

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 C
October 2003**



TEKELEC

© 2003 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.

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	1-7
Tekelec Technical Services	1-8
Emergency Response	1-8
Maintenance and Administration Subsystem	1-9
Database Partitions	1-10
Fixed Disk Drive	1-11
Removable Cartridge	1-12
List of Acronyms and Abbreviations	1-13

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	3-15
Card Slot Selection	3-16
Using the FORCE Parameter	3-17
Removing an IP Card	3-31
Changing an IP Card	3-40
Changing the IP Protocol Option	3-49
Changing IP Options other than SYNC and SCTPCSUM	3-56
Adding an IP Host	3-61
Removing an IP Host	3-63
Changing an IP Link	3-66
Adding an IP Route	3-81
Removing an IP Route	3-85
Adding an Application Socket	3-89
Removing an Application Socket	3-99
Changing an Application Socket	3-102
Configuring IP Socket Retransmission Parameters	3-114
Changing a DCM Parameter Set	3-120
Adding a Static Application Routing Key	3-124
Removing an Application Routing Key	3-133
Changing a Static Application Routing Key	3-139
Changing the PSTN Presentation and Normalization	
Attributes in an Application Routing Key	3-151
Increasing the TPS on the IP Card	3-165
IETF Adapter Layer Configuration	3-171
Adding an Association	3-172
Removing an Association	3-185
Changing an Association	3-190
Configuring SCTP Retransmission Control	
for an Association	3-211
Changing an M2PA Timer Set	3-220
Adding an Application Server Process	3-224
Removing an Application Server Process	3-228
Changing an Application Server Process	3-231
Adding an Application Server	3-238
Removing an Application Server	3-247

Table of Contents

Changing an Application Server	3-251
Adding a Network Appearance	3-256
Removing a Network Appearance	3-260
Changing the SCTP Checksum Algorithm Option	3-262
Changing a UA Parameter Set	3-293
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 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
Index	

List of Figures

Figure 1-1. Database Partitions	1-10
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

List of Figures

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	3-5
Figure 3-2. IP7 Secure Gateway Database Relationships	3-11
Figure 3-3. Typical System Configuration	3-12
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	3-13
Table 3-2. Typical IP Sockets	3-13
Table 3-3. Typical IP Routing Keys (SS7IPGW and IPGWI Applications)	3-14
Table 3-4. Card Type and Card Applications	3-15
Table 3-5. Example Card Configuration	3-16
Table 3-6. Number of Transactions per Second for each SCCP Card	3-17
Table 3-7. SS7 Card Applications and Signaling Link Types	3-18
Table 3-8. Valid Subnet Mask Parameter Values	3-67
Table 3-9. Valid Subnet Mask Parameter Values	3-82
Table 3-10. DCMPS Values	3-120
Table 3-11. Service Indicator Text String Values	3-124
Table 3-12. Routing Key Parameter Combinations for Adding Routing Keys	3-126
Table 3-13. Routing Key Parameter Combinations for Removing Routing Keys	3-134
Table 3-14. Service Indicator Text String Values	3-139

List of Tables

Table 3-15. Routing Key Parameter Combinations for Changing Socket Name Associations	3-144
Table 3-16. Service Indicator Text String Values	3-152
Table 3-17. Valid PVALUE Parameter Values if PARM=1	3-294
Table 3-18. Valid PVALUE Parameter Values if PARM=2	3-295
Table 3-19. Valid PVALUE Parameter Values if PARM=3	3-296
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. Changing an IP Card	3-46
Flowchart 3-4. Changing the IP Protocol Option	3-54
Flowchart 3-5. Changing an IP Option That Does Not Require Inhibiting the IP Card	3-60
Flowchart 3-6. Adding an IP Host	3-62
Flowchart 3-7. Removing an IP Host	3-65
Flowchart 3-8. Changing an IP Link	3-76
Flowchart 3-9. Adding an IP Route	3-84
Flowchart 3-10. Removing an IP Route	3-88
Flowchart 3-11. Adding an Application Socket	3-96
Flowchart 3-12. Removing an Application Socket	3-101
Flowchart 3-13. Changing an Application Socket	3-109
Flowchart 3-14. Configuring IP Retransmission Parameters	3-119
Flowchart 3-15. Changing an DCM Parameter Set	3-123
Flowchart 3-16. Adding an Application Routing Key	3-131
Flowchart 3-17. Removing an Application Routing Key	3-138
Flowchart 3-18. Changing a Static Application Routing Key	3-149
Flowchart 3-19. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key	3-159
Flowchart 3-20. Increasing the TPS on the IP Card	3-169
Flowchart 3-21. Adding an Association	3-180
Flowchart 3-22. Removing an Association	3-189
Flowchart 3-23. Changing an Association	3-202
Flowchart 3-24. Configuring an Association for SCTP Retransmission Control	3-218
Flowchart 3-25. Changing an M2PA Timer Set	3-223
Flowchart 3-26. Adding an Application Server Process	3-227
Flowchart 3-27. Removing an Application Server Process	3-230
Flowchart 3-28. Changing an Application Server Process	3-235

List of Flowcharts

Flowchart 3-29. Adding an Application Server	3-244
Flowchart 3-30. Removing an Application Server	3-250
Flowchart 3-31. Changing an Application Server	3-254
Flowchart 3-32. Adding a Network Appearance	3-259
Flowchart 3-33. Removing a Network Appearance	3-261
Flowchart 3-34. Changing the SCTP Checksum Option	3-286
Flowchart 3-35. Changing a UA Parameter Set	3-301
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.....	1-7
Tekelec Technical Services	1-8
Emergency Response	1-8
Maintenance and Administration Subsystem	1-9
Database Partitions.....	1-10
Fixed Disk Drive.....	1-11
Removable Cartridge.....	1-12
List of Acronyms and Abbreviations.....	1-13

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 *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.
- 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.

- *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.

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

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.

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

Introduction

- 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.

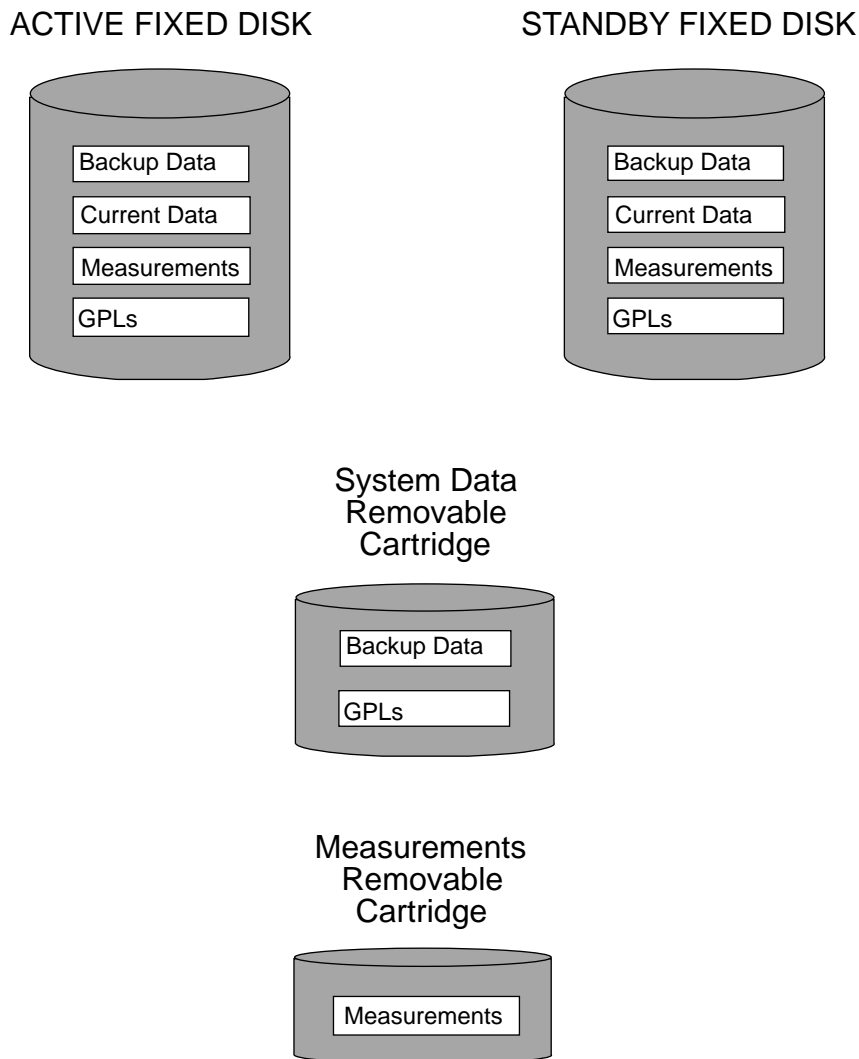
The procedures in the *Database Administration Manual – IP⁷ Secure Gateway* refer to the terms MASP and MDAL. The database commands, such as **rept-stat-db**, refer to the MASP because the MASP controls the input to the TDM and MDAL, and output from the TDM and MDAL. The MDAL is only referred to when 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 1-11 and the Removable Cartridge section on page 1-12 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.

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
ASM.....	Application Services Module
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
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

Introduction

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
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

Introduction

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
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

Introduction

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 Capability	2-56
Enhanced Security	2-56
SCTP Connectivity Concepts	2-56

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 41 cards (100 cards for a system containing more than 700 links) 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. For these applications, two IP cards, configured similarly, are required for hardware redundancy.

The system can support a maximum of two 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.

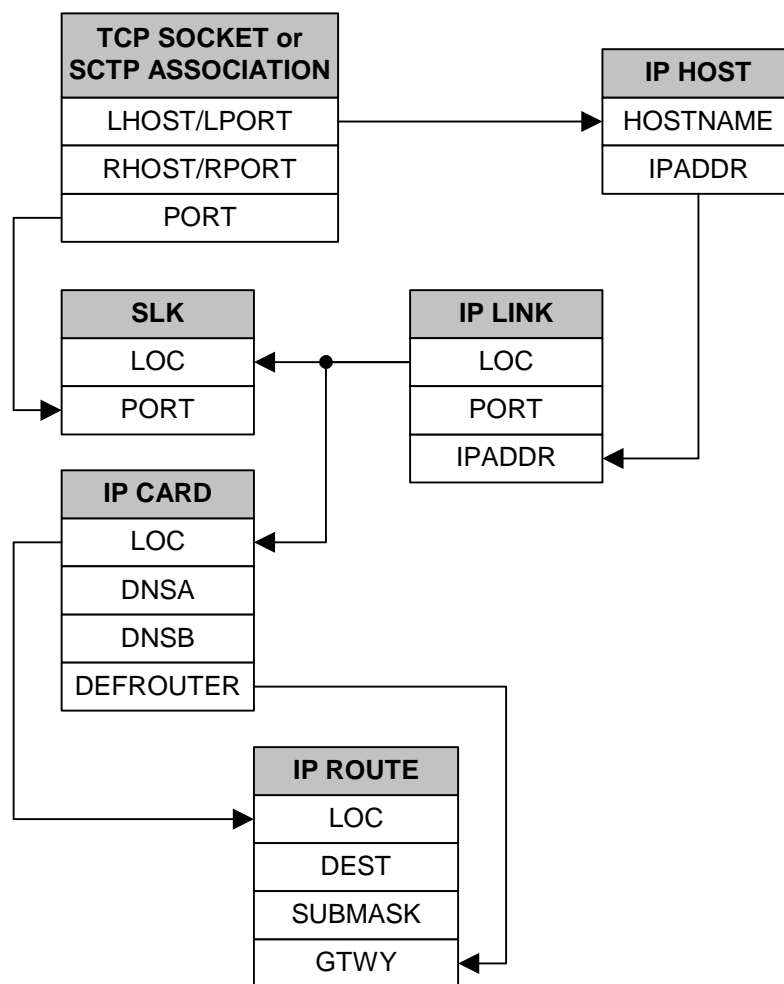
A TCP socket can establish a connection between one local host and one remote host. An SCTP association can establish a connection between one local host and one remote host (a uni-homed association) or between multiple local hosts and a remote host (a multi-homed association). It is possible that the 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.

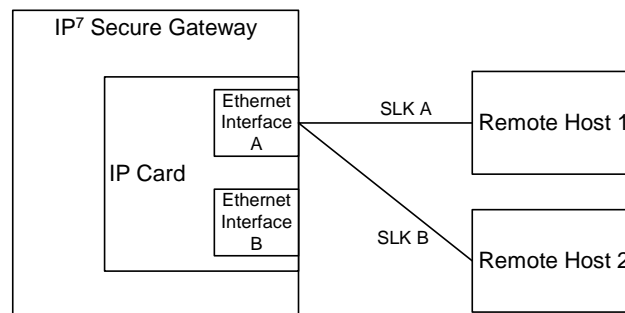
Table 2-1. Ethernet Interface and Signaling Link Port Combinations

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.

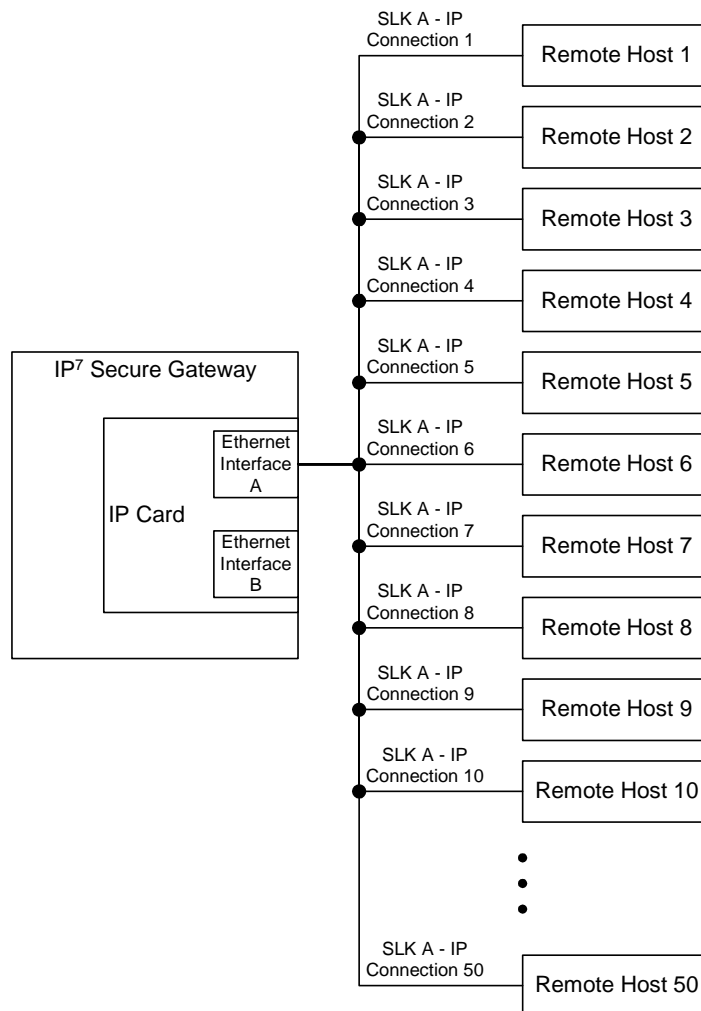
Figure 2-2. IP Connections using a Dual-Slot DCM running the IPLIMx Applications



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.

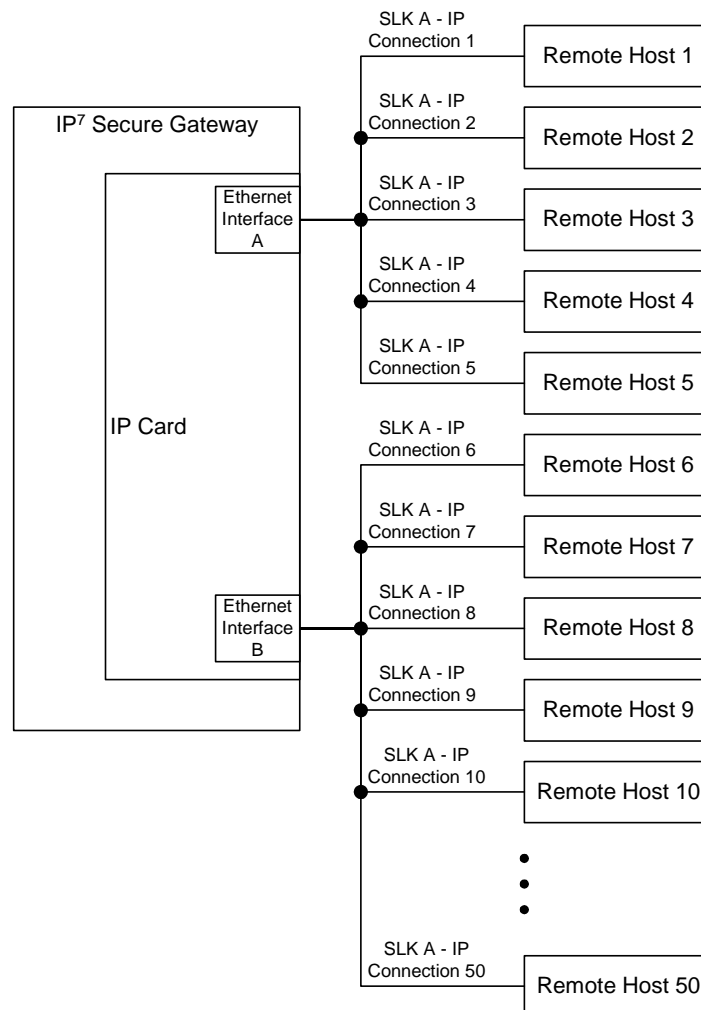
Figure 2-3. IP Connections using a Dual-Slot DCM running the IPGWx Applications



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.

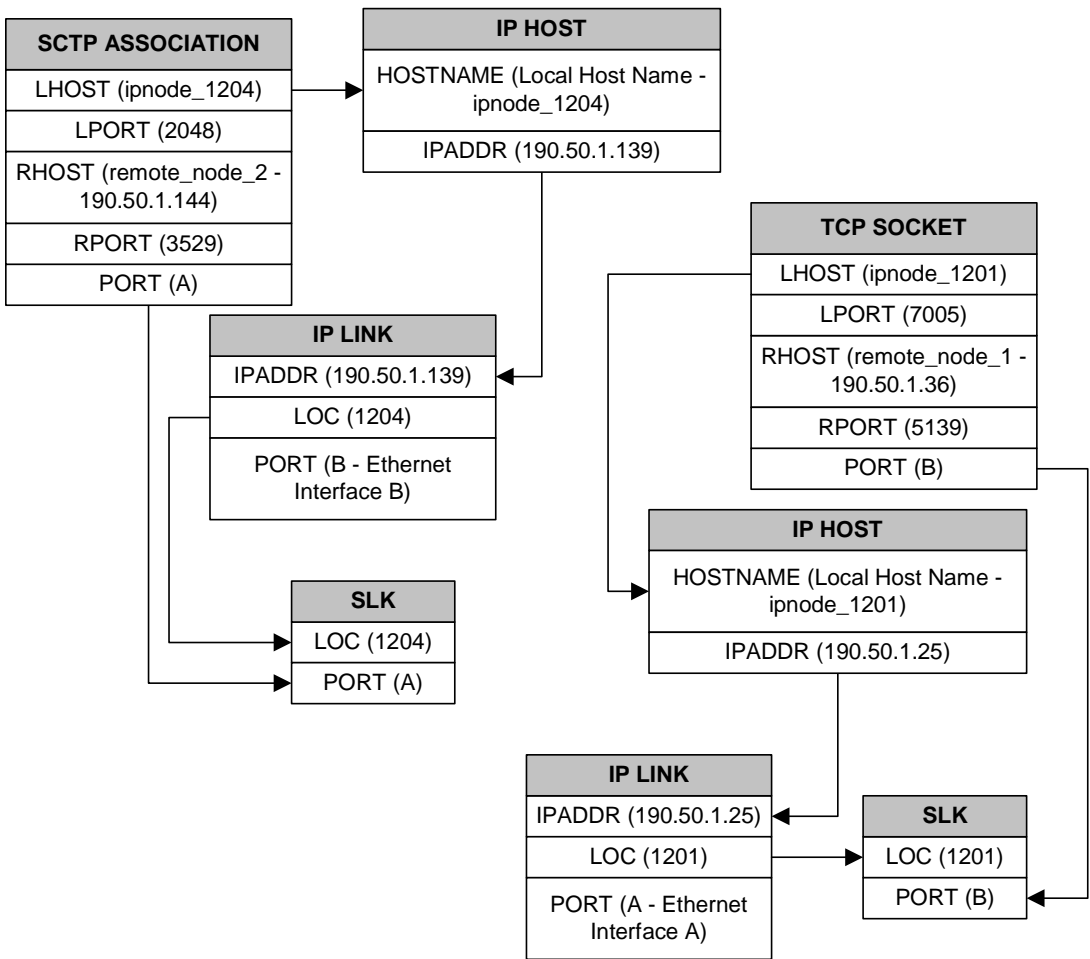
Figure 2-4. IP Connections using an EDCM running the IPGWx Applications



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

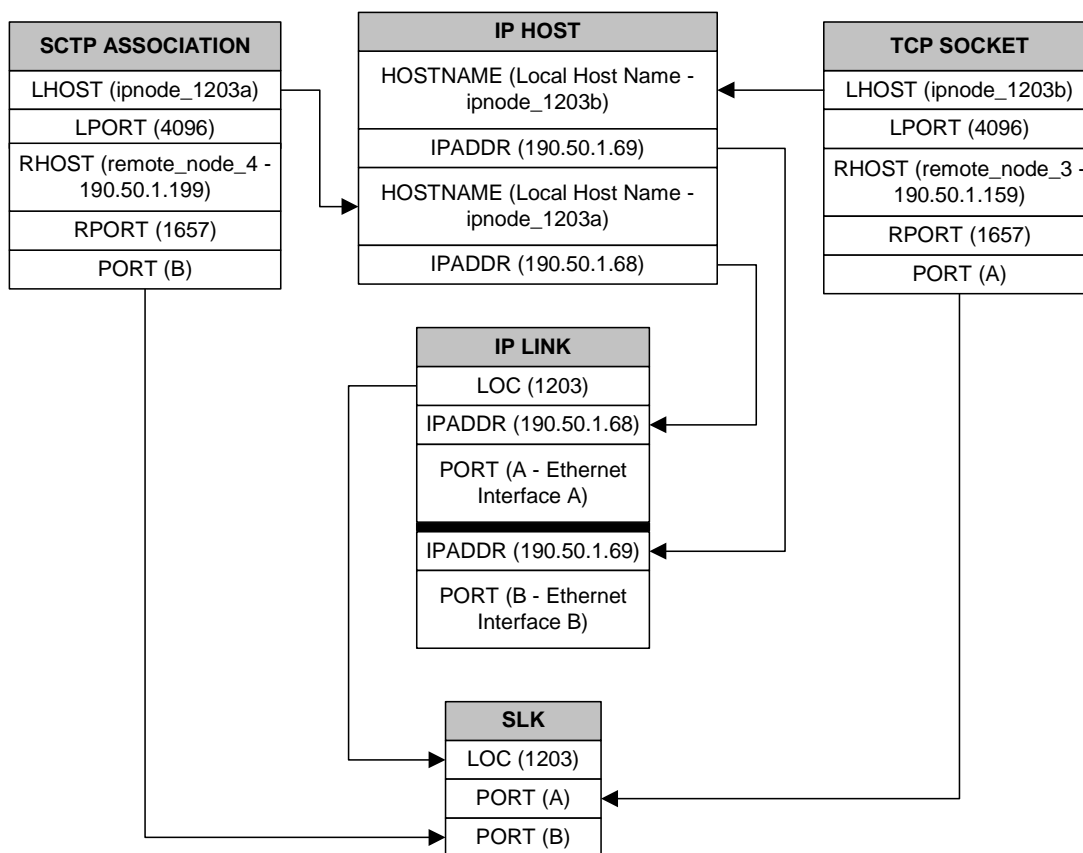


Using the data in Figure 2-5, the IP connection defined by the TCP socket is from local host ipnode-1201 (190.50.1.25), TCP port 7005, to remote host remote-node-1 (190.50.1.36), TCP port 5139, using Ethernet interface A on IP card 1201, and signaling link port B on IP card 1201.

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.

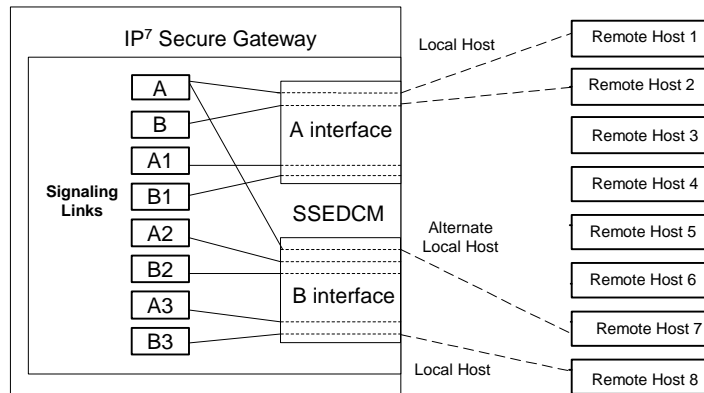
Figure 2-6. SCTP Association and TCP Socket on the Same IP Card



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

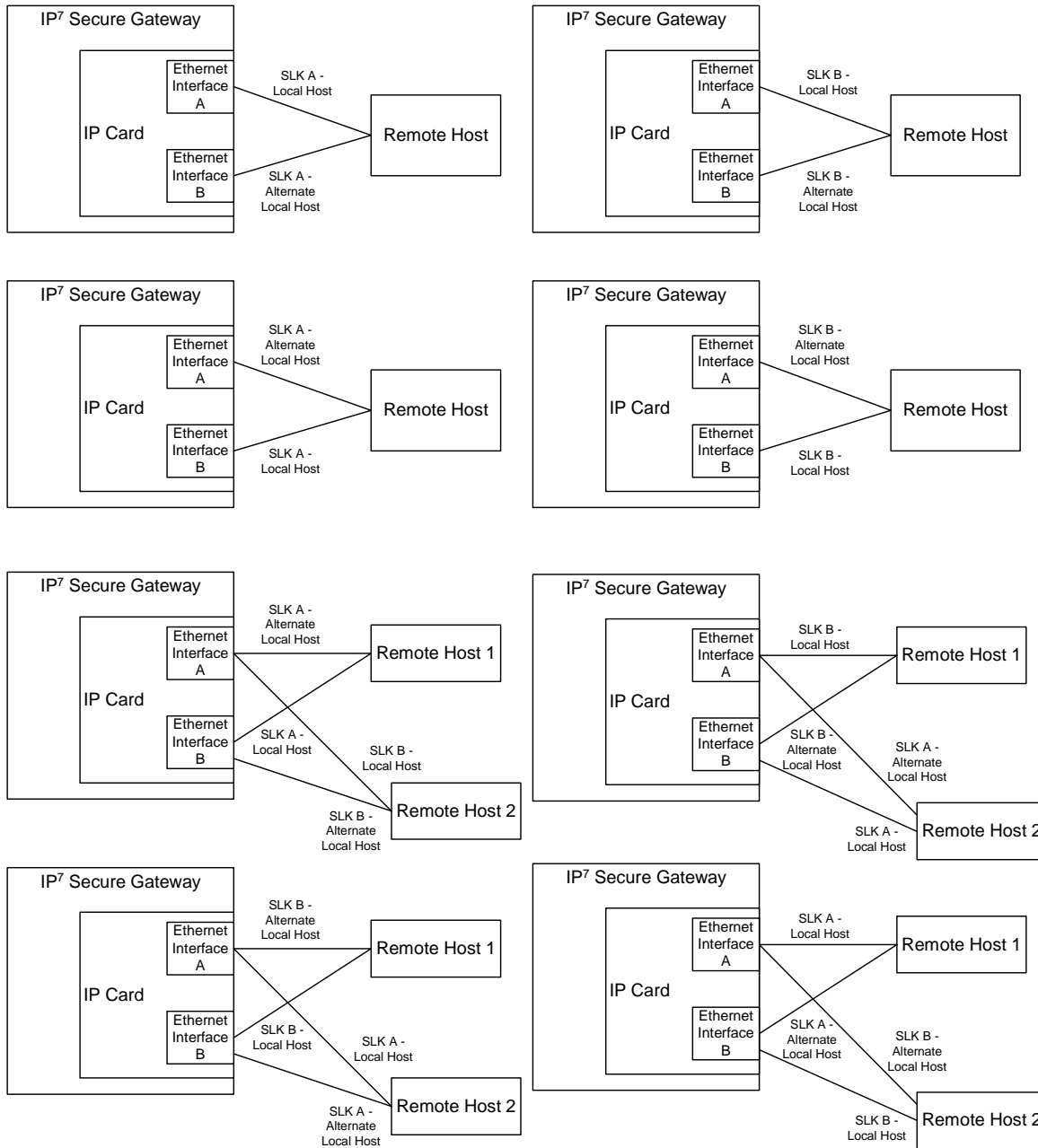
Node A	Node B
Uni-homed	Uni-homed
Uni-homed	Multi-homed
Multi-homed	Uni-homed
Multi-homed	Multi-homed

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

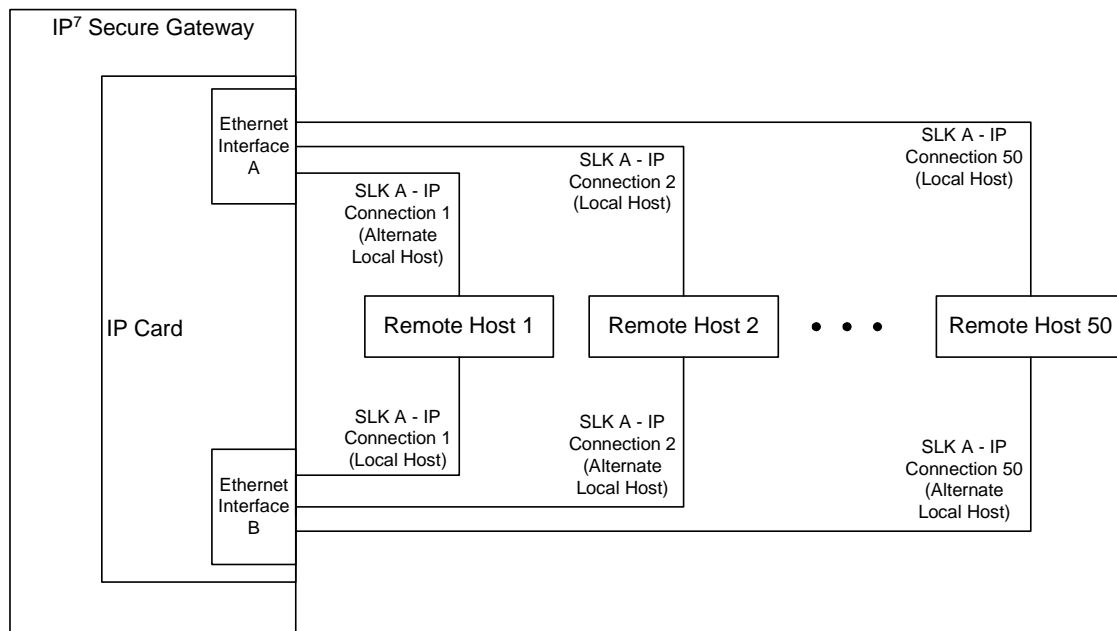
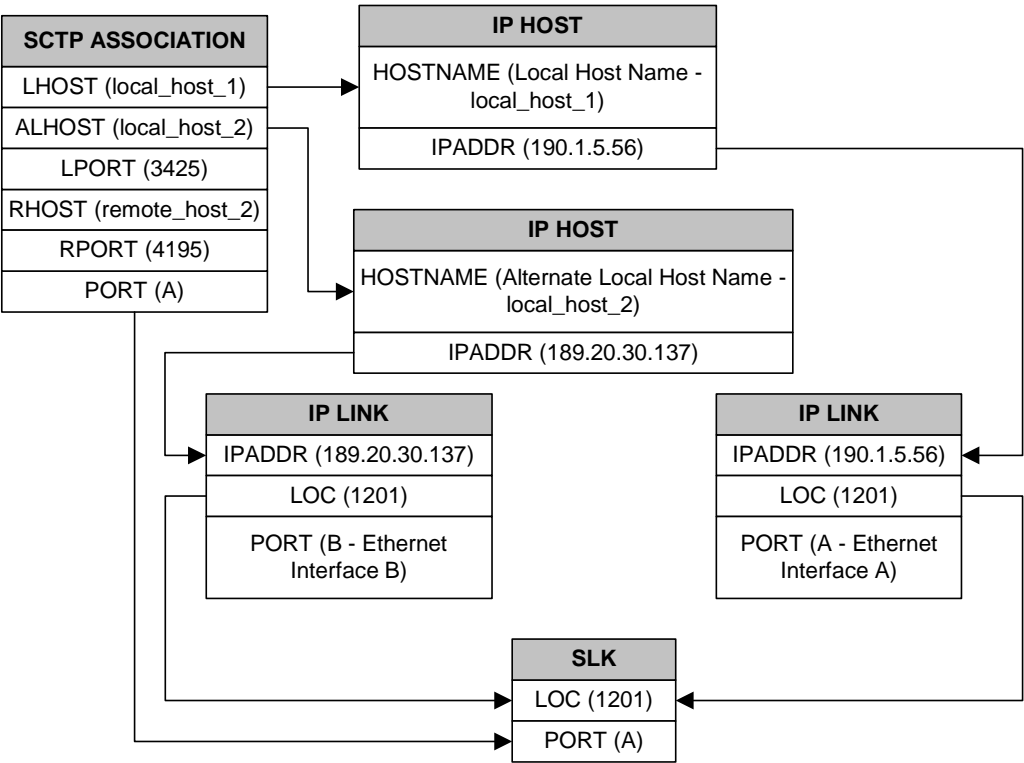


Figure 2-10 shows the components of the multi-homed Sctp association and how these components interact with each other.

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.

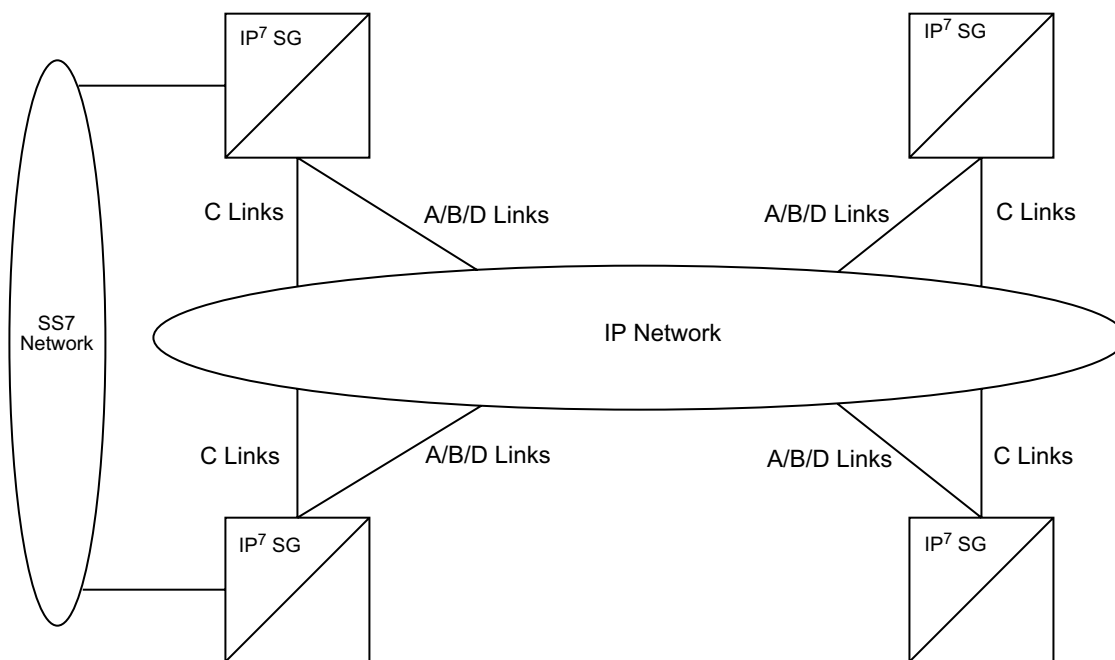
Point-to-Point Connectivity (IPLIM or IPLIMI Application)

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)

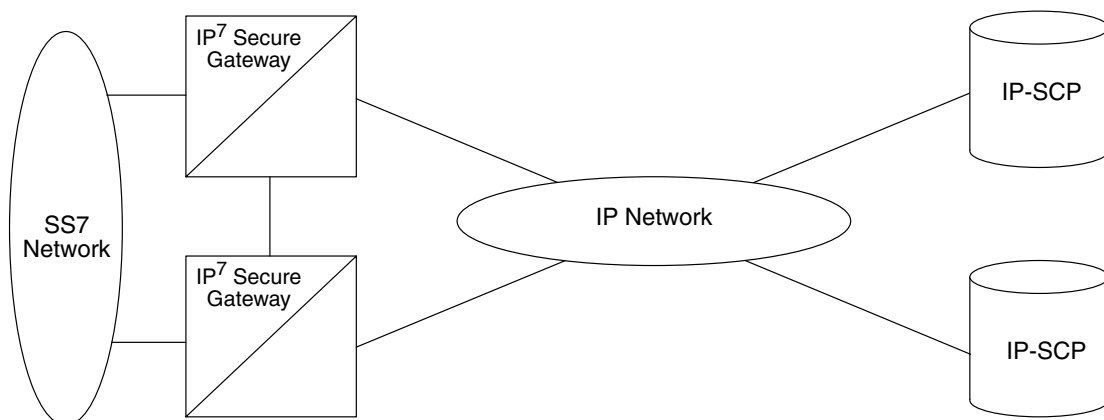
The following sections describe the types of point-to-multipoint connectivity, how routing is accomplished, and the MTP status functions provided by the `ss7ipgw` and `ipgwi` applications:

- “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.

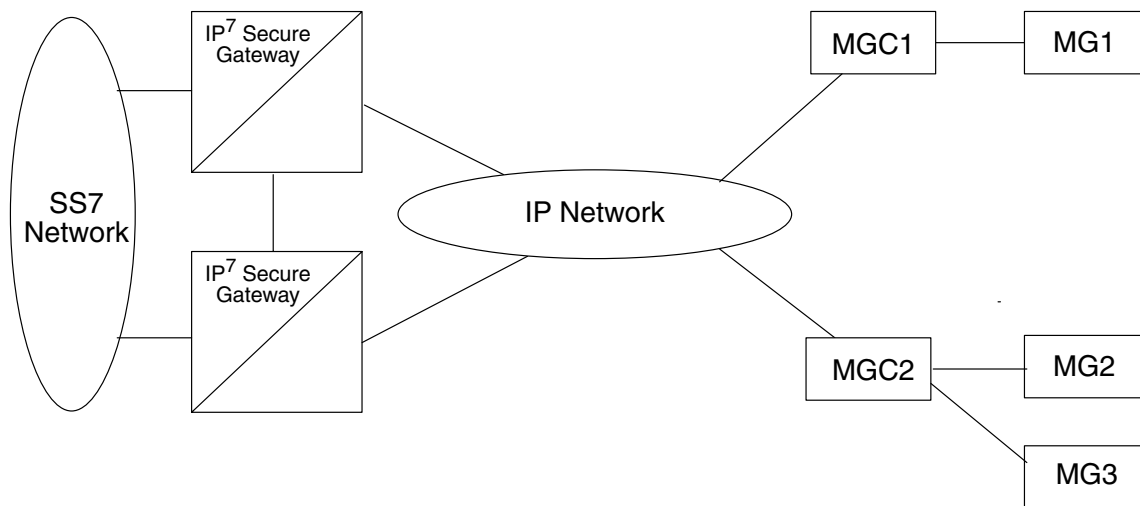
The following sequence of events illustrates this functionality:

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 socket names, as illustrated by the example in Table 2-4. MSUs that match the parameters in a given row are sent over one of the sockets shown for that row (up to 16 socket associations can be defined for a single routing key). Multiple sockets for a given row allow load sharing. In addition, multiple routing keys can be used to send traffic to a single socket.

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 SSEDCCM 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 a socket 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 a socket fails, all dynamic entries associated with the socket 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 socket, by failure of the socket, 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-SCCP/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-SCCP/non-ISUP/non-Q.BICC/non-TUP connectivity							
Static	5-5-7	02					sfhrlr11204

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

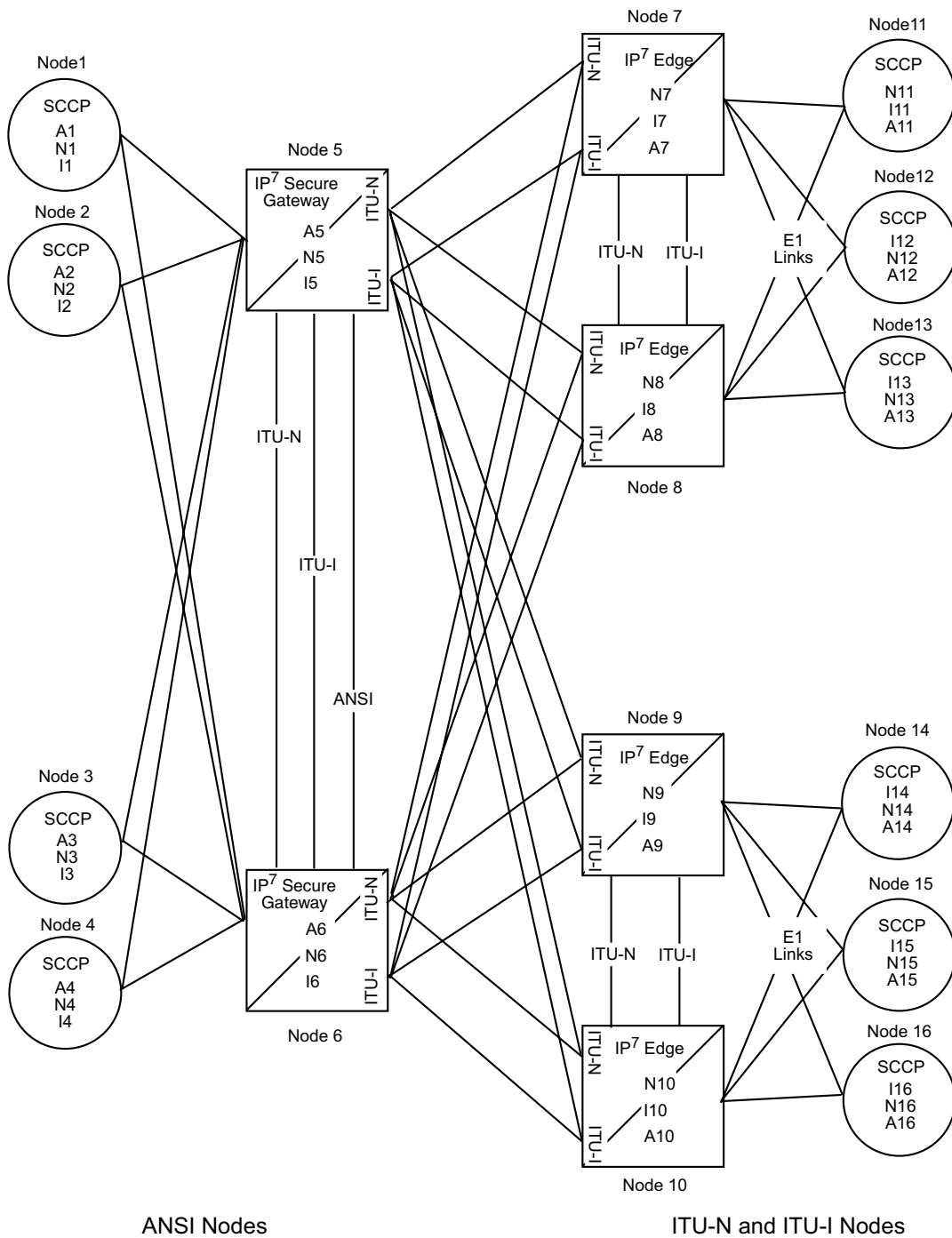


Table 2-8. Nodes and Point Codes in Complex Network Example

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.

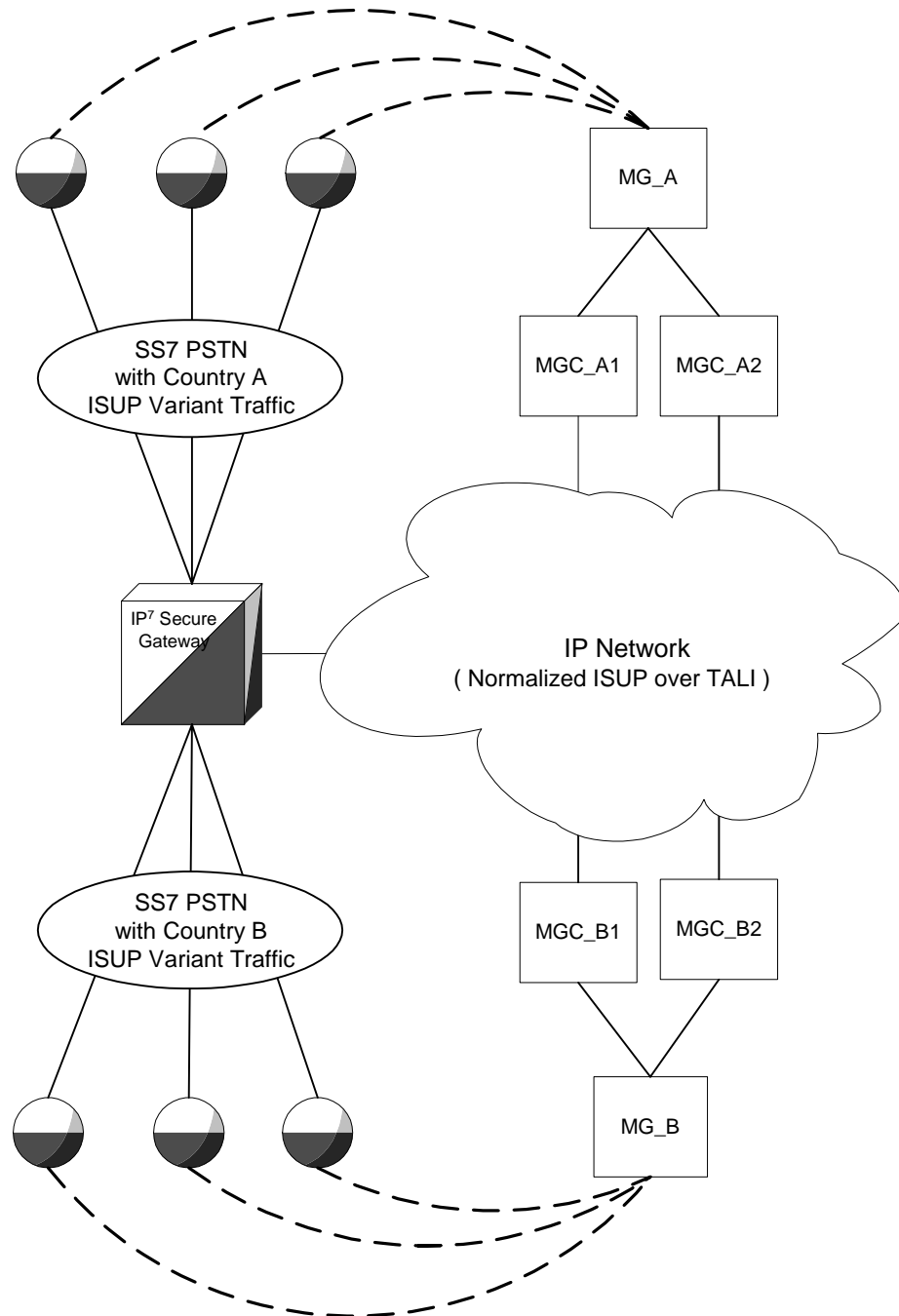
This feature allows an IP device (for example, an MGC providing Class 4 Tandem functionality) connected to an IP⁷ Secure Gateway to perform call setup for multiple countries without knowledge of the various countries' ISUP message formats. The MGC needs only to support encode and decode functionality 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

MSB	LSB
PSTN Category (16 Bits)	PSTN ID (16 Bits)

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-psn-pres** command. Use the **rtrv-psn-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 3-151 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.

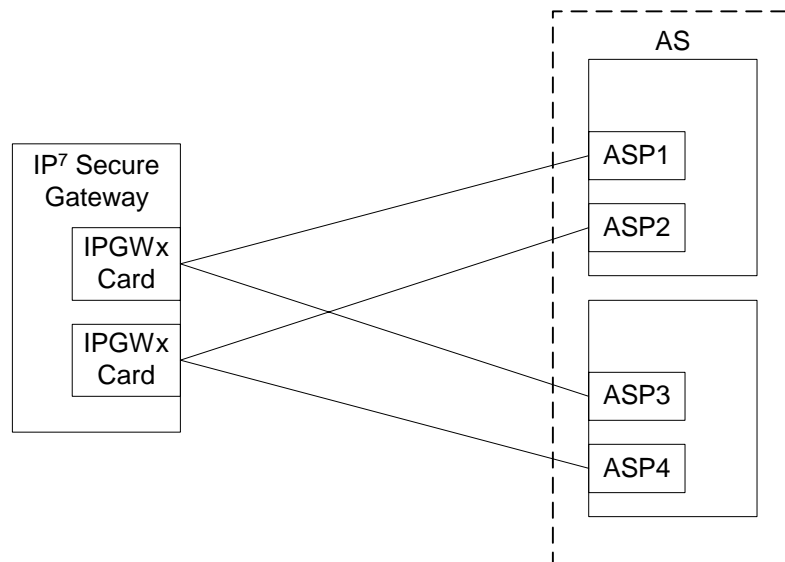
The three adapter layers used in the IP⁷ Secure Gateway are supported depending on the type of IP card being used for the IP connection. The SUA adapter layer can be used only on IPGWx cards (cards running either the SS7IPGW or IPGWI applications). The M2PA adapter layer can be used only on IPLIMx cards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

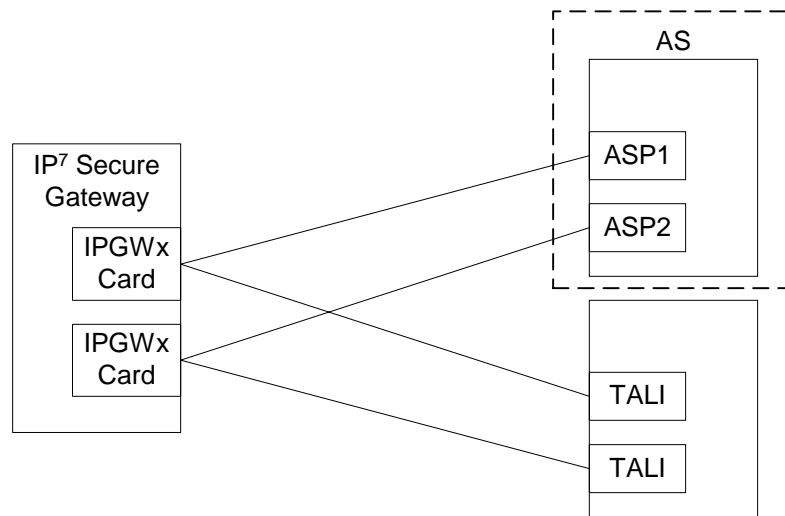
Interaction Between TALI and IETF Connections Within a Single System

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 only two IPGWx cards, resulting in a maximum of 100 connections for all IPGWx cards.

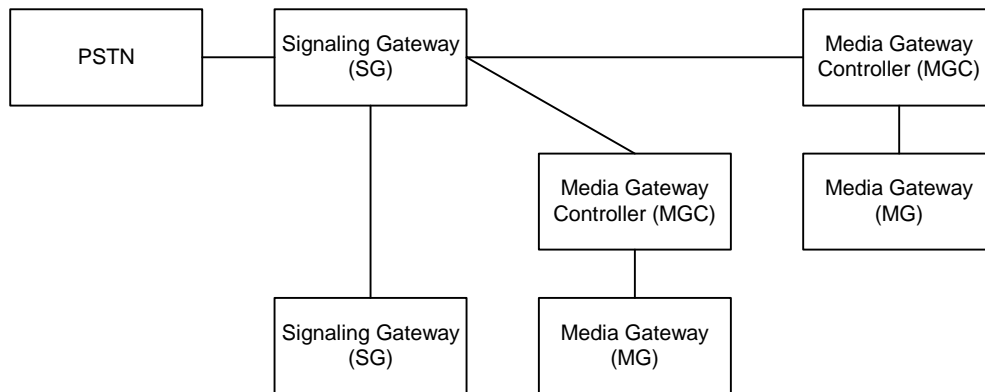
An IPLIMx card can have only one connection for each signaling link assigned to the card. The dual-slot DCM can contain only two signaling links, resulting in a maximum of two IP connections on these cards. The single-slot EDCM can contain a maximum of eight signaling links, resulting in a maximum of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

The system can contain a maximum of 250 IP connections, between IPGWx cards and IPLIMx cards.

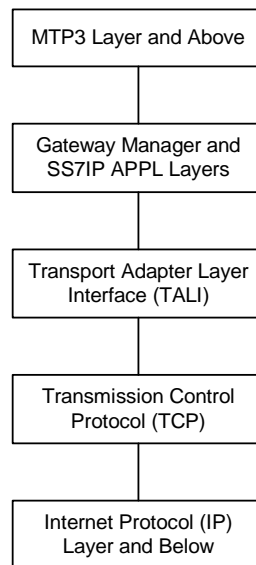
Figure 2-20. TCP Socket/SCTP Association Relationship

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.

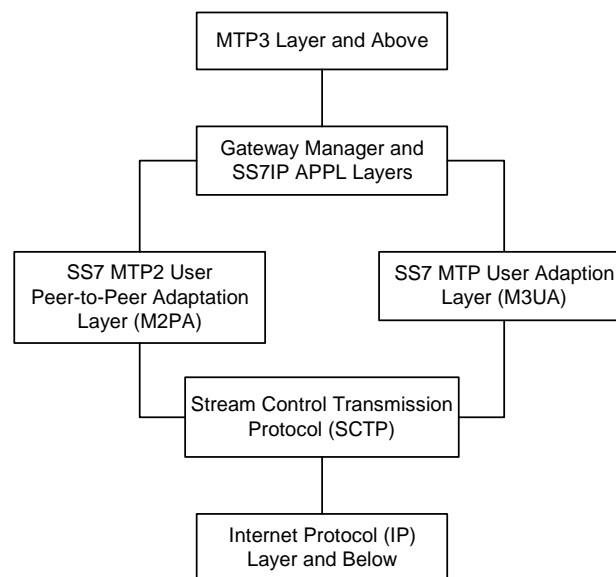
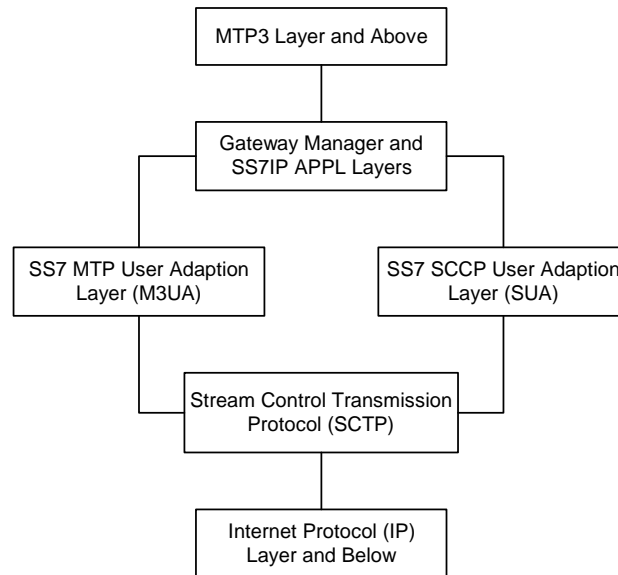
Figure 2-23. IPLIMx Protocol Stack with SCTP as the Transport Layer

Figure 2-24. IPGWx 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 IPLIMx applications, or an IPGWx card) and even a part of the same routing key (if the card is an IPGWx 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 (IPGWx 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.

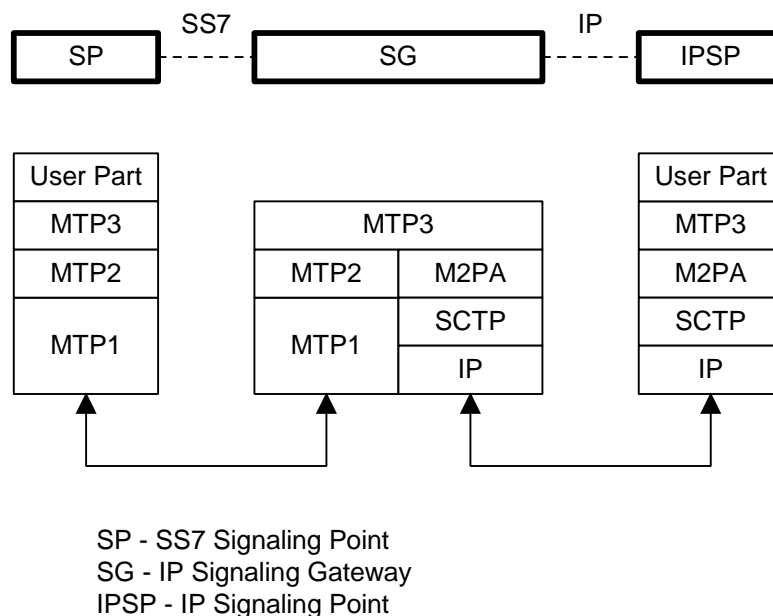
The M3UA layer at the signaling gateway maintains the availability of all configured remote application server processes, in order to manage the SCTP Associations and the traffic between the signaling gateway and application server processes. As well, the Active/Inactive state of remote application server 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 SAALTALI 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.

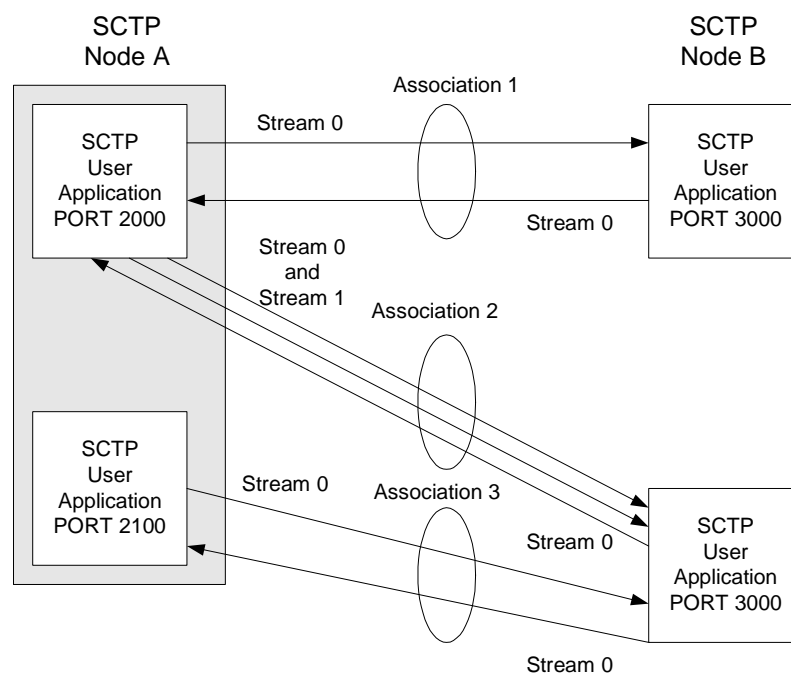
Enhanced Security

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

IP⁷ Secure Gateway Configuration Procedures

Overview	3-3
Adding an IP Card	3-15
Removing an IP Card	3-31
Changing an IP Card	3-40
Changing the IP Protocol Option	3-49
Changing IP Options other than SYNC and SCTPCSUM	3-56
Adding an IP Host	3-61
Removing an IP Host	3-63
Changing an IP Link	3-66
Adding an IP Route	3-81
Removing an IP Route	3-85
Adding an Application Socket	3-89
Removing an Application Socket	3-99
Changing an Application Socket	3-102
Configuring IP Socket Retransmission Parameters	3-114
Changing a DCM Parameter Set	3-120
Adding a Static Application Routing Key	3-124
Removing an Application Routing Key	3-133
Changing a Static Application Routing Key	3-139

Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key	3-151
Increasing the TPS on the IP Card	3-165
IETF Adapter Layer Configuration	3-171
Adding an Association	3-172
Removing an Association	3-185
Changing an Association	3-190
Configuring SCTP Retransmission Control for an Association	3-211
Changing an M2PA Timer Set	3-220
Adding an Application Server Process	3-224
Removing an Application Server Process	3-228
Adding an Application Server	3-238
Removing an Application Server	3-247
Changing an Application Server	3-251
Adding a Network Appearance	3-256
Removing a Network Appearance	3-260
Changing the SCTP Checksum Algorithm Option	3-262
Changing a UA Parameter Set	3-293

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 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*.
 - Linksets - see Chapter 3, “SS7 Configuration,” in the *Database Administration Manual - SS7*
 - Signaling links - 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.

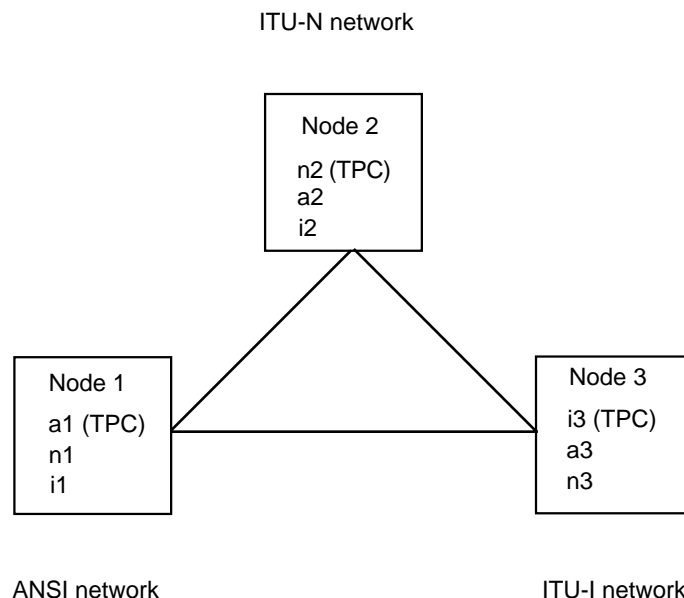
Once a feature has been turned on with the `chg-feat` command, the feature cannot be turned off.

Steps 4, 16, 17, and 18 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 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 must specify an adjacent point code (**apc**) with the **ipgwapc** parameter set to **yes** and the **mtprse** parameter set to **no**.

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. For a detailed procedure, refer to the *Database Administration Manual - SS7*.

7. The signaling links must be in the database. Verify this with the **rtrv-slk** command. The signaling links are assigned to linksets from step 6, and to IP cards with the **ss7ipgw**, **ipgwi**, **iplim**, or **iplimi** application, from step 4. 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 SSED CM 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. Linksets associated with the **ss7ipgw** or **ipgwi** application can have only one signaling link.

8. 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 6. 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.
9. When the IP cards are added to the database in step 4, 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.
10. When the IP cards are added to the database in step 4, 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.
11. Local IP hosts must be in the database. If name server capability (**dnsc** parameter) was not set up in step 10 with the **chg-ip-card** command, the remote IP hosts must also 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 related information. If the necessary IP hosts are not in the database, add them with the **ent-ip-host** command.
12. 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).

13. 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.

14. 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.

Single-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).

15. 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.

16. 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.
17. 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.
18. 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, 16, 17, and 18 are valid only for **ss7ipgw** and **ipgwi** applications.

