Tekelec
LSMS

Release 11.0 Maintenance Manual

910-5423-001 Revision B
September 2008

Copyright 2007 Tekelec
All Rights Reserved
Printed in USA

Notice

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

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

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

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

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

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

Trademarks

The Tekelec logo, EAGLE, G-Flex, G-Port, IP7, IP7 Edge, and IP7 Secure Gateway are registered trademarks of Tekelec. TekServer, A-Port, and V-Flex are trademarks of Tekelec. All other trademarks are the property of their respective owners.

Patents

This product is covered by one or more of the following U.S. and foreign patents:
U.S. Patent Numbers:
5,732,213; 5,953,404; 6,115,746; 6,167,129; 6,324,183; 6,327,350; 6,456,845; 6,606,379; 6,639,981; 6,647,113; 6,662,017; 6,735,441; 6,745,041; 6,765,990; 6,795,546; 6,819,932; 6,836,477; 6,839,423; 6,885,872; 6,901,262; 6,914,973; 6,940,866; 6,944,184; 6,954,526;6,954,794; 6,959,076; 6,965,592; 6,967,956; 6,968,048; 6,970,542; 6,987,781; 6,987,849; 6,990,089; 6,990,347; 6,993,038; 7,002,988; 7,020,707; 7,031,340; 7,035,239; 7,035,387; 7,043,000; 7,043,001; 7,043,002; 7,046,667; 7,050,456; 7,050,562; 7,054,422; 7,068,773; 7,072,678; 7,075,331; 7,079,524; 7,088,728; 7,092,505; 7,108,468; 7,110,780; 7,113,581; 7,113,781; 7,117,411; 7,123,710; 7,127,057; 7,133,420; 7,136,477; 7,139,388; 7,145,875; 7,146,181; 7,155,206; 7,155,243; 7,155,505; 7,155,512; 7,181,194; 7,190,702; 7,190,772; 7,190,959; 7,197,036; 7,206,394; 7,215,748; 7,219,264; 7,222,192; 7,227,927; 7,231,024; 7,242,695; 7,254,391; 7,260,086; 7,260,207; 7,283,969; 7,286,516; 7,286,647; 7,286,839; 7,295,579; 7,299,050; 7,301,910; 7,304,957; 7,318,091; 7,319,857; 7,327,670
Foreign Patent Numbers:
EP1062792; EP1308054; EP1247378; EP1303994; EP1252788; EP1161819; EP1177660; EP1169829; EP1135905; EP1364520; EP1192758; EP1240772; EP1173969; CA2352246

Ordering Information

Your Tekelec Sales Representative can provide you with information about how to order additional discs.

Table of Contents

Chapter 1: Introduction.....1

Overview.....2
Scope and Audience.....2
What's New in This Release.....2
What's New in This Manual.....3
Compatibility.....3
Manual Organization.....3
Documentation Packaging and Updates.....4
Documentation Admonishments.....4
Customer Care Center.....5
Using a System Maintenance Log.....6

Chapter 2: LSMS Overview.....9

Introduction.....10
LSMS System Architecture.....10
LSMS Connectivity.....11
LSMS Hardware Overview.....12
How to Replace NAS Disk Drive Assemblies.....15
DC LSMS Hardware Overview.....17
AC LSMS Hardware Overview.....23
LSMS Software Overview.....25
Operating System Layer.....26
Base Platform Software.....26
Support/Base Utilities Components.....27
LSMS Applications.....28
Overview of High Availability.....31
Hardware Redundancies.....31
Software Availability Design.....33
Enhancing High Availability with a Shadow LSMS.....33
Understanding the Surveillance Feature.....34
Controlling the Surveillance Feature.....35
Understanding Surveillance Notifications.....36
Understanding the Service Assurance Feature.....37
Understanding the SNMP Agent Process.....40
Stopping the SNMP Agent.....41

Starting the SNMP Agent....42
Determining the Status of the SNMP Agent....42
Logging SNMP Agent Actions....42

Chapter 3: Routine Procedures....43
Introduction....44
Using Login Sessions....44
Logging In to LSMS Server Command Line....45
Logging in from One Server to the Mate's Command Line....47
Starting an LSMS GUI Session....47
Logging Into the LSMS Console Window....51
Modifying Title Bar in LSMS Console Window....53
Command Line Interface Utility....54
Powering On the LSMS....55
Powering Off the LSMS....56
Accessing LSMS through a Dial-In Connection....58
Managing the System Clock....59
Automatically Controlling the LSMS Time Using NTP....59
Manually Controlling the LSMS Time Without an External NTP Source....61
Managing User Accounts....62
Non-Configurable Permission Groups....64
Configurable Permission Groups (LSMS Command Class Mgmt)....67
Managing User Accounts on the Primary and Secondary Servers....69
Activating the SPID Security Feature....78

Chapter 4: Preventive Maintenance....79
Introduction....80
Recommended Daily Monitoring....80
Once a Day Monitoring Activities....80
LSMS Preventive Maintenance Schedule....81
Using Backup Procedures....82
Understanding How the LSMS Backs Up File Systems and Databases....82
Understanding the Backup Results....83
Storing Backup Tapes Off-Site....84
Backing Up the LSMS Manually....87
Stopping an Automatic or Manual Backup....92
Checking for Running Backups....93
Performing Routine Cleaning....94

Additional Tools for Monitoring the LSMS Hardware and the Network.....95
Verifying Active Server Network Interfaces and NPAC Connections.....95
Managing Automatic File Transfers.....100
Displaying Remote Locations Used for Automatic File Transfers.....100
Adding a New Remote Location for Automatic File Transfers.....101
Deleting a Remote Location for Automatic File Transfers.....102
Displaying Previously Scheduled Automatic File Transfers.....103
Scheduling an Automatic File Transfer.....104
Removing a Scheduled Automatic File Transfer.....105

Chapter 5: Restarting Software Processes.....107
Introduction.....108
Automatically Restarting Software Processes.....108
Automatically Monitoring and Restarting Eagle Agent Processes.....111
Automatically Monitoring and Restarting NPAC Agent Processes.....112
Automatically Monitoring and Restarting OSI Process.....112
Automatically Monitoring and Restarting the Service Assurance Process.....113
Automatically Monitoring and Restarting the rmtpmgr Process.....114
Automatically Monitoring and Restarting the rmtpagent Process.....114
Automatically Monitoring and Restarting Other Processes.....115

Chapter 6: Managing Server States.....117
Introduction.....118
Understanding Server States.....118
Understanding Switchover.....119
Understanding Automatic Switchover.....120
Managing Server States Manually.....123
Using the lsmsmgr Interface to Determine the Server Status.....123
Using the hastatus Command to Determine the Server Status.....124
Manually Switching Over from the Active Server to the Standby Server.....124
Inhibiting a Standby Server.....127
Starting a Server.....129

Chapter 7: Recovering from Site Failures.....131
Introduction.....132
Choosing a Disaster Backup Strategy.....132
Synchronizing Data Between the Main LSMS and Shadow LSMS.....135

Preparing for a Disaster Situation....136
Determining When to Switch to Shadow LSMS....136
Disaster Recovery Procedure Overview....137
Performing Disaster Recovery with an Active Shadow LSMS....143
Performing Disaster Recovery with an Inactive Shadow LSMS....144
Performing Disaster Recovery without a Shadow LSMS....146
Returning Operation from Shadow LSMS to Main LSMS....148
Restoring LSMS Data from Backup Tape....152
Resynchronizing After an Outage Between an NPAC and the LSMS....152
Reconnecting Network Elements....153
Reconnecting Network Elements Procedures....155

Chapter 8: Verifying Recovery....157
Introduction....158
Verifying that the LSMS Is Fully Functional....158
Verifying the State of the Servers....159
Verifying the Processes Running on the Active Server....159
Verifying the GUI Operability on the Active Server....160

Appendix A: Commands....161
Introduction....162
Entering LSMS and Third-Party Application Commands....165
autoxfercfg....166
chglct....168
chkfilter....170
eagle....172
hastatus....175
import....177
keyutil....182
lsms....184
lsmsdb....187
lsmsSNMP....191
lsmssurv....192
massupdate....195
measdump....200
npac_db_setup....202
npacimport....204
report....206
resync_db_setup....212
SAagent....214

spidsec....220
start_cmdLine....222
start_mgui....224
sup....225
sup_db_setup....226
survNotify....229
syscheck....230
Using lsmsclaa Commands....230
Using the lsmsclaa Application Interactively....231
Using the lsmsclaa Application with a Script File....231
Actions Available Through lsmsclaa 232
ABORT....235
ASSOCIATE....237
AUDIT....239
EXIT....241
HELP....242
SYNCH....242

Appendix B: Automatic Monitoring of Events....247

Introduction....248
Overview of Monitored Events....248
Overview of GUI Notifications....250
Format of GUI Notifications....251
Variables Used in Message Text String of GUI Notifications....254
Examples of GUI Notifications....255
Logging GUI Notifications....255
Overview of Surveillance Notifications....256
Variables Used in Surveillance Notification Format Descriptions....256
Variables Used in Message Text String of Surveillance Notifications....257
Example of a Surveillance Notification....258
Logging Surveillance Notifications....258
Overview of Traps....259
Logging SNMP Agent Actions....260
Event Descriptions....261
Platform Alarms....358
How to Decode Platform Alarms....359
Platform Alarms....360

Appendix C: Downloading Files from an NPAC to the LSMS....369

Overview....370
NPAC-LSMS Download Procedure Summary....370
Prerequisite Information....371
File Naming Conventions....372
NPAC-LSMS Download Procedure....376
Copying Files to Other Server If Switchover Occurs....388
Copying All Downloaded Files After Switchover....388
Copying Partially Downloaded Files After Switchover....389

Appendix D: Worksheets....391
Introduction....392
Recovery Preparation Worksheet....392

Appendix E: Query Server Maintenance Procedures....397
Introduction....398
LSMS Maintenance Procedures....398
Automatic Monitoring of Query Servers....399
Check Connection Status of Directly Connected Query Servers....400
Maintain the Binary Log on Query Servers....400
Check MySQL Replication Status on Query Servers....401
Start MySQL Replication on Query Servers....401
Stop MySQL Replication on Query Servers....402
Check for Running Backups....402
Reload a Query Server Database from the LSMS....402
Reload a Query Server Database from Another Query Server....406
Clean Up After Failed or Interrupted Snapshot....408
Automated System Check....409
Query Server Error Log....410
Retrieving Information from LNP Database Fields....411
LNP Database Tables and Fields....413
Query Server Database Structure....417
Glossary....453

List of Figures

Figure 1: LSMS System Architecture....10
Figure 2: NAS Front View, Doors Closed....14
Figure 3: NAS Front View, Doors Open....14
Figure 4: NAS Rear View....14
Figure 5: NAS Drive Cover Door (Opened)....15
Figure 6: NAS Drive Latch....16
Figure 7: NAS Drive Carrier with Mounting Screws....16
Figure 8: DC LSMS System - Front View....17
Figure 9: T1100 LSMS Breaker Panel Front and Rear Views....18
Figure 10: Breaker Panel LEDs....19
Figure 11: T1100 LSMS Breakers....22
Figure 12: AC LSMS System....23
Figure 13: Power Distribution Unit, Front and Rear Views....24
Figure 14: Software Allocation on the LSMS Platform....25
Figure 15: LSMS Applications....28
Figure 16: LSMS Servers Connected with Heartbeat Links....31
Figure 17: T1100 - Rear View - Showing Serial Ports....34
Figure 18: Service Assurance System within a Network....37
Figure 19: lsmsmgr Text Interface Main Menu....46
Figure 20: Tekelec LSMS Building Smart Networks Web Page....49
Figure 21: LSMS Web GUI Start Page with Login Button....50
Figure 22: LSMS Welcome/Login Window....50
Figure 23: LSMS Welcome/Login Window....51
Figure 24: LSMS Console Window....52
Figure 25: Example of Login Message Dialog....53
Figure 26: LSMS Console Window with Modified Title Bar....54
Figure 27: T1100 Showing Power LEDs....56
Figure 28: Example Cautionary Message - Displayed after Selecting Stop Node....57
Figure 29: Example Message - Stop Node Completed Successfully....57
Figure 30: Set Clock Window....61
Figure 31: Edit Date or Time Window....61
Figure 32: Select AdminPassword TimeoutSystem LevelModify 72
Figure 33: Modify System Level Password Timeout....73
Figure 34: Update Successful....73
Figure 35: Select AdminPassword TimeoutUser LevelModify 74
Figure 36: Modify User Level Password Timeout....74
Figure 37: Update Successful....75

Figure 38: Select User/SessionView Active User Sessions 75
Figure 39: View Active User Sessions Dialog....76
Figure 40: Select User/SessionTerminate User Session 76
Figure 41: Terminate User Session Dialog....77
Figure 42: Confirm Delete Dialog....77
Figure 43: Delete Successful Dialog....77
Figure 44: Example of Successful Backup Log for STANDBY Server....83
Figure 45: Example of Successful Backup Log for ACTIVE Server....83
Figure 46: Example of Unsuccessful Backup Log for ACTIVE Server....83
Figure 47: System Busy - Retrieving Backup Server Directory Listing....84
Figure 48: Available Archives Menu....85
Figure 49: Specific Available db Archives....85
Figure 50: System Busy - Dumping Archive to Tape....86
Figure 51: Available Archives Menu....86
Figure 52: Select Backup Configuration Menu Window....88
Figure 53: Select Backup on Active Server....88
Figure 54: Backup Complete on Active Server....88
Figure 55: Select plat.xml on Standby Server....89
Figure 56: Select Backup on Standby Server....89
Figure 57: Performing Backup Screen....89
Figure 58: Backup Complete on Standby Server....89
Figure 59: Select lsmslogs.xml on Standby Server....90
Figure 60: Select Backup on Standby Server....90
Figure 61: Backup Complete on Standby Server....90
Figure 62: Select lsmsdb.xml on Standby Server....91
Figure 63: Select Action Menu....91
Figure 64: Backup....91
Figure 65: Backup Complete....92
Figure 66: TraceRoute....98
Figure 67: TraceRoute Results....98
Figure 68: Order of Automatically Restarting Processes....110
Figure 69: Unable to Switchover to Standby....121
Figure 70: LSMS Node Status....123
Figure 71: Inhibit Active Node....125
Figure 72: Check Network Status on Standby Node....125
Figure 73: Confirm Switchover....125
Figure 74: Manual Switchover In Progress....126
Figure 75: Manual Switchover Complete....126
Figure 76: Inhibit a Non-Active Server....127
Figure 77: Node Successfully Inhibited....128
Figure 78: Starting a Server....129

Figure 79: Overview of Main LSMS and Active Shadow LSMS.....132
Figure 80: Overview of Main LSMS and Inactive Shadow LSMS.....133
Figure 81: Overview of Main LSMS without a Shadow LSMS.....134
Figure 82: Example of SA Agent Status Output.....216
Figure 83: Example -- No Associations Status Output.....217
Figure 84: Example -- Marked Inhibited Status Output.....218
Figure 85: Example -- Active Associations Status Output.....218
Figure 86: GUI Notifications.....250
Figure 87: Query Server Configuration Scenario.....398
Figure 88: Automated System Check Output Example - OK.....409
Figure 89: Automated System Check Output Example - FAILURE.....410
Figure 90: Automated System Check Output Example - WARNING.....410
Figure 91: Query Server Error Log Example.....411

List of Tables

Table 2: Example of the System Maintenance Log Sheet....6
Table 3: LSMS Hardware Components....12
Table 4: Breaker Panel LED Settings....20
Table 5: Mapping of Active (Closed) Breakers to Devices....23
Table 6: Parameters Used in Accessing Server Command Line....45
Table 7: Parameters Used by Command Line Interface....55
Table 8: User Types....64
Table 9: Access to LSMS Commands....65
Table 10: Define GUI Permission Groups and Assign Command Privileges....68
Table 11: User Assignment Examples....68
Table 12: Interpreting traceroute Output....99
Table 13: Processes Monitored by the Automatic Software Recovery Feature....108
Table 14: LSMS Server States....118
Table 15: Comparison of Recovery Procedures to Perform....138
Table 16: Recovery Procedures When LSMS Shadow Is Active....143
Table 17: Recovery Procedures When LSMS Shadow Is Inactive....145
Table 18: Recovery Procedures When No LSMS Shadow Exists....147
Table 19: Procedures to Return Operations from Shadow LSMS to Main LSMS....149
Table 20: Recovery Acceptance Tests....158
Table 21: LSMS Application Functions and Third-Party Commands Available at the command-line Prompt....162
Table 22: LSMS Functions Available Through lsmsclaa and Through GUI....164
Table 23: Error Messages: autoxfercfg....167
Table 24: Files: autoxfercfg....168
Table 25: Time Value for chglct....169
Table 26: Error Messages: chglct....170
Table 27: Files: chkfilter....171
Table 28: Error Messages: chkfilter....172
Table 29: Exit Codes: eagle....174
Table 30: Error Messages: hastatus....175
Table 31: Files: import....180
Table 32: Error Messages: import....180
Table 33: Error Messages: keyutil....183
Table 34: Error Messages: lsms....186
Table 35: Files: lsmsSNMP....192
Table 36: Exit Codes: lsmsSNMP....192
Table 37: Files: lsmssurv....194

Table 38: Error Messages: lsmssurv....195
Table 39: Tables/Fields Affected By SIC-SMURF Processing....197
Table 40: Error Codes: massupdate....199
Table 41: Measurement Pegs Date....201
Table 42: Error Messages: measdump....202
Table 43: Error Messages: npac_db_setup....204
Table 44: Exit Codes: npacimport....206
Table 45: Files: report....209
Table 46: Error Messages: report....210
Table 47: Exit Codes: resync_db_setup....213
Table 48: Files: SAagent....216
Table 49: SAagent Command Usage....216
Table 50: Error Messages: SAagent....219
Table 51: Exit Codes: spidsec....221
Table 52: Error Messages: start_cmdLine....224
Table 53: Exit Codes: sup....226
Table 54: Error Messages: sup_db_setup....228
Table 55: Exit Codes: survNotify....229
Table 56: LSMS Functions Available Through lsmsclaa....232
Table 57: Return Codes Generated While Running lsmsclaa....233
Table 58: Possible Output and Return Codes Generated by ABORT....236
Table 59: Possible Output and Return Codes Generated by ASSOCIATE....238
Table 60: Possible Output and Return Codes Generated by AUDIT....240
Table 61: Possible Output and Return Codes Generated by SYNCH....245
Table 62: Notification Event Number Categories....249
Table 63: Variables Used in GUI Notifications....252
Table 64: Variables Used in Message Text of GUI Notifications....254
Table 65: Logs for GUI Notifications....255
Table 66: Variables Used in Surveillance Notifications....256
Table 67: Variables Used in Message Text of Surveillance Notifications....257
Table 68: Information Logged by the LSMS SNMP Agent....260
Table 69: Event 0001 Details....261
Table 70: Event 0002 Details....262
Table 71: Event 0003 Details....262
Table 72: Event 0004 Details....263
Table 73: Event 0006 Details....264
Table 74: Event 0007 Details....265
Table 75: Event 0008 Details....266
Table 76: Event 0009 Details....266
Table 77: Event 0010 Details....267
Table 78: Event 0011 Details....268

Table 79: Event 2000 Details....269
Table 80: Event 2001 Details....269
Table 81: Event 2002 Details....270
Table 82: Event 2003 Details....271
Table 83: Event 2004 Details....272
Table 84: Event 2005 Details....273
Table 85: Event 2006 Details....274
Table 86: Event 2007 Details....275
Table 87: Event 2008 Details....276
Table 88: Event 2009 Details....276
Table 89: Event 2010 Details....277
Table 90: Event 2011 Details....278
Table 91: Event 2012 Details....279
Table 92: Event 2014 Details....280
Table 93: Event 2015 Details....281
Table 94: Event 2018 Details....282
Table 95: Event 2019 Details....283
Table 96: Event 2020 Details....284
Table 97: Event 2021 Details....284
Table 98: Event 2022 Details....285
Table 99: Event 2023 Details....286
Table 100: Event 2024 Details....287
Table 101: Event 2025 Details....288
Table 102: Event 4000 Details....288
Table 103: Event 4001 Details....289
Table 104: Event 4002 Details....290
Table 105: Event 4004 Details....290
Table 106: Event 4007 Details....291
Table 107: Event 4008 Details....292
Table 108: Event 4009 Details....293
Table 109: Event 4011 Details....293
Table 110: Event 4012 Details....295
Table 111: Event 4013 Details....296
Table 112: Event 4014 Details....296
Table 113: Event 4015 Details....297
Table 114: Event 4020 Details....298
Table 115: Event 4021 Details....299
Table 116: Event 4022 Details....299
Table 117: Event 4023 Details....300
Table 118: Event 4024 Details....301
Table 119: Event 4025 Details....302

Table 120: Event 4026 Details....302
Table 121: Event 4027 Details....303
Table 122: Event 4030 Details....304
Table 123: Event 4031 Details....304
Table 124: Event 4032 Details....305
Table 125: Event 4033 Details....306
Table 126: Event 4100 Details....307
Table 127: Event 4101 Details....307
Table 128: Event 4200 Details....308
Table 129: Event 4201 Details....309
Table 130: Event 4300 Details....310
Table 131: Event 4301 Details....310
Table 132: Event 6000 Details....311
Table 133: Event 6001 Details....312
Table 134: Event 6002 Details....313
Table 135: Event 6003 Details....313
Table 136: Event 6004 Details....314
Table 137: Event 6005 Details....315
Table 138: Event 6006 Details....316
Table 139: Event 6008 Details....316
Table 140: Event 6009 Details....317
Table 141: Event 6010 Details....318
Table 142: Event 6020 Details....319
Table 143: Event 8000 Details....319
Table 144: Event 8001 Details....320
Table 145: Event 8003 Details....321
Table 146: Event 8004 Details....322
Table 147: Event 8005 Details....322
Table 148: Event 8024 Details....323
Table 149: Event 8025 Details....324
Table 150: Event 8026 Details....325
Table 151: Event 8027 Details....325
Table 152: Event 8037 Details....326
Table 153: Event 8038 Details....327
Table 154: Event 8039 Details....327
Table 155: Event 8040 Details....328
Table 156: Event 8049 Details....329
Table 157: Event 8050 Details....330
Table 158: Event 8051 Details....331
Table 159: Event 8052 Details....331
Table 160: Event 8053 Details....332

Table 161: Event 8054 Details....333
Table 162: Event 8055 Details....334
Table 163: Event 8059 Details....334
Table 164: Event 8060 Details....335
Table 165: Event 8061 Details....336
Table 166: Event 8064 Details....336
Table 167: Event 8065 Details....337
Table 168: Event 8066 Details....338
Table 169: Event 8067 Details....339
Table 170: Event 8068 Details....339
Table 171: Event 8069 Details....340
Table 172: Event 8070 Details....341
Table 173: Event 8071 Details....342
Table 174: Event 8072 Details....342
Table 175: Event 8073 Details....343
Table 176: Event 8078 Details....344
Table 177: Event 8079 Details....344
Table 178: Event 8080 Details....345
Table 179: Event 8081 Details....346
Table 180: Event 8082 Details....347
Table 181: Event 8083 Details....347
Table 182: Event 8084 Details....348
Table 183: Event 8085 Details....349
Table 184: Event 8088 Details....349
Table 185: Event 8089 Details....350
Table 186: Event 8090 Details....351
Table 187: Event 8091 Details....352
Table 188: Event 8096 Details....352
Table 189: Event 8097 Details....353
Table 190: Event 8098 Details....354
Table 191: Event 8099 Details....357
Table 192: Event 8100 Details....358
Table 193: LSMS Platform Alarms....360
Table 194: Determining Naming Conventions for NPAC Data Files....372
Table 195: NPAC File Naming Convention for Subscription Version Data File....373
Table 196: NPAC File Naming Convention for Number Pool Block Data File....374
Table 197: NPAC File Naming Convention for LRN, NPA-NXX, and NPA-NXXX Network Data Files....375
Table 198: NPAC File Naming Convention for SPID Network Data File....376
Table 199: NPAC Bulk Load Files and LSMS Database Object Classes....386
Table 200: Recovery Preparation Worksheet....392

Table 201: Regional Database Tables and Fields.....413
Table 202: Supplemental Database Tables and Fields (Part 1).....414
Table 203: Supplemental Database Tables and Fields (Part 2).....415

Chapter 1

Introduction

Topics:

- *Overview Page 2*
- *Scope and Audience Page 2*
- *What's New in This Release Page 2*
- *What's New in This Manual Page 3*
- *Compatibility Page 3*
- *Manual Organization Page 3*
- *Documentation Packaging and Updates Page 4*
- *Documentation Admonishments Page 4*
- *Customer Care Center Page 5*
- *Using a System Maintenance Log Page 6*

This manual contains the information necessary for system administration of a Local Service Management System (LSMS).

Overview

This manual contains the information necessary for system administration of a Local Service Management System (LSMS). Included are an overview of the LSMS design, routine operation procedures, preventive maintenance techniques, corrective maintenance procedures, and appendixes that describe LSMS commands and notifications.

Scope and Audience

This manual is written for system administrators of the LSMS. The manual provides routine operating procedures as well as preventive and corrective procedures that aid administrators maintaining the LSMS.

- *Preventive maintenance* procedures are routines implemented on a scheduled basis to help prevent system faults. These tasks are industry standard recommendations and are adaptable to any company's maintenance plan.
- *Corrective maintenance* procedures are those used in response to a system alarm or output message. These procedures are LSMS-specific and aid in the detection, isolation, and repair of faults.

The manual assumes the system administrator is familiar with the Linux operating system.

What's New in This Release

LSMS Release 11.0 retains all of the functionality of Release 10.0. Release 11.0 features changes to the LSMS GUI in support of a single VIP connection to ELAP 8.0. Release 11.0 also includes the new, optional 384 Million Records feature.

LSMS GUI supports a single VIP connection to ELAP 8.0. The LSMS GUI will also continue to support connections to ELAP 7.0 and older, where the entry of an IP address for both ELAP A and ELAP B is still required. GUI changes affect the Create, Modify, View, and Delete EMS Configuration components.

The optional 384 Million Records feature increases the maximum number of ported telephone numbers and number pool blocks supported on the LSMS from 228 million to 384 million. The maximum number of ported numbers supported is dependent on the number of NPAC regions configured. If only one NPAC is interfaced with the LSMS, up to 96 million ported numbers and NPBs can be supported in a single NPAC region. If multiple NPACs are interfaced with the LSMS, the total number of ported records supported across all NPAC databases is 384 million, where no individual region exceeds 96 million.

Part of the 384 Million Records feature is the Support ELAP Reload Via Database Image (SERVDI) function. SERVDI is a new method to perform BDDs that results in a significant reduction in the time needed to reload an ELAP database.

What's New in This Manual

Miscellaneous updates and clarifications occur throughout the manual.

Compatibility

For information about which products this release of LSMS is compatible with, refer to the *Feature Notice* for this release.

Manual Organization

The manual contains the following chapters:

- *Introduction* on page 1 contains general information about the organization of the manual, description of the LSMS document suite, and a list of acronyms and abbreviations.
- *LSMS Overview* on page 9 provides a high-level overview of the LSMS hardware and software design for high availability and an overview of software components.
- *Routine Procedures* on page 43 explains the routine procedures that system administrators regularly perform, such as establishing remote logins, setting the system clock, and managing user accounts.
- *Preventive Maintenance* on page 79 explains preventive maintenance topics, such as the LSMS preventive maintenance schedule, backup procedures, routine cleaning, and monitoring the hardware and network.
- *Restarting Software Processes* on page 107 explains how to verify whether software processes are running and how software processes can be automatically or manually restarted.
- *Managing Server States* on page 117 describes how automatic switchover occurs for certain failure conditions and how to manually manage the states of the primary and secondary servers.
- *Recovering from Site Failures* on page 131 describes and compares various backup strategies for disaster situations in which an entire LSMS site can no longer function. This chapter describes how to prepare for disaster recovery and, for each disaster recovery strategy, describes the recovery procedures and a list of assumptions.
- *Verifying Recovery* on page 157 describes the processes used to verify that recovery is acceptable after recovering from site failures.
- *Commands* on page 161 describes the purpose and syntax for all LSMS commands and provides sample output for each.
- *Automatic Monitoring of Events* on page 247 describes how the LSMS automatically monitors itself for certain events, including error conditions, and reports those events with GUI notifications, Surveillance notifications, and/or traps sent to a remote monitoring device. This appendix lists all events in numerical order and provides explanations and suggested recovery for each event.

- *Downloading Files from an NPAC to the LSMS* on page 369 contains the prerequisite information and procedure needed for downloading files from an NPAC. One example for using this procedure is when all the files for an entire regional database needs to be downloaded as part of recovering after a site failure.
- *Worksheets* on page 391 contains blank worksheets that you can copy and use in the procedures described in other chapters.
- *Query Server Maintenance Procedures* on page 397 contains detailed, step-by-step procedures for maintaining the query server.

Documentation Packaging and Updates

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

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

Documentation Admonishments

Admonishments are icons and text that may appear in this and other EAGLE 5 ISS and LSMS 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 ***personal injury*** .)
	WARNING: (This icon and text indicate the possibility of ***equipment damage*** .)
	CAUTION: (This icon and text indicate the possibility of ***service interruption*** .)

Customer Care Center

The Tekelec Customer Care Center 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 Customer Care Center can connect customers to the Tekelec Technical Services department, which is staffed with highly trained engineers to provide solutions to 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 customers' needs.

To receive technical assistance, call the Customer Care Center at one of the following locations:

- Tekelec, USA

  Phone (within the continental US) +1 888-367-8552 (888-FOR-TKLC)

  Phone (outside the continental US) +1 919-460-2150.

  Email: `support@tekelec.com`.

When your call is received, the Customer Care Center issues a Customer Service Report (CSR). Each CSR includes an individual tracking number. When a CSR is issued, the Customer Care Center determines the classification of the trouble. The CSR contains the serial number of the system, problem symptoms, and messages. The Customer Care Center assigns the CSR to a primary engineer, who will work to solve the problem. The Customer Care Center closes the CSR when the problem is resolved.

If a critical problem exists, the Customer Care Center initiates emergency procedures (see the following topic, *"Emergency Response"*).

