the table, rather than being stored in the table.

Table 5-1. Sample IPC Values

IPC	Assigned to EO Node	Assigned SSNs	Network Type	User-Part (SI)	Action taken when MSU is received for the TPC
0-1-0	FALSE	n/a	ANSI	0	No application can be assigned for SI=0. Note that TFCs are processed, replicated and sent to an EO Node, if an application is assigned to any other user part. UPUs are forwarded if the application specified by the affected SI is assigned.
	FALSE	n/a		1	No application can be assigned for SI=1.
	FALSE	n/a		2	No application can be assigned for SI=2.
	TRUE	3, 7, 100		3	SCCP messages destined to the TSPC and with SSN assigned are forwarded to an EO Node. SCCP messages destined to a TSPC and SSN not assigned are distributed to subsystems local to the system (e.g. LNP).
	FALSE	n/a		4	Terminate with UPU.
	TRUE	n/a		5	ISUP messages destined to a TSPC are forwarded to the EO Node.
	FALSE	n/a		6 - 15	Terminate with UPU.
110	FALSE	n/a	ITU-N	0	No application can be assigned for SI=0. TFCs are processed, replicated and sent to an EO Node, if an application is assigned to any other user part. UPUs are forwarded if the application specified by the affected SI is assigned.
	FALSE	n/a		1	No application can be assigned for SI=1.

End Office Support

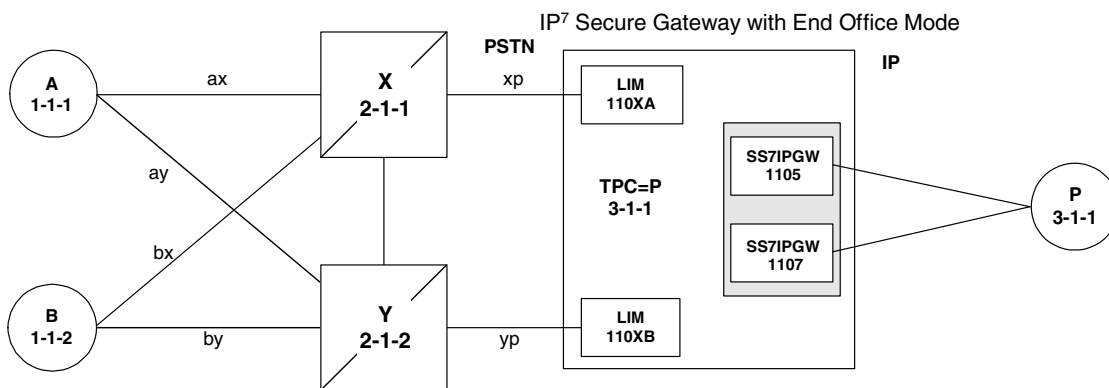
Table 5-1. Sample IPC Values (Continued)

IPC	Assigned to EO Node	Assigned SSNs	Network Type	User-Part (SI)	Action taken when MSU is received for the TPC
	FALSE	n/a		2	No application can be assigned for SI=2.
	FALSE	NULL		3	Distribute to local SCCP.
	TRUE	n/a		4	TUP messages destined to the TSPC are forwarded to the EO Node.
	FALSE	n/a		5 - 12	Terminate with UPU.
	TRUE	n/a		13	QBICC messages destined to the TSPC are forwarded to the EO Node.
	FALSE	n/a		14, 15	Terminate with UPU.
0-10-1	FALSE	n/a	ITU-I	0	No application can be assigned for SI=0. TFCs are processed, replicated and sent to an EO Node, if an application is assigned to any other user part. UPUs are forwarded if the application specified by the affected SI is assigned.
	FALSE	n/a		1	No application can be assigned for SI=1.
	FALSE	n/a		2	No application can be assigned for SI=2.
	FALSE	NULL		3	Distribute to local SCCP.
	TRUE	n/a		4	TUP messages destined to the TSPC are forwarded to the EO Node.
	FALSE	n/a		5 - 15	Terminate with UPU.

New Installation of VXI Behind a System with End Office Support

Figure 5-1 depicts a network in which a VXI node is deployed behind a system with End Office Support. Note that the VXI node resides in the IP network and shares the system's true point code. The PSTN views the system and VXI as one network element (one point code).

Figure 5-1. A System with End Office Support and VXI Node



One Node Migrates from PSTN to IP

Figure 5-2 and Figure 5-3 depict the migration of a signaling end point from the PSTN to an IP network using the system with the End Office Support feature.

Figure 5-2. Network Before a System with End Office, Node P is to Migrate

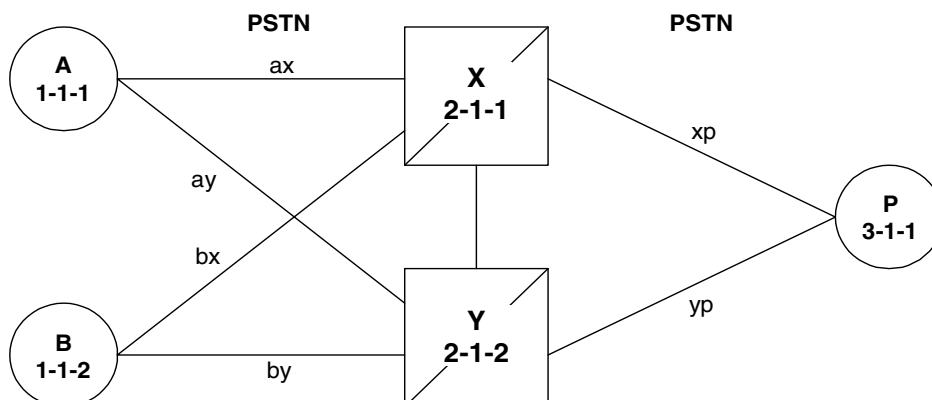
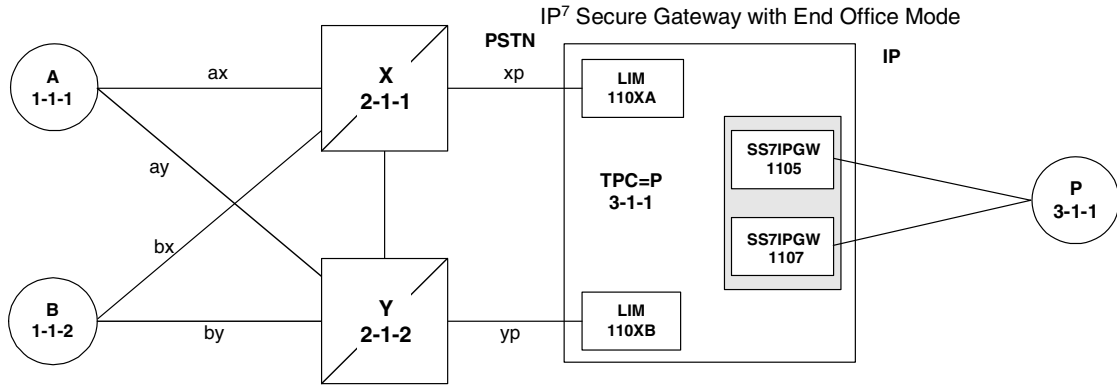


Figure 5-3. Network After a System with End Office, Node P has Migrated



In Figure 5-3 the system no longer acts like a signaling transfer point, but rather acts like a signaling end point that has an IP-attached application user-part. The system and the IP network element share the point code P. All messages received by the system should be destined to P and all messages sent to the PSTN from the system have an OPC of P.

A Signaling End Point is Added to a Deployed System Using End Office

Another possible scenario for the End Office feature is that a customer has a deployed system with attached IP nodes, and wants to make use of the End Office feature to add a new IP node. Consider the following network diagrams, Figure 5-4 and Figure 5-5.