19. 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.
20. 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-appl** 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-appl** command.
21. 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 3-11 shows the relationships of the database elements that are configured in these procedures.

Figure 3-2. IP⁷ Secure Gateway Database Relationships

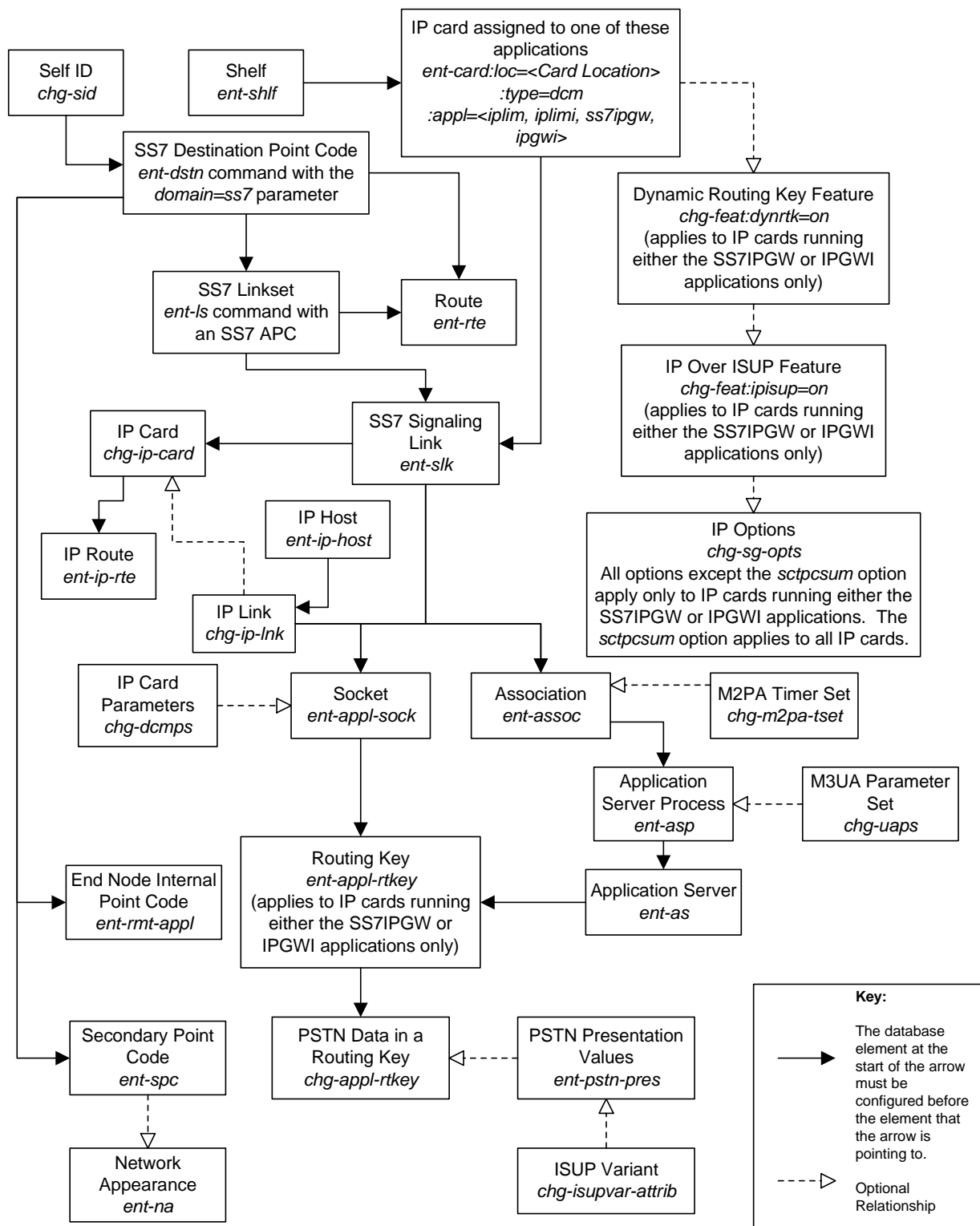


Figure 3-3 shows a typical network configuration and Tables 3-1, 3-2, 3-3 (following Figure 3-3) show the table information that would exist in the system with point code 2-2-2 after provisioning is completed.

Figure 3-3. Typical System Configuration

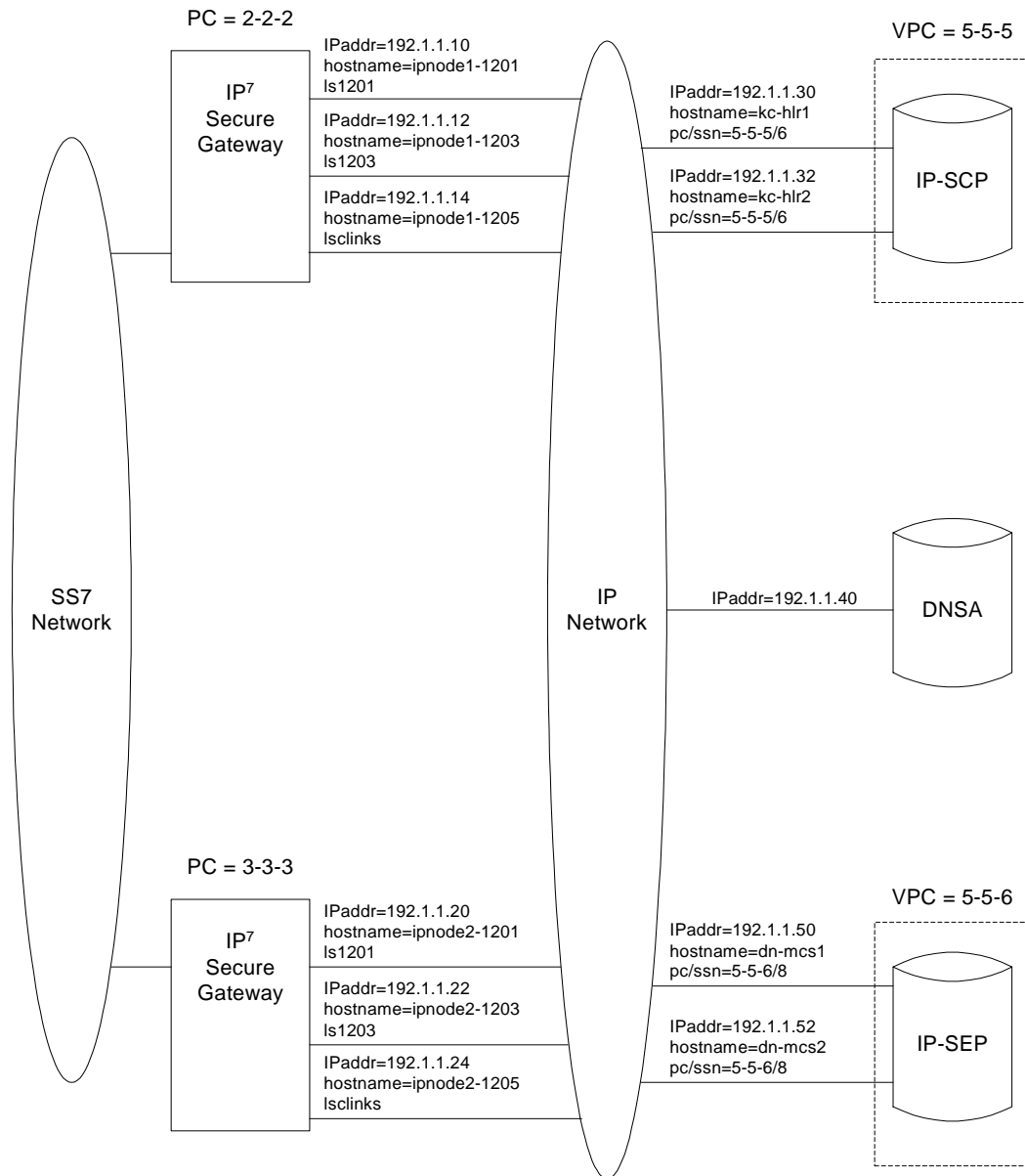


Table 3-1. Typical IP Routing

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

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 IP⁷ Secure Gateway and the **ent-card** command. 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
DCM	dcm	iplim/iplmi	ANSI/ITU	41*
EDCM (Dual- or single-slot)		ss7ipgw	ANSI	2
		ipgwi	ITU	2
* If the system contains from 701 to 1500 signaling links, the maximum number of cards running either the iplim or iplmi application is 100.				

: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 3-17.

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*
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 an ASM or 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
ASM	850
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 03-06-12 09:12:36 GMT Rel 31.0.0
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 03-06-12 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
CARD   TYPE      APPL      LSET NAME      PORT  SLC  LSET NAME      PORT  SLC
1101   ASM        SCCP      -----      --   --  -----      --   --
1102   ASM        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.

2. Verify that the card to be entered has been physically installed into the proper location (see the Card Slot Selection section on page 3-16).



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.

3. 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.

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

```
rlghncxa03w 03-06-12 09:12:36 GMT Rel 31.0.0
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.

5. 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:dynrtk=on
```

To enable both features, enter this command.

```
chg-feat:ipisup=on:dynrtk=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 03-06-12 09:12:36 GMT Rel 31.0.0
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 3-17. 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 03-06-12 09:12:36 GMT Rel 31.0.0
ENT-CARD: MASP A - COMPLTD
```

8. 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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
CARD   TYPE      APPL      LSET NAME      PORT SLC LSET NAME      PORT SLC
1317   DCM        IPGWI    -----      --  --  -----      --  --
```

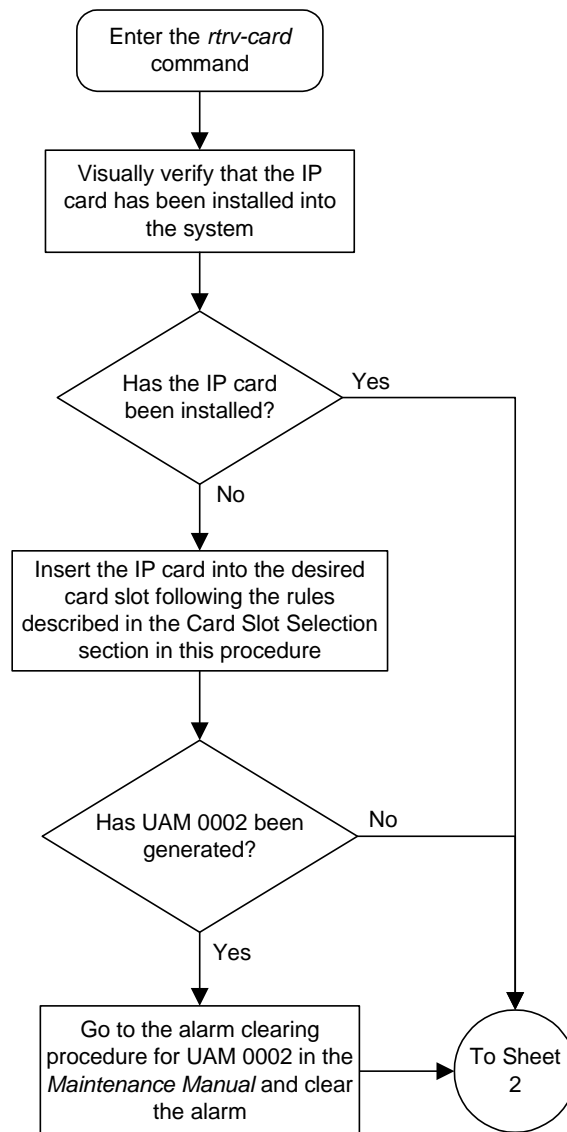
9. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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.
```

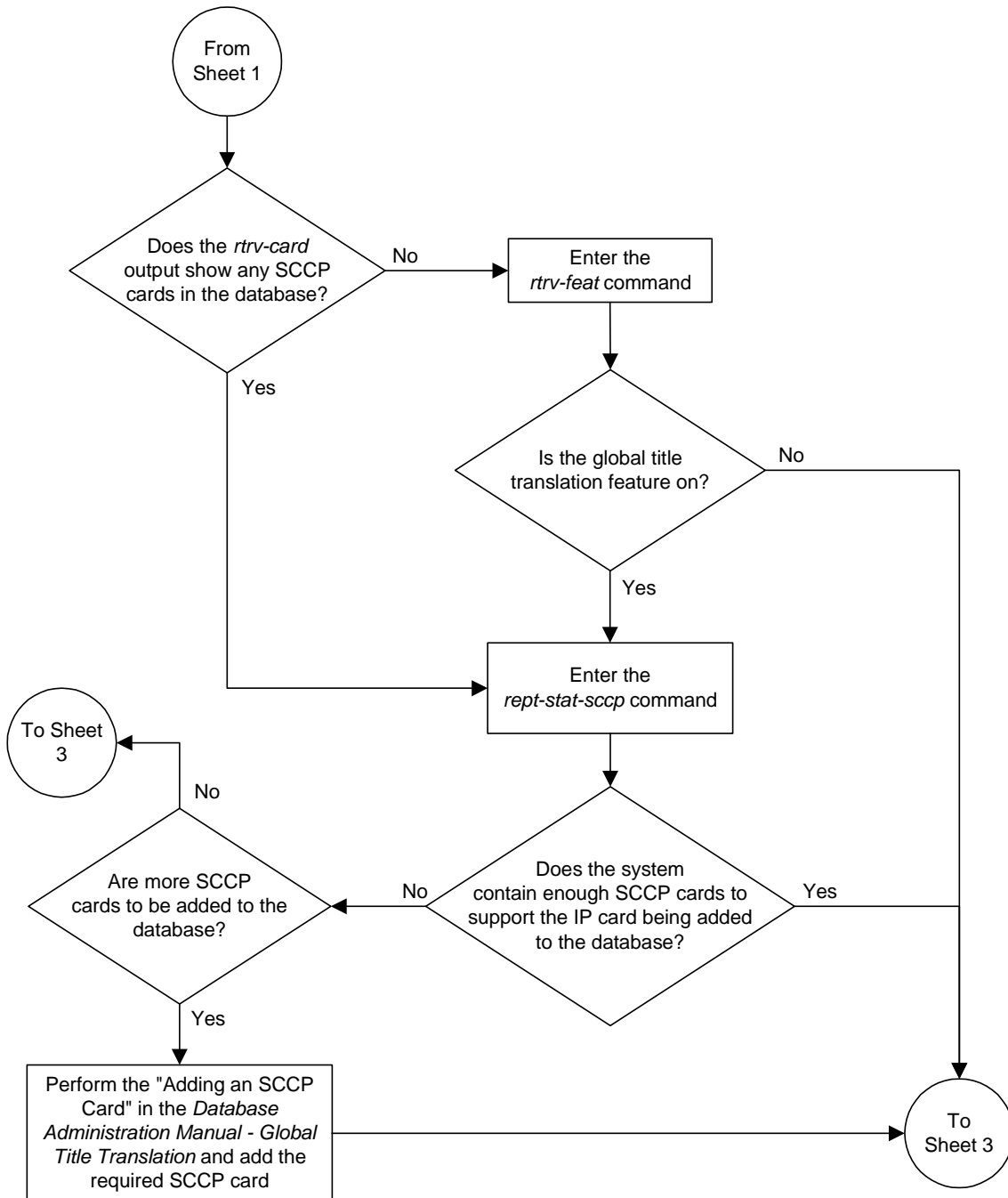
10. If you wish to change the quantity of static and dynamic routing keys in the database, perform the "Changing IP Options other than SYNC and SCTPCSUM" procedure on page 3-56. Otherwise, this procedure is finished.
-

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

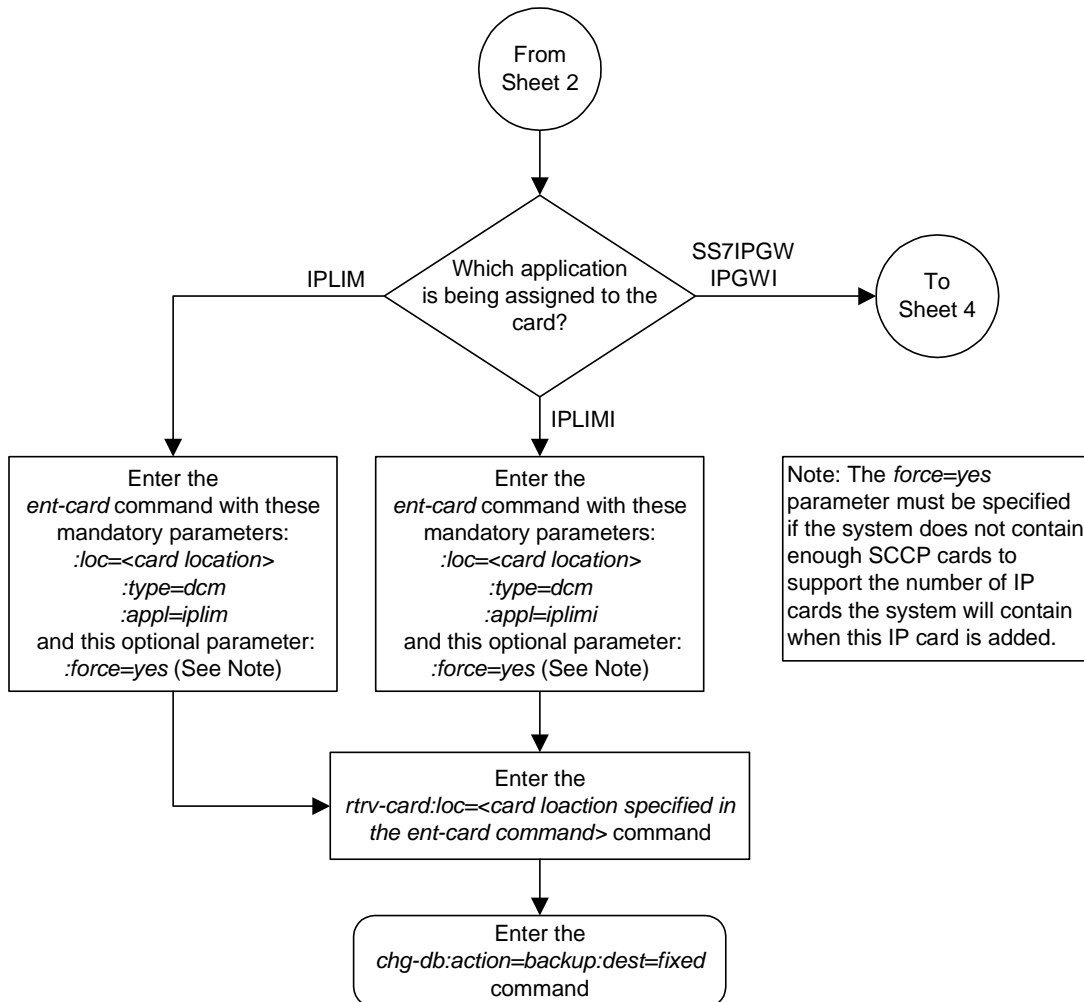
NOTE: Before executing this procedure, make sure you have purchased the ISUP-over-IP feature and Dynamic Routing Key features. If you are not sure whether you have purchased the ISUP-over-IP feature or Dynamic Routing Key features, contact your Tekelec Sales Representative or Account Representative.



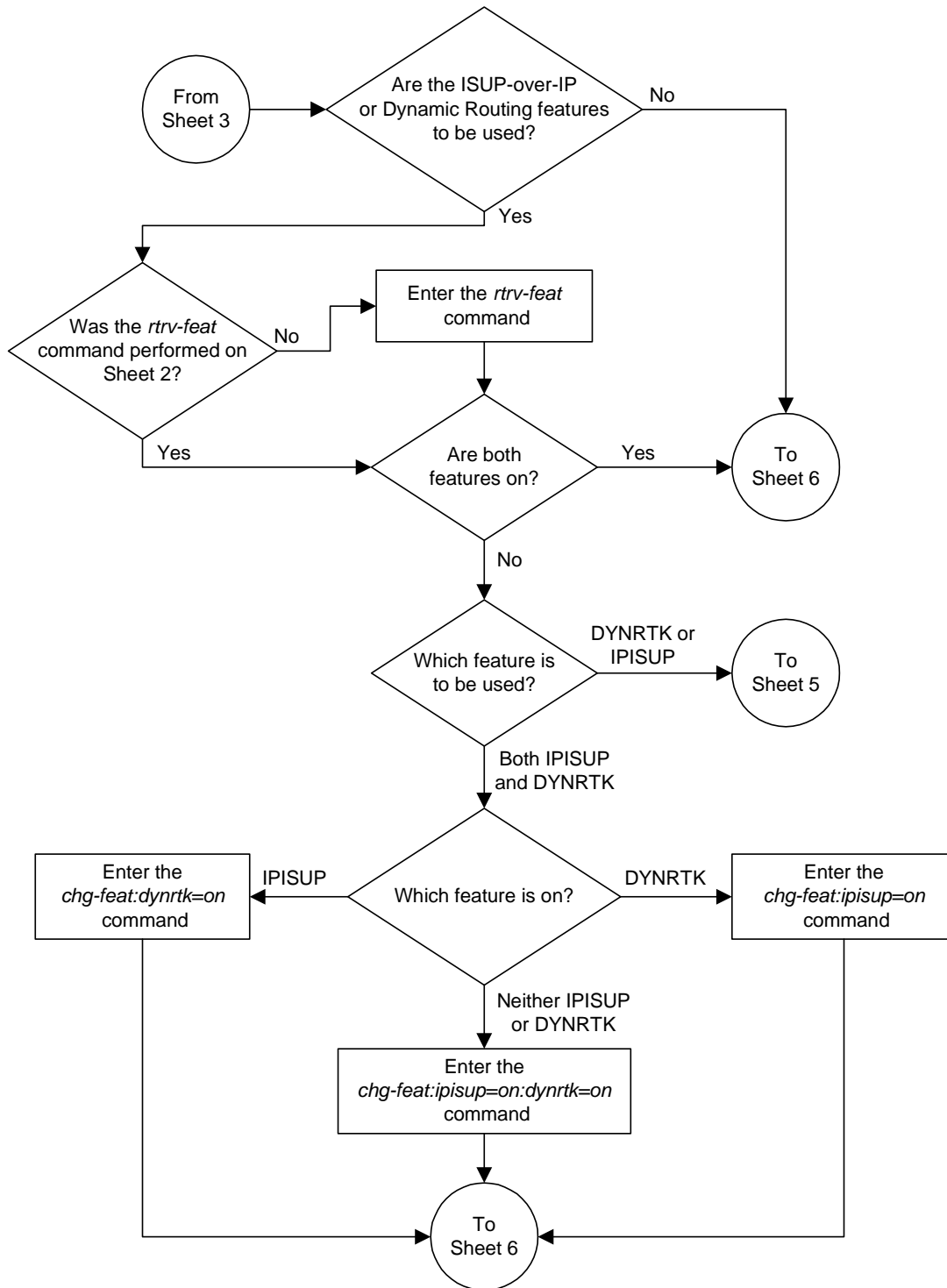
Flowchart 3-1. Adding an IP Card (Sheet 2 of 6)



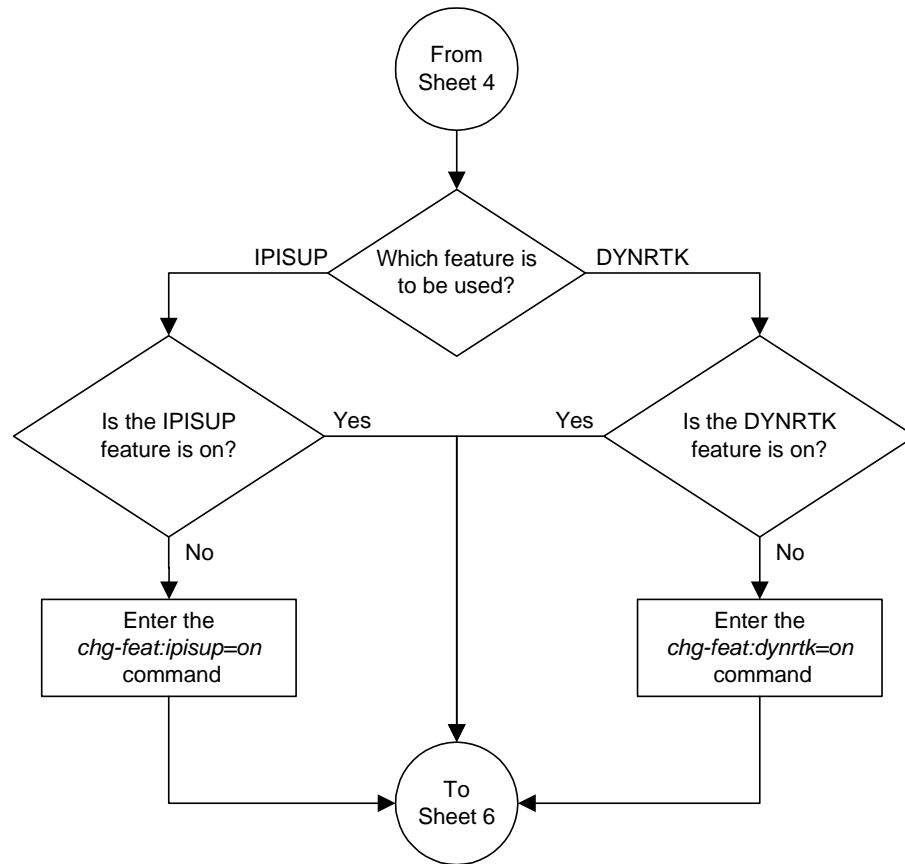
Flowchart 3-1. Adding an IP Card (Sheet 3 of 6)



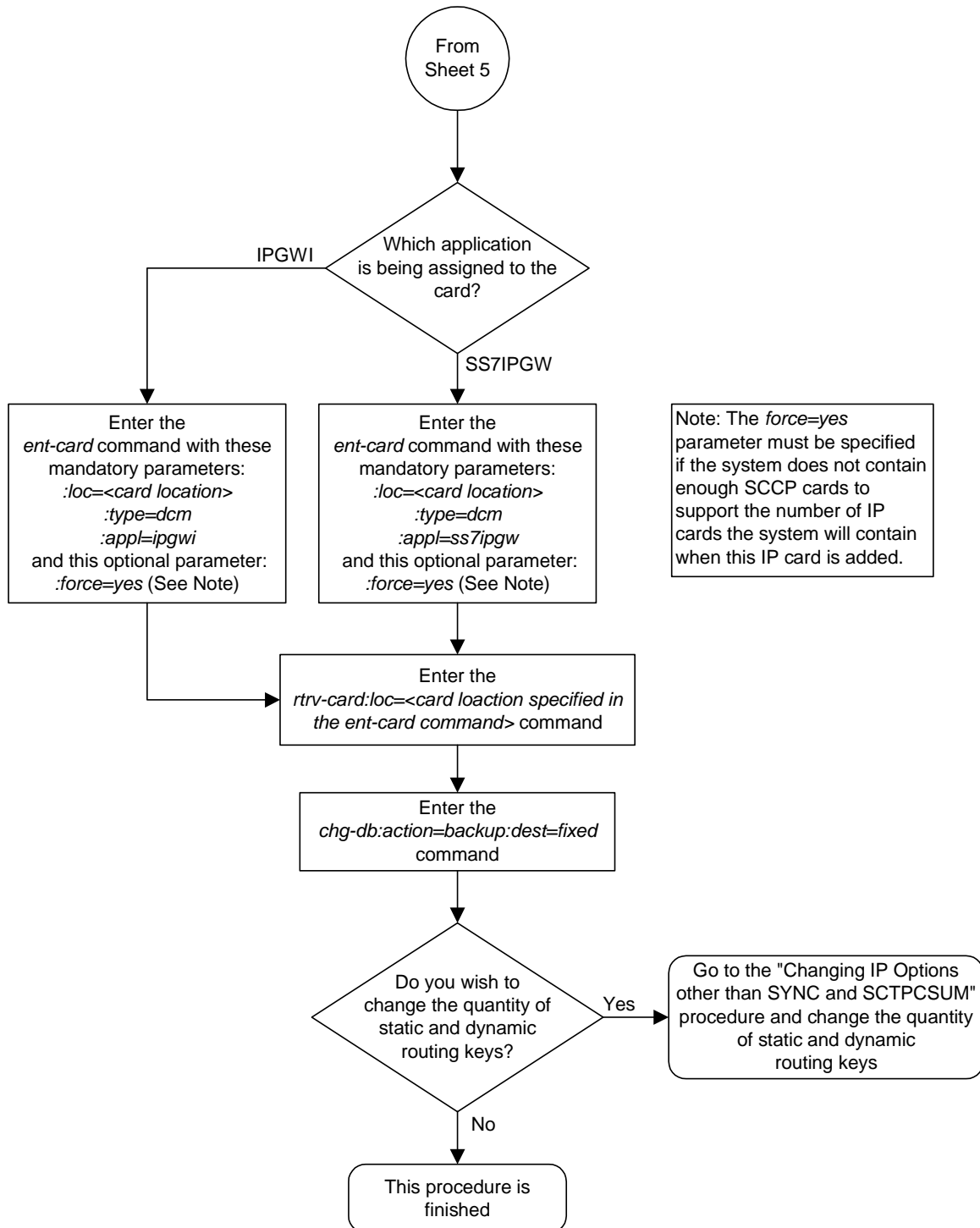
Flowchart 3-1. Adding an IP Card (Sheet 4 of 6)



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 **dlt-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 SS7 LIM or IP card in service, removing this card from the database will cause SS7 traffic to be lost and isolate the system from the network.

Procedure

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

```
rlghncxa03w 03-06-15 16:34:56 GMT Rel 31.0.0
CARD   TYPE      APPL      LSET NAME      PORT SLC LSET NAME      PORT SLC
1101   ASM        SCCP      -----      --  --  -----      --  --
1102   ASM        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 03-06-28 09:12:36 GMT Rel 31.0.0
SLK      LSN      CLLI      PST      SST      AST
1205,A ipgwy1  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 03-06-28 09:12:36 GMT Rel 31.0.0
SLK      LSN      CLLI      PST      SST      AST
1205,B ipgwy3  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 03-06-28 09:12:36 GMT Rel 31.0.0
SLK      LSN      CLLI      PST      SST      AST
1207,A ipgwy2  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 03-06-12 09:12:36 GMT Rel 31.0.0
Deactivate Link message sent to card
```

4. 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 03-06-28 09:12:36 GMT Rel 31.0.0
SLK      LSN      CLLI      PST      SST      AST
1205,A ipgwy1  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 03-06-28 09:12:36 GMT Rel 31.0.0
SLK      LSN      CLLI      PST      SST      AST
1205,B ipgwy3  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 03-06-28 09:12:36 GMT Rel 31.0.0
SLK      LSN      CLLI      PST      SST      AST
1207,A ipgwy2  ipnode2  ----- OOS-MT-DSBLD Avail  ----
  ALARM STATUS      = * 0236 REPT-LKS:not aligned.
  UNAVAIL REASON    = NA
Command Completed.
```

5. 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 03-06-27 16:43:42 GMT Rel 31.0.0
```

CARD	VERSION	TYPE	APPL	PST	SST	AST
1101	114-003-000	ASM	SCCP	IS-NR	Active	---
1102	114-003-000	ASM	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	GPSM	EOAM	IS-NR	Active	---
1114	114-002-000	TDM		IS-NR	Active	---
1115	114-002-000	GPSM	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 **dlr-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 03-06-28 16:31:35 GMT Rel 31.0.0
```

LSN	APCA	(SS7)	SCRN	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

CLLI	TFATCABMLQ	MTPRSE	ASL8
-----	2	yes	yes

LOC	PORT	SLC	TYPE	SET	BPS	MODE	TSET	ECM	N1	N2
1205	A	0	DCM	1	1544000	---	---	BASIC	---	----
1303	A	0	DCM	1	1544000	---	---	BASIC	---	----

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


```
rtrv-ls:lsn=ipnode2
```

This is an example of the possible output

```
rlghncxa03w 03-06-28 16:31:35 GMT Rel 31.0.0
                                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

                                CLLI                                TFATCABMLQ  MTPRSE  ASL8
                                -----  2                                yes      yes

                                L2T                                L1                                PCR  PCR
                                SET  BPS                                MODE TSET  ECM  N1  N2
                                1    1544000  ---  ---  BASIC  ---  -----
                                1207  A    0  DCM      1    1544000  ---  ---  BASIC  ---  -----
```

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

```
rtrv-ls:lsn=ipnode3
```

This is an example of the possible output

```
rlghncxa03w 03-06-28 16:31:35 GMT Rel 31.0.0
                                L3T SLT                                GWS GWS GWS
LSN          APCA   (SS7)  SCRNL  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

                                CLLI                                TFATCABMLQ  MTPRSE  ASL8
                                -----  2                                yes      yes

                                L2T                                L1                                PCR  PCR
                                SET  BPS                                MODE TSET  ECM  N1  N2
                                1    1544000  ---  ---  BASIC  ---  -----
                                1205  B    0  DCM      1    1544000  ---  ---  BASIC  ---  -----
                                1303  A    0  DCM      1    1544000  ---  ---  BASIC  ---  -----
```

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 03-06-12 09:12:36 GMT Rel 31.0.0
Card has been inhibited.
```

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

```
rlghncxa03w 03-06-27 16:43:42 GMT Rel 31.0.0
CARD  VERSION      TYPE      APPL      PST          SST          AST
1101  114-003-000    ASM       SCCP       IS-NR        Active       ---
1102  114-003-000    ASM       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    GPSM      EOAM        IS-NR        Active       ---
1114  114-002-000    TDM       EOAM        IS-NR        Active       ---
1115  114-002-000    GPSM      EOAM        IS-NR        Active       ---
1116  114-002-000    TDM       EOAM        IS-NR        Active       ---
1117  114-002-000    MDAL      EOAM        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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-12 09:12:36 GMT Rel 31.0.0
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.

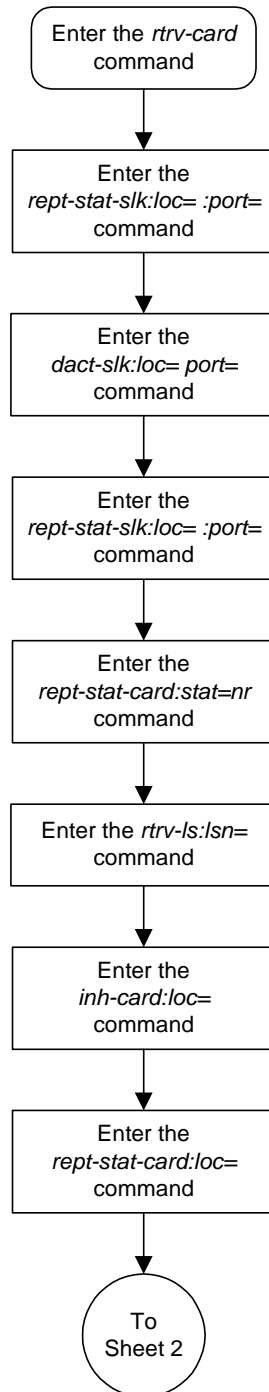
```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.
```

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

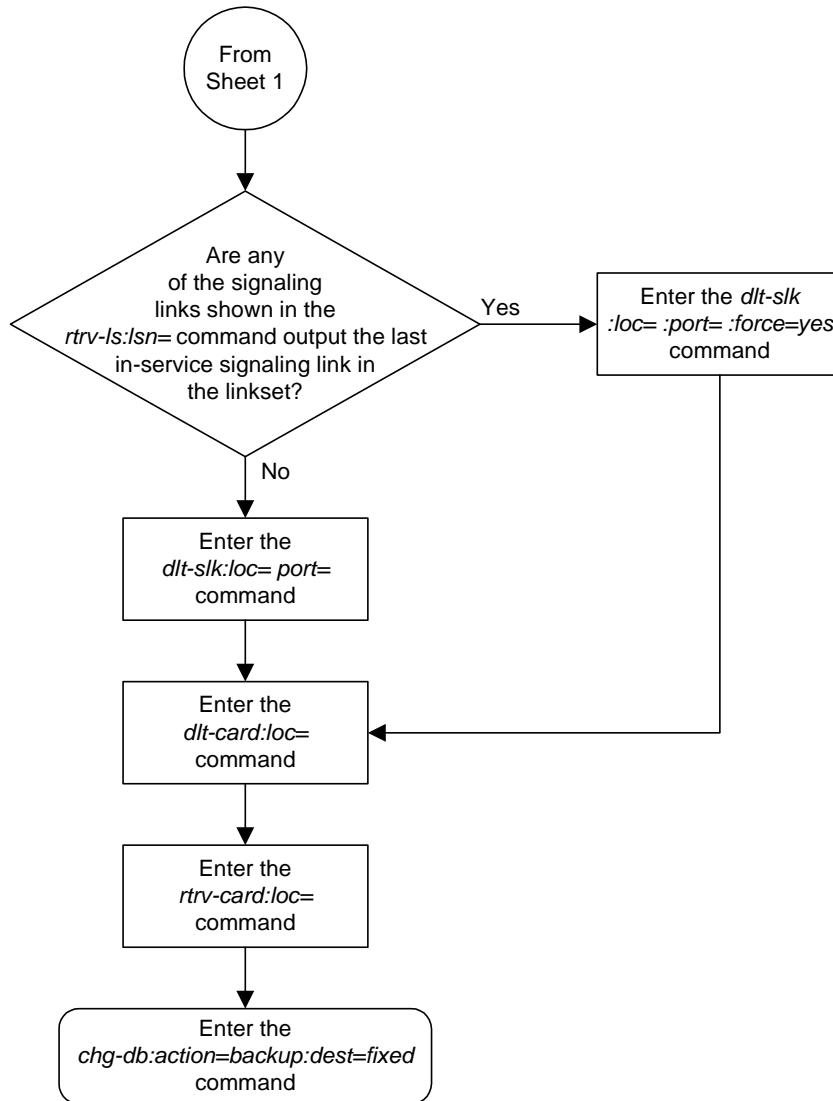
```
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.
```

```
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)



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.

The network portion of the default router IP addresses must match either the Ethernet A (**dnrsa**) or Ethernet B (**dnrsb**) IP address. The IP address of the Ethernet interface (**dnrsa** or **dnrsb**, the address whose network portion matches the network portion of the default router IP address) must be shown in the **rtrv-ip-lnk** output before the **defrouter** parameter can be specified.

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** – local
- **:dnrsa** – 0.0.0.0
- **:dnrsb** – 0.0.0.0
- **:domain** – No domain name specified

- **:defrouter** – 0.0.0.0
- **: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 3-12 and Table 3-3 on page 3-14.

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 03-06-28 21:17:37 GMT Rel 31.0.0
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 03-06-28 21:17:37 GMT Rel 31.0.0
LOC  PORT LSN          SLC TYPE  IPLIML2
1201  A    nc001        0  IPLIM  SAALTALI
```

- 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 03-06-28 21:16:37 GMT Rel 31.0.0
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.

-
- 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 03-06-12 09:12:36 GMT Rel 31.0.0
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 03-06-27 17:00:36 GMT Rel 31.0.0
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 03-06-27 17:00:36 GMT Rel 31.0.0
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.

- Inhibit the IP card using the **inh-card** command. For example, enter this command.

```
inh-card:loc=1201
```

This message should appear.

```
rlghncxa03w 03-06-28 21:18:37 GMT Rel 31.0.0
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 03-06-27 17:00:36 GMT Rel 31.0.0
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. The following is an example of the possible output.

```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
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 address is not shown in the **rtrv-ip-lnk** output, go to the “Changing an IP Link” procedure on page 3-66 and change the IP link to include the required IP address.

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 03-06-28 21:20:37 GMT Rel 31.0.0
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 03-06-28 21:21:37 GMT Rel 31.0.0
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  SRVONLY
  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 03-06-28 21:22:37 GMT Rel 31.0.0
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 03-06-27 17:00:36 GMT Rel 31.0.0
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 03-06-07 11:11:28 GMT Rel 31.0.0
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
```

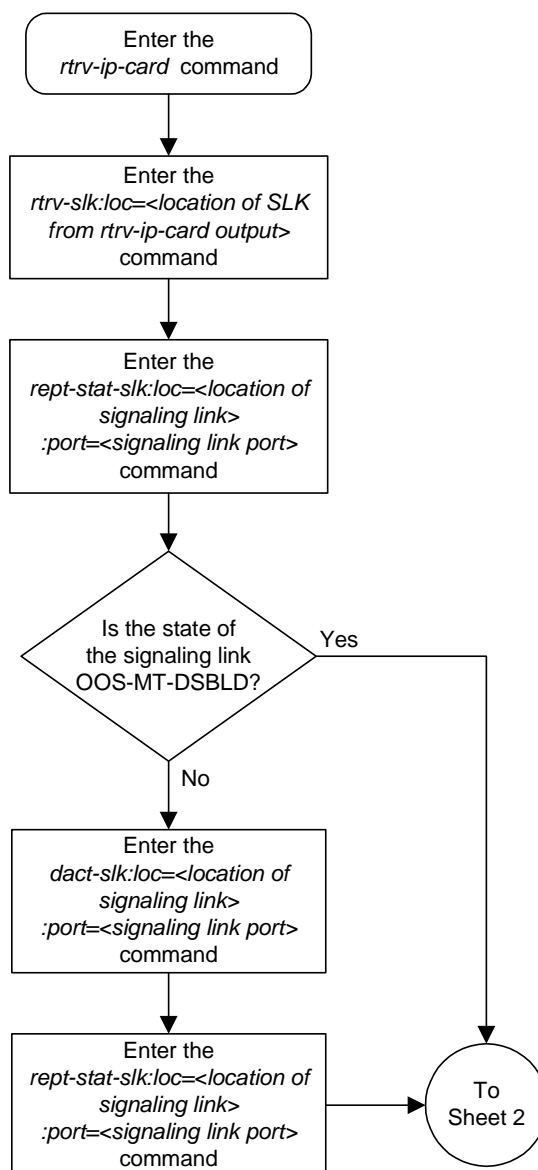
This message should appear.

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
SLK   LSN      CLLI      PST      SST      AST
1201,A nc001   -----  IS-NR     Avail    ----
Command Completed.
```

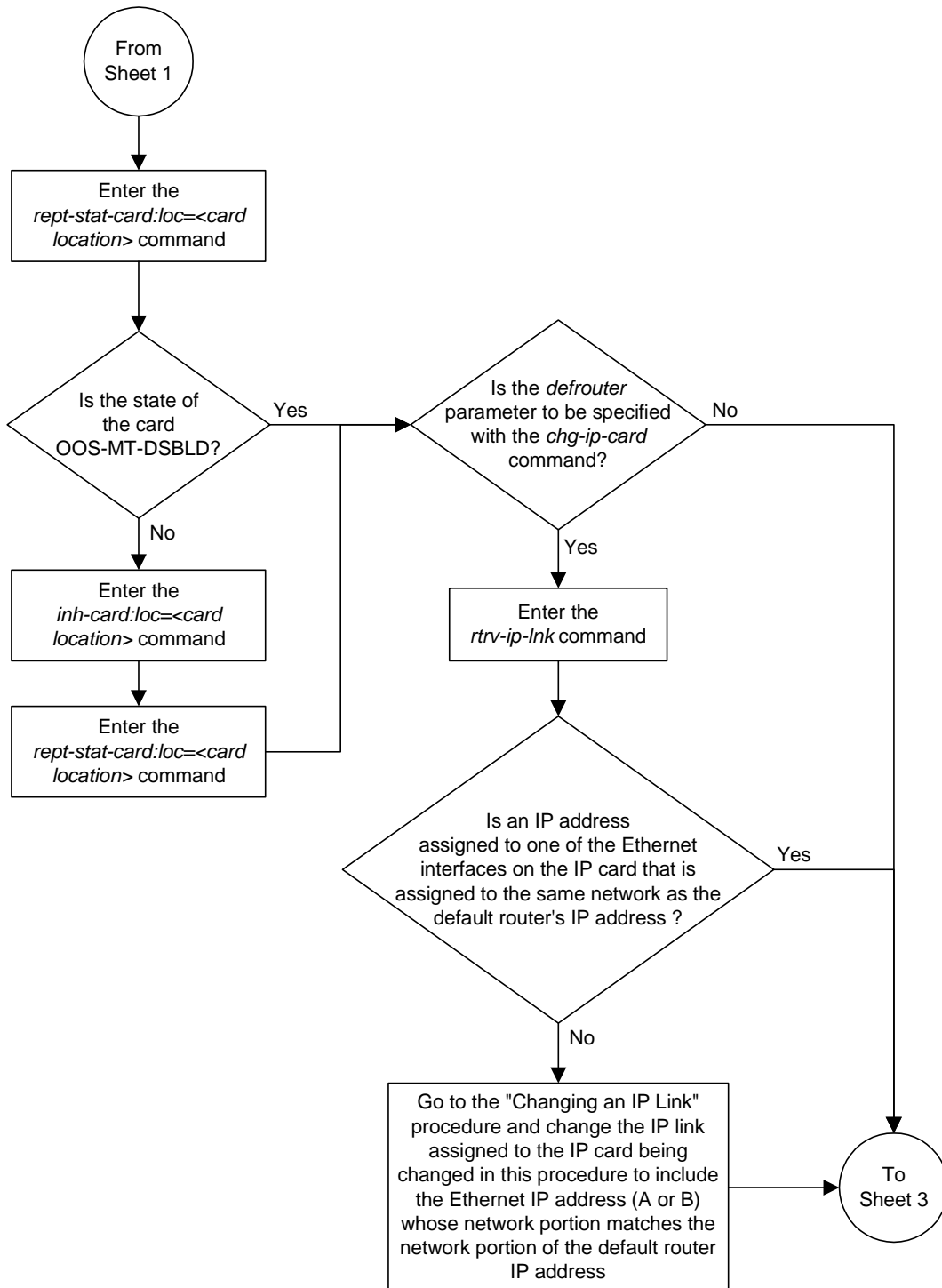
16. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

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.

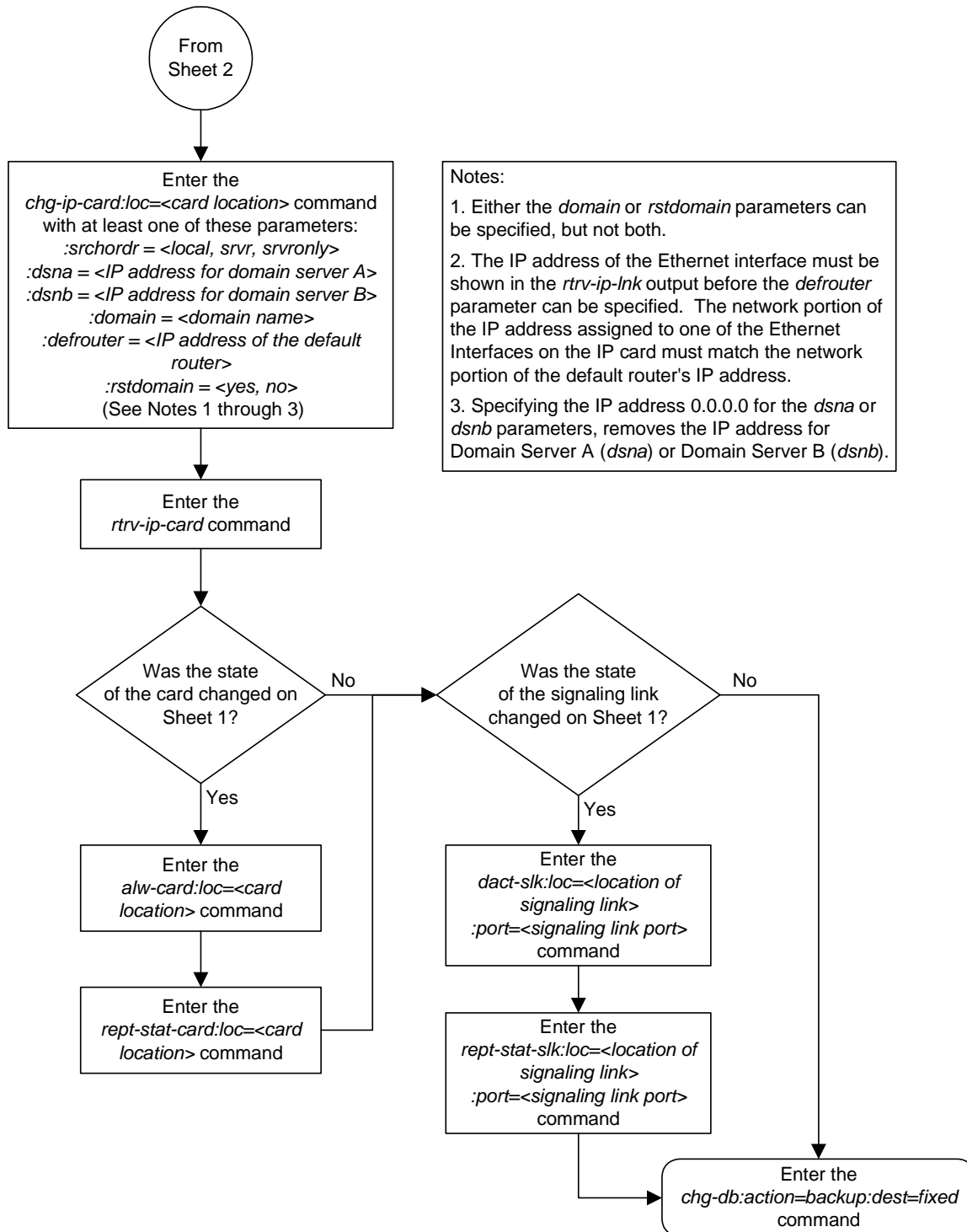
Flowchart 3-3. Changing an IP Card (Sheet 1 of 3)



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



Flowchart 3-3. Changing an IP Card (Sheet 3 of 3)



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 03-06-28 21:16:37 GMT Rel 31.0.0
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
```

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 03-06-28 21:17:37 GMT Rel 31.0.0
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 03-06-19 21:17:04 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-12 09:12:36 GMT Rel 31.0.0
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 03-06-27 17:00:36 GMT Rel 31.0.0
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.
```

7. 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 03-06-27 17:00:36 GMT Rel 31.0.0
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.

8. Inhibit the IP card using the **inh-card** command. For example, enter this command.

```
inh-card:loc=1201
```

This message should appear.

```
rlghncxa03w 03-06-28 21:18:37 GMT Rel 31.0.0
Card has been inhibited.
```

9. 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 03-06-27 17:00:36 GMT Rel 31.0.0
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 03-06-28 21:19:37 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
SYNC:          SASSI
SRKQ:          250
DRKQ:          750
SNMPCONT:      john doe 555-123-4567
GETCOMM:       public
SETCOMM:       private
TRAPCOMM:      public
INHFEPAALM:    NO
SCTPCSUM:      crc32c
IPGWABATE:     NO
IPLIMABATE:    NO
```

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 03-06-28 21:21:37 GMT Rel 31.0.0
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 03-06-27 17:00:36 GMT Rel 31.0.0
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 03-06-07 11:11:28 GMT Rel 31.0.0
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
```

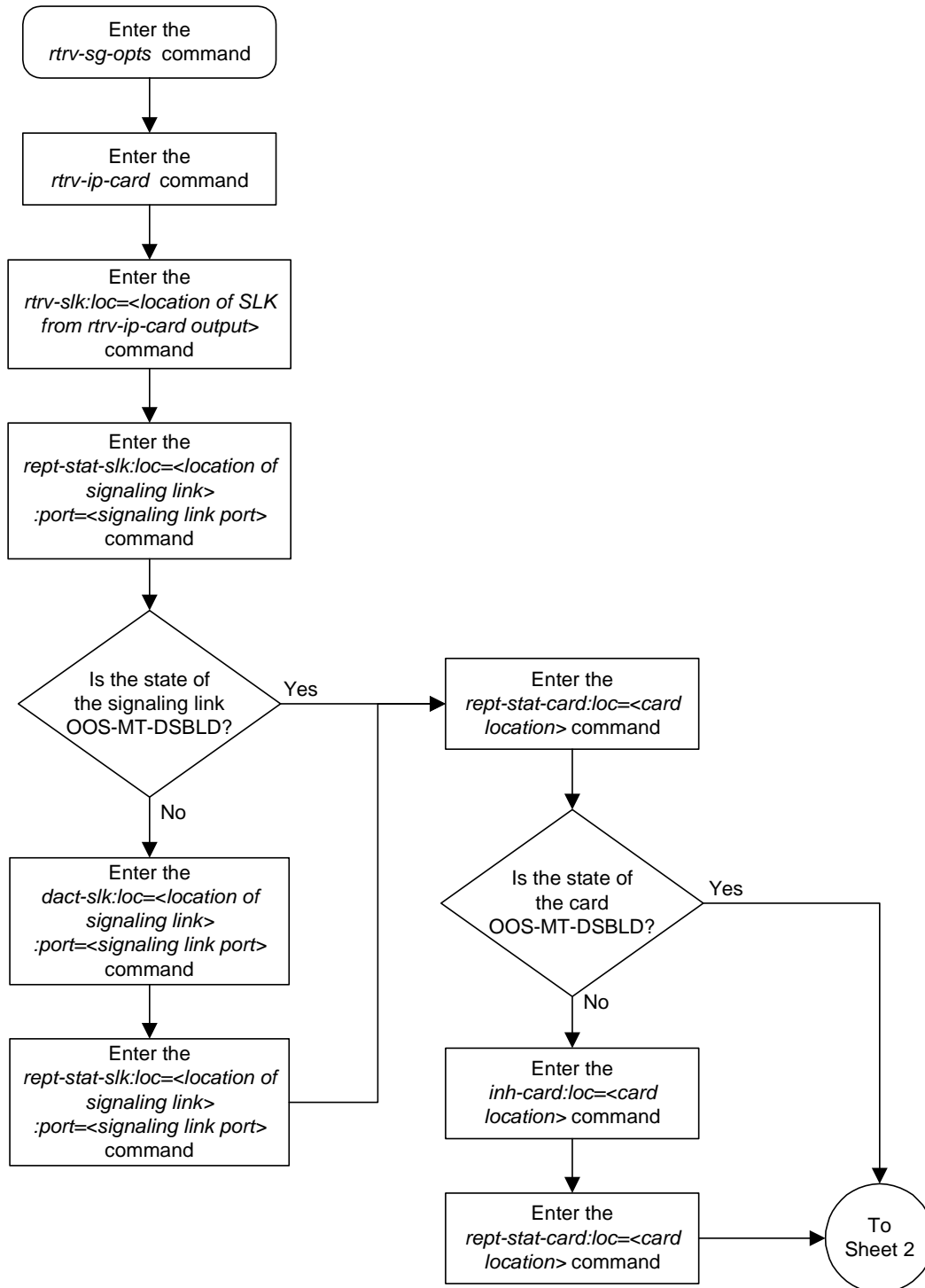
This message should appear.

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
SLK      LSN      CLLI      PST      SST      AST
1201,A   nc001     ----- IS-NR      Avail     ----
Command Completed.
```

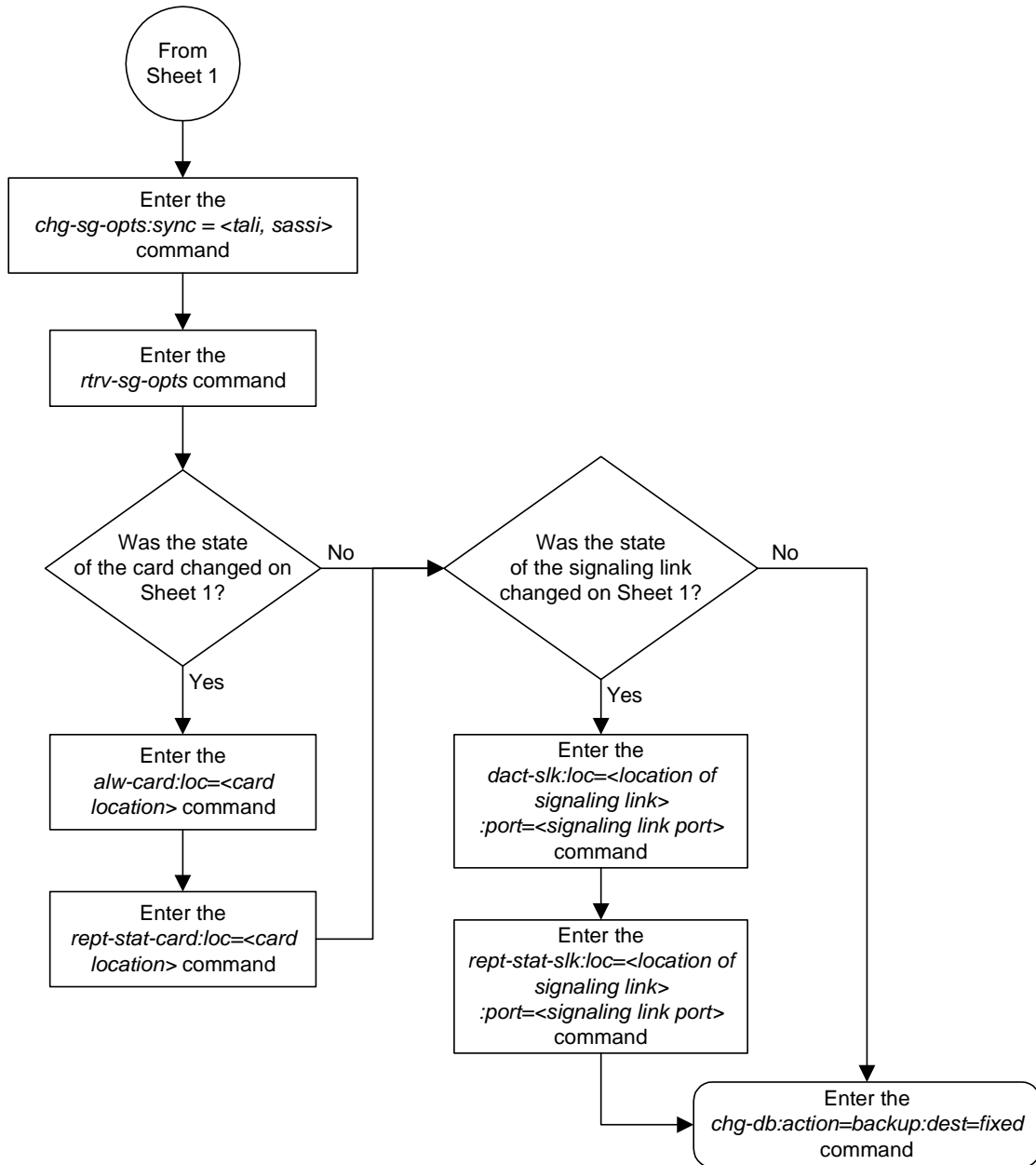
- 16.** Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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 3-4. Changing the IP Protocol Option (Sheet 1 of 2)



Flowchart 3-4. 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.

: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 (870-1671-xx or 870-1945-xx) running the **ss7ipgw** or **ipgwi** application.
- 2500 if all cards that are running the **ss7ipgw** or **ipgwi** application are SSED CM cards (870-2732-xx).

Replacing an SSED CM 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 running the **ss7ipgw** or **ipgwi** application
- 2500 if all cards that are running the **ss7ipgw** or **ipgwi** application are SSED CM 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 running the **ss7ipgw** or **ipgwi** application
- 2500 per card if all cards that are running the **ss7ipgw** or **ipgwi** application are SSED CM 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 03-06-28 21:17:37 GMT Rel 31.0.0
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
```

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 03-06-28 11:43:04 GMT Rel 31.0.0
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 03-06-28 21:18:37 GMT Rel 31.0.0  
CHG-SG-OPTS: MASP A - COMPLTD
```

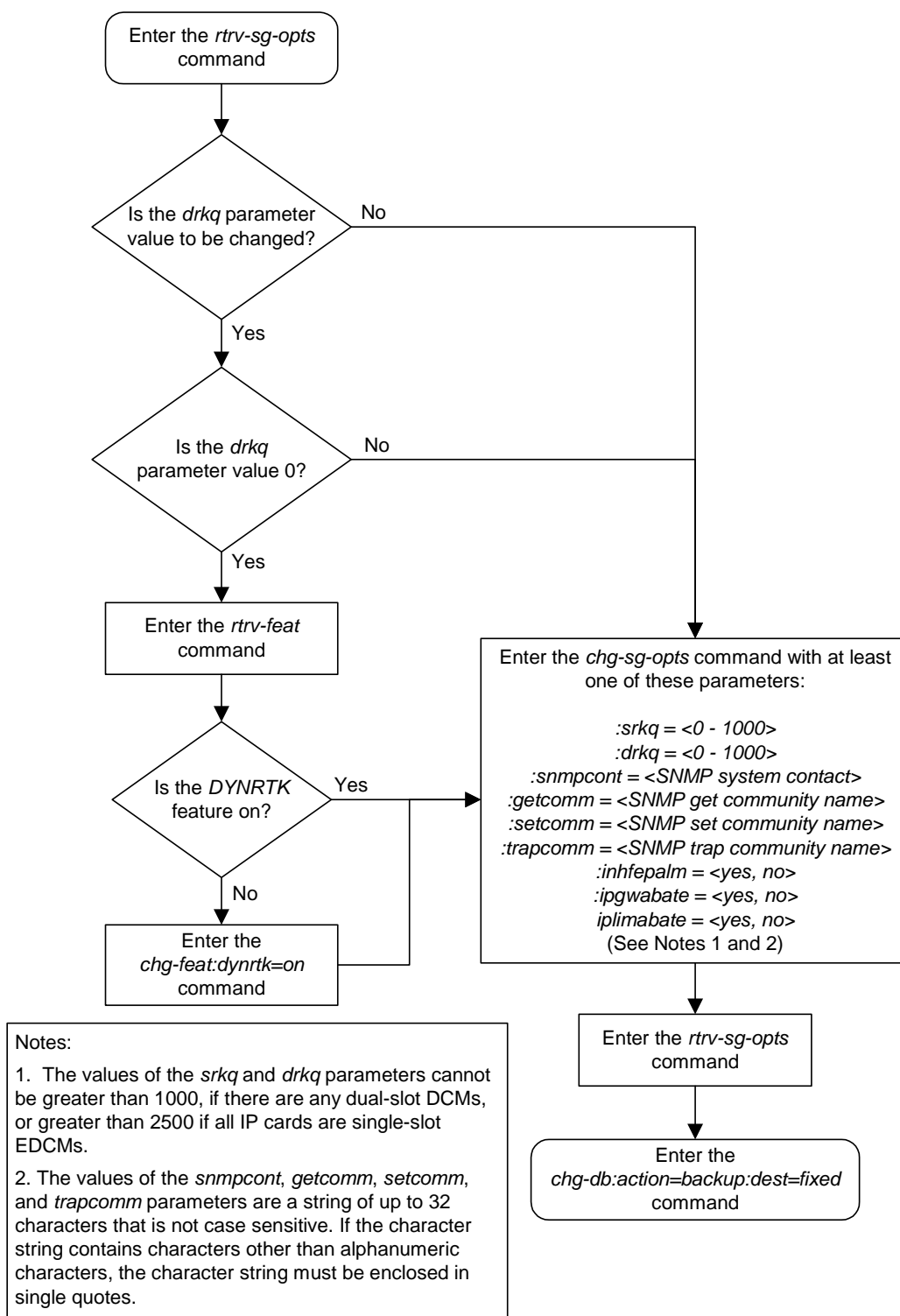
5. Verify the new IP options in the database by entering the **rtrv-sg-opts** command. The following is an example of the possible output.

```
rlghncxa03w 03-06-28 21:19:37 GMT Rel 31.0.0  
SYNC:      TALI  
SRKQ:      200  
DRKQ:      800  
SNMPCONT:  john doe 555-123-4567  
GETCOMM:   public  
SETCOMM:   private  
TRAPCOMM:  public  
INHFEPALE: NO  
SCTPCSUM:  crc32c  
IPGWABATE: NO  
IPLIMABATE: NO
```

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 3-5. 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 03-06-28 21:17:37 GMT Rel 31.0.0
```

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

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 03-06-28 21:18:37 GMT Rel 31.0.0
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.

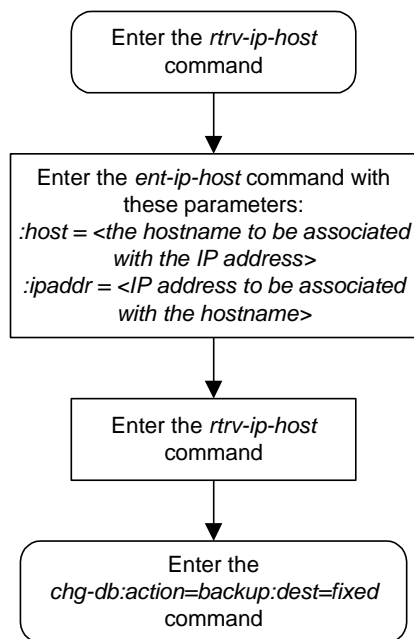
```
rlghncxa03w 03-06-28 21:19:37 GMT Rel 31.0.0
```

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

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 3-6. 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 03-06-28 21:17:37 GMT Rel 31.0.0
```

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
192.3.3.33	GW100.NC.TEKELEC.COM

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 03-06-28 21:17:37 GMT Rel 31.0.0
```

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 3-66.

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 03-06-28 21:19:37 GMT Rel 31.0.0
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.

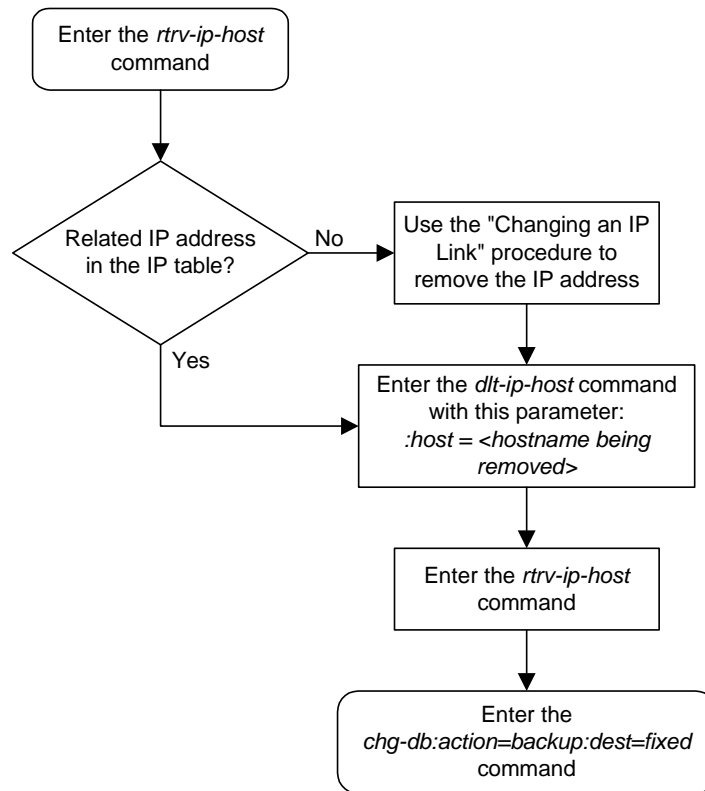
```
rlghncxa03w 03-06-28 21:20:37 GMT Rel 31.0.0
```

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

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 3-7. 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 3-8 on page 3-67 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 IP address of the IP link is being changed to a new network address, and the IP card contains a default router that is local to the current IP address of the IP link, the default router IP address must be changed to 0.0.0.0 (none) in the “Changing an IP Card” procedure on page 3-40 before the IP address of the IP link can be changed. After the IP address of the IP link has been changed, the new IP address of the default router, making sure it is local to the new IP address of the IP link, can be added in the “Changing an IP Card” procedure on page 3-40. The IP address of the default router can be verified with the **rtrv-ip-card** command.

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, **dnasa**, 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 3-8 for the valid input values for the **submask** and **ipaddr** parameter combinations.

Table 3-8. 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 3-8. 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

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 03-06-28 21:14:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0

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
```

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 3-61.