Emergency Response

If a critical service situation occurs, the Tekelec Customer Care Center 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 LSMS problem that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical problems affect service or system operation, resulting in:

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

Using a System Maintenance Log

Below is an example of a system maintenance log. Use this table to generate copies for your site. Tekelec recommends that you complete this log after every preventive and corrective maintenance procedure.

This log provides both maintenance personnel and the Tekelec Technical Services personnel a complete trouble history for the specific site. This aids in spotting trouble trends which, left unrecorded, would be impossible to detect.

This is a troubleshooting aid, and should be filled out completely. Printouts or any other supportive material should be referenced whenever possible. Tekelec Technical Services personnel may ask for some of this information at a later time if a particular trend begins to develop.

Table 1: Example of the System Maintenance Log Sheet

Date	Trouble Description	Action	Init

Date	Trouble Description	Action	Init

Chapter 2

LSMS Overview

Topics:

- *Introduction Page 10*
- *LSMS System Architecture Page 10*
- *LSMS Connectivity Page 11*
- *LSMS Hardware Overview Page 12*
- *LSMS Software Overview Page 25*
- *Overview of High Availability Page 31*
- *Enhancing High Availability with a Shadow LSMS Page 33*
- *Understanding the Surveillance Feature Page 34*
- *Understanding the Service Assurance Feature Page 37*
- *Understanding the SNMP Agent Process Page 40*

This chapter provides an overview of LSMS system architecture, proactive termination and re-establishment of LSMS connectivity, hardware and software design features that provide high availability of the LSMS, and third-party and Tekelec software components used by the LSMS.

Introduction

The LSMS is a secure and reliable LNP (Local Number Portability) system that enables customers to administer their LNP data in a central place. The LSMS provides the following functions:

- Receives LNP data from NPACs (Number Portability Administration Centers)
- Enables customers to enter locally provisioned data such as OGTT (Override Global Title Translation) data
- Forwards all NPAC and locally provisioned data to up to eight EAGLE 5 ISSs (Signaling Application Systems)

For more information about the LNP functions provided by the LSMS, refer to the LSMS Database *Administration Manual* and the LSMS-EAGLE 5 ISS LNP Database *Synchronization Manual*.

This chapter provides an overview of:

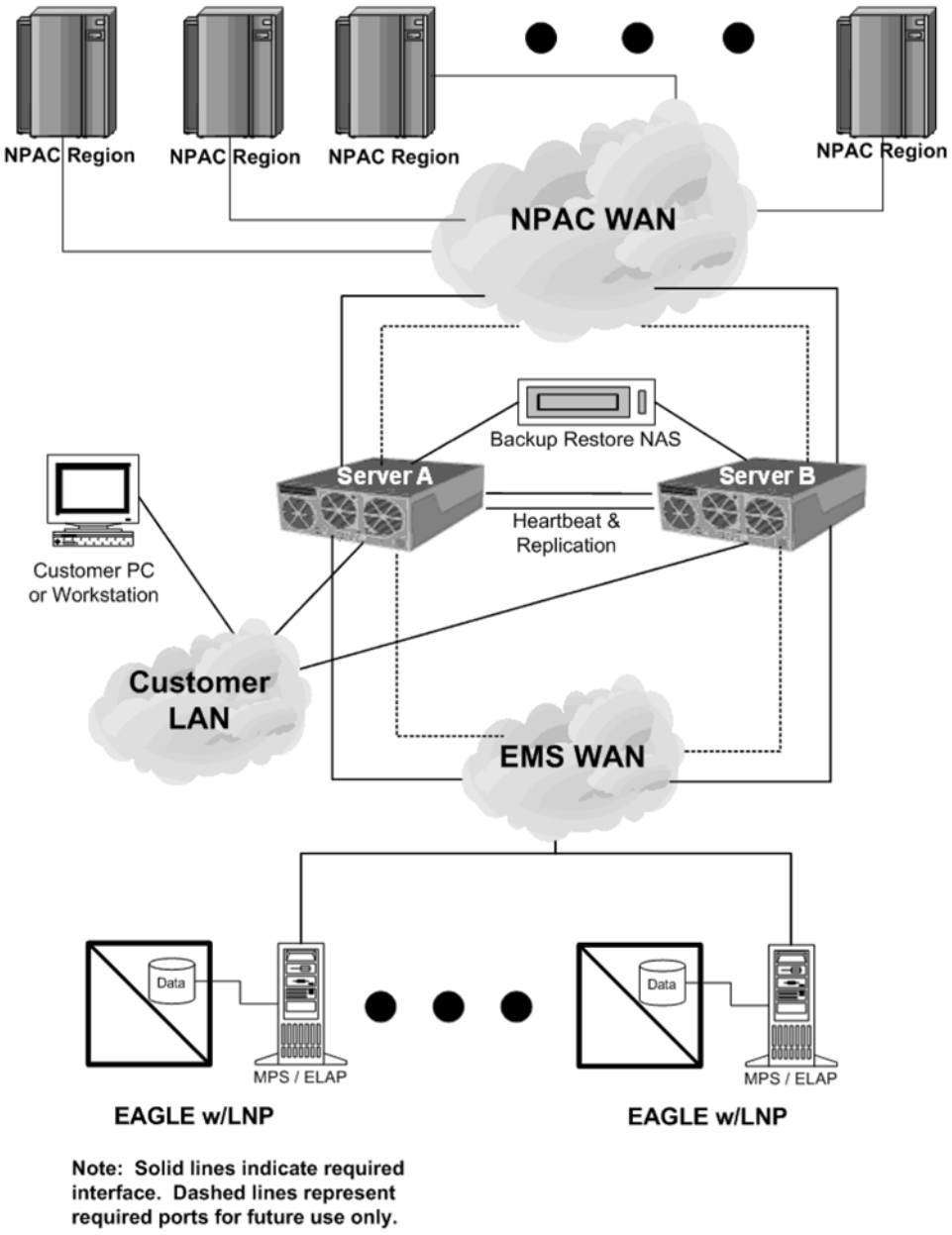
- LSMS system architecture
- Proactive termination and re-establishment of LSMS connectivity
- Hardware and software design features that provide high availability of the LSMS
- Third-party and Tekelec software components used by the LSMS

For additional information about the hardware, refer to the *T1100* Application Server *Hardware Manual*.

LSMS System Architecture

Figure 1: LSMS System Architecture on page 10 shows the LSMS system architecture.

Figure 1: LSMS System Architecture



LSMS Connectivity

The main function of the LSMS is to provision LNP data to the Eagle. In order to perform this task, the LSMS maintains active connections with one or more NPAC region servers and one or more Eagle nodes. While it is the goal of the LSMS to maintain active connections to each NPAC server and Eagle node as nearly full-time as possible, the more important goal is to reliably forward the data from the NPAC to the Eagle as quickly as possible. To that end, a number of protective problem detection and recovery mechanisms are built into the LSMS design. Several of these

protections actually allow for the termination of application connectivity in order to gracefully restore full connectivity and guarantee total recovery of data.

The performance of the LSMS is based on network connectivity that meets a Quality of Service expectation. The expectations by Tekelec for network Quality of Service are as follows:

- Network RTT latency of <= 70ms and network loss due to network error <= 0.1%

OR

- Network RTT latency of <= 120ms and network loss due to network error <= 0.01%

In the following situations, the LSMS proactively terminates and re-establishes application connectivity with the NPAC and Eagles:

- If the LSMS detects network level connectivity failures with either the NPAC or Eagle, the respective LSMS processes terminate the socket level connection and then reconnect. This disconnect and reconnect occurs in a matter of seconds. Built in resynchronization mechanisms ensure data recovery. The data transmission is delayed by the time required to disconnect and reconnect, but the execution of the recovery procedures prevents data loss.
- If the LSMS detects critical internal errors that would cause system outages, the LSMS processes are designed to terminate and allow the LSMS `sentry` process to restart them. This is only done for significant internal errors that jeopardize internal LSMS communications. Once the `sentry` process restarts the LSMS processes, resynchronization provides full data recovery.

LSMS Hardware Overview

LSMS hardware is available in either AC (Alternating Current) or DC (Direct Current) versions. The components are similar for each version, as described in *Table 2: LSMS Hardware Components* on page 12. The following sections describe the hardware common to each version, and the configuration and version-specific hardware for each version.

Table 2: LSMS Hardware Components

Qty	Hardware Item	For more detail, see:	To replace, see:
2	Tekelec 1100 AS main unit; each unit has the following cards added during manufacturing: • One quad-port gigabit Ethernet Peripheral Component Interconnect (PCI) cards • Two dual-port gigabit Ethernet PCI cards • One Out-of-Band-Management	*Tekelec 1100* Application Server *Hardware Manual*	*Tekelec 1100* Application Server *Hardware Manual*

Qty	Hardware Item	For more detail, see:	To replace, see:
	(OOBM) PCI card that contains: • One serial port • One modem interface • One Ethernet port • One interface for alarm relays Each Tekelec 1100 AS main unit has 8 gigabytes of Random Access Memory (RAM) installed and available.		
1	Network Attached Storage (NAS) 1	*Network Attached Storage* on page 13	Contact the Tekelec Customer Care Center.
1	Breaker panel (for DC version only)	*Breaker Panel* on page 18	*Tekelec 1100* Application Server *Hardware Manual*
2	Power Distribution Units (for AC version only)	*Tekelec 1100* Application Server *Hardware Manual*	*Tekelec 1100* Application Server *Hardware Manual*

T1100 Application Server

LSMS Release 9.0 runs on the Tekelec 1100 (T1100) Application Server (AS). For more information about the T1100 AS, including information about FRUs (Field Replaceable Units), refer to the *T1100* Application Server *Hardware Manual*.

Network Attached Storage

This section contains:

- *NAS Overview* on page 13
- *How to Replace NAS Disk Drive Assemblies* on page 15

NAS Overview

All automatic and manual backups are made to the Network Attached Storage (NAS), which is network-connected to both LSMS servers. The NAS contains:

- Three disk drives arranged in a 550+ GB RAID 5 array
- A hot-spare disk, which automatically replaces a failed disk when one of the three disks in the array fails

Note: When the hot-spare disk replaces a disk in the array, an alarm is reported. When the alarm is reported, the failed disk should be replaced. The disks are hot-swappable, which means the NAS does not need to be powered down during disk replacement.

- One CD/DVD drive
- One tape drive

The NAS keeps up to five archives for each of the following:

- Each server's configuration files
- The LSMS database

The LSMS automatically creates a backup of all the above each night. Also, users can manually create a backup at any time (see *Backing Up the LSMS Manually* on page 87). Whenever a backup is created (automatic or manual), the oldest previous backup is erased, so that a maximum of five backups is always kept.

Users are advised to copy backups from disk drives to tapes at regular intervals (every 5 to 7 days) and to send the tape to an off-site, secure location. The NAS uses Ultrium LTO (Linear Tape Open) tapes, which have a capacity of 400 GB native (800 GB compressed). For information about copying backups to tape, see *Storing Backup Tapes Off-Site* on page 84.

The figures below show various views of an AC version of the NAS. The DC version of the NAS differs in that the doors are symmetrical and the disk drive carriers are different.

Figure 2: NAS Front View, Doors Closed

Figure 3: NAS Front View, Doors Open

Figure 4: NAS Rear View

How to Replace NAS Disk Drive Assemblies

Use the procedure in this section to replace a failed hard disk drive in the network attached storage (NAS) for AC and DC LSMS systems.

Note: While the disk drive carriers are different for AC and DC NAS, the replacement hard drive is the same, and the removal and replacement instructions are the same for both drive assemblies.

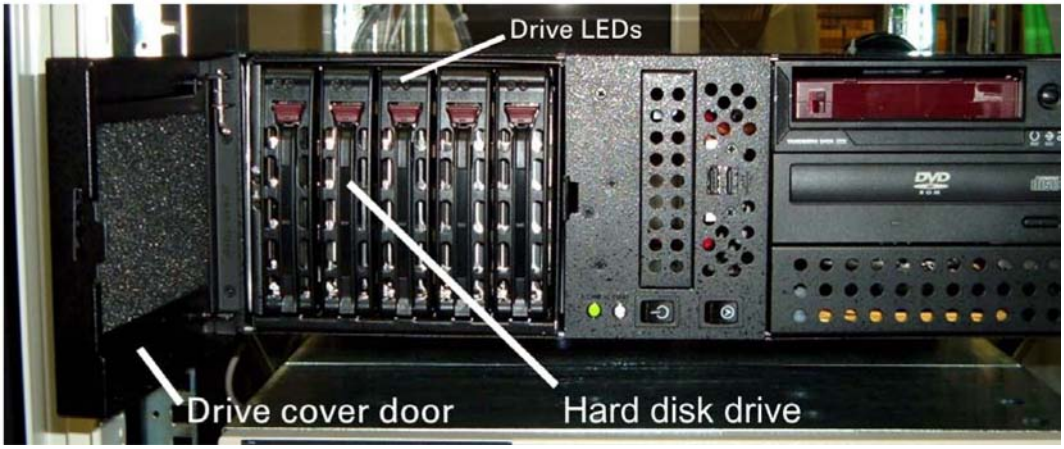
WARNING

WARNING: Always wear an ESD wrist strap grounded to the bench or frame when working on electronic components.

1. Unlock the drive cover door on the front left side of the NAS.

   Swing the door open (the door is hinged on the left side of the unit) to expose the hard disk drives.

   Figure 5: NAS Drive Cover Door (Opened)



CAUTION

CAUTION: This procedure to replace a failed hard drives can be performed while the NAS is powered on. However, do not remove all hard drives simultaneously.

2. Check the LEDs on the front of each of the five NAS drives for an indication of which drive needs to be replaced.

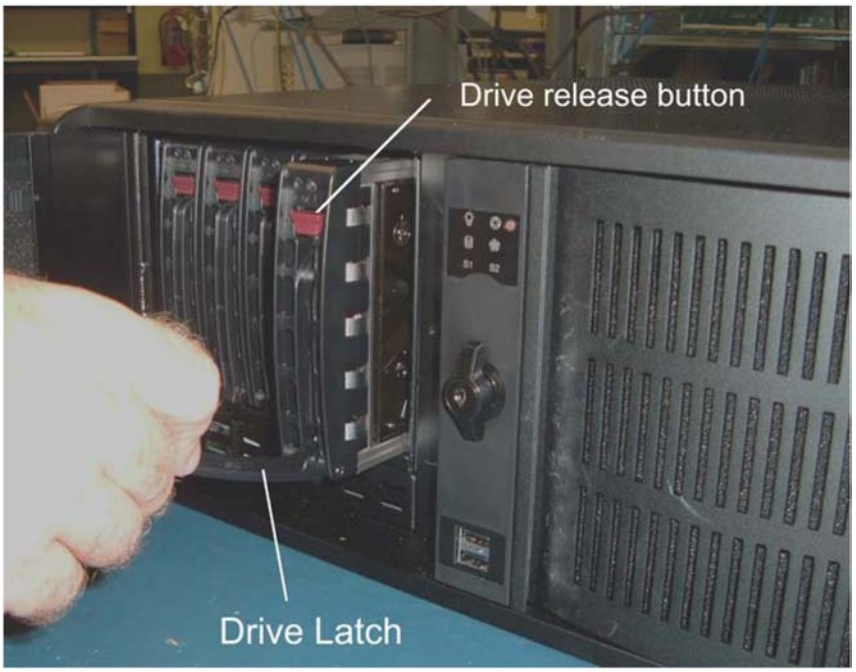
   Refer to the application manual to perform any procedures recommended to limit data loss or corruption. For example, the application manual may require:

   - Prepare the failed drive for replacement.
   - Data mirroring before replacing a failed hard disk drive.
   - Application shutdown before powering off the NAS.

3. To remove the hard drive, first push the red drive release latch button.

   The latch will pop away from the surface of the drive.

   Figure 6: NAS Drive Latch



4. Pull the latch down to disengage the drive and drive carrier and pull the drive carrier out of the chassis.

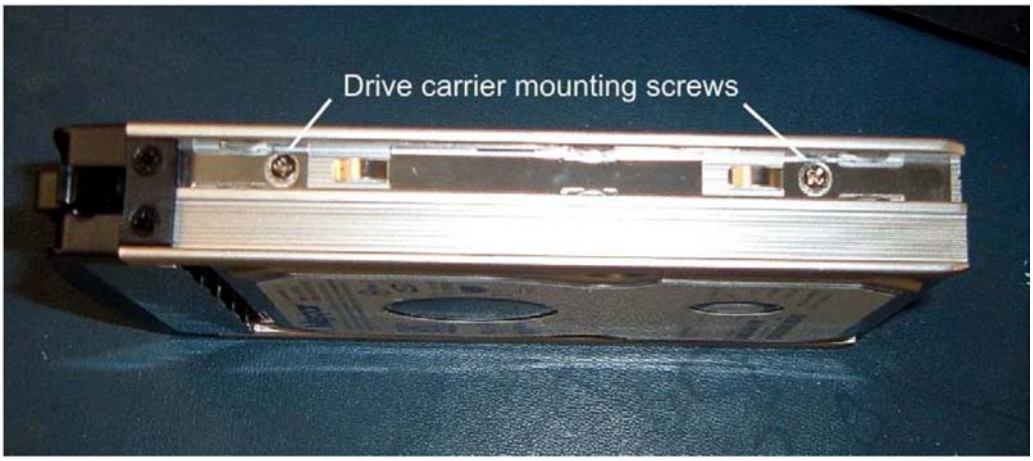
   Note:

   Be sure to support the drive with both hands as it is pulled out of the NAS.

5. Remove the four mounting screws on the sides of the drive carrier.

   Slide the drive out of the carrier and store the hard drive in an approved ESD package or place on a grounded bench.

   Figure 7: NAS Drive Carrier with Mounting Screws



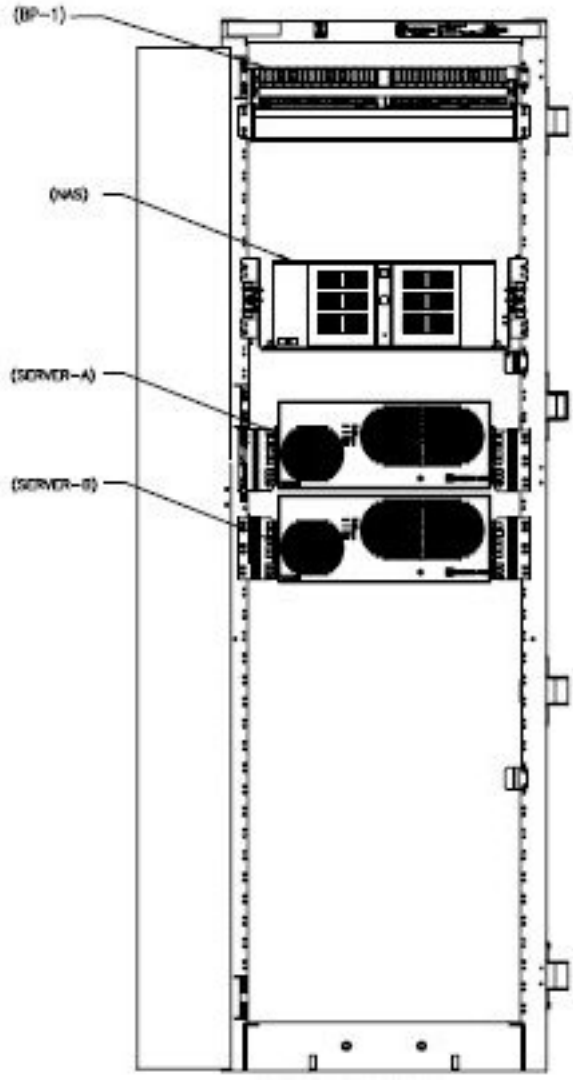
6. Slide the new drive into the drive carrier you removed in step *Step 5* on page 16 Tighten the screws to secure the new drive in the drive carrier.
7. Insert the new drive and drive carrier into the open drive bay in the NAS. When the drive is fully inserted, lock the drive latch.
8. Close the front drive cover.

You have now completed this procedure.

DC LSMS Hardware Overview

The figure below shows the components of a DC LSMS system in a frame.

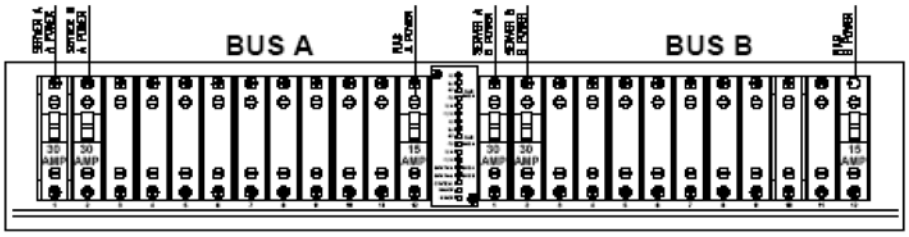
Figure 8: DC LSMS System - Front View



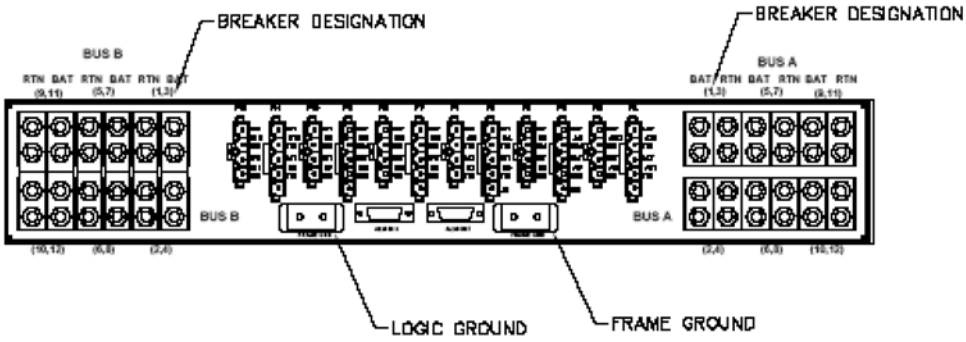
Breaker Panel

A breaker panel with two sides (called BUS A and BUS B) provides redundant power paths to the LSMS hardware.

Figure 9: T1100 LSMS Breaker Panel Front and Rear Views



DETAIL H – FRONT VIEW–CIRCUIT BREAKER



DETAIL F–REAR VIEW – CIRCUIT BREAKER

Breaker Panel LEDs

The figure below shows a close-up of the breaker panel LEDs on the front of each breaker panel.

Figure 10: Breaker Panel LEDs

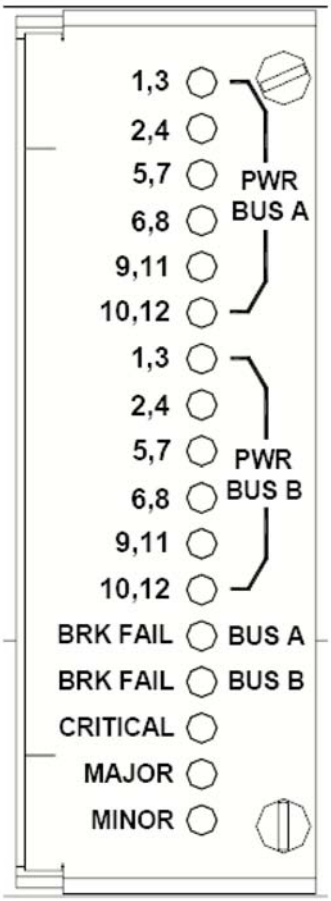


Table 3: Breaker Panel LED Settings on page 20 shows the possible LED settings and what each setting indicates.

Table 3: Breaker Panel LED Settings

LED Position (from top)	Label on left side:	Label on right side:	Color	Indicates:
Top 6 LEDs	**1, 2** through **11,12**	PWR BUS A	Green	Power is supplied from source A to breakers indicated by numbers on left
			Red	No power is supplied from source A to breakers indicated by numbers on left

LED Position (from top)	Label on left side:	Label on right side:	Color	Indicates:
			Off	Breakers indicated by numbers on left are not used
Next 6 LEDs	**1, 2** through **11,12**	PWR BUS B	Green	Power is supplied from source B to breakers indicated by numbers on left
			Red	No power is supplied from source B to breakers indicated by numbers on left
			Off	Breakers indicated by numbers on left are not used
13th LED	**BRK FAIL**	BUS A	Green	No breakers on side A have tripped
			Red	One or more breakers on side A have tripped
14th LED	**BRK FAIL**	BUS B	Green	No breakers on side B have tripped
			Red	One or more breakers on side B have tripped
15th LED	**CRITICAL**	No label	Green	No critical platform alarms are reported

LED Position (from top)	Label on left side:	Label on right side:	Color	Indicates:
			Red	One or more critical platform alarms are reported[1]
16th LED	**MAJOR**	No label	Green	No major platform alarms are reported[1]
			Red	One or major platform alarms are reported[1]
17th LED	**MINOR**	No label	Green	No minor platform alarms are reported[1]
			Red	One or minor platform alarms are reported[1]

[1] Both servers may send alarm information to the breaker panel for critical, major, or minor platform alarms.A CRITICAL, MAJOR, or MINOR LED is illuminated when one or more alarm of that type is reported from either or both servers. For more information about platform alarms, see *Platform Alarms* on page 358.

Breaker Panel Power

The breakers receive power from the input circuit on their respective side. Each breaker controls the power to its corresponding power feed on the back of the breaker panel. The power feeds connect to the individual hardware devices in the frame.

Power comes into each breaker panel on side A and on side B. Each input power line connects to the input power feeds in the rear of the breaker panel. Each input power feed has an input circuit breaker beside it that ensures that the power is within an acceptable range.

Mapping Breakers to Devices

On each side of the breaker panel, three breakers control power to the two servers and the Network Attached Storage (NAS).

The figure and table below show each active breaker and the device it controls.

Figure 11: T1100 LSMS Breakers

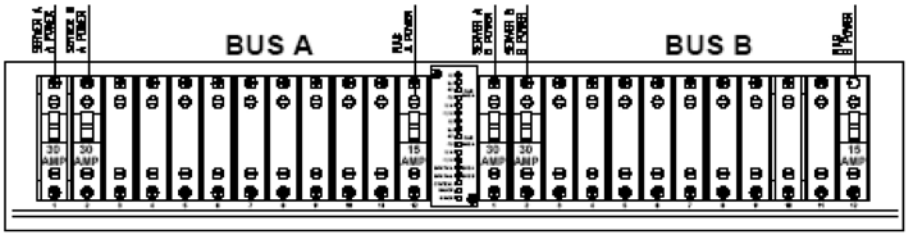


Table 4: Mapping of Active (Closed) Breakers to Devices

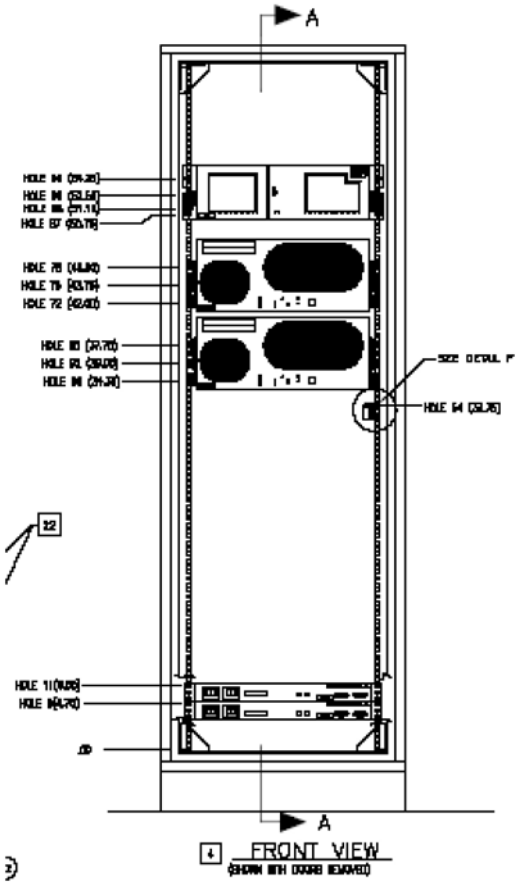
Breaker Panel Side	Breaker Position	Device
A	1	LSMS A
	2	LSMS B
	12	NAS
B	1	LSMS A
	2	LSMS B
	12	NAS

The table shows only end-to-end connectivity from the breaker panel breakers to the MPS.

AC LSMS Hardware Overview

The figure below shows the components of an AC LSMS system in a frame.

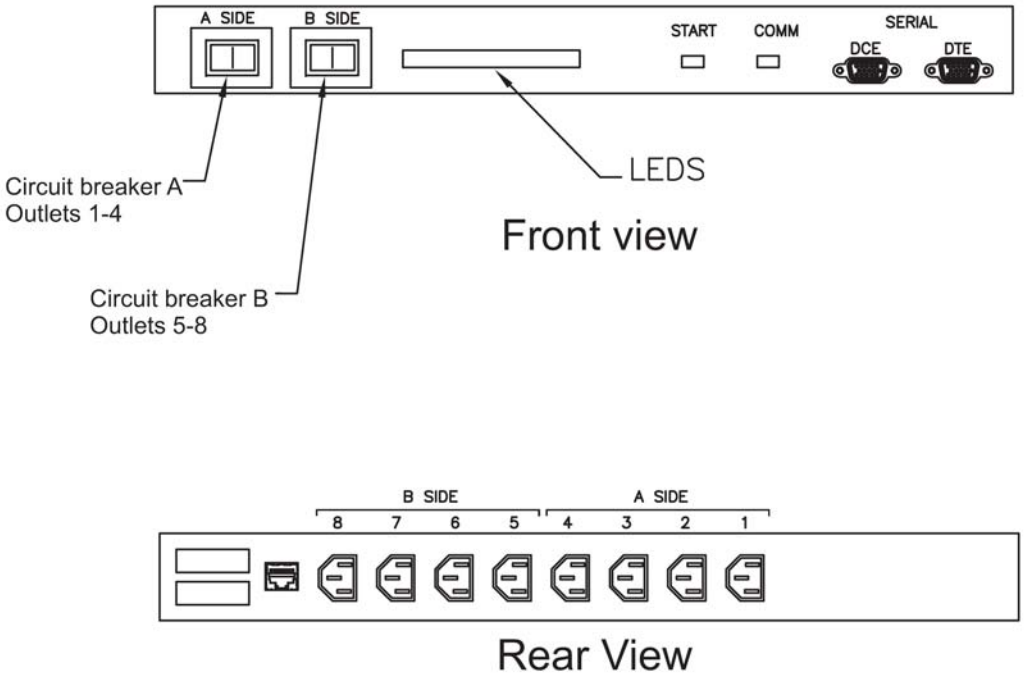
Figure 12: AC LSMS System



Power Distribution Unit

The AC Power Distribution Unit (PDU) is connected to a 240 V AC power source and distributes power to the components of the LSMS frame. Power is distributed to A side and B side feeds. There is one ON/OFF breaker switch for four A side power outlets and one ON/OFF breaker switch for four B side power outlets. *Figure 13: Power Distribution Unit, Front and Rear Views* on page 24 shows front and rear views of the PDU.