Figure 5-4. Original Network with Deployed System

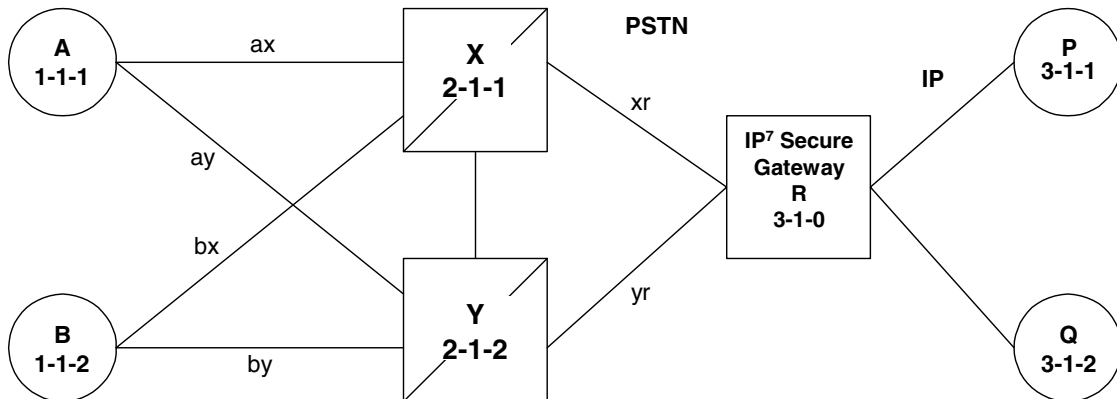
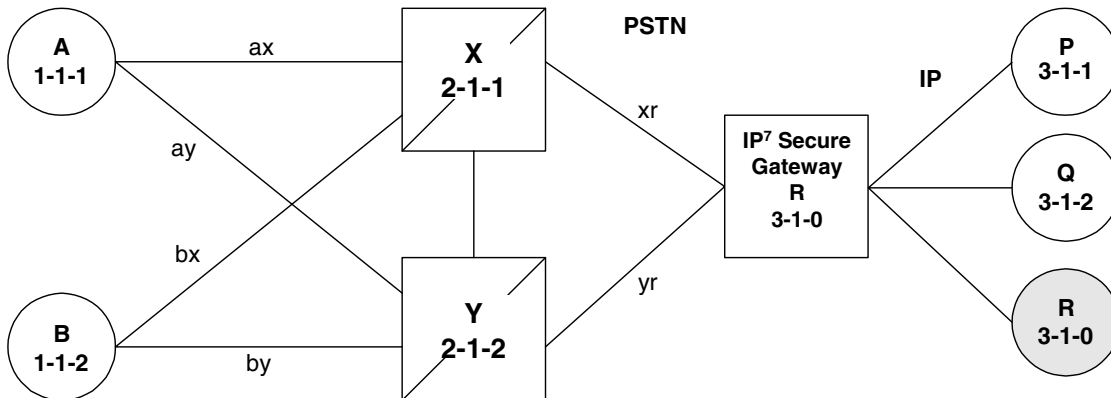


Figure 5-5. New Network with a System Using End Office and End Node R



In Figure 5-5 the customer saves a point code by using the End Office feature and making the new IP network element an end office node. No change is required in the PSTN or at P or Q. Non-network-management and non-test messages destined to R are now forwarded to an IP network element, rather than terminated by the system.

Two Signaling End Points Move from PSTN to IP Using End Office

A more complex scenario arises when multiple signaling end points are to migrate from the PSTN to an IP network using the End Office feature. Consider Figure 5-6 and Figure 5-7.

Figure 5-6. Network before Two Signaling End Points Migrate from PSTN to IP

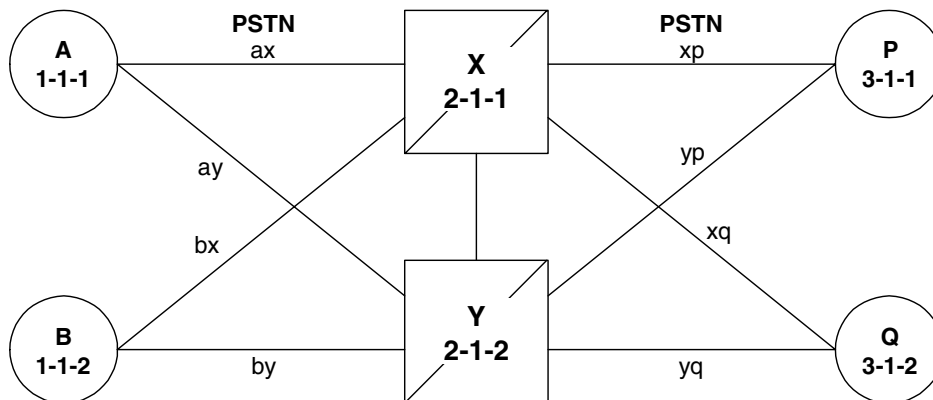
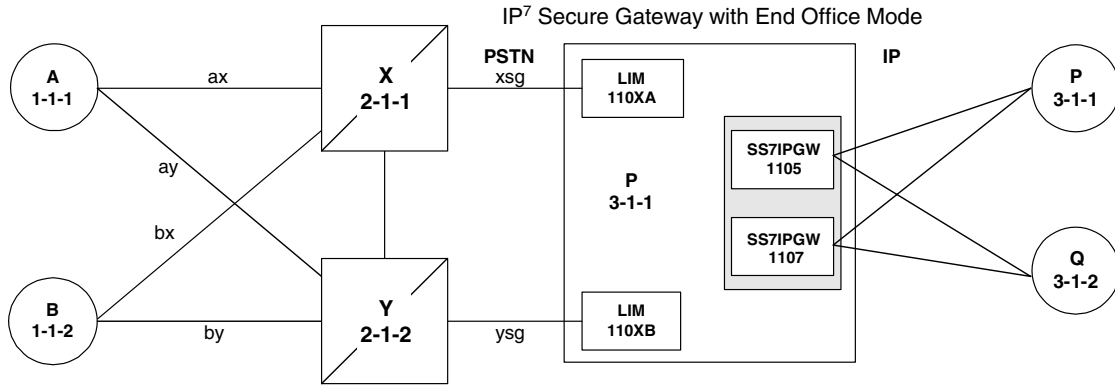


Figure 5-7. Network after Two Signaling End Points Migrate from PSTN to IP



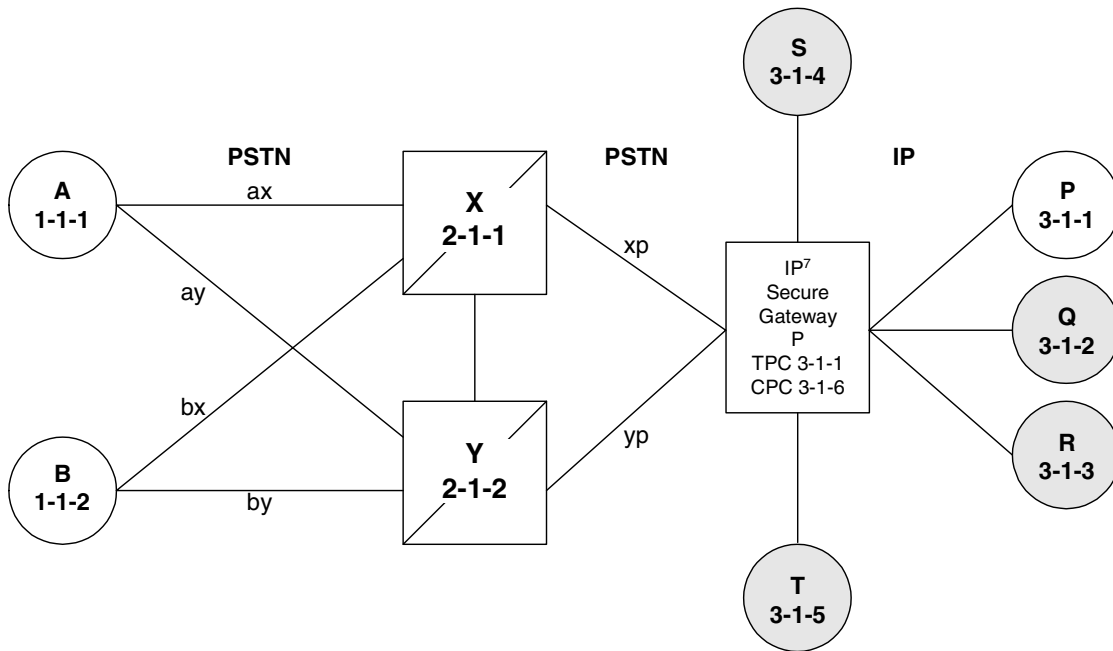
In Figure 5-7, P is an end office node, and so P serves as the adjacent point code for nodes X and Y. The following are key points about this figure:

- Q is not an end office node, and so the system behaves as an STP for messages originated by and destined to Q.
- Reprovisioning is required in the PSTN, since the Q is now behind P. One example of this is that the linksets between X and Q and between Y and Q must change.
- Traffic between P and Q are no longer routed through X/Y, but are routed within the system.