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 03-06-19 21:17:04 GMT Rel 31.0.0
LOC  PORT LSN          SLC TYPE  IPLIML2
1201  A    nc001        0  IPLIM  SAALTALI
```

4. 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 03-06-28 21:16:37 GMT Rel 31.0.0
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.

5. 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 03-06-12 09:12:36 GMT Rel 31.0.0
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 03-06-27 17:00:36 GMT Rel 31.0.0
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.
```

7. 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 03-06-27 17:00:36 GMT Rel 31.0.0
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.

8. Inhibit the IP card using the **inh-card** command. For example, enter this command.

```
inh-card:loc=1201
```

This message should appear.

```
rlghncxa03w 03-06-28 21:18:37 GMT Rel 31.0.0
Card has been inhibited.
```

9. 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 03-06-27 17:00:36 GMT Rel 31.0.0
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 if 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 03-06-28 21:17:37 GMT Rel 31.0.0
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 of the IP address of the IP link being changed, go to the “Changing an IP Card” procedure on page 3-40 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 03-06-28 21:17:37 GMT Rel 31.0.0
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 3-85 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:localhost="ipnode1-1201"
```

This is an example of the possible output.

```
rlghncxa03w 03-06-28 21:14:37 GMT Rel 31.0.0
SNAME kchlr11201
  LHOST ipnode1-1201
  LPORT 7000
  SERVER YES
  RHOST kc-hlr1
  RPORT 7000
  OPEN YES
  ALW NO
  DCMPS 1
  PORT A
  REXMIT FIXED
  RTT 60
```

If the **rtrv-appl-sock** output shows that the **open** parameter is **yes**, go to the “Changing an Application Socket” procedure on page 3-102 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 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME swbel32
  LHOST   ipnode1-1201
  ALHOST  ---
  LPORT   1030
  RHOST   gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  RPORT   2345
  OPEN    YES
  ALW     YES
  PORT    A
  ADAPTER M3UA
  VER     M3UA RFC
  RMODE   LIN
  RMIN    120
  RMAX    800
  RTIMES  10
  CWMIN   3000
  ISTRMS  2
  OSTRMS  2
```

If the **rtrv-assoc** output shows that the **open** parameter is **yes**, go to the "Changing an Association" procedure on page 6-37 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 03-06-28 21:18:37 GMT Rel 31.0.0
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 03-06-28 21:19:37 GMT Rel 31.0.0
```

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 03-06-28 21:20:37 GMT Rel 31.0.0
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 03-06-27 17:00:36 GMT Rel 31.0.0
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 03-06-07 11:11:28 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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 3-40 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 3-81 and add the IP routes back into the database.

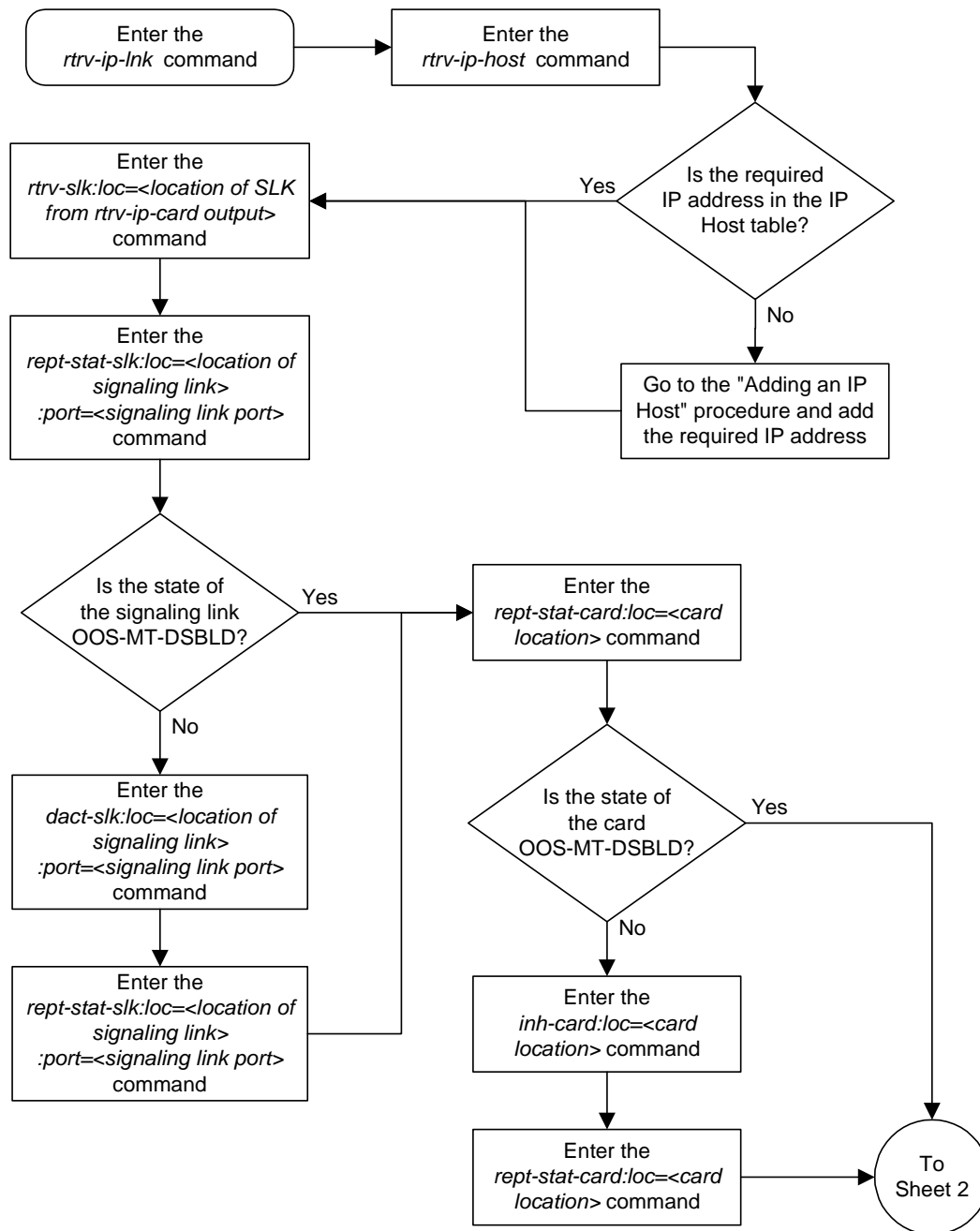
NOTE: If the `open` parameter value for either an application socket or an association was not changed in either steps 12 or 13, skip step 22, and go to step 23.

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 3-102
 - For an association – “Changing an Association” on page 6-37

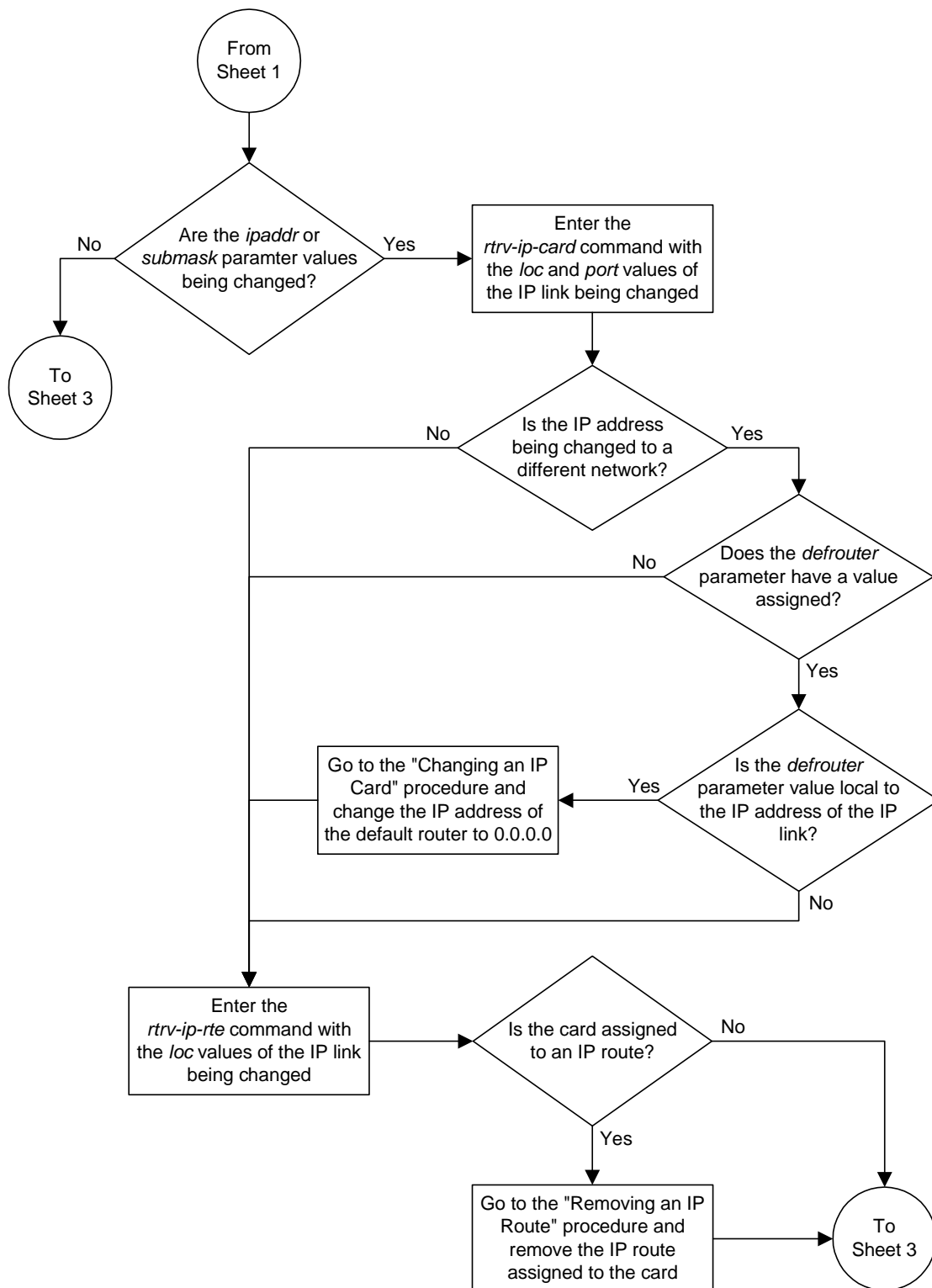
-
23. Back up the new changes using the `chg-db:action=backup:dest=fixed` command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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.
```

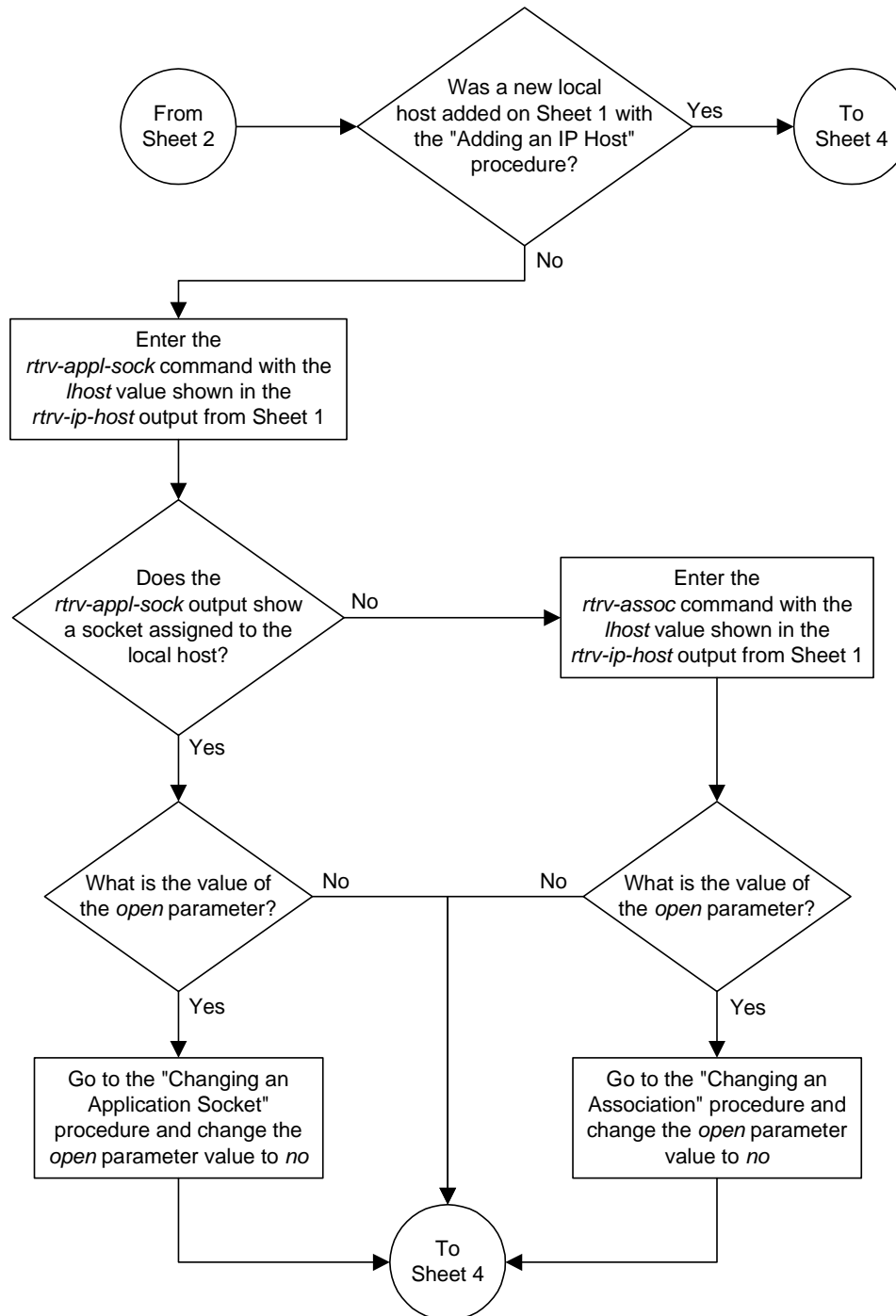
Flowchart 3-8. Changing an IP Link (Sheet 1 of 5)



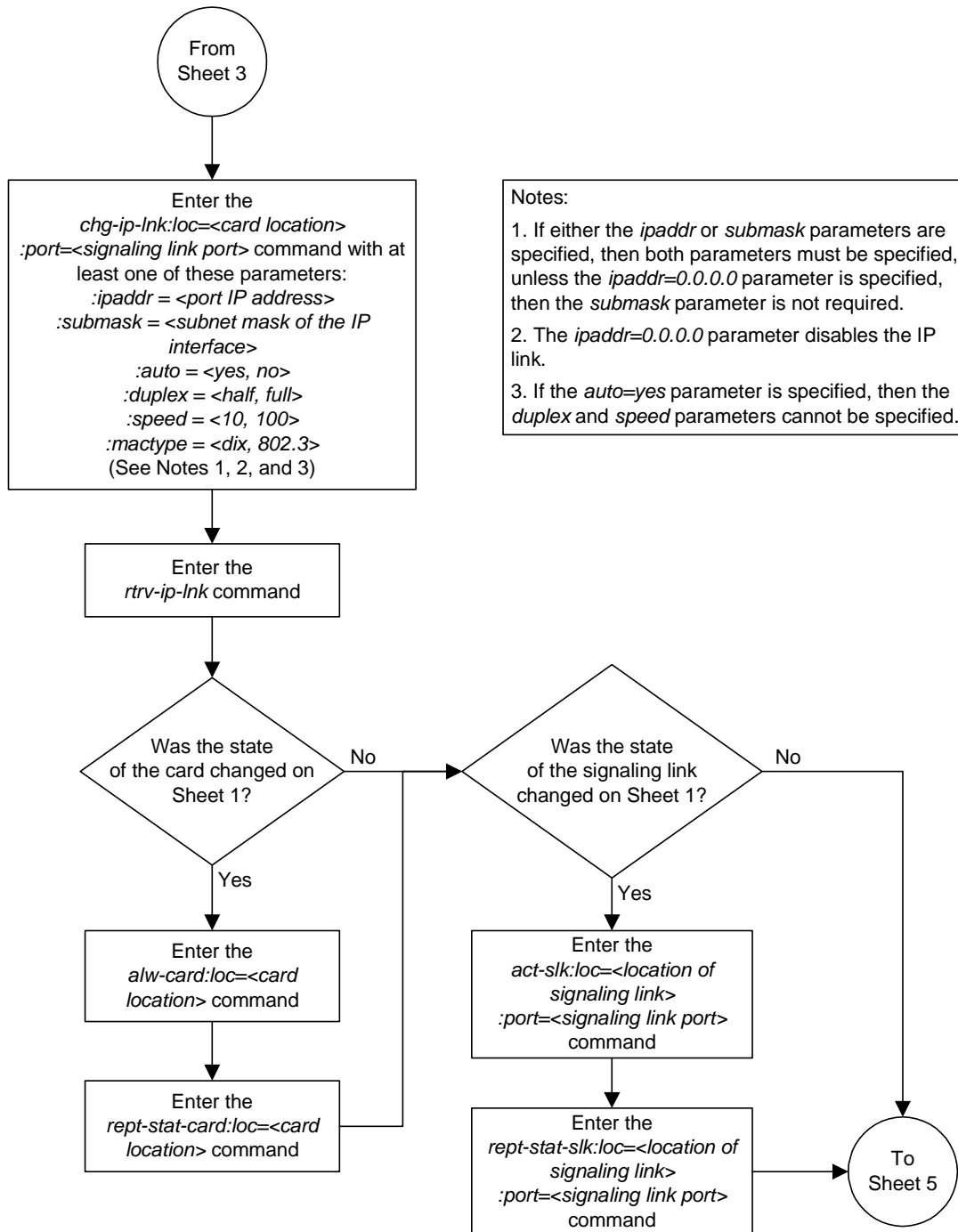
Flowchart 3-8. Changing an IP Link (Sheet 2 of 5)



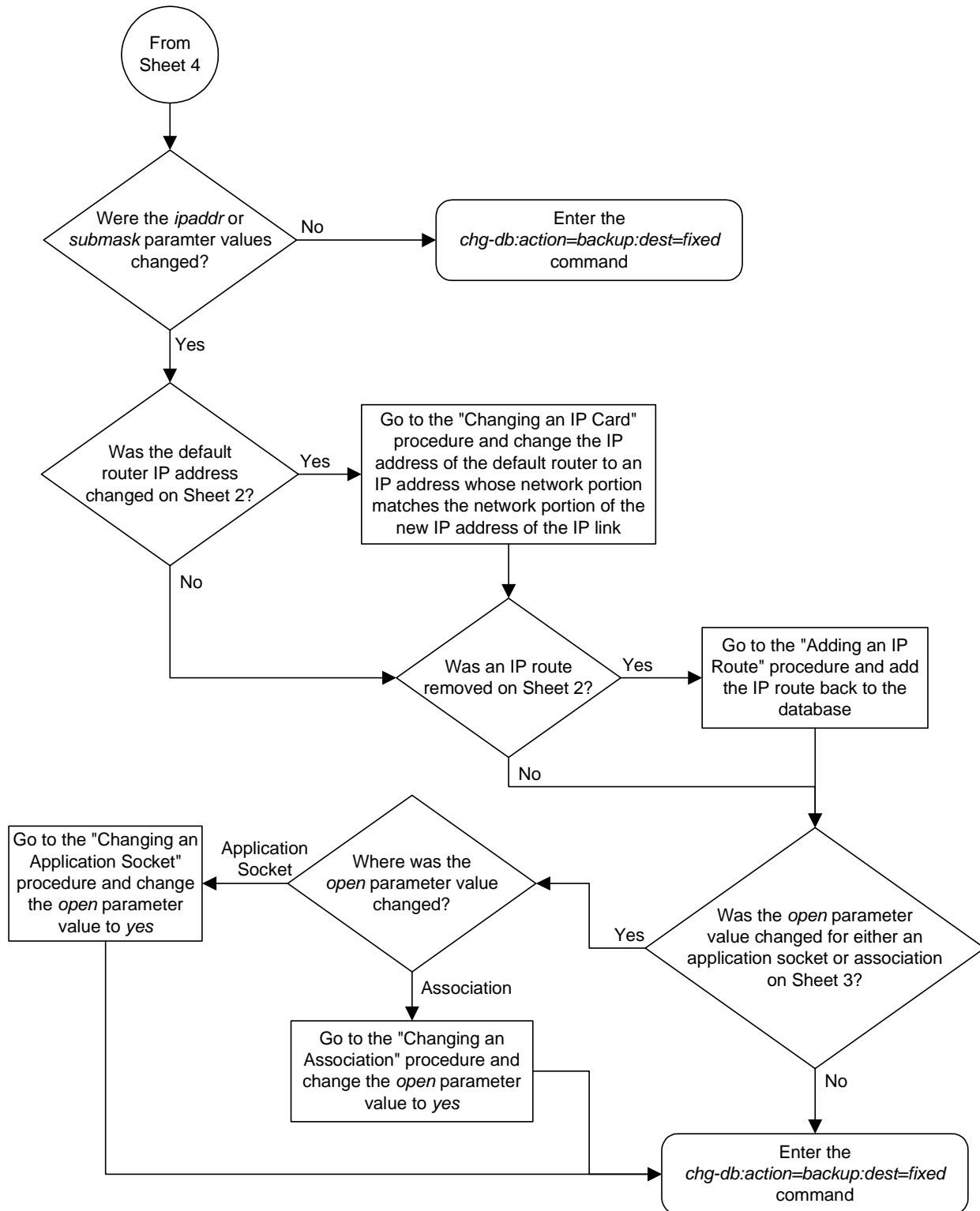
Flowchart 3-8. Changing an IP Link (Sheet 3 of 5)



Flowchart 3-8. Changing an IP Link (Sheet 4 of 5)



Flowchart 3-8. Changing an IP Link (Sheet 5 of 5)



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 3-9 for the valid input values for the **submask** and **dest** parameter combinations.

Table 3-9. 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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 21:17:37 GMT Rel 31.0.0
LOC 1212
  SRCHORDR  LOCAL
  DNSA      150.1.1.1
  DNSB      -----
  DEFROUTER 150.1.1.100
  DOMAIN    NC.TEKELEC.COM

LOC 1301
  SRCHORDR  SRVRONLY
  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
```

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 03-06-12 09:12:36 GMT Rel 31.0.0
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.

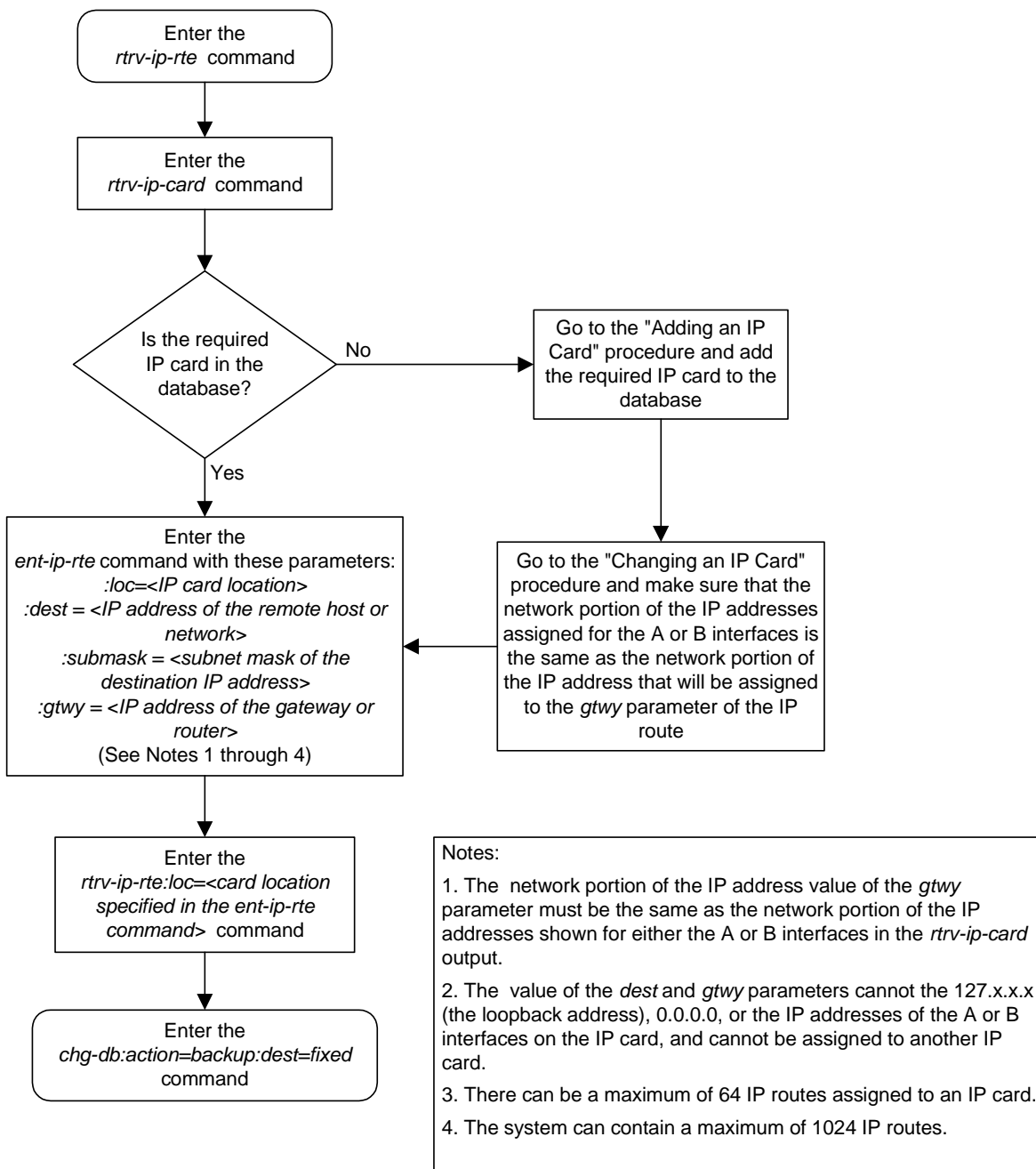
```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
LOC  DEST          SUBMASK          GTWY
1212  132.10.175.20   255.255.255.255  150.1.1.50

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 3-9. 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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-27 17:00:36 GMT Rel 31.0.0
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 03-06-12 09:12:36 GMT Rel 31.0.0
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 03-06-12 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
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
```

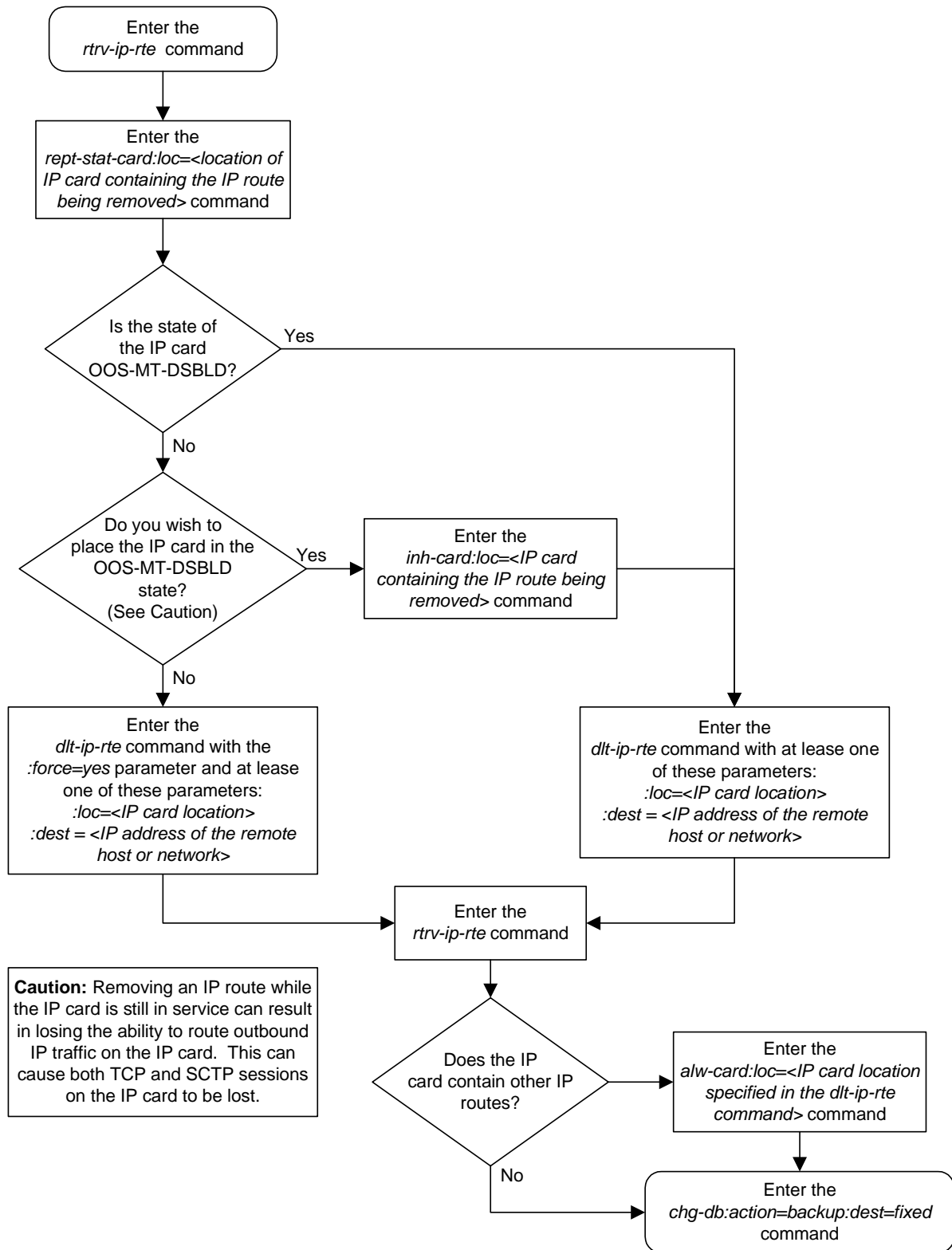
This message should appear.

```
rlghncxa03w 03-06-28 21:22:37 GMT Rel 31.0.0
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 3-10. 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 250 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:

open=no	dcmps=10
alw=no	rexmit=fixed
server=yes	rtt=60

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 3-102 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.

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 03-06-28 21:14:37 GMT Rel 31.0.0
SNAME kchlr11201
  LHOST ipnode1-1201
  LPORT 7000
  SERVER YES
  RHOST kc-hlr1
  RPORT 7000
  OPEN YES
  ALW NO
  DCMPS 1
  PORT A
  REXMIT FIXED
  RTT 60
```

2. 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 03-06-28 21:15:37 GMT Rel 31.0.0

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
```

If the required hostname is not in the database, add the IP host name using the “Adding an IP Host” on page 3-61 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 03-06-28 21:19:37 GMT Rel 31.0.0
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 3-66 procedure.

4. 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 03-06-27 17:00:36 GMT Rel 31.0.0
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 03-06-19 21:17:04 GMT Rel 31.0.0
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 SS7 Signaling Link" procedure in the *Database Administration Manual - SS7*. Add the signaling link back into the database with the **ipliml2=saaltali** parameter, and without activating the signaling link, using the "Adding an SS7 Signaling Link" procedure in the *Database Administration Manual - SS7*.

NOTE: If the “Adding an SS7 Signaling Link” procedure in the *Database Administration Manual - SS7* 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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-07 11:11:28 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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=kchlrl1203:lhost="ipnode-1203"
:lport=7005:rhost="kc-hlr1":rport=7005:port=a
```

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

```
rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
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=kchlrl1203:open=yes:alw=yes
```

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

```
rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
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 03-06-07 11:11:28 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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

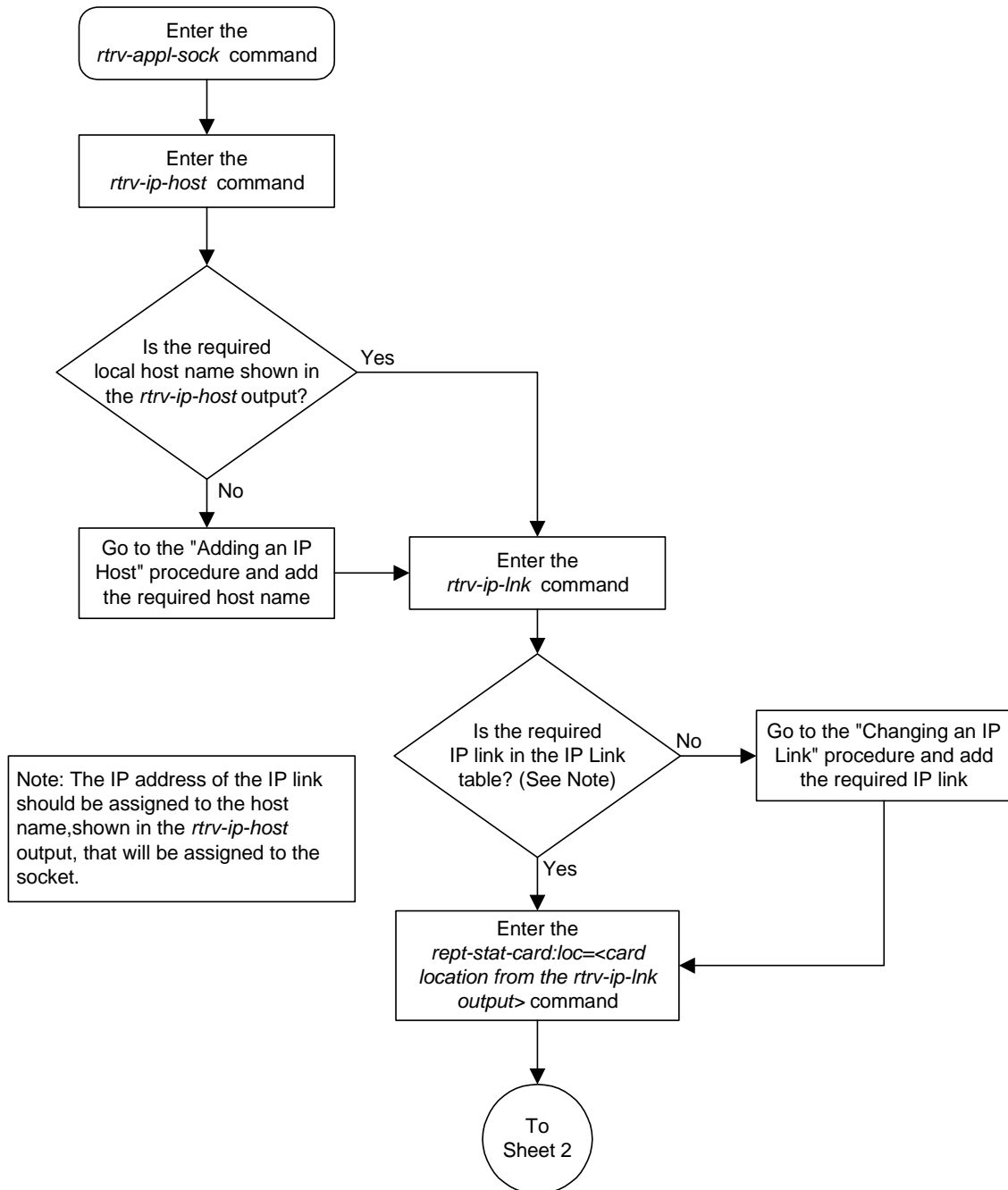
The following is an example of the possible output.

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
SNAME kchlr11203
  LHOST ipnode1-1203
  LPORT 7005
  SERVER YES
  RHOST kc-hlr1
  RPORT 7005
  OPEN YES
  ALW YES
  DCMPS 10
  PORT A
  REXMIT FIXED
  RTT 60
```

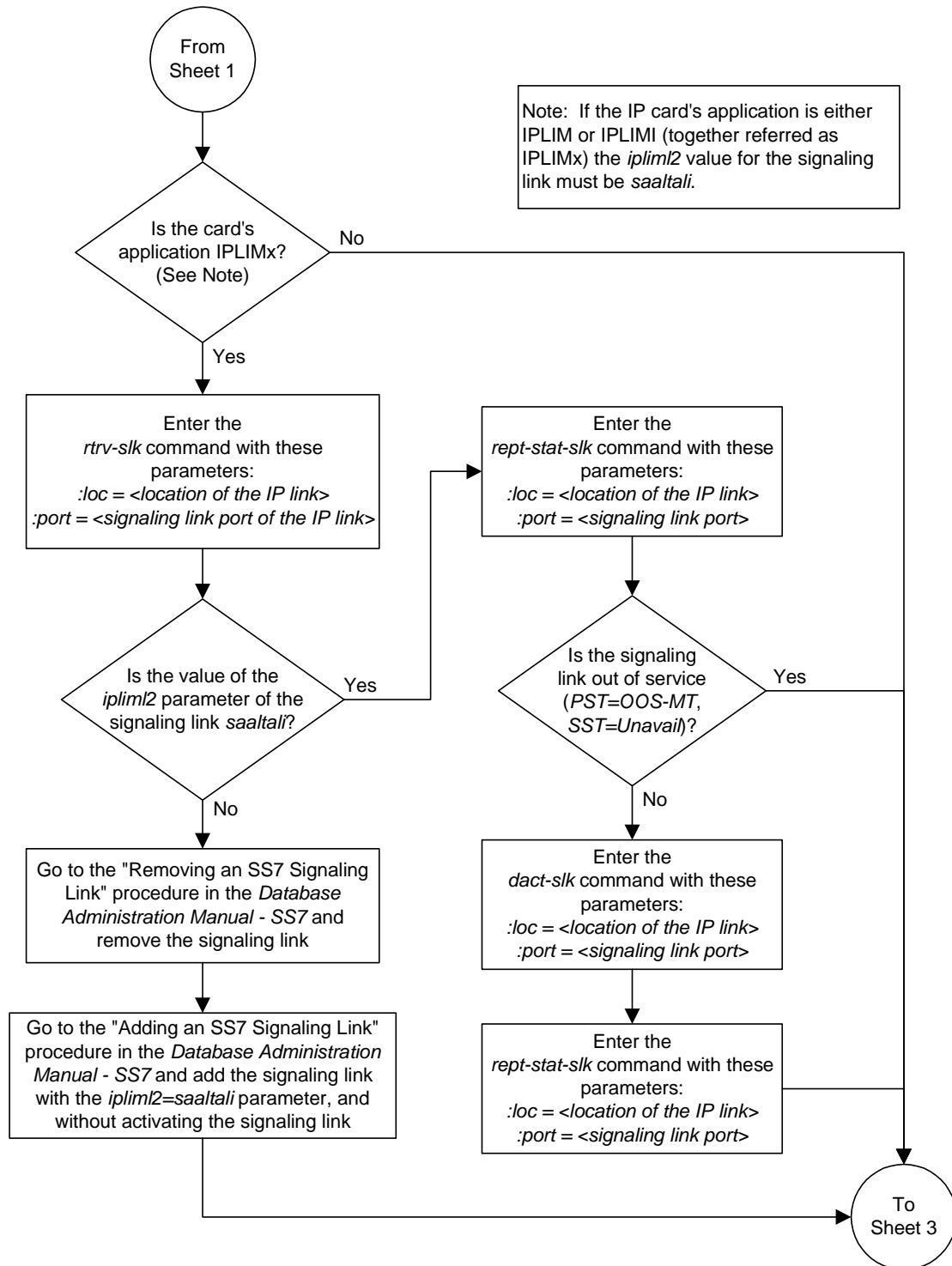
14. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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.
```

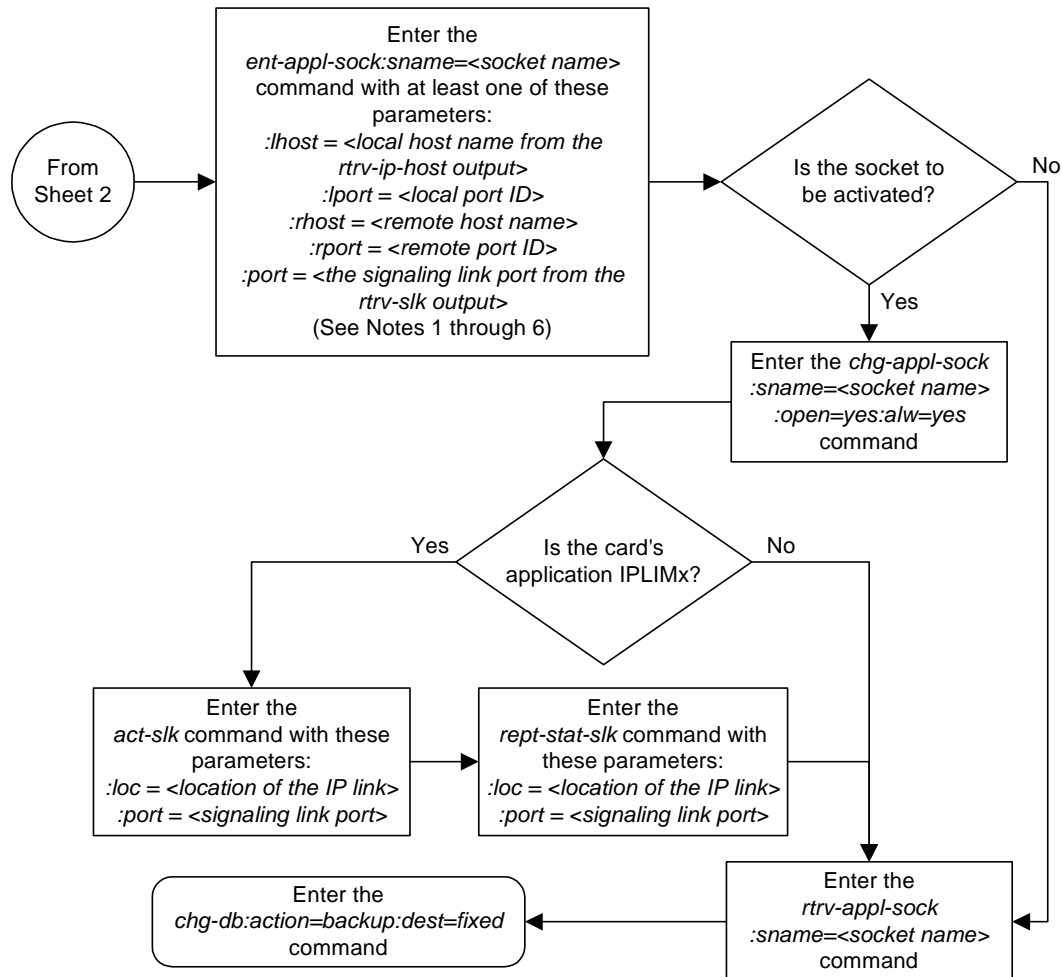
Flowchart 3-11. Adding an Application Socket (Sheet 1 of 3)



Flowchart 3-11. Adding an Application Socket (Sheet 2 of 3)



Flowchart 3-11. 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 250 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.

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 03-06-28 21:15:37 GMT Rel 31.0.0
SNAME kchlr11201
  LHOST  ipnode1-1201
  LPORT  7000
  SERVER YES
  RHOST  kc-hlr1
  RPORT  7000
  OPEN   YES
  ALW    NO
  DCMPS  1
  PORT   A
  REXMIT FIXED
  RTT    60

SNAME kchlr11203
  LHOST  ipnode1-1203
  LPORT  7005
  SERVER YES
  RHOST  kc-hlr1
  RPORT  7005
  OPEN   NO
  ALW    NO
  DCMPS  10
  PORT   A
  REXMIT FIXED
  RTT    60
```

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-appl-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-appl-sock:sname=kchlr11201:open=no
```

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

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
CHG-APPL-SOCK: MASP A - COMPLTD
```

3. Remove the application socket information from the database by entering the **dlr-appl-sock** command. For example, enter this command.

```
dlr-appl-sock:sname=kchlr11201
```

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

```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
DLT-APPL-SOCK: MASP A - COMPLTD
```

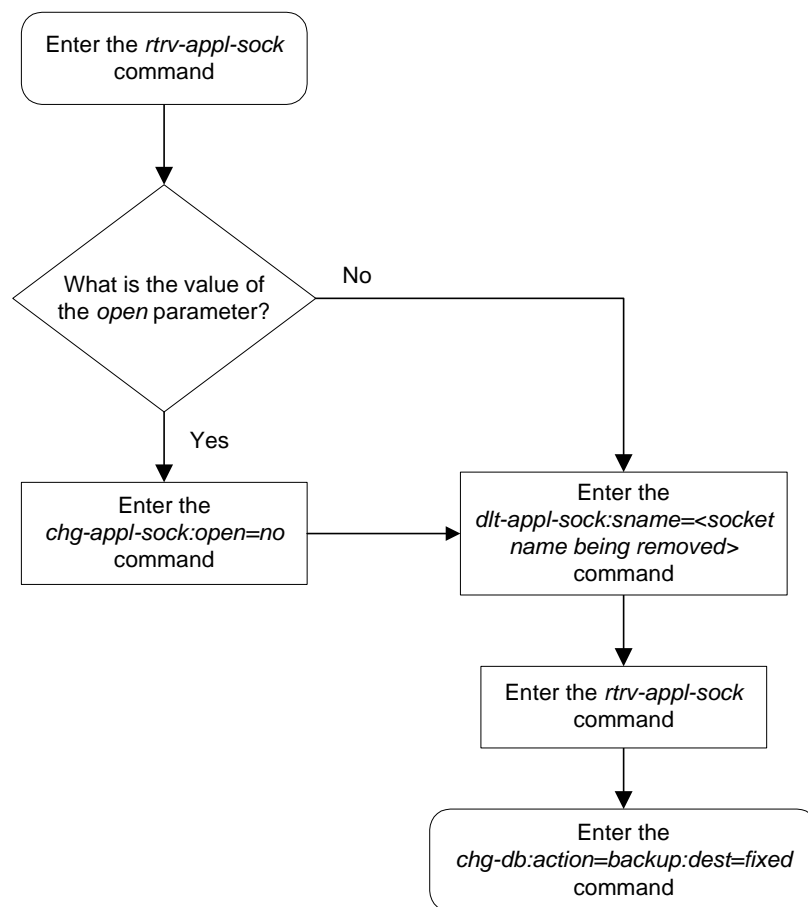
4. Verify the new application socket information in the database by entering the **rtrv-appl-sock** command. The following is an example of the possible output.

```
rlghncxa03w 03-06-28 21:18:37 GMT Rel 31.0.0
SNAME kchlr11203
  LHOST ipnode1-1203
  LPORT 7005
  SERVER YES
  RHOST kc-hlr1
  RPORT 7005
  OPEN NO
  ALW NO
  DCMPS 10
  PORT A
  REXMIT FIXED
  RTT 60
```

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 3-12. 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.
- :rexmit** – 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 **rexmit** and **rtt** parameters, go to the "Configuring IP Socket Retransmission Parameters" procedure on page 3-114.

The **open** parameter must be set to **no** before changes can be made to **server**, **lhost**, **lport**, **rhost**, **rport**, **rtt**, **rexmit**, 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 250 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.

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 03-06-28 21:15:37 GMT Rel 31.0.0
SNAME kchlr11201
  LHOST ipnode1-1201
  LPORT 7000
  SERVER YES
  RHOST kc-hlr1
  RPORT 7000
  OPEN YES
  ALW NO
  DCMPS 1
  PORT A
  REXMIT FIXED
  RTT 60

SNAME kchlr11203
  LHOST ipnode1-1203
  LPORT 7005
  SERVER YES
  RHOST kc-hlr1
  RPORT 7005
  OPEN YES
  ALW YES
  DCMPS 10
  PORT A
  REXMIT FIXED
  RTT 60
```

NOTE: To change the values of these parameters: **server**, **lhost**, **lport**, **rhost**, **port**, **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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
```

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

If the required hostname is not in the database, add the IP host name using the “Adding an IP Host” on page 3-61 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 03-06-28 21:19:37 GMT Rel 31.0.0
```

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 3-66 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 03-06-27 17:00:36 GMT Rel 31.0.0
```

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 03-06-19 21:17:04 GMT Rel 31.0.0
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 SS7 Signaling Link" procedure in the *Database Administration Manual - SS7*. Add the signaling link back into the database with the **ipliml2=saaltali** parameter, and without activating the signaling link, using the "Adding an SS7 Signaling Link" procedure in the *Database Administration Manual - SS7*.

NOTE: If the "Adding an SS7 Signaling Link" procedure in the *Database Administration Manual - SS7* 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 03-06-28 21:16:37 GMT Rel 31.0.0
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 **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 03-06-07 11:11:28 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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=kchlrl1201:rhost="kc-kc-kc":alw=yes
```

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

```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
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=kchlrl1201:open=yes
```

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

```
rlghncxa03w 03-06-28 21:18:37 GMT Rel 31.0.0
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 03-06-07 11:11:28 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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
```

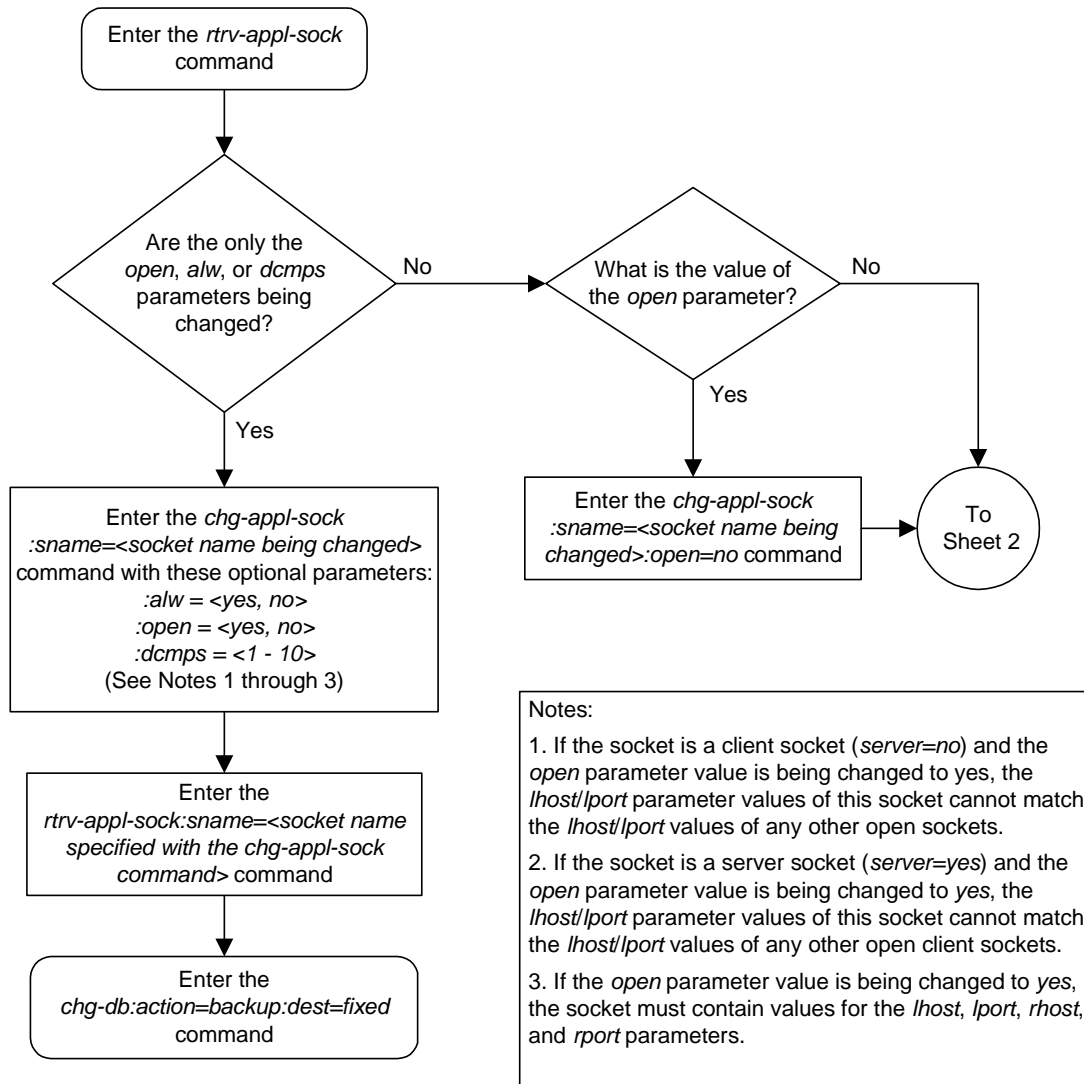
The following is an example of the possible output.

```
rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
SNAME kchlr11201
      LHOST ipnode1-1201
      LPORT 7000
      SERVER YES
      RHOST kc-kc-kc
      RPORT 7000
      OPEN  YES
      ALW   YES
      DCMPS 1
      PORT  A
      REXMIT FIXED
      RTT   60
```

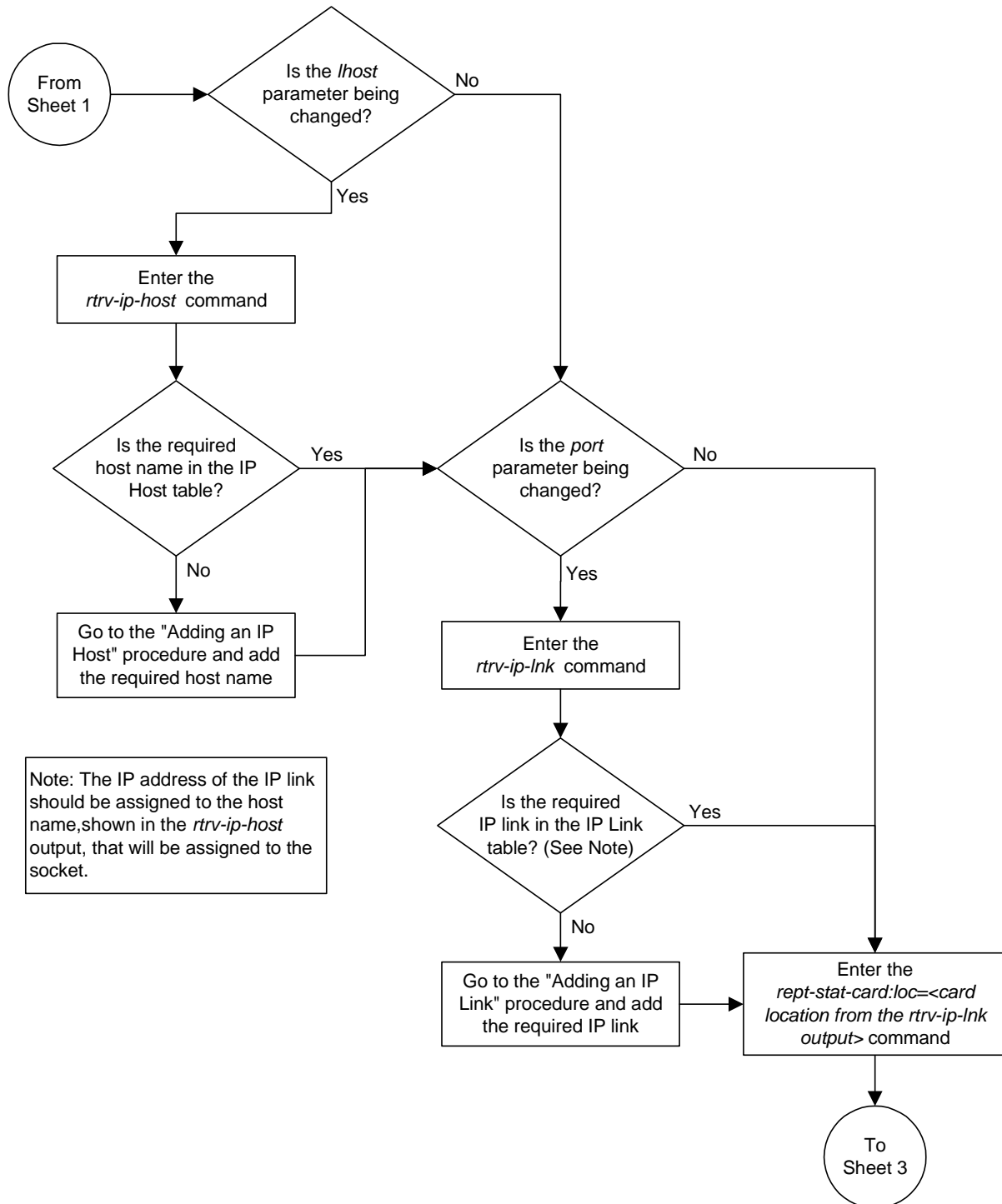
15. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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.
```

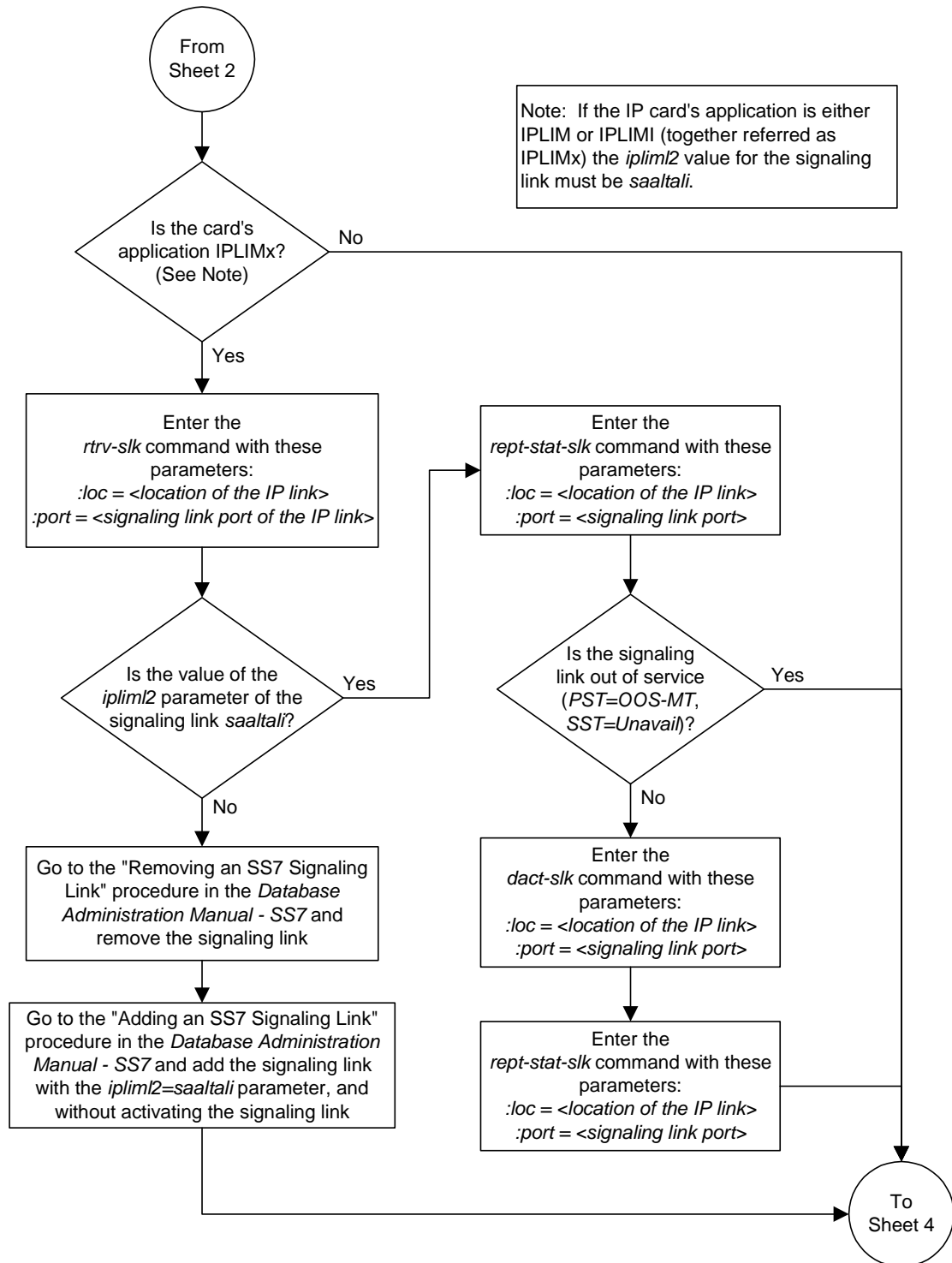
Flowchart 3-13. Changing an Application Socket (Sheet 1 of 5)



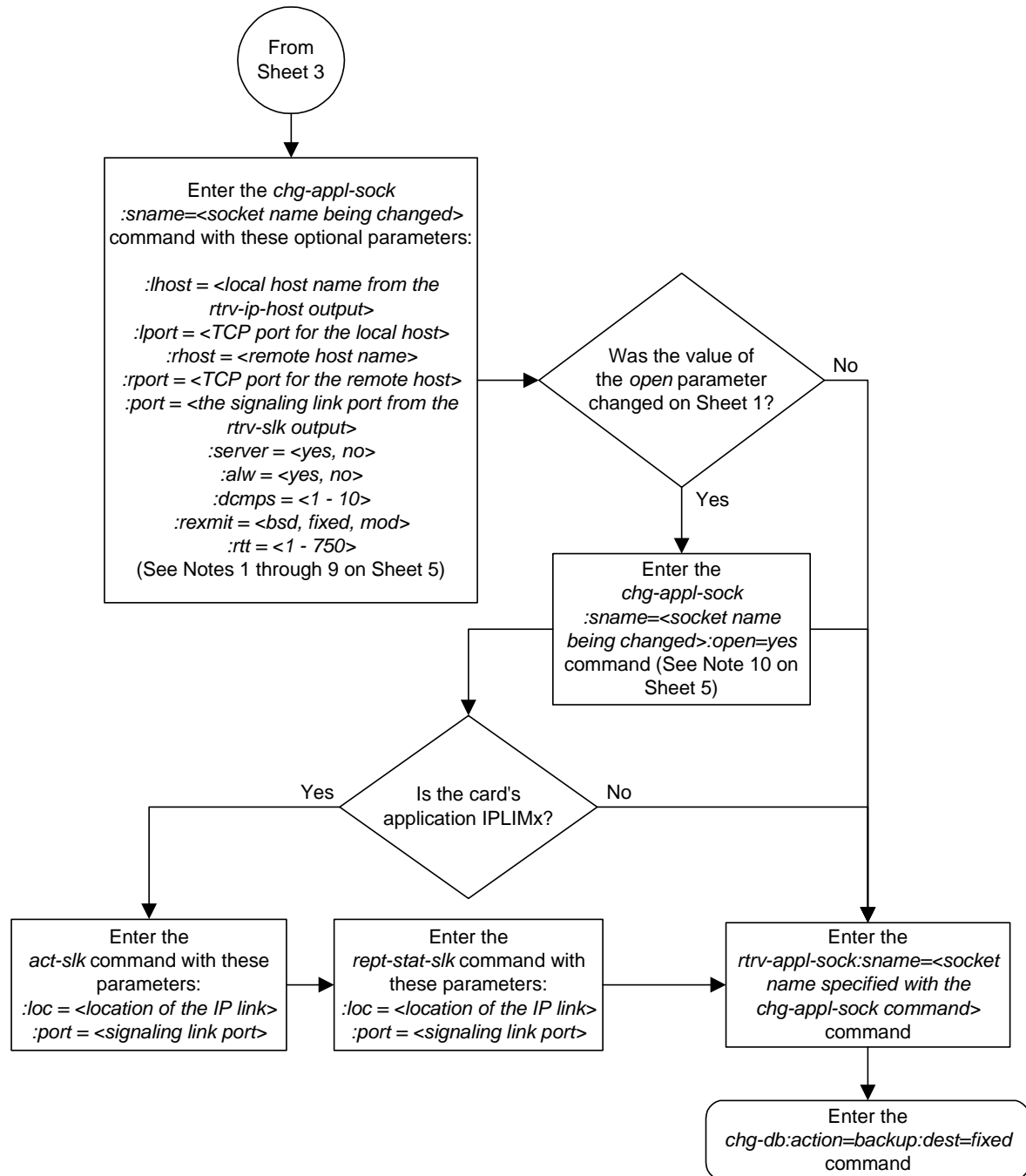
Flowchart 3-13. Changing an Application Socket (Sheet 2 of 5)



Flowchart 3-13. Changing an Application Socket (Sheet 3 of 5)



Flowchart 3-13. Changing an Application Socket (Sheet 4 of 5)



Flowchart 3-13. 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 250 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 **rexmit** and **rtt** parameters of the **chg-appl-sock** command.

:rexmit – 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 3-102 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 **rexmit** and **rtt** parameter values are set using the data collected from the **pass** commands.

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.

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 03-06-28 21:15:37 GMT Rel 31.0.0
SNAME kchlr11201
  LHOST ipnode1-1201
  LPORT 7000
  SERVER YES
  RHOST kc-hlr1
  RPORT 7000
  OPEN YES
  ALW NO
  DCMPS 1
  PORT A
  REXMIT FIXED
  RTT 60

SNAME kchlr11203
  LHOST ipnode1-1203
  LPORT 7005
  SERVER YES
  RHOST kc-hlr1
  RPORT 7005
  OPEN YES
  ALW YES
  DCMPS 10
  PORT A
  REXMIT FIXED
  RTT 60
```