Figure 13: Power Distribution Unit, Front and Rear Views

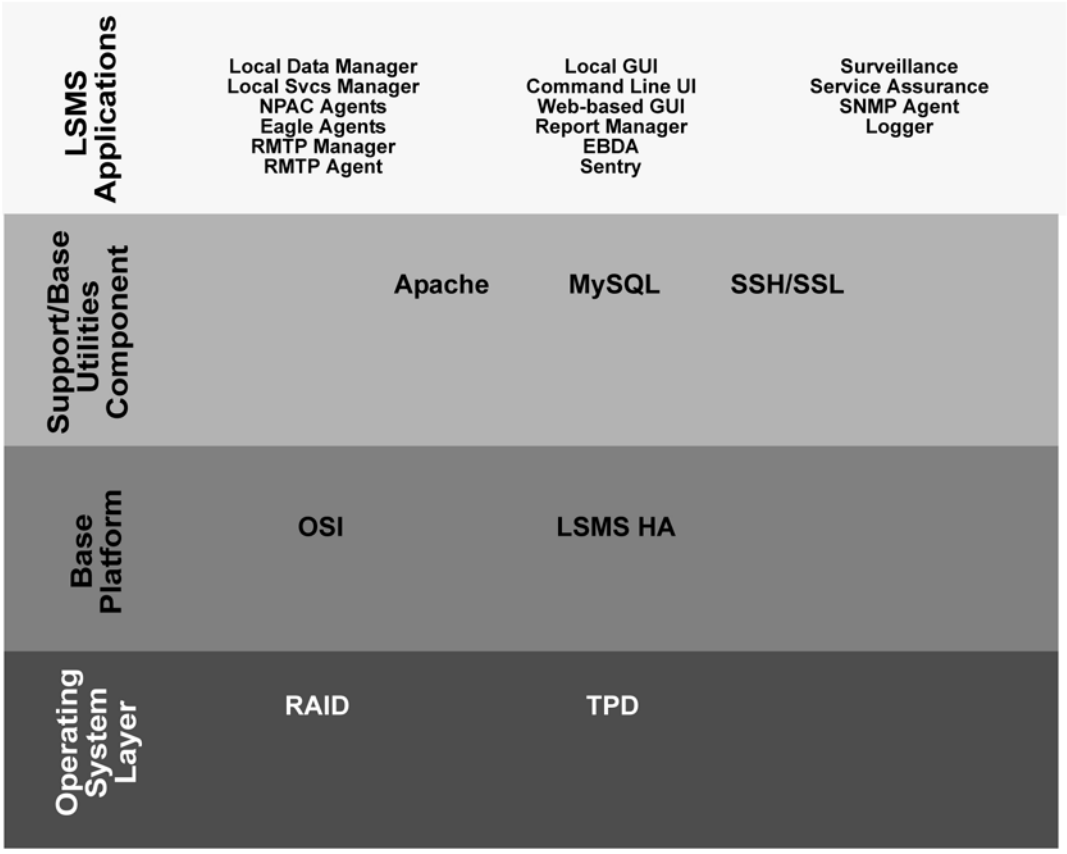


For more information about the PDU, refer to the documentation that was delivered with the product.

LSMS Software Overview

Figure 14: Software Allocation on the LSMS Platform on page 25 shows the layered organization of third party and Tekelec application software used in the LSMS system. For more information about the LSMS applications, see *LSMS Applications* on page 28.

Figure 14: Software Allocation on the LSMS Platform



Following are descriptions of the various software elements by layer.

Operating System Layer

The following elements appear in the Operating System Layer.

TPD (Tekelec Platform Distribution)

This is Tekelec's distribution of the operating system for T1100 Application Servers. The TPD software is installed on one internal disk drive and mirrored to a second internal disk for each server.

RAID (Redundant Array on Inexpensive Disks)

The TPD uses Linux RAID for monitoring disks and recovery from disk problems. RAID provides the following benefits:

- Redundancy
- Recoverability from hard-disk crashes

Base Platform Software

Following are the elements of the base platform software.

OSI Stack

This package implements the OSI protocol to allow communications between the LSMS and the NPACs.

LSMS HA

LSMS HA (High Availability) is software for a two-node cluster that provides automated switchover from an active server to a standby server when a server or monitored application experiences a failure. In the LSMS, the two servers are peers: either server can act as the active server (although only one server at a time can be the active server). When either automatic or manual switchover causes the standby server to become the active server, it can continue to be the active server until another switchover is needed.

Note: After switchover, the state of the previously active server is UNINITIALIZED "INHIBITED". As soon as possible, you need to perform the procedure described in *Starting a Server* on page 129 to return the state of that server to STANDBY so that it is available when switchover is needed again.

Support/Base Utilities Components

The following elements make up the Support/Base software utilities.

Apache

The Apache process (*httpd*) is a Web server. When the optional IP User Interface feature is enabled, the Apache process serves the GUI based on Java™ technology to client browsers.

MySQL

The MySQL Database was selected for the LNP database to store all the LNP and service provider data. This database consists of a runtime application programming interface (API) and data files. The data files are organized as follows:

- One database that stores locally provisioned data
- One database for each supported NPAC region
- A resynchronization database that is used for automatic resynchronizations with network elements; this database can store up to one million data objects

Whenever the two LSMS servers are in active/standby mode, all databases are replicated between the two servers, with the active server acting as the master and the standby server acting as the slave.

SSH/SSL

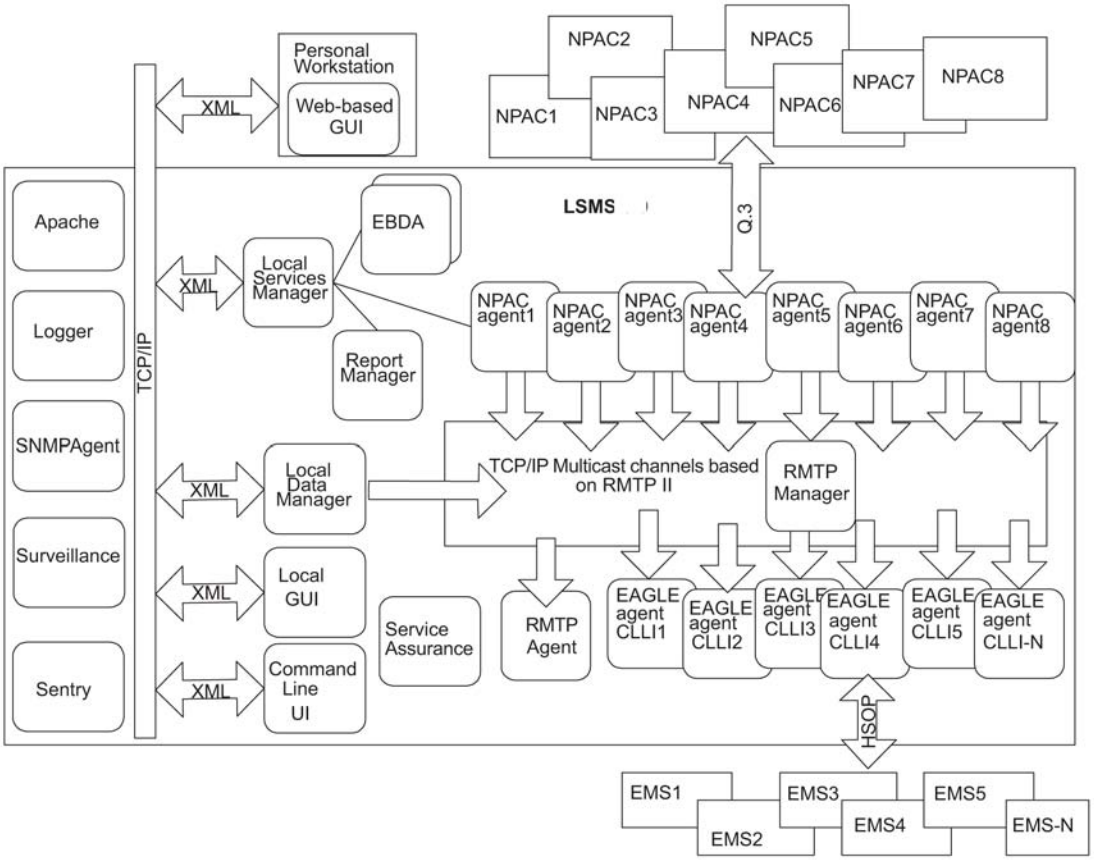
SSH/SSL is a robust, commercial-grade, and full-featured toolkit that implements the security and network encryption.

SSH/SSL provides secure data transmission through encryption keys. Encryption is required for the connection between the NPAC and the LSMS. The LSMS has a key for each NPAC that it services. For more information about keys, refer to the LSMS *Configuration Manual*.

LSMS Applications

The LSMS applications work together as shown below.

Figure 15: LSMS Applications



The LSMS applications provide the following functions:

Local Services Manager

The Local Services Manager (`lsman`) is responsible for providing an interface between the Local GUI and the web-based GUIs and other LSMS processes. It acts as a gateway to the GUIs for processes (EBDA, Report Manager, and NPAC agents) that do not have direct access to the GUIs, using XML (Extensible Markup Language) messages to communicate.

The Local Services Manager also manages how many users can be running simultaneously. The maximum number of users allowed on the LSMS system is eight. A terminal is defined as any of the following:

- A local GUI
- A web-based GUI
- A running *lsmsclaa* application instance. An *lsmsclaa* application instance provides a command-line interface that can be used by a script or by entering commands on a keyboard.

For more information, see *Command Line Application* on page 30 and *Overview of LSMS Application Commands Entered at the Command-Line Prompt* on page 162.

The Support for Additional Users optional feature enables you to have a maximum of 25 simultaneous users.

If you attempt to exceed the maximum allowable number of GUI sessions, an error message displays. For example, if you do not have the optional Support for Additional Users feature enabled and you start LSMS GUI sessions on eight different terminals and then attempted to start a ninth GUI session on another terminal, the following error message displays stating that the maximum number of users had been reached:

```
Maximum number of users reached.
```

Local Data Manager

The Local Data Manager (`supman`) is responsible for:

- Provisioning of LSMS configuration information and local data
- Communicating with the GUIs using XML messages
- Broadcasts all locally provisioned LNP data updates using a RMTP II (Reliable Multicast Transport Protocol) multicast mechanism on a single channel
- Updating the resynchronization database with locally provisioned data to facilitate automatic resynchronization with EMSs (Element Management Systems) at the supported network elements

NPAC Agents

The NPAC Agent application (`npacagent`) is responsible for:

- Connecting with a single NPAC system using the Q.3 protocol and providing all functions required by published NPAC standards
- Broadcasting all its updates using the RMTP II multicast mechanism over one broadcast channel
- Communicating with GUIs through the Local Services Manager

One instance of the `npacagent` process exists for each enabled NPAC region.

Eagle Agents

The Eagle Agent application (`eagleagent`) is responsible for:

- Subscribing to the broadcast channels to receive all NPAC and local data updates
- Connecting with a single EAGLE 5 ISS node using the HSOP (High Speed Operations Protocol) protocol and forwarding LNP updates to the EAGLE 5 ISS
- Filtering LNP data based on the provisioned filter information before forwarding it to the EAGLE 5 ISS (for more information, refer to the LSMS Database *Administration Manual*)
- Performing automatic resynchronization with an EAGLE 5 ISS node upon connection establishment (for more information, refer to the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual*)

One instance of the `eagleagent` process exists for each supported EAGLE 5 ISS node.

RMTPManager

The RMTPManager (`rmtpmgr`) is responsible for facilitating the reliable multicast mechanism that allows LNP data updates to reach every Eagle agent. It acts as a top node in an RMTP broadcast tree. A maximum of 9 broadcast channels exists (up to 8 channels for NPAC agents and 1 for the Local Data Manager).

RMTPAgent

The RMTPAgent (`rmtpagent`) is responsible for keeping the broadcast mechanism flowing even when no Eagle agents are running. The RMTPAgent subscribes to all (up to 9) broadcast channels.

Local GUI

The Local GUI application is responsible for providing a graphical user interface to allow operation of the LSMS by users who are logged into the LSMS administration console or a network-connected workstation through which they have made a telnet connection to the LSMS. Multiple instances of the Local GUI can exist.

Command Line Application

This application enables users to enter text commands to control certain LSMS application functions otherwise available through the GUI. For more information, see *Using lsmsclaa Commands* on page 230. Each instance of this application counts in the number of GUIs and command-line interfaces that can be run simultaneously, as described in *Local Services Manager* on page 28.

Web-BasedGUI

The Web-based GUI application runs outside of the LSMS system on a client platform. It provides an IP-based GUI to operate the LSMS and has the same appearance and functionality as the local GUI. Multiple instances of the Web-based GUI can exist.

Report Manager

The Report Manager (`reportman`) is responsible for producing reports on demand. It can produce up to 10 reports simultaneously.

EBDA

The Enhanced Bulk Download and Audit process (*ebda*) is responsible for providing the capability of performing audits, reconciles, bulk loads and user-initiated resynchronizations of an EAGLE 5 ISS's LNP database. Multiple instances of the *ebda* process can exist for different EAGLE 5 ISSs.

Sentry

The Sentry process (`sentryd`) monitors other software processes and attempts to restart them automatically in certain failure conditions. For more information about the Sentry application, see *Automatically Restarting Software Processes* on page 108.

Surveillance

The LSMS Surveillance process (*survMon*) continually surveys the LSMS hardware and software and sends surveillance notifications to the server's serial port. Users who want to display

surveillance notifications on an administration console can connect Serial Port 1 to the administration console (see *"Configuring a Customer-Provided Administration Console"*).

Surveillance is also responsible for monitoring and restarting the `sentryd` and Service Assurance processes. For more information, see *Understanding the Surveillance Feature* on page 34.

Service Assurance

The Service Assurance feature allows an external system to access subscription version data from the LNP databases in the LSMS. For more information, see *Understanding the Service Assurance Feature* on page 37.

SNMPAgent

The SNMPAgent (*lsmsSNMPAgent*) is a process running on the LSMS platform; it supports only the SNMP version 1 *trap* operation. This process receives (through UDP Linux sockets) LSMS notification events from other LSMS processes and formats these events into *trap* requests. For more information, see *Understanding the SNMP Agent Process* on page 40.

Logger

The Logger process (*lsmslogd*) is responsible for:

- Receiving log entries from application processes
- Storing them in appropriate log files
- Starting new log files every midnight

Overview of High Availability

To provide a high likelihood of the LSMS being able to function (high availability), the LSMS is implemented with hardware redundancies and with software that monitors hardware status and allows the LSMS functions to be run on either server (but not both at once).

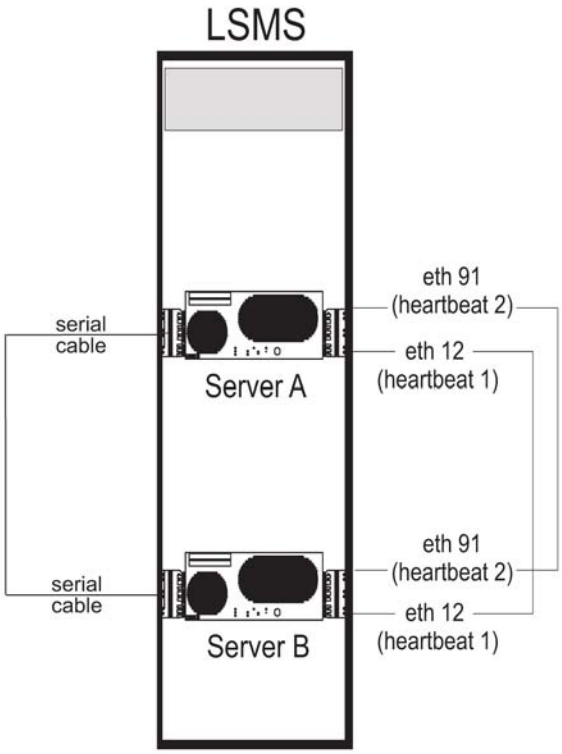
Hardware Redundancies

Each server contains two internal mirrored disks.

The LSMS is implemented with a pair of redundant servers and the following redundant heartbeat connections between them:

- A bonded pair of Ethernet connections for heartbeats
- A serial cable connection for heartbeats

Figure 16: LSMS Servers Connected with Heartbeat Links



Redundant Servers

Two servers, one active and one standby, provide redundancy in processing. If the active server fails, the LSMS can run on the standby server.

Changing from one server to another is called *switchover*. The server on which the LSMS is running at a given time is called the *active server* and the other server is called the *standby server*.

For some types of failure on the active server, the LSMS automatically attempts to switch over. You can also manually switch over at any time. For more information about switching over, see the following:

- *Understanding Switchover* on page 119
- *Understanding Automatic Switchover* on page 120
- *Manually Switching Over from the Active Server to the Standby Server* on page 124

Redundant Data

The LSMS is designed with the following data redundancies:

- Each server contains mirrored disks. If both sides of the mirrors fail on the active server, the LSMS automatically attempts to switch over to the standby server. For more information, see *Automatic Switchover Due to Hardware-Related Failure* on page 120.
- The database on the active server is replicated by the standby server.

Redundant Heartbeats

The servers use heartbeats to monitor each other. The servers are connected by a pair of redundant Ethernet connections and a serial connection. As long as each server is functioning, it sends its *heartbeat* to the other server over these connections. These two Ethernet connections are implemented on separate Ethernet cards, so that the failure of one Ethernet card does not prevent heartbeats from being sent.

The heartbeats are monitored by the Surveillance feature. If a heartbeat cannot be detected, one of the following notifications is posted:

```
LSMS4015|14:58 Jun 22, 2000|xxxxxxx|Notify:Sys Admin - Heartbeat 1 failure
```

```
LSMS4016|14:58 Jun 22, 2000|xxxxxxx|Notify:Sys Admin - Heartbeat 2 failure
```

Software Availability Design

The following LSMS software design features enhance the availability of the LSMS:

- The LSMS HA utility monitors the states of both servers, detects failure conditions, and automatically switches over for certain failures on the active server. For more information, see *Managing Server States* on page 117
- The Surveillance feature monitors critical processes and interfaces and posts notifications. For more information, see *Understanding the Surveillance Feature* on page 34.
- The `sentryd` feature detects certain application failures and automatically attempts to restart the failed applications. Full functionality of this feature requires that the Surveillance feature be enabled. For more information about `sentryd`, see *Restarting Software Processes* on page 107
- The LSMS provides the following automatic attempts to reassociate and resynchronize after outages between NPACs and the LSMS or between the LSMS and network elements (when automatic recovery is not possible, notifications are posted, and operator-initiated recovery procedures are documented as indicated):
  - Automatic reassociation with an NPAC after some association outages (for operator-initiated recovery procedures, refer to the LSMS *Configuration Manual)*
  - Automatic resynchronization of NPAC and LSMS data after reassociation (when automatic resynchronization is not possible, notifications are posted, and operator-initiated recovery procedures are documented in *Resynchronizing After an Outage Between an NPAC and the LSMS* on page 152)
  - Automatic resynchronization of the LSMS and network element data after outage (when automatic recovery is not possible, notifications are posted, and operator-initiated recovery procedures are documented in the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual*)

Enhancing High Availability with a Shadow LSMS

To further enhance the availability of LSMS functions, you can choose to implement a shadow LSMS, where a shadow LSMS is an entire LSMS (with its own service provider ID) located in a

separate geographical location from the main LSMS. Having a shadow LSMS available reduces the time needed to restore service in situations of severe error or disaster, such as fire or flood. The following types of shadow strategies are available:

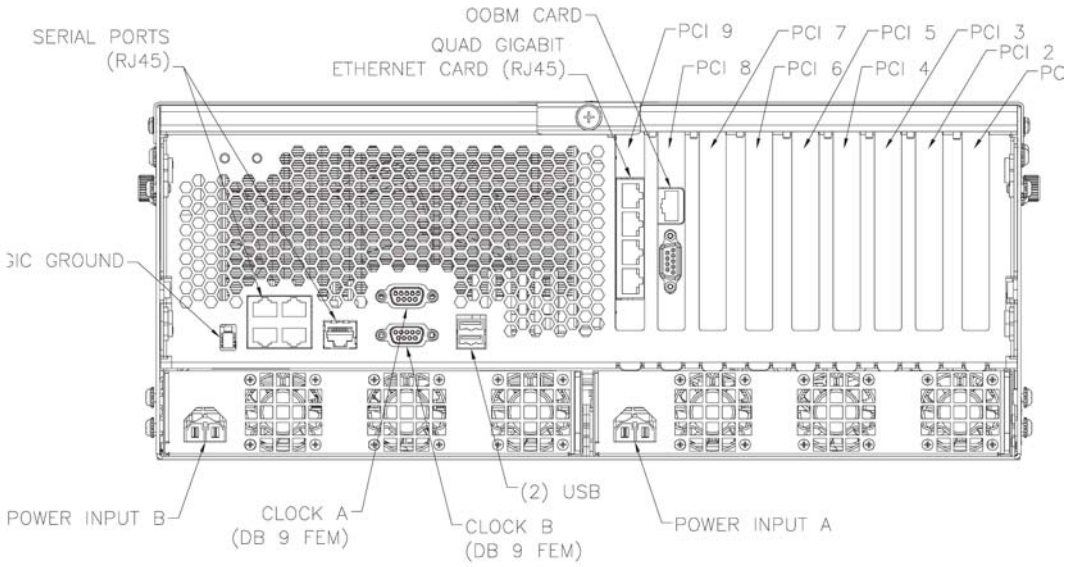
- Active shadow—a shadow LSMS that is connected to NPACs
- Inactive shadow—a shadow LSMS exists but is not connected to NPACs

For more information about a shadow LSMS, and recovery procedures for each strategy, see *Recovering from Site Failures* on page 131 This chapter also describes the procedure for restoring a main LSMS after a site failure when no shadow is available.

Understanding the Surveillance Feature

On each server, the LSMS Surveillance feature continually surveys the LSMS hardware and software and sends surveillance notifications to Serial Port 1 on each server. The Surveillance feature also logs all surveillance notifications in the file `survlog.log` in the`/var/TKLC/lsms/logs` directory. The Surveillance feature starts when LSMS starts.

Figure 17: T1100 - Rear View - Showing Serial Ports



The Surveillance feature also monitors network interfaces. For information about configuring the Surveillance feature for this purpose, refer to the LSMS *Configuration Manual*.

The Surveillance feature enables remote personnel to monitor the LSMS and detect conditions that require immediate action. Some surveillance notifications are sent only when the event occurs; other notifications are sent both when the event first occurs and also every five minutes thereafter until the condition is cleared. Every five minutes, the Surveillance feature also sends a *keep alive* notification to the Surveillance serial port and logs the *keep alive* in the file `survlog.log`.

The following topics are described in this section:

- *Configuring a Customer-Provided Administration Console* on page 35

- *Controlling the Surveillance Feature* on page 35
  - *Starting the Surveillance Feature* on page 35
  - *Stopping the Surveillance Feature* on page 36
  - *Determining the Surveillance Status* on page 36
- *Understanding Surveillance Notifications*
- *Logging Surveillance Notifications* on page 36

Configuring a Customer-Provided Administration Console

If customers desire a local administration console for displaying Surveillance notifications, they can attach their own administration console to Serial Port 1 on each of the LSMS servers. The following requirements are needed to provide and configure a customer-provided administration console:

- A workstation that can display text
- Two cables that connect to the RJ-45 interface used by Serial Port 1 on each LSMS server
- Configure the connections as:
  - 9600 baud
  - Parity 8E1
- Software running on the workstation that can determine from which cable the Surveillance notification is arriving (the Surveillance notifications do not identify which server is generating them)

Controlling the Surveillance Feature

The Surveillance feature starts on each server when the server starts. The following topics explain how to use LSMS commands to start, stop, and check the status of the Surveillance feature.

Note: These commands affect only the server on which they are entered.

Starting the Surveillance Feature

Use the `lsmssurv start` command to start the Surveillance feature on the server that you are logged into.

1. Log in as `root` on either server.
2. Type the following command to start surveillance:

   ```
   lsmssurv start
   ```

   Either of the following messages appears, depending on whether surveillance was already running:

   ```
   LSMS Surveillance feature started
   LSMS Surveillance feature is currently running
   ```

3. Repeat this procedure for the other server, if desired.

You have now completed this procedure.

Stopping the Surveillance Feature

Use the `lsmssurv stop` command to stop the Surveillance feature on the server that you are logged into.

1. Log in as `root` on either server.
2. Type the following command to stop surveillance:
   `lsmssurv stop`
   Either of the following messages appears, depending on whether surveillance was already stopped:

```
LSMS Surveillance feature stopped
LSMS Surveillance feature is not currently running
```

3. Repeat this procedure for the other server, if desired.

You have now completed this procedure.

Determining the Surveillance Status

Use the `lsmssurv status` command to check the status of the Surveillance feature. This command allows you to determine if the Surveillance feature is already running or has already been stopped.

1. Log in as `root` on either server.
2. Type the following command to get surveillance status:
   `# lsmssurv status`
   You will receive one of the following messages:

```
LSMS Surveillance feature is currently started
LSMS Surveillance feature is currently stopped
```

3. Repeat this procedure for the other server, if desired.

You have now completed this procedure.

Understanding Surveillance Notifications

Introduction on page 248 provides information about the format of Surveillance notifications and how they correlate to GUI notifications and traps. In addition, for each Surveillance notification, ordered by its event number, the appendix provides the following information:

- It output text string
- Explanation of possible cause, beyond the text that fits into the notification text string
- Suggested recovery actions
- Source from which the notification is sent
- Frequency with which the notification appears

Logging Surveillance Notifications

In addition to displaying Surveillance notifications, the Surveillance feature logs all Surveillance notifications in the file `survlog.log` in the `/var/TKLC/lsms/logs` directory.

If the LSMS Surveillance feature becomes unable to properly report conditions, it logs the error information in a file, named `lsmsSurv.log`, in the `/var/TKLC/lsms/logs` directory on each server's system disk. When the size of `lsmsSurv.log` exceeds 1MB, it is copied to a backup file, named `lsmsSurv.log.bak`, in the same directory. There is only one LSMS Surveillance feature backup log file, which limits the amount of log disk space to approximately 2MB.

Understanding the Service Assurance Feature

The Service Assurance feature allows an external system to access subscription version data from the LNP databases in the LSMS. This information is useful in verifying correct porting of data, and helps in troubleshooting problems. There is one LNP database for each of the NPACs associated with the LSMS.

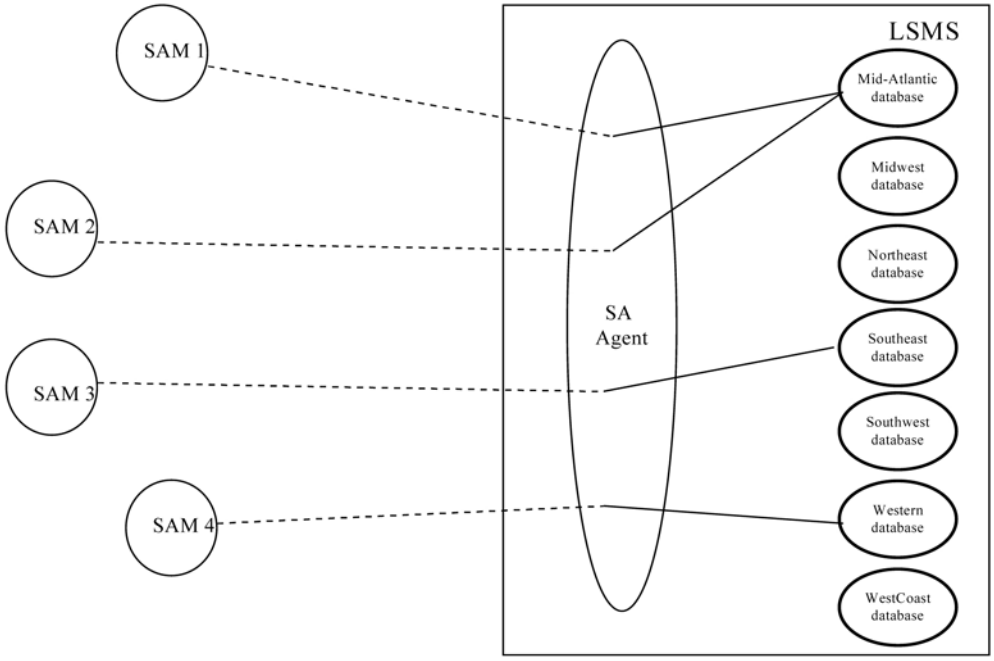
The external system uses Service Assurance Manager (SAM) application software to initiate service assurance data requests and associations. Single or multiple SAMs may exist on the external computer system. The SAM communicates with the LSMS through the Service Assurance Agent (SAA) application software that resides in the LSMS. The SAM application software is not Tekelec software and is only resident on the external system.

The SAA decodes the queries from the SAM and then accesses the LNP database. The SAA forms the subscription version data into a message and that message is sent to the SAM making the query.

Service Assurance works in conjunction with the Surveillance feature. The Surveillance feature issues the command to start the Service Assurance agent (part of the Service Assurance feature that is described in this document), and it monitors the status of the Service Assurance agent.

A maximum of eight SAM/SAA sessions are allowed at one time.