The System Simultaneously Acts as STP and End Office

Figure 5-8 on page 5-10 depicts the system supporting three IP network elements, only one of which use the End Office feature, and two PSTN network elements. In addition, a capability point code is provisioned on the system, thereby allowing the use of GTT.

Figure 5-8. The System Simultaneously Acts as STP and End Office



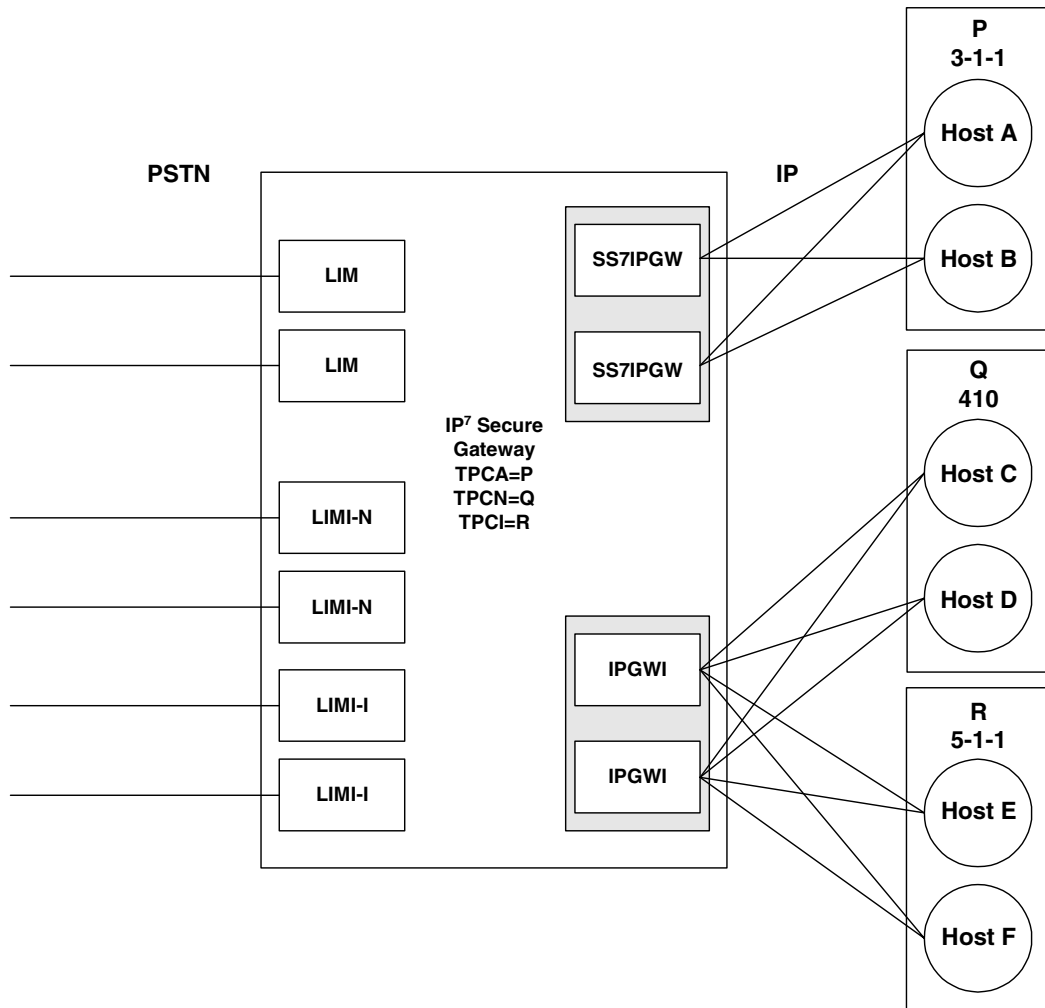
Notes regarding Figure 5-8:

- P is the end office node, and so the system TPC=P.
- Assume that end node P has an application assignment for SCCP.
- SCCP traffic destined to P is forwarded to the IP node via the SS7IPGW application.
- SCCP traffic destined to the CPC is distributed to the system's local SCCP application (e.g. GTT).
- Network elements Q, R, S, and T are not end office nodes, and so the system generates TFX network management concerning them.
- IP Network element P is an end office node, and so the system generates only UPU/SSP concerning it.

The System Supports Multiple Network Types and Multiple Hosts as an End Node

In Figure 5-9 on page 5-11 the system supports an end office node for each of the three network types. Each end office node comprises multiple IP network elements. The IP network elements are distinguished by rhost+rport (IP address parameters).

Figure 5-9. Three Multiple-Element End Office Nodes



Mated Pair Supports Two End Office Nodes

Figure 5-10 depicts a mated pair of systems with each system supporting an End Office Node. Note that system P lacks IP links to IPNE-Q and system Q lacks IP links to IPNE-P, since such links would conflict with the C-links of linkset pq.

Figure 5-10. Mated Pair Supports Two End Office Nodes

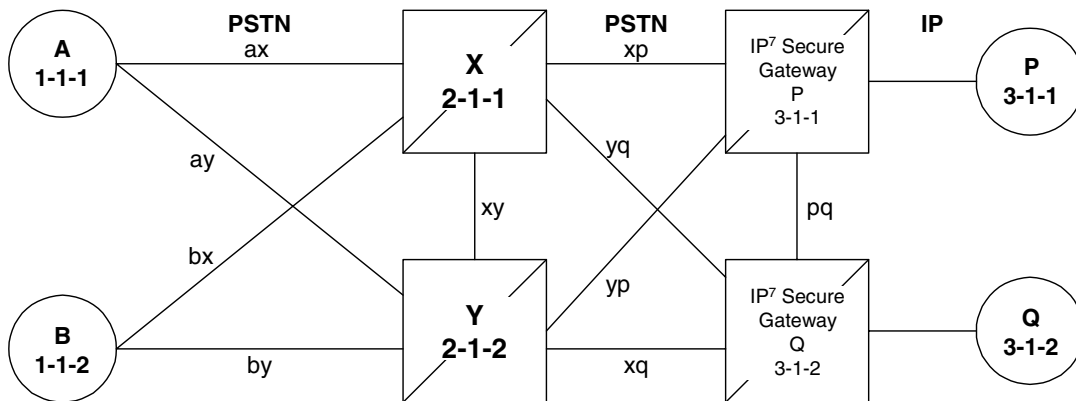


Figure 5-10 shows that a mated pair of systems cannot share an End Office Node. Each system requires its own unique point code and so any attached End Office Nodes share those point codes. It would be possible for a single IP network element to act as both P and Q (have IP connections to both system P and system Q). This configuration, however, would not provide true redundancy. Messages destined to P are terminated either at system P or IPNE-P, and message destined to Q are terminated either at system Q or IPNE-Q. Should the IP link between system P and IPNE-P fail, this feature provides no way for system P to forward messages to the End Office Node using the linkset pq (the linkset between systems P and Q).

End Office Support Configuration

In addition to the internal point code provisioned in the database with the “Adding an End Node Internal Point Code” procedure on page 5-14, these entities must be configured in the database to support the End Office feature.

- The internal point code must be in the destination point code table - go to the “Adding a Destination Point Code” procedure in the *Database Administration Manual - SS7*.
- An SS7 route to the internal point code - “Adding a Route” procedure in the *Database Administration Manual - SS7*.
- Signaling links assigned to the cards running either the SS7IPGW or IPGWI applications - “Adding an IP Signaling Link” procedure on page 3-82.
- Sockets or associations (with the corresponding ASPs and application servers):
 - “Adding an Application Socket” procedure on page 3-192
 - “Adding an Association” procedure on page 3-332
 - “Adding an Application Server Process” procedure on page 3-383
 - “Adding an Application Server” procedure on page 3-397
- Routing key matching the user part specified in the “Adding an End Node Internal Point Code” procedure and with the DPC of the routing key equal to the true point code of the system (shown in the `rtrv-sid` output) - “Adding an Application Routing Key Containing a Socket” procedure on page 3-228 or “Adding an Application Routing Key Containing an Application Server” procedure on page 3-240.

Adding an End Node Internal Point Code

This procedure is used to assign user parts to an internal point code (IPC), and thereby to an end office node using the `ent-rmt-appl` command. An internal point code is assigned to remote applications. The IPC value is assigned when the first `ent-rmt-appl` command is issued. Subsequent `ent-rmt-appl` commands must have a matching IPC. The IPC value must be in the DPC table. This can be verified with the `rtrv-dstn` command.