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 03-06-28 21:15:37 GMT Rel 31.0.0

IPADDR      HOST
192.1.1.30   kc-hlr1
```

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 03-06-28 21:19:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
PASS: Command sent to card

rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
PING command in progress

rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
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 3-102 and change the retransmission parameters (**rtt** and **reemit**) 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 03-06-28 21:15:37 GMT Rel 31.0.0
PASS: Command sent to card

rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0

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 03-06-28 21:15:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
PASS: Command sent to card

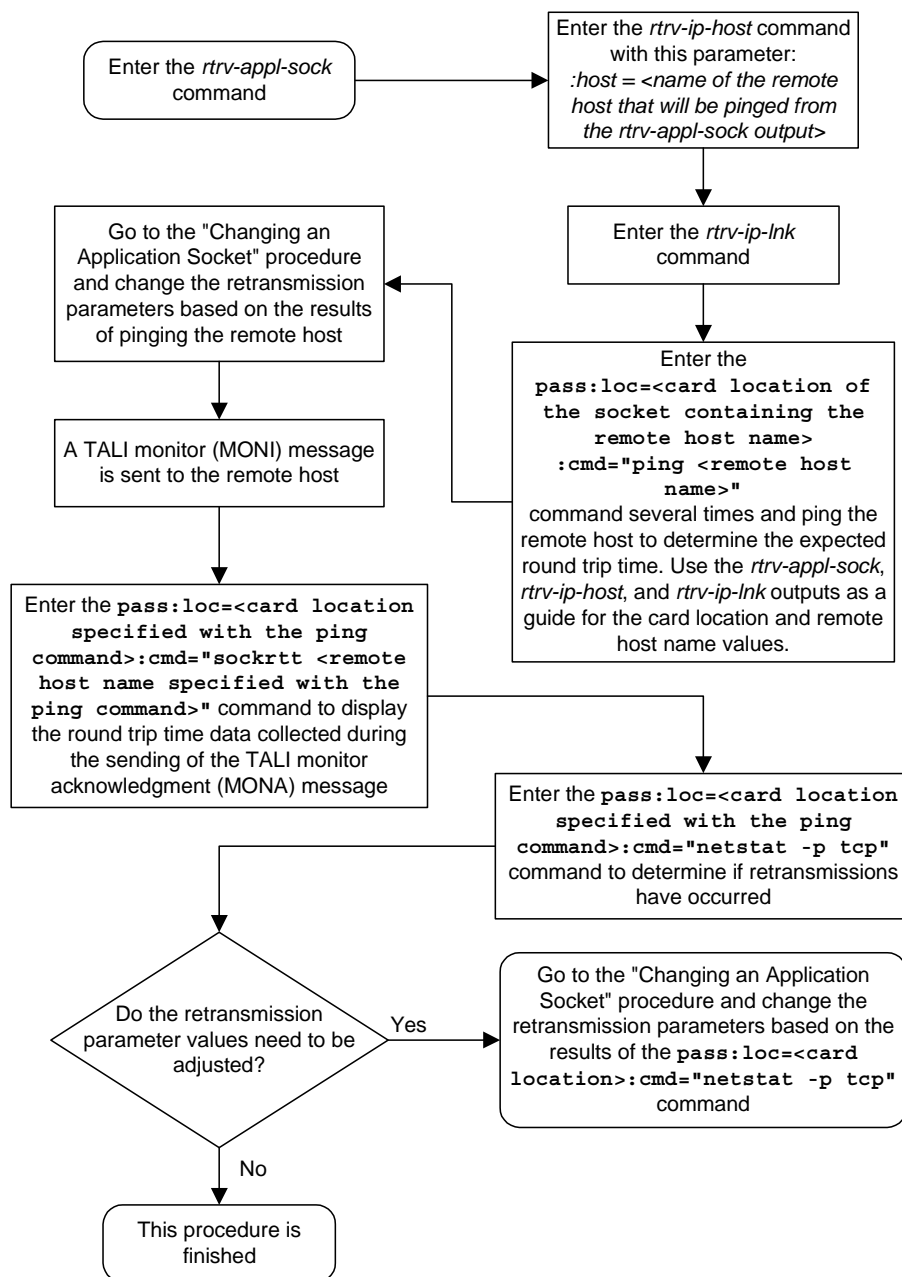
rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
TCP:
    0 packet sent
        0 data packet (0 byte)
        0 data packet (0 byte) retransmitted
        0 ack-only packet (0 delayed)
        0 URG only packet
        0 window probe packet
        0 window update packet
        0 control packet
    0 packet 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 03-06-28 21:15:37 GMT Rel 31.0.0
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 3-102 and adjust the retransmission parameter (`rtt` and `rexmit`) values of the socket based on the results of the `pass:cmd="netstat -p tcp"` command entered in step 8.

Flowchart 3-14. 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 3-10 shows the decimal equivalent for the bit values shown in the **rtrv-dcmps** output.

Table 3-10. 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.

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 03-06-28 21:15:37 GMT Rel 31.0.0
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
      0=Broadcast Phase MTPP Primitives;
      1=Response Method MTPP Primitives;
      2=SCCP with MTP;
      3=ISUP via MTP;
      4=Group Code in MTPP;
      5=Use XSRV;
      6-31=Reserved
      BIT VALUE
      0=Disabled , 1=Enabled
      0=Disabled , 1=Enabled
      0=Disabled , 1=Enabled
      0=Disabled , 1=Enabled
      0=Disabled , 1=Enabled
      0=Disabled , 1=Enabled
      0=Disabled , 1=Enabled
```

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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
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

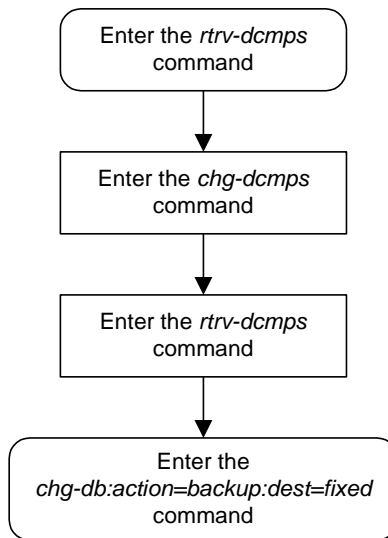
PARM 3: Default SORP Flags socket option. Each bit is used as an
enabled/disabled flag for a particular socket option.
PVALUE : Valid range = 32-bits

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 3-15. Changing an DCM Parameter Set



Adding a Static Application Routing Key

This procedure is used for the **ss7ipgw** and **ipgwi** applications to add a static application routing key to the database using the **ent-appl-rtkey** command. A routing key entry associates a routing key with a socket name or an application server (AS) name. 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 – Destination point code. The 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. 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 3-11 shows the text strings that can be used in place of numbers for the service indicator values.

Table 3-11. 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. 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.

:opc/opca/opci/opcn/opcn24 - The originating point code. 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.

:cics - Starting circuit identification code. 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 - Ending circuit identification code. 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 - 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 3-12 on page 3-126). If **type** is not explicitly specified, **type = full** is assumed.

:asname - Application server (AS) name.

Application socket names are shown in the **rtrv-appl-sock** output. Application server names are shown in the **rtrv-as** output.

A routing key can be associated with up to 16 socket names or 1 application server name. 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 AS 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 3-151.

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 3-12.

Table 3-12. Routing Key Parameter Combinations for Adding Routing Keys

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 ¹⁰	dpc ^{1, 2}	sname ¹⁰	dpc ^{1, 2}	sname ¹⁰	sname ¹⁰
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 ¹⁰	dpc ^{1, 2, 3}	asname ¹⁰
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 ¹⁰	asname ¹⁰	cice ^{5, 6, 7, 8, 9}	opc ^{1, 2, 3}	asname ¹⁰	asname ¹⁰	
asname ¹⁰		type=full	asname ¹⁰			
		sname ¹⁰				
		asname ¹⁰				

Table 3-12. Routing Key Parameter Combinations for Adding Routing Keys (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>Notes:</p> <p>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 si parameter is 4, the point codes must be either an ITU-I, 14-bit ITU-N, or 24-bit ITU-N point code. 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.</p> <p>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.</p> <p>3. These parameters are optional for partial routing keys, but at least one these parameters must be specified with the ent-appl-rtkey command.</p> <p>4. Text strings can be used in place of some numerical service indicator values. See Table 3-11 on page 3-124 for a list of these text strings.</p> <p>5. When the service indicator parameter value equals 4 and an ANSI dpc is specified, the opc, cics, and cice parameters cannot be used. If the service indicator parameter value equals 4 and an ITU dpc is specified, the opc, cics, and cice parameters are required.</p> <p>6. If the service indicator parameter (si) value is 4, the values of the cics and cice parameters is from 0 to 4095.</p> <p>7. If the service indicator parameter (si) 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 cics and cice parameters is from 0 to 4095. If the point code in the routing key is an ANSI point code, the values of the cics and cice parameters is from 0 to 16383.</p> <p>8. If the service indicator parameter value is 13, the values of the cics and cice parameters is from 0 to 4294967295.</p> <p>9. The CIC range, defined by the cics and cice parameters, cannot overlap the CIC range in an existing routing key.</p> <p>10. The sname or asname parameters must be specified, but not both.</p>						

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 03-06-28 21:15:37 GMT Rel 31.0.0

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
```

NOTE: If an application server (**asname**) is being assigned to the routing key instead of a socket, skip this step and go to step 3.

2. 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 03-06-28 21:15:37 GMT Rel 31.0.0
SNAME kchlr11201
  LHOST ipnode1-1201
  LPORT 7000
  SERVER YES
  RHOST kc-hlr1
  RPORT 7000
  OPEN YES
  ALW NO
  DCMPS 1
  PORT A
  REXMIT FIXED
  RTT 60

SNAME kchlr11203
  LHOST ipnode1-1203
  LPORT 7005
  SERVER YES
  RHOST kc-hlr1
  RPORT 7005
  OPEN YES
  ALW YES
  DCMPS 10
  PORT A
  REXMIT FIXED
  RTT 60
```

If the required socket is not in the database, go to the “Adding an Application Socket” procedure on page 3-89 to add the socket.

NOTE: If a socket (**sname**) is being assigned to the routing key instead of an application server, skip this step and go to step 4.

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 03-06-28 09:12:36 GMT Rel 31.0.0
      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 required application server is not in the database, go to the “Adding an Application Server” procedure on page 6-85 to add the application server.

NOTE: If a default routing key is being added to the database, skip steps 3 and 4, and go to step 5.

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 03-06-28 11:43:04 GMT Rel 31.0.0
CHG-FEAT: MASP A - COMPLTD
```

6. Add a static 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 3-12 on page 3-126 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.

For this example, a full ISUP routing key is being added to the database. Enter this command.

```
ent-appl-rtkey:dpca=123-234-123: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 03-06-28 21:15:37 GMT Rel 31.0.0
ENT-APPL-RTKEY: MASP A - COMPLTD
```

7. Verify the new application routing key information in the database by entering the **rtrv-appl-rtkey** command with the socket name (**sname**) or application server name (**asname**) 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 03-06-28 21:16:37 GMT Rel 31.0.0

KEY:LOC      DPC          SI SSN OPCA          CICS          CICE
  STATIC 123-234-123  5 --- 100-100-100 1          50
      ATTR:PSTNCAT PSTNID NORM DUP
              0          0 N    -
      SNAME:socket5

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 (3 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
```

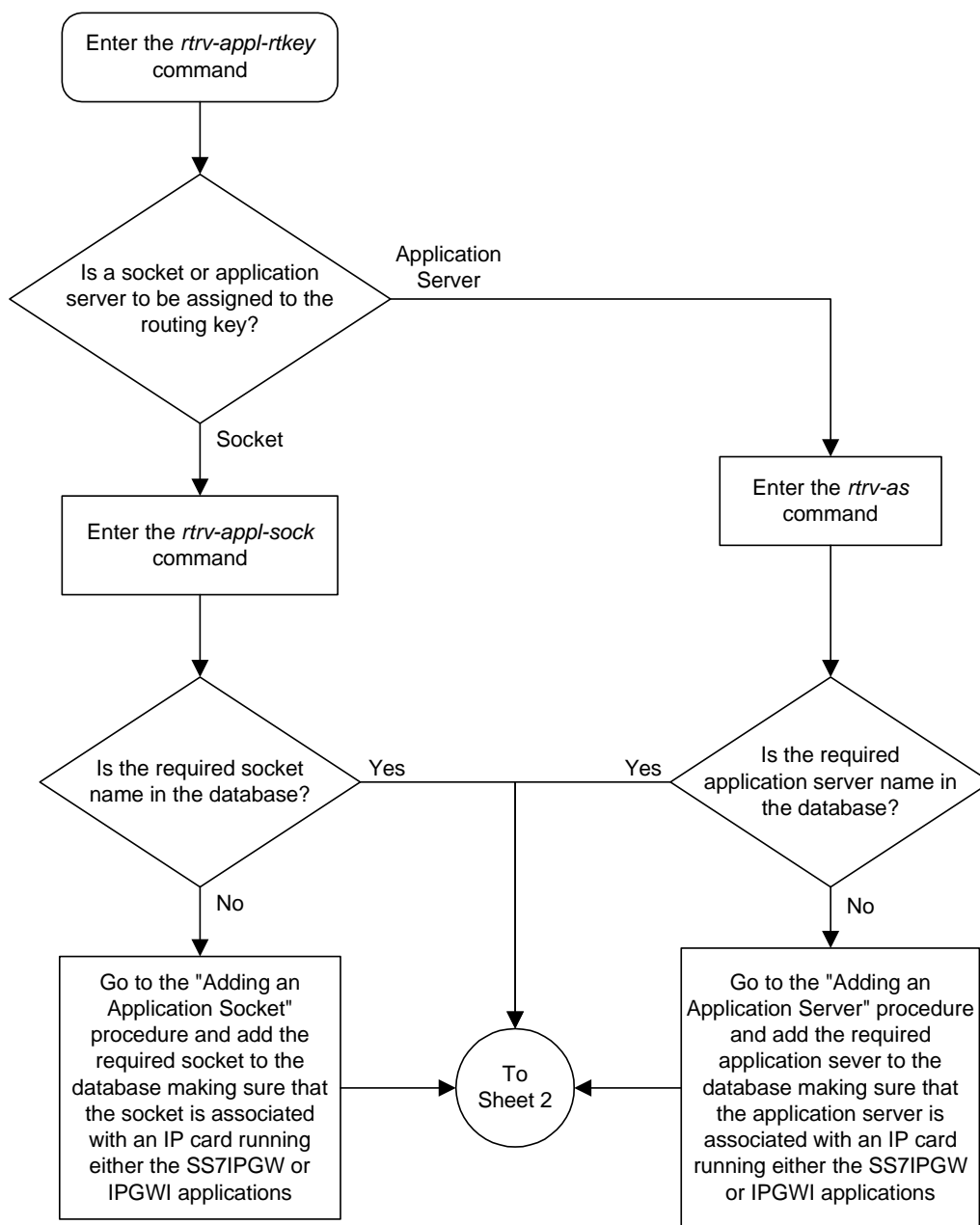
8. If you wish to change the PSTN presentation information in the routing key that was added in step 6, go to the “Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key” procedure on page 3-151.
-

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.

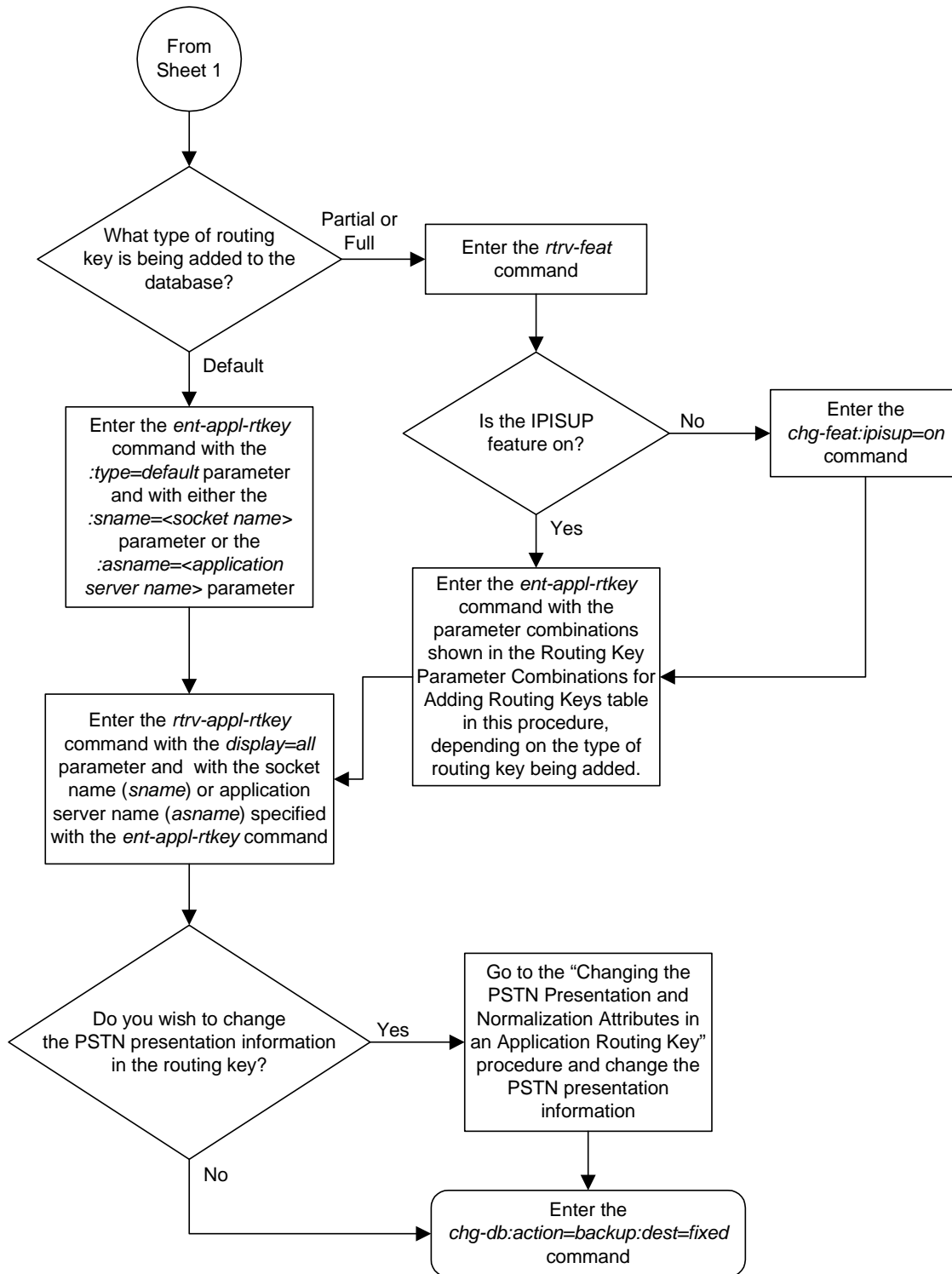
```

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 3-16. Adding an Application Routing Key (Sheet 1 of 2)



Flowchart 3-16. Adding an Application Routing Key (Sheet 2 of 2)



Removing an Application Routing Key

This procedure is used for the **ss7ipgw** and **ipgwi** applications to remove a static or dynamic application routing key from the database using the **dlt-appl-rtkey** command. For more information about static and dynamic routing keys, see “Understanding Routing for SS7IPGW and IPGWI Applications” on page 2-23.

The **dlt-appl-rtkey** command uses these parameters.

:dpc/dpca/dpci/dpcn/dpca24 – Destination point code. The 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. The service indicator value that is used to filter incoming MSUs.

:ssn – The subsystem number. 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.

: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.

:cics – Starting circuit identification code. 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 – Ending circuit identification code. 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** - Key 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-appl-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 3-13.

Table 3-13. Routing Key Parameter Combinations for Removing Routing Keys

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 ¹⁰	dpc ^{1, 2}	sname ¹⁰	dpc ^{1, 2}	sname ¹⁰	sname ¹⁰
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 ¹⁰	dpc ^{1, 2, 3}	asname ¹⁰
type=full	si=3 ^{3, 4}	cics ^{5, 6, 7, 8, 9, 11}	si=4, 5, 13 ^{3, 4}	type=full	si=value other than 3, 4, 5, 13 ^{3, 4}	loc ¹²
sname ¹⁰	asname ¹⁰	cice ^{5, 6, 7, 8, 9, 11}	opc ^{1, 2, 3}	asname ¹⁰	asname ¹⁰	
asname ¹⁰	loc ¹²	type=full	asname ¹⁰	loc ¹²	loc ¹²	
loc ¹²		sname ¹⁰	loc ¹²			
		asname ¹⁰				
		loc ¹²				

Table 3-13. Routing Key Parameter Combinations for Removing Routing Keys (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	
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 si parameter is 4, the point codes must be either an ITU-I, 14-bit ITU-N, or 24-bit ITU-N point code. 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 dlt-appl-rtkey command.						
4. Text strings can be used in place of some numerical service indicator values. See Table 3-11 on page 3-124 for a list of these text strings.						
5. When the service indicator parameter value equals 4 and an ANSI DPC is specified, the opc , cics , and cice parameters cannot be used. If the service indicator parameter value equals 4 and an ITU DPC is specified, the opc , cics , and cice parameters are required.						
6. If the service indicator parameter (si) value is 4, the values of the cics and cice parameters is from 0 to 4095.						
7. If the service indicator parameter (si) 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 cics and cice parameters is from 0 to 4095. If the point code in the routing key is an ANSI point code, the values of the cics and cice parameters is from 0 to 16383.						
8. If the service indicator parameter value is 13, the values of the cics and cice parameters is from 0 to 4294967295.						
9. The CIC range, defined by the cics and cice parameters, cannot overlap the CIC range in an existing routing key.						
10. The sname or asname parameters must be specified, but not both.						
11.The value of the cics parameter must be less than the or equal to the cice parameter value.						
12. If the loc parameter is not specified, a static entry that matches the other specified parameters is deleted.						

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 03-06-28 21:15:37 GMT Rel 31.0.0

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 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 this command.

rtrv-appl-rtkey:dpc=006-006-001:cics=501:cice=1000:display=all

This is an example of the possible output.

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0

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 (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
```

- 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 3-13 on page 3-134 for the parameter combinations that can be used for the type of routing key being added to the database. For example, enter this command.

```
dlt-appl-rtkey:dpc=006-006-001:loc=1107:si=5:cics=501
:cice=1000:sname=socket31
```

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

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
DLT-APPL-RTKEY: MASP A - COMPLTD
```

- Verify the new application routing key information in the database by entering the **rtrv-appl-rtkey** command. The following is an example of the possible output.

```
rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
```

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

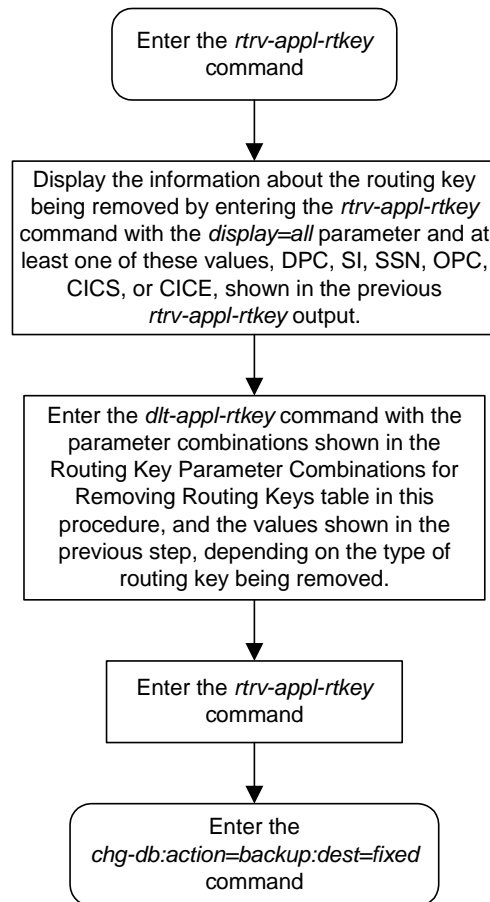
```
STATIC Route Key table is (2 of 2000) 1% full
1105 Route Key table is (2 of 500) 1% full
1107 Route Key table is (1 of 500) 1% full
```

```
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 (1 of 8000) 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 3-17. Removing an Application Routing Key



Changing a Static Application Routing Key

This procedure is used for the **ss7ipgw** and **ipgwi** applications to change a static application routing key entry in the database using the **chg-appl-rtkey** command. An application routing key defines a filter that checks the specified values in an incoming SS7 MSU to determine which socket or application server receives the MSU. For more information about static routing keys, see “Understanding Routing for SS7IPGW and IPGWI Applications” on page 2-23.

The **chg-appl-rtkey** command uses these parameters.

: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 3-14 shows the text strings that can be used in place of numbers for the service indicator values.

Table 3-14. 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 socket associations for the routing key.

: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 *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.

: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 the routing key specified by the **cics** and **cice** values is to be split into two entries. One entry ranges from the **cics** value to a value equal to one less than the **split** value. The other entry ranges from the **split** value to the **cice** value. All other parameters of both entries remain the same as in the entry that was split.

: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.

: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. The new application server name replaces all of the existing application server associations for the routing key.

The **chg-appl-rtkey** command can be used to perform these operations to a routing key:

- Splitting a routing key into two entries with adjacent CIC ranges. The resulting entries retain the socket associations of the original entry.
- Changing the range of CICs assigned to a routing key, as long as new range does not overlap any ranges of values assigned to other routing keys. The new entry retains the socket associations of the original routing key.
- The socket name associations for a routing key can be replaced by a single socket name. All the existing routing data is retained.
- Changing the socket name or application server name for a default routing key.
- Changing the **pstncat**, **pstnid**, and **norm** parameter values in the routing key.

Only one of these operations can be performed with each execution of the **chg-appl-rtkey** command. This procedure shows how to split the CIC ranges for a routing key, change the range of CIC values for a routing key, and change the socket name association for routing keys. Changing the **pstncat**, **pstnid**, and **norm** parameter values in the routing key is discussed in more detail in the “Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key” procedure on page 3-151.

Default Routing Key Rules

If the routing key type is **default** or changed to default, only the **type=default** and either the **nsname** or **nasname** parameters can be specified with the **chg-appl-rtkey** command. When the routing key type is **default**, either the **nsname** or **nasname** parameter must be specified. The **nsname** and **nasname** parameters cannot be specified at the same time.

Rules for Changing the Range of CIC Values in the Routing Key

Only these parameters can be specified for this operation: **dpc**, **si**, **opc**, **cics**, **cice**, **ncics**, **ncice**, **type=full**.

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.

The **type=full**, **dpc**, and **si** parameters must be specified.

The **cics** and **cice** parameters must be specified and either the **ncics** or **ncice** parameters, or both, must be specified. If both the **ncics** and **ncice** parameters are specified, the value of the **ncics** parameter must be less than the value of the **ncice** parameter. If the **ncics** parameter is not specified, the value of the **ncice** parameter must be greater than or equal to the **cics** parameter value. If the **ncice** parameter is not specified, the value of the **ncics** parameter must be less than or equal to the **cice** parameter value.

The value of the **si** parameter must be 4, 5, or 13.

The value entered for the starting circuit identification code (**cics**) must be less than or equal to the value entered for the ending circuit identification code (**cice**).

The new CIC range cannot overlap the CIC range in an existing routing key.

If **si=4** and an ANSI **dpc** is specified, the **opc**, **cics**, **cice**, **ncics**, and **ncice** parameters cannot be used. If **si=4** and an ITU **dpc** (**dpci**, **dpcn**, or **dpcn24**) is specified, the **opc**, **cics**, **cice**, **ncics**, and **ncice** parameters are required.

If the **si** parameter value is 4, the point codes must be either an ITU-I, 14-bit ITU-N, or 24-bit ITU-N point code.

If the service indicator parameter (**si**) value is 4, the values of the **cics** and **cice** parameters is from 0 to 4095.

If the service indicator parameter (**si**) 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 **cics** and **cice** parameters is from 0 to 4095. If the point code in the routing key is an ANSI point code, the values of the **cics** and **cice** parameters is from 0 to 16383.

If the value of the **si** parameter is 13, the values of the **cics**, **cice**, **ncics**, and **ncice** parameters is from 0 to 4294967295.

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.

Rules for Splitting the Range of CIC Values in the Routing Key

These parameters must be specified for this operation: **dpc**, **si**, **opc**, **cics**, **cice**, **split**, **type=full**.

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.

The **cics**, **cice**, and **split** parameters must be specified. The value of the **cics** parameter must be less or equal to than the value of the **cice** parameter. The value of the **split** parameter must be greater than the **cics** parameter value and less than the **cice** parameter value.

The value of the **si** parameter must be 4, 5, or 13.

If **si=4** and an ANSI **dpc** is specified, the **opc**, **cics**, **cice**, and **split** parameters cannot be used. If **si=4** and an ITU **dpc** (**dpci**, **dpcn**, or **dpcn24**) is specified, the **opc**, **cics**, **cice**, and **split** parameters are required.

If the **si** parameter value is 4, the point codes must be either an ITU-I, 14-bit ITU-N, or 24-bit ITU-N point code.

If the service indicator parameter (**si**) value is 4, the values of the **cics**, **cice**, **ncics**, and **ncice** parameters is from 0 to 4095.

If the service indicator parameter (**si**) 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 **cics**, **cice**, **ncics**, and **ncice** parameters is from 0 to 4095. If the point code in the routing key is an ANSI point code, the values of the **cics**, **cice**, **ncics**, and **ncice** parameters is from 0 to 16383.

If the service indicator parameter value is 13, the values of the **cics**, **cice**, **ncics**, and **ncice** parameters is from 0 to 4294967295.

If the ITU National Duplicate Point Code feature is on, the values for the **dpcn** and **opc** 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.

Rules for Changing the Socket Name or Application Server Name Association in the Routing Key

The parameter combinations used by the **chg-appl-rtkey** command to change the socket name or application server name associations in the routing key are based on the type of routing key and the service indicator value in the routing key. The parameter combinations are shown in Table 3-15 on page 3-144.

Table 3-15. Routing Key Parameter Combinations for Changing
Socket Name Associations

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 ⁹	nsname ⁹	nsname ⁹	nsname ⁹	nsname ⁹	nsname ⁹	nsname ⁹
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}	nasname ⁹
ssn	si=3 ^{3, 4}	opc ^{1, 2}	si=4, 5, 13 ^{3, 4}	type=full	si=value other than 3, 4, 5, 13 ^{3, 4}	
type=full	nasname ⁹	cics ^{5, 6, 7, 8}	opc ^{1, 2, 3}	nasname ⁹	nasname ⁹	
nasname ⁹		cice ^{5, 6, 7, 8}	nasname ⁹			
		type=full				
		nasname ⁹				

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 **si** parameter is 4, the point codes must be either an ITU-I, 14-bit ITU-N, or 24-bit ITU-N point code. 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 **chg-appl-rtkey** command.
4. Text strings can be used in place of some numerical service indicator values. See Table 3-14 on page 3-139 for a list of these text strings.
5. When the service indicator parameter value equals 4 and an ANSI dpc is specified, the **opc**, **cics**, and **cice** parameters cannot be used. If the service indicator parameter value equals 4 and an ITU dpc is specified, the **opc**, **cics**, and **cice** parameters are required.
6. If the service indicator parameter (**si**) value is 4, the values of the **cics** and **cice** parameters is from 0 to 4095.
7. If the service indicator parameter (**si**) 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 **cics** and **cice** parameters is from 0 to 4095. If the point code in the routing key is an ANSI point code, the values of the **cics** and **cice** parameters is from 0 to 16383.
8. If the service indicator parameter value is 13, the values of the **cics** and **cice** parameters is from 0 to 4294967295.
9. The **nsname** or **nasname** parameters must be specified, but not both.

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 03-06-28 21:15:37 GMT Rel 31.0.0
```

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**, **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 03-06-28 21:16:37 GMT Rel 31.0.0
```

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: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
```

NOTE: If the application server name (**asname**) is being changed in the routing key, skip this step and go to step 4.

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 03-06-28 21:15:37 GMT Rel 31.0.0
SNAME kchlr11201
  LHOST ipnode1-1201
  LPORT 7000
  SERVER YES
  RHOST kc-hlr1
  RPORT 7000
  OPEN YES
  ALW NO
  DCMPS 1
  PORT A
  REXMIT FIXED
  RTT 60

SNAME kchlr11203
  LHOST ipnode1-1203
  LPORT 7005
  SERVER YES
  RHOST kc-hlr1
  RPORT 7005
  OPEN YES
  ALW YES
  DCMPS 10
  PORT A
  REXMIT FIXED
  RTT 60
```

If the required socket is not in the database, go to the “Adding an Application Socket” procedure on page 3-89 to add the socket.

NOTE: If the application socket (**sname**) is being changed in the routing key, skip this step and go to step 5.

4. 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 03-06-28 09:12:36 GMT Rel 31.0.0
      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 required application server is not in the database, go to the “Adding an Application Server” procedure on page 6-85 to add the application server.

NOTE: If a default routing key is being added to the database, or if ITU-N point codes are not being specified for the routing key, skip this step 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 should 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 application routing key information to the database 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, the type of routing key being changed, and the service indicator value in the routing key. Go to one of these sections to determine the required parameter combination.
 - “Default Routing Key Rules” on page 3-141
 - “Rules for Changing the Range of CIC Values in the Routing Key” on page 3-141
 - “Rules for Splitting the Range of CIC Values in the Routing Key” on page 3-142
 - “Rules for Changing the Socket Name or Application Server Name Association in the Routing Key” on page 3-143.

For this example, the socket name association is being changed. Enter this command.

```
chg-appl-rtkey:dpca=123-234-123:si=5:opca=122-124-125:cics=1
:cice=1000:nsname=socket2
```

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 03-06-28 21:16:37 GMT Rel 31.0.0
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 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
```

This is an example of the possible output.

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
```

```
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
```

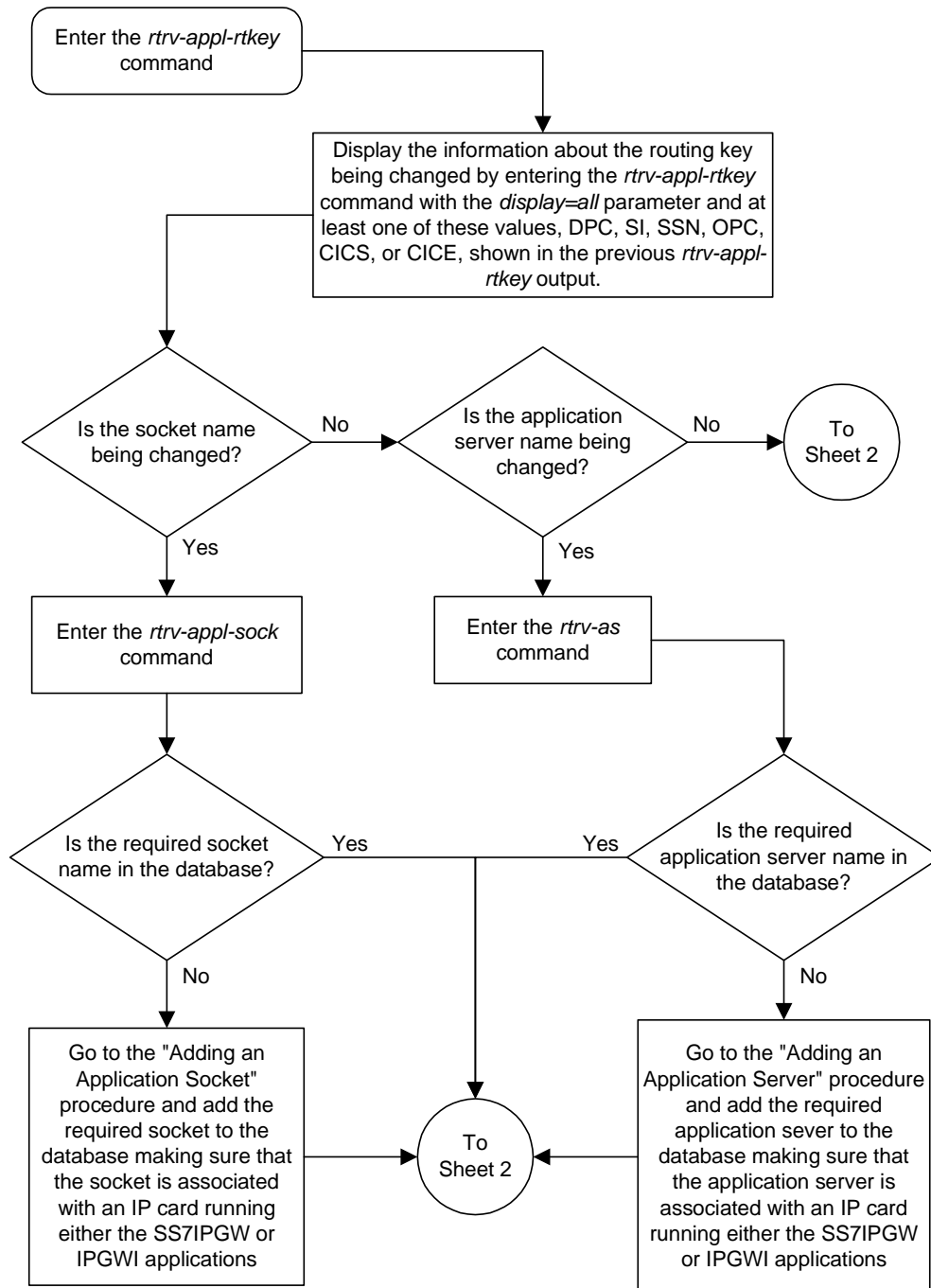
```
STATIC Route Key Socket Association table is (2 of 32000) 1% full
1105  Route Key Socket Association table is (2 of 8000) 1% full
1107  Route Key Socket Association table is (2 of 8000) 1% full
```

8. If you wish to change the PSTN presentation information in the routing key that was changed in step 6, go to the “Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key” procedure on page 3-151.
-

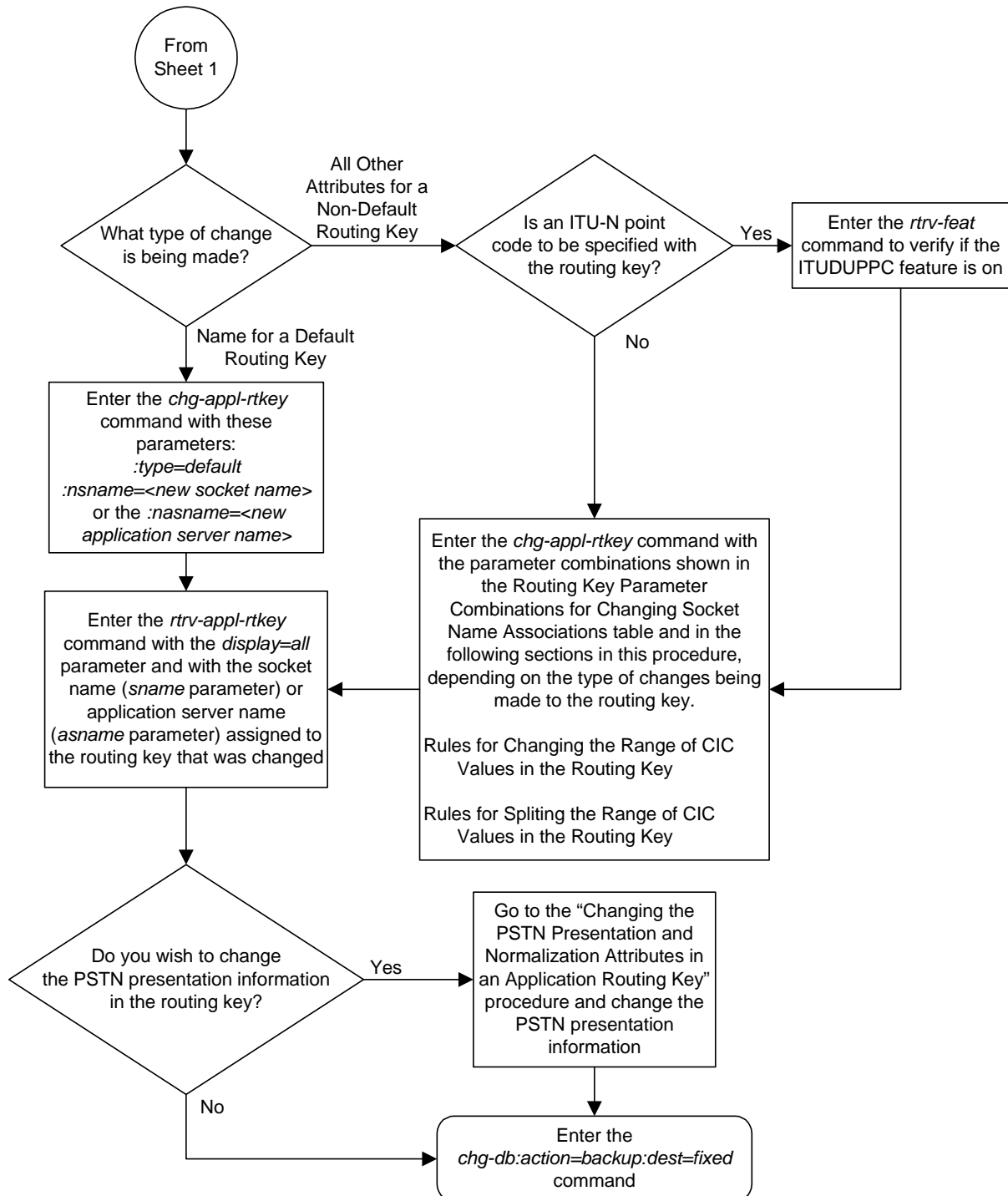
9. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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 3-18. Changing a Static Application Routing Key (Sheet 1 of 2)



Flowchart 3-18. Changing a Static Application Routing Key (Sheet 2 of 2)



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 03-06-28 21:17:37 GMT Rel 31.0.0

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 3-16 shows the text strings that can be used in place of numbers for the service indicator values.

Table 3-16. 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 “Changing a Static Application Routing Key” procedure on page 3-139.

: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. The new application server name replaces all of the existing application server associations for 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.

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 03-06-28 21:15:37 GMT Rel 31.0.0
```

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 03-06-28 21:16:37 GMT Rel 31.0.0
```

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 03-06-28 21:15:37 GMT Rel 31.0.0
The following features have been permanently enabled:
Feature Name          Partnum      Status  Quantity
TPS                   893000110  on      1000
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 03-06-28 21:17:37 GMT Rel 31.0.0
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 **ptsnid** parameter values that can be used in this procedure.

NOTE: If 14-bit ITU-N point codes (**dpcn**, **opc**) 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**, **ptsnid**, and **norm** parameters.

```
chg-appl-rtkey:dpcn=12323-de:si=5:opc=12212-de:cics=1
:cice=1000:pstncat=1:ptsnid=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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
```

```
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
```

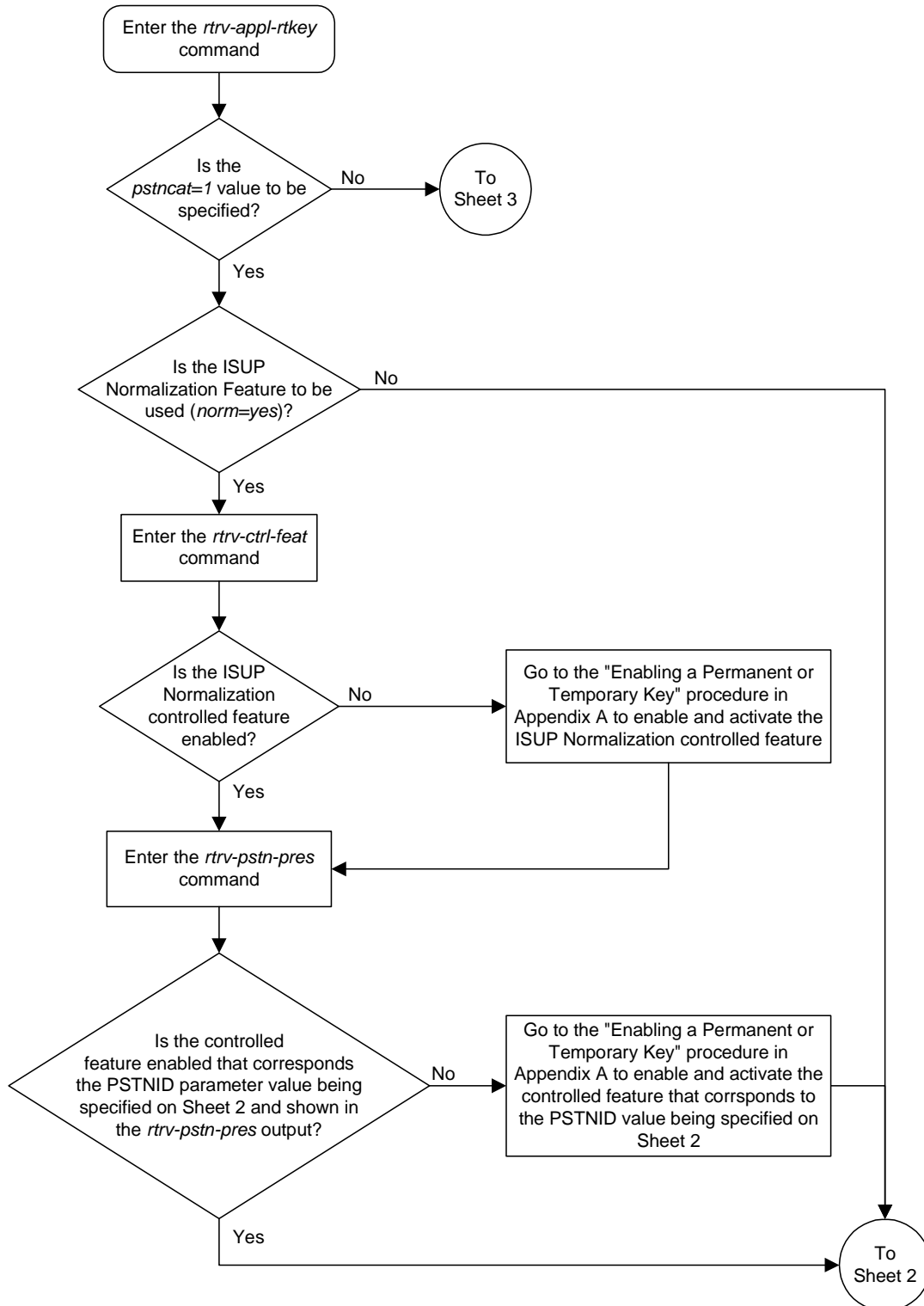
```
STATIC Route Key table is (2 of 2000) 1% full
1105   Route Key table is (2 of 500) 1% full
1107   Route Key table is (2 of 500) 1% full
```

```
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
```

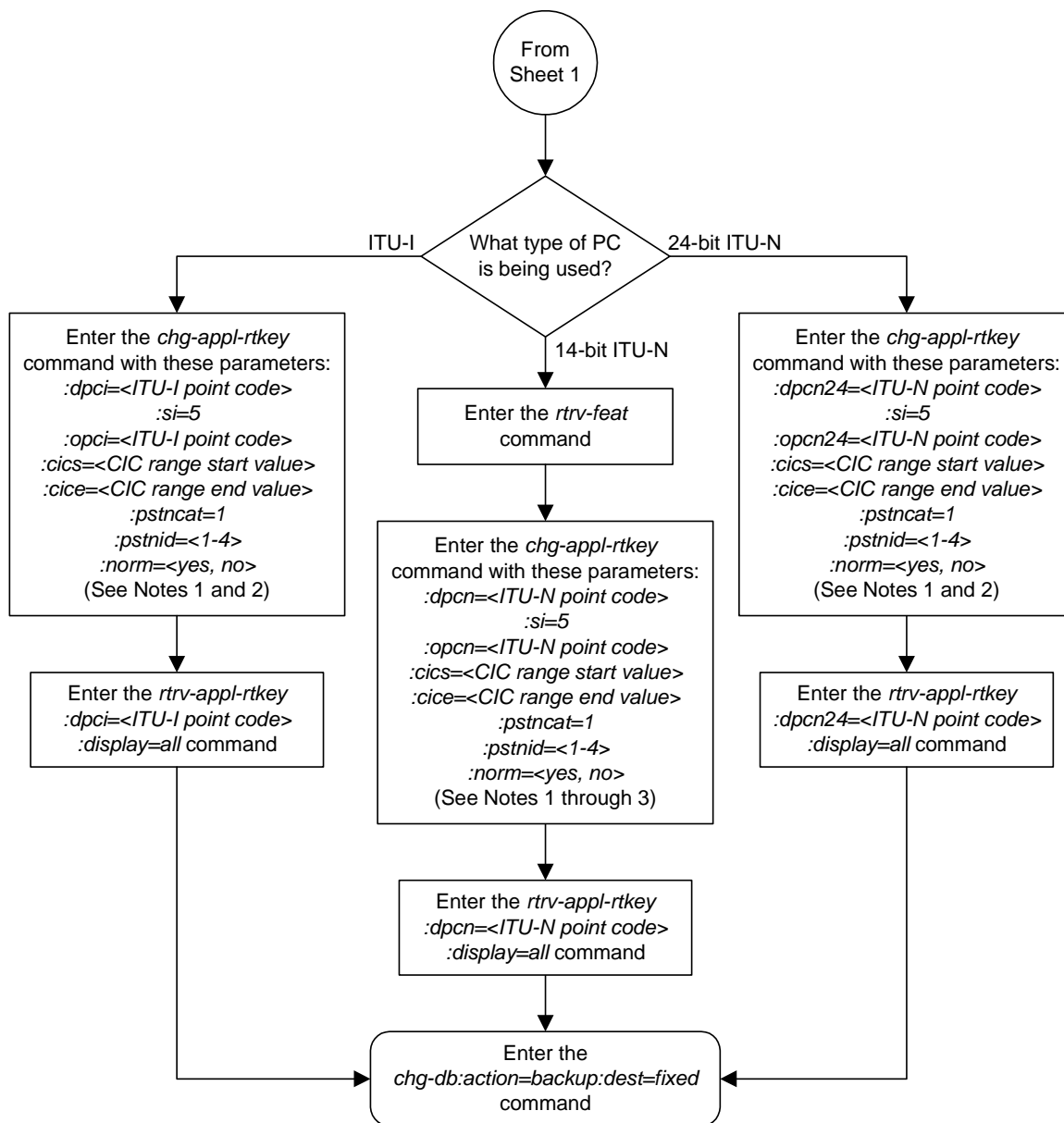
8. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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 3-19. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key (Sheet 1 of 6)



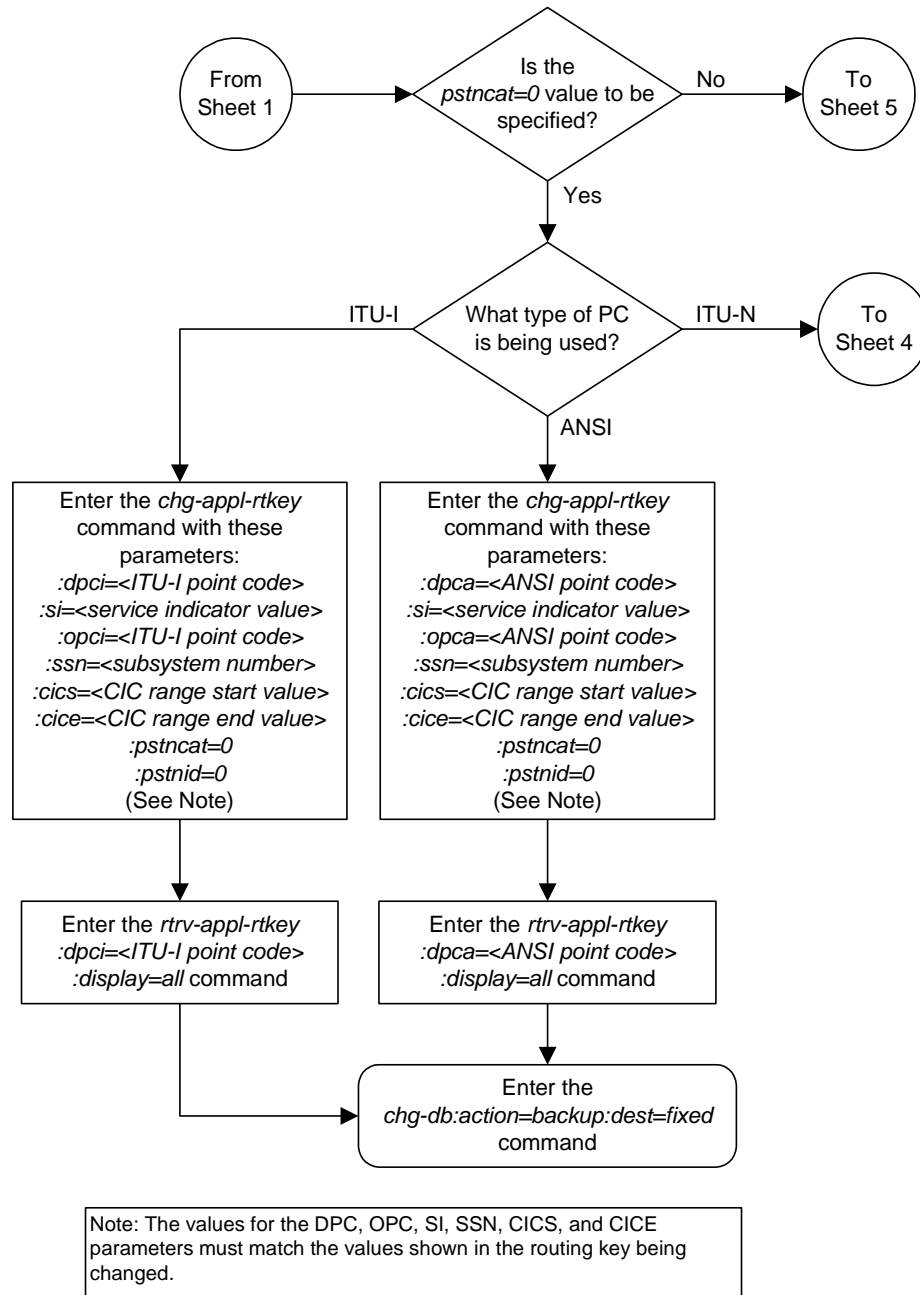
Flowchart 3-19. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key (Sheet 2 of 6)



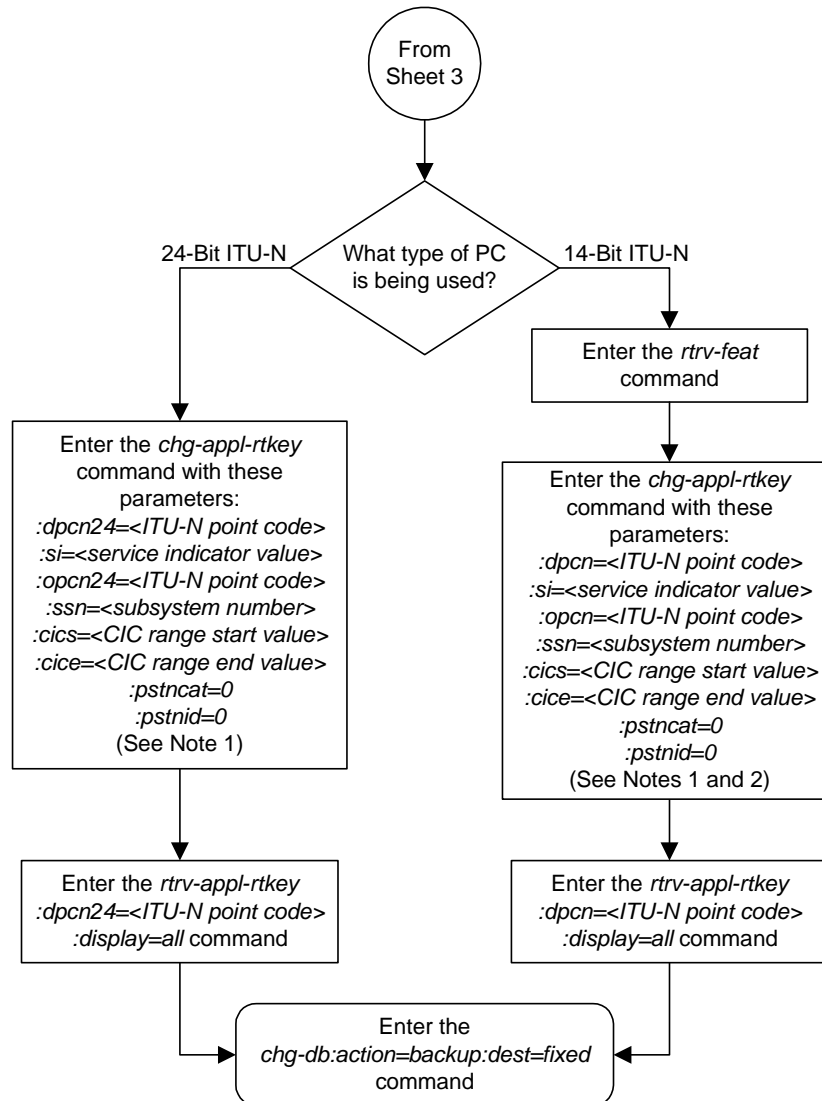
Notes:

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 3-19. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key (Sheet 3 of 6)



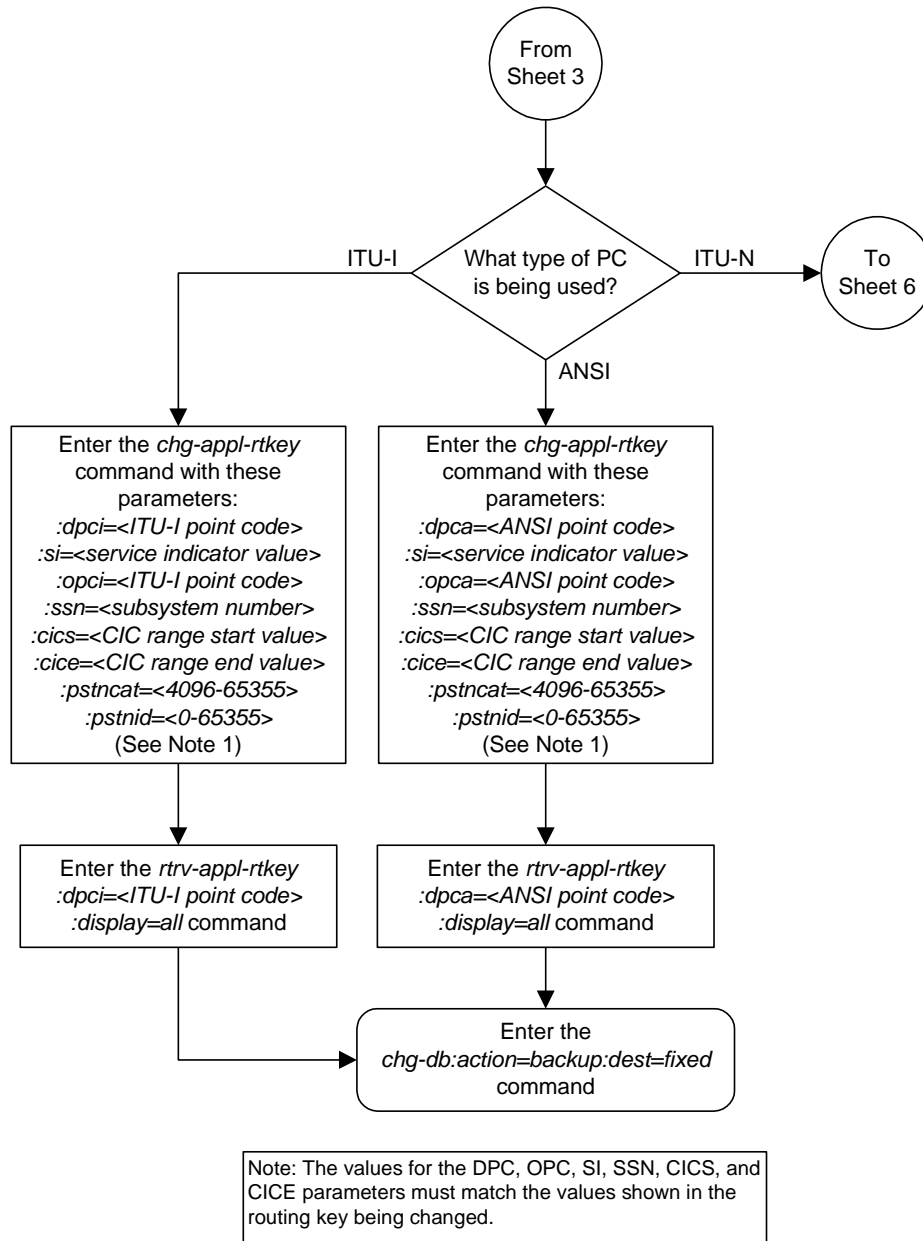
Flowchart 3-19. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key (Sheet 4 of 6)



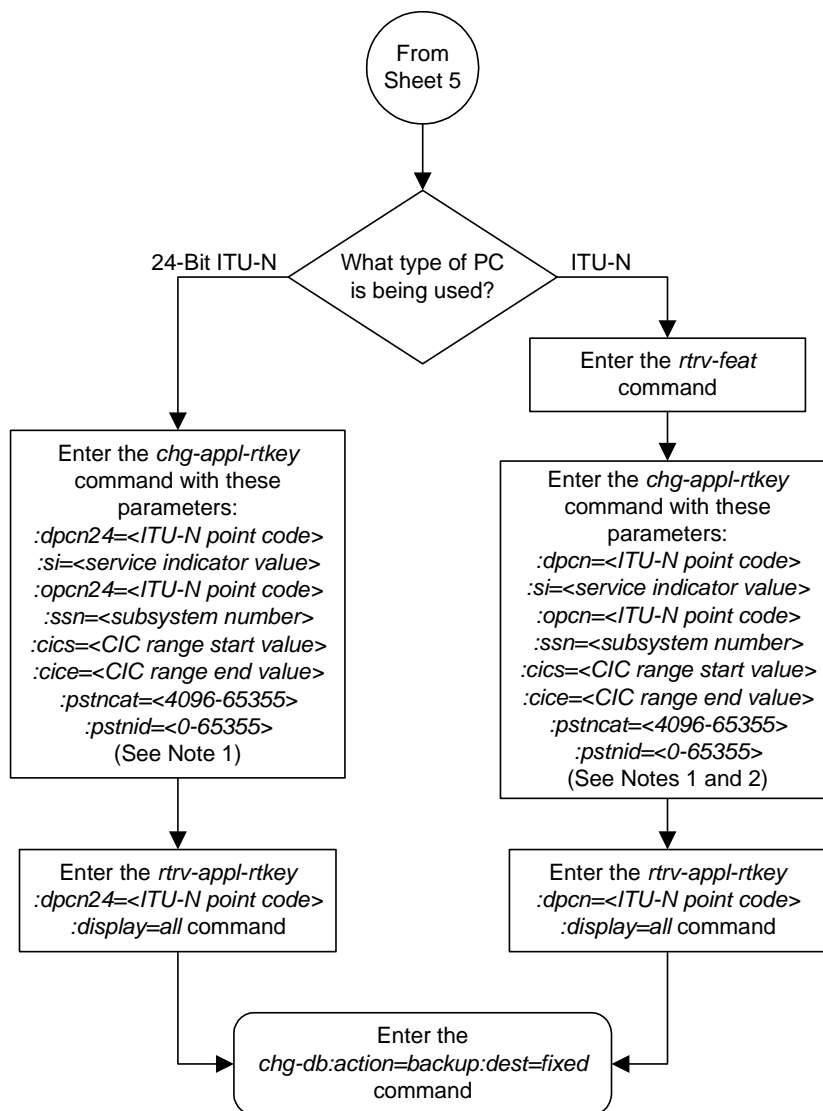
Notes:

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 3-19. Changing the PSTN Presentation and Normalization Attributes in an Application Routing Key (Sheet 5 of 6)



Flowchart 3-19. 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 *rtvr-feat* command shows whether or not this feature is on.