Figure 18: Service Assurance System within a Network



The architecture used to provide the access is a Connection Oriented Manager/Agent using CMIP (Common Management Information Protocol). CMIP provides an industry standard interface between Manager and Agent applications. This allows you to use standard products and tool kits to develop applications.

Service Assurance Terminology

The following terms are used to describe Service Assurance:

- *Service Assurance Manager* (SAM): Initiator of service assurance associations and data requests. This is *not* part of the LSMS application. A SAM application runs on a computer but is not the computer itself. Multiple SAMs can run on the same computer, or each SAM can run on a different computer.
- *Service Assurance Agent* (SAA): Software residing on the LSMS and considered part of the LSMS application. This software consists of one or more Linux processes and one or more Linux scripts.
- NPAC Database : This refers to the database stored on the NPAC.
- LNP Database : This refers to the database that contains subscriptionVersions, Service Provider Network, Service Provider LRN and Service Provider NPA-NXX objects. This database resides on the LSMS. Each NPAC has one LNP Database on the LSMS.
- *Manager/Agent*: This term describes the two peer processes that work together to implement the Service Assurance feature. The Manager is the customer's application, which is used to initiate the association and send the query to the Agent process. The Agent process decodes the query message, then accesses the LNP Database.

  The Agent extracts the data from the database, then builds and sends the reply to the Manager. This feature allows the Manager to send a single subscription TN or list of subscription TNs to query. The Agent extracts each instance that it can find from the LNP Database and returns a response to the Manager.

The architecture is connection oriented to restrict access to the LNP databases. This system is assumed to be within the customer's private network, so no encryption security is included. The CMIP protocol defines the method for establishing and terminating associations. This application uses the access control and user data space in the association messages to restrict access to the system.

The SAM is restricted to querying subscription versions by the subscriptionTN field. Up to four SAMs can query the LSMS at the same time.

The Service Assurance feature interfaces to the LSMS by means of a 10 Mbps Ethernet interface. The Application WAN is also used as the interface for the X-terminals connected to the LSMS. The network connecting the Service Assurance systems to the LSMS is the responsibility of the customer.

Interface Implementation

The LSMS Service Assurance interface is implemented over a standard CMIP/CMISE-based OSI protocol stack (Q.3). RFC1006 is used for the transport layer.

This interface is limited to the retrieve capabilities of the local LSMS database. The object to be retrieved is the subscriptionVersion defined in NPAC SMS *Interoperable Interface Specification*, NANC Version 1.5, September 1997.

Allowed Functions on the Interface

The LSMS responds to association (bind) requests, release (unbind) requests, aborts, and subscription query (m-get) messages. No other functions are allowed over this interface and will be rejected.

Support of OSI Addresses

The LSMS supports four OSI address connections for Service Assurance interfaces, which correspond to eight domains.

Each Service Assurance system needs to establish only the associations it requires, without regard to whether the LSMS is operating with the primary or secondary server. Upon switchover, the association is momentarily lost. The Service Assurance system tries to reestablish the association. When the active system finishes coming up, it then responds to the Service Assurance system association requests. The Service Assurance system does not know whether the primary or secondary system is running.

Association information is specified by Tekelec. This information must be present in the bind request. This data in the association information, such as the system name, is used to verify the source of a bind request. Bind requests with invalid association information are rejected.

Establishment of association between the LSMS and the Service Assurance system is initiated by the Service Assurance Manager. This applies to initial association as well as to reestablishing the association after outages (regardless of the cause of the loss of association). When it does not have an association, the Service Assurance system periodically tries to establish the association until a successful response is received from the LSMS. The minimum retry interval is one minute.

The LSMS provides a response to the bind request to indicate:

- Successful connection
- Access control failure (authority violation - unknown address requesting association)
- LSMS data access failure

- Resource failure (maximum number of associations already established)

Number of Associations Per Service Assurance System

The LSMS supports one association per Service Assurance system.

If a Service Assurance agent within the LSMS is unable to establish a connection with the LSMS NPAC database, the association with the Service Assurance system is aborted.

Notification Upon Loss of Association

The LSMS provides a notification when the association with any of the Service Assurance Manager is lost or established.

Understanding the SNMP Agent Process

The optional Remote Monitoring feature provides the capability for the LSMS to report certain events and alarms to a remote location, using the industry-standard Simple Network Management Protocol (SNMP). The LSMS implements an SNMP agent with the SNMP agent process running on the LSMS platform.

Customers can use this feature to cause the LSMS to report events and alarms to another location, which implements an SNMP Network Management System (NMS). An NMS is typically a standalone device, such as a workstation, which serves as an interface through which a human network manager can monitor and control the network. The NMS typically has a set of management applications (for example, data analysis and fault recovery applications).

Overview of SNMP Protocols

An SNMP agent, such as that implemented by the LSMS, is responsible for SNMP managed objects; each managed object represents a data variable. A collection of managed objects is called a management information base (MIB). A copy of the MIB is maintained both at the SNMP agent and also at the NMS. The MIB can be read with a text editor.

An SNMP agent can do the following:

- Respond to requests from the NMS for information and/or action. The SNMP architecture defines a limited set of management commands and responses. The NMS can issue *Get*, *GetNext*, and *Set* messages to retrieve single or multiple object variables or to modify the value of a single variable. The SNMP agent sends a response message to complete the *Get*, *GetNext*, or *Set*. This release of the LSMS does not support these functions.
- Send event notifications, called *trap* requests, to the NMS to identify the occurrence of conditions, such as the failure or restoration of a link interface.

The SNMP protocol uses the User Datagram Protocol (UDP) transport protocol in a TCP/IP network. UDP is a connectionless protocol and does not guarantee reliable delivery of data. Therefore, SNMP does not use a preestablished connection to send data and does not guarantee reliable delivery of data.

The LSMS SNMP Agent Implementation

The LSMS SNMP agent process supports only the SNMP version 1 *trap* operation. The SNMP agent receives (through UDP Linux sockets) LSMS notification events from the following processes and formats these events into *trap* requests:

- The Surveillance process, which continually monitors the LSMS hardware and software.
- The LSMS graphical user interface (GUI) process.
- One or more regional agent (`npacagent`) processes, each of which receives commands from Number Portability Administration Centers (NPACs) and the GUI process, interprets those commands, and initiates appropriate LSMS activities to manage regional NPAC data. The LSMS can support up to eight regions; each region corresponds to an NPAC.
- One or more `eagleagent` processes, each of which receives commands from the GUI process, interprets those commands, and initiates appropriate LSMS activities to send data to the network elements. The LSMS can support up to eight pairs of network elements.
- The Local Data Manager (`supman`) process, which manages locally provisioned data that is entered through the GUI and sent to the network elements which the LSMS supports.

The LSMS SNMP agent formats the information received from these processes into an SNMPv1 *trap* protocol data unit (PDU) and sends the *trap* request to one or more NMSs. Each NMS (provided by the customer) has a local copy of the LSMS MIB. When the NMS receives a *trap* request from the LSMS, it compares the information in the *trap* request to information in its own MIB to determine what event has occurred at the LSMS.

For information about the format of a *trap* and which events are reported in traps, see *Automatic Monitoring of Events* on page 247

Configuring the SNMP Agent

If you install the optional Remote Monitoring feature, refer to the LSMS *Configuration Manual* to configure the IP addresses and community names for each of the NMSs to which you want the LSMS to send *trap* requests. You can also perform this procedure if you want to add or delete NMSs after you have started the LSMS. The LSMS can support up to five NMSs simultaneously.

Controlling the SNMP Agent

If the optional Remote Monitoring feature is installed, it is managed by the Surveillance agent, and can also be controlled by the user.

After the LSMS boots up, the Surveillance process constantly monitors the LSMS SNMP agent process. If the SNMP agent process exits abnormally, the Surveillance process restarts it.

Any user who belongs to the `lsmsadm` permission group can use the new `lsmsSNMP` command to start, stop, or display status of the LSMS SNMP agent.

Stopping the SNMP Agent

Perform the following procedure to stop the SNMP agent process:

1. Log in to the active server as a member of the `lsmsadm` permission group.
2. To stop the SNMP agent, enter the following command:
   ```
   $LSMS_DIR/lsmsSNMP stop
   ```

You have now completed this procedure.

Starting the SNMP Agent

Perform the following procedure to start the SNMP agent process:

1. Log in to the active server as a member of the `lsmsadm` permission group.
2. To start the SNMP agent, enter the following command:
   `$LSMS_DIR/lsmsSNMP start`

You have now completed this procedure.

Determining the Status of the SNMP Agent

Perform the following procedure to determine the status of the SNMP agent process:

1. Log in to the active server as a member of the `lsmsadm` permission group.
2. To stop the SNMP agent, enter the following command:
   `$ $LSMS_DIR/lsmsSNMP status`

   Output similar to the following appears:

```
LSMS SNMP AGENT PROCESS STATUS:
TOTAL SUCCESSFUL TRAP REQUEST= 12
TOTAL FAILED TRAP REQUEST = 2
   == IP-ADDRESS ==   == STATUS ====
   177.88.34.7         Failed
   198.77.39.2         Connected
```

   This output provides the following information:

   - A title line to indicate that the output is LSMS SNMP agent process status
   - The total number of successful SNMP trap requests sent by the LSMS SNMP agent since it started
   - The total number of failed SNMP trap requests sent by the LSMS SNMP agent since it started
   - The status of each UDP socket session to an NMS, along with the IP address of the NMS:
     - `Failed` indicates that a session to the NMS was never established
     - `Connected` indicates that a session to the NMS was successfully established

You have now completed this procedure.

Logging SNMP Agent Actions

When the LSMS SNMP agent process starts, stops, or sends a *trap* request, it logs information about the action in a log file. The log file is named `lsmsSNMP.log<MMDD>`, where `<MMDD>` represents the current month and day. The log file is stored in the directory `var/TKLC/lsms/logs/snmp` and is automatically deleted after 7 days. If either the log file or its directory does not already exist, the agent process creates the file or the directory, or both, when one of these actions occurs.

For more information about what is logged in this file, see *Logging SNMP Agent Actions* on page 260.

Chapter 3

Routine Procedures

Topics:

- *Introduction Page 44*
- *Using Login Sessions Page 44*
- *Powering On the LSMS Page 55*
- *Powering Off the LSMS Page 56*
- *Accessing LSMS through a Dial-In Connection Page 58*
- *Managing the System Clock Page 59*
- *Managing User Accounts Page 62*

This chapter explains the procedures that system administrators regularly perform. These procedures include establishing remote login procedures, starting up and shutting down the LSMS system, setting the system clock, and managing user accounts.

Introduction

This chapter explains the procedures that system administrators regularly perform. These procedures include establishing remote login procedures, starting up and shutting down the LSMS system, setting the system clock, and managing user accounts.

The procedures in this chapter assume that you are familiar with the LSMS hardware. For more information about the hardware, refer to the *T1100* Application Server *Hardware Manual.*

Using Login Sessions

Login sessions are used for the following user functions:

- To use the command line for any of the following functions:
  - To access the `lsmsmgr` text interface, which is used for configuring and maintaining the LSMS system
  - To enter LSMS commands (generally used for managing LSMS applications); for more information, see *Commands* on page 161
  - To start the optional Command Line Administration Capability feature (the `lsmsclaa` utility); for more information, see *Using lsmsclaa Commands* on page 230 .
- To use the graphical user interface (GUI), which is generally used for the following functions:
  - Configuration (for more information, refer to the LSMS *Configuration Manual*)
  - Database administration (for more information, refer to the LSMS Database *Administration Manual*)
  - Synchronization of the LSMS LNP database with the LNP databases at network elements (for more information, refer to the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual*)

Support of Multiple Users

The LSMS allows, as a standard feature, a maximum of eight simultaneous users. The Support for Additional Users optional feature enables you to have a maximum of 25 simultaneous users. A user is defined to be any of the following:

- `lsmsmgr` user (a user who logs in as the `lsmsmgr` user to start the `lsmsmgr` text interface)
- Server-side GUI user (a user who has logged into the command line of a server and started a GUI with the `start_mgui` command)
- Web-based GUI user (a user who has logged into the active server GUI over the web; this function requires the IP User Interface optional feature)
- `lsmsclaa` user (a user who is using the optional LSMS Command Class Management optional feature)

Establishing Login Sessions

From any network-connected terminal, you can establish a variety of sessions with the active server or with a specific server in one of the following ways:

- Display the `lsmsmgr` text interface of either the active server or of a specific server.
- Display the command line of either the active server or a specific server for entering commands; see *Logging In to LSMS Server Command Line* on page 45.

  From the displayed command line, you can start a server-side GUI, as described in *Starting a Server-Side LSMS GUI Session* on page 48.
- Display the GUI remotely (if the optional IP User Interface feature is installed) by using a web browser; see *Starting a Web-Based LSMS GUI Session* on page 48

Logging In to LSMS Server Command Line

You can log into the LSMS active server or into a specific server from any terminal that has an `ssh` (Secure Shell utility) client installed.

Note: If your terminal does not already have ssh installed, PuTTY (Tekelec does not make any representations or warranties about this product) is an open source `ssh` utility for Windows that you can download from the web.

You must have a user ID and password before you can log in to LSMS.

1. From a command-line prompt, enter one of the following commands (depending on the terminal operating system) to start a secure shell session with the LSMS server:

   - On a Windows-based or Linux-based terminal, enter:

     ```
     ssh -X <username>@<server_IP_address>
     ```

     For `<username>` and `<server_IP_address>`, specify values shown in *Table 5: Parameters Used in Accessing Server Command Line* on page 45 that are appropriate to the procedure you are performing:

     Table 5: Parameters Used in Accessing Server Command Line

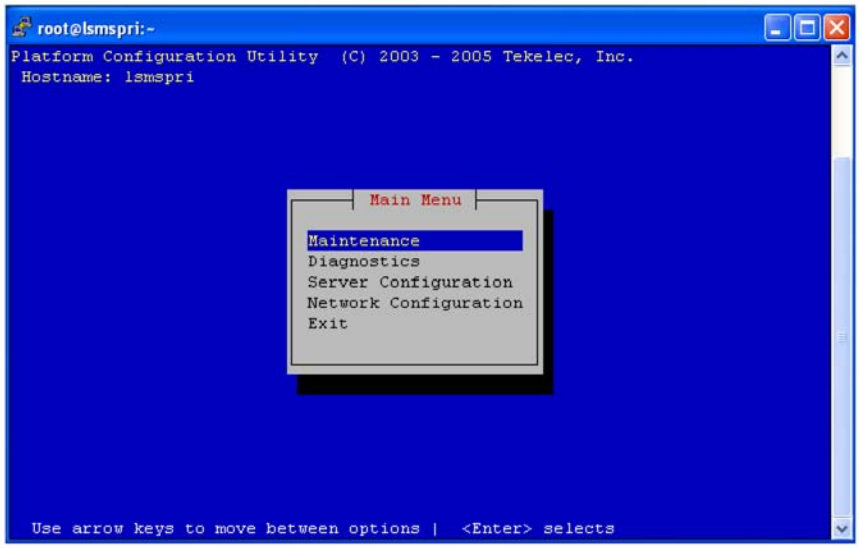
Parameter	Value
`<username>`	Use one of the following: • `lsmsmgr` to access the `lsmsmgr` text interface for configuration, diagnostics, and other maintenance functions • `syscheck` to run the `syscheck` command with no options, which returns overall health checks and then exits the login session (for more information about the `syscheck` command, see *syscheck* on page 230) • Other user names, as directed by a procedure

Parameter	Value
<server_IP_address>	Use one of the following: • VIP (Virtual IP address) to access the LSMS Web GUI • IP address of the specific server, when directed by a procedure to access a particular server

2. When prompted, enter the password associated with the user name.
3. You can now continue with any of the following functions:

   - If you entered `lsmsmgr` as the username, the `lsmsmgr` text interface displays. You can use any of the `lsmsmgr` functions.

     Figure 19: lsmsmgr Text Interface Main Menu



     Note: Selections in the `lsmsmgr` text interface are made by either using the Up and Down Arrow keys on your keyboard or typing the first letter of any menu item to change which menu item is highlighted. When the desired menu item is highlighted, press the Enter key.

     In this manual, menu selections are indicated as a series; for example, select Maintenance>Start Node indicates that you should highlight the Maintenance item on the main menu, press Enter, then highlight the Start Node item on the next menu, and press Enter.

   - If you entered `syscheck` as the username, the command line window displays the System Health Check output. For more information about `syscheck`, see *syscheck* on page 230.
   - If you entered any other username the command line prompt displays a prompt that shows the username and host name, similar to the following example (in this example, the user logged in as the `lsmsadm` user to the server whose host name is `lsmspri`):

```
[lsmsadm@lsmspri lsmsadm] $
```

Note: In this manual, the prompt will be indicated simply by `$`.

At this prompt, you can do any of the following:

- Enter LSMS commands.
- Start the `lsmsclaa` utility, if you have the LSMS Command Class Management optional feature installed.
- If you need to start an LSMS GUI session, see *Starting a Server-Side LSMS GUI Session* on page 48.

You have now completed this procedure.

Logging in from One Server to the Mate's Command Line

Sometimes it may be necessary to have access to the command line interfaces for both servers. You can log into each server separately using `ssh`, or you can use `ssh` to go back and forth between servers.

To log in from one server's command line to the mate server's command line, use the following procedure:

1. Log in as any user except `lsmsmgr` or `syscheck`, using the procedure described in *Logging In to LSMS Server Command Line* on page 45 to log into a server command line.
2. Enter the following command to access the command line on the mate server:

   ```
   $ ssh mate
   ```

   If you have not previously logged into the mate, the following information displays:

   ```
   The authenticity of host 'mate (192.168.1.1)' can't be established.
   RSA key fingerprint is 1c:14:0e:ea:13:c8:68:07:3d:7c:4d:71:b1:0c:33:04.
   Are you sure you want to continue connecting (yes/no)?
   ```

   Type `yes`, and press **Enter**.
3. When prompted, enter the password for the same user name.
4. The prompt on your terminal now displays the host name of the mate server, and you can enter commands for the mate server.

   Following is an example of the sequence of commands and prompts that display during this procedure:

   ```
   [lsmsadm@lsmspri lsmsadm]$ ssh mate
   lsmsadm@mate's password:
   [lsmsadm@lsmssec lsmsadm]$
   ```

You have now completed this procedure.

Starting an LSMS GUI Session

You can start an LSMS GUI session in either of the following ways:

- If you have activated the optional IP User Interface feature, you can use a web browser to connect to the LSMS, as described in *Starting a Web-Based LSMS GUI Session* on page 48

- If you have not activated the optional IP User Interface feature, establish a login session first from an X-windows compatible terminal (as described in *Establishing Login Sessions* on page 45) and then start a GUI (as described in *Starting a Server-Side LSMS GUI Session* on page 48)

Starting a Server-Side LSMS GUI Session

To start an LSMS GUI session on an X-windows compatible terminal through which you have made a secure shell connection to the LSMS, use the following procedure.

1. Use the procedure described in *Logging In to LSMS Server Command Line* on page 45 to log into the active server as an `lsmsadm` (system configuration), `lsmsuser` (database administration), `lsmsview` (viewer), `lsmsuext` (external user), or `lsmsall` (all) user.

   (For more information about user types, see *Non-Configurable Permission Groups* on page 64.)

2. Do one of the following:

   - If you are performing this procedure on a Linux-based terminal, go to the next step (the `-X` you specified when you logged into the server command line enables the GUI to be displayed on your terminal).
   - If you are performing this procedure on a Windows terminal, enter the following command to cause the GUI display to be sent to the terminal, where `<ipaddress>` is the IP address of the terminal:

     ```
     export DISPLAY=<ipaddress>:0
     ```

3. Verify that the Netscape browser is not running on the terminal from which you logged into the server command line.

   (If the Netscape browser is running, you will not be able to view reports or log files.)

4. Enter the following command to start the GUI session:

   ```
   $LSMS_DIR/start_mgui
   ```

   The **Welcome/Login** window displays. Next, perform the procedure described in *Logging Into the LSMS Console Window* on page 51.

You have now completed this procedure.

Starting a Web-Based LSMS GUI Session

The LSMS offers, as the optional IP User Interface feature, a web-based graphical user interface (GUI) intended for remote users. The web-based GUI can be run:

- On a PC with Microsoft® Windows installed, using Microsoft Internet Explorer (version 5.0 or higher)
- On a Linux workstation, using Netscape Navigator

The web-based GUI is accessible from any machine that can access the network on which the LSMS resides. The functionality of the web-based GUI is the same as that of the server-side GUI.

Note: When you have completed logging into a web-based LSMS GUI, the session has these operating characteristics:

- Pressing the Back button from the browser from which the GUI was launched terminates that GUI session. To reopen the GUI, you must click the Refresh button and begin the login process again.

- Pressing the Refresh button from the browser from which the GUI was launched terminates that GUI session. To reopen the GUI, you must begin the login process again.
- You cannot use a browser window that was started by selecting File > New > Window from the browser window to launch another web-based LSMS GUI.

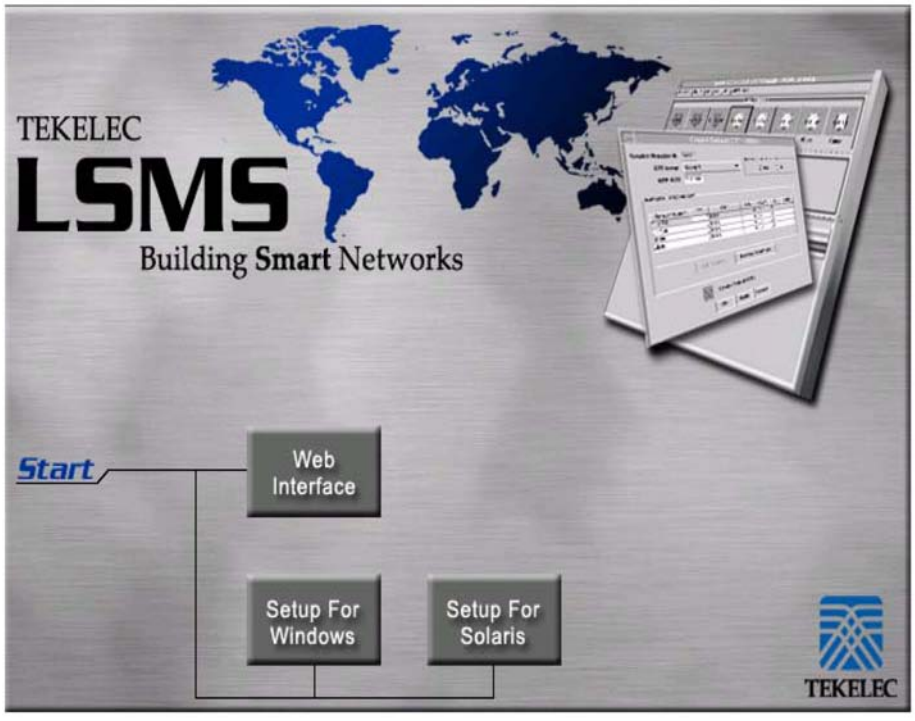
To start the web-based GUI, verify that the IP User Interface feature has been activated and perform the following procedure:

1. Start your web browser (Netscape Navigator or Internet Explorer).
2. Enter the LSMS VIP (Virtual IP) address, followed by `:8200`, in either of the following locations, depending on which platform your web-based GUI runs:
   a) For Netscape Navigator in the Location: field
   b) For Internet Explorer, in the Address: field

   For example, enter `http://<VIP_address>:8200`, where `<VIP_address>` is the Virtual IP address used by your LSMS system. (The VIP address is always associated with the active server; when switchover occurs, the VIP address association is switched over from previously active server to the newly active server.)
3. Press **Return**.

   The LSMS Web GUI Start Page displays.

   Figure 20: Tekelec LSMS Building Smart Networks Web Page



4. If you are logging in for the first time from this terminal, click either the Setup For Windows button or the Setup For Solaris button and follow the instructions in the displayed page to install a Java plug-in and set up a security policy.

   Otherwise, go to step *Step 5* on page 50.

Note: LSMS only supports the Java 1.5.

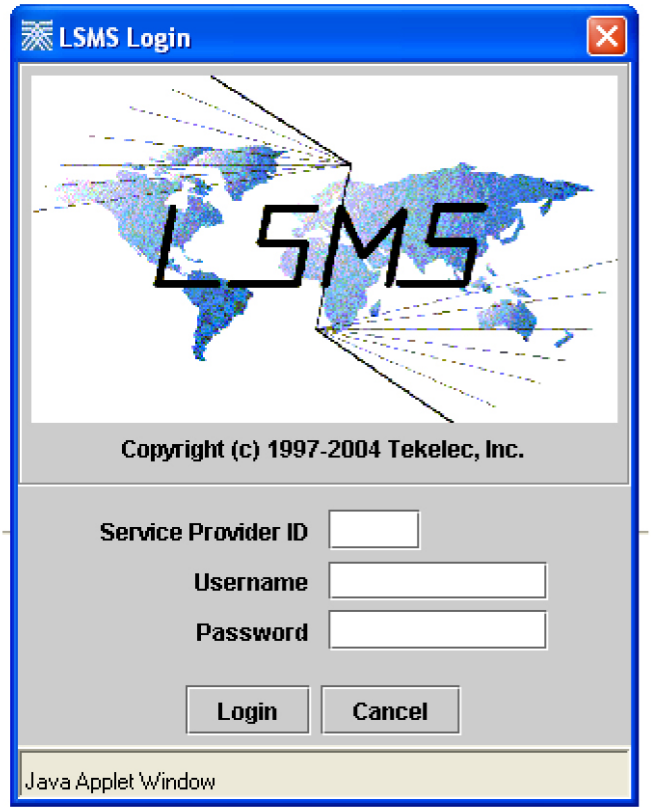
5. Click the Web Interface button, and the LSMS Web GUI Start Page displays.

Figure 21: LSMS Web GUI Start Page with Login Button

6. Click the **Login** button.

The LSMS Login screen displays. From this point on, the web-based GUI works exactly like the server-side GUI. Next, perform the procedure described in *Logging Into the LSMS Console Window* on page 51.

Figure 22: LSMS Welcome/Login Window



Note: If you log out of this web-based LSMS GUI session, you must start a new browser to log back in. If you only want to change user, select User/Session>Change User from the main LSMS menu.

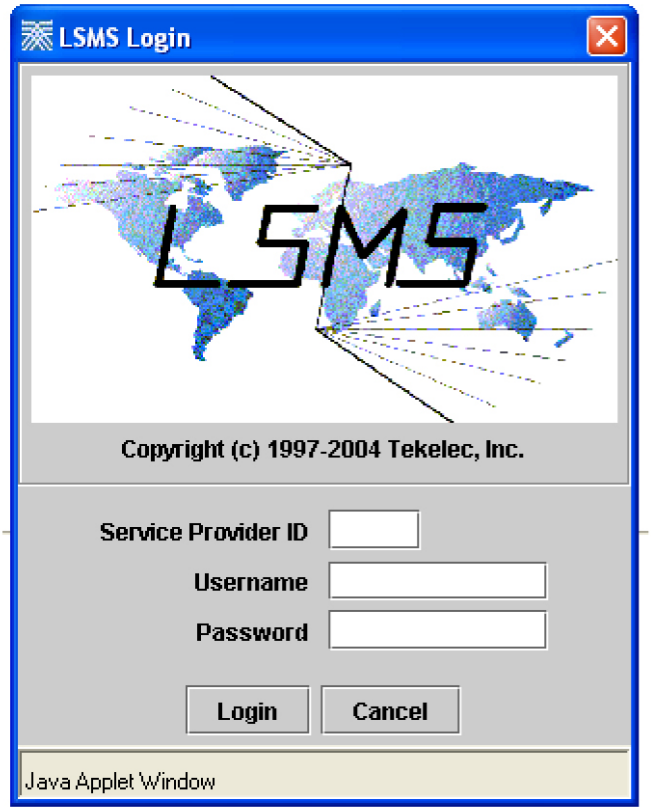
You have now completed this procedure.

Logging Into the LSMS Console Window

After one or more SPIDs have been defined, use the following procedure to log into the LSMS console.

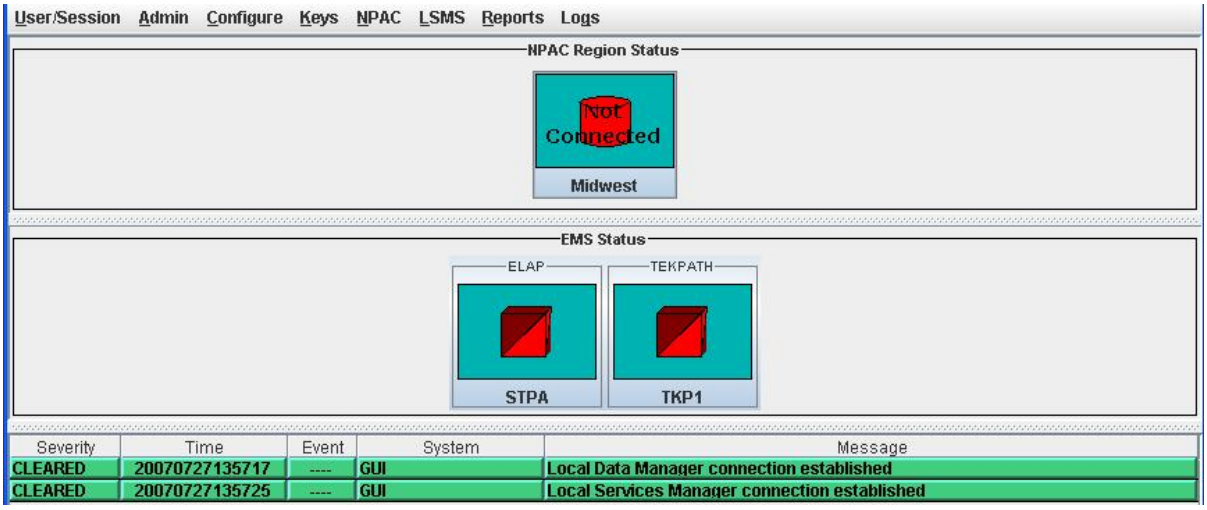
1. After you have completed the procedure described in *Starting a Server-Side LSMS GUI Session* on page 48 or the procedure described in *Starting a Web-Based LSMS GUI Session* on page 48, the **LSMS Welcome/Login Window** displays.