The `ent-rmt-appl` command uses these parameters:

- `:ipc/ipca/ipci/ipcn/ipcn24` – The end node's internal point code can be for an ANSI destination (`ipc/ipca`), ITU-I destination (`ipci`), ITU-N destination (`ipcn`), or ITU-N24 (`ipcn24`) destination.
- `:si` – The service indicator value designates which MSU user part is being assigned to a remote application. Valid values range from 3 to 15.
- `:ssn` – The SCCP subsystem number parameter. This parameter is required if the `si=3` parameter is specified and is not valid for any other `si` value. If the `ssne` parameter is also specified, then the `ssn` parameter serves as the starting value of a range. Valid values range from 0 to 255.
- `:ssne` – The SCCP subsystem number range end parameter. The `ssne` value can be specified only if the `si=3` parameter is specified and is not valid for any other `si` value. This parameter serves as an end of a range, and so must be greater than the `ssn` parameter value. Valid values range from 1 to 255.

The specified assignment cannot be an existing assignment, including SSN subsets.

Procedure

1. Display a report listing the remote application assignments using the `rtrv-rmt-appl` command. This is an example of possible output:

```
rlghncxa03w 04-06-28 09:12:36 GMT Rel 31.6.0
IPCA                SI SSN
003-003-003        3 100, 110-119, 200
                   5

IPCI                SI SSN
3-003-3            3 5, 50-100, 250
                   5

IPCN                SI SSN
16380              3 250
                   5

IPCN24             SI SSN
```

2. Display the current destination point codes, using the `rtrv-dstn` command. This is an example of the possible output.

```

rlghncxa03w 04-06-17 16:02:05 GMT Rel 31.6.0
DPCA          CLLI          BEI  ELEI  ALIASI          ALIASN          DOMAIN
030-045-*    rlghncbb010  yes  yes  -----        -----        SS7
111-011-*    rlghncbb000  yes  yes  -----        -----        SS7
240-012-004  rlghncbb001  yes  ---  1-111-1        2500           SS7
240-012-005  rlghncbb002  yes  ---  1-112-2        1357           SS7
240-012-006  rlghncbb003  yes  ---  1-112-3        4257           SS7
240-012-008  -----      yes  ---  1-113-5        6939           SS7
244-020-004  ls06c11i     yes  ---  -----        -----        X25
244-020-005  ls07c11i     yes  ---  -----        -----        X25
244-020-006  ls08c11i     yes  ---  -----        -----        X25
244-020-007  -----      yes  ---  -----        -----        X25
244-020-008  -----      yes  ---  -----        -----        X25
003-003-003  -----      yes  ---  -----        -----        SS7

DPCI          CLLI          BEI  ELEI  ALIASA          ALIASN/N24      DOMAIN
2-131-1      rlghncbb023  no   ---  222-210-000    10789           SS7
2-131-2      -----      no   ---  222-211-001    1138            SS7
2-131-3      -----      no   ---  222-211-002    1298            SS7
3-003-3      -----      no   ---  -----        -----        SS7

DPCN          CLLI          BEI  ELEI  ALIASA          ALIASI          DOMAIN
7701         rlghncbb013  no   ---  222-200-200    2-121-1         SS7
11038        rlghncbb013  no   ---  222-200-201    2-121-2         SS7
16380        -----      no   ---  -----        -----        SS7

DPCN24        CLLI          BEI  ELEI  ALIASA          ALIASI          DOMAIN

DESTINATION ENTRIES ALLOCATED:    2000
  FULL DPC(s):                    17
  NETWORK DPC(s):                  0
  CLUSTER DPC(s):                  2
  TOTAL DPC(s):                    19
  CAPACITY (% FULL):               1%
ALIASES ALLOCATED:                12000
  ALIASES USED:                    18
  CAPACITY (% FULL):               1%
X-LIST ENTRIES ALLOCATED:         500

```

If the IPC being added to the database is not shown in the `rtrv-dstn` output, go to the “Adding a Destination Point Code” procedure in the *Database Administration Manual - SS7* and add the IPC to the DPC table.

3. Add the remote application assignments using the `ent-rmt-appl` command. For this example, enter these commands.

```
ent-rmt-appl:ipc=0-0-1:si=3:ssn=5
ent-rmt-appl:ipc=0-0-1:si=3:ssn=50:ssne=100
ent-rmt-appl:ipc=0-0-1:si=13
```

When each of these commands have successfully completed, the following message should appear.

```
rlghncxa03w 04-06-28 09:12:36 GMT Rel 31.6.0
ENT-RMT-APPL: MASP A - COMPLTD;
```

4. Verify the changes using the `rtrv-rmt-appl` command. This is an example of possible output:

```
rlghncxa03w 04-06-28 09:12:36 GMT Rel 31.6.0
IPCA          SI SSN
000-000-001   3  5, 50-100
              13
003-003-003   3  100, 110-119, 200
              5

IPCI          SI SSN
3-003-3       3  5, 50-100, 250
              5

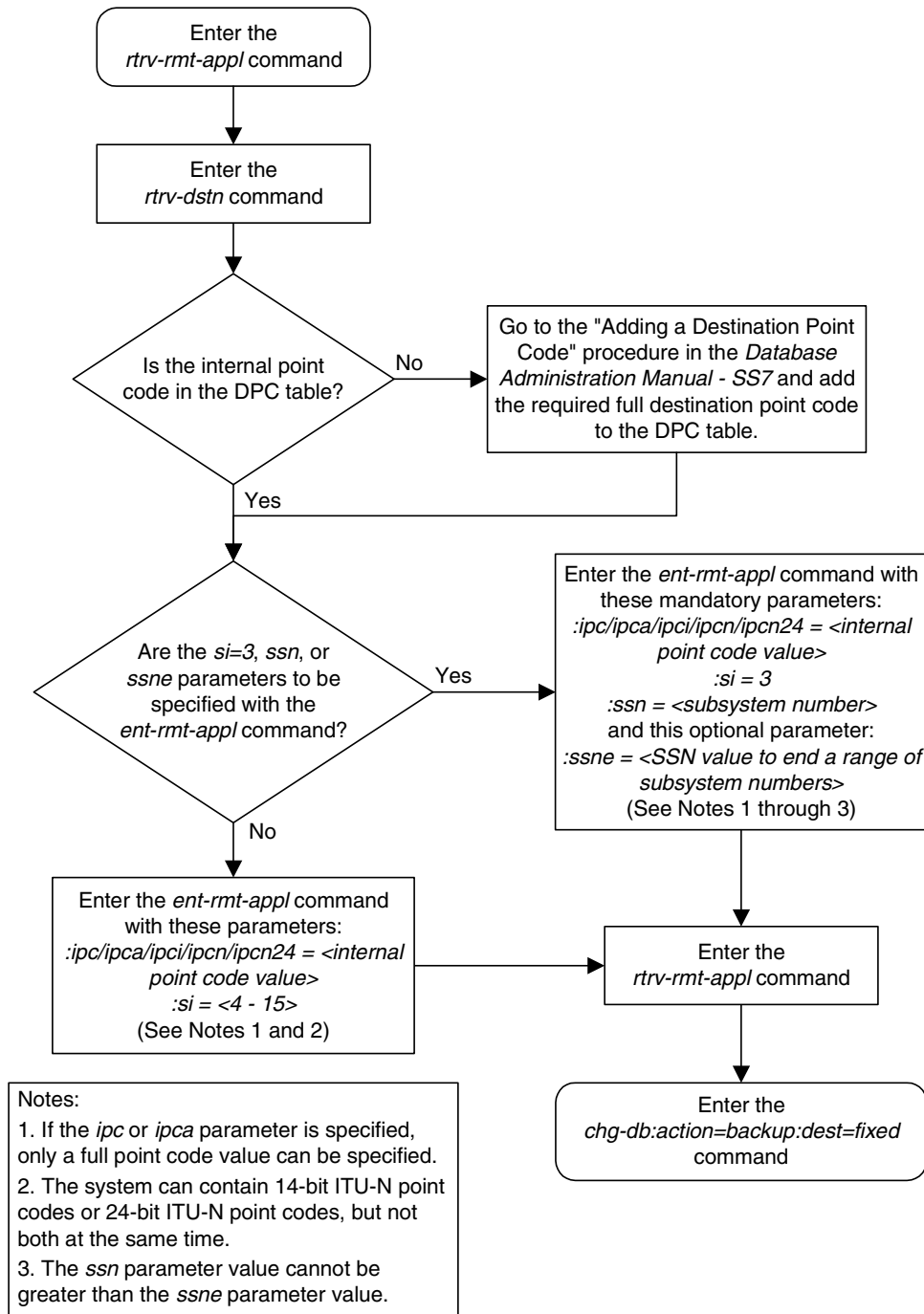
IPCN          SI SSN
16380         3  250
              5

IPC24         SI SSN
```

5. Back up the new changes, using the `chg-db:action=backup:dest=fixed` command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 5-1. Adding an End Node Internal Point Code



Removing an End Node Internal Point Code

The `dlt-rmt-appl` command is used to remove remote application assignments from the database.