Increasing the TPS on the IP Card

This procedure is used with **IPGWx** applications (IP cards running either the **ss7ipgw** or **ipgwi** applications) and increases the transactions per second (TPS) on the IP card, using the **enable-ctrl-feat** command. The TPS on the IP card controls the number of message signaling units (MSUs) that are transferred over the IP card per second.

NOTE: If you are not sure whether you have purchased this controlled feature, contact your Tekelec Sales Representative or Account Representative.

NOTE: Once the TPS on the IP card is permanently increased, it cannot be decreased or disabled.

The system is shipped with a default rate of TPS-100 per IP card and a password that can be used to increase the rate to TPS-200. The TPS can be increased in increments of 100 to TPS-4000.

The TPS-3000 rate can be reached, assuming the following guidelines are met:

- No more than 150 active cards are present in the system.
- The average size of an MSU is no greater than 120 octets.
- Nagle's Algorithm is enabled for all traffic-carrying sockets. To learn more about Nagle's Algorithm, see "Nagle's Algorithm" on page 2-37.

NOTE: The STPLAN feature on outbound messages is supported for rates up to TPS-2000.

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).

: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: If you do not have the part number or 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).

When the system is shipped, the default TPS value is 100.

The controlled feature part number must be valid. It must match the part number of the controlled feature you are enabling.

The TPS rate specified in this procedure must be greater than the current TPS rate.

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 03-06-28 21:15:37 GMT Rel 31.0.0
The following features have been permanently enabled:
Feature Name          Partnum    Status   Quantity
TPS                   893000101  on       100
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 TPS quantity is greater than 100, 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 03-06-28 21:15:37 GMT Rel 31.0.0
System serial number = nt00001231
```

System serial number is not locked.

```
rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
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
```

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 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.

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 03-02-28 21:15:37 GMT Rel 30.0.0
ENT-SERIAL-NUM:  MASP A - COMPLTD
```

6. Increase the TPS on the IP card by entering the **enable-ctrl-feat** command. For example, enter this command.

```
enable-ctrl-feat:partnum=893000120:fak=<feature access key>
```

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

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
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=893000120
```

The following is an example of the possible output.

```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
The following features have been permanently enabled:
Feature Name          Partnum    Status   Quantity
TPS                   893000120  ----    2000
```

The following features have been temporarily enabled:

```
Feature Name          Partnum    Status   Quantity   Trial Period Left
Zero entries found.
```

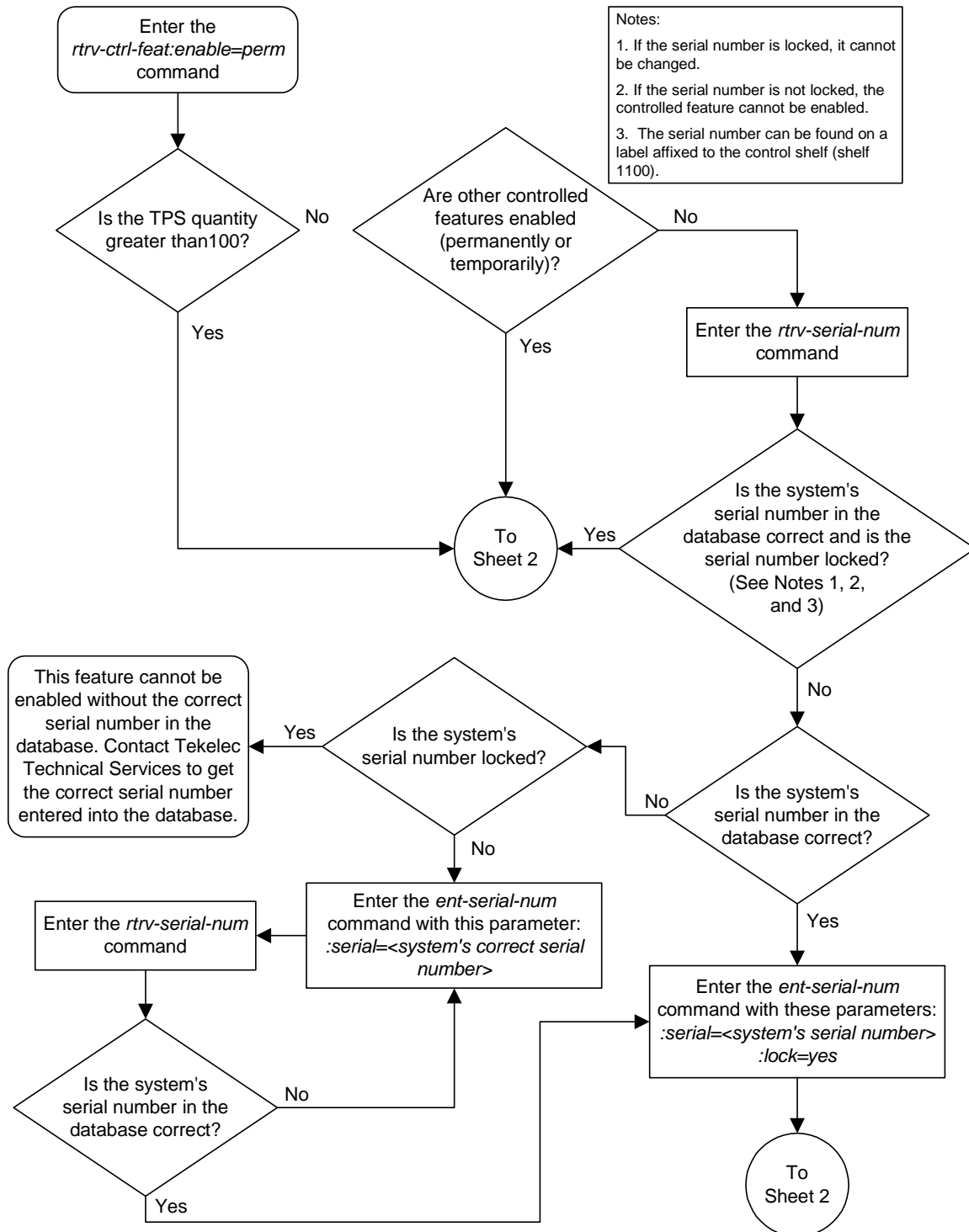
The following features have expired temporary keys:

```
Feature Name          Partnum
Zero entries found.
```

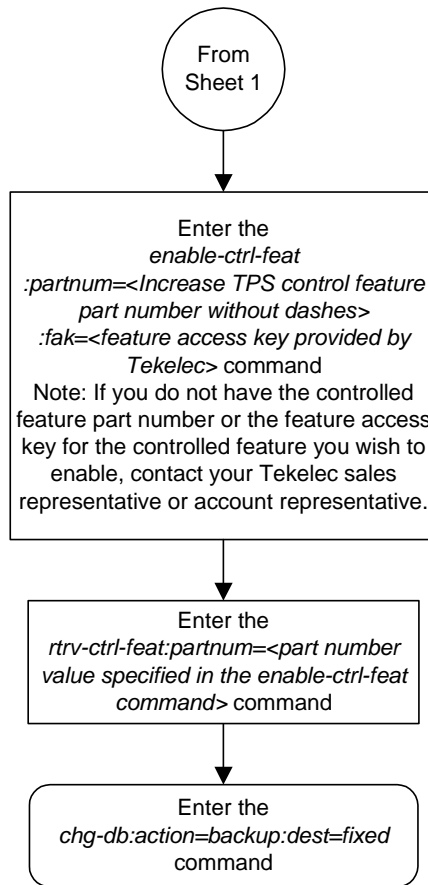
8. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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 3-20. Increasing the TPS on the IP Card (Sheet 1 of 2)



Flowchart 3-20. Increasing the TPS on the IP Card (Sheet 1 of 2)



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 3-190 to complete the entry of the host names.

Each local host can contain a maximum of 50 connections (associations plus sockets).

The system can contain a maximum of 250 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.

Procedure

1. Display the associations in the database using the **rtrv-assoc** command.
This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME swbel32
  LHOST  gw105.nc.tekelec.com
  ALHOST  ---
  LPORT  1030
  RHOST  gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  RPORT  2345
  OPEN   YES
  ALW    YES
  PORT   A
  ADAPTER M3UA
  VER    M3UA RFC
  RMODE  LIN
  RMIN   120
  RMAX   800
  RTIME  10
  CWMIN  3000
  ISTRMS 2
  OSTRMS 2

ANAME a2
  LHOST  gw105.nc.tekelec.com
  ALHOST  ---
  LPORT  1030
  RHOST  gw100.nc.tekelec.com
  RPORT  2345
  OPEN   YES
  ALW    YES
  PORT   A
  ADAPTER SUA
  VER    SUA DRAFT 3
  RMODE  LIN
  RMIN   120
  RMAX   800
  RTIME  10
  CWMIN  3000
  ISTRMS 2
  OSTRMS 2

ANAME a3
  LHOST  gw105.nc.tekelec.com
  ALHOST  ---
  LPORT  1030
  RHOST  gw106.nc.tekelec.com
  RPORT  2346
  OPEN   YES
  ALW    YES
  PORT   A
  ADAPTER SUA
  VER    SUA DRAFT 3
  RMODE  LIN
  RMIN   120
  RMAX   800
  RTIME  10
  CWMIN  3000
  ISTRMS 2
  OSTRMS 2
IP Appl Sock table is (3 of 250) 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 03-06-28 21:15:37 GMT Rel 31.0.0
```

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

If the required hostname is not in the database, add the IP host name using the “Adding an IP Host” on page 3-61 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 03-06-28 21:19:37 GMT Rel 31.0.0
```

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 3-66 procedure.

4. 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 03-06-27 17:00:36 GMT Rel 31.0.0
```

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 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 03-06-19 21:17:04 GMT Rel 31.0.0
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 SS7 Signaling Link" procedure in the *Database Administration Manual - SS7*. 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 SS7 Signaling Link" procedure in the *Database Administration Manual - SS7*.

NOTE: If the "Adding an SS7 Signaling Link" procedure in the *Database Administration Manual - SS7* 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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-07 11:11:28 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
```

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 3-220 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.

NOTES:

1. For associations assigned to IPLIMx cards, the value of the **adapter** parameter must match the value of the **iplim12** parameter for the signaling link being assigned to the association. For example, if the value of the signaling link's **iplim12** parameter is **m3ua**, then the **adapter=m3ua** parameter must be specified for the association. If the value of the signaling link's **iplim12** parameter is **m2pa**, then the **adapter=m2pa** parameter must be specified for the association.
2. For associations assigned to IPGWx cards, the value of the **adapter** parameter defaults to **m3ua**, if the **adapter** parameter is not specified. The only values for the **adapter** parameter that an IP gateway association can have is **m3ua** or **sua**.
3. If the **m2patset** parameter is not specified when adding an association with the **adapter=m2pa** parameter, the M2PA timer set 1 will be assigned to the association. The **m2patset** parameter can be specified only with the **adapter=m2pa** parameter.

```
ent-assoc:aname=assoc1:lhost=gw105.nc.tekelec.com:lport=1030:
rhost=gw100.nc.tekelec.com:rport=1030:adapter=m3ua
```

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

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
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 03-06-07 11:11:28 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME assoc1
  LHOST   gw105.nc.tekelec.com
  ALHOST  ---
  LPORT   1030
  RHOST   gw100.nc.tekelec.com
  RPORT   1030
  OPEN    NO
  ALW     NO
  PORT    A
  ADAPTER M3UA
  VER     M3UA RFC
  RMODE   LIN
  RMIN    120
  RMAX    800
  RTIMES  10
  CWMIN   3000
  ISTRMS  2
  OSTRMS  2
IP Appl Sock table is (4 of 250) 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.

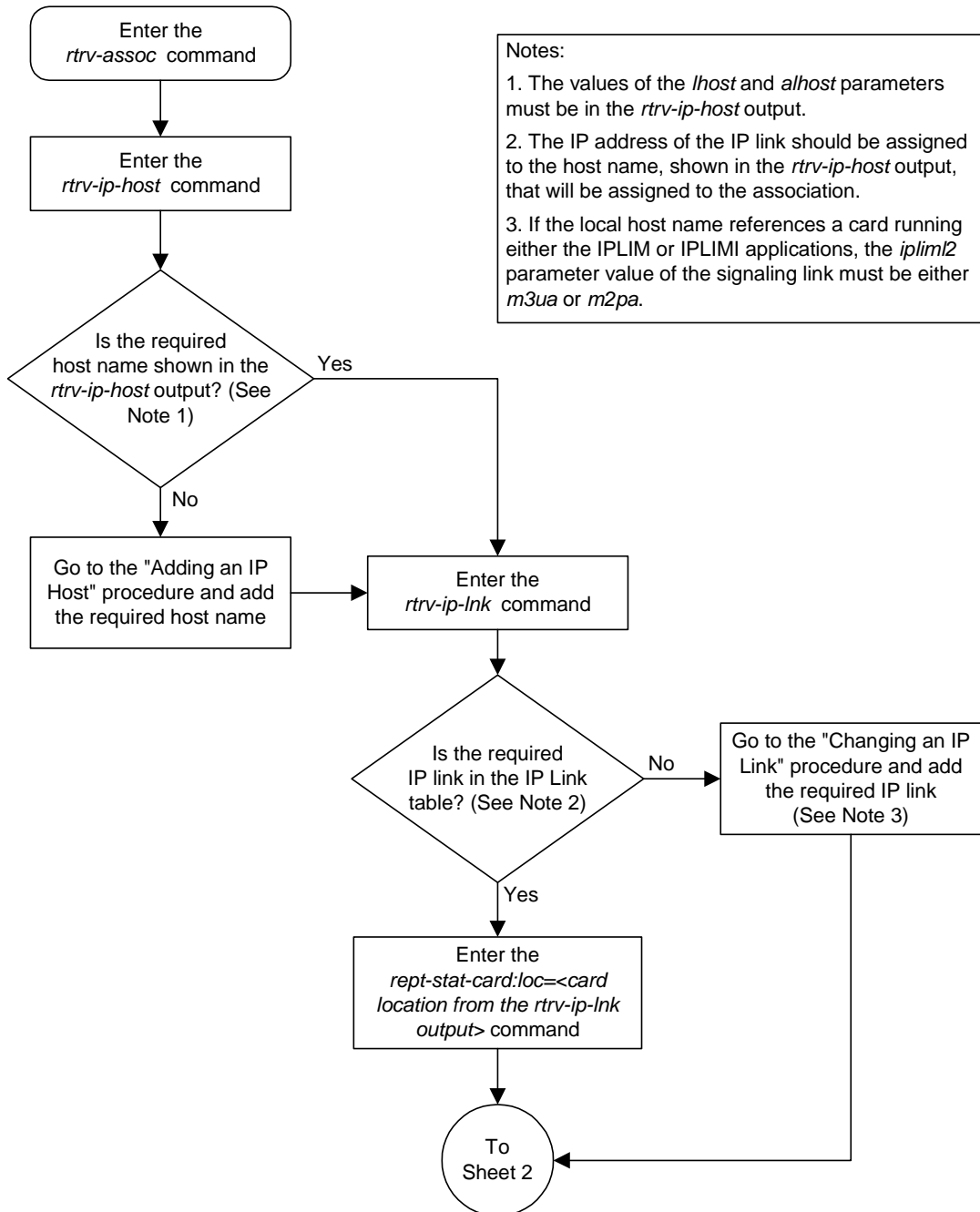
BACKUP (FIXED) : MASP A - Backup starts on active MASP.

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

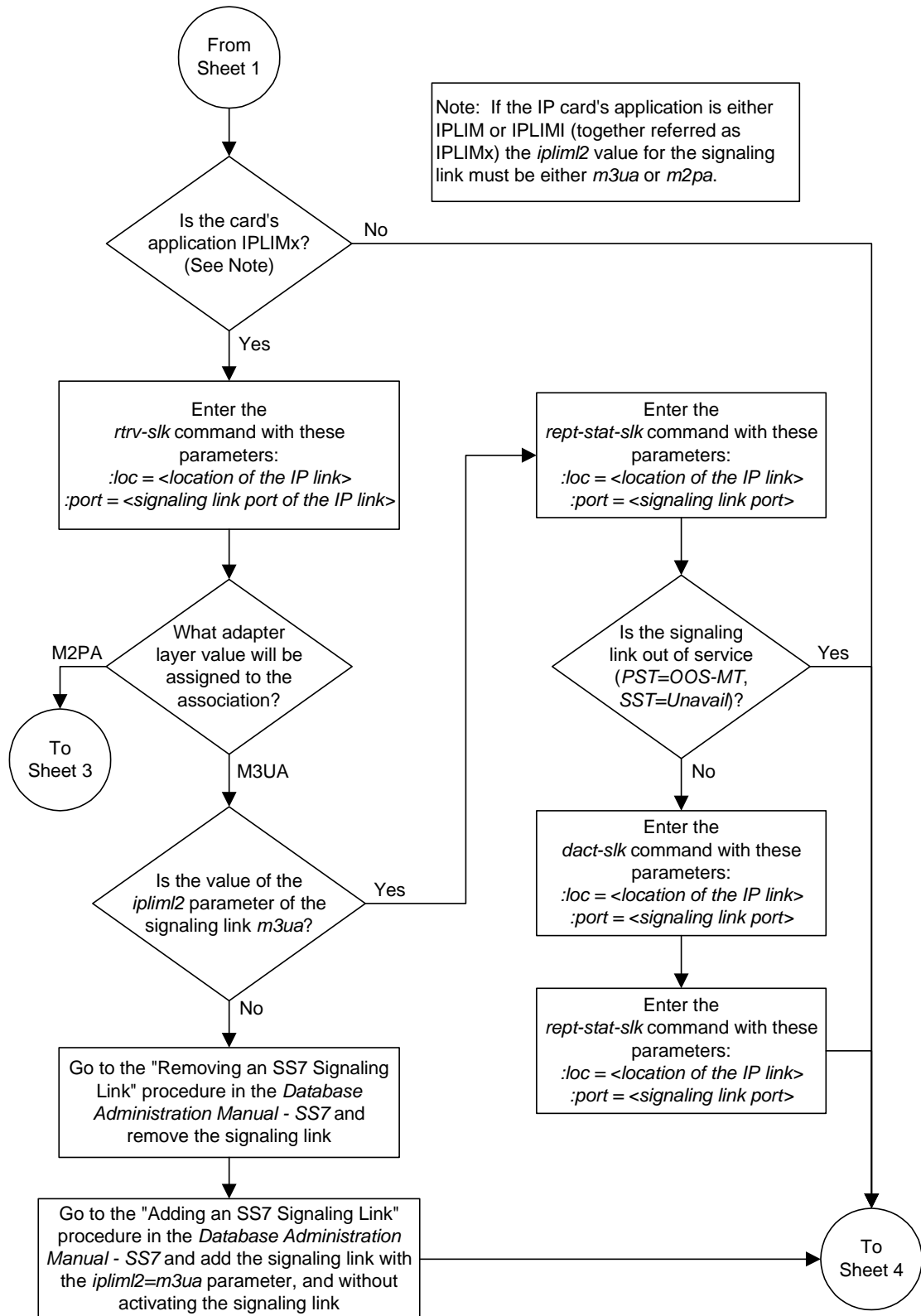
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.

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

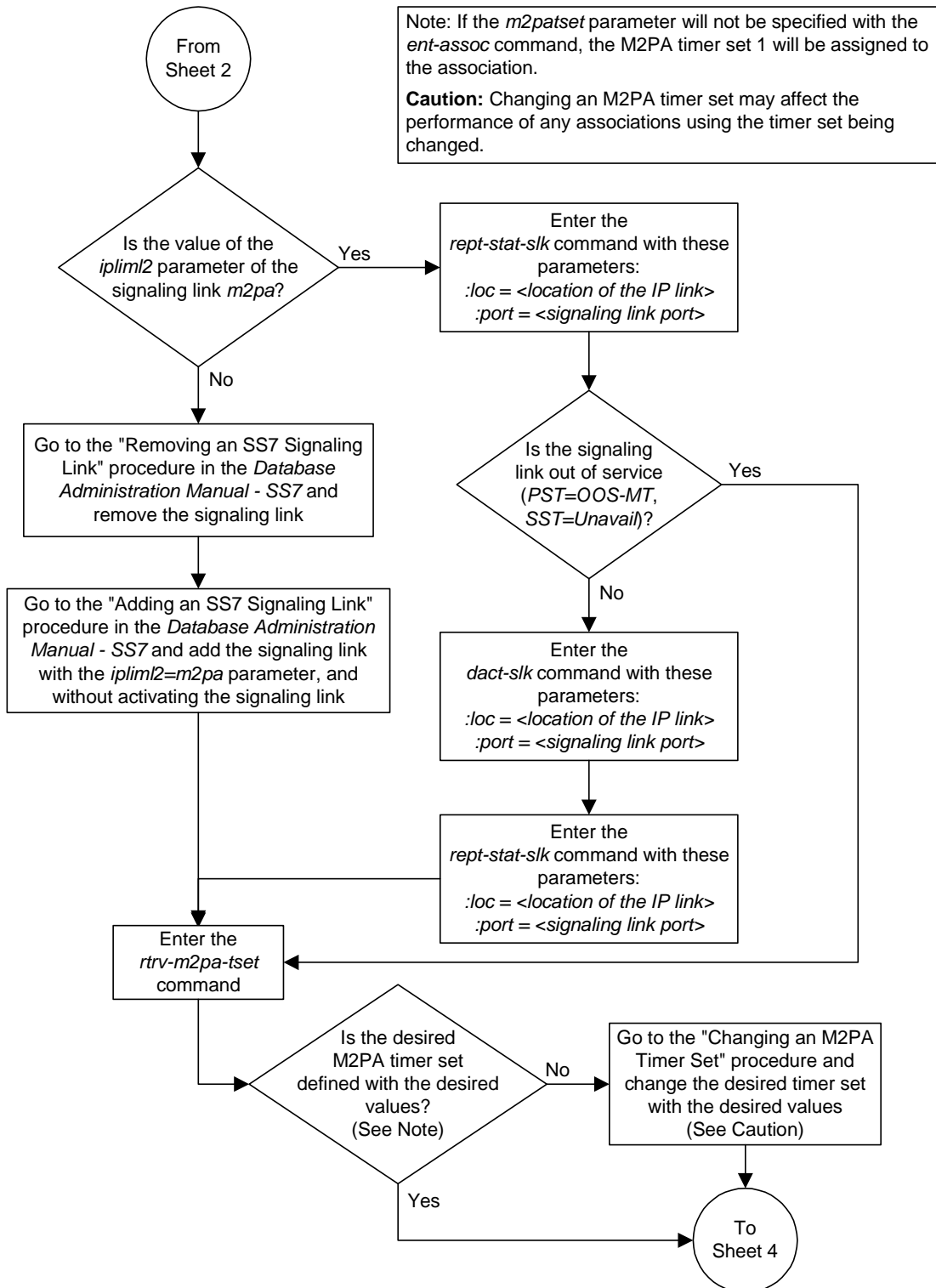
Flowchart 3-21. Adding an Association (Sheet 1 of 5)



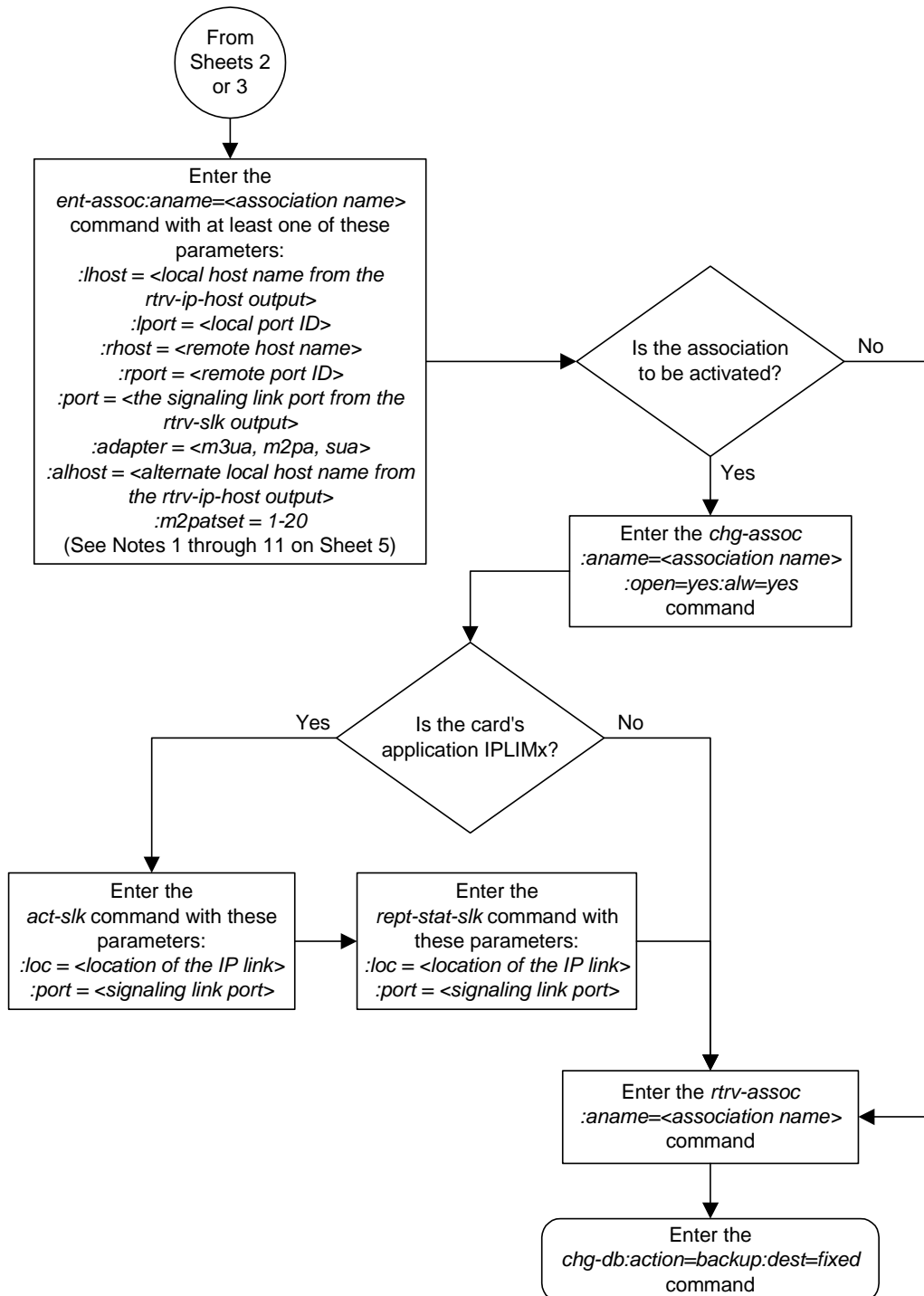
Flowchart 3-21. Adding an Association (Sheet 2 of 5)



Flowchart 3-21. Adding an Association (Sheet 3 of 5)



Flowchart 3-21. Adding an Association (Sheet 4 of 5)



Flowchart 3-21. 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 *iplim2* parameter of the signaling link being assigned to 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 250 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 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 *m2patset* parameter can be specified only with the *adapter=m2pa* parameter.
11. 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 3-228 and remove the ASP assignment to the association.

Procedure

1. Display the associations in the database using the **rtrv-assoc** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME swbel32
  LHOST    gw105.nc.tekelec.com
  ALHOST   ---
  LPORT    1030
  RHOST    gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  RPORT    2345
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  M3UA
  VER      M3UA RFC
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2
```

```

ANAME a2
  LHOST    gw105.nc.tekelec.com
  ALHOST   ---
  LPORT    1030
  RHOST    gw100.nc.tekelec.com
  RPORT    2345
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  SUA
  VER      SUA DRAFT 3
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2

```

```

ANAME a3
  LHOST    gw105.nc.tekelec.com
  ALHOST   ---
  LPORT    1030
  RHOST    gw106.nc.tekelec.com
  RPORT    2346
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  SUA
  VER      SUA DRAFT 3
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2

```

```

ANAME assoc1
  LHOST    gw105.nc.tekelec.com
  ALHOST   ---
  LPORT    1030
  RHOST    gw100.nc.tekelec.com
  RPORT    1030
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  M3UA
  VER      M3UA RFC
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2

```

```

IP Appl Sock table is (4 of 250) 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 03-06-28 09:12:36 GMT Rel 31.0.0
ASP           Association      UAPS
ASP1          swbel32          1
ASP2          a2               1
ASP3          a3               1
ASP4          assoc1           10
ASP Table is (4 of 250) 1% full
```

If the association is assigned to an ASP, go to the “Removing an Application Server Process” procedure on page 3-228 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 03-06-28 09:12:36 GMT Rel 31.0.0
CHG-ASSOC: MASP A - COMPLTD;
```

4. Remove the association from the database using the **dlr-assoc** command. For this example, enter this command.

dlr-assoc:aname=assoc1

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

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
DLR-ASSOC: MASP A - COMPLTD
```

5. Verify the changes using the **rtrv-assoc** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME swbel32
  LHOST  gw105.nc.tekelec.com
  ALHOST  ---
  LPORT  1030
  RHOST  gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  RPORT  2345
  OPEN   YES
  ALW    YES
  PORT   A
  ADAPTER M3UA
  VER     M3UA RFC
  RMODE  LIN
  RMIN    120
  RMAX    800
  RTIMES  10
  CWMIN   3000
  ISTRMS  2
  OSTRMS  2

ANAME a2
  LHOST  gw105.nc.tekelec.com
  ALHOST  ---
  LPORT  1030
  RHOST  gw100.nc.tekelec.com
  RPORT  2345
  OPEN   YES
  ALW    YES
  PORT   A
  ADAPTER SUA
  VER     SUA DRAFT 3
  RMODE  LIN
  RMIN    120
  RMAX    800
  RTIMES  10
  CWMIN   3000
  ISTRMS  2
  OSTRMS  2

ANAME a3
  LHOST  gw105.nc.tekelec.com
  ALHOST  ---
  LPORT  1030
  RHOST  gw106.nc.tekelec.com
  RPORT  2346
  OPEN   YES
  ALW    YES
  PORT   A
  ADAPTER SUA
  VER     SUA DRAFT 3
  RMODE  LIN
  RMIN    120
  RMAX    800
  RTIMES  10
  CWMIN   3000
  ISTRMS  2
  OSTRMS  2
IP Appl Sock table is (3 of 250) 1% full
```

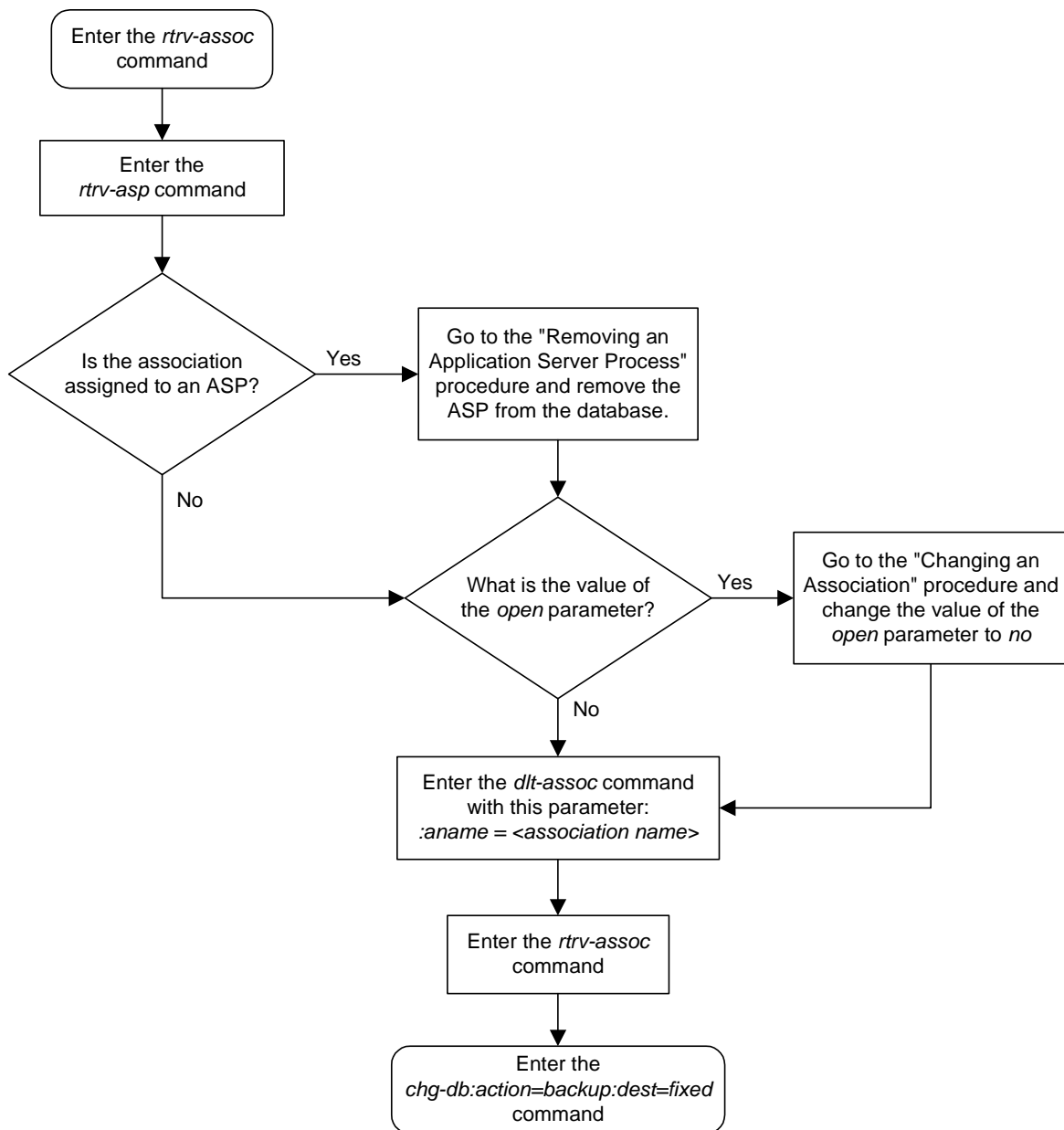
6. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```

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 3-22. 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.

:cwmmin – 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 **cwmmin** 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 3-211 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 **d8** (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 **adatper=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 can contain a maximum of 50 connections (associations plus sockets).

The system can contain a maximum of 250 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 3-228 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.

Procedure

1. Display the associations in the database using the **rtrv-assoc** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME swbel32
  LHOST    gw105.nc.tekelec.com
  ALHOST    ---
  LPORT    1030
  RHOST    gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  RPORT    2345
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  M3UA
  VER      M3UA RFC
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2
ANAME a2
  LHOST    gw105.nc.tekelec.com
  ALHOST    ---
  LPORT    1030
  RHOST    gw100.nc.tekelec.com
  RPORT    2345
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  SUA
  VER      SUA DRAFT 3
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2
ANAME a3
  LHOST    gw105.nc.tekelec.com
  ALHOST    ---
  LPORT    1030
  RHOST    gw106.nc.tekelec.com
  RPORT    2346
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  SUA
  VER      SUA DRAFT 3
```

```

RMODE    LIN
RMIN      120
RMAX      800
RTIMES    10
CWMIN     3000
ISTRMS    2
OSTRMS    2

```

```

ANAME assoc1
LHOST     gw105.nc.tekelec.com
ALHOST    ---
LPORT     1030
RHOST     gw100.nc.tekelec.com
RPORT     1030
OPEN      YES
ALW       YES
PORT      A
ADAPTER    M3UA
VER        M3UA RFC
RMODE     LIN
RMIN      120
RMAX      800
RTIMES    10
CWMIN     3000
ISTRMS    2
OSTRMS    2

```

IP Appl Sock table is (4 of 250) 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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
```

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

If the required hostname is not in the database, add the IP host name using the “Adding an IP Host” on page 3-61 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 03-06-28 21:19:37 GMT Rel 31.0.0
```

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 3-66 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 03-06-19 21:17:04 GMT Rel 31.0.0
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 SS7 Signaling Link” procedure in the *Database Administration Manual - SS7* 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 03-06-28 09:12:36 GMT Rel 31.0.0
ASP          Association      UAPS
ASP1         swbel32          1
ASP2         a2              1
ASP3         a3              1
ASP4         assoc1         10
ASP Table is (4 of 250) 1% full
```

If the association is assigned to an ASP, go to the “Removing an Application Server Process” procedure on page 3-228 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 03-06-27 17:00:36 GMT Rel 31.0.0
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 03-06-19 21:17:04 GMT Rel 31.0.0
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**. If the **ipliml2** parameter is not **m3ua** or **m2pa**, remove the signaling link using the "Removing an SS7 Signaling Link" procedure in the *Database Administration Manual - SS7*. 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 SS7 Signaling Link" procedure in the *Database Administration Manual - SS7*.

NOTE: If the “Adding an SS7 Signaling Link” procedure in the *Database Administration Manual - SS7* 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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-07 11:11:28 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
```

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 3-220 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.

NOTES:

1. If any optional parameters are not specified with the **chg-assoc** command, those values are not changed.
2. For associations assigned to IPLIMx cards, the value of the **adapter** parameter must match the value of the **iplim12** parameter for the signaling link being assigned to the association. For example, if the value of the signaling link's **iplim12** 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 **iplim12** 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.
3. Associations assigned to IPGWx cards can have the values **m3ua** or **sua** for the **adapter** parameter value.
4. 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.

chg-assoc:aname=assoc1:rhost=gw200.nc-tekelec.com:rport=2048

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

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-07 11:11:28 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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
```

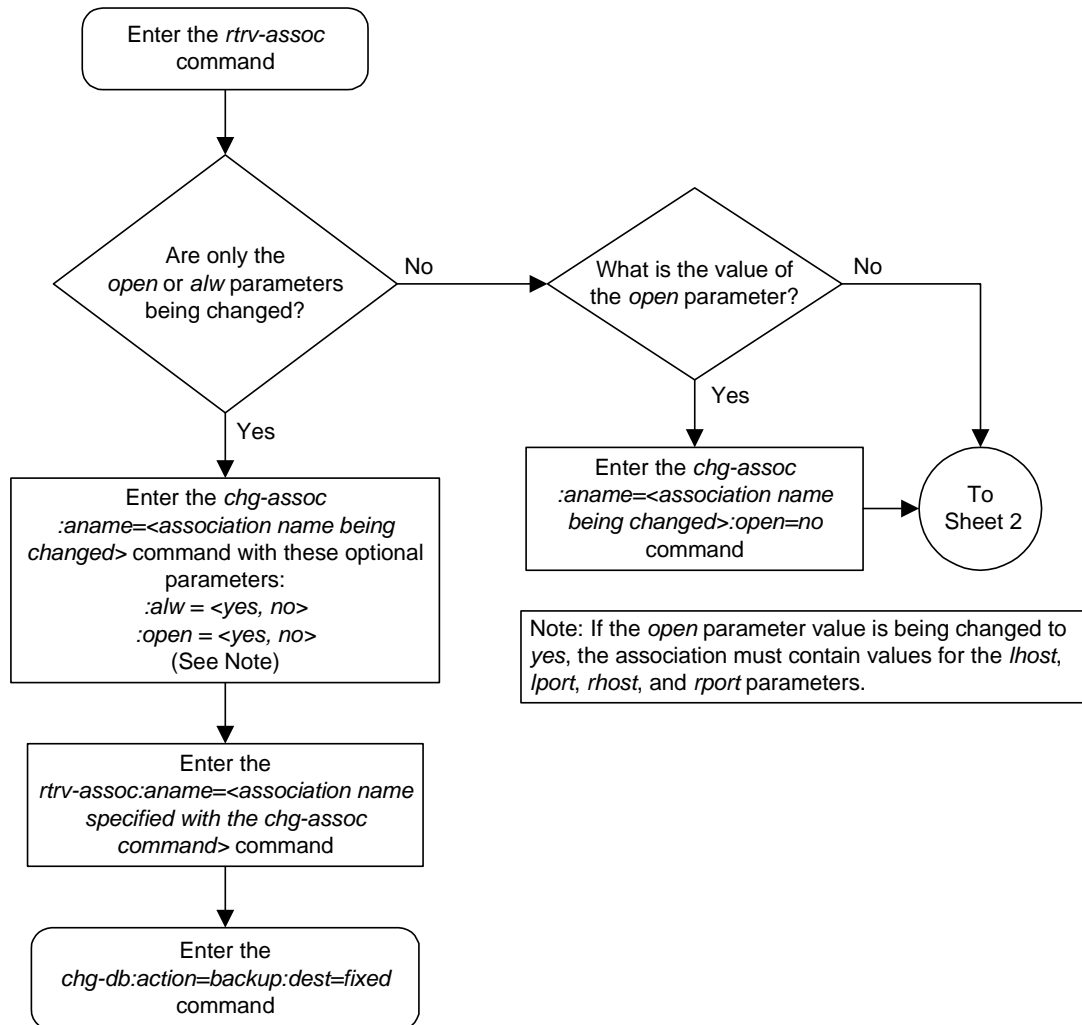
This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME assoc1
LHOST   gw105.nc.tekelec.com
ALHOST  ---
LPORT   1030
RHOST   gw200.nc-tekelec.com
RPORT   2048
OPEN     NO
ALW      NO
PORT     A
ADAPTER  M3UA
VER      M3UA RFC
RMODE    LIN
RMIN     120
RMAX     800
RTIMES   10
CWMIN    3000
ISTRMS   2
OSTRMS   2
IP Appl Sock table is (4 of 250) 1% full
```

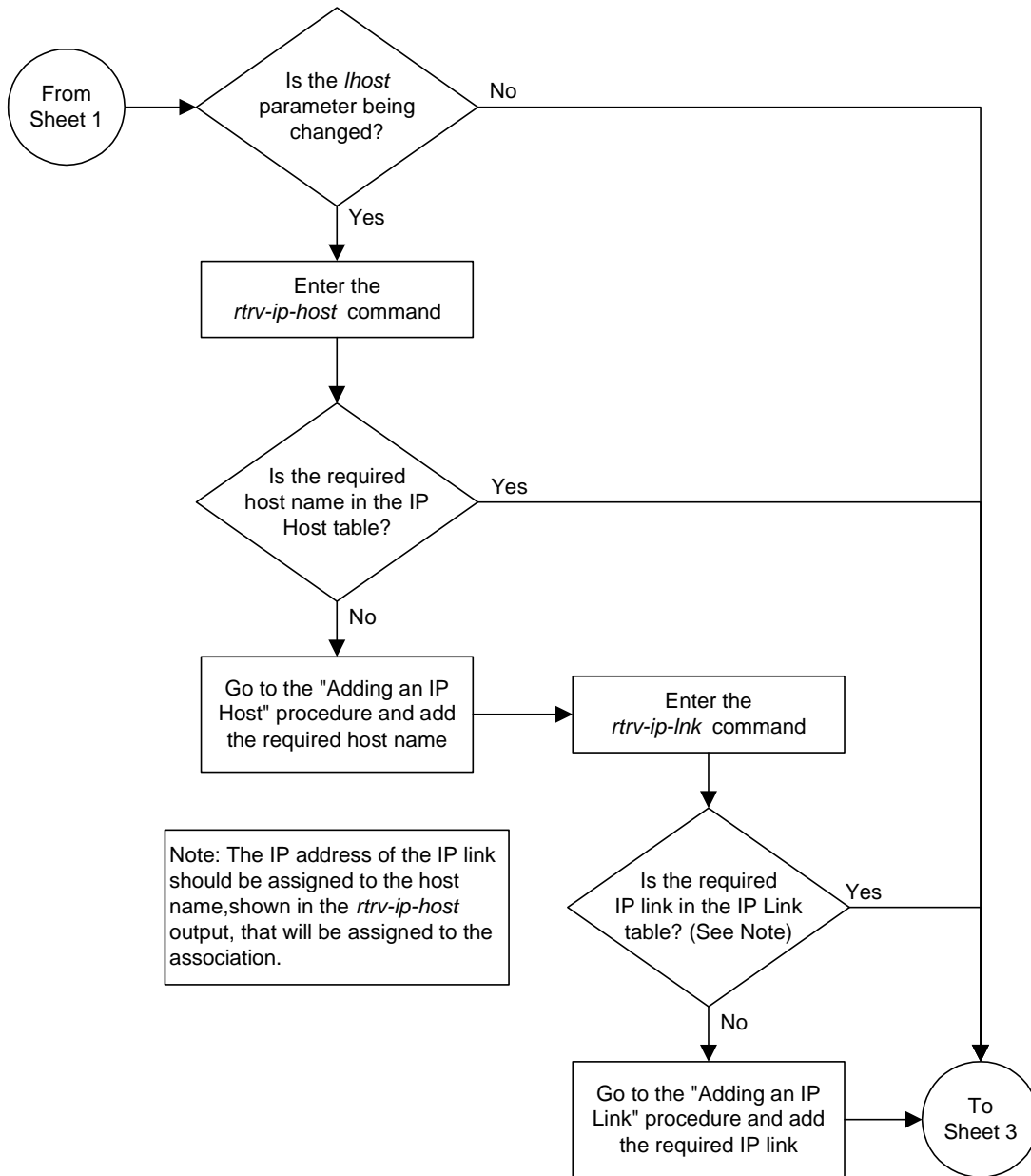
18. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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.
```

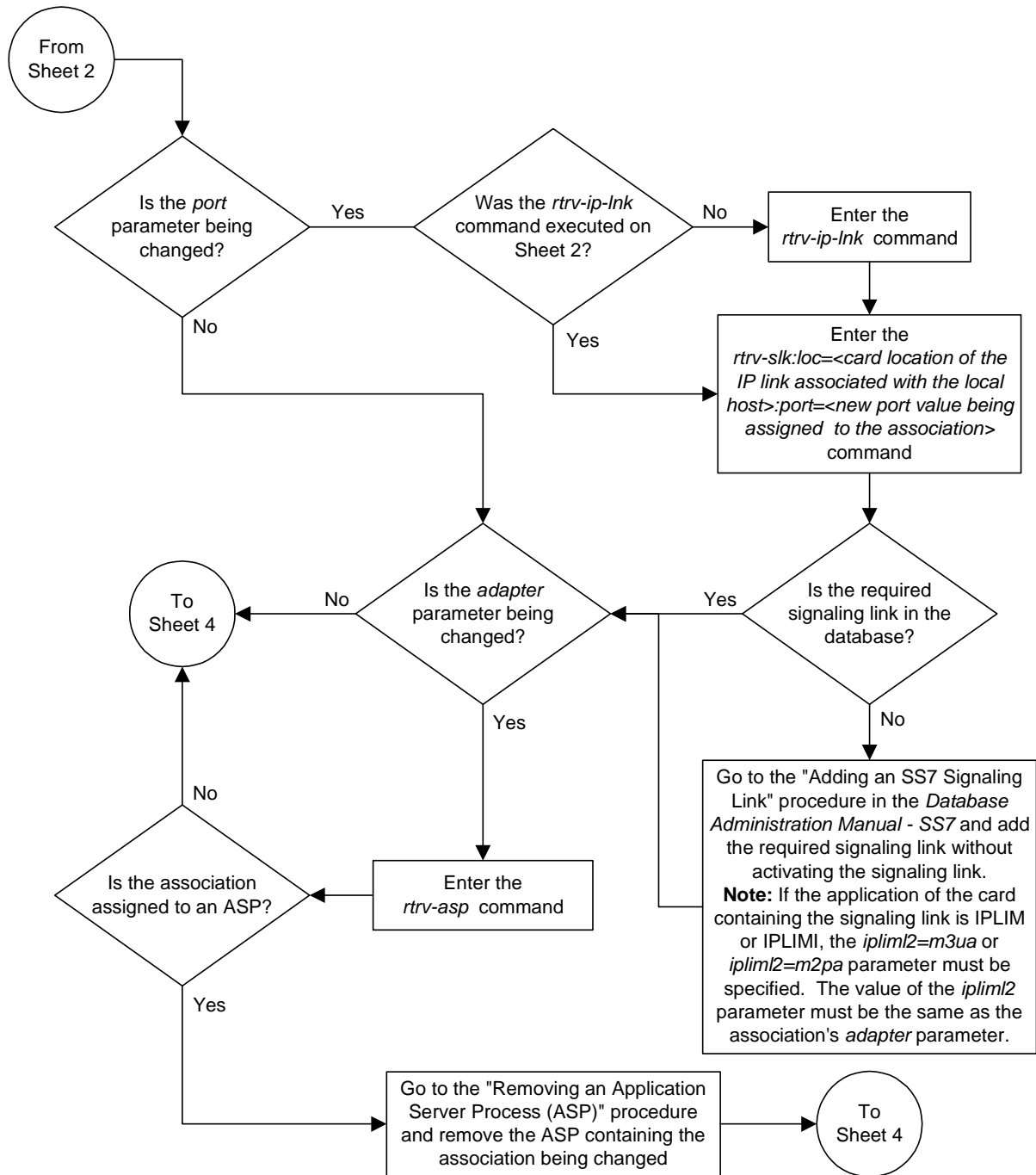
Flowchart 3-23. Changing an Association (Sheet 1 of 9)



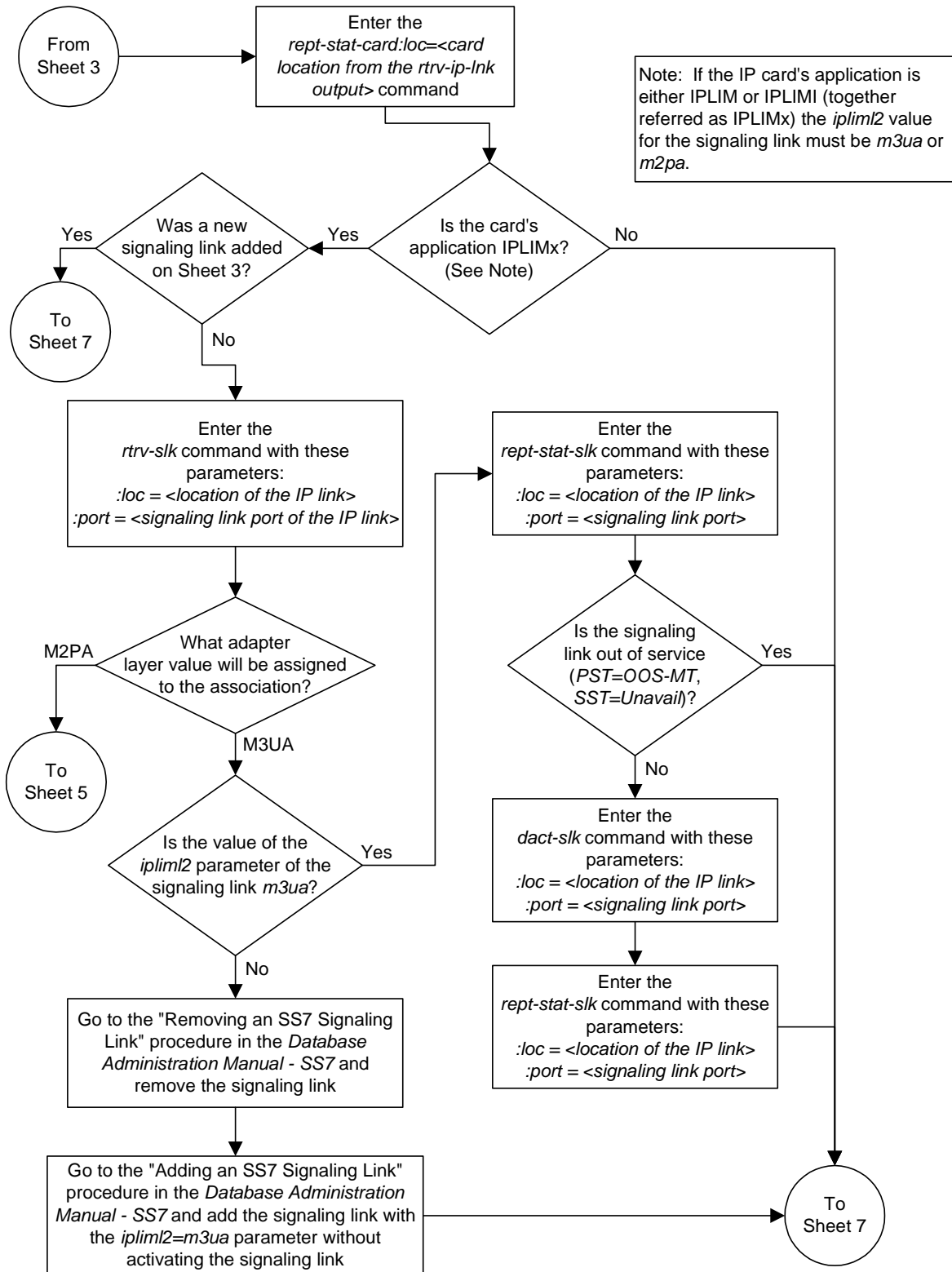
Flowchart 3-23. Changing an Association (Sheet 2 of 9)



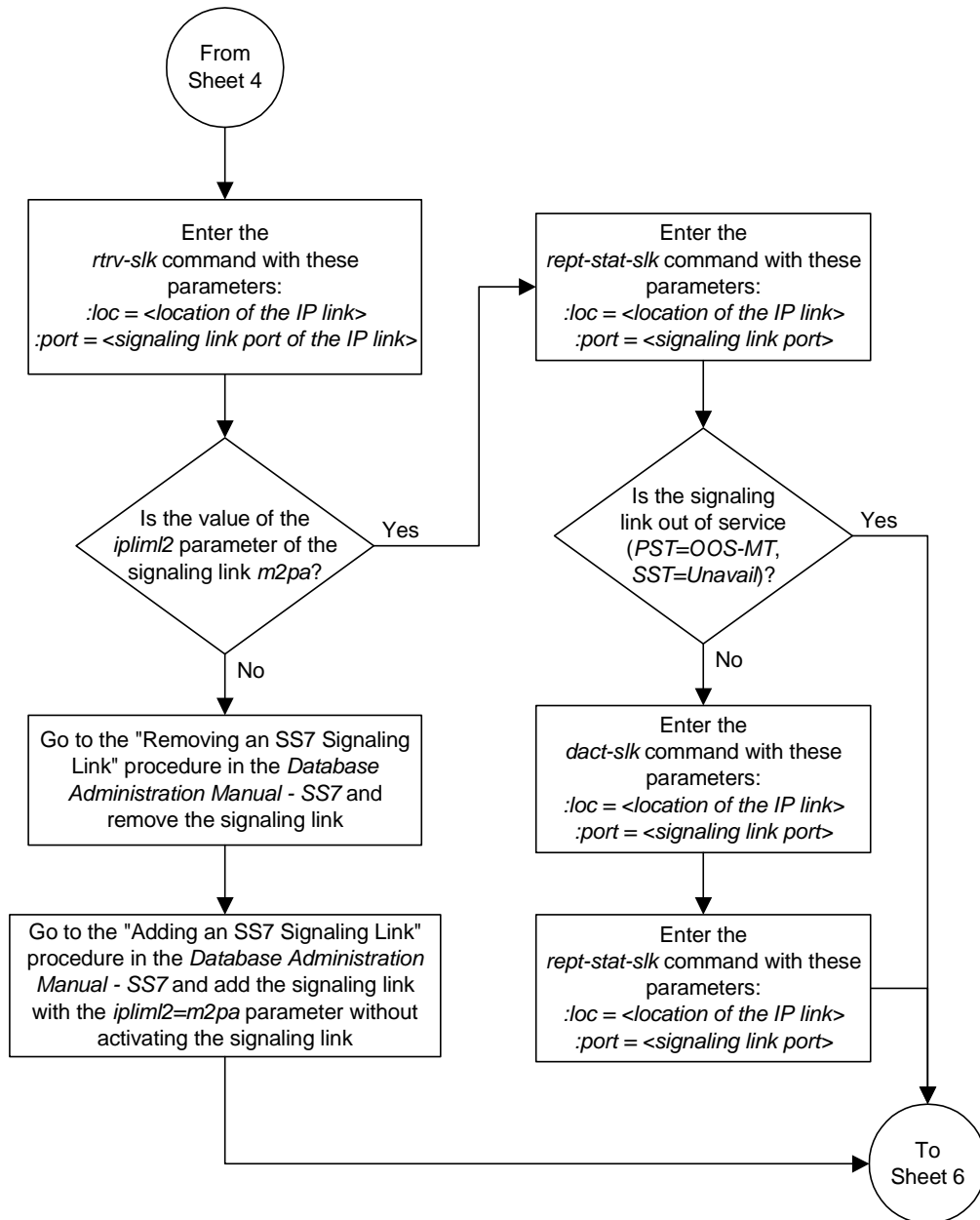
Flowchart 3-23. Changing an Association (Sheet 3 of 9)



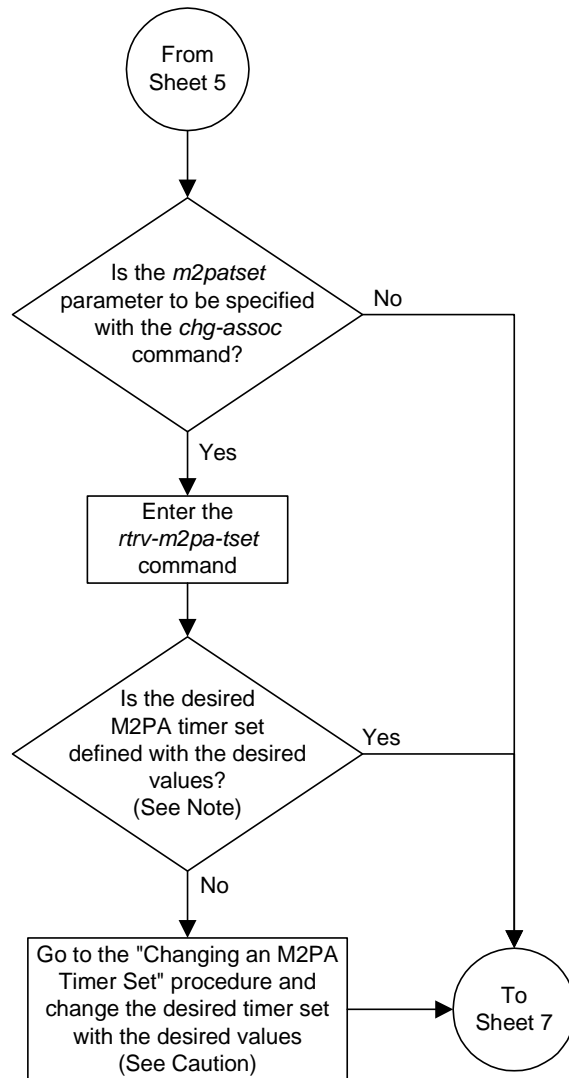
Flowchart 3-23. Changing an Association (Sheet 4 of 9)



Flowchart 3-23. Changing an Association (Sheet 5 of 9)



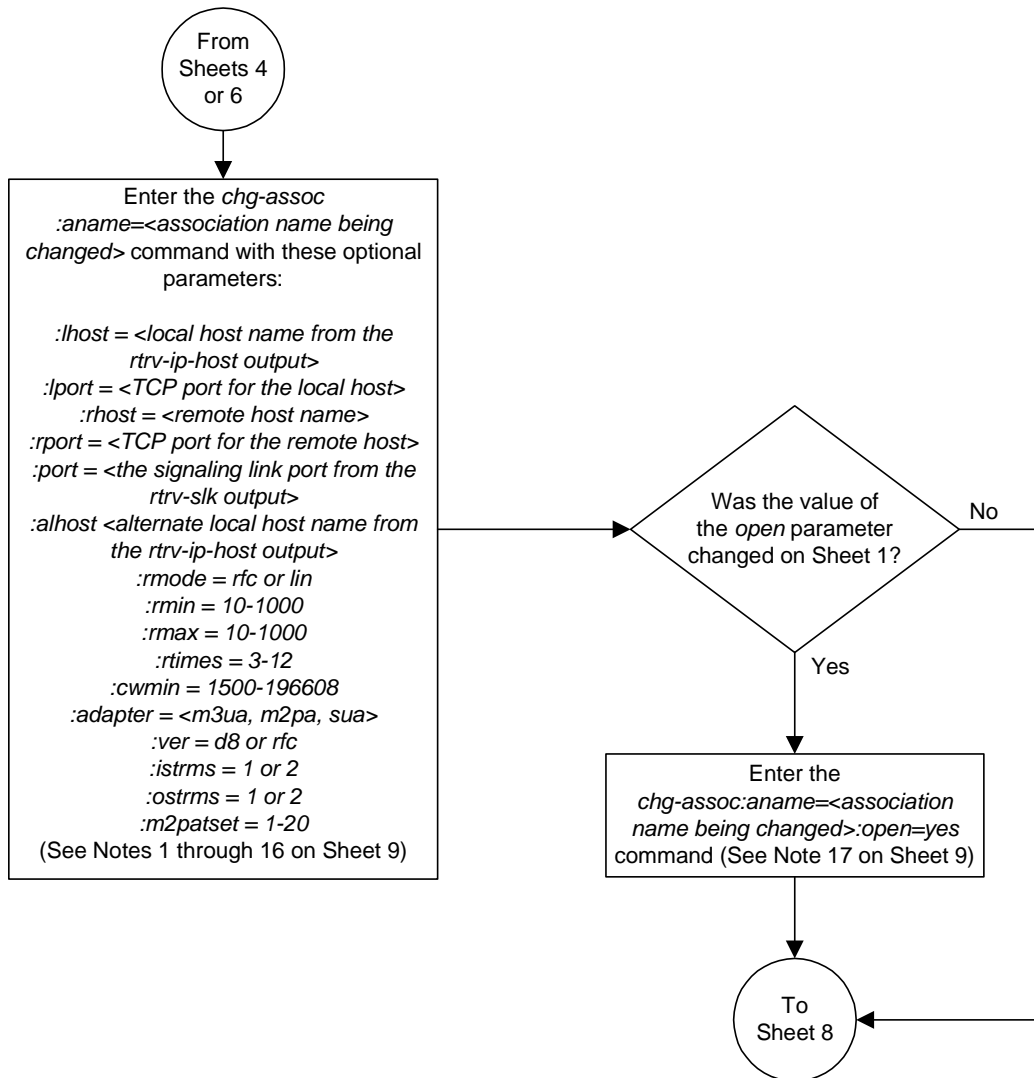
Flowchart 3-23. Changing an Association (Sheet 6 of 9)



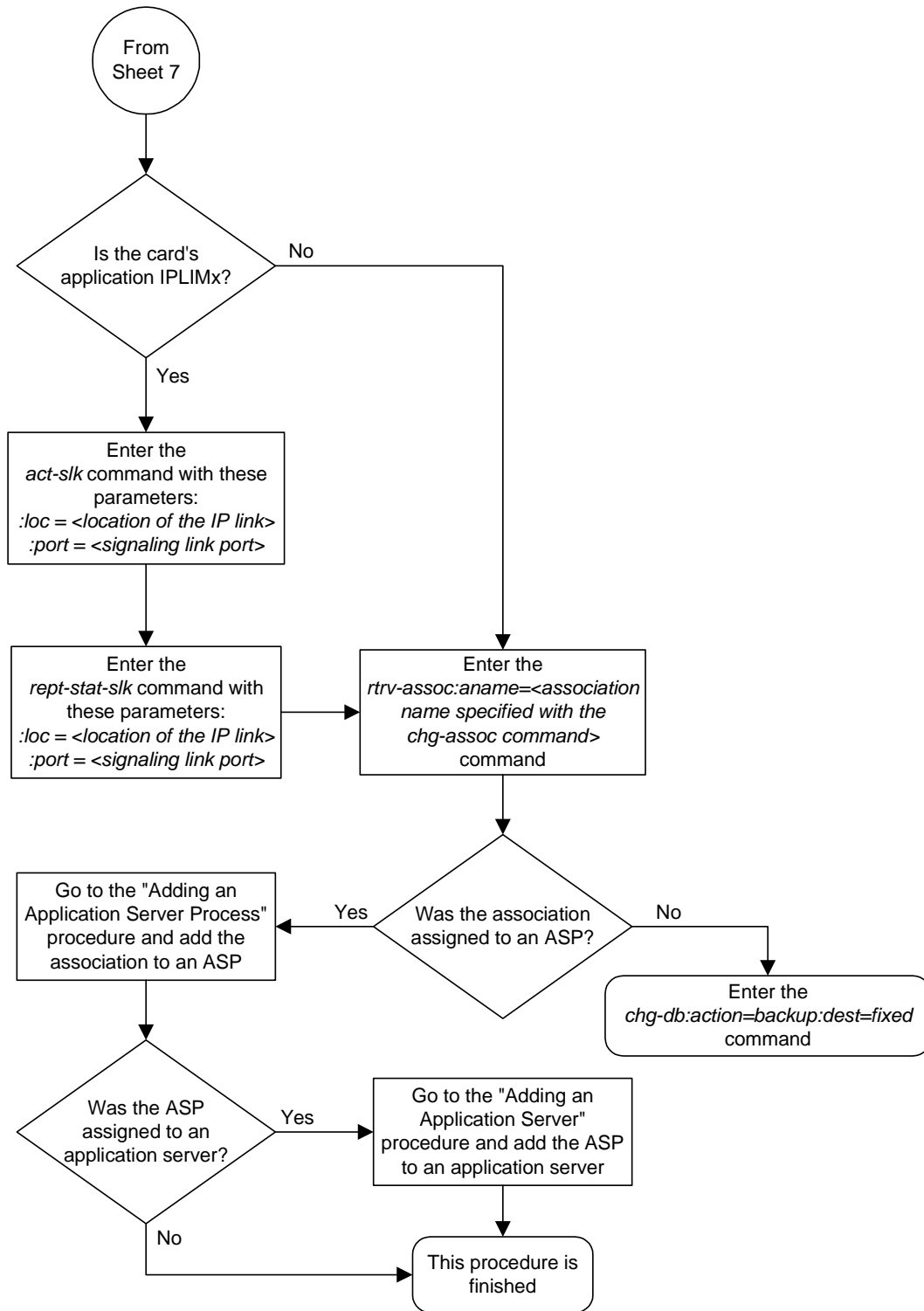
Note: If the *m2patset* parameter will not be specified with the *chg-assoc* command, and the *adapter* parameter value is being changed to *m2pa*, the M2PA timer set 1 will be assigned to the association.

Caution: Changing an M2PA timer set may affect the performance of any associations using the timer set being changed.

Flowchart 3-23. Changing an Association (Sheet 7 of 9)



Flowchart 3-23. Changing an Association (Sheet 8 of 9)



Flowchart 3-23. Changing an Association (Sheet 9 of 9)

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 250 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 input is limited to 150 characters, including the hostnames.
6. 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.
7. 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.
8. 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.
9. The *alhost=none* parameter removes the alternate local host from the specified association, which also removes the multi-homed endpoint capability.
10. 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*.
11. The value of the *rmin* parameter must be less than or equal to the *rmax* parameter value.
12. For associations assigned to the *ss7ipgw* or *ipgwi* applications, the value of the *cwmin* parameter must be less than or equal to 16384.
13. The *ver* parameter cannot be specified for SUA or M2PA connections.
14. Cards running either *ss7ipgw* or *ipgwi* applications can have only the values *m3ua* or *sua* for the *adapter* parameter.
15. The *m2patset* parameter can be specified only with the *adapter=m2pa* parameter, or if the current *adapter* parameter value for the association is *m2pa*.
16. If the *m2patset* 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*).
17. 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 3-190 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 stcp** – provides a summary list of all SCTP instances.

- **sctp -g peps** – displays the peps 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 3-190, or in the **chg-assoc** command description in the *Commands Manual*.

Procedure

1. Display the associations in the database using the **rtrv-assoc** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME swbel32
  LHOST    gw105.nc.tekelec.com
  ALHOST    ---
  LPORT    1030
  RHOST    gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  RPORT    2345
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  M3UA
  VER      M3UA RFC
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2

ANAME a2
  LHOST    gw105.nc.tekelec.com
  ALHOST    ---
  LPORT    1030
  RHOST    gw100.nc.tekelec.com
  RPORT    2345
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  SUA
  VER      SUA DRAFT 3
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2
```

```

ANAME a3
  LHOST    gw105.nc.tekelec.com
  ALHOST   ---
  LPORT    1030
  RHOST    gw106.nc.tekelec.com
  RPORT    2346
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  SUA
  VER      SUA DRAFT 3
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2

ANAME assoc1
  LHOST    gw105.nc.tekelec.com
  ALHOST   ---
  LPORT    1030
  RHOST    gw100.nc.tekelec.com
  RPORT    1030
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  M3UA
  VER      M3UA RFC
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2

IP Appl Sock table is (4 of 250) 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 03-06-28 21:15:37 GMT Rel 31.0.0

IPADDR      HOST
192.1.1.30   GW100.NC.TEKELEC.COM