   Figure 23: LSMS Welcome/Login Window



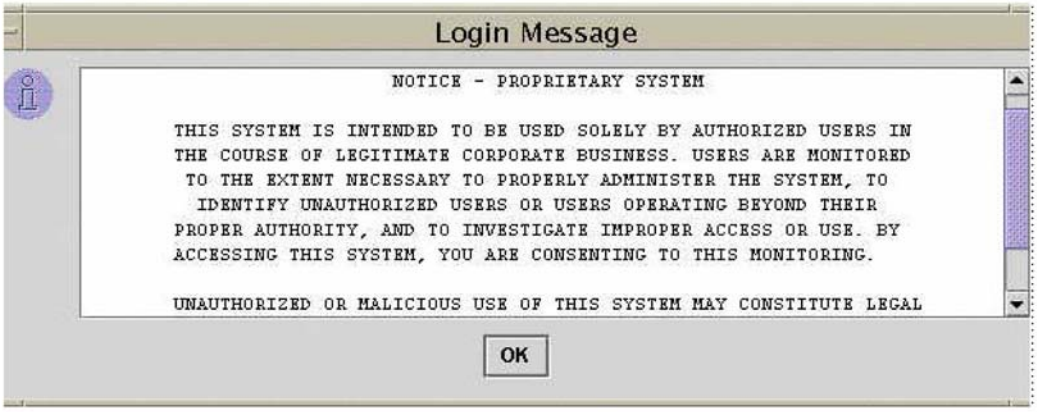
2. Enter the Service Provider ID (SPID), username, and password, which must be as follows:
   - The username and password must have been defined as described in *Managing User Accounts* on page 62 (the group definition determines to which GUI menu items the username will have access).
   - The SPID must be one that has been defined on this LSMS, as described in "Service Provider Contact Information" in the LSMS *Configuration Manual*. In addition, if the SPID Security feature has been enabled, you must enter a username that has been authorized to access the SPID you enter. For information about authorizing usernames to SPIDs, refer to the LSMS *Configuration Manual*.
3. Click **Login**.
   - If the Customizable Login Message feature is not enabled (or it is enabled, but no message text has been created), the **LSMS Console** window displays.

Figure 24: LSMS Console Window



- If the Customizable Login Message feature is enabled and there is user-defined login message text configured, the Login Message dialog displays the message as shown in *Figure 25: Example of Login Message Dialog* on page 53 before the **LSMS Console** window is displayed. System administrators are responsible for creating the customizable login message text (for information about how to create this message text, refer to the LSMS *Configuration Manual*). Tekelec Customer Service is responsible for enabling the feature.

Figure 25: Example of Login Message Dialog



The Login Message dialog displays a 10 line by 80 character viewing area, with a scrollable text area up to a maximum of 5000 characters. Users must acknowledge this message by clicking the **OK** button.

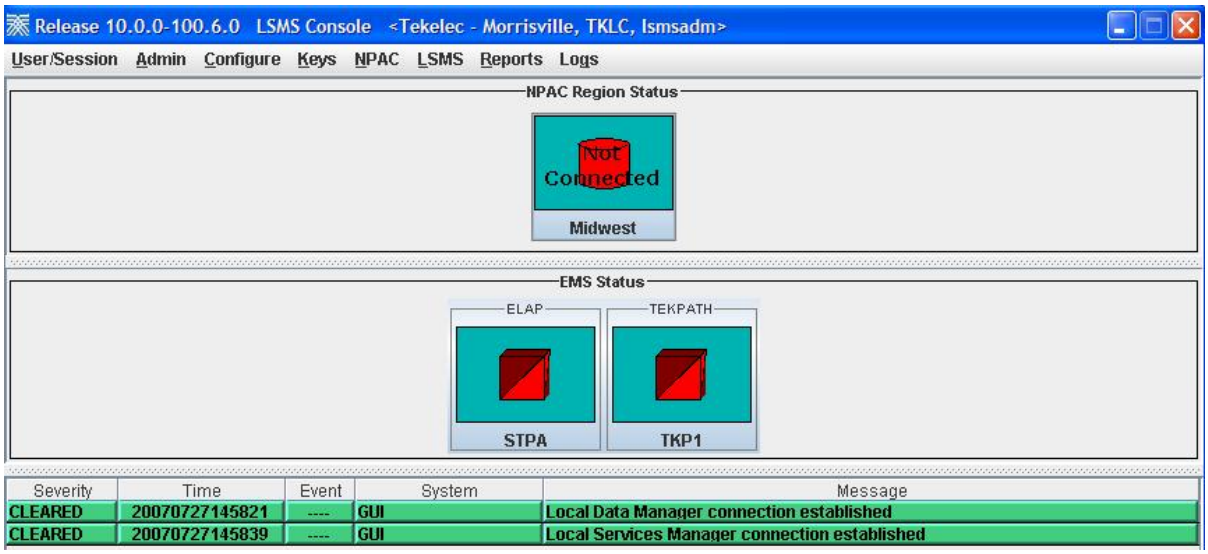
You have now completed this procedure.

Modifying Title Bar in LSMS Console Window

After you successfully log in to LSMS, the console window displays. If the `/usr/TKLC/lsms/config/LSMSname` file exists and contains a (0–30 character) unique LSMS name, the name (in this example, “Tekelec - Morrisville”) is displayed in the title bar along with

the SPID and user name. If the file does not exist or is empty (null), no name will be displayed and the title bar will look as before—displaying only the SPID and user name.

Figure 26: LSMS Console Window with Modified Title Bar



Command Line Interface Utility

To use the command line interface, use the following procedures to start and exit the command line interface utility.

Starting the Command Line Interface

You can use the command line interface utility, `lsmsclaa`, to manage some functions that can also be managed from the LSMS graphical user interface. Once the command line interface is running, you can enter as many of its allowed actions as are required to fulfill a task.

For detailed information about using the command line interface utility, including error situations, see *Using lsmsclaa Commands* on page 230.

Use the following procedure to start the command line interface utility:

1. Use the procedure described in *Logging In to LSMS Server Command Line* on page 45 to log in to the command line of the active server as a member of the permission group required for the function you need to perform.

   For more information about permission groups and authorized functions, and for more information about the command line interface, see *Using lsmsclaa Commands* on page 230.

2. Start the command line interface by entering the following command with parameters as defined in *Table 6: Parameters Used by Command Line Interface* on page 55:

   ```
   $ LSMS_DIR/start_cmdLine <SPID> <REGION> [<COMMANDFILE>]
   ```

Table 6: Parameters Used by Command Line Interface

Parameter	Description	Required?	Characters
<SPID>	Service Provider ID	Yes	4
<REGION>	Name of NPAC region	Yes	6 to 11
<COMMANDFILE>	Full name of a text file that contains a series of commands to be run by the command line interface utility	No	1 to 256

3. The following prompt appears, at which you enter the action you desire:

```
Enter command ->
```

You have now completed this procedure.

Exiting the Command Line Interface

Use the following procedure to exit the command line interface utility:

Enter the following at the command line interface prompt:

```
Enter Command -> EXIT
```

You have now completed this procedure.

Powering On the LSMS

For information about powering on the LSMS servers (LSMSPRI and LSMSSEC), refer to the *T1100* Application Server *Hardware Manual*.

Note: Powering on the LSMS servers (which can be done in any order) does not start the LSMS application and MySQL database services. To start those functions after restoring power to the servers, perform the following steps:

1. Log in to LSMSPRI as `lsmsmgr`.
   (For information about logging in, see *Logging In to LSMS Server Command Line* on page 45.)
2. Select **Maintenance ➤ Start Node** to initiate the following activities:
   - Uninhibit LSMSPRI
   - Transition LSMSPRI to the HA ACTIVE state

   Note: The database on LSMSPRI becomes the master.
3. Log in to LSMSSEC as `lsmsmgr`.

(For information about logging in, see *Logging In to LSMS Server Command Line* on page 45.)

4. Select **Maintenance ➤ Start Node** to initiate the following activities:
   - Copy the database on LSMSPRI to LSMSSEC
   - Begin database replication on LSMSSEC.

     Note: The LSMSSEC database becomes a slave.
   - HA uninhibits LSMSSEC, allowing LSMSSEC to transition to a HA STANDBY state

     LSMSPRI is now active and running the LSMS application; LSMSSEC is in a standby state.

You have now completed this procedure.

Powering Off the LSMS

Before you turn off the system power, all applications on each server must be stopped and the operating system on each server must be stopped. Use the following procedure to power off the LSMS; contact the Tekelec Customer Care Center if additional assistance is needed.

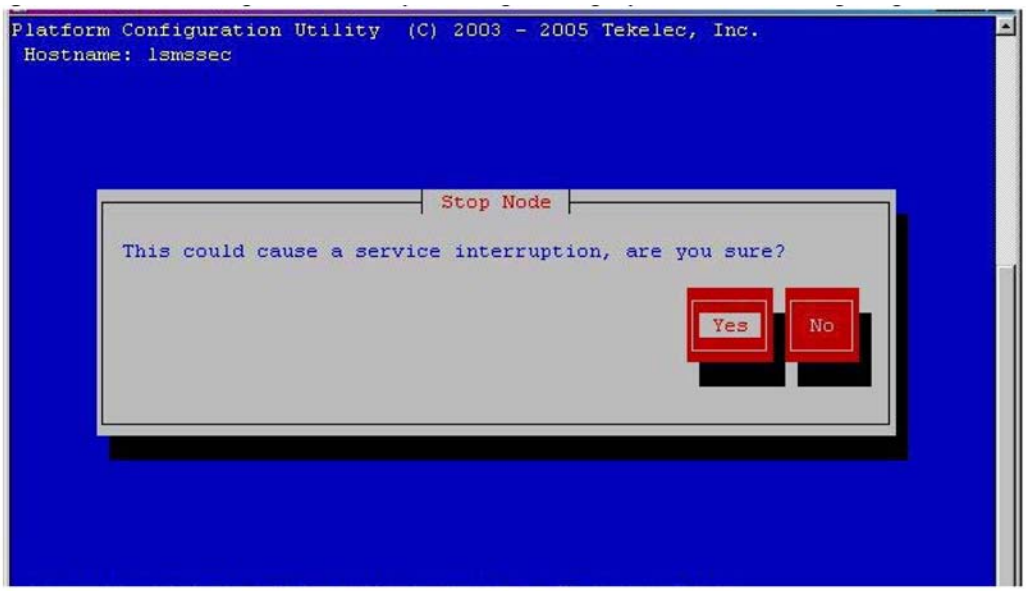
warning: Do not disconnect or connect any cables to the system while the power is on. This action can damage the internal circuits.

1. On the **inactive server:**
   a) Log in to the inactive server as `root`.
   (For information about logging in, see *Logging In to LSMS Server Command Line* on page 45.)
   b) Enter:
   ```
   # init 0
   ```
   The inactive server shuts down and powers off.
   c) Check to ensure the Power Indicator on the T1100 is off.

   Figure 27: T1100 Showing Power LEDs

2. On the **active server:**
   a) Log in to the active server as `lsmsmgr`.
   (For information about logging in, see *Logging In to LSMS Server Command Line* on page 45.)
   b) Select **Maintenance ➤ Stop Node** (see *Figure 28: Example Cautionary Message - Displayed after Selecting Stop Node* on page 57 and *Figure 29: Example Message - Stop Node Completed Successfully* on page 57 for example screens that display after selecting Stop Node).

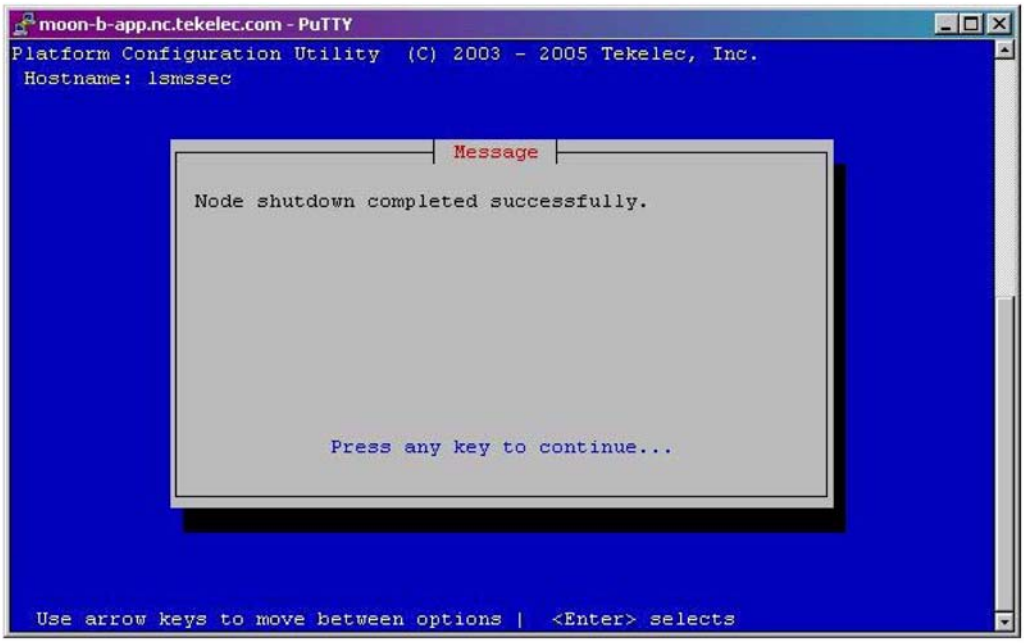
Figure 28: Example Cautionary Message - Displayed after Selecting Stop Node



   c) Select **Yes** to continue the Stop Node process.

   Note: Selecting **Yes** on this screen stops the LSMS application and it also stops the MySQL database services from running.

Figure 29: Example Message - Stop Node Completed Successfully



d) Press any key to continue.

e) Exit the lsmsmgr interface by highlighting **Exit** and pressing **Enter** until you have completely exited.

f) Log in as `root` on the active server.

(For information about logging in, see *Logging In to LSMS Server Command Line* on page 45.)

g) Enter:

```
# init 0
```

The active server shuts down and powers off.

h) Check to ensure the Power LEDs on the T1100 are off (see *Figure 27: T1100 Showing Power LEDs* on page 56).

You have now completed this procedure.

Accessing LSMS through a Dial-In Connection

Tekelec engineers can access your system through a dial-in connection using the modems on the OOBM (Out-of-Band Management) cards in the servers.

Note: This type of connection is for use only by Tekelec Technical Services, and is used by them only when access to LSMS servers is required but network connections are not available.

Managing the System Clock

T he NPAC and LSMS system times must be within five minutes of each other, with the NPAC serving as the master. If the NPAC and LSMS system times are not within five minutes of each other, one of the following GUI notifications may be posted:

```
[Critical]:  <Timestamp> 2003: NPAC [<PRIMARY|SECONDARY>] Connection Aborted by
 PEER : Access Control Failure
```

```
[Critical]:  <Timestamp> 2012: NPAC [<PRIMARY|SECONDARY>]  Connection Attempt
Failed : Access Control Failure
```

If one of these notifications appears, verify and, if necessary, reset the LSMS time using the methods described in either of the following sections:

- *Automatically Controlling the LSMS Time Using NTP* on page 59. Using the Network Time Protocol (NTP) requires access to accurate NTP servers, but results in the LSMS rarely, if ever, being out of synchronization with the NPAC. This section describes how to troubleshoot the rare problems with NTP.
- *Manually Controlling the LSMS Time Without an External NTP Source* on page 61. Using only manual methods to control the LSMS time can result in cases of the LSMS being out of synchronization with the NPAC.

Automatically Controlling the LSMS Time Using NTP

The LSMS allows you to configure the LSMS as an industry-standard Network Time Protocol (NTP) client that communicates with one or more NTP servers elsewhere in your network. NTP reads a time server's clock and transmits the reading to one or more clients with each client adjusting its clock as required.

Configuring the LSMS as an NTP Client

The NTP client protocol is incorporated with the operating system that is included with LSMS. If you choose to implement the LSMS as an NTP client, you must set up one or more NTP servers in your own network (or synchronize with some portion of the existing NTP subnet that runs on the Internet) and configure the LSMS to contact those NTP servers. For information about selecting NTP servers and configuring the LSMS as an NTP client and about displaying current settings for NTP, refer to the LSMS *Configuration Manual*.

If you prefer not to configure the LSMS as an NTP client, you can manually reset the LSMS time when it drifts out of synchronization with the NPAC time, as described in *Manually Controlling the LSMS Time Without an External NTP Source* on page 61.

Verifying NTP Service

Use the following procedure to verify that the time server is working.

Log in to lsmspri as `root` and enter the following command:

```
$ ntpdate -q ntpserver1
```

- If the time server is working, output similar to the following displays:

```
server 198.89.40.60, stratum 2, offset 106.083658, delay 0.02632
22 May 14:23:41 ntpdate[7822]: step time server 198.89.40.60 offset
106.083658 sec
```

- If the time server is not working or is unavailable, output similar to the following displays:

```
server 198.89.40.60, stratum 0, offset 0.000000, delay 0.000000
22 May 14:33:41 ntpdate[7822]: no server suitable for synchronization found
```

Troubleshooting NTP Problems

If you configure the LSMS to communicate with several NTP servers, you should rarely encounter any problems with NTP. This section describes how to troubleshoot the following rare, but possible, error conditions:

- *Reference Time Off By More Than Twenty Minutes* on page 60
- *Violation of Maximum Oscillator Frequency in Network* on page 60

Reference Time Off By More Than Twenty Minutes

The LSMS's NTP client daemon expects that the LSMS system time has been set close to the real time. If the reference time received from the NTP server is significantly different from the LSMS system time, the daemon waits up to twenty minutes until it sets the time. However, if the reference time is off more than about twenty minutes (which is rare), the daemon terminates and does not set the system time.

If you think that the daemon may have terminated, perform the following procedure:

1. Determine whether the `ntpd` daemon process is running by logging in as `root` and entering the following command:

   ```
   # ntpq -p
   ```

   If the daemon is not running, check the `/var/log/messages` file.

2. To set the system clock, either perform the process described in *Manually Controlling the LSMS Time Without an External NTP Source* on page 61 or enter the following command:

   ```
   # ntpdate <IP_address_of_NTP_server>
   ```

3. Start the `ntpd` daemon by entering the following commands:

   ```
   # /etc/rc4.d/S58ntpd start
   ```

4. Verify that the `ntpd` daemon started by repeating step 1.

You have now completed this procedure.

Violation of Maximum Oscillator Frequency in Network

The NTP protocol specifies that systems should have a maximum oscillator frequency tolerance of plus or minus 100 parts-per-million (ppm). This tolerance allows relatively inexpensive workstation platforms to use the NTP protocol. For platforms that meet this tolerance, NTP automatically compensates for the frequency errors of the individual oscillator, such that no additional adjustments are required to either the configuration file or to various kernel variables.

However, some platforms routinely violate this tolerance, and their violation can affect other time servers or time clients in a network. Although the LSMS meets the tolerance requirement, if your

network contains other systems that do not meet the tolerance requirement, you may need to adjust the values of certain kernel variables.

Manually Controlling the LSMS Time Without an External NTP Source

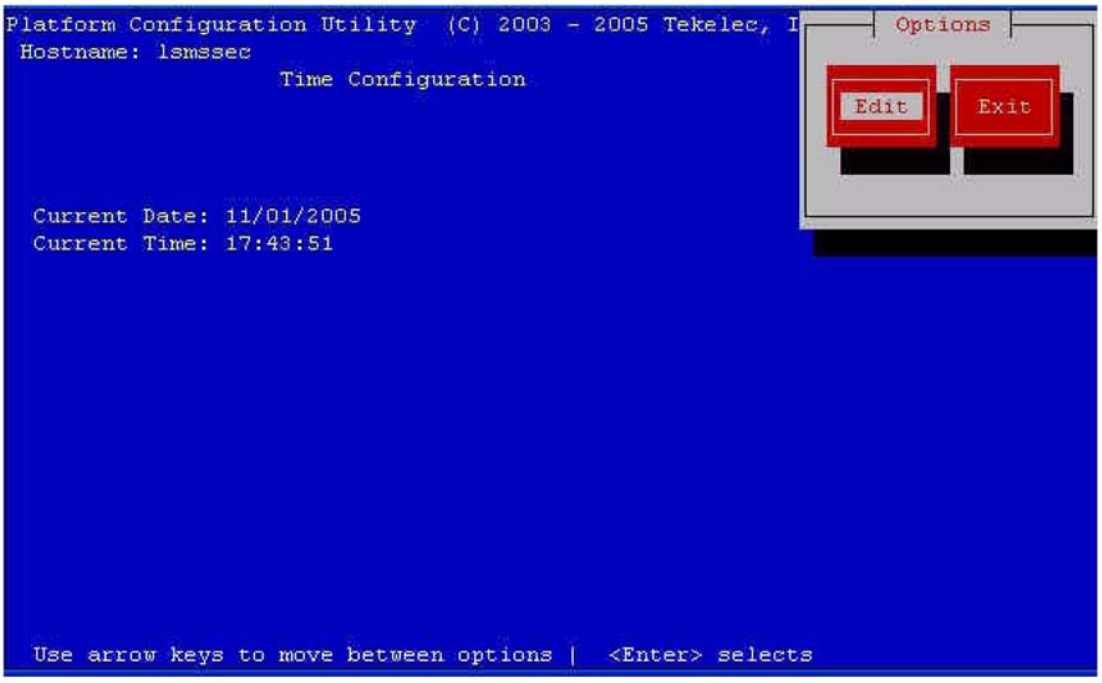
If you choose not to configure the LSMS to use an NTP server, you can use the following procedure to resynchronize the LSMS system time with the NPAC time when one of the notifications described in *Managing the System Clock* on page 59 is posted:

Generally, the following procedure is used only when the LSMS is first installed. However, if you are not able to use another method of synchronizing time with an NPAC (as described in *Automatically Controlling the LSMS Time Using NTP* on page 59), you can contact the NPAC administrator, inquire the time used at the NPAC, and use the following procedure to manually set the LSMS system time and date.

Internal system times are stored in GMT; however, the time and date are typed in the local time zone and converted automatically. If you need to check the local time zone, you can use the `env` command with the `TZ` variable.

1. Log in to active server as `lsmsmgr`.
   (For information about logging in, see *Logging In to LSMS Server Command Line* on page 45.)
2. From the main `lsmsmgr` menu, select **Server Configuration ➤ Set Clock**.
   A window similar to *Figure 30: Set Clock Window* on page 61 displays.

   Figure 30: Set Clock Window



3. If you need to change the current date or time, press Enter while the Edit button is highlighted.
   A window similar to *Figure 31: Edit Date or Time Window* on page 61 displays.

   Figure 31: Edit Date or Time Window

4. Use the down and up arrow keys to move to the field that you want to change.

   Within a field, use the right and left arrow keys to move within a field, delete digits by pressing the Delete key and enter digits by typing them in. When you the values are what you want, press the down arrow key until the OK button is highlighted, and then press Enter. The window shown in *Figure 30: Set Clock Window* on page 61 is displayed again, and it should now display the date and time you set in this step.

5. Log in to the standby server as `lsmsmgr`, and repeat steps 1 through 4.
6. If you have changed the time by more than five minutes, it is recommended that you reboot each server.

You have now completed this procedure.

Managing User Accounts

This section provides information about the following topics:

- Overview information about user names and passwords
- Overview information about the SPID Security feature
- Non-configurable permission groups
- Configurable permission groups
- Managing user accounts on the primary and secondary servers
- Managing user accounts on the administration console

- Changing account passwords using Linux commands
- Activating the SPID Security feature

Overview of User Names and Passwords

The system administrator assigns user names and passwords. Each user name is assigned to one of the following permission groups:

Note: It is possible for an individual user name to have the same value as a group name. For example, usually a user named `lsmsadm` is assigned to the `lsmsadm` permission group. Some LSMS commands require the user to be logged in with the `lsmsadm` user name.

- `lsmsall`
- `lsmsadm`
- `lsmsuser`
- `lsmsuext`
- `lsmsview`

The permission groups govern which commands and which GUI functions the user is allowed to use.

Overview of SPID Security Feature

In addition, the LSMS offers the optional SPID Security feature that allows the LSMS administrator to assign only certain usernames to be allowed to log on with a specified SPID. Alternatively, the LSMS administrator can assign a username to be given access to all SPIDs; such a user is called a "golden user."

Association of a username with a SPID allows the LSMS system administrator to restrict access to the following types of locally provisioned data (for more information about associating usernames with SPIDs, see *Activating the SPID Security Feature* on page 78):

- Default GTT (global title translation)
- Override GTT
- GTT Groups
- TN (telephone number) filters
- Assignment of GTT groups and TN filters to an EMS (element management system). For more information about GTT groups, refer to the LSMS Database *Administration Manual*.

Accessibility to these types of data are protected by SPID security for any access method (for example, through the GUI, through input data by file, audit, and reconcile).

The SPID Security feature is especially useful for LSMS customers that act as service bureaus, offering LSMS services to other service providers. The service bureau may administer locally provisioned data for a client and may choose to allow the client to administer or view its own data without allowing that client to view or change data belonging to other clients.

Note: Without this optional feature, any user can log in using any Service Provider Identifier (SPID) that is defined on the LSMS. The user is able to view any data for any SPID, and depending on which user privileges were assigned to that username, may be able to change data associated with any SPID.

Non-Configurable Permission Groups

Table 7: User Types on page 64 shows a summary of privileges allowed to each user type.

Table 7: User Types

User type	Privileges	User secondary group name	SPID value for logging in
System Administration User	Allows the user to inherit all the privileges of all other user types	`lsmsall`	NPAC-assigned SPID (refer to the LSMS *Configuration Manual*).
System Configuration User	Allows the user to: • Create, modify and maintain the LNP systems, key lists, associations, and the MySQL databases • Stop automatic audits. • Inherit all the privileges of the Viewer User	`lsmsadm`	NPAC-assigned SPID (refer to the LSMS *Configuration Manual*).
Database Administration User	Allows the user to: • Modify and maintain the NPAC and supported service provider data • Have unlimited access to all LNP related-logs, data, and tables • Inherit all the privileges of the Viewer User	`lsmsuser`	Any SPID. If a shadow LSMS exists, use the same SPID for similar functions on main and shadow LSMS.
External User	Allows the user the same access as `lsmsuser`, but the user is not permitted	`lsmsuext`	Any SPID. If a shadow LSMS exists, use the same SPID for similar functions on main and shadow LSMS.

User type	Privileges	User secondary group name	SPID value for logging in
	access to the NPAC menu on LSMS GUI		
Viewer User	Allows the user: • Read access to the LNP data and tables • Limited read access to resource displays and logs • Unlimited access to viewing and acknowledging all alarms	`lsmsview`	Any SPID.

User Permissions for LSMS Commands

Table 8: Access to LSMS Commands on page 65 shows the commands each user type has permission to execute. For more information about the commands, see *Commands* on page 161.

Table 8: Access to LSMS Commands

Command	root	lsmsadm	lsmsuser	lsmsview	lsmsall	lsmsuext
Command permissions: X = Users in this group have permission to use this command. lsmsadm = The user must be logged in with the name lsmsadm to have permission to use this command. root = The user must be logged in with the name root to have permission to use this command.						
`autoxfercfg`		X				
`chglct`		X				
`chkfilter`		X				
`eagle`		lsmsadm				
`import`		X	X	X	X	X
`keyutil`		lsmsadm				
`lsms`		lsmsadm				

Command		root	lsmsadm	lsmsuser	lsmsview	lsmsall	lsmsuext
lsmsdb		root	X	X	X	X	X
lsmsSNMP		root					
lsmssurv		root					
massupdate			lsmsadm				
measdump				X	X	X	X
npac_db_setup			lsmsadm				
npacimport			lsmsadm				
report			X	X	X	X	X
resync_db_setup			lsmsadm				
SAagent			X				
spidsec			lsmsadm				
start_cmdLine			Permissions for following actions depend on type of user who enters this command				
	ABORT		X				
	ASSOCIATE		X				
	AUDIT		X	X			
	EXIT		X	X	X		
	GET		X	X	X		
	HELP		X	X	X		
	SYNCH		X				
start_mgui			Access to local GUI functions depends on type of user who enters this command (see *User Permissions for LSMS Commands* on page 65).				

Command	root	lsmsadm	lsmsuser	lsmsview	lsmsall	lsmsuext
`sup`		lsmsadm				
`sup_db_setup`		lsmsadm				
`survNotify`	root	X	X	X	X	X
`syscheck`	root					

User Permissions for GUI Functions

For information about the GUI functions each permission group can access, refer to the tables in the LSMS *Configuration Manual* (Admin GUI Access, Configure User Access, and Keys GUI Access) and the LSMS Database *Administration Manual* (User/Session GUI Access, NPAC GUI Access, LSMS GUI Access, Reports GUI Access, Logs GUI Access, and Popup Menus GUI Access).

Configurable Permission Groups (LSMS Command Class Mgmt)

When the optional LSMS Command Class Management feature is enabled, LSMS supports configurable GUI permission groups *in addition to* the five non-configurable GUI permission groups (`lsmsadm`, `lsmsuser`, `lsmsview`, `lsmsall`, and `lsmsuext`).

The LSMS supports the creation of 128 additional, configurable GUI permission groups that can be used to ensure a specific and secure environment. After creating the new, configurable GUI permission groups, the system administrator can assign users to the appropriate group.

The configurable GUI permission groups control access to GUI commands, the CLAA (Command Line Administration Application) equivalent, or any command-line equivalent of GUI functions.

A method to control access to a fixed set of commands is provided. Existing commands, executables, and scripts are classified as follows:

- Command-line equivalents of GUI commands (Reports and functions of CLAA)

  These commands are controlled by the assignment of the corresponding GUI function.

- Optional command-line capability for Report Generator (LQL)

  This command may be assigned individually, similar to GUI commands, to one or more permission groups.

- Root privilege-only commands

  These commands are root-only and are not assignable to any permission group.

- Other commands owned by `lsmsadm`

  These commands include those used by the LSMS application, those used to control processes, and those for setup and configuration. Commands in this category are grouped as a single set of administration commands. Users may or may not be granted access to this command-line group, in addition to being assigned to the appropriate GUI group.