The `dlt-rmt-appl` command uses these parameters:

:ipc/ipca/ipci/ipcn/ipcn24 – The end node's internal point code can be for an ANSI destination (**ipc/ipca**), ITU-I destination (**ipci**), ITU-N destination (**ipcn**), or ITU-N24 (**ipcn24**) destination.

:si – The service indicator value designates which MSU user part is being assigned to a remote application. Valid values range from 3 to 15.

:ssn – The SCCP subsystem number parameter. This parameter is required if the **si=3** parameter is specified and is not valid for any other **si** value. If the **ssne** parameter is also specified, then the **ssn** parameter serves as the starting value of a range. Valid values range from 0 to 255.

:ssne – The SCCP subsystem number range end parameter. The **ssne** value can be specified only if the **si=3** parameter is specified and is not valid for any other **si** value. This parameter serves as an end of a range, and so must be greater than the **ssn** parameter value. Valid values range from 1 to 255.

Procedure

1. Display a report listing the remote application assignments using the `rtrv-rmt-appl` command. This is an example of possible output:

```
rlghncxa03w 04-06-28 09:12:36 GMT Rel 31.6.0
IPCA          SI SSN
000-000-001   3  5, 50-100
              13
003-003-003   3  100, 110-119, 200
              5

IPCI          SI SSN
3-003-3       3  5, 50-100, 250
              5

IPCN          SI SSN
16380         3  250
              5

IPCN24        SI SSN
```

2. Delete remote application assignments using the `dlt-rmt-appl` command. For this example, enter these commands.

```
dlt-rmt-appl:ipc=0-0-1:si=3:ssn=5
```

```
dlt-rmt-appl:ipc=0-0-1:si=13
```

When each of these commands have successfully completed, the following message should appear.

```
rlghncxa03w 04-06-28 09:12:36 GMT Rel 31.6.0  
DLT-RMT-APPL: MASP A - COMPLTD;
```

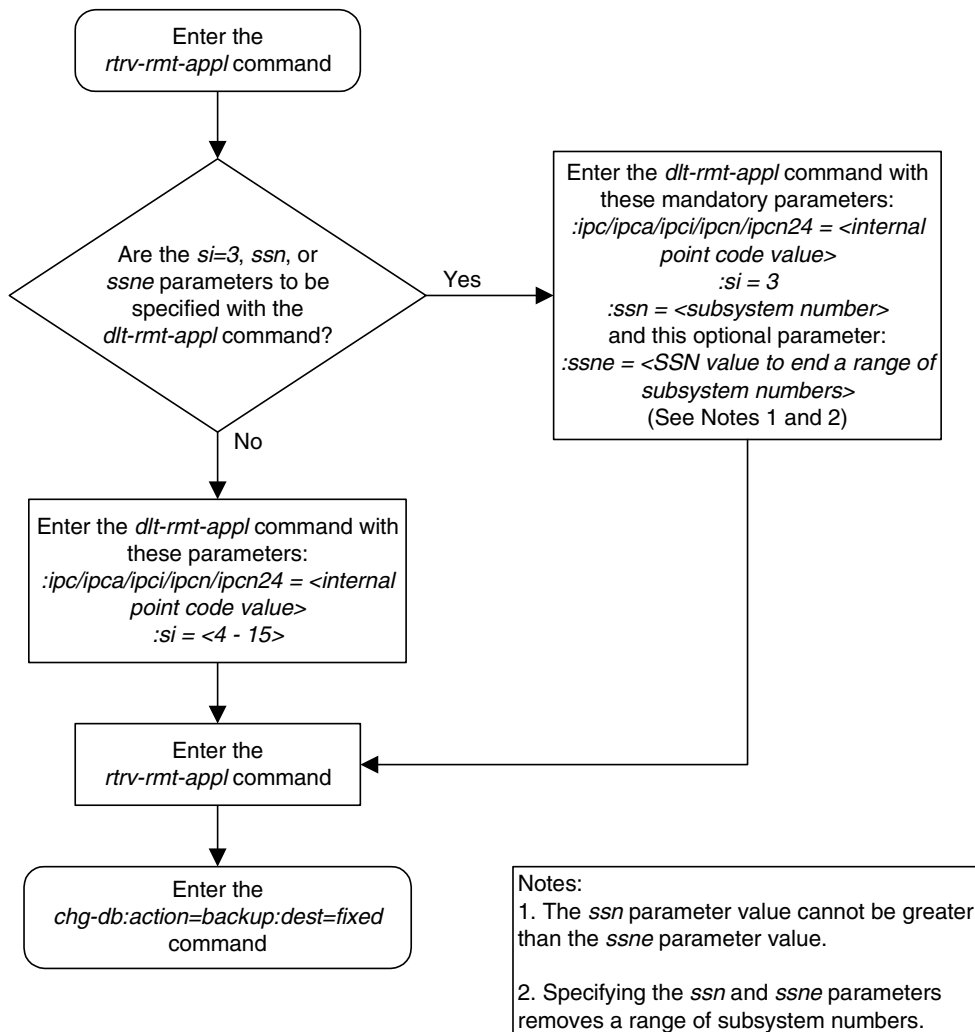
3. Verify the changes using the `rtrv-rmt-appl` command. This is an example of possible output:

```
rlghncxa03w 04-06-28 09:12:36 GMT Rel 31.6.0  
IPCA          SI SSN  
000-000-001   3  50-100  
003-003-003   3  100, 110-119, 200  
              5  
  
IPCI          SI SSN  
3-003-3      3  5, 50-100, 250  
              5  
  
IPCN          SI SSN  
16380        3  250  
              5  
  
IPCN24       SI SSN
```

4. Back up the new changes, using the `chg-db:action=backup:dest=fixed` command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 5-2. Removing an End Node Internal Point Code



6

Activating Controlled Features

Introduction.....	6-2
Enabling Controlled Features	6-2
Enabling a Permanent or Temporary Key.....	6-3
Temporary Feature Keys.....	6-7
Turning On and Off Controlled Features.....	6-10
Turning On an Enabled Controlled Feature	6-10
Turning Off an Enabled Controlled Feature	6-12

Introduction

Controlled features are features that are activated using a feature access key. These features can be either features that can be turned on or off, or features that operate at a particular performance level.

Enabling Controlled Features

The `enable-ctrl-feat` command is used to enable a controlled feature by entering the controlled feature's access key and the controlled feature's part number with these parameters:

- `: fak` – The feature access key generated by Tekelec's feature access key generator, and supplied to you when you purchase or temporarily try a controlled feature. The feature access key contains 13 alphanumeric characters and is not case sensitive.
- `: partnum` – The Tekelec-issued part number associated with the controlled feature. The part number is a 9-digit number, not including dashes; the first three digits must be 893 (that is, 893xxxxxx, where x is a numeric value).

The `enable-ctrl-feat` command requires that the database contain a valid serial number for the system, and that this serial number is locked. This can be verified with the `rtrv-serial-num` command. The system is shipped with a serial number in the database, but the serial number is not locked. The serial number can be changed, if necessary, and locked once the system is on-site, by using the `ent-serial-num` command. The `ent-serial-num` command uses these parameters.

- `: serial` – The serial number assigned to the system. The serial number is not case sensitive.
- `: lock` – Specifies whether or not the serial number is locked. This parameter has only one value, `yes`, which locks the serial number. Once the serial number is locked, it cannot be changed.

NOTE: To enter and lock the system's serial number, the `ent-serial-num` command must be entered twice, once to add the correct serial number to the database with the `serial` parameter, then again with the `serial` and the `lock=yes` parameters to lock the serial number. You should verify that the serial number in the database is correct before locking the serial number. The serial number can be found on a label affixed to the control shelf (shelf 1100).

Features can be enabled by entering a permanent feature access key. Some features can be tried or tested by entering a temporary feature access key. By requiring a feature access key to enable and activate a controlled feature, unauthorized enabling and activation of a controlled feature can be prevented.

Activating Controlled Features

Features enabled with a permanent feature access key remain enabled for as long as the system remains in service. Once features are permanently enabled, they cannot be disabled.