```

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 03-06-28 21:19:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
PASS: Command sent to card

rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
PING command in progress

rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
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 3-190 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 03-06-28 21:15:37 GMT Rel 31.0.0
PASS: Command sent to card

rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
PASS: Command sent to card

rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0

SCTP command complete
```

8. 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 03-06-28 21:15:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0

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 03-06-28 21:15:37 GMT Rel 31.0.0
PASS: Command sent to card

rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
      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
      rcv timer count = 0
      heartbeat timer count = 244

      none left tosend = 0
      none left rwnd gate = 5
      none left cwnd gate = 8

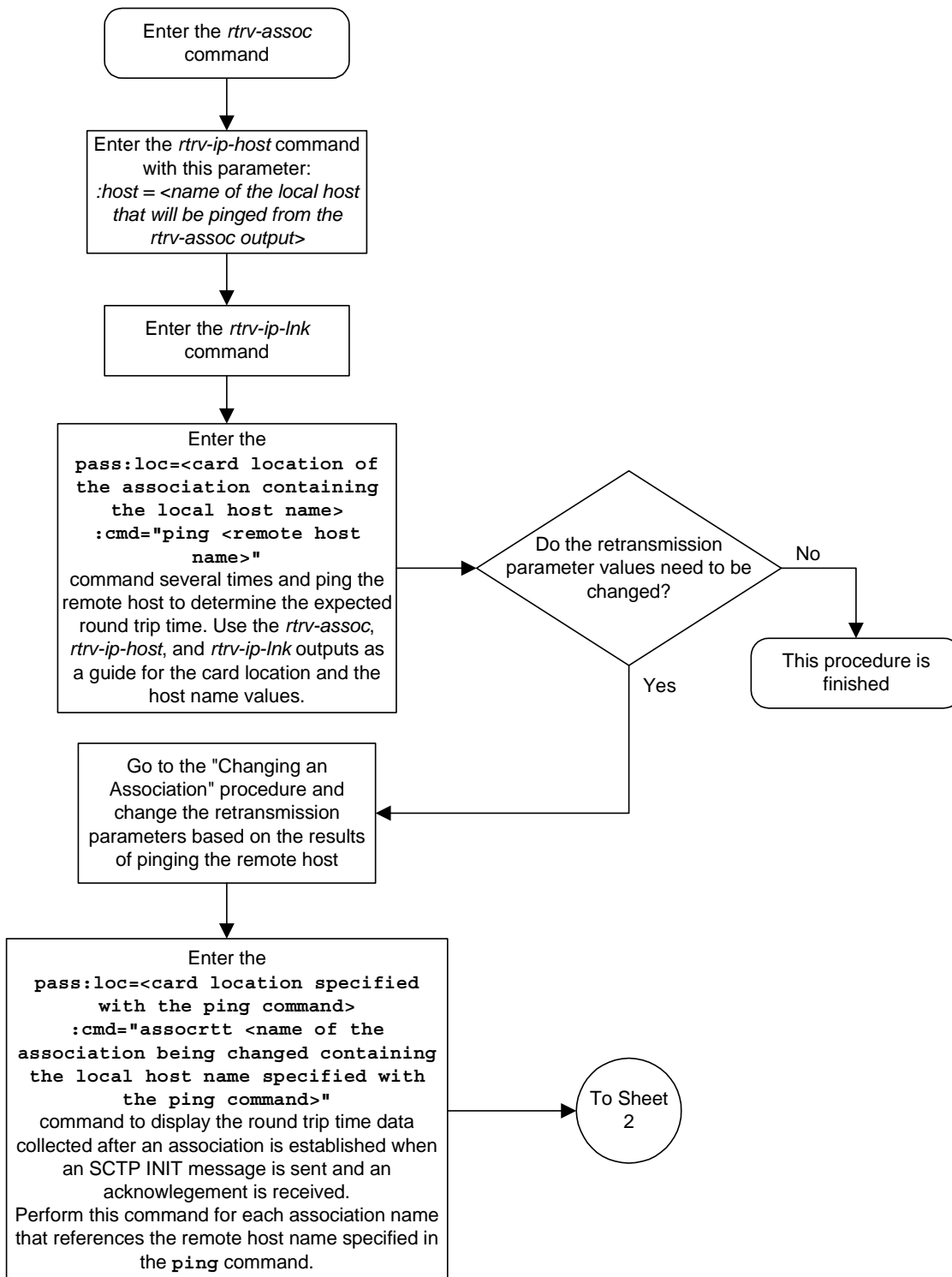
rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0

SCTP command complete
```

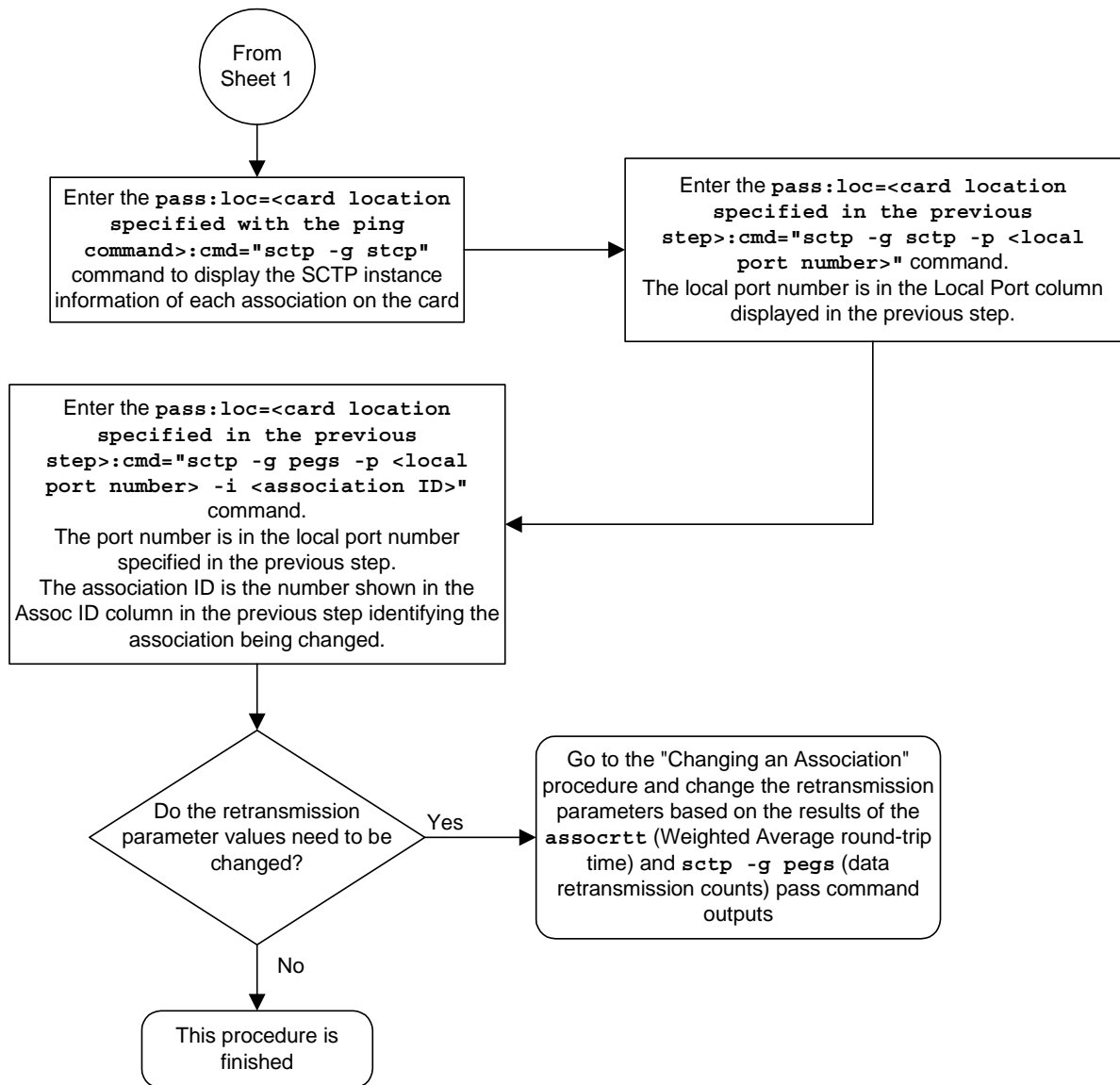
NOTE: The **Weighted Average round-trip time** shown in the **assocrtt** pass command output in step 6, and the data retransmission counts shown in the `sctp -g peps` pass command output in step 9 are used as a guide to determine the appropriate values for the **rmode**, **rmin**, **rmax**, and **rtimes** 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 3-190 and change the retransmission parameters of the association based on the results of the outputs of steps 6 and 9.
-

Flowchart 3-24. Configuring an Association for SCTP Retransmission Control (Sheet 1 of 2)



Flowchart 3-24. 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.
- :srtset** – The timer values in an existing M2PA timer set can be copied to another M2PA timer set, specified by the **tset** parameter. The **srtset** parameter specifies the timer set that is to be copied. If the **srtset** parameter is specified, no other timer values can be specified. The **srtset** 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 03-06-28 21:16:37 GMT Rel 31.0.0
```

```
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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
```

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 03-06-28 21:16:37 GMT Rel 31.0.0
```

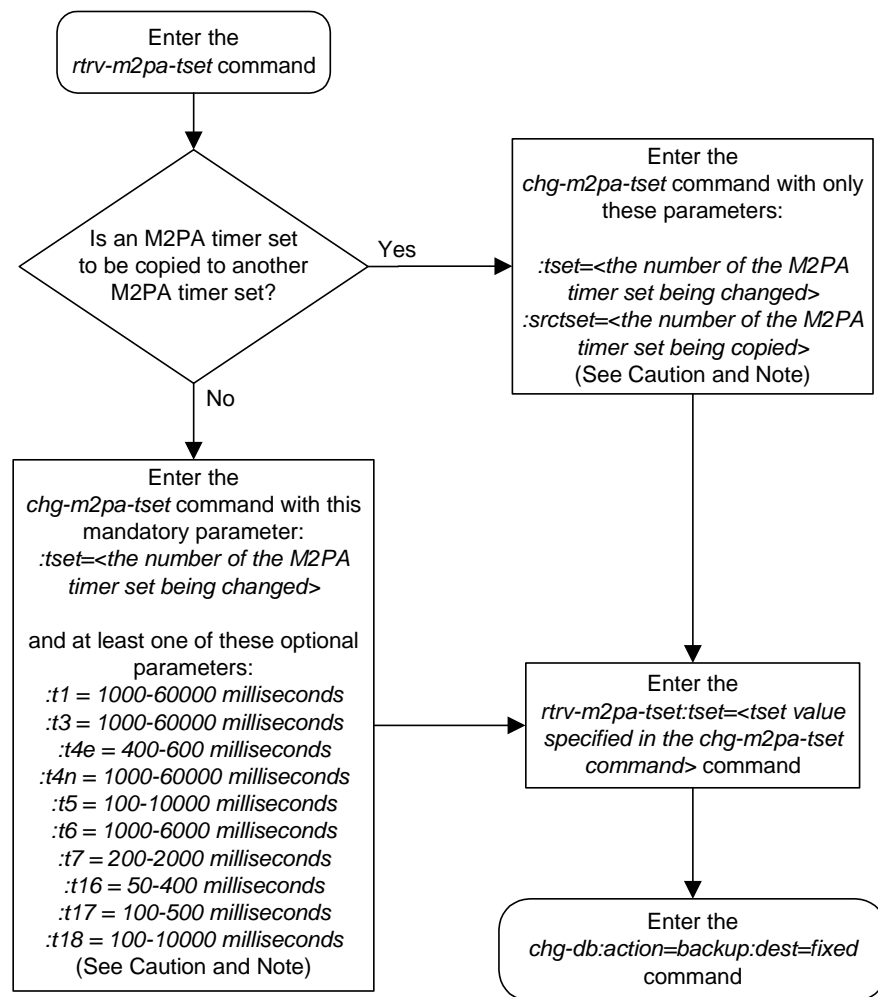
M2PA Timers (in msec)

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 3-25. 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 3-251 to change the UA parameter set value.

Procedure

1. Display the application server processes in the database using the **rtrv-asp** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
ASP          Association      UAPS
ASP1         swbel32          1
ASP2         a2                1
ASP3         a3                1
ASP Table is (3 of 250) 1% full
```

2. Display the associations in the database using the **rtrv-assoc** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME swbel32
LHOST gw105.nc.tekelec.com
ALHOST ---
LPORT 1030
RHOST gw100.ncd-economic-development.southeastern-cooridor-ash.gov
RPORT 2345
OPEN YES
ALW YES
PORT A
ADAPTER M3UA
VER M3UA RFC
RMODE LIN
RMIN 120
RMAX 800
RTIMES 10
CWMIN 3000
ISTRMS 2
```

IP⁷ Secure Gateway Configuration Procedures

```
OSTRMS 2
ANAME a2
LHOST gw105.nc.tekelec.com
ALHOST ---
LPORT 1030
RHOST gw100.nc.tekelec.com
RPORT 2345
OPEN YES
ALW YES
PORT A
ADAPTER M3UA
VER M3UA RFC
RMODE LIN
RMIN 120
RMAX 800
RTIMES 10
CWMIN 3000
ISTRMS 2
OSTRMS 2

ANAME a3
LHOST gw105.nc.tekelec.com
ALHOST ---
LPORT 1030
RHOST gw106.nc.tekelec.com
RPORT 2346
OPEN YES
ALW YES
PORT A
ADAPTER M3UA
VER M3UA RFC
RMODE LIN
RMIN 120
RMAX 800
RTIMES 10
CWMIN 3000
ISTRMS 2
OSTRMS 2

ANAME assoc1
LHOST gw105.nc.tekelec.com
ALHOST ---
LPORT 1030
RHOST gw100.nc.tekelec.com
RPORT 1030
OPEN YES
ALW YES
PORT A
ADAPTER M3UA
VER M3UA RFC
RMODE LIN
RMIN 120
RMAX 800
RTIMES 10
CWMIN 3000
ISTRMS 2
OSTRMS 2
```

IP Appl Sock table is (4 of 250) 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 3-172 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 03-06-28 09:12:36 GMT Rel 31.0.0
ENT-ASP:  MASP A - COMPLTD
```

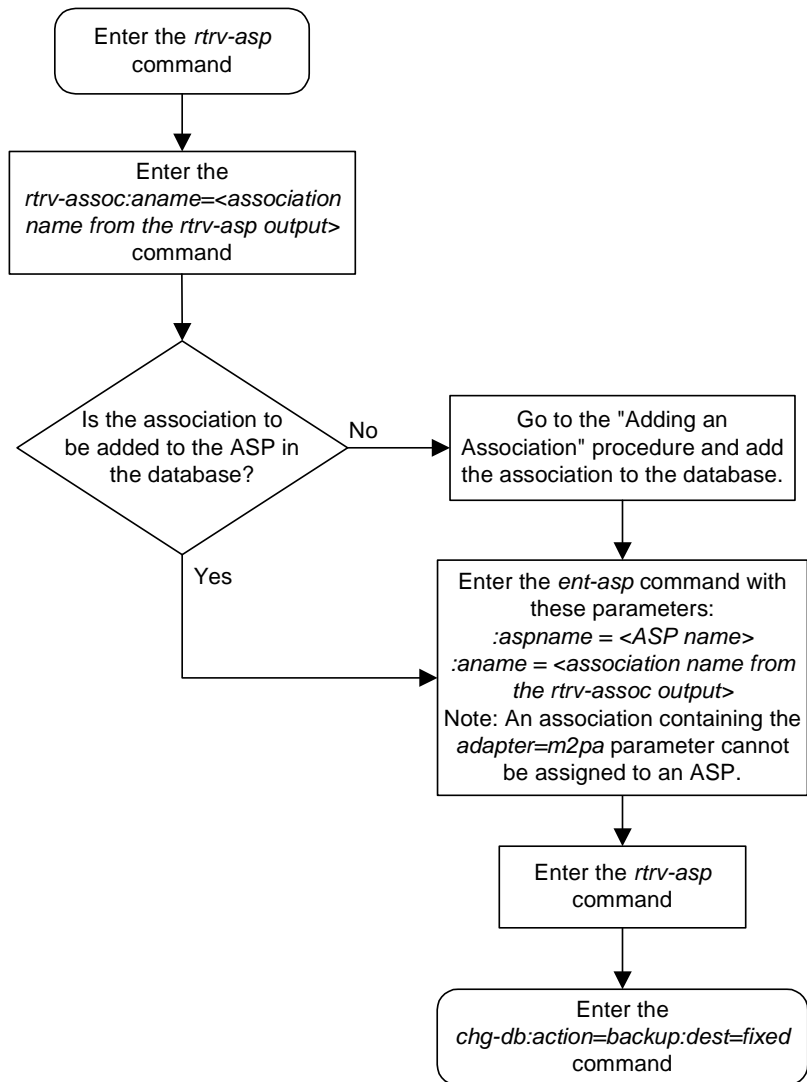
4. Verify the changes using the **rtrv-asp** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
ASP           Association      UAPS
ASP1          swbel32          1
ASP2          a2                1
ASP3          a3                1
ASP4          assoc1           10
ASP Table is (4 of 250) 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. 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 3-247 and remove the application server assignment to the ASP.

Procedure

1. Display the application server processes in the database using the **rtrv-asp** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
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 250) 2% full
```

2. Display the application servers in the database using the **rtrv-as** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
      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 3-247 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 03-06-28 09:12:36 GMT Rel 31.0.0
DLT-ASP:  MASP A - COMPLTD
```

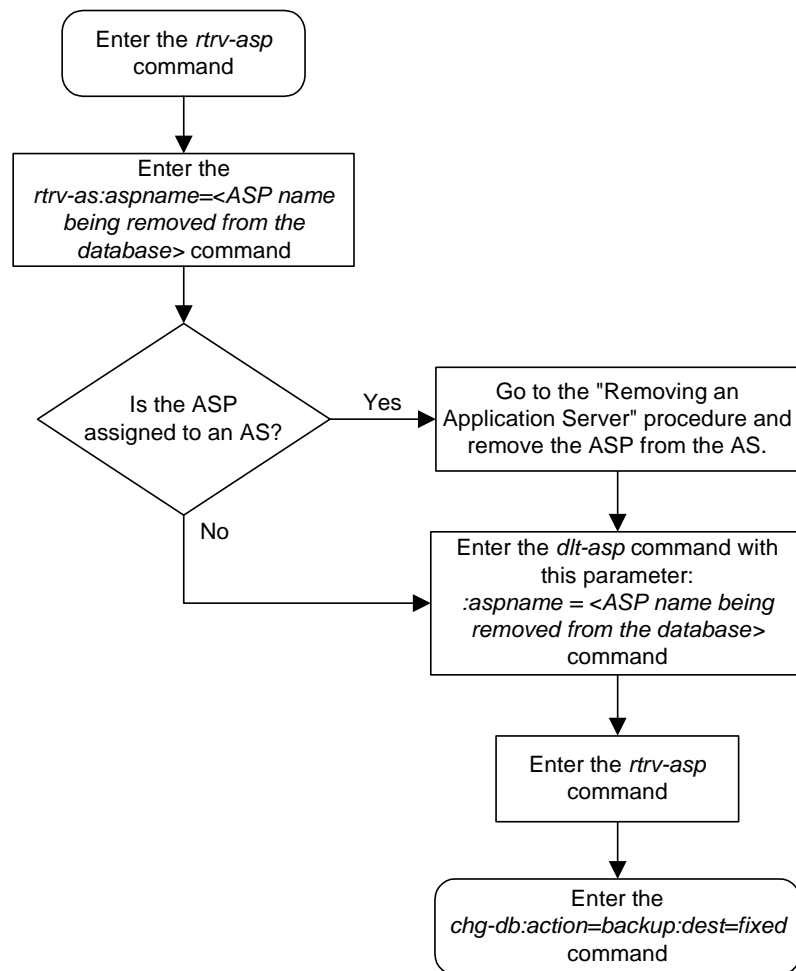
4. Verify the changes using the **rtrv-asp** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
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 250) 2% 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 3-27. 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.

Procedure

1. Display the application server processes in the database using the **rtrv-asp** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
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 250) 2% 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 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME swbel32
  LHOST    gw105.nc.tekelec.com
  ALHOST   ---
  LPORT    1030
  RHOST    gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  RPORT    2345
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  M3UA
  VER      M3UA RFC
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2
```

```
IP Appl Sock table is (4 of 250) 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 03-06-28 09:12:36 GMT Rel 31.0.0
      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 03-06-28 09:12:36 GMT Rel 31.0.0

SET	TIMER	TVALUE	PARM	PVALUE
3	1	10	1	255
3	2	0	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 10-200(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 3-293 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 3-190 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 03-06-28 09:12:36 GMT Rel 31.0.0
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.

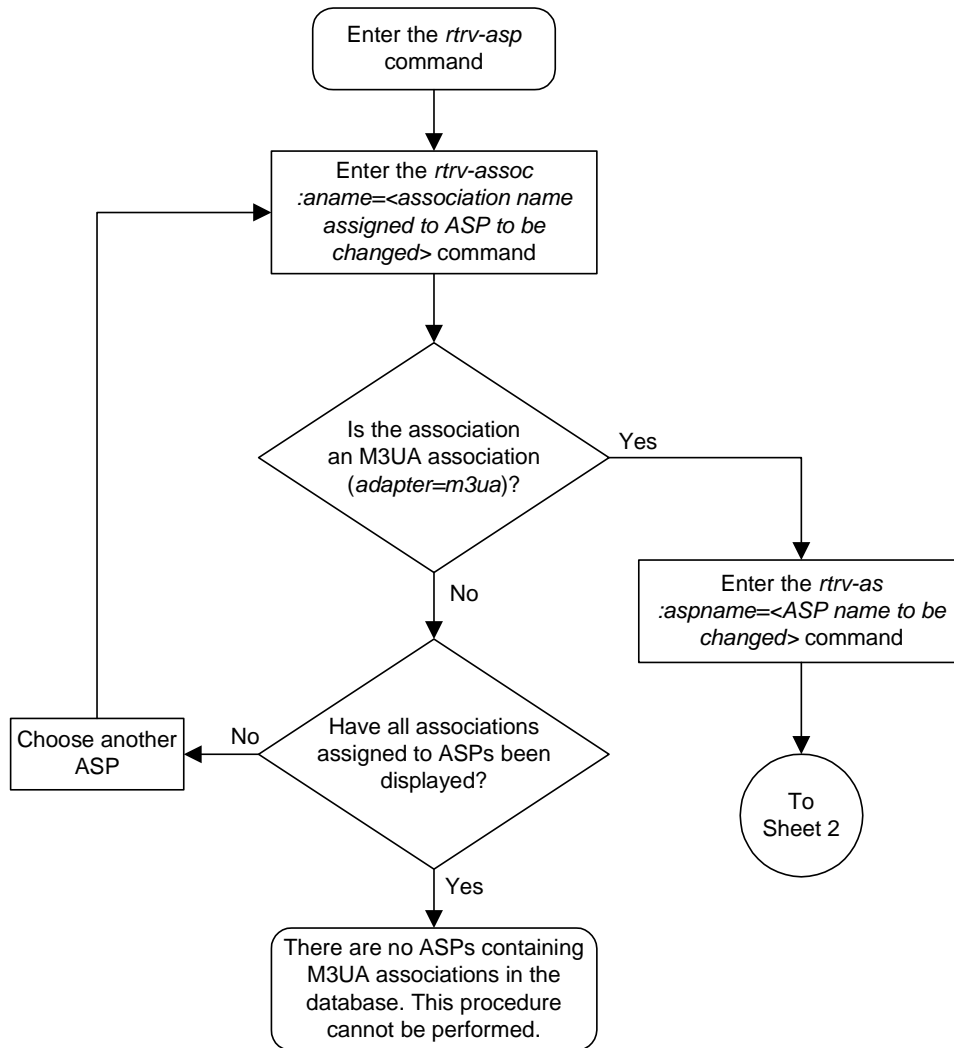
```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
ASP           Association      UAPS
ASP1          swbel32           3
ASP Table is (7 of 250) 2% full
```

-
8. Go to the “Changing an Association” procedure on page 3-190 and change the value of the **open** parameter to **yes**.

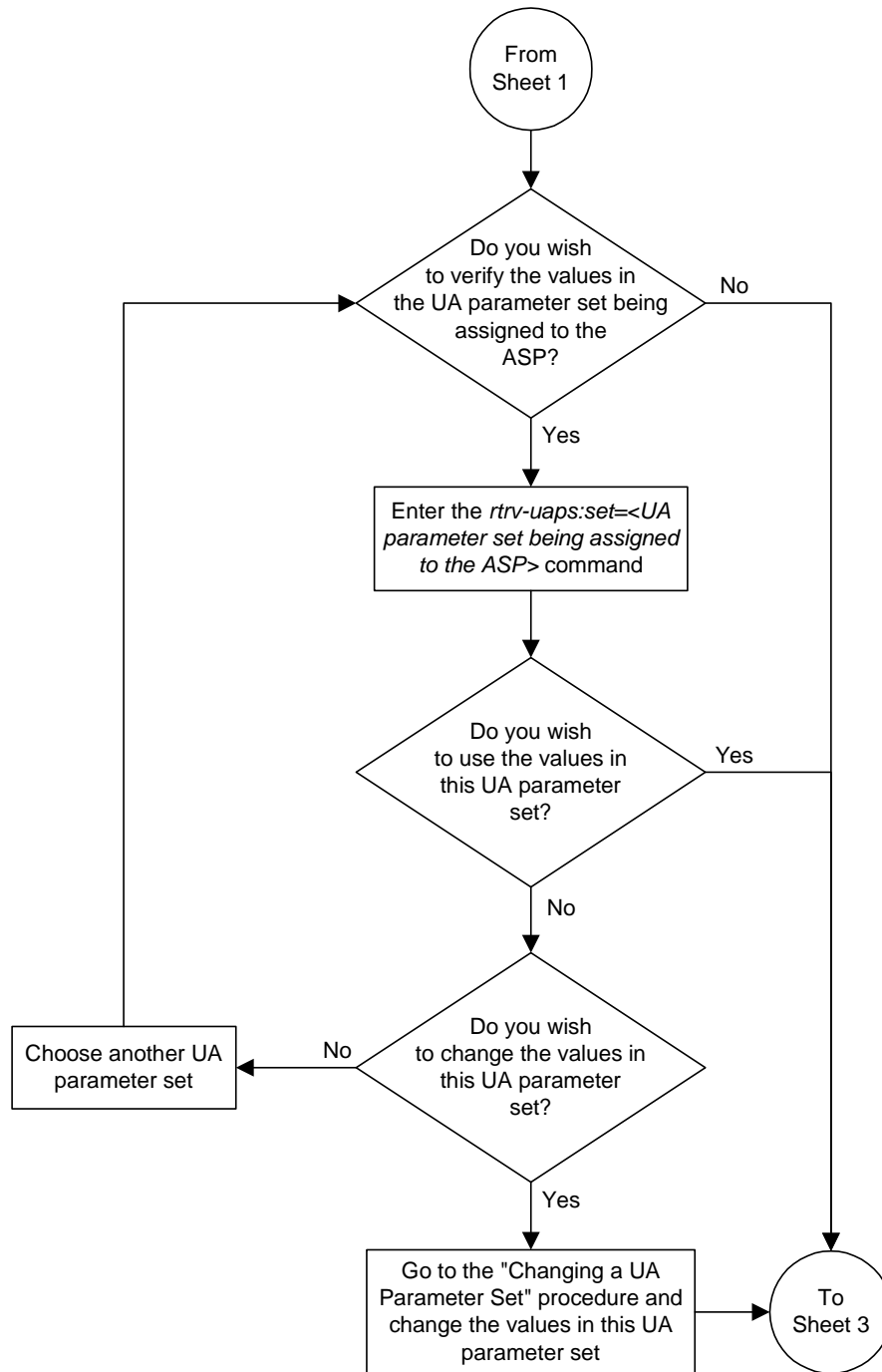
-
9. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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.
```

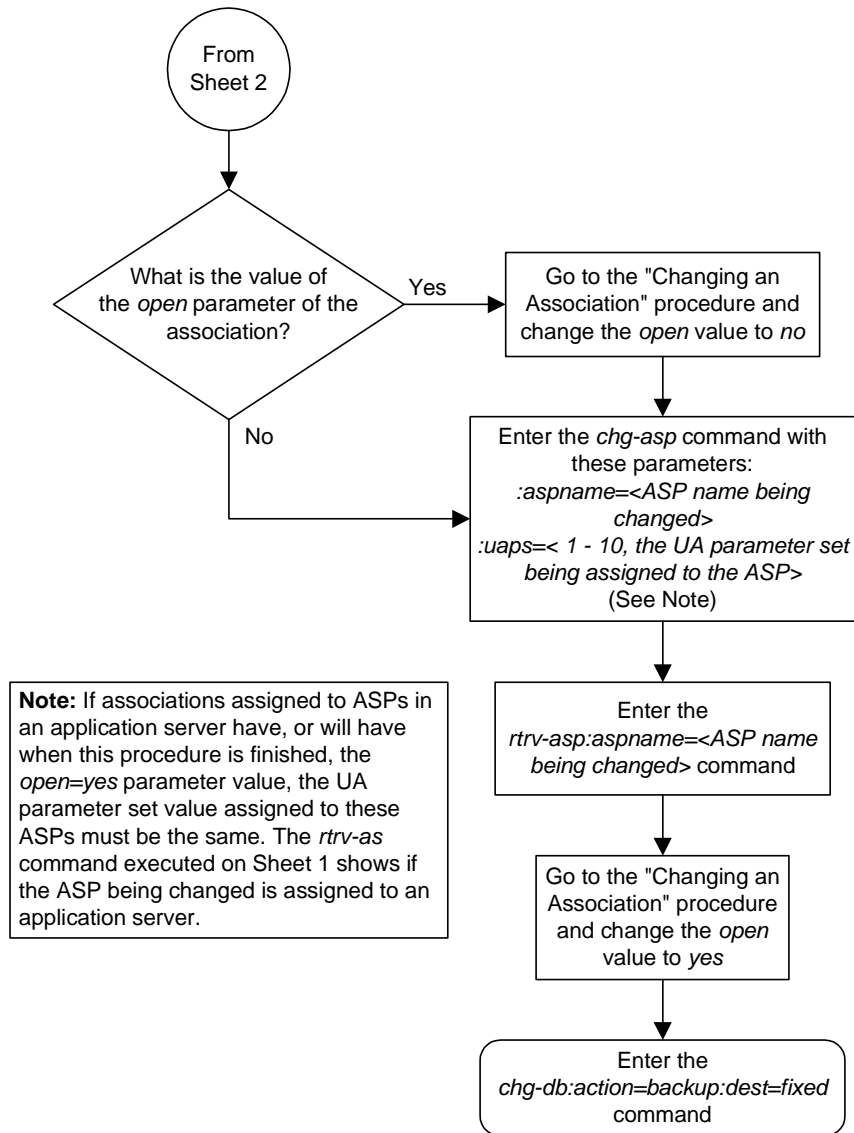
Flowchart 3-28. Changing an Application Server Process (Sheet 1 of 3)



Flowchart 3-28. Changing an Application Server Process (Sheet 2 of 3)



Flowchart 3-28. 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 3-231 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.

Procedure

1. Display the application servers in the database using the **rtrv-as** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
      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 03-06-28 09:12:36 GMT Rel 31.0.0
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 250) 2% 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 3-224 and add the ASP to the database following these rules:

- The **adapter** parameter value of the association assigned to this ASP is the same as the other ASPs in the application server.
- The value of the **open** parameter of the association is **no**.
- The application of the card containing the signaling link assigned to the association is either SS7IPGW or IPGWI.

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 ASPs in the application server. If the UA parameter set assigned to the other ASPs in the application server is not UA parameter set 10, the UA parameter assignment of the ASP being added must be changed using to the “Changing an Application Server Process” procedure on page 3-231.

NOTE: If the ASP was added to the database in step 2, skip steps 3 through 7, and go to step 8.

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 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME assoc1
  LHOST  gw105.nc.tekelec.com
  ALHOST ---
  LPORT  1030
  RHOST  gw100.nc.tekelec.com
  RPORT  1030
  OPEN   YES
  ALW    YES
  PORT   A
  ADAPTER SUA
  VER    SUA DRAFT 3
  RMODE  LIN
  RMIN   120
  RMAX   800
  RTIME  10
  CWMIN  3000
  ISTRMS 2
  OSTRMS 2
IP Appl Sock table is (4 of 250) 1% full
```

4. Display the IP address assigned to the LHOST 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 03-06-28 21:15:37 GMT Rel 31.0.0

IPADDR      HOST
192.1.1.10   GW105.NC.TEKELEC.COM
```

5. Display the IP links in the database by entering the **rtrv-ip-lnk** command. The following is an example of the possible output.

```
rlghncxa03w 03-06-28 21:19:37 GMT Rel 31.0.0
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
```

- 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 5 corresponding to the IP address shown in the **rtrv-ip-host** output in step 4.

rept-stat-card:loc=1201

This is an example of the possible output.

```
rlghncxa03w 03-06-27 17:00:36 GMT Rel 31.0.0
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 3-224 and add a new ASP to the database following these rules:

- The adapter parameter value of the association assigned to this ASP is the same as the other ASPs in the AS.
- The value of the **open** parameter of the association is **no**.
- The application of the card containing the signaling link assigned to the association is either SS7IPGW or IPGWI.

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 ASPs in the application server. If the UA parameter set assigned to the other ASPs in the application server is not UA parameter set 10, the UA parameter assignment of the ASP being added must be changed using to the "Changing an Application Server Process" procedure on page 3-231.

NOTE: If the value of the **open** parameter shown in step 3 is **no**, skip this step and go to step 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 03-06-28 09:12:36 GMT Rel 31.0.0
CHG-ASSOC: MASP A - COMPLTD;
```

8. 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 03-06-28 09:12:36 GMT Rel 31.0.0
ENT-AS: MASP A - COMPLTD;
```

9. Verify the changes using the **rtrv-as** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
```

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 8 was added as a result of the actions in either steps 2 or 6, or does not contain an M3UA association, skip this step and go to step 11.

10. 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 9, 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 3-231 and change the UAPS value of the ASP that was specified in step 8.
-

11. 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
```

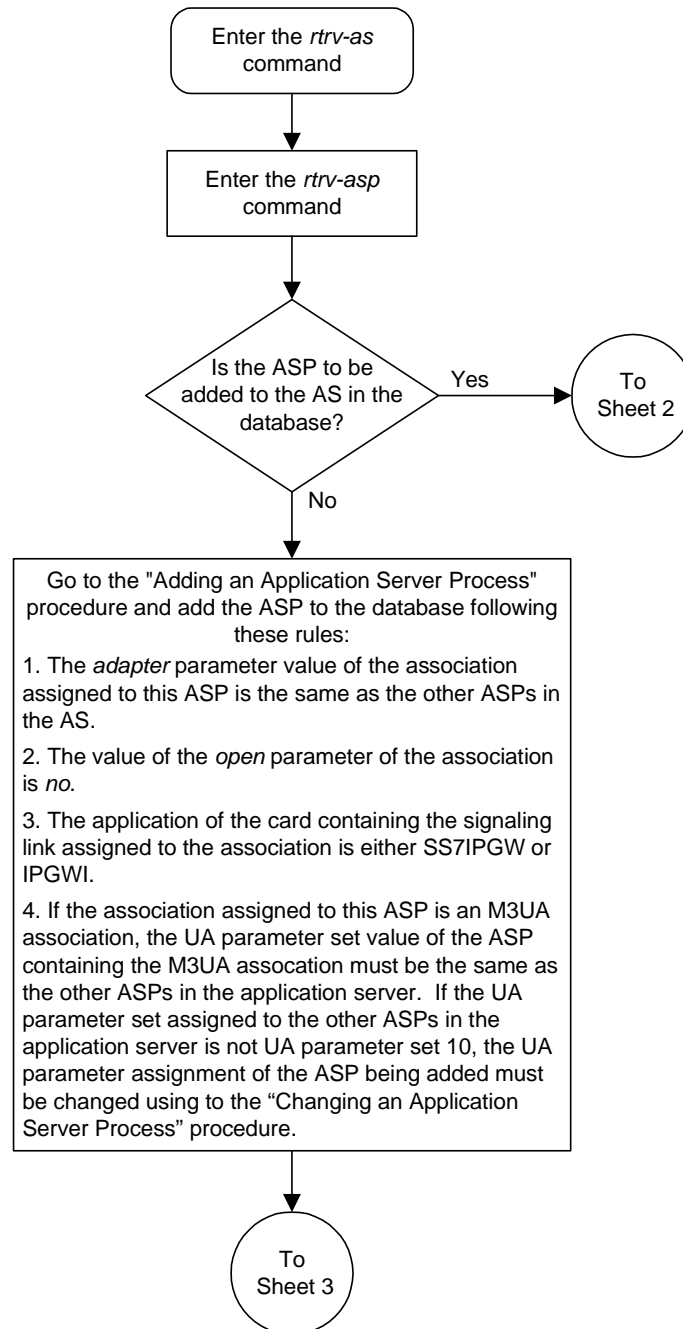
When this command has successfully completed, this message should appear.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
CHG-ASSOC: MASP A - COMPLTD;
```

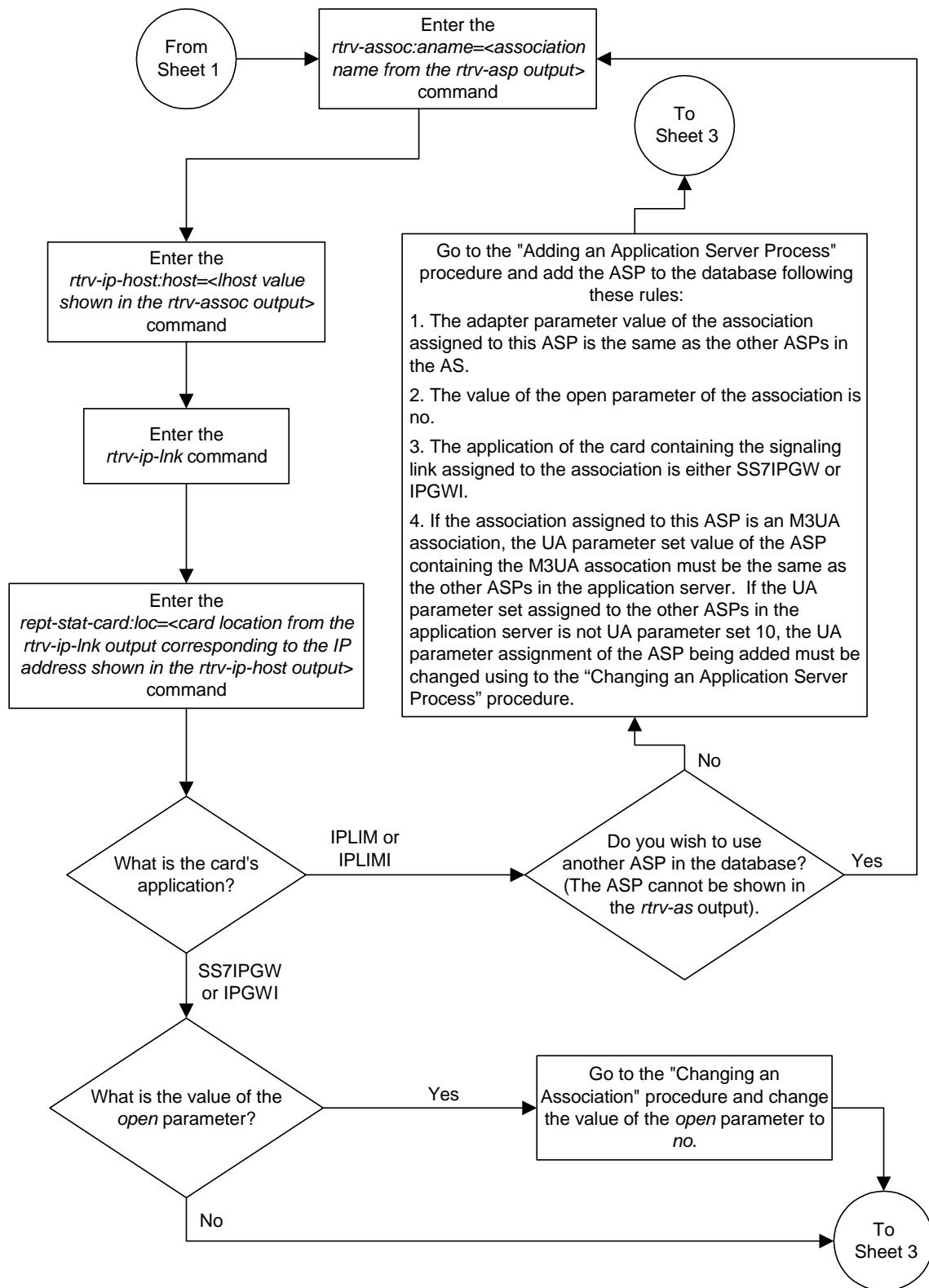
12. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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.
```

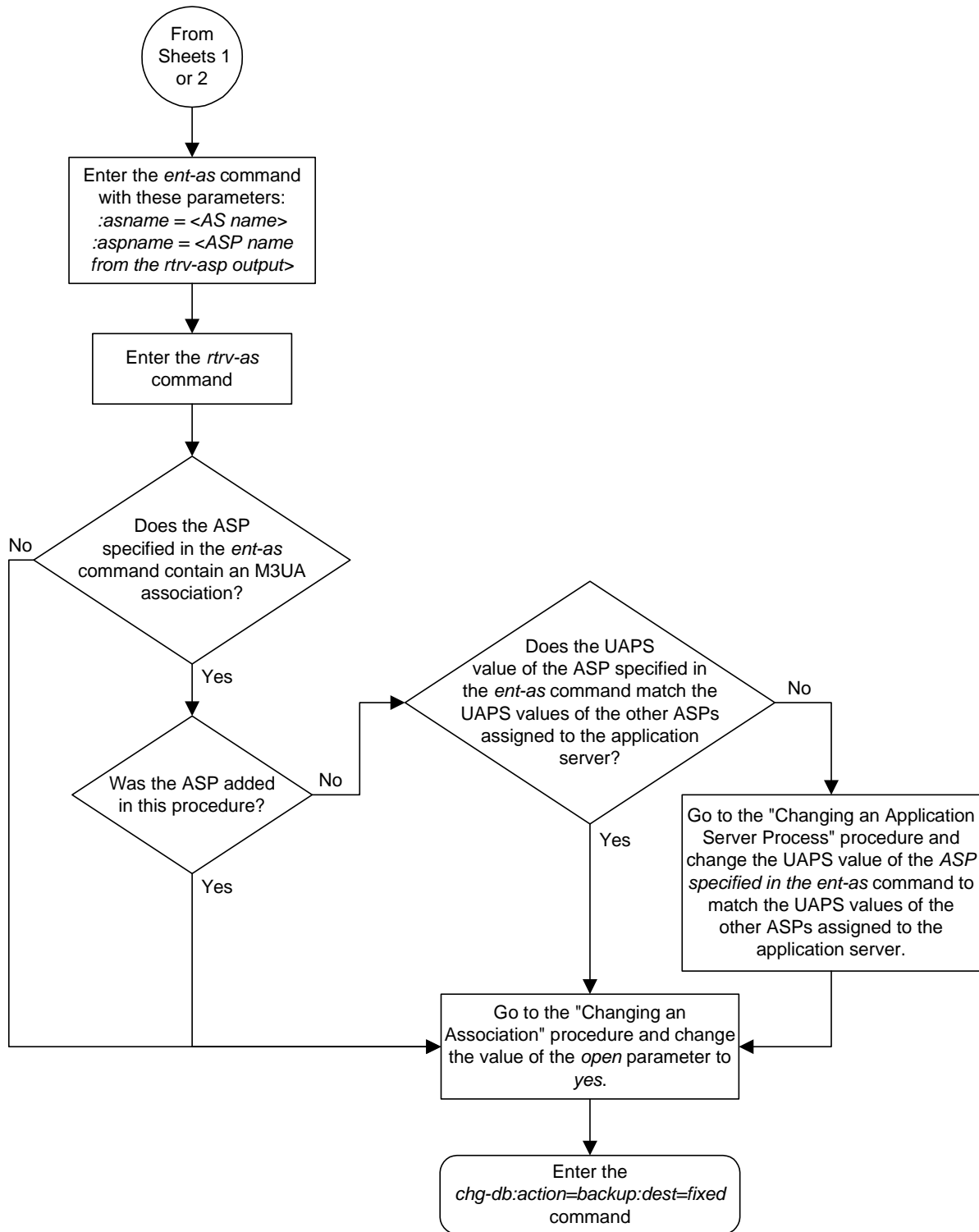
Flowchart 3-29. Adding an Application Server (Sheet 1 of 3)



Flowchart 3-29. Adding an Application Server (Sheet 2 of 3)



Flowchart 3-29. Adding an Application Server (Sheet 3 of 3)



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.

Procedure

1. Display the application servers in the database using the **rtrv-as** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
      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 03-06-28 09:12:36 GMT Rel 31.0.0
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 250) 2% 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 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME assoc1
  LHOST    gw105.nc.tekelec.com
  ALHOST   ---
  LPORT    1030
  RHOST    gw100.nc.tekelec.com
  RPORT    1030
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  M3UA
  VER      M3UA RFC
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2
IP Appl Sock table is (4 of 250) 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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
ENT-AS: MASP A - COMPLTD;
```

6. Verify the changes using the **rtrv-as** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
      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
```

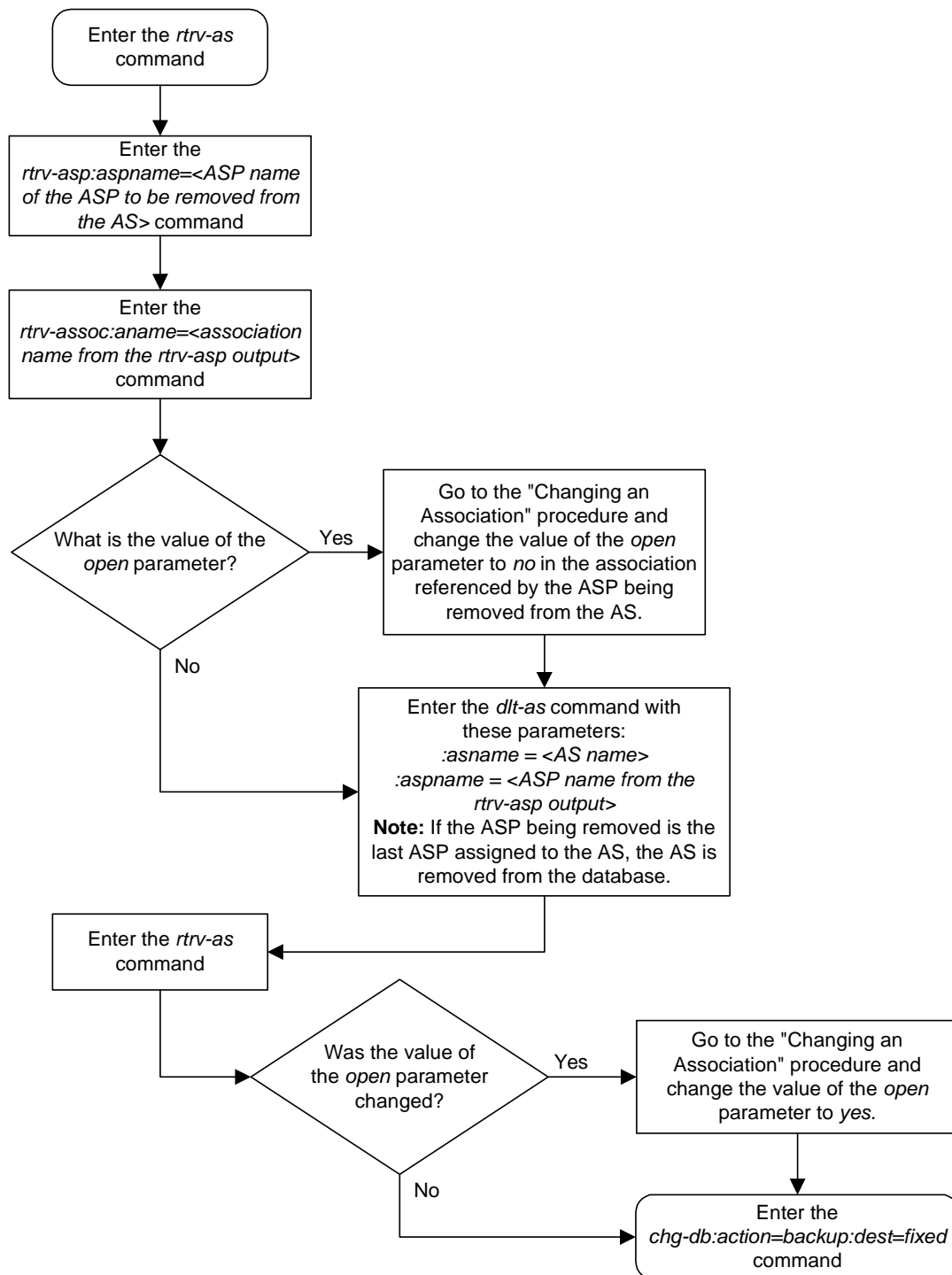
When this command has successfully completed, this message should appear.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
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 3-30. 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 3-247 and remove the ASP from the application server, then go to the "Adding an Application Server" procedure on page 3-238 and add the new ASP to the application server.

Procedure

1. Display the application servers in the database using the **rtrv-as** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
      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 03-06-28 09:12:36 GMT Rel 31.0.0
ASP      Association      UAPS
ASP1     swbel32                1
ASP Table is (7 of 250) 2% 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 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME swbel32
  LHOST    gw105.nc.tekelec.com
  ALHOST   ---
  LPORT    1030
  RHOST    gw100.ncd-economic-development.southeastern-cooridor-ash.gov
  RPORT    2345
  OPEN     YES
  ALW      YES
  PORT     A
  ADAPTER  M3UA
  VER      M3UA RFC
  RMODE    LIN
  RMIN     120
  RMAX     800
  RTIMES   10
  CWMIN    3000
  ISTRMS   2
  OSTRMS   2
IP Appl Sock table is (4 of 250) 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=swbel32:open=no
```

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

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
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.

5. Repeat steps 2 through 4 for all ASPs assigned to the application server being changed.
-

6. Change the application server in the database using the **chg-as** command. For this example, enter this command

```
chg-as:asname=as1:mode=override
```

This is an example of possible inputs and outputs:

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
CHG-AS: MASP A - COMPLTD;
```

7. Verify the changes using the **rtrv-as** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
      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.

8. 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=swbel32:open=yes
```

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

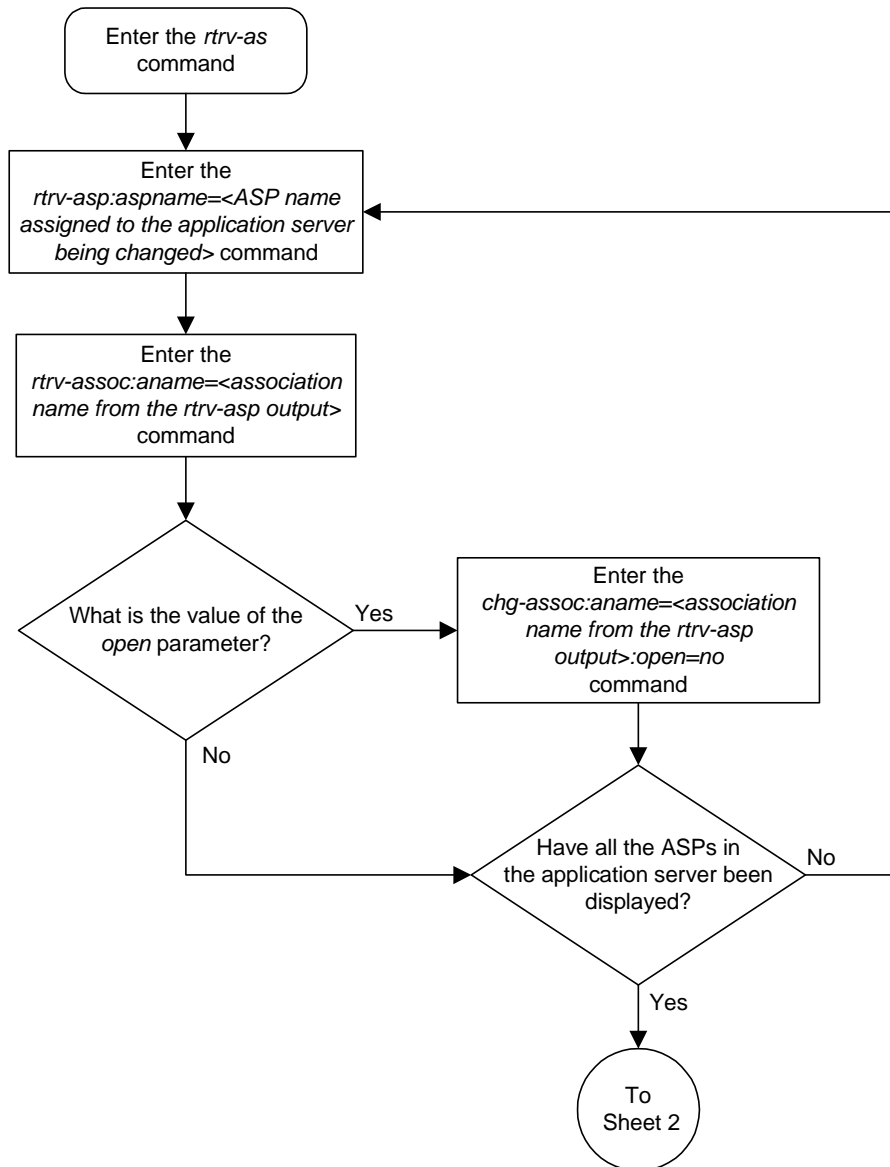
```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
CHG-ASSOC: MASP A - COMPLTD;
```

Repeat this step for all associations that were changed in step 4.