  Some commands in this group, although owned by `lsmsadm`, are accessible to non-owners for limited operation, such as status. The incorporation of this feature will not have any impact on the current privileges of commands for non-owners.

Example:

To set up a custom environment, system administrators should define the GUI permission groups and populate those groups with the appropriate commands:

Table 9: Define GUI Permission Groups and Assign Command Privileges

GUI Permission Group	Command Privileges
Custom GUI CONFIG	All Configuration Commands
Custom GUI EMS	All EMS-related Commands
Custom GUI SUPER	All GUI Commands

Optionally, assign users (for example, Mike, Sally, and Bill) to a specific command-line permission group (in this example, `lsmsadm`) or GUI permission group.

Table 10: User Assignment Examples

User	Linux Permission Group	GUI Permission Group
Mike	`lsmsadm`	Custom GUI CONFIG
Joe	`lsmsall`	Custom GUI EMS
Sally	`lsmsadm`	`lsmsadm`
Bill	`lsmsadm`	Custom GUI SUPER

Note: Secure activation is required because this is an optional feature.

After activating this feature, you can create permission groups and assign users to these new groups.

Note: Changes in privileges do not automatically occur upon feature activation.

Permission Group Naming

- The LSMS supports the ability to uniquely name each configurable GUI permission group.
- A group name can consist of a minimum of one character to a maximum of 40 characters (only alphanumeric characters are permitted).

Permission Group Contents

- Each configurable GUI permission group supports any or all of the LSMS GUI commands.

  Note: The GUI command represents the function, via either the GUI, CLAA, or command-line equivalent of GUI commands.

- Any GUI command may be associated with multiple GUI permission groups.
- The optional LQL command for the Report Generator feature can be placed in GUI permission groups.
- The LSMS supports a group containing the current LSMS `lsmsadm` commands with the exception of Report, Audit, and LQL.

Permission Group Commands

The LSMS enables you to perform the following tasks:

- Create and modify GUI permission groups.
- Assign a user to a single GUI permission group.
- Assign a user access to the command group in addition to a GUI permission group.
- Retrieve the names of all permission groups, all the commands permitted within a permission group, and the names of all permission groups that contain a particular command.

Permission Group Processing

GUI Functions:

The LSMS allows a GUI user access to GUI commands, CLAA commands, or command-line equivalents of GUI commands only if that user is an authorized user.

Command-Line-Level:

The LSMS allows a user access to command-line-level scripts and executables only if that user is an authorized user.

Note: For more information about command class management and configurable permission groups, refer to the LSMS *Configuration Manual*.

Managing User Accounts on the Primary and Secondary Servers

To manage user accounts, LSMS utilizes the `lsmsdb command`. This command allows you to add and delete user accounts, change passwords, and list users. The `lsmsdb` command makes the appropriate changes in the system `/etc/password` file.

The following topics explain how to use the `lsmsdb` command to administer LSMS user accounts:

- *Adding a User* on page 70
- *Deleting a User* on page 71
- *Setting the System Level Password Timeout Using the Command Line* on page 72
- *Setting the User Level Password Timeout Using the Command Line* on page 73
- *Displaying All LSMS User Accounts* on page 75

Note: The `lsmsdb` command modifies files on the local system (the system on which lsmsdb is executed). It does not modify or update global network databases.

Therefore, if you add or modify users on one server, make the same change on the other server. Sometimes, for specific administration purposes, you might add or modify users on the servers without adding or modifying them on the administration console.

The following topics explain how to use the LSMS GUI to administer LSMS user accounts:

- *Setting the System Level Password Timeout Using the GUI* on page 72
- *Setting the User Level Password Timeout Interval Using the GUI* on page 74
- *Viewing the Active User List* on page 75

- *Terminating an Active User Session* on page 76

Adding a User

Use the following procedure to add a user account:

1. Log in as `root` and type your password.
   For more information, see *Logging In to LSMS Server Command Line* on page 45.
2. Execute `lsmsdb` with the `adduser` command option:
   ```
   $ cd $LSMS_TOOLS_DIR
   $ lsmsdb -c adduser -u <username>
   ```
3. When the following prompt appears, enter the user password.
   ```
   Enter password:
   ```
4. When the following prompt appears, enter the user password again.
   ```
   Re-enter password:
   ```
   Note: If you did not enter the same password in Steps 3 and 4, the following warning is displayed:
   ```
   WARNING: Passwords must match.
   #
   ```
   In this case, go back to Step *Step 1* on page 70; otherwise, proceed with Step *Step 5* on page 70.
5. When the following prompt is displayed, select the LSMS group name (`lsmsadm`, `lsmsuser`, `lsmsview`, `lsmsuext`, or `lsmsall`) for the user by entering the corresponding number in the `CHOICE` field, then press <return>.
   ```
   Select Secondary Permission Group From List:
   1) lsmsadm
   2) lmsuser
   3) lsmsview
   4) lsmsuext
   5) lsmsall
   CHOICE:
   ```
6. When the following prompt appears, enter **Y** or **N** in the `CHOICE` field to indicate whether you want to enter an expiration date for this login.
   ```
   Set expiration date? Y/N
   CHOICE:
   ```
   Note: If you enter an expiration date, the user will not be allowed to login to this account after that date.

   If you enter **Y** in the `CHOICE` field, the following prompt appears:
   ```
   Enter expiration date (mm/dd/yyyy):
   ```

7. When the following prompt appears, enter **Y** or **N** in the `CHOICE` field to indicate whether you want to enter an **Inactivity Value** (in days) for this account.

```
Set inactivity value? Y/N
CHOICE:
```

Note: If you enter a value (in days), the account will be declared invalid and the user will not be allowed to use that account for the number of days specified.

If you enter **Y** in the `CHOICE` field, the following prompt appears:

```
Enter a number (of days):
```

8. If any other error or warning message displays, contact the Tekelec Customer Care Center.
9. Repeat on other server, if desired.

You have now completed this procedure.

Deleting a User

Use the following procedure to remove a user account:

1. Log in as `root` and type your password.
   For more information, see *Logging In to LSMS Server Command Line* on page 45.
2. Execute `lsmsdb` with the `rmuser` command option:
   ```
   $ cd $LSMS_TOOLS_DIR
   $ lsmsdb -c rmuser -u <username>
   ```
   Upon completion of the command, the prompt will be returned.
3. If an error or warning message displays, contact the Tekelec Customer Care Center.

You have now completed this procedure.

Changing a User Password

Use the following procedure to change a user password:

Note: The `lsmsdb -c chguserpw -u <username>` command must be run on both the primary and the secondary servers to completely change the password.

1. Log in as `root`, or as the user for which the password is going to be changed, and type your password.
   For more information, see *Logging In to LSMS Server Command Line* on page 45.
2. Execute `lsmsdb` with the `chguserpw` command option:
   ```
   $ cd $LSMS_TOOLS_DIR
   $ lsmsdb -c chguserpw -u <username>
   ```
3. When the following prompt appears, enter the current user password.

```
Enter current password:
```

4. When the following prompt appears, enter the new user password.

```
Enter new password:
```

5. When the following prompt appears, enter the new user password again.

```
Re-enter new password:
```

Note: If you did not enter the same password in Steps 3 and 4, the following warning is displayed:

```
WARNING: Passwords must match. #
```

In this case, go back to Step 1; otherwise, proceed with Step 6.

6. If any other error or warning message displays, contact the Tekelec Customer Care Center.

You have now completed this procedure.

Setting the System Level Password Timeout Using the Command Line

Use the following procedure to set the system level password timeout using the command line:

1. Log in as `lsmsadm` and type your password.
   For more information, see *Logging In to LSMS Server Command Line* on page 45.
2. Execute `lsmsdb` with the `syspwexp` command option:

```
$ cd $LSMS_TOOLS_DIR
$ lsmsdb -c syspwexp
```

3. When the following prompt appears, enter **Y**.

```
Configured value: -1
Set password expiration interval? Y/N
```

Note: A configured value of -1 indicates the password timeout has not been configured. A configured value of 0 indicates the password timeout has been configured and the password is valid for an indefinite period of time.

4. When the following prompt appears, enter the password timeout interval.

```
Set maximum number of days before password expires for users.
This will set the default password expiration interval for all users.
Valid values are 0 (never expire) or 1 to 180 days.
Enter value:
```

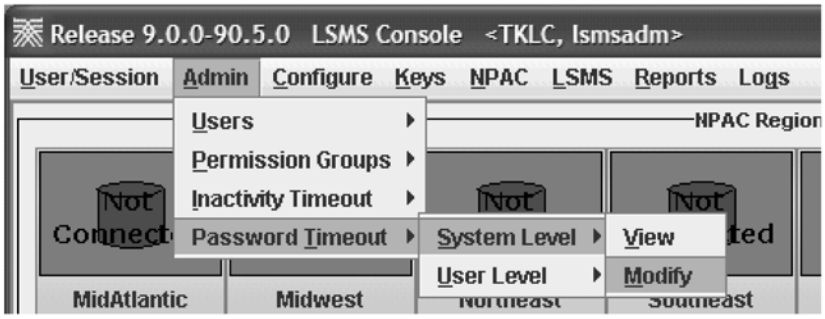
You have now completed this procedure.

Setting the System Level Password Timeout Using the GUI

Use the following procedure to set the system level password timeout using the GUI:

1. Log in to the **LSMS Console** as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin ➤ Password Timeout ➤ System Level ➤ Modify**.

Figure 32: Select Admin ➤ Password Timeout ➤ System Level ➤ Modify



3. Click **Modify**, and the Modify System Level Password Timeout dialog displays.

Figure 33: Modify System Level Password Timeout

4. Type in the number of days for the password timeout interval, then click **OK**.
   If you have successfully modified the password timeout, then the Update Successful dialog displays.

Figure 34: Update Successful

5. Click **OK**.

You have now completed this procedure.

Setting the User Level Password Timeout Using the Command Line

Use the following procedure to set the system level password timeout using the command line:

1. Log in as `lsmsadm` and type your password.
   For more information, see *Logging In to LSMS Server Command Line* on page 45.

2. Execute `lsmsdb` with the `usrpwexp` command option:

   ```
   $ cd $LSMS_TOOLS_DIR
   $ lsmsdb -c usrpwexp -u <username>
   ```

3. When the following prompt appears, enter **Y**.

   ```
   Configured value: -1
   Set password expiration interval? Y/N
   ```

   Note: A configured value of -1 indicates the password timeout has not been configured. A configured value of 0 indicates the password timeout has been configured and the password is valid for an indefinite period of time.

4. When the following prompt appears, enter the password timeout interval.

   ```
   Set maximum number of days before password expires for the user.
   Valid values are 0 (never expire) or 1 to 180 days.
   Enter value:
   ```

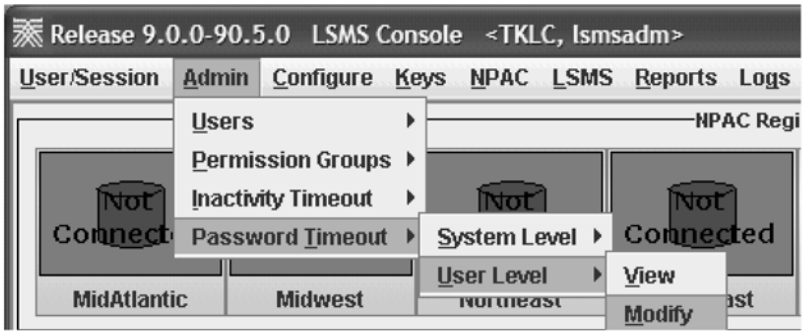
You have now completed this procedure.

Setting the User Level Password Timeout Interval Using the GUI

Use the following procedure to set the system level password timeout using the GUI:

1. Log in to the **LSMS Console** as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **Admin ➤ Password Timeout ➤ User Level ➤ Modify**.

   Figure 35: Select Admin ➤ Password Timeout ➤ User Level ➤ Modify



3. Click **Modify**, and the **Modify User Level Password Timeout** dialog displays.

   Figure 36: Modify User Level Password Timeout

4. Select a user whose password timeout interval you want to modify.
5. Type in the number of days for the password timeout interval, then click **OK**.

   If you have successfully modified the password timeout, then the Update Successful dialog displays.

   Figure 37: Update Successful

6. Click **OK**.

You have now completed this procedure.

Displaying All LSMS User Accounts

Use the following procedure to display a list of all LSMS GUI Users:

1. Log in as `root` and type your password.

   For more information, see *Logging In to LSMS Server Command Line* on page 45.
2. Execute `lsmsdb` with the `users` command option:

   ```
   $ cd $LSMS_TOOLS_DIR
   $ lsmsdb -c users
   ```

   The configured LSMS users will be output one user per line.

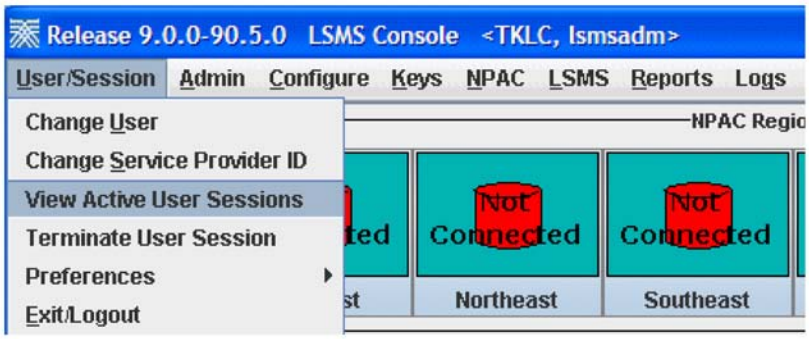
You have now completed this procedure.

Viewing the Active User List

Use the following procedure to display a list of active LSMS GUI Users:

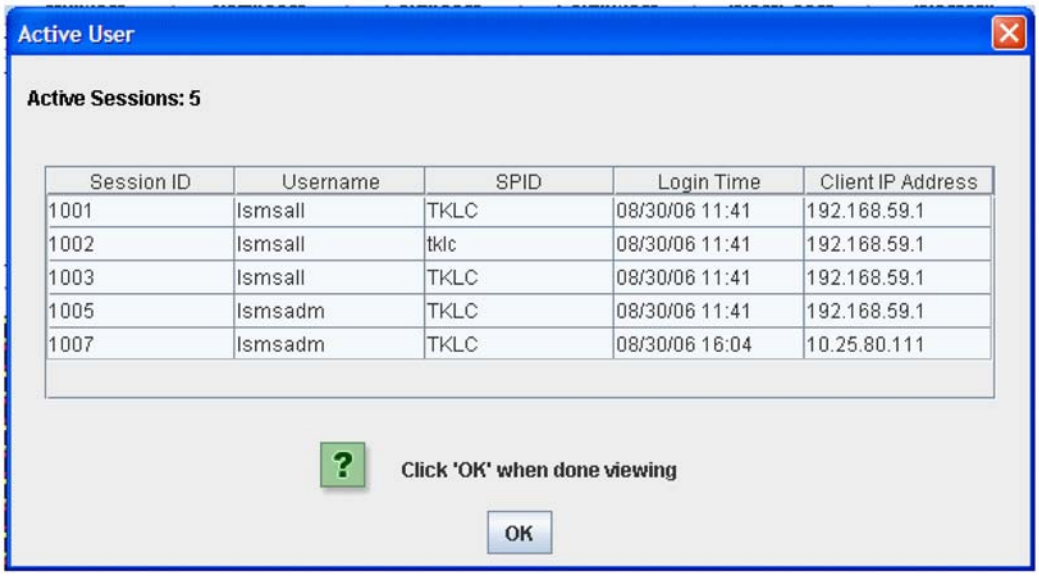
1. Log in to the **LSMS Console** as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **User/Session ➤ View Active User Sessions**.

   Figure 38: Select User/Session ➤ View Active User Sessions



3. Click **View Active User Sessions**, and the View Active User Sessions dialog displays.

Figure 39: View Active User Sessions Dialog



4. Click OK when you are done viewing the Active User list.

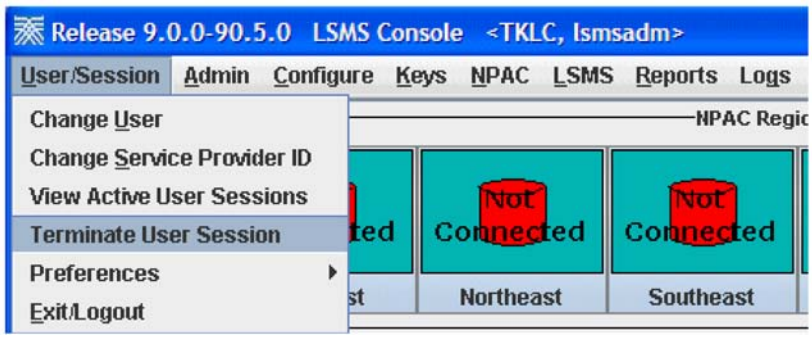
You have now completed this procedure.

Terminating an Active User Session

Use the following procedure to terminate the session of an active LSMS GUI User:

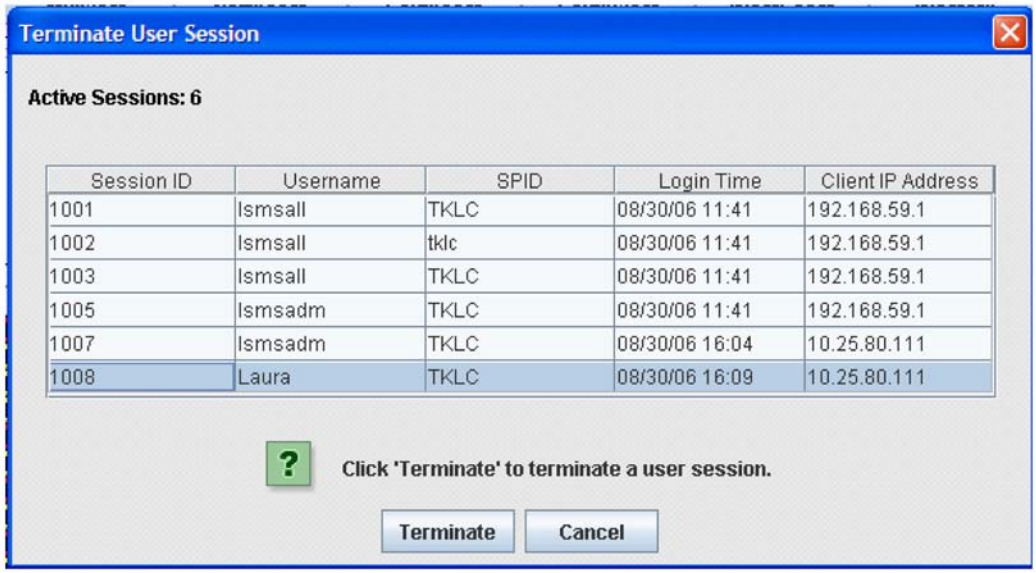
1. Log in to the **LSMS Console** as a user in the `lsmsadm` or `lsmsall` group.
2. From the main menu, select **User/Session ➤ Terminate User Session**.

Figure 40: Select User/Session ➤ Terminate User Session



3. Click **Terminate User Session**, and the Terminate User Session dialog displays.

Figure 41: Terminate User Session Dialog

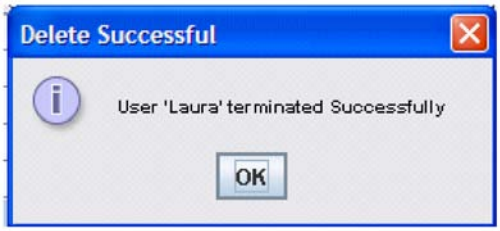


4. Click on the user session you want to end and click **Terminate**.
5. If you are sure you want to terminate the session, click **Yes** in the Confirm Delete dialog, otherwise click **No**.

Figure 42: Confirm Delete Dialog

6. After you successfully terminate a user session, click **OK** in the Delete Successful dialog.

Figure 43: Delete Successful Dialog



You have now completed this procedure.

Activating the SPID Security Feature

This feature is activated by Tekelec customer service using secure activation procedures. Once the feature is activated, the following actual usernames (not user group names) are defined to be "golden users" having access to all SPID and all other usernames are defined to have no access to any SPIDs:

- `lsmsadm`
- `lsmsview`
- `lsmsall`
- `lsmsuser`
- `lsmsuext`

After the feature has been activated, the LSMS administrator (`lsmsadm`) is advised to immediately define associations between usernames and SPIDs as described in the following procedure:

1. Log in as `lsmsadm` on the active server.
2. If you do not wish the username `lsmsadm` to have access to all SPIDs, enter the following command to remove the username from golden access:

   ```
   $ spidsec -r -u lsmsadm -s golden
   ```

3. If desired, repeat step *Step 2* on page 78 for the usernames `lsmsview`, `lsmsall`, `lsmsuser`, and `lsmsuext`.
4. To display all the usernames currently defined on the LSMS, see *Displaying All LSMS User Accounts* on page 75.
5. For each displayed username, determine which SPIDs you wish to allow this user access to and enter the following command to authorize this username for the specified SPID:

   ```
   $ spidsec -a -u <username> -s {<spid>|golden}
   ```

   The following parameters and options apply to this command:

`<username>`	A valid LSMS username that has been provisioned using admintool
`<spid>`	A valid SPID defined on the LSMS (alternatively, you can enter `golden` to allow this username access to all SPIDs defined on the LSMS)

   To authorize this username to multiple SPIDs, but not for all SPIDs, you must enter the command once for each SPID.

6. Repeat step *Step 5* on page 78 for each user displayed in step *Step 4* on page 78.

You have now completed this procedure.

Chapter 4

Preventive Maintenance

Topics:

- *Introduction Page 80*
- *Recommended Daily Monitoring Page 80*
- *LSMS Preventive Maintenance Schedule Page 81*
- *Using Backup Procedures Page 82*
- *Performing Routine Cleaning Page 94*
- *Additional Tools for Monitoring the LSMS Hardware and the Network Page 95*
- *Managing Automatic File Transfers Page 100*

This chapter describes preventive maintenance of the LSMS. Included are topics on backing up databases and file systems, monitoring hardware and network performance, and routine cleaning.

Introduction

This chapter describes preventive maintenance of the LSMS. Included are topics on backing up databases and file systems, monitoring hardware and network performance, and routine cleaning.

Use the system monitoring features regularly, especially during times of peak load, to verify that the system has adequate resources. This practice provides an insight into system resource utilization and provides early warning if the system capacity limits are being approached.

The procedures in this chapter assume that you are familiar with the LSMS hardware. For more information about the hardware, refer to the *T1100* Application Server *Hardware Manual.*

Recommended Daily Monitoring

To properly maintain your LSMS system, it is recommended that you perform the activities described in this section on a daily basis.

Continuous Monitoring Activities

Perform the following activities continually:

- Always keep at least one graphical user interface (GUI) open. Monitor the GUI especially for any red or yellow conditions, either on the NPAC and EMS status icons or in the notifications display area. For more information about the display areas of the GUI, refer to the LSMS Database *Administration Manual*. For information about notifications displayed in the notifications display area, see *Automatic Monitoring of Events* on page 247.
- Monitor the latest Surveillance notifications in either or both of the following ways:
  - Connect a customer-provided administration console to Serial Port 1 of each server so that Surveillance notifications can be displayed there.
  - View the Surveillance log file, `/var/TKLC/lsms/logs/survlog.log`. To display the latest contents of this file, log in as any user and enter the following command:

    ```
    $ tail -f /var/TKLC/lsms/logs/survlog.log
    ```

    For more information about the Surveillance feature, see *Understanding the Surveillance Feature* on page 34.

Once a Day Monitoring Activities

It is recommended that once each day you perform the following:

- Examine logs for abnormalities. For more information, see *Daily Examination of Logs for Abnormalities* on page 81.
- Determine the success or failure of the database and file system backups by examining the backup log (`/var/TKLC/log/backup/backup.log`) and the surveillance log (`/var/TKLC/lsms/logs/survlog.log`). For more information, see *Daily Determination of Success or Failure of Backup* on page 81.

Daily Examination of Logs for Abnormalities

Examine the following logs for any abnormalities once a day, preferably near the end of the day. In each of these logs, `<MMDD>` indicates the month and day. Each log is kept for seven days. For more information about these logs, refer to the LSMS Database *Administration Manual*. You can view the logs using the GUI or you can use any text editor.

- Examine the following exception log files:
  - Run the `chkfilter` command and then examine `/var/TKLC/lsms/logs/trace/LsmsSubNotFwd.log.<MMDD>`. This log contains subscription versions (SVs) or number pool blocks (NPBs) that have been received from an NPAC but could not be forwarded to a network element because the LSMS has no EMS routing defined for the SVs or NPBs.
  - `/var/` TKLC `/lsms/logs/<clli>/LsmsRejected.log.<MMDD>`. This log contains transactions that the LSMS attempted to forward to a network element, but which were rejected by the network element.
- Examine the following alarm logs to verify that you are aware of all alarms (these events will also have been reported in the GUI notifications display).
  - `/var/TKLC/lsms/logs/alarm/LsmsAlarm.log.<MMDD>`. This log contains events associated with the Local Data Manager, the Local Services Manager and regional NPAC agent processes.
- Examine the following transaction logs for any abnormalities:
  - `/var/TKLC/lsms/logs/<clli>/LsmsTrans.log.<MMDD>` for each network element identified by `<clli>`. These logs contain all transactions forwarded to EMS agents, including information associated with M-Create, M-Set, and M-Delete operations initiated from the NPAC.
- Examine the Surveillance log `/var/TKLC/lsms/logs/survlog.log` for any abnormalities. This log contains all surveillance notifications that have been posted.

Daily Determination of Success or Failure of Backup

Each day, check the backup log from the previous day on each server (as you can see from the timestamps in *Figure 44: Example of Successful Backup Log for STANDBY Server* on page 83 and *Figure 45: Example of Successful Backup Log for ACTIVE Server* on page 83, backups generally begin a few minutes before midnight). Ensure that the backup logs contain text similar to that shown in the referenced figures. If you need help interpreting the logs, contact the Tekelec Customer Care Center.

If you determine that the automatic backup(s) did not complete successfully, perform a manual backup right away.

LSMS Preventive Maintenance Schedule

Follow this preventive maintenance schedule, completing each item at least as frequently as recommended.

Weekly Procedures:

- Copy the most recent backup to the tape on the NAS (Network Access Storage), and store the tape off-site (see *Storing Backup Tapes Off-Site* on page 84).
- Check LED indicators on the servers; for details about the server LEDs, refer to the *T1100* Application Server *Hardware Manual*.

Monthly Procedures:

- Change the filters on the T1100 servers; for details about the T1100 filters, refer to the *T1100* Application Server *Hardware Manual*.

Quarterly Procedures:

- Remove dust buildup (*Preventing Dust Buildups* on page 94)

As Needed Procedures:

- Clean CD-ROM disks before use (*Cleaning CD-ROM Disks* on page 95)

Using Backup Procedures

The most basic form of backup happens continuously and automatically, as the redundant LSMS servers contain duplicate hardware, and the standby server replicates the active server's database.

However, if data becomes corrupted on the active server's database, because data on the active server's database is automatically replicated to the standby server, you must also follow more conventional backup procedures so that you can recover from a corrupted database. A database saved to file on the NAS (Network Attached Storage) device or copied from the disk to tape on the NAS and then stored off-site is a precaution against database corruption.

Understanding How the LSMS Backs Up File Systems and Databases

Each night at midnight, the LSMS automatically backs up the following to disk:

- Platform configuration (for each server), stored as `plat.xml`
- The entire LSMS database, stored as `lsmsdb.xml`
- The entire LSMS logs filesystem, stored as `lsmslogs.xml`

When both servers are functioning, the automatic backup function backs up the database (lsmsdb.xml) and logs (lsmslogs.xml) from the standby server, and backs up only the platform configuration (plat.xml) from the active server.

If only one server is active, the automatic backup function backs up all the files shown in the bulleted list above from the active server.

In addition, you can perform the same backups manually at any time (see *Backing Up the LSMS Manually* on page 87).

Note: Both the nightly automatic backup and any manual backups are stored only to disk on the NAS. To ensure that you have safely stored backups, you should periodically (for example, once

a week) copy the desired archives on the NAS disk to a tape on the NAS, as described in *Storing Backup Tapes Off-Site* on page 84.

Understanding the Backup Results

The result of each backup is posted to the log file on the server on which the backup was scheduled to take place.

1. Log into the server as `lsmsview`.
2. At the command line prompt, enter the following command to view the log:
   ```
   # more /var/TKLC/log/backup/backup.log
   ```
3. Output:
   a) The example backup log for the standby server indicates that on Wednesday, December 7, an automatic backup was performed on the standby server.

   After completing the backup task for each respective backup type (platform, database, and logs), an entry was generated and stored in the backup log. If the backup was successful, output similar to the following displays:

   Figure 44: Example of Successful Backup Log for STANDBY Server

   ```
   lsmsbkp:*** Backup started at Wed Dec  7 23:55:04 EST 2005 ***
   lsmsbkp: Local HA status:  STANDBY.
   lsmsbkp: Remote HA status: ACTIVE.

   lsmsbkp: Backup type:      Platform.

   lsmsbkp: Backup type:      DataBase.

   lsmsbkp: Backup type:      Logs.
   ```

   The example backup log for the active server indicates that on Wednesday, December 7, an automatic backup was also performed on the active server. After completing the backup task for the platform files, an entry was generated and stored in the backup log. If the backup was successful, output similar to the following displays:

   Figure 45: Example of Successful Backup Log for ACTIVE Server

   ```
   lsmsbkp:*** Backup started at Wed Dec  7 23:55:05 EST 2005 ***
   lsmsbkp: Local HA status:  ACTIVE.
   lsmsbkp: Remote HA status: STANDBY.

   lsmsbkp: Backup type:      Platform.
   ```

   ---

   b) If the backup was unsuccessful, output similar to the following displays:

   Figure 46: Example of Unsuccessful Backup Log for ACTIVE Server

```
lsmsbkp:*** Backup started at Thu Jan 12 14:03:52 EST 2006 ***
lsmsbkp: Local HA status:  ACTIVE.
lsmsbkp: Remote HA status: STANDBY.

lsmsbkp: Backup type:      Platform.

ERROR: Remote command failed: RC=1
ERROR: reported: ssh: connect to host backupserver-lsmspri port 22: No route to
host

WARNING: Could not create lockfile /Volumes/LVstorage/LOCK.lsmspri
err | Repository is already locked!
```

You have now completed this procedure.