Enabling a Permanent or Temporary Key

This procedure explains how to enable controlled features in the system by entering either a permanent feature access key or a temporary feature access key for the controlled features. This procedure uses the `enable-ctrl-feat`, and `ent-serial-num` commands.

If the temporary key is being enabled, it must not be in the *in-use*, *expired*, or *unavailable* state.

The examples in this procedure are used to enable the controlled features in Table 6-1.

Table 6-1. Sample Controlled Feature Part Numbers

Feature Name	Part Number
ISUP Normalization	893000201
ETSI v3 Normalization	893000601

Procedure

1. Display the serial number in the database with the `rtrv-serial-num` command. This is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
System serial number = nt00001231
```

```
System serial number is not locked.
```

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
Command Completed
```

NOTE: If the serial number is correct and locked, skip steps 2, 3, and 4, and go to step 5. If the serial number is correct but not locked, skip steps 2 and 3, and go to step 4. If the serial number is not correct, but is locked, this feature cannot be enabled and the remainder of this procedure cannot be performed. Contact Tekelec Technical Services to get an incorrect and locked serial number changed. See "Tekelec Technical Services" on page 1-8. The serial number can be found on a label affixed to the control shelf (shelf 1100).

2. Enter the correct serial number into the database using the **ent-serial-num** command with the **serial** parameter.

For this example, enter this command.

```
ent-serial-num:serial=<system's correct serial number>
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 03-02-28 21:15:37 GMT Rel 30.0.0
ENT-SERIAL-NUM:  MASP A - COMPLTD
```

3. Verify that the serial number entered into step 2 was entered correctly using the **rtrv-serial-num** command. This is an example of the possible output.

```
rlghncxa03w 03-02-28 21:15:37 GMT Rel 30.0.0
System serial number = nt00001231

System serial number is not locked.

rlghncxa03w 03-02-28 21:15:37 GMT Rel 30.0.0
Command Completed
```

If the serial number was not entered correctly, repeat steps 3 and 4 and re-enter the correct serial number.

4. Lock the serial number in the database by entering the **ent-serial-num** command with the serial number shown in step 1, if the serial number shown in step 1 is correct, or with the serial number shown in step 3, if the serial number was changed in step 2, and with the **lock=yes** parameter.

For this example, enter this command.

```
ent-serial-num:serial=<system's serial number>:lock=yes
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 03-02-28 21:15:37 GMT Rel 30.0.0
ENT-SERIAL-NUM:  MASP A - COMPLTD
```

5. Display an update of all of the controlled features that have been purchased and all of the temporary keys that have been issued by entering the **rtrv-ctrl-feat** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
The following features have been permanently enabled:

Feature Name          Partnum    Status  Quantity
IPGWx Signaling TPS   893012814  on      20000

The following features have been temporarily enabled:

Feature Name          Partnum    Status  Quantity  Trial Period Left
Zero entries found.

The following features have expired temporary keys:

Feature Name          Partnum
Zero entries found.
```

Activating Controlled Features

6. Enable the purchased permanent key or temporary key for controlled features being enabled by entering the **enable-ctrl-feat** command. For this example, enter this command using the part numbers shown in Table 6-1 on page 6-3.

```
enable-ctrl-feat:partnum=893000201:fak=<feature access key>
```

```
enable-ctrl-feat:partnum=893000601:fak=<feature access key>
```

NOTE: The values for the feature access key (the **fak** parameter) are provided by Tekelec. If you do not have the controlled feature part number or the feature access key for the feature you wish to enable, contact your Tekelec Sales Representative or Account Representative.

When the **enable-ctrl-feat** command has successfully completed, this message should appear.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
ENABLE-CTRL-FEAT: MASP B - COMPLTD
```

7. Verify the changes by entering the **rtrv-ctrl-feat** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
The following features have been permanently enabled:
```

Feature Name	Partnum	Status	Quantity
IPGWx Signaling TPS	893012814	on	20000
ISUP Normalization	893000201	off	----
ETSI v3 Normalization	893000601	off	----

The following features have been temporarily enabled:

Feature Name	Partnum	Status	Quantity	Trial Period Left
Zero entries found.				

The following features have expired temporary keys:

Feature Name	Partnum
Zero entries found.	

8. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

9. If the controlled features enabled in step 4 are On/Off features, the features must be turned on using the **chg-ctrl-feat** command. Specify the controlled feature part number used in step 4 and the **status=on** parameter. For this example, enter these commands. Go to the procedure in "Turning On and Off Controlled Features" on page 6-10 to turn each feature on.
-

Activating Controlled Features

Temporary Feature Keys

Features enabled with a temporary feature access key are enabled for only 30 days. On the twenty-third day, seven days before the temporary key expires, a major alarm (UAM 0367) is generated to inform the user that the one or more temporary feature access keys will expire soon.

```
0367.0181 ** SYSTEM      Temp Key(s) expiring soon.
```

If a temporary feature access key expires, the controlled feature is disabled and a critical alarm (UAM 0368) is generated.

```
0368.0181 *C SYSTEM      Temp Key(s) have expired.
```

Any attempts to enable the controlled feature with the temporary feature access key are rejected. The controlled feature can be enabled only by entering the permanent feature access key for the controlled feature.

To clear the critical alarm (UAM 0368), the user can either enter the **chg-ctrl-feat** command with the **alarm=clear** parameter, or permanently enable the controlled feature by entering the permanent feature access key for the controlled feature.

If the critical alarm is cleared with the **chg-ctrl-feat** command, the controlled feature is disabled and cannot be enabled with the temporary feature access key. The feature can be enabled only by entering the permanent feature access key for the controlled feature.

Clearing a Temporary Feature Access Key Alarm

This procedure is used to clear the system alarms using the **chg-ctrl-feat** command after a temporary feature access key has expired.

NOTE: The alarm is cleared when no temporary feature access keys are in danger of expiration or in an *expired* state.

The **chg-ctrl-feat** command uses the following parameters:

:partnum - The part number of the controlled feature that was temporarily enabled and is causing the alarm.

:alarm - Clear. Specifying **clear** for this parameter clears the alarm.

The following dependencies apply to this procedure:

The controlled feature part number must be valid. It must match the part number of the temporary controlled feature that is causing the alarm.

The controlled feature must have been temporarily enabled and is now in danger of expiration or in an *expired* state.

Procedure

1. Display enabled controlled feature information that is causing the system alarm in the database by entering the **rtrv-ctrl-feat:expired=yes** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:17:37 GMT EAGLE5 31.10.0
The following features have expired temporary keys:
Feature Name          Partnum
ISUP Normalization   893000201
```

2. Clear the system alarm in the database by entering the **chg-ctrl-feat** command. For example, enter this command.

```
chg-ctrl-feat:partnum=893000201:alarm=clear
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-30 21:16:37 GMT EAGLE5 31.10.0
CHG-CTRL-FEAT: MASP A - COMPLTD
```

3. Verify that the alarm has cleared in the database by using the **rtrv-ctrl-feat:expired=yes** command. The following is an example of the possible output.

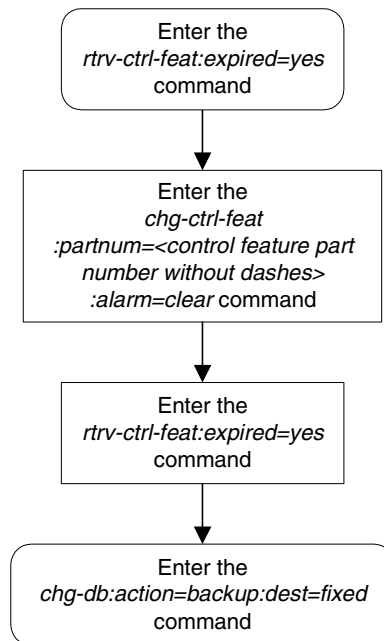
```
rlghncxa03w 04-12-28 21:16:37 GMT EAGLE5 31.10.0
0367.0181 * SYSTEM      Temp Key(s) expiration alarm cleared.
```

4. Back up the changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Activating Controlled Features

Flowchart 6-2. Clearing a Temporary Feature Access Key Alarm



Turning On and Off Controlled Features

Some controlled features must be turned on after they are enabled, and can be turned off without disabling them in the system. The **chg-ctrl-feat** command is used to turn the features on and off, and to clear the critical alarm that occurs when a temporary feature key expires (see “Temporary Feature Keys” on page 6-7).