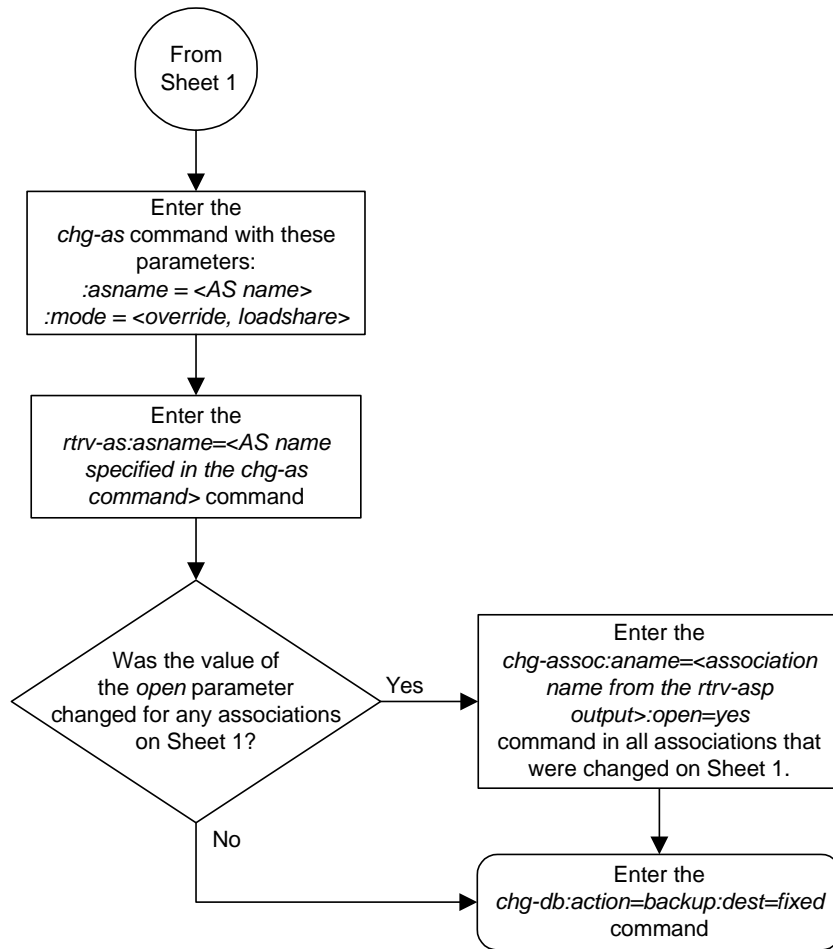
-
9. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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 3-31. Changing an Application Server (Sheet 1 of 2)



Flowchart 3-31. 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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
ENT-NA: MASP A - COMPLTD
```

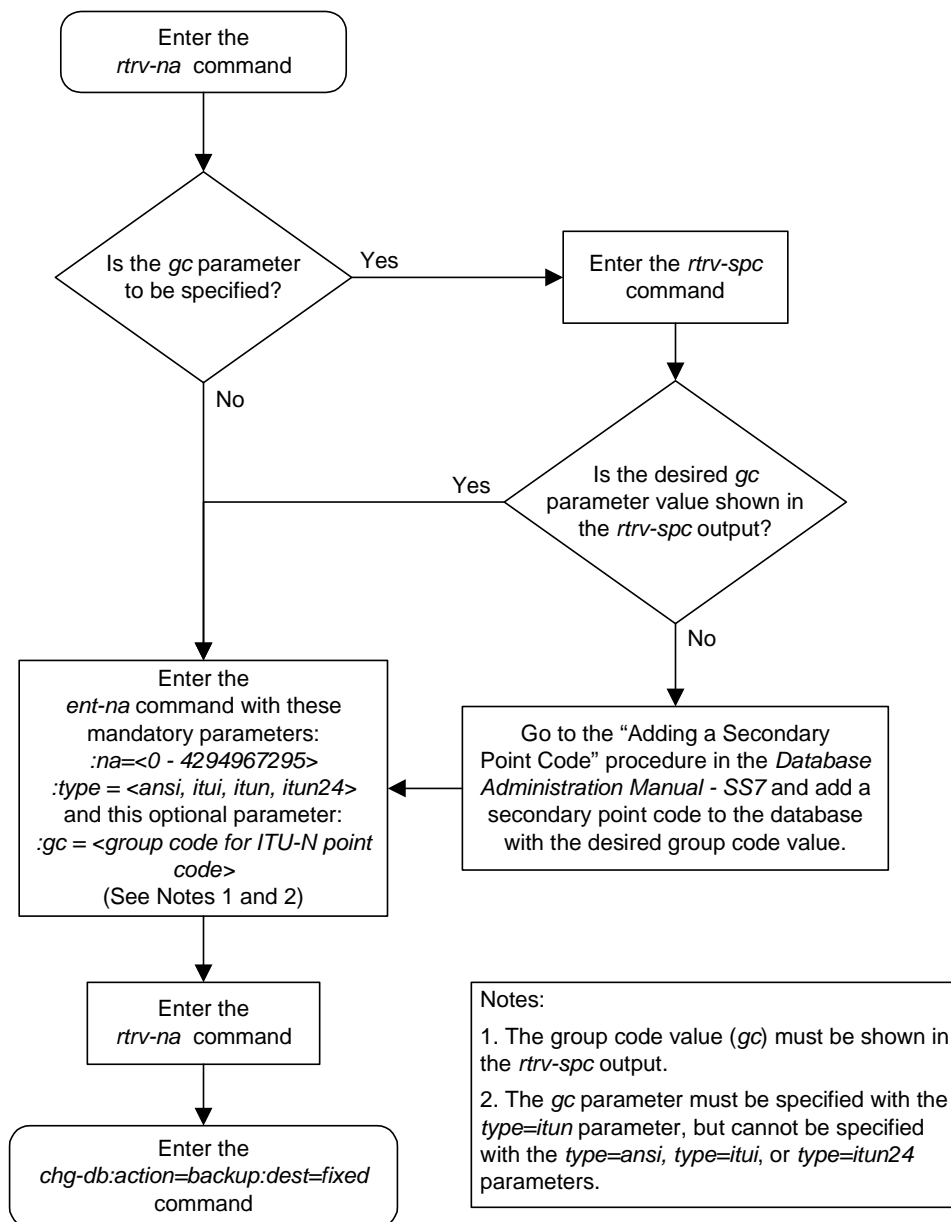
4. Verify the changes using the **rtrv-na** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
TYPE      GC      NA
ANSI      --      100
ITUI      --      1000
ITUN      UK      150000
ITUN      FR      4000000000
ITUN      GE      1000000000
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 3-32. 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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
DLT-NA:  MASP A - COMPLTD
```

3. Verify the changes using the **rtrv-na** command. This is an example of possible output.

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
TYPE      GC      NA
ITUI      --      1000
ITUN      UK      150000
ITUN      GE      1000000000
ITUN24    --      3
```

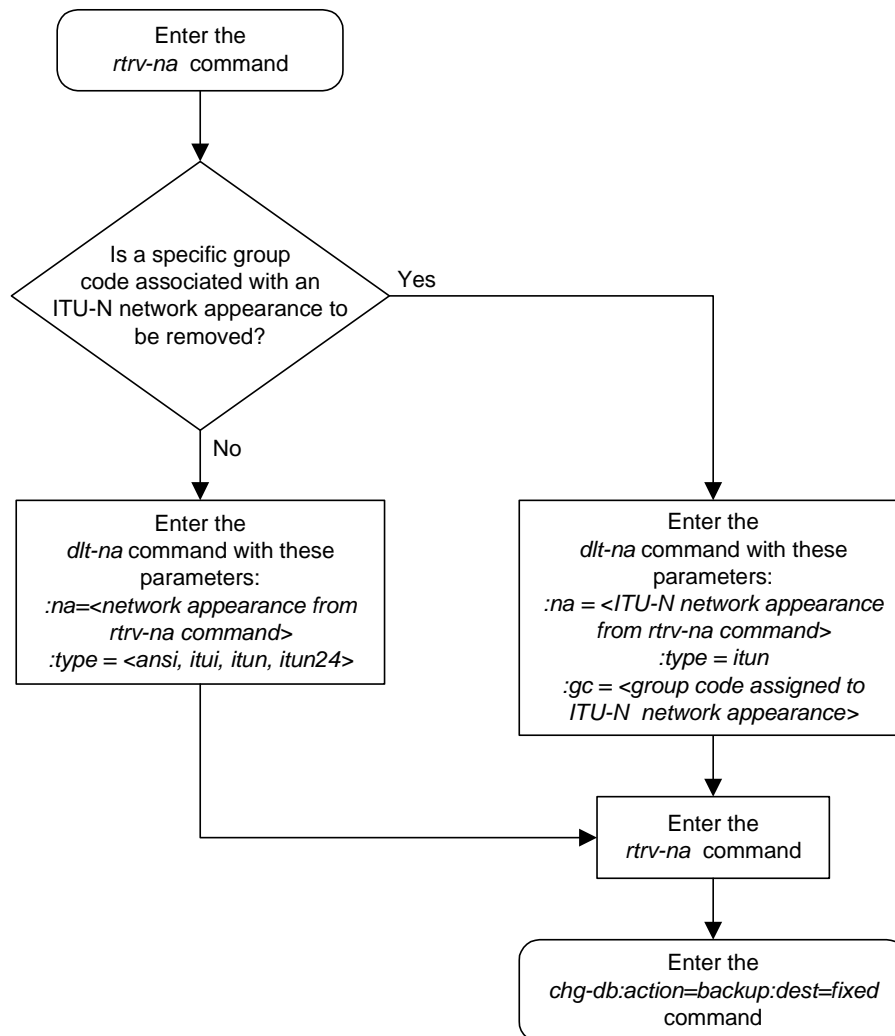
4. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```

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 3-33. 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.

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 03-06-28 21:16:37 GMT Rel 31.0.0
SYNC:      TALI
SRKQ:      250
DRKQ:      750
SNMPCONT:  john doe 555-123-4567
GETCOMM:   public
SETCOMM:   private
TRAPCOMM:  public
INHFEPALE: NO
SCTPCSUM:  adler32
IPGWABATE: NO
IPLIMABATE: NO
```

2. Display the cards in the system by entering the **rtrv-card** command. This is an example of the possible output.

```
rlghncxa03w 03-06-15 16:34:56 GMT Rel 31.0.0
CARD   TYPE      APPL      LSET NAME      PORT SLC   LSET NAME      PORT SLC
1101   ASM        SCCP      -----      --  --   -----      --  --
1102   ASM        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 03-06-28 21:19:37 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
SYNC:      TAL1
SRKQ:      250
DRKQ:      750
SNMPCONT:  john doe 555-123-4567
GETCOMM:   public
SETCOMM:   private
TRAPCOMM:  public
INHFEPALE: NO
SCTPCSUM:  crc32c
IPGWABATE: NO
IPLIMABATE: NO
```

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 03-06-12 09:12:36 GMT Rel 31.0.0
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 03-06-28 21:17:37 GMT Rel 31.0.0
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 03-06-28 21:17:37 GMT Rel 31.0.0

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
```

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:localhost=ipnode2-1205
```

The following is an example of the possible output.

```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
```

```
ANAME assoc2
```

```
LHOST    ipnode2-1205
ALHOST   ---
LPORT    2187
RHOST    remotehost2
RPORT    1025
OPEN     YES
ALW      YES
PORT     A1
ADAPTER  M2PA
ISTRMS   2
OSTRMS   2
RMODE    LIN
RMIN     120
RMAX     800
RTIMES   10
CWMIN    3000
M2PATSET 5
```

```
ANAME assoc4
```

```
LHOST    ipnode2-1205
ALHOST   ---
LPORT    3290
RHOST    remotehost1
RPORT    1025
OPEN     YES
ALW      YES
PORT     B
ADAPTER  M2PA
ISTRMS   2
OSTRMS   2
RMODE    LIN
RMIN     120
RMAX     800
RTIMES   10
CWMIN    3000
M2PATSET 5
```

```
ANAME assoc5
```

```
LHOST    ipnode2-1205
ALHOST   ---
LPORT    1057
RHOST    remotehost1
RPORT    1025
OPEN     YES
ALW      YES
PORT     B2
ADAPTER  M2PA
ISTRMS   2
OSTRMS   2
RMODE    LIN
RMIN     120
RMAX     800
RTIMES   10
CWMIN    3000
M2PATSET 5
```

```
IP Appl Sock/Assoc table is (9 of 250) 3% 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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-07 11:11:28 GMT Rel 31.0.0
PASS: Command sent to card
```

```
rlghncxa03w 03-06-07 11:11:28 GMT Rel 31.0.0
```

```
Checksum Algorithm is crc32c
```

```
rlghncxa03w 03-06-07 11:11:28 GMT Rel 31.0.0
```

```
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 03-06-07 11:11:28 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0

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
0 heartbeat requests sent
0 milliseconds cookie life at 4-way start-up handshake
0 retransmission attempts are allowed at start-up phase
```

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
```

```
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 03-06-28 21:16:37 GMT Rel 31.0.0
PASS: Command sent to card

rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
MSUCOUNT: Command In Progress

rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0

MSUCOUNT: MSU Count Report

-----
Link Measurements (Port A)
-----

Transmit Counts
-----
tx bytes:                      927186
tx msus:                       35661
tx average rate (msus/second): 00441

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 sock avail to pc: 00000
discarded tx due to no sock avail to rtkey: 00001
discarded tx due to all sock congested: 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

Receive Counts
-----
rcv bytes:                      775302
rcv msus:                       29826
rcv average rate (msus/second): 00342

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
```

IP⁷ Secure Gateway Configuration Procedures

```
discarded rcv due to M3UA PDU error:      00001
discarded rcv due to SUA PDU error:      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
```

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

83 01 05 05 0a 01 03 94 09 01 03 08 0d 05 c3 05
01 05 05 05 c3 05 0a 01 03 08 e2 06 c7 04 28 10

83 01 05 05 0a 01 03 ec 10 00 00 00 00 00 00 00
02 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

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

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

53 41 53 49 73 63 63 70 17 00 09 80 03 05 0a 02
c1 05 05 c3 05 01 05 05 08 e2 06 c7 04 00 00 00

53 41 53 49 73 63 63 70 17 00 09 80 03 05 0a 02
c1 05 05 c3 05 01 05 05 08 e2 06 c7 04 00 00 00
```

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 03-06-28 21:17:37 GMT Rel 31.0.0
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 03-06-28 21:17:37 GMT Rel 31.0.0

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
```

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-MSC1. Enter this command.

rtrv-assoc: lhost=dn-msc1

The following is an example of the possible output.

rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0

ANAME assoc3

```
LHOST    dn-msc1
ALHOST    ---
LPORT    2345
RHOST    remotehost2
RPORT    1025
OPEN     YES
ALW      YES
PORT     A
ADAPTER  SUA
VER      SUA DRAFT 3
ISTRMS   2
OSTRMS   2
RMODE    LIN
RMIN     120
RMAX     800
RTIMES   10
CWMIN    3000
```

ANAME assoc6

```
LHOST    dn-msc1
ALHOST    host3
LPORT    4156
RHOST    remotehost2
RPORT    1025
OPEN     YES
ALW      YES
PORT     A
ADAPTER  SUA
VER      SUA DRAFT 3
ISTRMS   2
OSTRMS   2
RMODE    LIN
RMIN     120
RMAX     800
RTIMES   10
CWMIN    3000
```

IP Appl Sock/Assoc table is (9 of 250) 3% 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 03-06-28 21:17:37 GMT Rel 31.0.0
PASS: Command sent to card

rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
MSUCOUNT: Command In Progress

rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
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
```


IP⁷ Secure Gateway Configuration Procedures

```
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 03-06-28 21:17:37 GMT Rel 31.0.0
PASS: Command sent to card
```

```
rlgh
ncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
MSUCOUNT: Command In Progress
```

```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
```

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

-
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 03-06-12 09:12:36 GMT Rel 31.0.0
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 03-06-28 21:19:37 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
SYNC:      TAL1
SRKQ:      250
DRKQ:      750
SNMPCONT:  john doe 555-123-4567
GETCOMM:   public
SETCOMM:   private
TRAPCOMM:  public
INHFEPALM: NO
SCTPCSUM:  crc32c
IPGWABATE: NO
IPLIMABATE: NO
```

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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-07 11:11:28 GMT Rel 31.0.0
PASS: Command sent to card
;

rlghncxa03w 03-06-07 11:11:28 GMT Rel 31.0.0

Checksum Algorithm is crc32c
;

rlghncxa03w 03-06-07 11:11:28 GMT Rel 31.0.0

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 03-06-07 11:11:28 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0
ASSOCIATION      PST          SST
assoc3           IS-NR          -----
Command Completed.
```

```
rept-stat-assoc:aname=assoc6
```

The following is an example of the possible output.

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
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 03-06-28 21:16:37 GMT Rel 31.0.0

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
0 heartbeat requests sent
0 milliseconds cookie life at 4-way start-up handshake
0 retransmission attempts are allowed at start-up phase

```

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
```

```
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 03-06-28 21:16:37 GMT Rel 31.0.0
PASS: Command sent to card
```

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
MSUCOUNT: Command In Progress
```

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
```

```
MSUCOUNT: MSU Count Report
```

```
-----
Link Measurements (Port A)
-----
```

```
Transmit Counts
```

```
-----
tx bytes:                      927186
tx msus:                        35661
tx average rate (msus/second): 00441
```

```
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
```

IP⁷ Secure Gateway Configuration Procedures

```
discarded tx due to no ss7 rtkey:          00001
discarded tx due to no sock avail to pc:    00000
discarded tx due to no sock avail to rtkey: 00001
discarded tx due to all sock congested:    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
```

Receive Counts

```
-----
rcv bytes:          775302
rcv msus:          29826
rcv average rate (msus/second): 00342
```

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
```

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
```

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

83 01 05 05 0a 01 03 94 09 01 03 08 0d 05 c3 05
01 05 05 05 c3 05 0a 01 03 08 e2 06 c7 04 28 10

83 01 05 05 0a 01 03 ec 10 00 00 00 00 00 00 00
02 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

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

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

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
```

```
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
```

```
53 41 53 49 73 63 63 70 17 00 09 80 03 05 0a 02
c1 05 05 c3 05 01 05 05 08 e2 06 c7 04 00 00 00
```

```
53 41 53 49 73 63 63 70 17 00 09 80 03 05 0a 02
c1 05 05 c3 05 01 05 05 08 e2 06 c7 04 00 00 00
```

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 03-06-28 21:17:37 GMT Rel 31.0.0
PASS: Command sent to card
```

```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
MSUCOUNT: Command In Progress
```

```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
```

```
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
```


IP⁷ Secure Gateway Configuration Procedures

```
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 03-06-28 21:17:37 GMT Rel 31.0.0
PASS: Command sent to card
```

```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
MSUCOUNT: Command In Progress
```

```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
```

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

```

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.

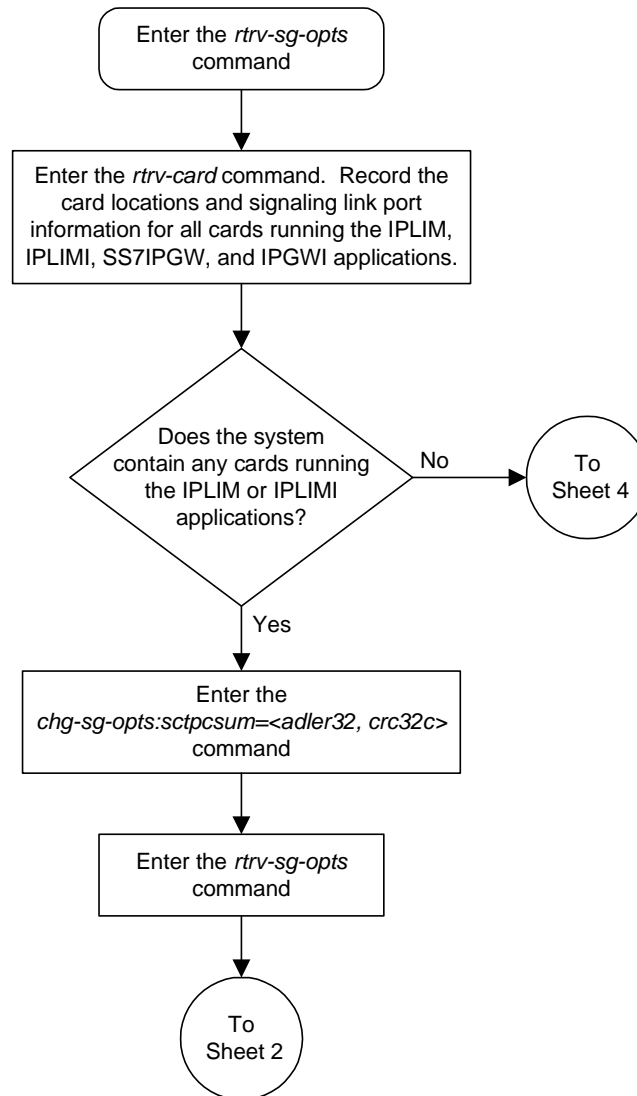
40. At the IP near end node, activate all the other associations attached to the IP card specified in step 39.
-

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.
-

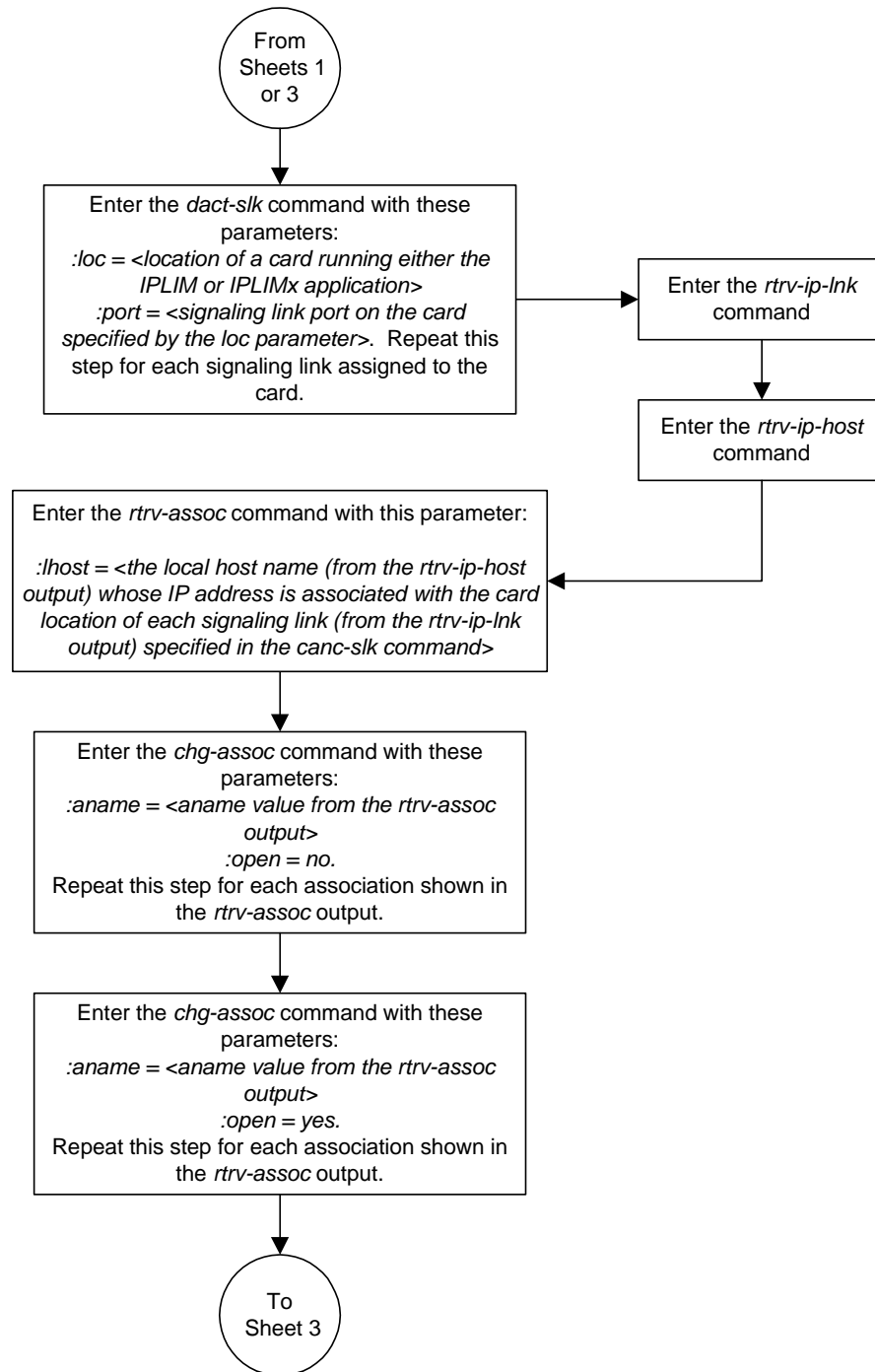
42. Back up the new changes using the **chg-db:action=backup:dest=fixed** command. These messages should appear, the active Maintenance and Administration Subsystem Processor (MASP) appears first.

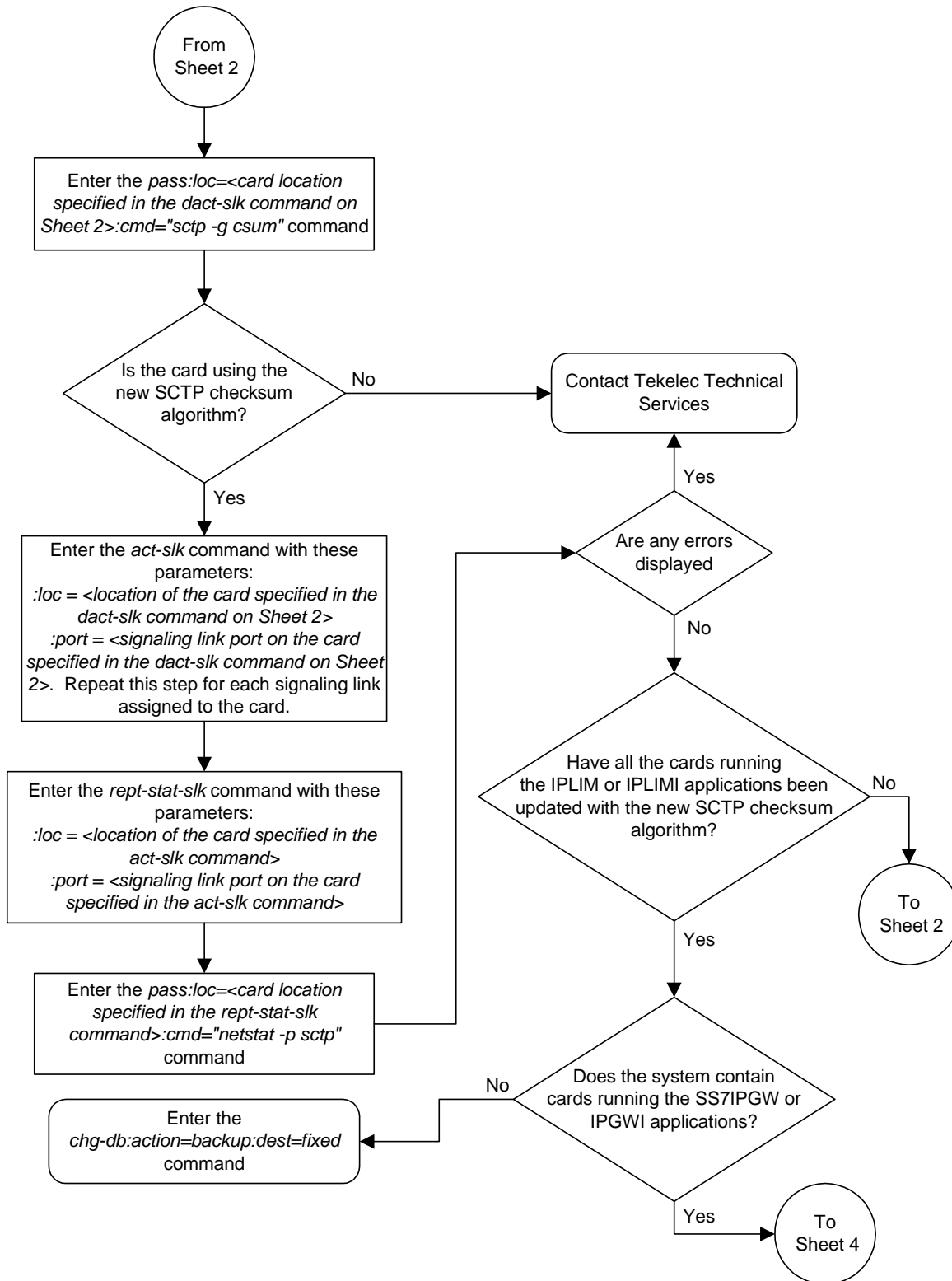
```
BACKUP (FIXED) : MASP A - Backup starts on active MASP.  
BACKUP (FIXED) : MASP A - Backup on active MASP to fixed disk complete.  
BACKUP (FIXED) : MASP A - Backup starts on standby MASP.  
BACKUP (FIXED) : MASP A - Backup on standby MASP to fixed disk complete.
```

Flowchart 3-34. Changing the SCTP Checksum Option (Sheet 1 of 7)

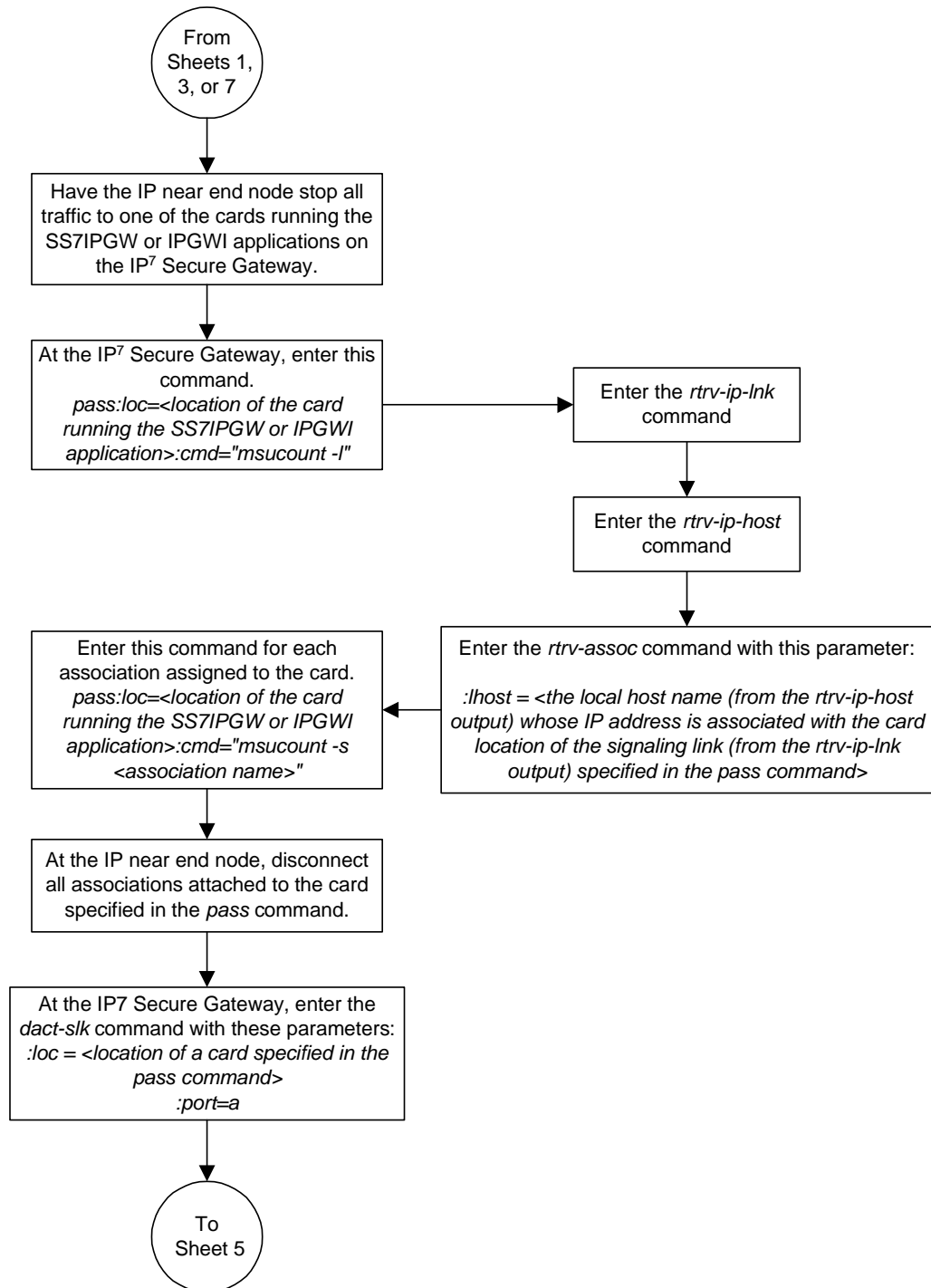


Flowchart 3-34. Changing the SCTP Checksum Option (Sheet 2 of 7)

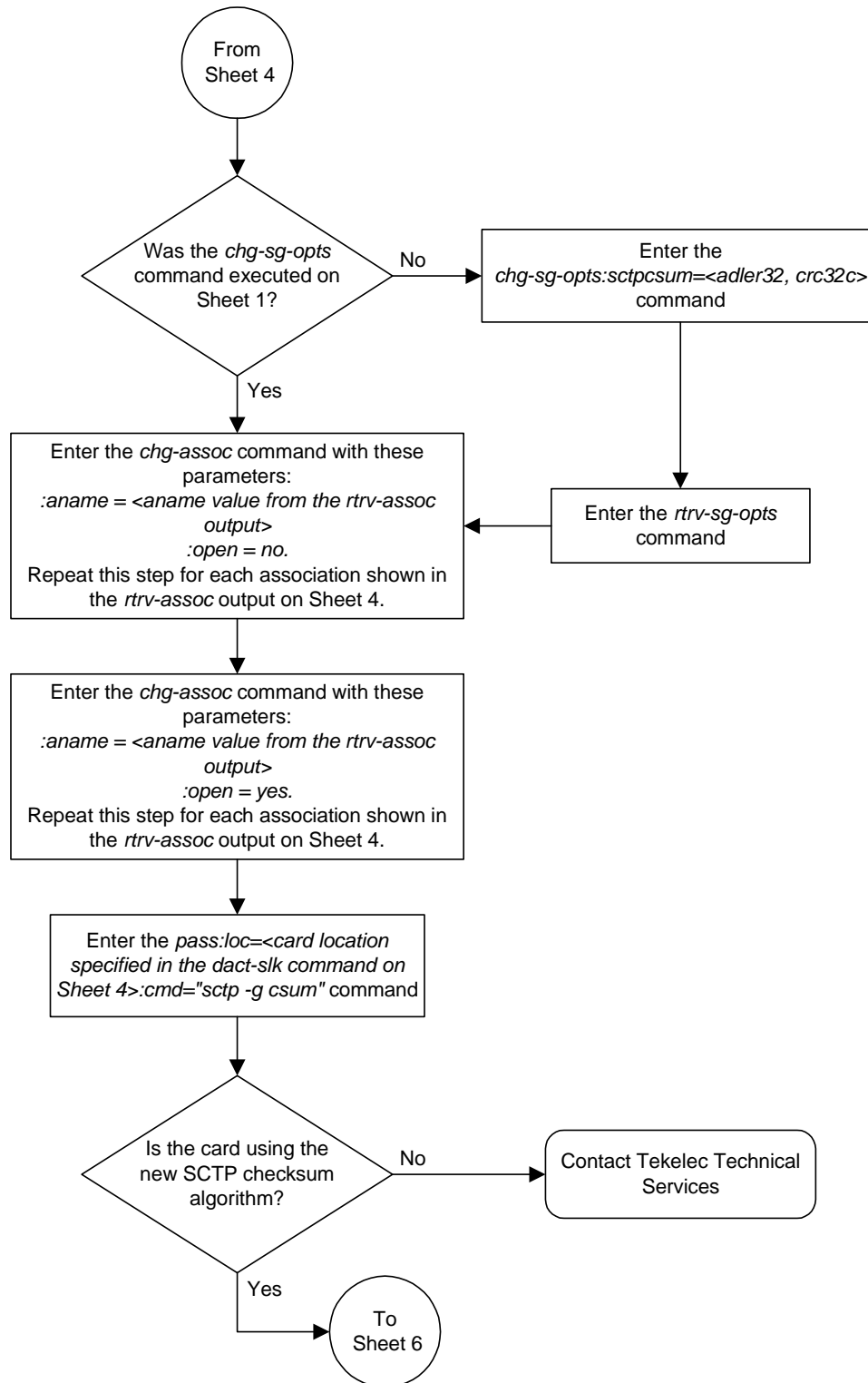


Flowchart 3-34. Changing the SCTP Checksum Option (Sheet 3 of 7)

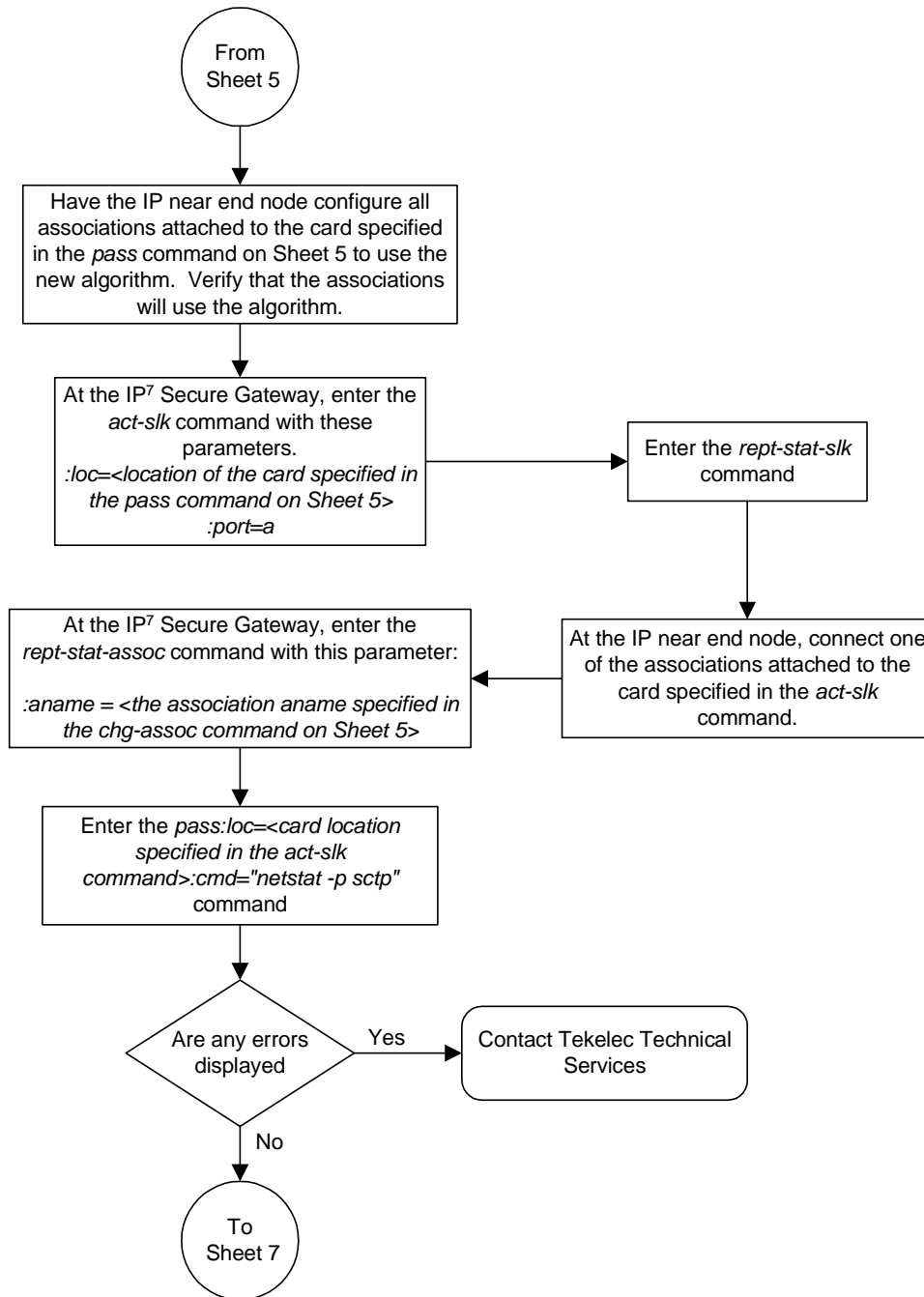
Flowchart 3-34. Changing the SCTP Checksum Option (Sheet 4 of 7)



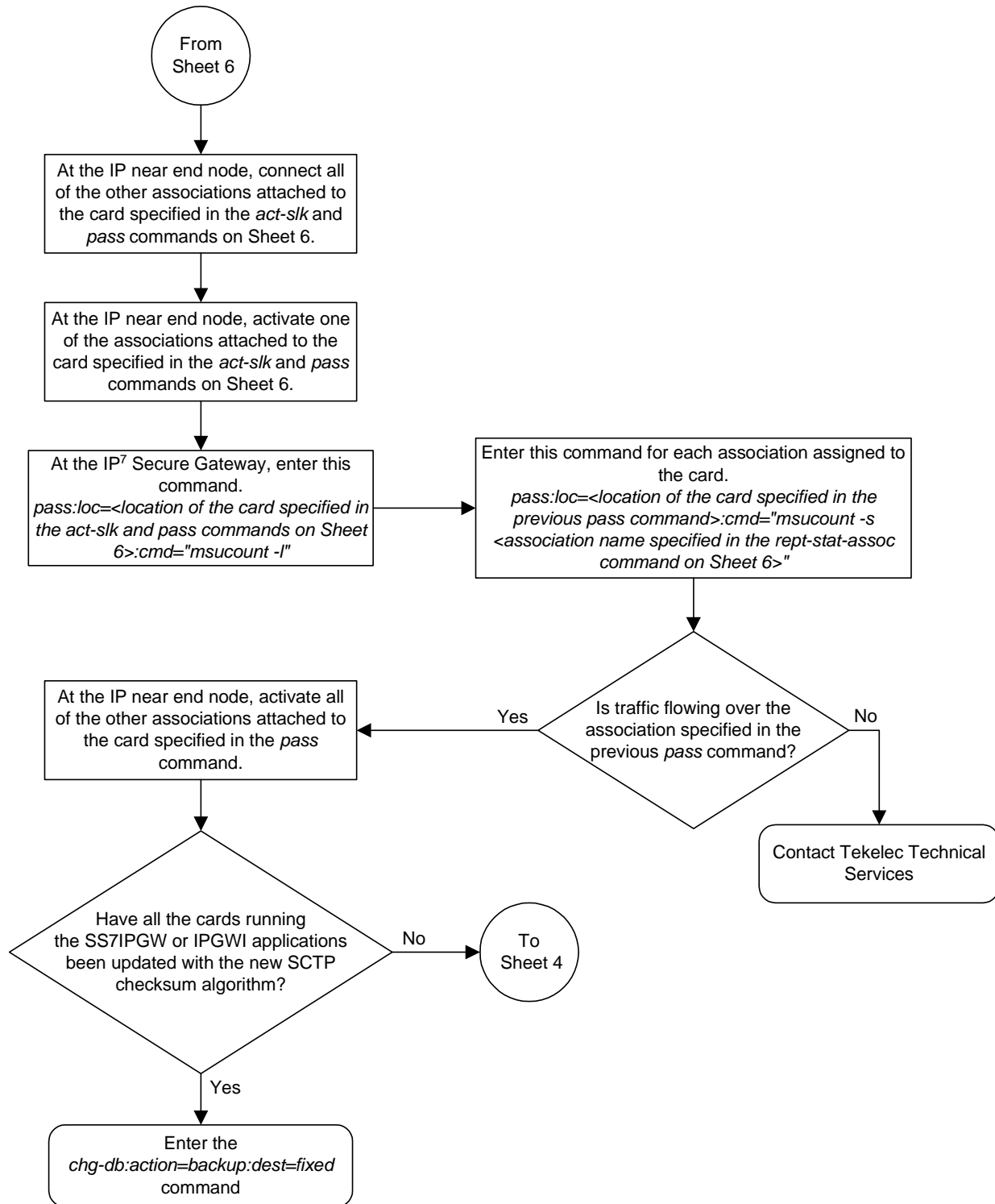
Flowchart 3-34. Changing the SCTP Checksum Option (Sheet 5 of 7)



Flowchart 3-34. Changing the SCTP Checksum Option (Sheet 6 of 7)



Flowchart 3-34. 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, only one timer is defined, timer 1 - the maximum amount of time messages are queued when an application server transitions from the AS-Active state to the AS-Pending state.

:tvalue – the value of the timer specified by the **timer** parameter, from 10 to 200 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 3-17 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 3-17. 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 3-18 on page 3-295.

- 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 3-18 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 3-18. 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 3-19 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 3-19. 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.

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 03-06-28 09:12:36 GMT Rel 31.0.0

SET	TIMER	TVALUE	PARM	PVALUE
3	1	10	1	3
3	2	0	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 10-200(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 03-06-28 09:12:36 GMT Rel 31.0.0
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 250) 2% 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 03-06-28 09:12:36 GMT Rel 31.0.0
ANAME swbel32
LHOST      gw105.nc.tekelec.com
ALHOST     ---
LPORT      1030
RHOST      gw100.ncd-economic-development.southeastern-cooridor-ash.gov
RPORT      2345
OPEN       YES
ALW        YES
PORT       A
ADAPTER    M3UA
VER        M3UA RFC
RMODE      LIN
RMIN       120
RMAX       800
RTIMES     10
CWMIN      3000
ISTRMS     2
OSTRMS     2
```

IP Appl Sock table is (4 of 250) 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 3-190 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.

4. 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 3-17 on page 3-294, Table 3-18 on page 3-295, or Table 3-19 on page 3-296 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 03-06-28 09:12:36 GMT Rel 31.0.0  
CHG-UAPS: MASP A - COMPLTD
```

5. 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 03-06-28 09:12:36 GMT Rel 31.0.0

SET	TIMER	TVALUE	PARM	PVALUE
3	1	200	1	3
3	2	0	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 10-200(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

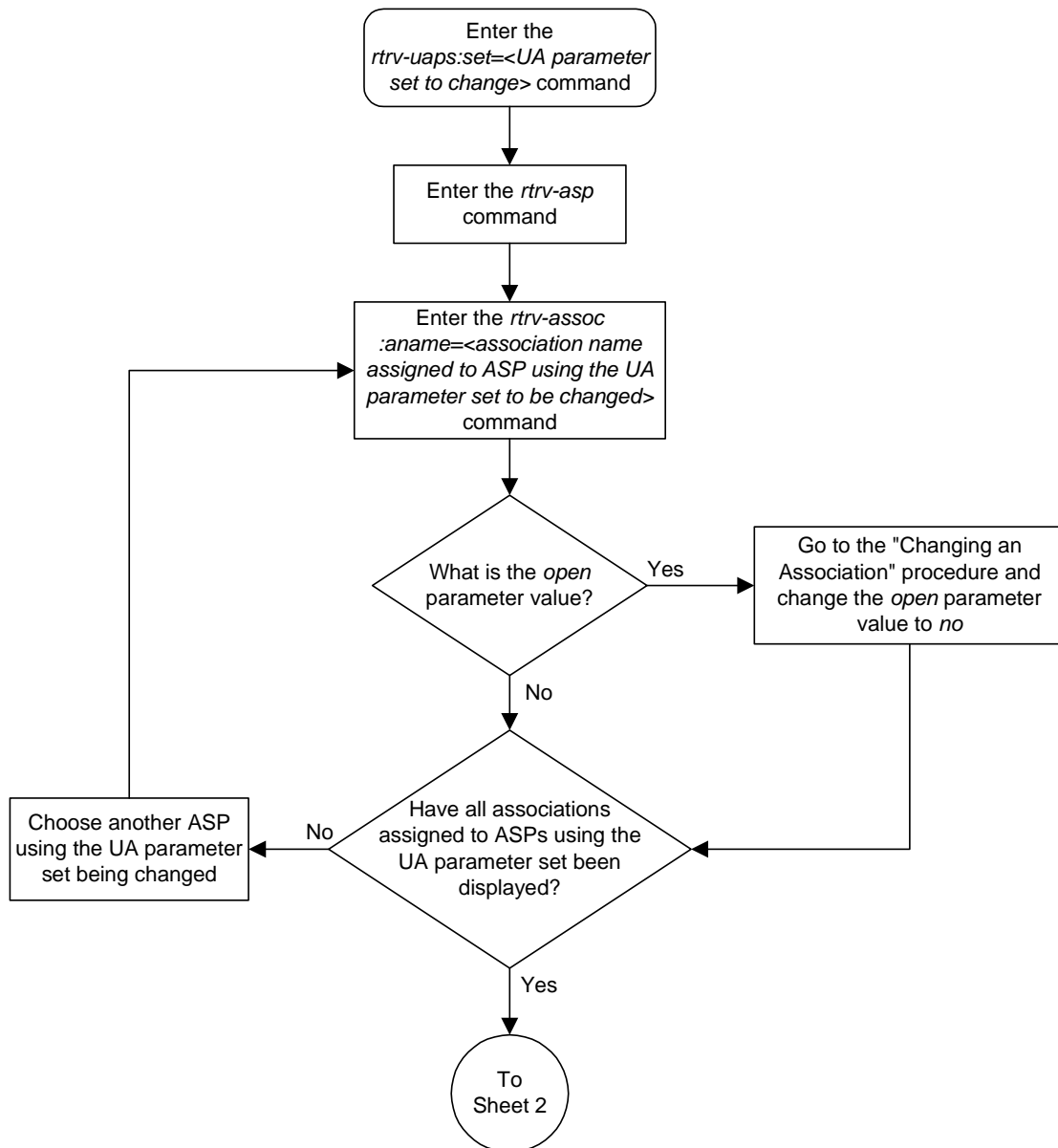
BIT	BIT VALUE
0=Strict ASP-ID checking	0=Disabled , 1=Enabled
1-31=Reserved	

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 3-190 and change the value of the **open** parameter in these associations to **yes**.

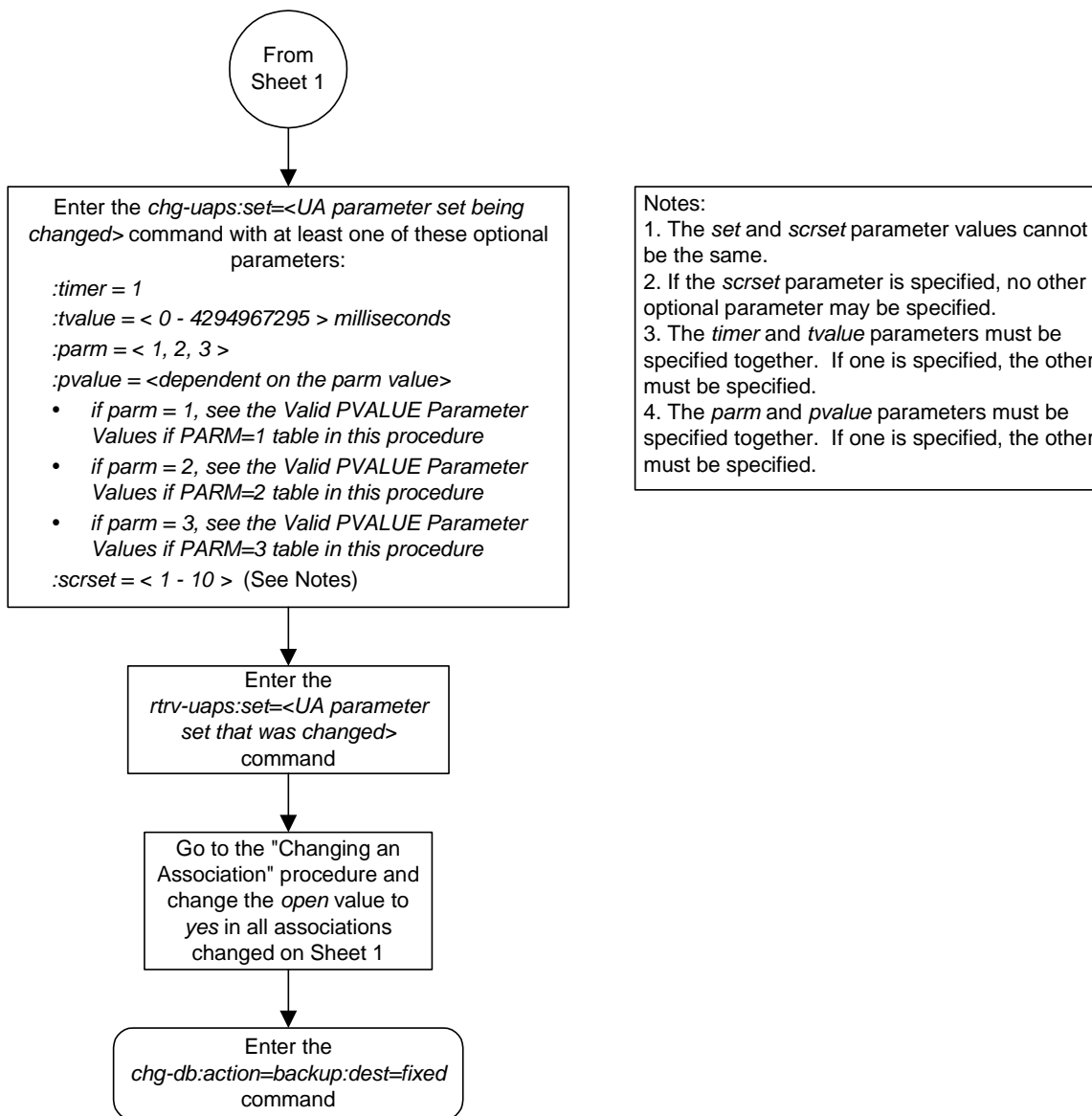
7. Back up the new changes, using the **chg-db:action=backup:dest=fixed** command. These messages should appear; the active Maintenance and Administration Subsystem Processor (MASP) appears first.

```
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 3-35. Changing a UA Parameter Set (Sheet 1 of 2)



Flowchart 3-35. Changing a UA Parameter Set (Sheet 2 of 2)



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 03-06-28 21:17:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
The following features have been permanently enabled:
Feature Name          Partnum    Status    Quantity
TPS                   893000101  on        100
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 03-06-10 11:43:04 GMT Rel 31.0.0
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 03-06-28 21:17:37 GMT Rel 31.0.0
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
```

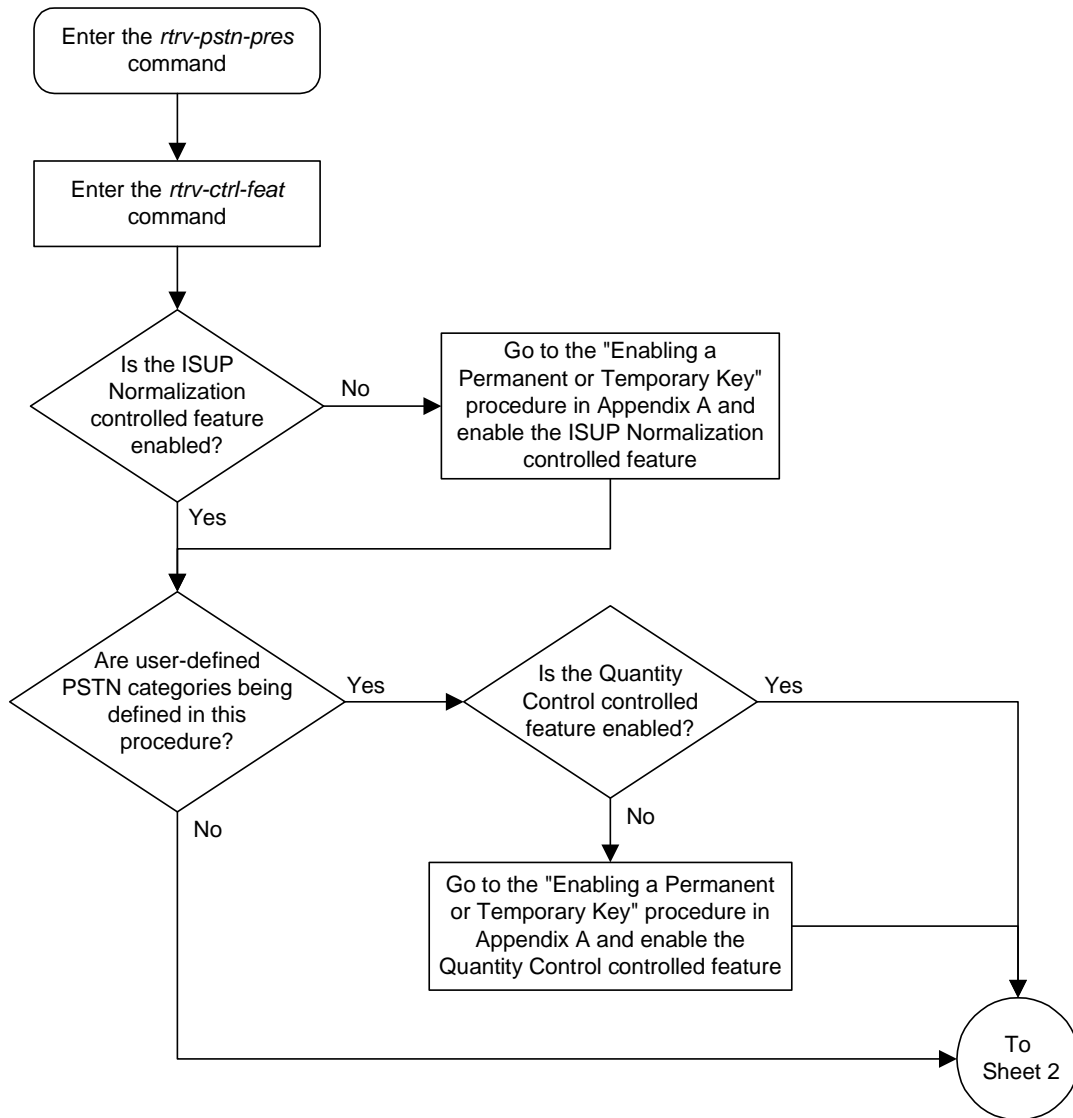
ISUP Variant table is (7 of 21) 33% full

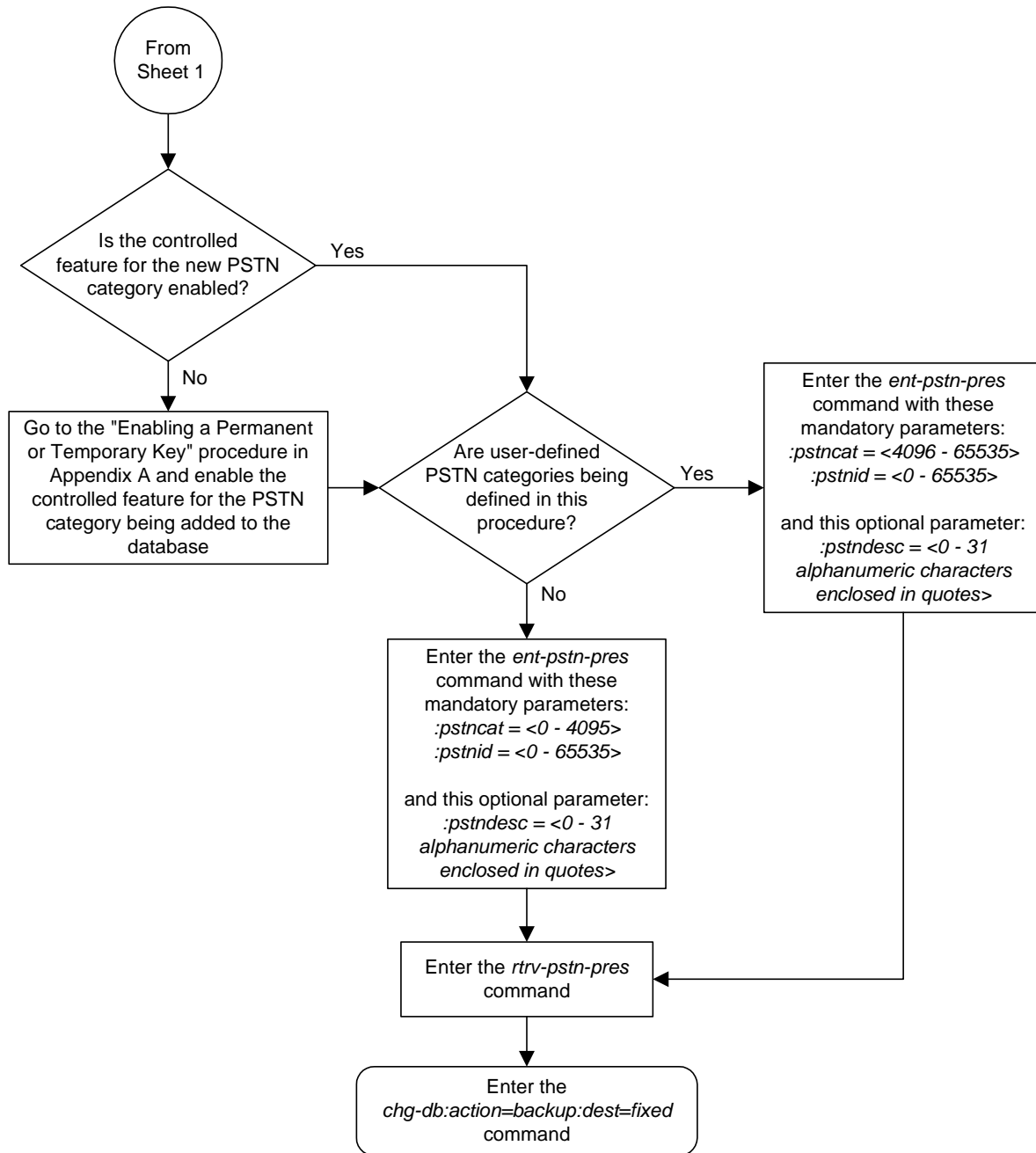
NOTE: An * will be displayed next to the PSTN Category for entries that are no longer usable. These are entries that are disabled because their temporary feature key expired.

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.
```

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 03-06-28 21:17:37 GMT Rel 31.0.0
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 03-06-10 11:43:04 GMT Rel 31.0.0
CHG-PSTN-PRES: MASP A - COMPLTD
```

3. Verify the changes using the **rtrv-pstn-pres** command. This is an example of possible output:

```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
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
```

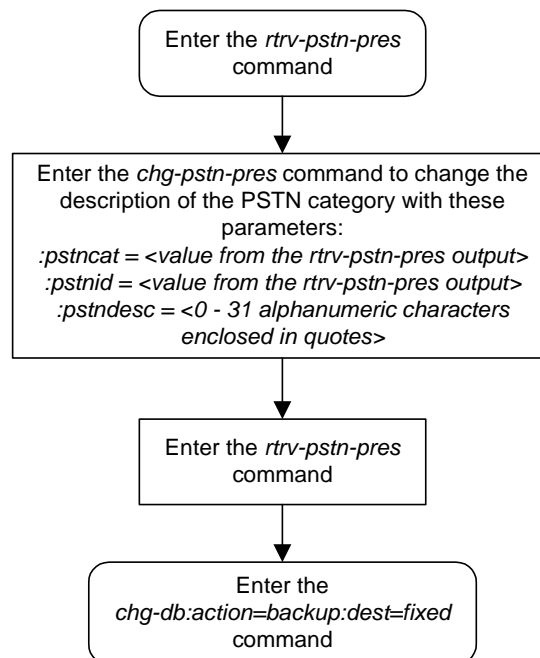
ISUP Variant table is (7 of 21) 33% full

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 03-06-10 11:43:04 GMT Rel 31.0.0
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. For this example, enter this command.