Storing Backup Tapes Off-Site

Once a week, Tekelec recommends that you do the following, as described in the procedure below:

- Copy the most recent backup stored on the NAS to the tape in the NAS. Verify the date of the backup tape before you remove the tape from the NAS. Also copy the platform files from the primary and secondary servers, and the log files.

  Note: See *Figure 48: Available Archives Menu* on page 85 to view the Available Archives Menu, which lists the files you can save to tape. Select **db** to archive database files, **logs** to archive all log files, **lsmspri** to archive the platform files on the primary server, and **lsmssec** to archive the platforms on the secondary server.

- Remove the tape from the NAS.
- Insert new, blank, write-enabled tape into the NAS. Tekelec recommends using LTO-2 type tape cartridge or equivalent.
- Label the removed tape.
- Store the removed tape in a secure, off-site location.

To accomplish these recommended actions, perform the following procedure:

1. Insert an LTO-2 tape into the NAS tape drive.
2. Log into the active server as `lsmsmgr`.
   (For information about logging in, see *Logging In to LSMS Server Command Line* on page 45.)
3. From the Main Menu, select **Maintenance ➤ Backup and Restore ➤ Backup Server Tape Device**.

   The **System Busy** window displays, and no action is required. After a few minutes, the **Available Archives Menu** window displays.

   Figure 47: System Busy - Retrieving Backup Server Directory Listing

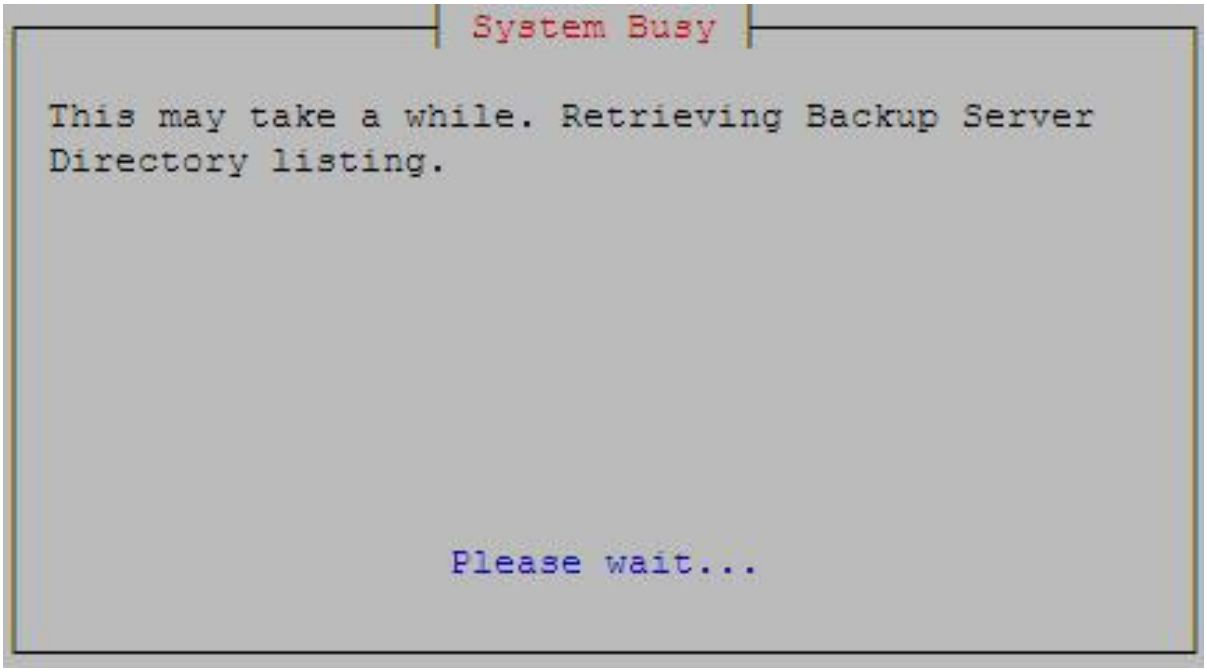
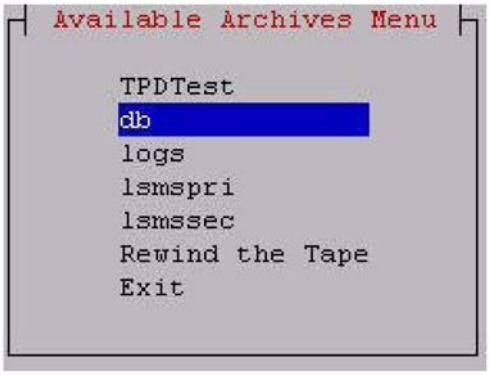


Figure 48: Available Archives Menu



4. Select **db** and press Enter.

   Note: The most important archive to store on tape is the **db** (database) archive. Before copying a db image to tape, check the backup.log on the LSMS to be sure that backups are completing. Usually the db is backed up on the standby server, but if the LSMS is running in simplex mode (only one server is functioning) the db is backed up on the active server.

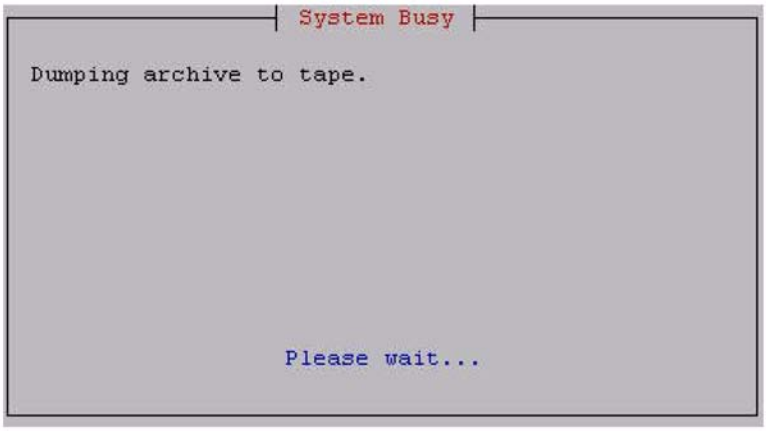
   A window that features specific db archives displays.

   Figure 49: Specific Available db Archives

5. Select the archive you want to store to tape (usually, you will choose the archive with the most recent date) and press **Enter**.

   The System Busy window displays.

   Figure 50: System Busy - Dumping Archive to Tape



6. When the NAS has finished copying the selected archive to the tape, select **Exit**, and then press **Enter**.
7. If you do not need to copy any other archives of this type to tape, select **Exit**, and then press **Enter**.

   The **Available Achives Menu** displays again.

   Note: It is recommended that you also copy archives of the log files (**logs**), the primary server platform files (**lsmspri**), and the secondary server platform files (**lsmssec**). Select the archive type you desire, and repeat steps *Step 4* on page 85 through this step for each additional archive type that you want to copy to tape.

8. From the **Available Archives Menu**, select **Rewind the Tape** and press **Enter**.

   Rewinding the tape make take a few minutes.

9. After the tape has been rewound, the **Available Archives Menu** displays again.

   Figure 51: Available Archives Menu

10. To exit the **lsmsmgr** interface select **Exit** and press **Enter** until you have completely exited.
11. Remove the backup tape from the NAS.
    Apply a label that contains the date of the backup and which archive is included.
12. Insert a new, blank, write-enabled tape into the NAS.
    Tekelec recommends using LTO-2 type tape cartridge or equivalent.
13. Transport the backup tapes to a safe and secure off-site location.

You have now completed this procedure.

Backing Up the LSMS Manually

Before beginning a manual backup, read *Understanding How the LSMS Backs Up File Systems and Databases* on page 82. Also, check the GUI notification information and surveillance logs for database errors before beginning the manual backup procedure to ensure that the LSMS is functioning correctly.

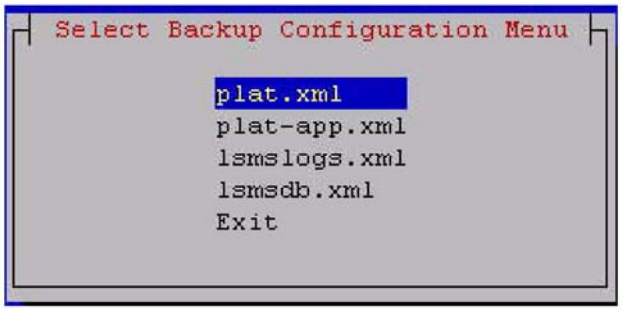
The following procedure explains how to start a backup manually. If a backup procedure fails, contact the Tekelec Customer Care Center.

1. Perform the procedure described in *Checking for Running Backups* on page 93 to ensure that no other backup (automatic or manual) is already running.
2. Ensure that none of the following processes are running.
   All of these processes use temporary file space on the LSMS. If you attempt to start a backup, you may run out of file space.
   - Starting a standby node (to change its state from UNINITIALIZED "INHIBITED" to STANDBY)
   - An `import` command
   - An `lsmsdb quickaudit` command
   - A query server snapshot (`lsmsdb snapshot`)
3. Log into the active server as `lsmsmgr`.
   (For more information, see *Logging In to LSMS Server Command Line* on page 45.)
4. View the backup log and ensure that the backup completed successfully.
   Note: The backup log shows only the active server's backup results.
   For more information, see *Daily Determination of Success or Failure of Backup* on page 81.

5. From the Main Menu on the active server, select **Maintenance ➤ Backup and Restore ➤ Network Backup**.

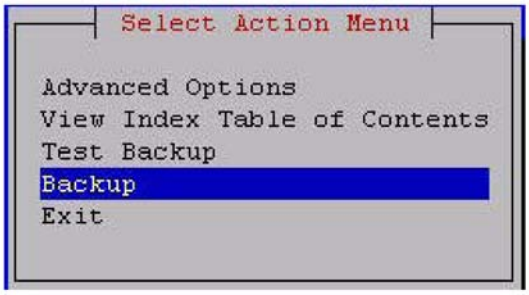
   Select **plat.xml**.

   Figure 52: Select Backup Configuration Menu Window



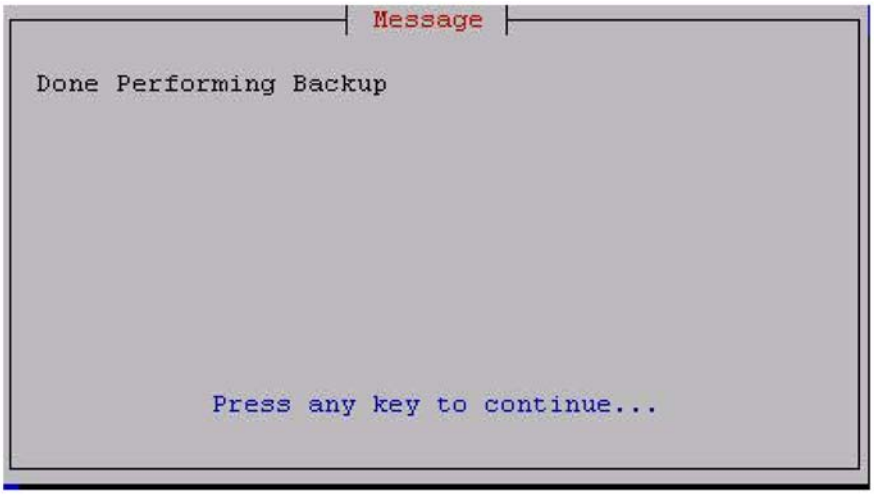
6. Press **Enter**, then select **Backup**.

   Figure 53: Select Backup on Active Server



7. When the backup is complete, press any key to continue.

   Figure 54: Backup Complete on Active Server

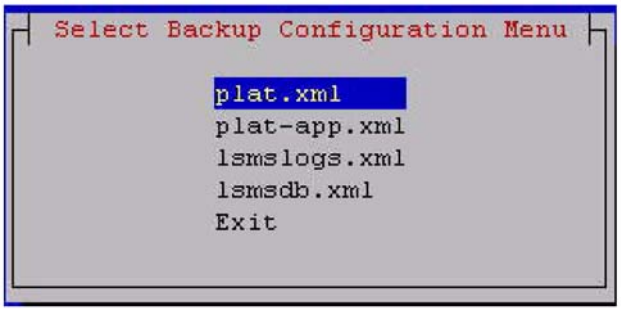


8. Log into the standby server as **lsmsmgr**.
   (For information, see *Logging in from One Server to the Mate's Command Line* on page 47.)

Note: If the standby server is not functional, perform the rest of the procedures on the active server.

9. Select **plat.xml** on the standby server, and press **Enter**.

Figure 55: Select plat.xml on Standby Server



10. Select **Backup**.

Figure 56: Select Backup on Standby Server

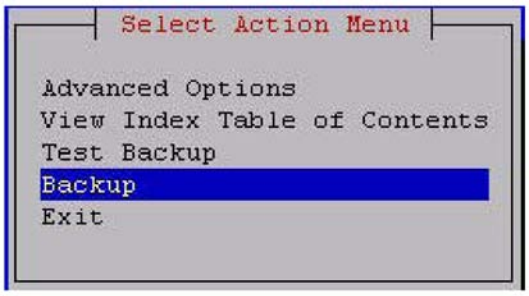
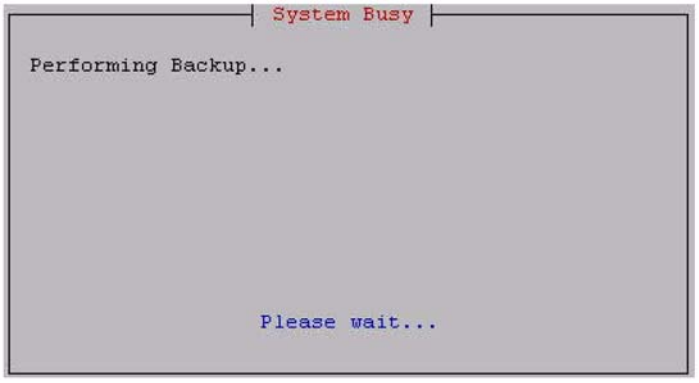
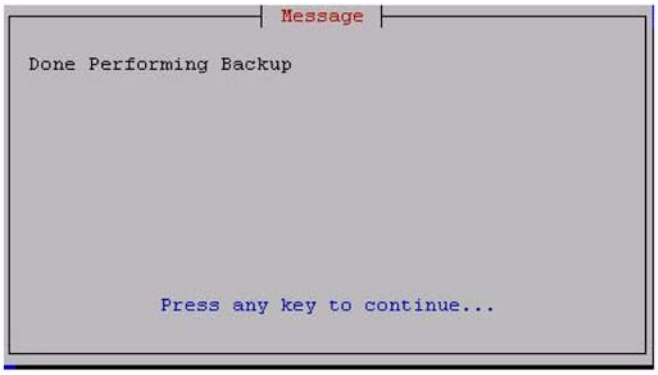


Figure 57: Performing Backup Screen



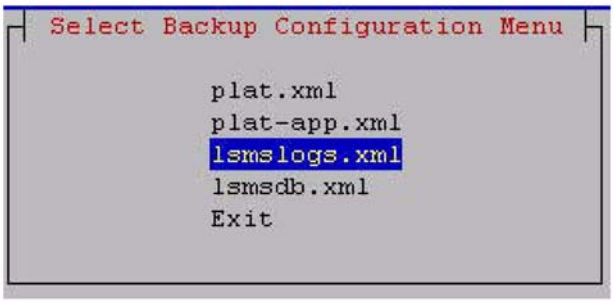
11. When the backup is complete, press any key to continue.

Figure 58: Backup Complete on Standby Server



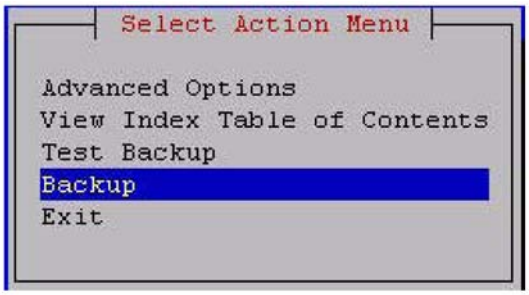
12. Select **lsmslogs.xml** on the standby server, and press **Enter**.

Figure 59: Select lsmslogs.xml on Standby Server



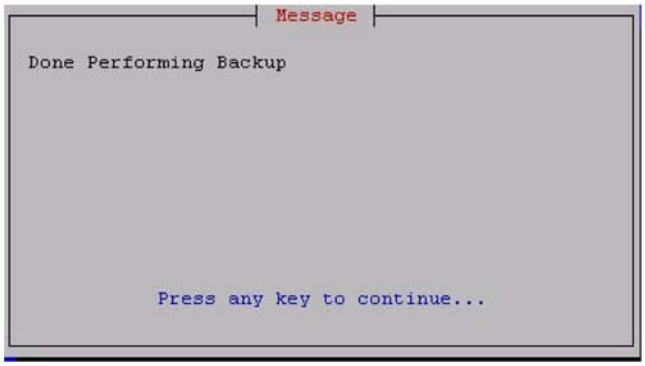
13. Select **Backup**.

Figure 60: Select Backup on Standby Server



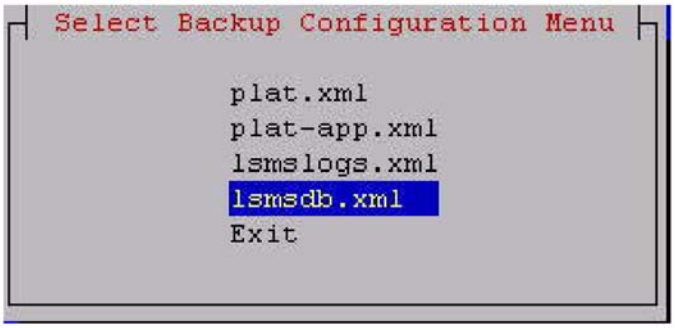
14. When the backup is complete, press any key to continue.

Figure 61: Backup Complete on Standby Server



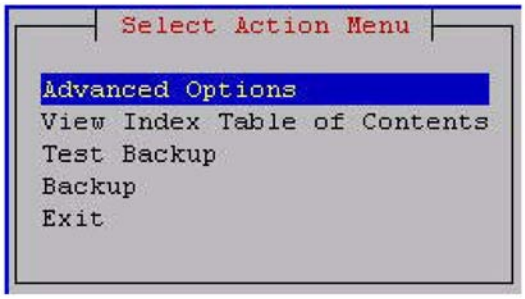
15. Select **lsmsdb.xml**, and press **Enter**.

Figure 62: Select lsmsdb.xml on Standby Server



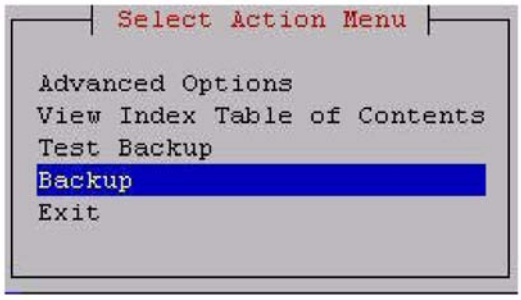
16. When the server has completed loading the **Select Action Menu** displays.

Figure 63: Select Action Menu



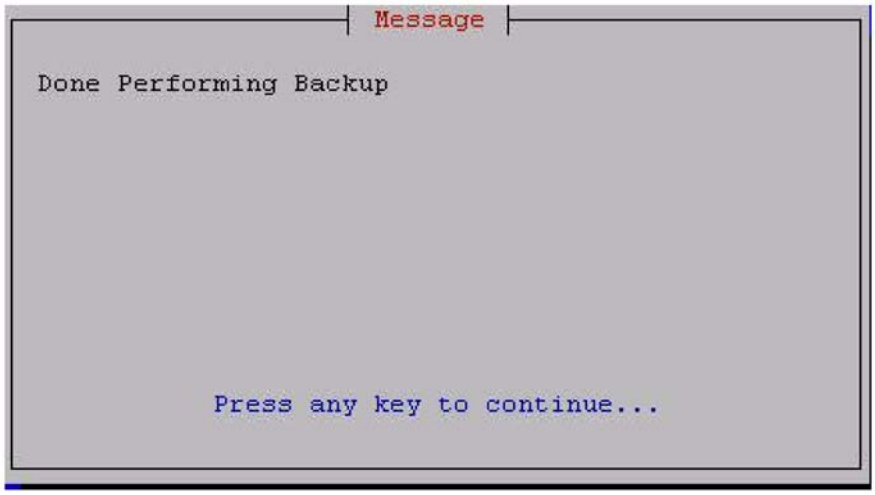
17. Select **Backup**, and press **Enter**.

Figure 64: Backup



18. When the backup completes, press any key to continue.

Figure 65: Backup Complete



You can now exit to the Main Menu, or choose another menu item.

You have now completed this procedure.

Stopping an Automatic or Manual Backup

Under normal conditions, backups complete relatively quickly (in less than 45 minutes). However, if no backup has been previously performed or if the previous backup was stopped before it completed, the next backup can take up to 4 hours.

It is advisable to allow a backup to complete. However, if you accidentally start a backup or need to stop the backup process, use the following procedure. You must log into both the active and standby servers to stop a backup.

Note that a backup cannot restart at the point where it was aborted because various lock files are created to prevent conflicting backups. To restart a manual backup, start the procedure from the beginning. See *Backing Up the LSMS Manually* on page 87 if you need help.

If you need to restore data from a previously recorded backup, contact the Tekelec Customer Care Center.

1. Log in as `root` on active server.
2. To find the process ID of the processes involved in backing up the databases, enter the following command:

```
# ps -ef | egrep "rsync|netbackup|lsmsbkp" | grep -v grep
```

The output from the above command includes the process ID (PID), also referred to as the job number, for each process that has the characters `rsync`, `netbackup`, or `lsmsbkp` in its name. Note the first PID (shown in**bold** text in the following example) displayed on the line for each process.

```
root      5673 32428  0 13:43 pts/0    00:00:00 /bin/sh
/usr/TKLC/lsms/tools/lsmsbkp
root      5759  5673  4 13:43 pts/0    00:00:00 /usr/bin/perl -T
/usr/TKLC/plat/bin/netbackup
--config=/usr/TKLC/plat/etc/BackupTK/plat.xml
root      5942  5759 25 13:43 pts/0    00:00:00 /usr/bin/rsync --archive
--delete --delete-excluded --relative --sparse --files-from=-
--rsh=/usr/bin/ssh /
root@backupserver-lsmssec:/Volumes/LVstorage/lsmssec/00-Oct21_13:43
root      5943  5942 12 13:43 pts/0    00:00:00 /usr/bin/ssh -l root
backupserver-lsmssec rsync --server -logDtpRS --delete-excluded .
/Volumes/LVstorage/lsmssec/00-Oct21_13:43
```

3. To stop the backup, enter the following command:

   ```
   # kill <jobnumber1> <jobnumber2> ...
   ```

   where `<jobnumber1>` is the PID of the first process to stop and `<jobnumber2>` is the PID of the second process to stop. Enter a job number for each line that displays in step 2 on page 92. For the example output in step 2 on page 92, enter the following command:

   ```
   kill 5673 5759 5942 5943
   ```

4. Verify that all relevant processes have been stopped by entering the following command and ensuring that no output appears:

   ```
   # ps -ef | egrep "rsync|netbackup|lsmsbkp" | grep -v grep
   ```

   If no output appears, the backup has been stopped.

5. Clean up any remaining lock files by entering the following command:

   ```
   # rm -f /TOC
   ```

6. Repeat steps 1 through 5 on the standby server to stop that server's backup.
7. To clear up any lingering lock files on the NAS, enter the following command on either server:

   ```
   # ssh backupserver /etc/rc3.d/S99TKLCclearlocks start
   ```

   When the OK in the following output displays, all lock files on the NAS have been cleared.

   ```
   Clearing backup locks:[  OK  ]
   ```

You have now completed this procedure.

Checking for Running Backups

Both database backups and query server snapshots use the same file space on the LSMS. If a backup is in process and a query server snapshot or another backup is started, the first backup process will terminate prematurely, and the next backup will take significantly longer to complete. Therefore, it is very important that you perform the following procedure to check for a running backup before starting a manual backup or creating a query server snapshot.

In addition, the following tasks all use temporary file space on the LSMS. If you attempt to run these processes simultaneously, you may run out of disk space. Since backups can be run automatically, it is recommended that you perform the following procedure before attempting any of these tasks to ensure that no database backups are running:

- Starting a standby node (changing its state from UNINITIALIZED "INHIBITED" to STANDBY)
- Running the `import` command
- Running the `lsmsdb quickaudit` command.

1. Log in as the `lsmsadm` or `lsmsall` user to the active server (for information about logging in, see *Logging In to LSMS Server Command Line* on page 45).
2. Enter the following command to determine whether any database backups are running:

   ```
   $ ps -ef | grep netbackup
   ```

   - If output similar to the following displays (only `grep netbackup` displays after `00:00:00`), no backup is running, and you may continue with the procedure you were performing:

     ```
     lsmsadm   6826  6312  0 16:58 pts/12   00:00:00 grep netbackup
     ```

   - If output similar to the following displays (with one or more processes after `00:00:00`), a backup is running. DO NOT proceed with the procedure that you are performing. (This output displays all on one line although it does not fit on one line in this manual.)

     ```
     lsmsadm 25742 25596  0 11:20 ?        00:00:00 /usr/bin/perl -T
     /usr/TKLC/plat/bin/netbackup --config=/usr/TKLC/plat/etc/BackupTK/lsmsdb.xml
     ```


     CAUTION: While a backup is in progress, do not attempt to start a standby node (change its state from UNINITIALIZED "INHIBITED" to STANDBY), run the `import` command, run the `lsmsdb quickaudit` command, create a query server snapshot, or start another backup. All of these tasks use temporary file space. If you attempt to start one of these processes, you may run out of disk space.

   Before restarting or attempting to proceed with the procedure you were performing, run the command in this step again.

You have now completed this procedure.

Performing Routine Cleaning

Use the procedures in this section to prevent dust buildups and to clean CD-ROM disks.

Preventing Dust Buildups

Perform quarterly the following procedure to prevent dust buildup in and around the frames. Collection of dust within the server can allow electrostatic charges to build up around circuit cards, possibly damaging cards installed in the system.

CAUTION: Do not use a vacuum cleaner for dust removal, since dust in motion can generate static electricity. For the same reason, do not use compressed air to remove dust.

You will need a damp, lint-free cloth for this procedure.

Procedure

1. Open the doors on the front of the frames. Using a damp cloth, wipe the dust from the doors and from the front of the card cages.
2. Using the same cloth, wipe the dust from the air intakes and around the exterior of the system frames.
3. Change the fan filters (for instructions, refer to the *T1100 Hardware Manual*).

You have now completed this procedure.

Cleaning CD-ROM Disks

This procedure explains how to clean CD-ROM disks. If your CD-ROM drive cannot read a compact disk, the cause could be a dirty disk.

You will need a clean, soft, lint-free dry cloth to complete this procedure.

CAUTION: Do not use solvents like benzine, paint thinner, antistatic aerosol spray or abrasive cleaners to clean compact disks.

Wipe the nonlabeled side of the disk with a clean, soft, lint-free dry cloth radially from the center to the outside.

You have now completed this procedure.

Additional Tools for Monitoring the LSMS Hardware and the Network

LSMS provides various tools that you can use to monitor the LSMS hardware and the network. Monitoring can help you prevent and diagnose errors.

Use the system monitoring features regularly, especially during times of peak load, to verify that the system has adequate resources. This practice provides an insight into system resource utilization and provides early warning if the system capacity limits are being approached.

Verifying Active Server Network Interfaces and NPAC Connections

Use one or more of the following methods to verify network connectivity:

- The `ifconfig` command
- The `traceroute` utility to verify network connectivity and routing between hosts
- The LSMS graphical user interface (GUI) to determine connectivity to NPACs

Using the `ifconfig` Command

Use the `ifconfig -a` command on the target host to verify that the eth11, eth31, and eth32 ports are in the UP state.

1. Log in as `root` on the active server.
2. Enter the following command to test the interfaces:

   ```
   # ifconfig -a
   ```

   Verify the output. The successful completion is indicated by the word UP in the output, which is highlighted in **bold** in the following example. A failure is indicated by the absence of the word UP in the output.

```
bond0     Link encap:Ethernet  HWaddr 00:00:00:00:00:00
          BROADCAST MASTER MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
bond0.2   Link encap:Ethernet  HWaddr 00:04:23:B6:7B:F2
          inet addr:192.168.2.1  Bcast:192.168.2.255  Mask:255.255.255.0
          BROADCAST MASTER MULTICAST  MTU:1500  Metric:1
          RX packets:28394 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28417 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1675798 (1.5 Mb)  TX bytes:1828380 (1.7 Mb)
eth11     Link encap:Ethernet  HWaddr 00:04:23:B6:7B:F3
          inet addr:192.168.60.10  Bcast:192.168.60.255
Mask:255.255.255.0
           UP
 BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4512637 errors:0 dropped:0 overruns:0 frame:0
          TX packets:347651 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:595985264 (568.3 Mb)  TX bytes:44627212 (42.5 Mb)
          Base address:0xac00 Memory:fe6e0000-fe700000
eth12     Link encap:Ethernet  HWaddr 00:04:23:B6:7B:F2
          inet addr:192.168.1.1  Bcast:192.168.1.255
Mask:255.255.255.0
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:79899 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72870 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29323089 (27.9 Mb)  TX bytes:7250646 (6.9 Mb)
          Base address:0xa800 Memory:fe6c0000-fe6e0000
eth31     Link encap:Ethernet  HWaddr 00:04:23:B6:6B:EF
          inet addr:192.168.61.10  Bcast:192.168.61.255
Mask:255.255.255.0
           UP
 BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6716535 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29490 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:430086939 (410.1 Mb)  TX bytes:6260031 (5.9 Mb)
          Base address:0x9800 Memory:fe3c0000-fe3e0000
eth32     Link encap:Ethernet  HWaddr 00:04:23:B6:6B:EE
          inet addr:192.168.59.15  Bcast:192.168.59.255
Mask:255.255.255.0
           UP
 BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:52926081 errors:0 dropped:0 overruns:0 frame:0
```

```
          TX packets:21076677 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:259902695 (247.8 Mb)  TX bytes:2838249902 (2706.7 Mb)
          Base address:0x9400 Memory:fe320000-fe340000
eth32:0   Link encap:Ethernet  HWaddr 00:04:23:B6:6B:EE
          inet addr:192.168.59.14  Bcast:192.168.59.255
Mask:255.255.255.0
           UP
 BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28394 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28417 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1675798 (1.5 Mb)  TX bytes:1828380 (1.7 Mb)
          Base address:0x9400 Memory:fe320000-fe340000
eth91     Link encap:Ethernet  HWaddr 00:00:17:0C:6A:86
          inet addr:192.168.1.1  Bcast:192.168.1.255
Mask:255.255.255.0
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Base address:0xc800 Memory:fe9c0000-fe9e0000
eth92     Link encap:Ethernet  HWaddr 00:00:17:0C:6A:87
          inet addr:192.168.3.1  Bcast:192.168.3.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5184694 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3082476 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2546446730 (2428.4 Mb)  TX bytes:623843356 (594.9 Mb)
          Base address:0xcc00 Memory:fe9e0000-fea00000
eth93     Link encap:Ethernet  HWaddr 00:00:17:0C:6A:84
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Base address:0xb800 Memory:fe8c0000-fe8e0000
eth94     Link encap:Ethernet  HWaddr 00:00:17:0C:6A:85
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Base address:0xbc00 Memory:fe8e0000-fe900000
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:93844642 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93844642 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1705668622 (1626.6 Mb)  TX bytes:1705668622 (1626.6 Mb)
```

You have now completed this procedure.