The **chg-ctrl-feat** command uses the following parameters:

- :partnum** – The Tekelec-issued part number associated with the controlled feature. The part number is a 9-digit number, not including dashes; the first three digits must be 893 (that is, 893xxxxxx, where x is a numeric value).
- :status** – Changes the activation status of the feature (On or Off).
- :alarm=clear** – Use only to clear the critical alarm that is generated when a temporary feature key expires.

The part number that you enter must be for an On/Off feature that has already been enabled with the **enable-ctrl-feat** command (see “Enabling Controlled Features” on page 6-2).

Turning On an Enabled Controlled Feature

This procedure allows the user to turn on enabled controlled features in the system, by using the **chg-ctrl-feat** command.

The **chg-ctrl-feat** command uses these parameters:

- :partnum** – The Tekelec-issued part number associated with the controlled feature. The part number is a 9-digit number, not including dashes. The first three digits must be 893 (that is, 893xxxxxx, where x is a numeric value).
- :status** – used to activate the controlled features that customer has purchased and enabled.

The examples in this procedure are used to enable and activate the controlled features in Table 6-2.

Table 6-2. Sample Controlled Feature Part Numbers

Feature Name	Part Number
ISUP Normalization	893000201
ETSI v3 Normalization	893000601

Procedure

1. Enter the **rtrv-ctrl-feat** command to display the status of the controlled features in the system. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
The following features have been permanently enabled:
```

Feature Name	Partnum	Status	Quantity
IPGWx Signaling TPS	893012814	on	20000
ISUP Normalization	893000201	off	----
ETSI v3 Normalization	893000601	off	----

The following features have been temporarily enabled:

Feature Name	Partnum	Status	Quantity	Trial Period Left
Zero entries found.				

The following features have expired temporary keys:

Feature Name	Partnum
Zero entries found.	

2. The controlled features listed in Table 6-2 on page 6-10 must be turned on using the **chg-ctrl-feat** command, specifying the controlled feature part number used to enable the feature and the **status=on** parameter. For this example, enter these commands.

```
chg-ctrl-feat:partnum=893000201:status=on
```

```
chg-ctrl-feat:partnum=893000601:status=on
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
CHG-CTRL-FEAT: MASP B - COMPLTD
```

3. Verify the changes by entering the **rtrv-ctrl-feat** command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
The following features have been permanently enabled:
```

Feature Name	Partnum	Status	Quantity
IPGWx Signaling TPS	893012814	on	20000
ISUP Normalization	893000201	on	----
ETSI v3 Normalization	893000601	on	----

The following features have been temporarily enabled:

Feature Name	Partnum	Status	Quantity	Trial Period Left
Zero entries found.				

The following features have expired temporary keys:

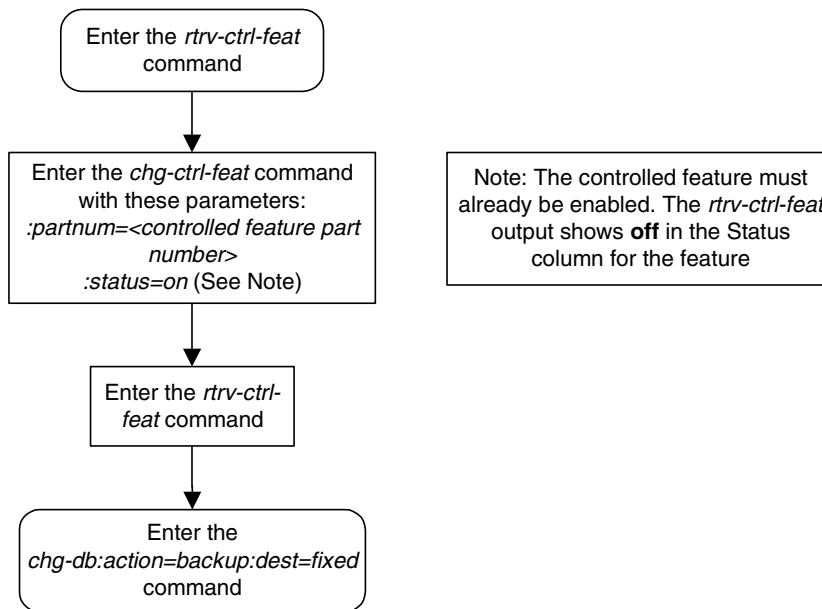
Feature Name	Partnum
Zero entries found.	

- Back up the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```

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

Flowchart 6-3. Turning On an Enabled Controlled Feature



Turning Off an Enabled Controlled Feature

Some controlled features that have been enabled and turned on can be turned off without disabling them in the system. This procedure allows the user to turn off enabled controlled features in the system, by using the `chg-ctrl-feat` command.



CAUTION: Refer to the Feature Notice or the appropriate feature manual to determine the results of turning a feature off. For example, you might use a feature to add entries to a database table. When the feature is turned off after entries have been added to the table, the commands to delete and retrieve the entries might still function, but the commands to enter or change entries no longer function.

Activating Controlled Features

The **chg-ctrl-feat** command uses these parameters:

:partnum – The Tekelec-issued part number associated with the controlled feature. The part number is a 9-digit number, not including dashes. The first three digits must be 893 (that is, 893xxxxxx, where x is a numeric value).

:status – used to activate the controlled features that customer has purchased and enabled.

The examples in this procedure are used to enable and activate the controlled features in Table 6-3.

Table 6-3. Sample Controlled Feature Part Numbers

Feature Name	Part Number
ISUP Normalization	893000201
ETSI v3 Normalization	893000601

Procedure

1. Enter the **rtrv-ctrl-feat** command to display the status of the controlled features in the system. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
The following features have been permanently enabled:
```

```
Feature Name          Partnum    Status    Quantity
IPGWx Signaling TPS   893012814 on        20000
ISUP Normalization    893000201 on        ----
ETSI v3 Normalization 893000601 on        ----
```

```
The following features have been temporarily enabled:
```

```
Feature Name          Partnum    Status    Quantity    Trial Period Left
Zero entries found.
```

```
The following features have expired temporary keys:
```

```
Feature Name          Partnum
Zero entries found.
```

2. The controlled features listed in Table 6-2 on page 6-10 are turned on using the **chg-ctrl-feat** command, specifying the controlled feature part number used to enable the feature and the **status=off** parameter. For this example, enter these commands.

```
chg-ctrl-feat:partnum=893000201:status=off
```

```
chg-ctrl-feat:partnum=893000601:status=off
```

When this command has successfully completed, the following message should appear.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
CHG-CTRL-FEAT: MASP B - COMPLTD
```

- Verify the changes by entering the `rtrv-ctrl-feat` command. The following is an example of the possible output.

```
rlghncxa03w 04-12-28 21:15:37 GMT EAGLE5 31.10.0
The following features have been permanently enabled:
```

Feature Name	Partnum	Status	Quantity
IPGWx Signaling TPS	893012814	on	20000
ISUP Normalization	893000201	off	----
ETSI v3 Normalization	893000601	off	----

The following features have been temporarily enabled:

Feature Name	Partnum	Status	Quantity	Trial Period Left
Zero entries found.				

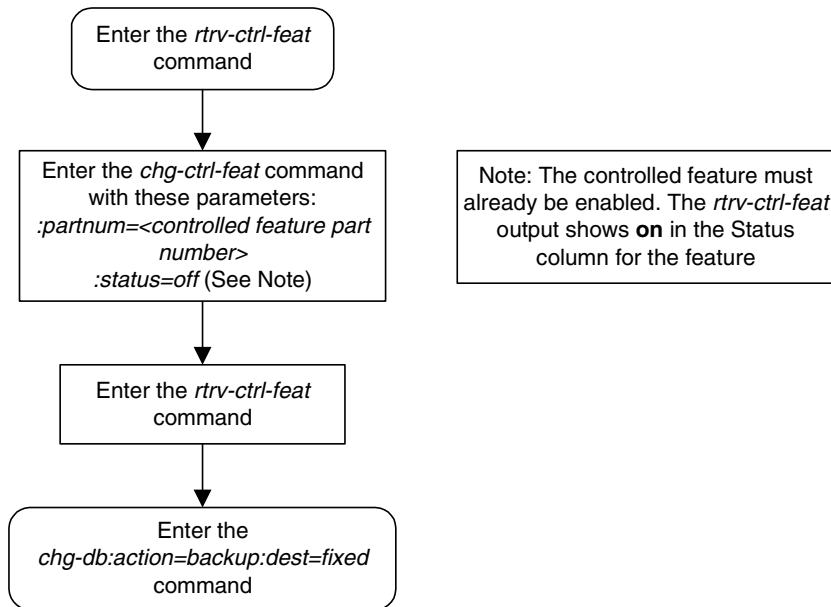
The following features have expired temporary keys:

Feature Name	Partnum
Zero entries found.	