```
rtrv-appl-rtkey:pstncat=04096:pstnid=01000
```

This is an example of the possible output.

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
```

```
KEY:LOC      DPC          SI SSN OPCA          CICS          CICE
  STATIC 12323-DE      5 --- 12212-DE      1             1000
      ATTR:PSTNCAT PSTNID NORM DUP
           4096      1000  Y      -
      SNAME: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 3-151 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 **dlt-pstn-pres** command with the **pstncat**, **pstnid**, and **force=yes** parameters. For this example, enter this command.

```
dlt-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 03-06-10 11:43:04 GMT Rel 31.0.0
DLT-PSTN-PRES: MASP A - COMPLTD
```

4. Verify the changes using the **rtrv-pstn-pres** command. This is an example of possible output:

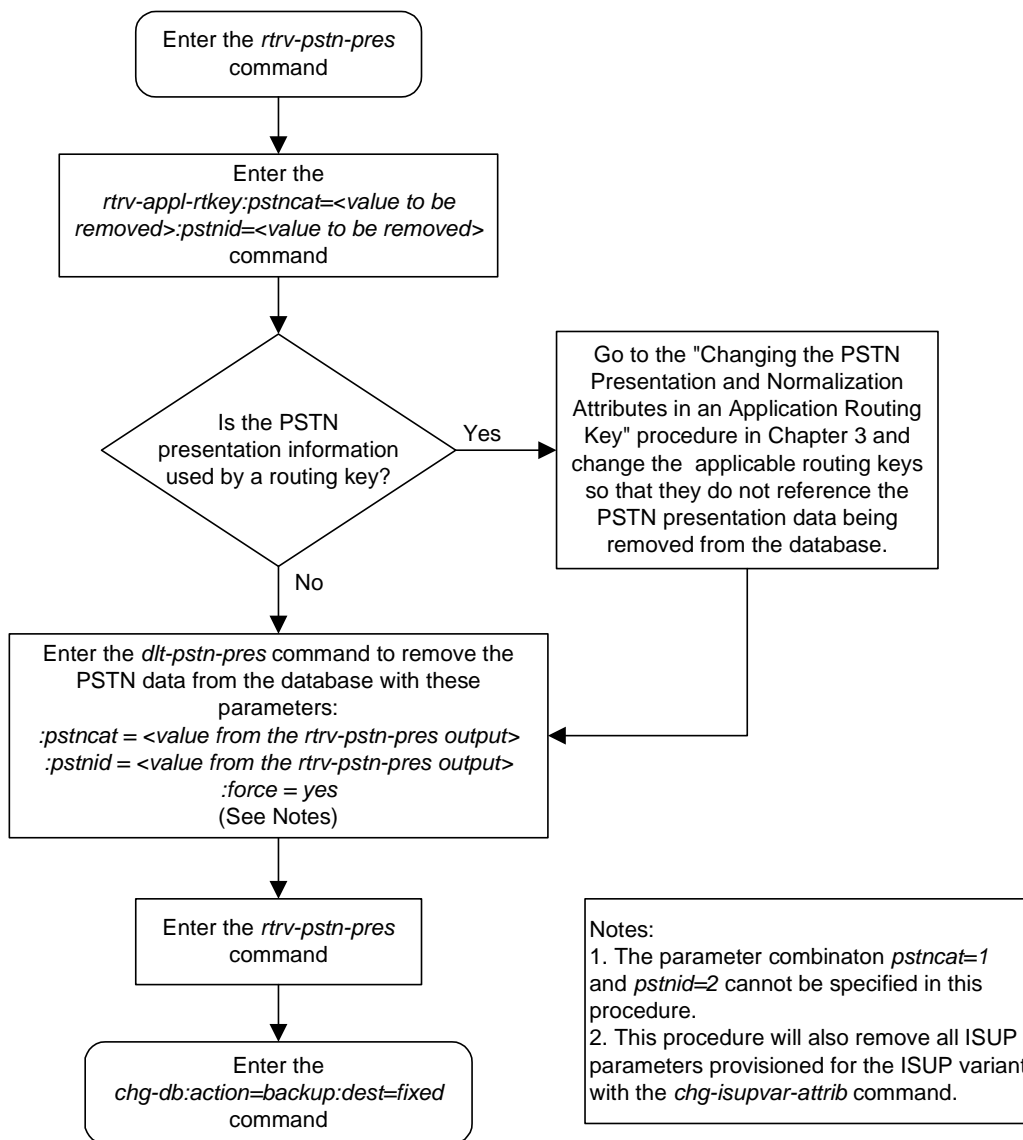
```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
PSTNCAT PSTNID PSTNDESC
00001 00001 ITU Q.767
00001 00002 ETSI V3
00001 00003 UK PNO-ISC7
00001 00004 GERMAN ISUP
00001* 00020 Mexico
05000 00001 Mexican ISUP v1.8
```

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-attrib** 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.

: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	
Notes: 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.				

Procedure

1. Display the current value of the ISUP supported parameters for all the variants using the **rtrv-isupvar-attrib** command. This is an example of possible output.

```
rlghncxa03w 03-06-10 11:43:04 GMT Rel 31.0.0
```

```
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 03-06-28 21:15:37 GMT Rel 31.0.0
The following features have been permanently enabled:
Feature Name          Partnum    Status  Quantity
TPS                   893000101  on      100
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 03-06-10 11:43:04 GMT Rel 31.0.0
CHG-ISUPVAR-ATTRIB: MASP A - COMPLTD
```

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 03-06-10 11:43:04 GMT Rel 31.0.0
PSTNCAT PSTNID
04097 00001
```

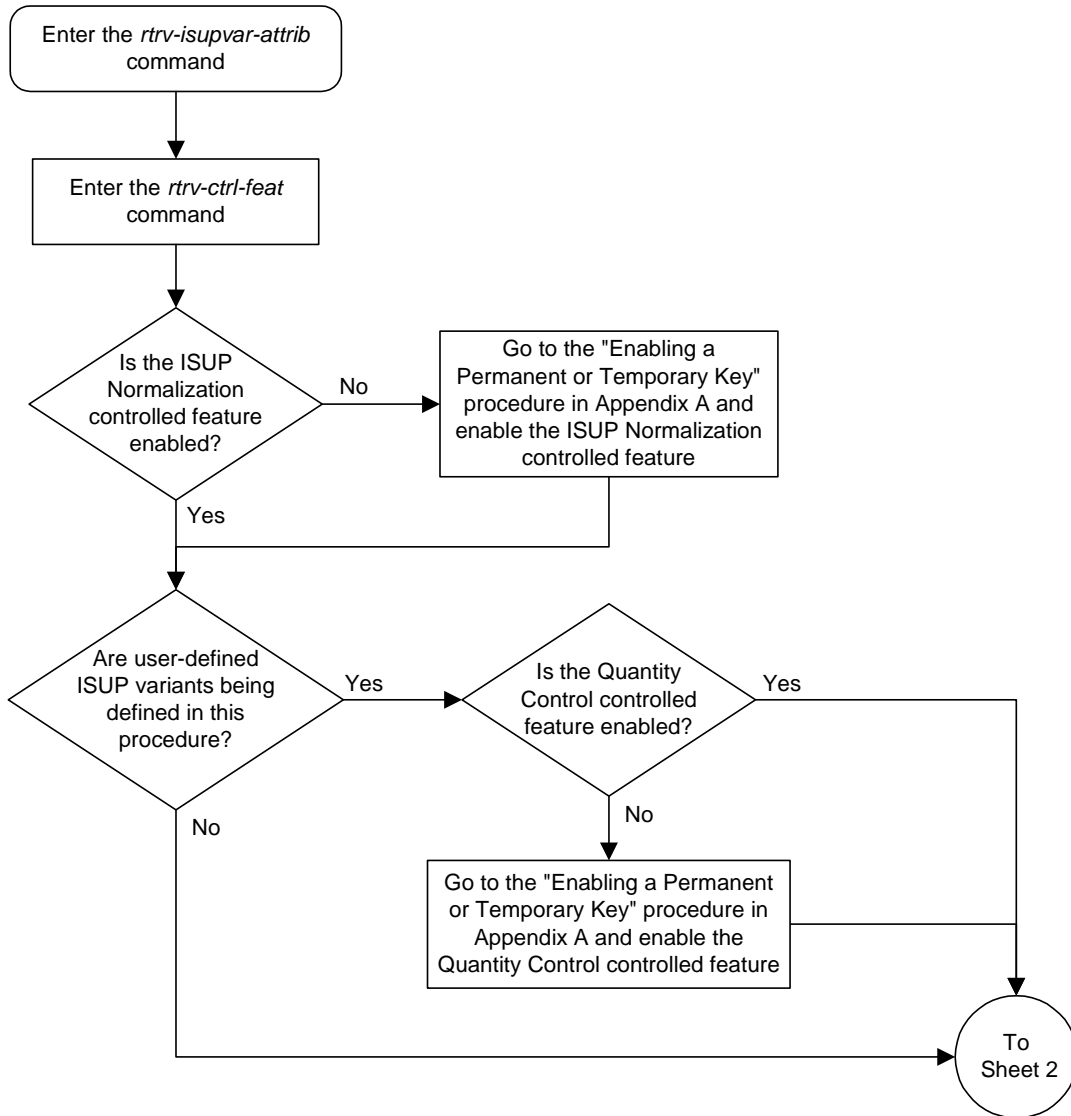
MSGCODE	PARMCODE	TYPE	ORDER	ACTION
01h	---	---	-	NONE
	45h	MF	1	NONE
	00h	OPT	-	NONE
	40h	OPT	-	PASSTHRU

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

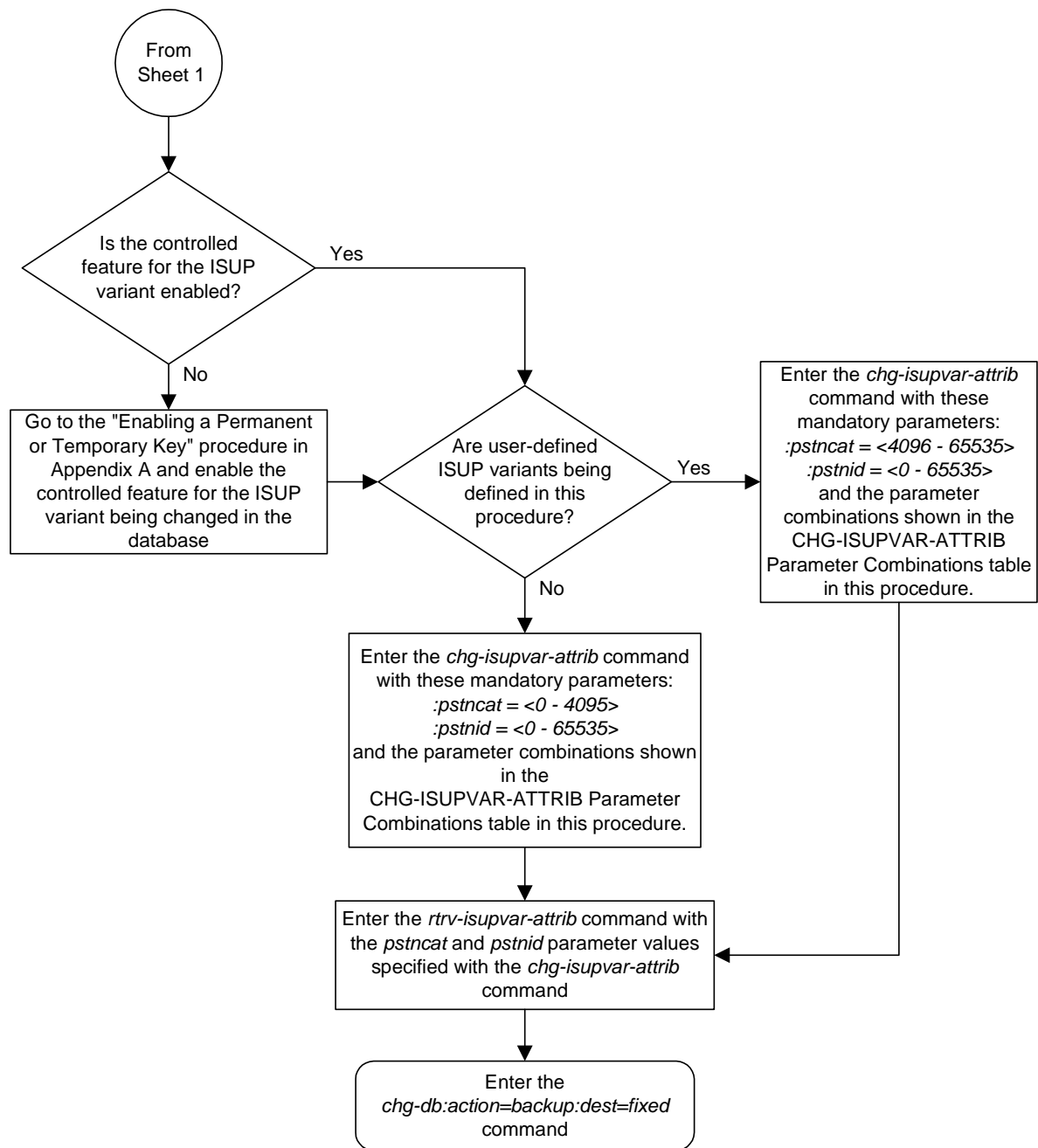
ISUP Variant table is (5 of 20) 25% full

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)

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.

Procedure

1. Display the current value of the ISUP supported parameters for all the variants using the **rtrv-isupvar-attrib** command. This is an example of possible output:

```
rlghncxa03w 03-06-28 21:17:37 GMT Rel 31.0.0
```

```
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 03-06-28 21:15:37 GMT Rel 31.0.0
The following features have been permanently enabled:
Feature Name          Partnum    Status   Quantity
TPS                   893000101  on       100
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 03-06-10 11:43:04 GMT Rel 31.0.0
COPY-ISUPVAR-ATTRIB: MASP A - COMPLTD
```

- 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

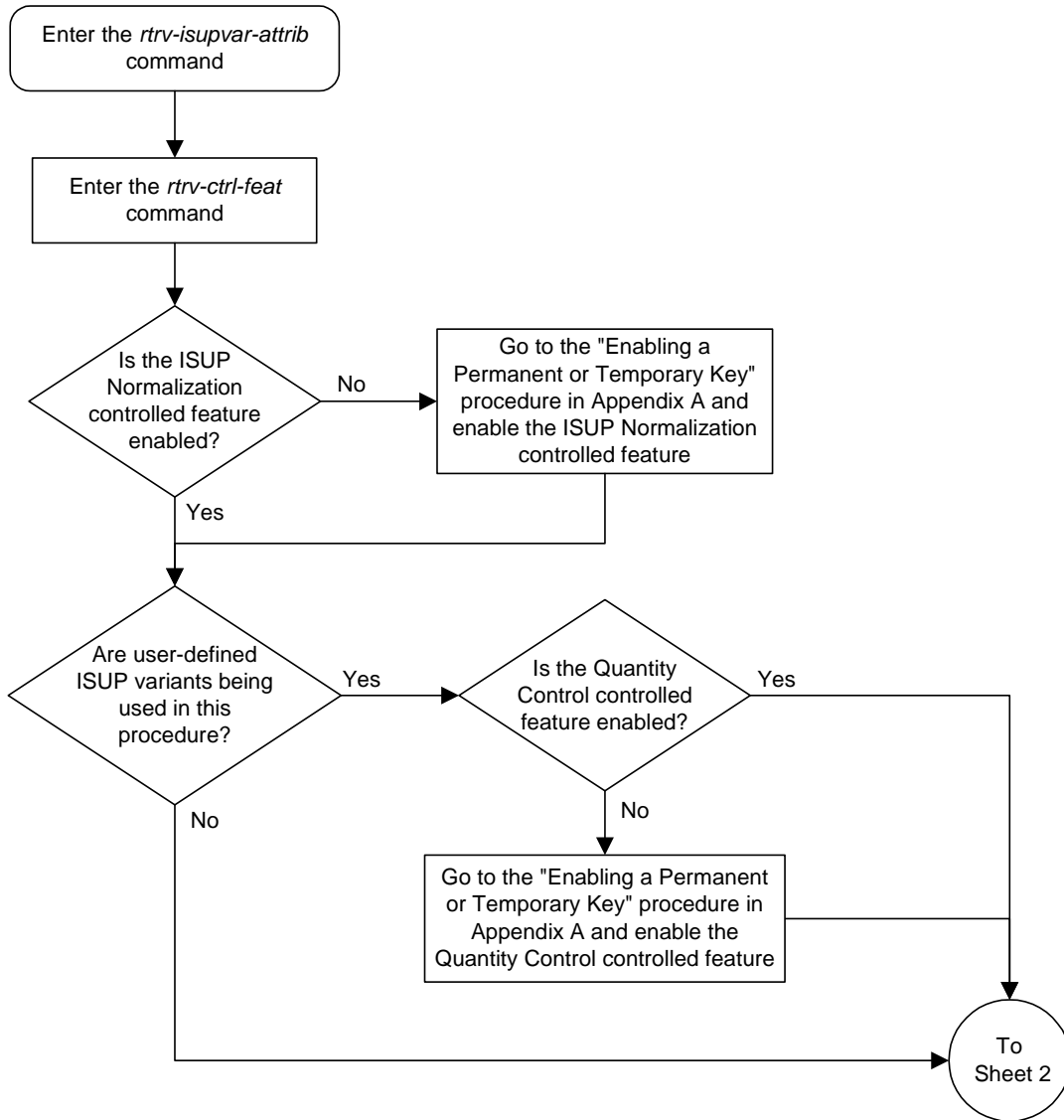
This is an example of the possible output.

```
PSTNCAT  PSTNID
00001    00020

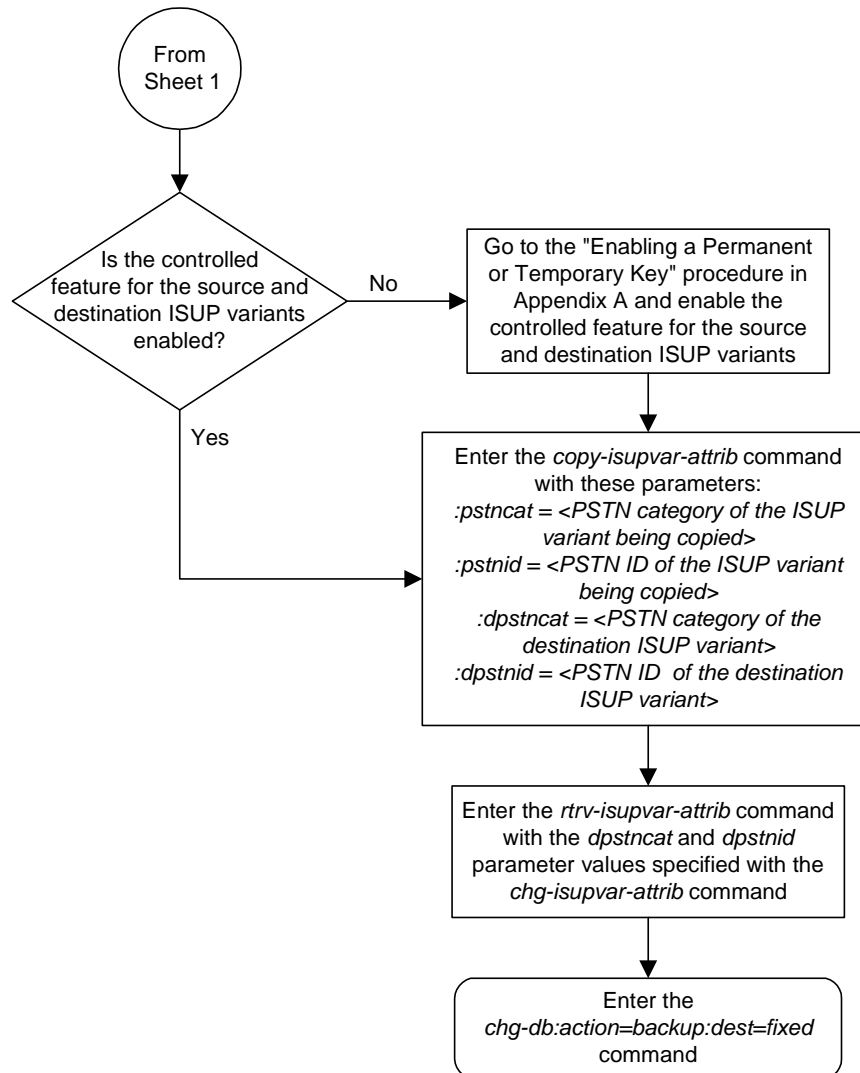
MSGCODE  PARMCODE  TYPE  ORDER  ACTION
01h      ---      ---   -      NONE
          45h      MF    1      NONE
          00h      OPT   -      NONE
          40h      OPT   -      NONE
MSGCODE  PARMCODE  TYPE  ORDER  ACTION
0Ah      ---      ---   -      NONE
          45h      MF    1      NONE
          4Ch      MV    1      NONE
          00h      OPT   -      NONE
          10h      OPT   -      NONE
          56h      OPT   -      NONE
```

- 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)



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 UPUs 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.

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 SCCP 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.

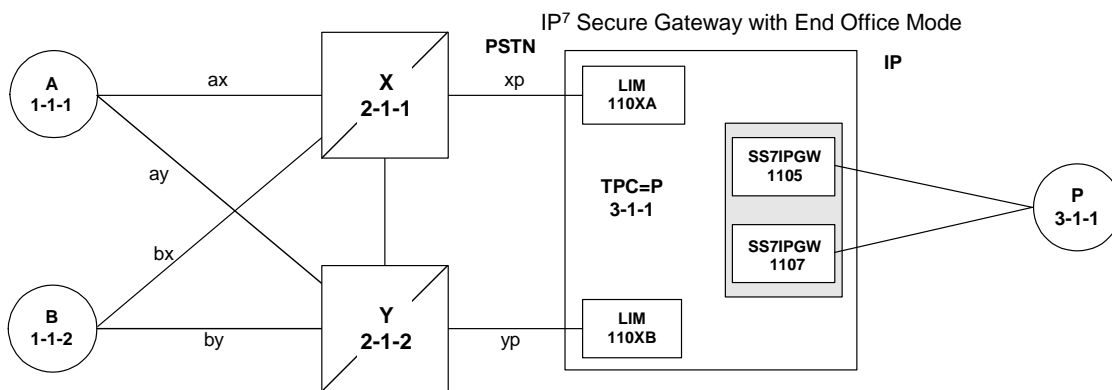
Table 5-1. Sample IPC Values (Continued)

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

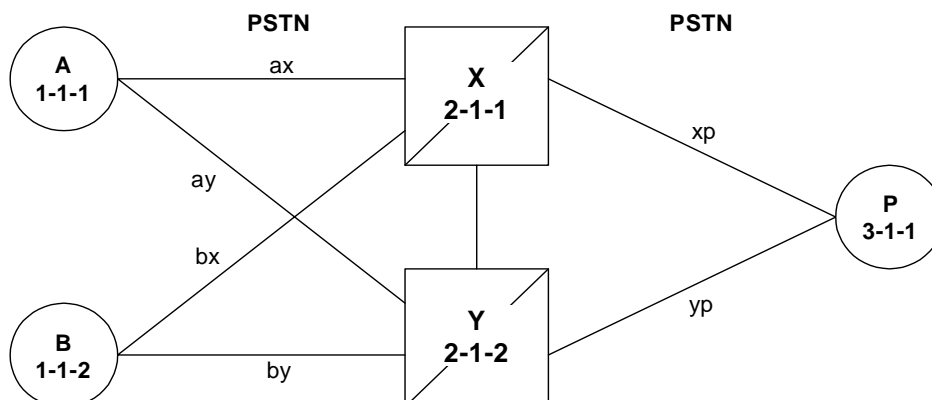
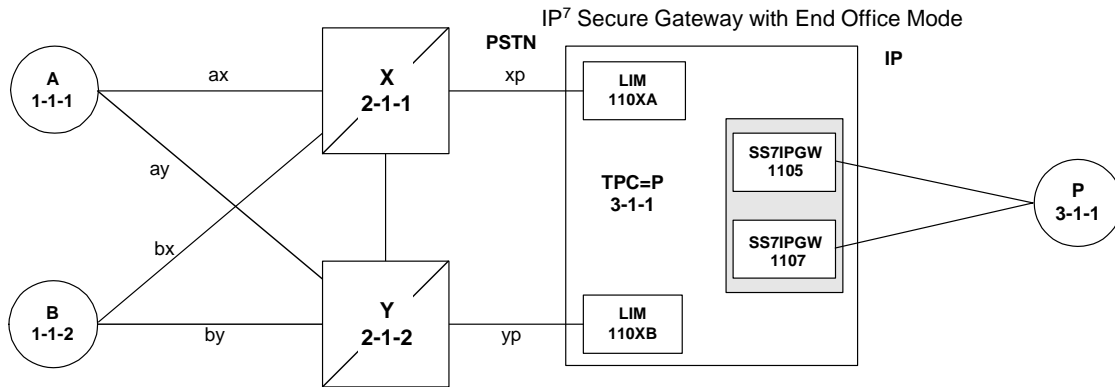


Figure 5-3. Network After a System with End Office, Node P has Migrated



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

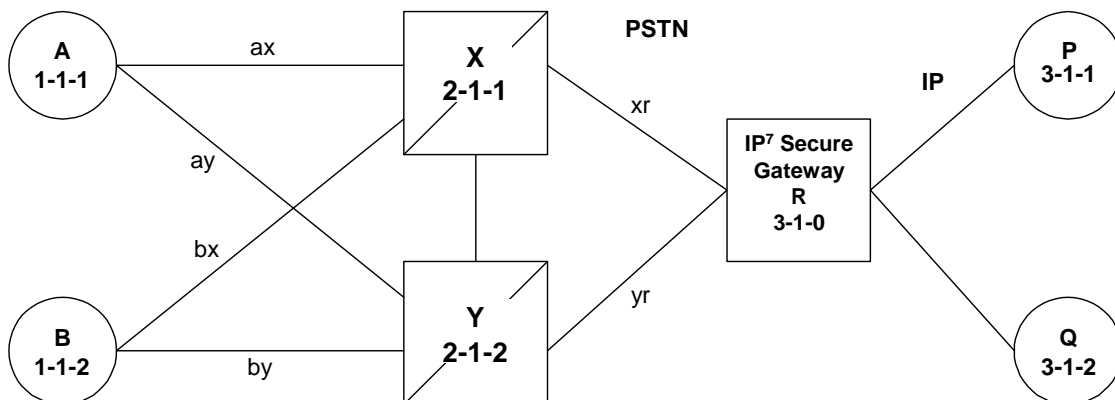
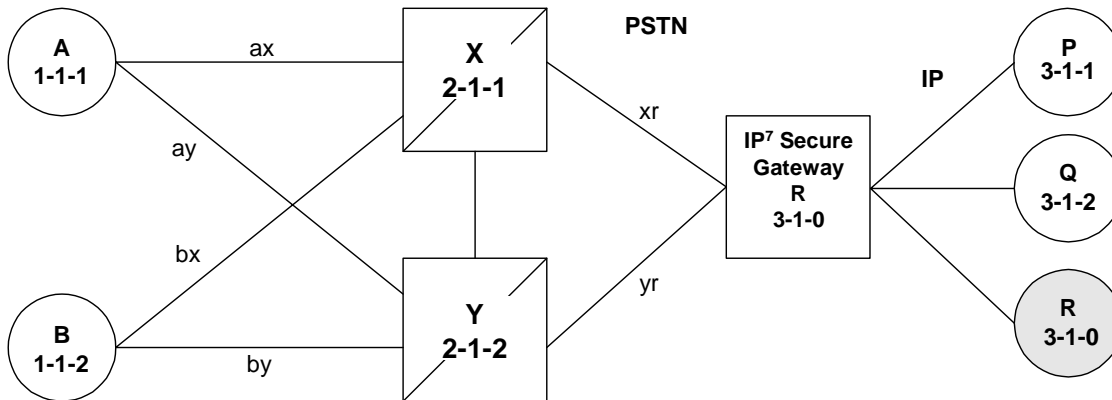


Figure 5-5. New Network with a System Using End Office and End Node R



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

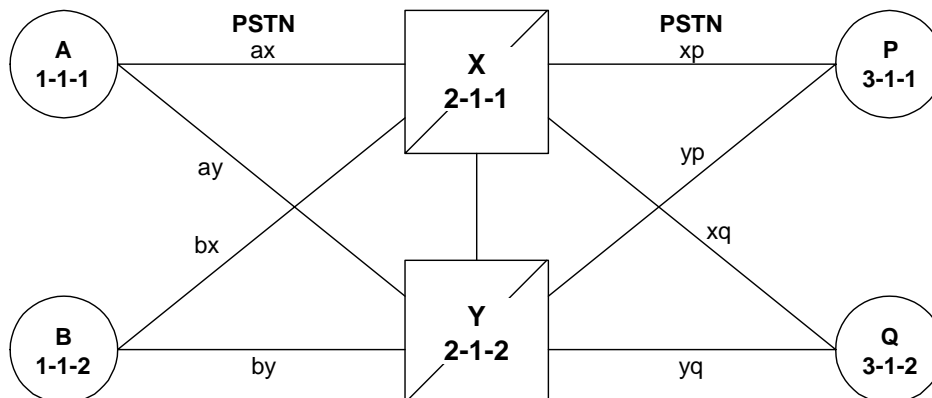
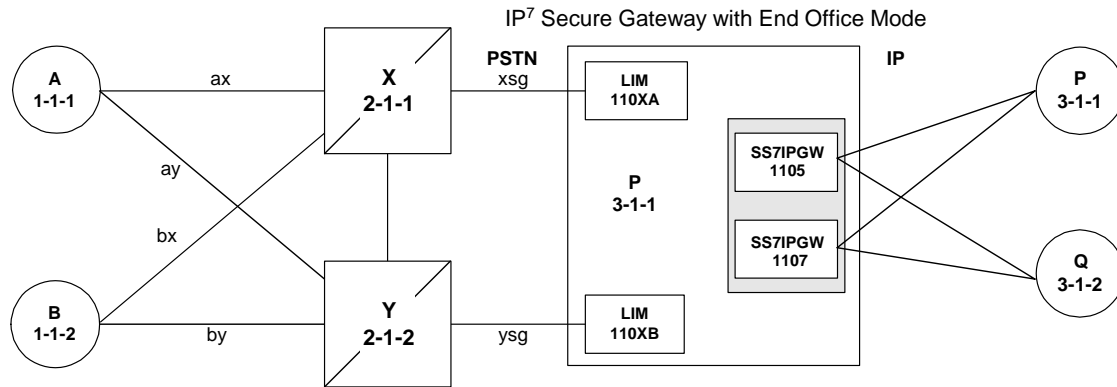


Figure 5-7. Network after Two Signaling End Points Migrate from PSTN to IP



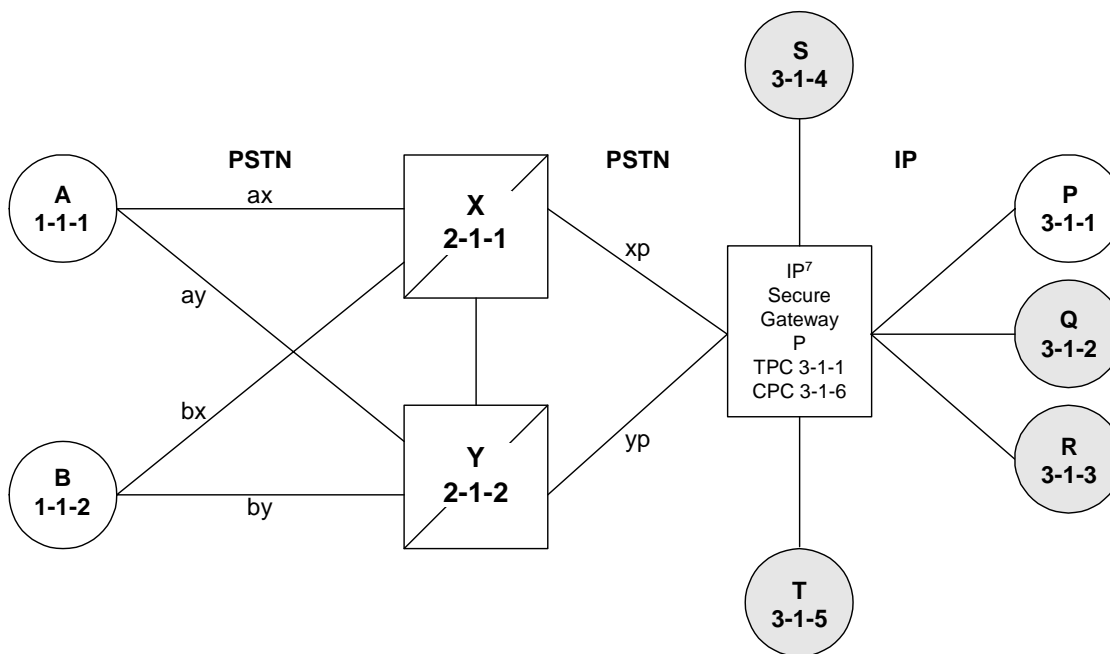
In Figure 5-7, P is an end office node, and so P serves as the adjacent point code for nodes X and Y. The following are key points about this figure:

- 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



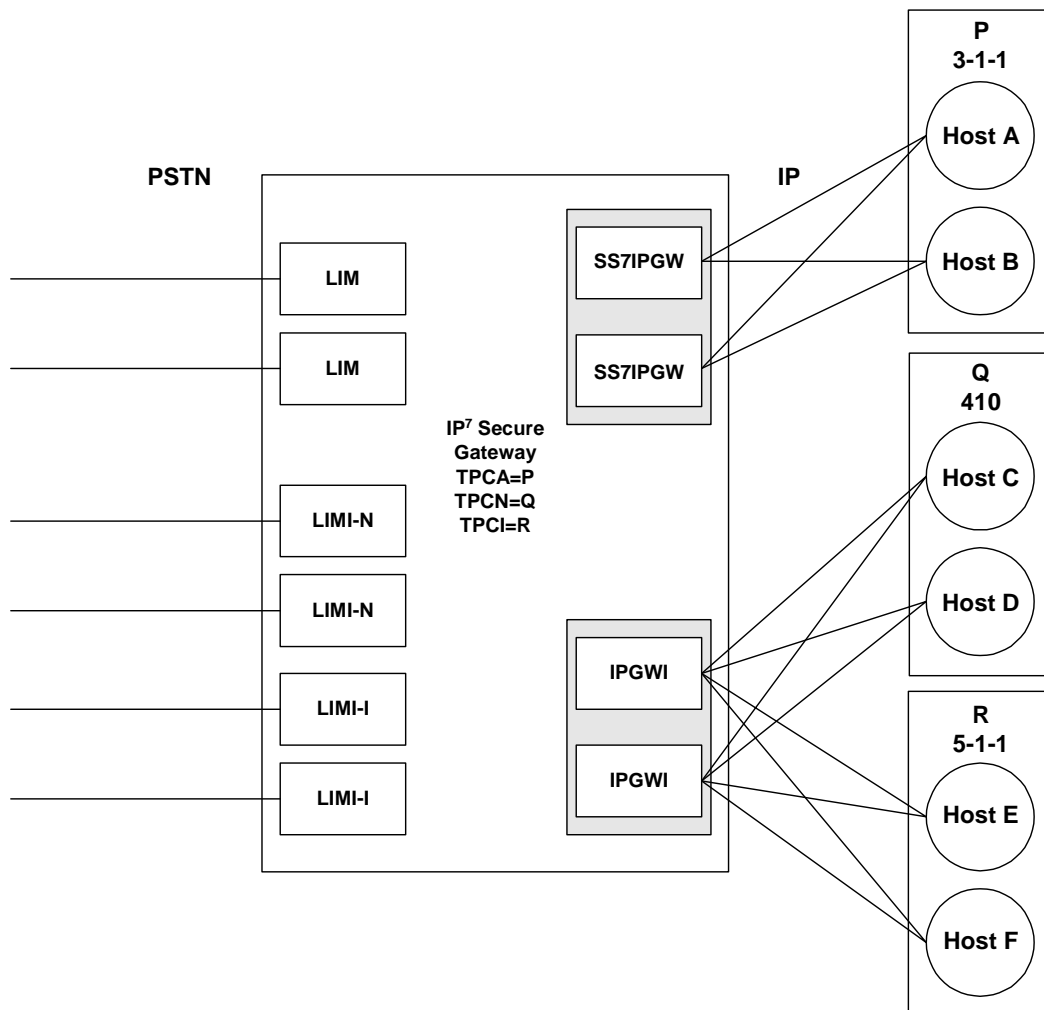
Notes regarding Figure 5-8:

- 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

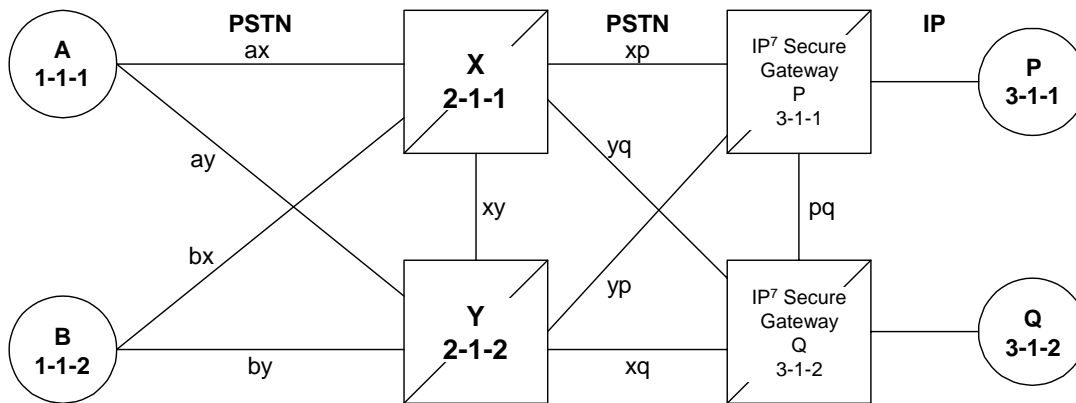


Figure 5-10 shows that a mated pair of systems cannot share an End Office Node. Each system requires its own unique point code and so any attached End Office Nodes share those point codes. It would be possible for a single IP network element to act as both P and Q (have IP connections to both system 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 SS7 Signaling Link” procedure in the *Database Administration Manual* - SS7.
- Sockets or associations (with the corresponding ASPs and application servers):
 - “Adding an Application Socket” procedure on page 3-89
 - “Adding an Association” procedure on page 6-19
 - “Adding an Application Server Process” procedure on page 6-71
 - “Adding an Application Server” procedure on page 6-85
- 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 `rttrv-sid` output) - “Adding a Static Application Routing Key” procedure on page 3-124.

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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-17 16:02:05 GMT Rel 31.0.0
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%
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 03-06-28 09:12:36 GMT Rel 31.0.0
ENT-RMT-APPL: MASP A - COMPLTD;
```

4. Verify the changes using the **rtrv-rmt-appl** command. This is an example of possible output:

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0
IPCA          SI SSN
000-000-001   3  5, 50-100
              13
003-003-003   3  100, 110-119, 200
              5

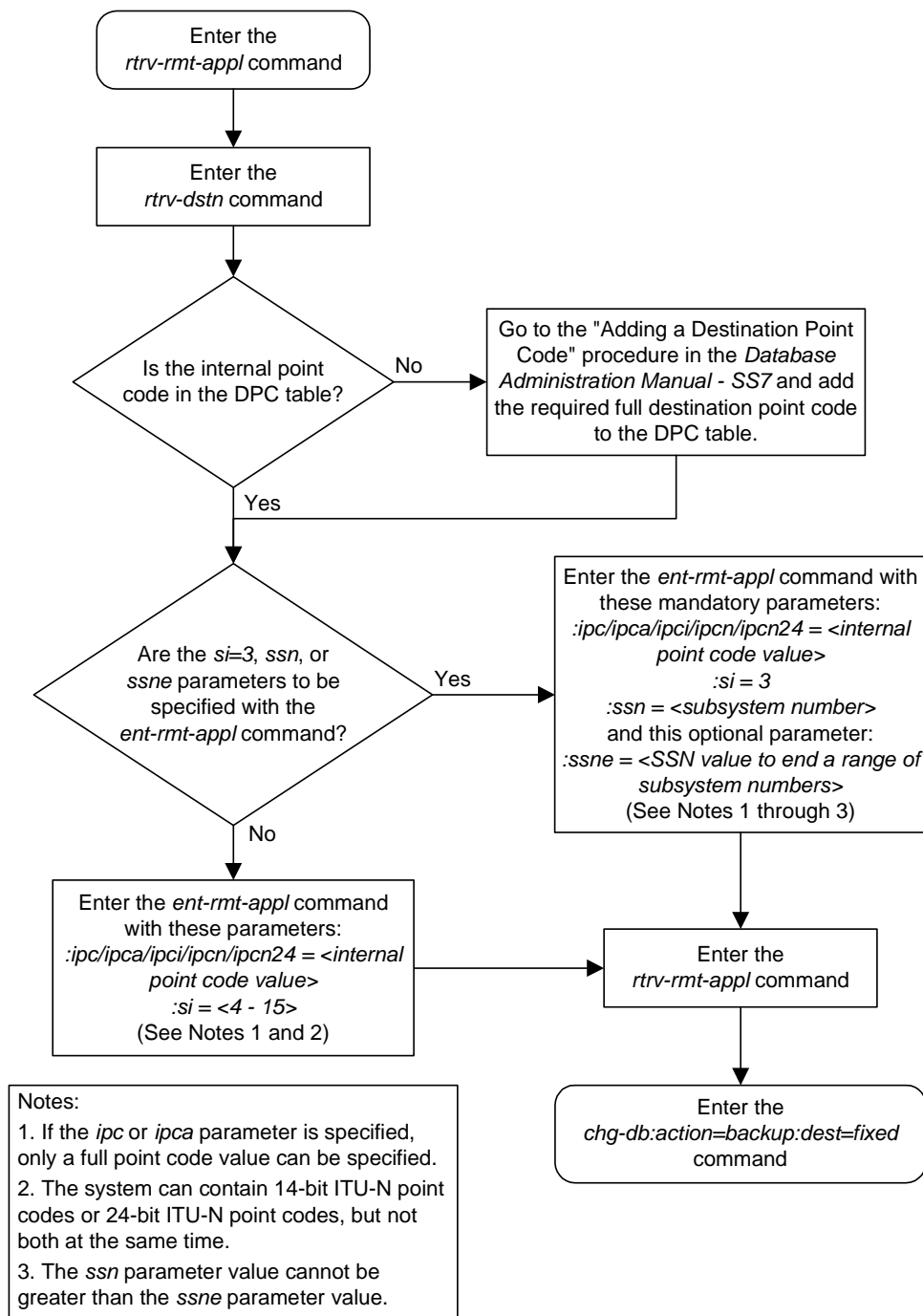
IPCI          SI SSN
3-003-3       3  5, 50-100, 250
              5

IPCN          SI SSN
16380         3  250
              5

IPCN24        SI SSN
```

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 03-06-28 09:12:36 GMT Rel 31.0.0
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 03-06-28 09:12:36 GMT Rel 31.0.0  
DLT-RMT-APPL: MASP A - COMPLTD;
```

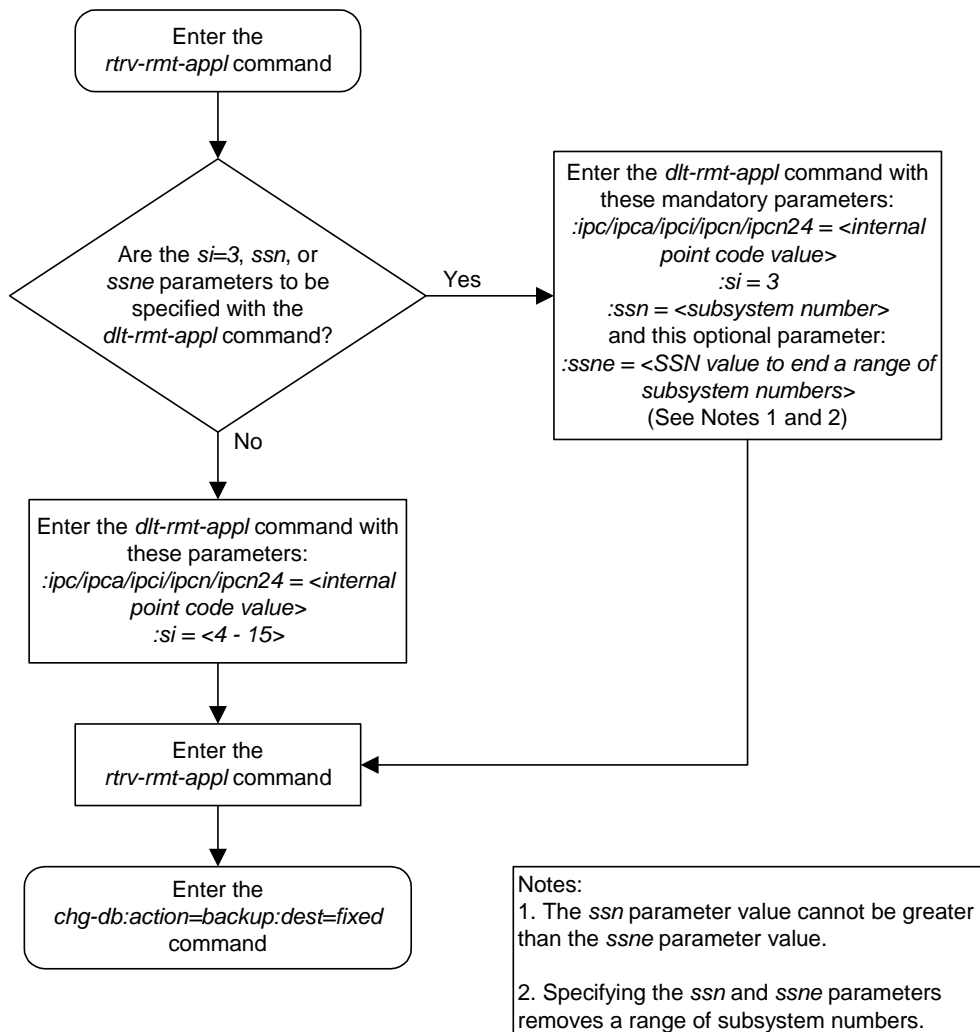
3. Verify the changes using the **rtrv-rmt-appl** command. This is an example of possible output:

```
rlghncxa03w 03-06-28 09:12:36 GMT Rel 31.0.0  
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



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 03-06-28 21:15:37 GMT Rel 31.0.0
System serial number = nt00001231
```

```
System serial number is not locked.
```

```
rlghncxa03w 03-06-28 21:15:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
The following features have been permanently enabled:
Feature Name      Partnum    Status    Quantity
TPS               893000101  on        100
```

```
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.
```

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 03-06-28 21:15:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
The following features have been permanently enabled:
Feature Name          Partnum    Status    Quantity
TPS                   893000101  on        100
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.
```

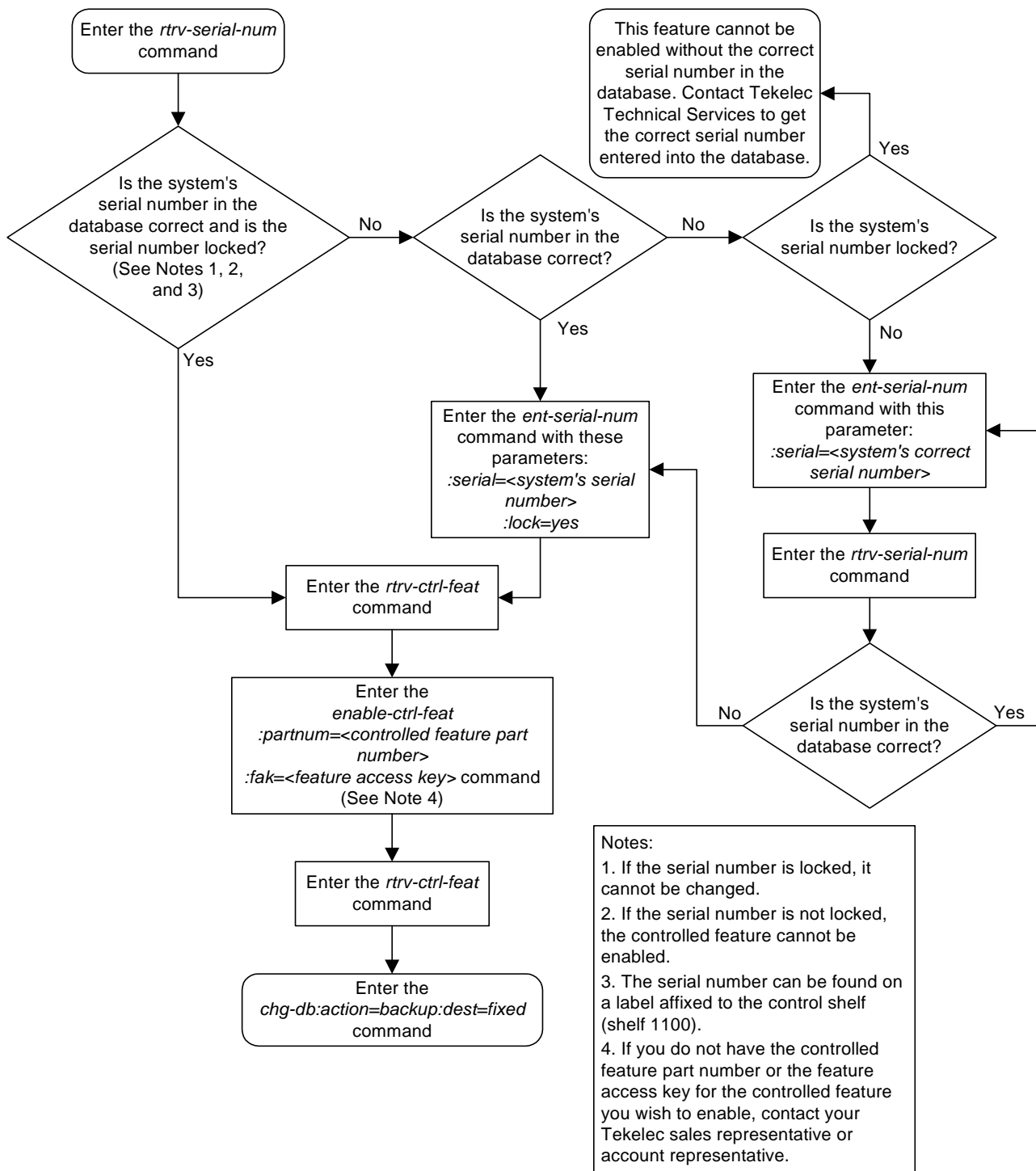
```
The following features have expired temporary keys:
Feature Name          Partnum
Zero entries found.
```

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.

Flowchart 6-1. Enabling a Permanent or Temporary Key



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 03-06-28 21:17:37 GMT Rel 31.0.0
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 03-06-30 21:16:37 GMT Rel 31.0.0
CHG-CTRL-FEAT: MASP A - COMPLTD
```

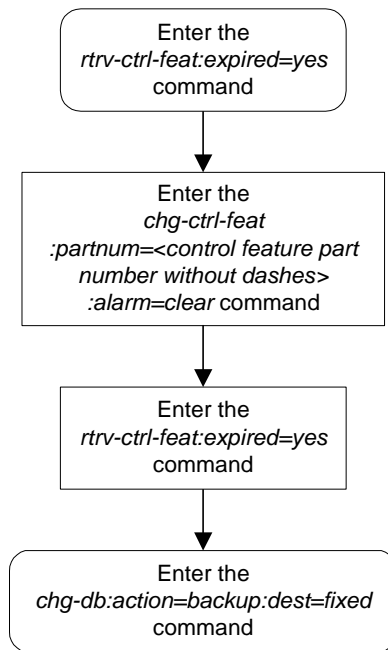
3. Verify that the alarm has cleared in the database by using the **rtrv-ctrl-feat:expired=yes** command. The following is an example of the possible output.

```
rlghncxa03w 03-06-28 21:16:37 GMT Rel 31.0.0
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.
```

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 03-06-28 21:15:37 GMT Rel 31.0.0
The following features have been permanently enabled:
Feature Name          Partnum    Status  Quantity
TPS                   893000101  on      100
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 03-06-28 21:15:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
The following features have been permanently enabled:
Feature Name          Partnum    Status  Quantity
TPS                   893000101  on      100
ISUP Normalization    893000201  on      ----
ETSI v3 Normalization 893000601  on      ----

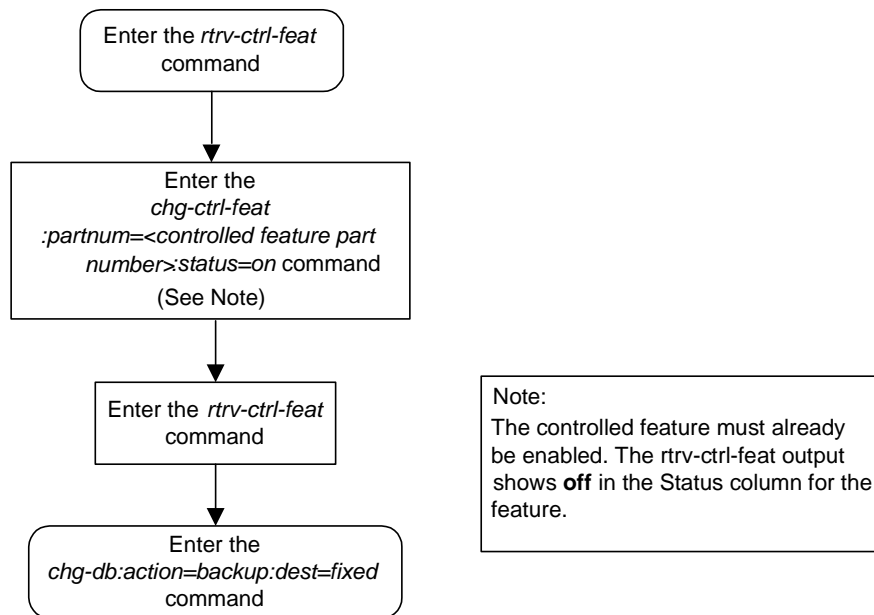
The following features have been temporarily enabled:
Feature Name          Partnum    Status  Quantity  Trial Period Left
Zero entries found.

The following features have expired temporary keys:
Feature Name          Partnum
Zero entries found.
```

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 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.

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 03-06-28 21:15:37 GMT Rel 31.0.0
The following features have been permanently enabled:
Feature Name      Partnum      Status      Quantity
TPS               893000101    on          100
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 03-06-28 21:15:37 GMT Rel 31.0.0
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 03-06-28 21:15:37 GMT Rel 31.0.0
The following features have been permanently enabled:
Feature Name          Partnum    Status  Quantity
TPS                   893000101  on      100
ISUP Normalization    893000201  off     ----
ETSI v3 Normalization 893000601  off     ----

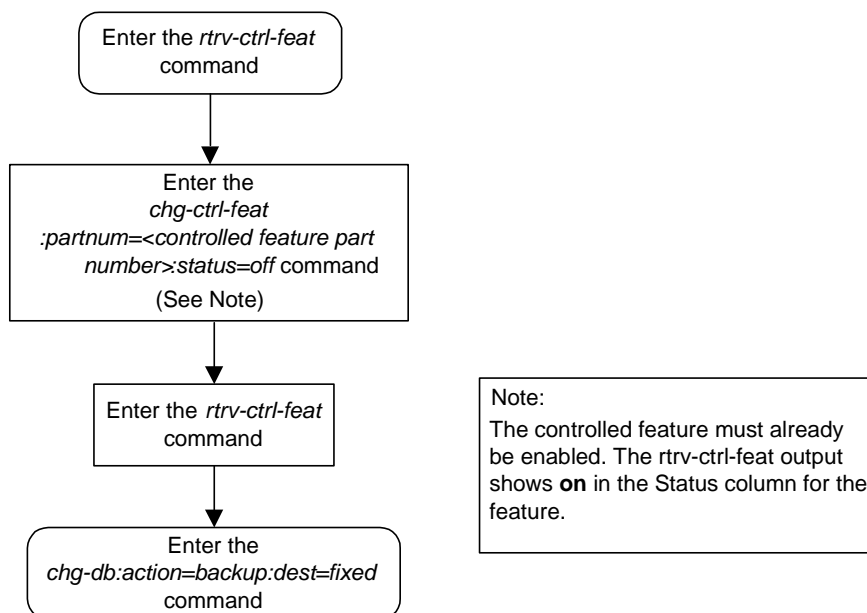
The following features have been temporarily enabled:
Feature Name          Partnum    Status  Quantity  Trial Period Left
Zero entries found.

The following features have expired temporary keys:
Feature Name          Partnum
Zero entries found.
```

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 6-4. Turning Off an Enabled Controlled Feature



Index

A

acronyms, 1-13
activate signaling link, act-slk
 IPGWI, 3-45, 3-53, 3-74, 3-93, 3-94,
 3-106, 3-107, 3-176, 3-179, 3-198, 3-200
 IPLIM, 3-53, 3-74
 SS7IPGW, 3-45, 3-53, 3-74, 3-93, 3-94,
 3-106, 3-107, 3-176, 3-179, 3-198, 3-200
Adding an Application Socket, 3-89
Adding an IP Host, 3-61
alw, 3-102
appl, 3-4
Applications, 2-3, 2-4

C

Changing a DCM Parameter Set, 3-120
Changing an Application Socket, 3-102
Changing an IP Card, 3-40, 3-61
Changing an IP Link, 3-66
Changing an IP7 Secure Gateway
 Option, 3-40
cice, 3-125, 3-133, 3-134, 3-140, 3-152
cics, 3-125, 3-133, 3-140, 3-152
Clearing a Temporary FAK alarm, 6-7
C-link linkset, 3-6
Configuring IP Retransmission
 Parameters, 3-114
Connectivity, 2-20, 2-21
customer support, 1-8
 Tekelec Technical Services, 1-8

D

database partitions
 overview, 1-10
dcm, 3-4
DCM parameter set, 3-3
dcmps, 3-102
Default Routing Keys, 2-25
Display, 3-43
display card status, rept-stat-card
 IPGWI, 3-43, 3-51, 3-71
 IPLIM, 3-43, 3-71
 SS7IPGW, 3-43, 3-51, 3-71

display signaling link status, rept-stat-slk
 IPGWI, 3-42, 3-45, 3-50, 3-53, 3-69, 3-74,
 3-93, 3-106, 3-176, 3-198, 3-268, 3-278
 IPLIM, 3-42, 3-53, 3-69, 3-74, 3-268,
 3-278
 SS7IPGW, 3-42, 3-45, 3-50, 3-53, 3-69,
 3-74, 3-93, 3-94, 3-107, 3-108, 3-177,
 3-179, 3-198, 3-201, 3-268, 3-278
documentation set, 1-3, 1-7
dpc, 3-133
drkq, 3-56

E

Eagle
 documentation set, 1-3
emergency response (Tekelec Technical
 Services), 1-8
Enabling a Permanent or Temporary
 Key, 6-3
End node internal point codes, 3-4
Errors
 contacting Tekelec Technical
 Services, 1-8

F

fixed disk drive
 overview, 1-11
Full Routing Keys, 2-24

G

getcomm, 3-56

I

in, 3-45, 3-53, 3-268, 3-278
inhfepalm, 3-56
internal point codes, 3-4
IP application routing key, 3-3
IP application server processes, 3-3
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, 3-56
 getcomm, 3-56
 inhfepalm, 3-56
 ipgwabate, 3-56
 iplimabate, 3-56
 sctpcsum, 3-56, 3-262, 3-293
 setcomm, 3-56
 snmpcont, 3-56
 srkq, 3-56
 sync, 3-49, 3-56
 trapcomm, 3-56
 IP protocol option, 3-49
 IP routes, 3-3
 IP7 Secure Gateway Options, 3-3
 ipgwabate, 3-56
 IPGWI
 activate signaling link, act-slk, 3-45,
 3-53, 3-74, 3-93, 3-94, 3-106, 3-107,
 3-176, 3-179, 3-198, 3-200
 display card status, rept-stat-card, 3-43,
 3-51, 3-71
 display signaling link status,
 rept-stat-slk, 3-42, 3-45, 3-50, 3-53,
 3-69, 3-74, 3-93, 3-106, 3-176, 3-198,
 3-268, 3-278
 ipgwi, 2-4, 2-21
 IPLIM
 activate signaling link, act-slk, 3-53,
 3-74
 display card status, rept-stat-card, 3-43,
 3-71
 display signaling link status,
 rept-stat-slk, 3-42, 3-53, 3-69, 3-74,
 3-268, 3-278
 iplim, 2-3
 iplimabate, 3-56
 iplimi, 2-3
 ISUP Normalization, 2-38
 ISUP variant provisioning, 3-4

M

maintenance and administration subsystem
 overview, 1-9

manual
 admonishments, 1-7
 organization, 1-2
 related publications, 1-3
 mated gateways, 3-6

N

Nagle's Algorithm, 2-37
 ncice, 3-140, 3-153
 ncics, 3-140, 3-153
 Network appearances, 3-3

O

opc/opca, 3-125, 3-133, 3-140, 3-152
 open, 3-102
 overview
 database partitions, 1-10
 fixed disk drive, 1-11
 maintenance and administration
 subsystem, 1-9
 removable cartridge, 1-12

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, 1-12
 Removing an Application Socket, 3-99
 Removing an DCM, 3-31, 3-85
 Removing an IP Card, 3-31, 3-85
 Routing Key Lookup Hierarchy, 2-27
 Routing Key Tables, 2-25

S

SCTP checksum algorithm option, 3-262,
 3-293
 sctpcsum, 3-56, 3-262, 3-293
 server, 3-102
 setcomm, 3-56

Index

si, 3-133
sname, 3-133
snmpcont, 3-56
split, 3-140, 3-153
srkq, 3-56
SS7IPGW
 activate signaling link, act-slk, 3-45,
 3-53, 3-74, 3-93, 3-94, 3-106, 3-107,
 3-176, 3-179, 3-198, 3-200
 display card status, rept-stat-card, 3-43,
 3-51, 3-71
 display signaling link status,
 rept-stat-slk, 3-42, 3-45, 3-50, 3-53,
 3-69, 3-74, 3-93, 3-94, 3-107, 3-108,
 3-177, 3-179, 3-198, 3-201, 3-268, 3-278
ss7ipgw, 2-4, 2-21
ssn, 3-133
sync, 3-49, 3-56

T

technical services, 1-8
Tekelec Technical Services, 1-8
 emergency response, 1-8
TPS on the DCM, 3-165
trapcomm, 3-56
turning On and Off Controlled
 Features, 6-10
Type of Service, 2-37