- Back up the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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

Flowchart 6-4. Turning Off an Enabled Controlled Feature



Index

Numerics

1500 Signaling Links, 3-108

A

acronyms, 1-14

activate signaling link, act-slk

IPGWI, 3-73, 3-131, 3-145, 3-167, 3-179,
3-196, 3-197, 3-210, 3-211, 3-337,
3-339, 3-358, 3-360

IPLIM, 3-73, 3-131, 3-145, 3-167

SS7IPGW, 3-73, 3-131, 3-145, 3-167,
3-179, 3-196, 3-197, 3-210, 3-211,
3-337, 3-339, 3-358, 3-360

Adding an Application Socket, 3-192

Adding an IP Host, 3-153

alw, 3-205

appl, 3-4

Applications, 2-3, 2-4

C

calculate number of high-speed signaling
links in system, 3-86

calculate number of low-speed signaling
links in system, 3-86

cancel

rtrv-dstn, 3-44

rtrv-ls, 3-44

Changing a DCM Parameter Set, 3-223

Changing an Application Socket, 3-205

Changing an IP Card, 3-40, 3-173

Changing an IP Link, 3-158

Changing an IP7 Secure Gateway
Option, 3-40

cice, 3-229, 3-241, 3-259, 3-268, 3-275, 3-276,
3-283, 3-294, 3-308

cics, 3-229, 3-241, 3-258, 3-268, 3-275, 3-283,
3-294, 3-308

Clearing a Temporary FAK alarm, 6-7

C-link linkset, 3-7

Configuring a Mate IPGWx Linkset, 3-60

Configuring an IPGWx Linkset, 3-40

Configuring IP Retransmission
Parameters, 3-217

Connectivity, 2-20, 2-21

Controlled Feature

Large System # Links - Enabling, 3-108
customer support, 1-8

Tekelec Technical Services, 1-9

D

database partitions

overview, 1-11

dcm, 3-4

DCM parameter set, 3-3

dcmps, 3-205

Default Routing Keys, 2-25

Display, 3-177

display card status, rept-stat-card

IPGWI, 3-143, 3-163, 3-177

IPLIM, 3-163, 3-177

SS7IPGW, 3-143, 3-163, 3-177

display signaling link status, rept-stat-slk

IPGWI, 3-142, 3-145, 3-162, 3-167, 3-175,
3-179, 3-196, 3-210, 3-337, 3-358,
3-427, 3-437

IPLIM, 3-145, 3-162, 3-167, 3-175, 3-427,
3-437

SS7IPGW, 3-142, 3-145, 3-162, 3-167,
3-175, 3-179, 3-197, 3-198, 3-210,
3-211, 3-337, 3-339, 3-358, 3-360,
3-427, 3-437

documentation set, 1-3, 1-7

dpc, 3-258

drkq, 3-148

E

Eagle

documentation set, 1-3

emergency response (Tekelec Technical
Services), 1-9

Enabling a Permanent or Temporary
Key, 6-3

Enabling the Large System # Links
Controlled Feature, 3-108

End node internal point codes, 3-4

Errors

- contacting Tekelec Technical Services, 1-9

F

- fixed disk drive

- overview, 1-12

- Full Routing Keys, 2-24

G

- getcomm, 3-148

I

- in, 3-145, 3-179, 3-427, 3-437

- inhfepalm, 3-148

- internal point codes, 3-4

- IP application routing key, 3-3

- IP application server processes, 3-4

- IP application servers, 3-3

- IP application socket, 3-3

- IP associations, 3-3

- IP card, 3-3

- IP host, 3-3

- IP link, 3-3

- IP options

- drkq, 3-148

- getcomm, 3-148

- inhfepalm, 3-148

- ipgwabate, 3-148

- iplimabate, 3-148

- sctpcsum, 3-148, 3-422, 3-451

- setcomm, 3-148

- snmpcont, 3-148

- srkq, 3-148

- sync, 3-141, 3-148

- trapcomm, 3-148

- IP protocol option, 3-141

- IP routes, 3-3

- IP7 Secure Gateway Options, 3-3

- ipgwabate, 3-148

- IPGWI

- activate signaling link, act-slk, 3-73,

- 3-131, 3-145, 3-167, 3-179, 3-196,

- 3-197, 3-210, 3-211, 3-337, 3-339,

- 3-358, 3-360

- display card status,

- rept-stat-card, 3-143, 3-163, 3-177

- display signaling link status,

- rept-stat-slk, 3-142, 3-145, 3-162,

- 3-167, 3-175, 3-179, 3-196, 3-210,

- 3-337, 3-358, 3-427, 3-437

- ipgwi, 2-4, 2-21

- IPGWx Linkset

- Configuring, 3-40

- Mate - Configuring, 3-60

- IPGWx M3UA connections - migrating

- IPLIMx M3UA links to, 3-125, 3-135,

- 3-136, 3-137, 3-138, 3-139, 3-140

- IPLIM

- activate signaling link, act-slk, 3-73,

- 3-131, 3-145, 3-167

- display card status,

- rept-stat-card, 3-163, 3-177

- display signaling link status,

- rept-stat-slk, 3-145, 3-162, 3-167,

- 3-175, 3-427, 3-437

- iplim, 2-3

- iplimabate, 3-148

- iplimi, 2-3

- IPLIMx M3UA Signaling Links - Migrating

- to IPGWx M3UA connections, 3-125,

- 3-135, 3-136, 3-137, 3-138, 3-139, 3-140

- ISUP Normalization, 2-38

- ISUP variant provisioning, 3-4

L

- Large System # Links Controlled Feature

- Enabling, 3-108

- Linkset

- IPGWx

- Configuring, 3-40

- Mate IPGWx - Configuring, 3-60

M

- M3UA signaling links - migrating IPLIMx to

- IPGWx, 3-125, 3-135, 3-136, 3-137,

- 3-138, 3-139, 3-140

- maintenance and administration subsystem

- overview, 1-10

Index

manual

- admonishments, 1-8
- organization, 1-2
- related publications, 1-3

Mate IPGWx Linkset - Configuring, 3-60

mated gateways, 3-7

Migrating IPLIMx M3UA signaling links to
IPGWx M3UA connections, 3-125,
3-135, 3-136, 3-137, 3-138, 3-139, 3-140

N

Nagle's Algorithm, 2-37

ncice, 3-268, 3-275, 3-284, 3-294, 3-309

ncics, 3-268, 3-275, 3-284, 3-294, 3-309

Network appearances, 3-4

O

opc/opca, 3-228, 3-240, 3-258, 3-267, 3-275,
3-283, 3-293, 3-308

open, 3-205

overview

- database partitions, 1-11
- fixed disk drive, 1-12
- maintenance and administration
subsystem, 1-10
- removable cartridge, 1-13

P

Partial Routing Keys, 2-25

Point-to-Multipoint, 2-21

Point-to-Point, 2-20

PSTN presentation data, 3-4

R

removable cartridge

- overview, 1-13

removing

- signaling link, 3-115

Removing an Application Socket, 3-202

Removing an DCM, 3-31, 3-188

Removing an IP Card, 3-31, 3-188

Routing Key Lookup Hierarchy, 2-27

Routing Key Tables, 2-25

S

SCTP checksum algorithm option, 3-422,
3-451

sctpcsum, 3-148, 3-422, 3-451

server, 3-205

setcomm, 3-148

signaling link

- removing, 3-115

signaling links, 1500, 3-108

sname, 3-258

snmpcont, 3-148

split, 3-268, 3-275, 3-284, 3-294, 3-309

srkq, 3-148

SS7IPGW

- activate signaling link, act-slk, 3-73,
3-131, 3-145, 3-167, 3-179, 3-196,
3-197, 3-210, 3-211, 3-337, 3-339,
3-358, 3-360

display card status,

- rept-stat-card, 3-143, 3-163, 3-177

display signaling link status,

- rept-stat-slk, 3-142, 3-145, 3-162,
3-167, 3-175, 3-179, 3-197, 3-198,
3-210, 3-211, 3-337, 3-339, 3-358,
3-360, 3-427, 3-437

ss7ipgw, 2-4, 2-21

ssn, 3-258

sync, 3-141, 3-148

T

technical services, 1-8

Tekelec Technical Services, 1-8

- emergency response, 1-9

trapcomm, 3-148

turning On and Off Controlled

- Features, 6-10

Type of Service, 2-37