Using the `traceroute` Utility

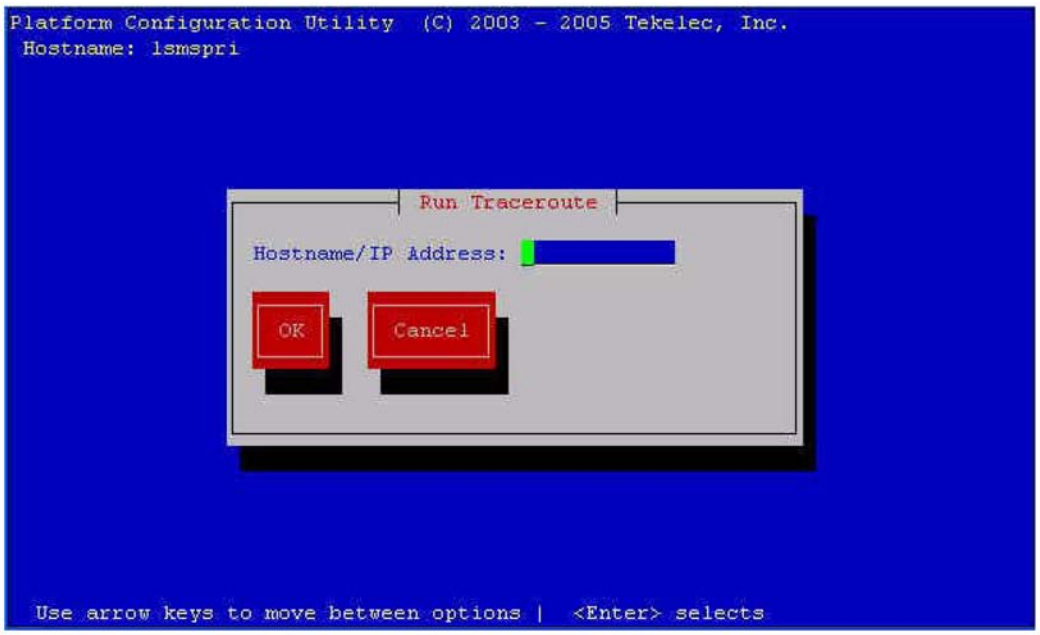
The `traceroute` utility determines the path between the host where the utility is run and the remote host named by the utility's input parameter. The utility also reports the latency of each hop along the route.

Note: If the network between the hosts contains firewalls, this utility may fail unless the firewalls are properly set up. Setting up firewalls is the responsibility of the customer.

Use the following procedure to run the `traceroute` utility:

1. Log in as the `lsmsmgr` user on the server from which you want to test the route. (For information, see *Logging In to LSMS Server Command Line* on page 45.)
2. From the `lsmsmgr` interface, select **Diagnostics ➤ Network Diagnostics ➤ Traceroute**.

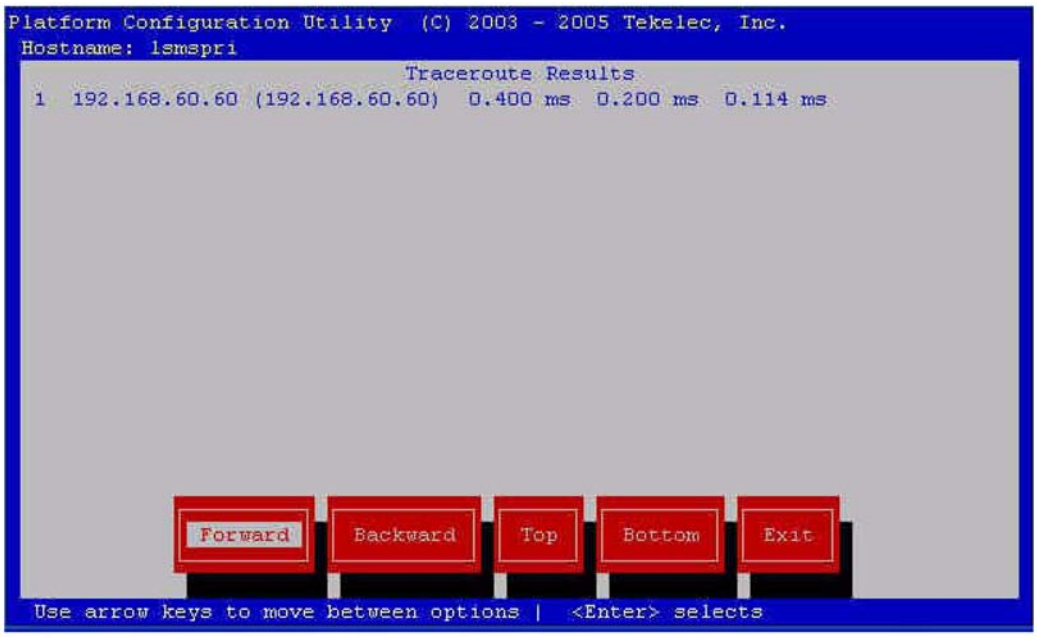
   Figure 66: TraceRoute



3. Ensure the cursor is placed in the Hostname/IP Address field, and type the IP address of the system to which you wish to trace the route, then use the down arrow key to highlight the **OK** button, and press **Enter**.

   The results display in a window similar to the following.

   Figure 67: TraceRoute Results



4. The output depends on how many hops exist between the server you logged into and the IP address you entered.

   To interpret output similar to the following example, see *Table 11: Interpreting traceroute Output* on page 99.

```
traceroute to 198.89.34.19 (198.89.34.19), 30 hops max, 40 byte packets
 1  192.168.51.250 (192.168.51.250)  2 ms  2 ms  2 ms
 2  198.89.39.250 (198.89.39.250)  3 ms  4 ms  1 ms
 3  198.89.34.19 (198.89.34.19)  5 ms *  4 ms
```

Table 11: Interpreting `traceroute` Output

Line Number	Meaning
1	Indicates the IP address of the interface from which the `traceroute` packets left the originating host
2	Indicates the IP address of the router that routed the `traceroute` packets
3	Indicates the IP address of the remote host. The * shown in this line indicates that there was packet loss connecting to this computer.

You have now completed this procedure.

Managing Automatic File Transfers

The LSMS generates many logs, measurements, and data files on a regular basis. These files are maintained on the LSMS for seven days. Customers can use the data in these files for traffic pattern analysis, identification of various network events, and investigation of problems.

The optional Automatic File Transfer feature enables customers to set up an automatic method of transferring selected files to specified remote sites at a specified frequency. Using this feature can reduce costs and also the chance of user error that could result in missed transfers of required data.

Whenever an error occurs during an automatic file transfer, an entry is made in the file `aft.log.<MMDD>` in the directory `/var/TKLC/lsms/logs/aft` (where `<MMDD>` is the month and day when the error occurred).

Use the `autoxfercfg` command, as described in the following subsections, to set up and manage automatic file transfers. To initially set up an automatic transfer of files, perform in the order shown below, the procedures in the following sections:

1. *Adding a New Remote Location for Automatic File Transfers* on page 101
2. *Scheduling an Automatic File Transfer* on page 104

In addition, you can use the `autoxfercfg` command to perform the following functions:

- *Displaying Remote Locations Used for Automatic File Transfers* on page 100
- *Deleting a Remote Location for Automatic File Transfers* on page 102
- *Displaying Previously Scheduled Automatic File Transfers* on page 103
- *Removing a Scheduled Automatic File Transfer* on page 105

Displaying Remote Locations Used for Automatic File Transfers

To display all remote locations that have been previously added using this feature, perform the following procedure.

1. Log in to the active server as `lsmsadm`.
2. Enter the following command (for more information about the format of this command, see *autoxfercfg* on page 166):

   ```
   $ $LSMS_DIR/autoxfercfg
   ```

3. The following output displays:

```
Tekelec Automatic File Transfer Configuration Utility v1.0
Copyright 2000, Tekelec
Select one of the following menu options:
1) Display valid remote locations
2) Add new remote location
3) Remove remote location
4) Display all scheduled transfers
5) Add new scheduled transfer
6) Remove scheduled transfer
7) Exit
```

4. Enter `1`.

   Output similar to the following displays:

```
Valid remote machine names:
1. lnp3
2. ftp.lnp25
<hit any key to continue>
```

5. After you have pressed any key, the output displayed in step 3 is displayed again.

   If you desire to perform other functions, enter a number and follow the procedure described in one of the other sections that describe this feature. For a list of the sections, *Managing Automatic File Transfers* on page 100.

6. If you do not need to perform any other function, type `7`.

You have now completed this procedure.

Adding a New Remote Location for Automatic File Transfers

To add a new remote location for files to be automatically transferred to, perform the following procedure.

1. Log in to the active server as `lsmsadm`.
2. Enter the following command (for more information about the format of this command, see *autoxfercfg* on page 166):

   ```
   $ $LSMS_DIR/autoxfercfg
   ```

3. The following output displays:

```
Tekelec Automatic File Transfer Configuration Utility v1.0
Copyright 2000, Tekelec
Select one of the following menu options:
1) Display valid remote locations
2) Add new remote location
3) Remove remote location
4) Display all scheduled transfers
5) Add new scheduled transfer
6) Remove scheduled transfer
7) Exit
```

4. Enter `2`.

   Output similar to the following displays:

```
Enter remote machine name:
Enter user name:
Enter password: ............
Verify password: ............
```

5. Type the desired values in all four fields, and then press **Return**.

   For example, type the following values shown in **bold** and press Return. (The passwords do not display as you type them; they are shown here to demonstrate that you must enter the same value twice.)

```
Enter remote machine name:  ftp.tekelec.com
Enter user name:  anonymous
```

```
Enter password:  xy1524wp
Verify password:  xy1524wp
```

The following output displays:

```
Site configured. ** Make sure the host is reachable from this system **
<hit any key to continue>
```

6. After you have pressed any key, the output displayed in step 3 is displayed again.

   If you desire to perform other functions, enter a number and follow the procedure described in one of the other sections that describe this feature. For a list of the sections, *Managing Automatic File Transfers* on page 100.

7. If you do not need to perform any other function, type 7.

You have now completed this procedure.

Deleting a Remote Location for Automatic File Transfers

To delete a remote locations that has been previously added using this feature, perform the following procedure.

1. Log in to the active server as `lsmsadm`.
2. Enter the following command (for more information about the format of this command, see *autoxfercfg* on page 166):

   ```
   $ $LSMS_DIR/autoxfercfg
   ```

   The following output displays:

   ```
   Tekelec Automatic File Transfer Configuration Utility v1.0
   Copyright 2000, Tekelec
   Select one of the following menu options:
   1) Display valid remote locations
   2) Add new remote location
   3) Remove remote location
   4) Display all scheduled transfers
   5) Add new scheduled transfer
   6) Remove scheduled transfer
   7) Exit
   ```

3. Enter 3.

   Output similar to the following displays:

   ```
   Enter remote machine name:
   ```

4. Type the name of the location you wish to delete and press **Return**.

   For example:

   ```
   Enter remote machine name:  ftp.tekelec.com
   ```

   The following output displays:

   ```
   Verify: remove ftp.tekelec.com (y/n)?
   ```

5. Enter y to verify that the site shown is the remote site you wish to delete.

The following output displays:

```
Site removed.
<hit any key to continue>
```

6. After you have pressed any key, the output displayed in step 3 is displayed again.

   If you desire to perform other functions, enter a number and follow the procedure described in one of the other sections that describe this feature. For a list of the sections, *Managing Automatic File Transfers* on page 100.

7. If you do not need to perform any other function, type 7.

You have now completed this procedure.

Displaying Previously Scheduled Automatic File Transfers

To display all automatic transfers that have been previously set up using this feature, perform the following procedure.

Note: Any file transfers that have been set up to be performed one time only are not displayed.

1. Log in to the active server as `lsmsadm`.
2. Enter the following command (for more information about the format of this command, see *autoxfercfg* on page 166):

   ```
   $ $LSMS_DIR/autoxfercfg
   ```

   The following output displays:

   ```
   Tekelec Automatic File Transfer Configuration Utility v1.0
   Copyright 2000, Tekelec
   Select one of the following menu options:
   1) Display valid remote locations
   2) Add new remote location
   3) Remove remote location
   4) Display all scheduled transfers
   5) Add new scheduled transfer
   6) Remove scheduled transfer
   7) Exit
   ```

3. Enter 4.

   Output similar to the following displays:

   ```
   Scheduled transfers:
     # SMTWHFS HHMM Filespec                                    Remote
   001  *      0200 /var/TKLC/lsms/logs/Midwest/Lsms
   *         ftp.lnp25:/tmp
   002 ******* 0230 /var/TKLC/lsms/logs/survlog.log           lnp3:/common/logs
   <hit any key to continue>
   ```

   This display shows that all files with filenames that start with `Lsms` in the directory /var/TKLC/lsms/logs/Midwest are transferred to `ftp.lnp25:/tmp` at 2 a.m. every Monday, and that the file `survlog.log` in the /var/TKLC/lsms/logs directory is transferred to `lnp3:/common/logs` every night at 2:30 a.m.

4. After you have pressed any key, the output displayed in step 3 is displayed again.

If you desire to perform other functions, enter a number and follow the procedure described in one of the other sections that describe this feature. For a list of the sections, *Managing Automatic File Transfers* on page 100.

5. If you do not need to perform any other function, type 7.

You have now completed this procedure.

Scheduling an Automatic File Transfer

To set up files to be transferred automatically, perform the following procedure. It is recommended that you schedule transfers according to the following guidelines:

- Choose an off-peak time, such as very early in the morning.
- Avoid planning transfers that would result in the same file being transferred more than once. For example, because LSMS application logs are maintained on the LSMS for seven days, they only need to be scheduled for a weekly transfer. If you schedule a daily transfer for logs of that type, the same file will be transferred each day for seven days. For this reason the display described in *Displaying Previously Scheduled Automatic File Transfers* on page 103 shows that the files with filenames that start with `Lsms` in the `/var/TKLC/lsms/logs/Midwest` directory are transferred only on Mondays.

Transferring large numbers of files does not impact the processing performance of the LSMS, but it can impact network performance, especially networks that use the single-subnet design. (For more information about network design, refer to the LSMS *Configuration Manual*.) This feature is designed for insignificant network degradation for up to 10 configured remote locations with up to 600 transferred files.

1. Log in to the active server as `lsmsadm`.
2. Enter the following command (for more information about the format of this command, see *autoxfercfg* on page 166):

   ```
   $LSMS_DIR/autoxfercfg
   ```

   The following output displays:

   ```
   Tekelec Automatic File Transfer Configuration Utility v1.0
   Copyright 2000, Tekelec
   Select one of the following menu options:
   1) Display valid remote locations
   2) Add new remote location
   3) Remove remote location
   4) Display all scheduled transfers
   5) Add new scheduled transfer
   6) Remove scheduled transfer
   7) Exit
   ```

3. Enter 5.

   Output similar to the following displays:

   ```
   Enter filespec:
   Enter remote machine name:
   Enter remote directory:
   Enter FTP port [21]:
   Enter transfer time (HHMM):
   Run (O)nce, (D)aily, (W)eekly:
   Enter day of the week: (SU,MO,TU,WE,TH,FR,SA):
   ```

4. Type the desired values in all four fields, and then press Return.

   For the time, use the twenty-four hour notation, where 11 p.m is represented as `2300`. To specify multiple files, you can use a wildcard character (*) in file names. For example, to set up a weekly transfer of the file `haEvents.err` in the `/var/TKLC/lsms/logs` directory every Tuesday morning at 1:30 a.m, type the following values, as shown in **bold**, and press Return:

```
Enter filespec:  /var/TKLC/lsms/logs/haEvents.err
Enter remote machine name:  lnp3
Enter remote directory:  /common/logs
Enter FTP port [21]:  80
Enter transfer time (HHMM):  0130
Run (O)nce, (D)aily, (W)eekly:  W
Enter day of the week: (SU,MO,TU,WE,TH,FR,SA):  TU
```

   Output similar to the following displays to verify your input. If the display agrees with your input, type **y**, as shown in **bold**, and press Return:

```
SMTWHFS HHMM Filespec                                    Remote
  *     0230 /var/TKLC/lsms/logs/haEvents.err       lnp3:/common/logs
Is this correct (y/n)?  y
```

   The following output displays:

```
Automatic transfer successfully scheduled.
<hit any key to continue>
```

5. After you have pressed any key, the output displayed in step 3 is displayed again.

   If you desire to perform other functions, enter a number and follow the procedure described in one of the other sections that describe this feature. For a list of the sections, *Managing Automatic File Transfers* on page 100.

6. If you do not need to perform any other function, type 7.

You have now completed this procedure.

Removing a Scheduled Automatic File Transfer

To remove an automatic transfer that has been previously set up using this feature, perform the following procedure.

Note: Any file transfers that have been set up to be performed one time only cannot be removed.

1. Log in to the active server as `lsmsadm`.
2. Enter the following command (for more information about the format of this command, see *autoxfercfg* on page 166):

   `$LSMS_DIR/autoxfercfg`

   The following output displays:

```
Tekelec Automatic File Transfer Configuration Utility v1.0
Copyright 2000, Tekelec
Select one of the following menu options:
1) Display valid remote locations
2) Add new remote location
3) Remove remote location
4) Display all scheduled transfers
```

```
5) Add new scheduled transfer
6) Remove scheduled transfer
7) Exit
```

3. Enter `6`.

   Output similar to the following displays to show all currently scheduled transfers. Enter the number of the transfer that you want to remove (in this example, the first transfer is to be removed. as shown by `1`, in **bold**), or enter `0` to quit:

```
Scheduled transfers:
  # SMTWHFS HHMM Filespec                                  Remote
001  *      0200 /var/TKLC/lsms
/
logs/Midwest/Lsms*     ftp.lnp25:/tmp
002 ******* 0230 /var/TKLC/lsms/logs/survlog.log        lnp3:/common/logs
Remove transfer # (0-3, 0=quit):  1
```

4. The following output displays.

```
Scheduled transfer successfully removed.
<hit any key to continue>
```

5. After you have pressed any key, the output displayed in step 3 is displayed again.

   If you desire to perform other functions, enter a number and follow the procedure described in one of the other sections that describe this feature. For a list of the sections, *Managing Automatic File Transfers* on page 100.

6. If you do not need to perform any other function, type `7`.

You have now completed this procedure.

Chapter 5

Restarting Software Processes

Topics:

- *Introduction Page 108*
- *Automatically Restarting Software Processes Page 108*

This chapter describes how the LSMS automatically attempts to restart certain types of failures. It also describes how to manually verify and restart LSMS software components.

Introduction

This chapter describes how the LSMS automatically attempts to restart certain types of failures. It also describes how to manually verify and restart LSMS software components.

Automatically Restarting Software Processes

The LSMS Automatic Software Recovery feature, available as a standard feature for LSMS Release 2.0 and later, detects failures in certain LSMS processes and attempts to restart the processes without the need for manual intervention by the customer. This feature is implemented by the `sentryd` utility.

Detecting Failure Conditions

Table 12: Processes Monitored by the Automatic Software Recovery Feature on page 108 shows which processes are checked by `sentryd` and the error conditions for which they are checked.

Table 12: Processes Monitored by the Automatic Software Recovery Feature

Process	Unintentional Exit	Inability to Perform Defined Tasks	Failed to Initialize During Startup	See section:
Eagle agents	X	X	X	*Automatically Monitoring and Restarting Eagle Agent Processes* on page 111
Regional NPAC agents	X	X	X	*Automatically Monitoring and Restarting NPAC Agent Processes* on page 112
OSI	X			*Automatically Monitoring and Restarting OSI Process* on page 112
Service Assurance	X			*Automatically Monitoring and Restarting the Service Assurance Process* on page 113

Process	Unintentional Exit	Inability to Perform Defined Tasks	Failed to Initialize During Startup	See section:
Local Services Manager	X	X	X	*Automatically Monitoring and Restarting Other Processes* on page 115
Local Data Manager	X	X	X	*Automatically Monitoring and Restarting Other Processes* on page 115
Logger Server	X		X	*Automatically Monitoring and Restarting Other Processes* on page 115
Apache web server	X		X	*Automatically Monitoring and Restarting Other Processes* on page 115
RMTP Manager	X		X	*Automatically Monitoring and Restarting the rmtpmgr Process* on page 114
RMTP Agent	X		X	*Automatically Monitoring and Restarting the rmtpagent Process* on page 114
Report Manager	X		X	*Automatically Monitoring and Restarting Other Processes* on page 115

The `sentryd` process uses either of the following methods to detect failures:

- Verifying that the process has updated its timestamp in the supplemental database periodically
- Using standard Linux commands to determine whether a process is running

For more information about specific methods used to detect failures, see the section shown in the last column of *Table 12: Processes Monitored by the Automatic Software Recovery Feature* on page 108.

Reporting Failures Through the Surveillance Feature

If the Surveillance feature is not enabled, `sentryd` still detects failures and attempts to restart processes, but important information concerning the state of the LSMS is neither displayed nor logged.

To obtain the full benefit of this feature, the Surveillance feature must be enabled. The Surveillance feature displays and logs (in `/var/TKLC/lsms/logs/survlog.log`) the following notifications regarding the following conditions:

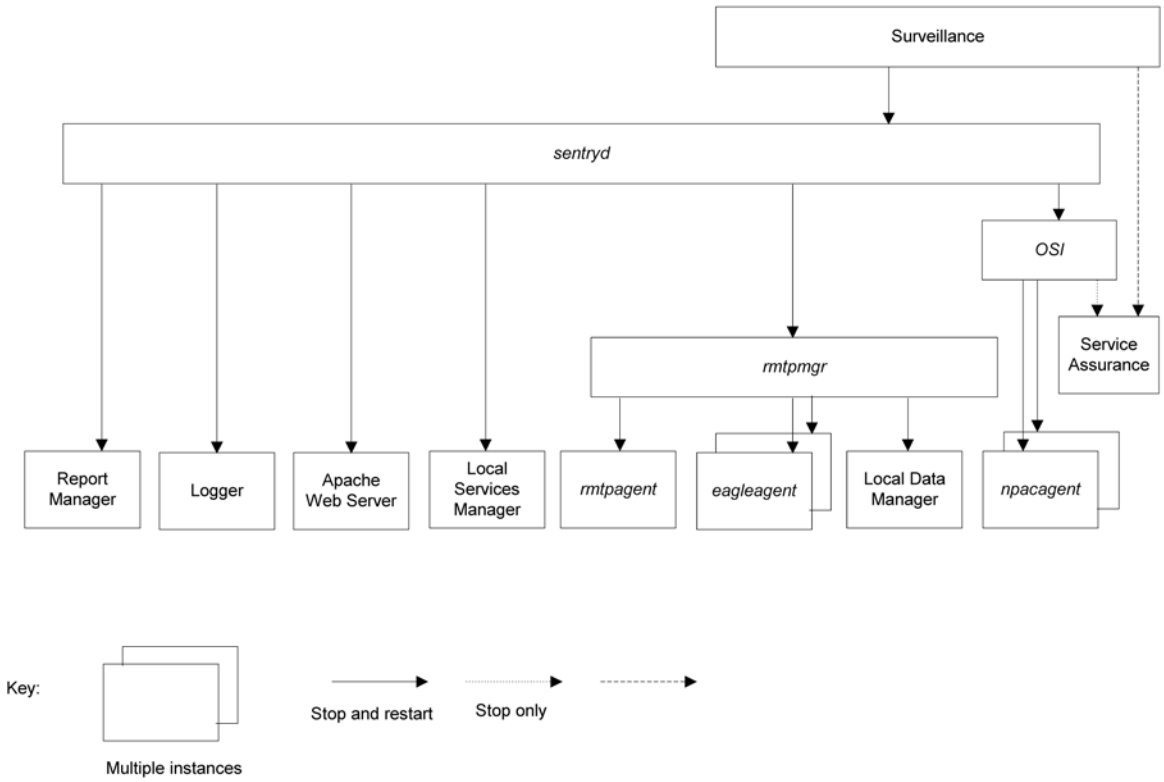
- Software failures
- Successful recovery of the software
- Unsuccessful recovery of the software

Also, whether or not the Surveillance feature is enabled, surveillance agents will restart the `sentryd` process if it exits abnormally.

Automatically Restarting Processes Hierarchically

Figure 68: Order of Automatically Restarting Processes on page 110 shows how `sentryd` restarts processes in a hierarchical order.

Figure 68: Order of Automatically Restarting Processes



This figure illustrates:

- Which processes `sentryd` monitors.

- When a failure is detected in a process, `sentryd` attempts to restart the failed process and all processes shown below it.
- The optional Service Assurance process is monitored for failure, but is not restarted by `sentryd`. Also, if `sentryd` restarts the OSI process, it stops the Service Assurance process. (The Surveillance feature restarts the Service Assurance process whenever it detects that the Service Assurance process has stopped.)

All recovery procedures start within 60 seconds of failure detection.

Automatically Monitoring and Restarting Eagle Agent Processes

The following sections describe the failure conditions for which `sentryd` monitors the Eagle agent processes (`eagleagent`) and the steps performed in attempts to restart the process after failure has been detected.

Monitoring Eagle Agent Processes

The `sentryd` process monitors each Eagle agent process for the following conditions:

- Failure to initialize during automatic system startup
- Failure to initialize during manual startup using the `eagle` command
- An abnormal exit during normal operation
- Inability to perform its defined tasks, for example, because it is in an infinite loop

Restarting an Eagle Agent Process

When one of conditions described in *Monitoring Eagle Agent Processes* on page 111 has been detected, `sentryd` performs the following tasks:

1. Generates the following surveillance notification, where represents the Common Language Location Identified (CLLI) of the EAGLE 5 ISS:

```
LSMS6004|08:40 Sep 11, 1998|xxxxxxx|Notify:Sys Admin - FAILD: eagleagent <CLLI>
```

2. Attempts to stop and restart the `eagleagent`. If the `eagleagent` restarts, `sentryd` generates the following Surveillance notification:

```
LSMS6005|08:40 Sep 11, 1998|xxxxxxx|Notify:Sys Admin - RECOV: eagleagent <CLLI>
```

Continuing Attempts to Restart an Eagle Agent Process

If the attempt to restart the `eagleagent` fails, `sentryd` attempts again.

If this attempt is also unsuccessful, the `sentryd` process generates the following Surveillance notification and continues to attempt to restart the `eagleagent` process.

```
LSMS6006|08:40 Sep 11, 1998|xxxxxxx|Notify:Sys Admin - RFAILD: eagleagent <CLLI>
```

If this notification appears several times in a row, contact the Tekelec *Customer Care Center* on page 5.

Automatically Monitoring and Restarting NPAC Agent Processes

The following sections describe the failure conditions for which `sentryd` monitors the regional NPAC agent processes (`npacagents`) and the steps performed in attempts to restart an `npacagent` process after failure has been detected.

Monitoring NPAC Agent Processes

For each region, `sentryd` monitors its `npacagent` process for the following conditions:

- Failure to initialize during automatic system startup
- Failure to initialize during manual startup using the `lsms` command
- An unintentional exit or crash during normal operation
- Inability to perform its defined tasks, for example, because it is in an infinite loop

Restarting NPAC Agent Processes

When one of conditions described in *Monitoring NPAC Agent Processes* on page 112 has been detected, `sentryd` performs the following tasks:

1. Generates the following surveillance notification:

```
LSMS6008|08:40 Sep 11, 1998|xxxxxxx| Notify:Sys Admin - FAILD:
<NPAC_region> agent
```

   where `<NPAC_region>` indicates the name of the region whose `npacagent` process has failed.

2. Attempts to stop and restart the failed `npacagent`. If the `npacagent` restarts, `sentryd` generates the following Surveillance notification:

```
LSMS6009|08:40 Sep 11, 1998|xxxxxxx| Notify:Sys Admin - RECOV:
<NPAC_region> agent
```

Continuing Attempts to Restart NPAC Agent Processes

If the attempt to restart the `npacagent` fails, `sentryd` attempts again. If this attempt is also unsuccessful, the `sentryd` process generates the following Surveillance notification and continues to attempt to restart the `npacagent` process.

```
LSMS6010|08:40 Sep 11, 1998|xxxxxxx|Notify:Sys Admin - RFAILD:
<region> agent
```

If this notification appears several times in a row, contact the Tekelec *Customer Care Center* on page 5.

Automatically Monitoring and Restarting OSI Process

The following sections describe the failure conditions for which `sentryd` monitors the OSI process and the steps performed in attempts to restart the processes after failure has been detected.

Monitoring the OSI Process

The `sentryd` process monitors the OSI process for the following conditions:

- An unintentional exit or crash during normal operation

Restarting the OSI Process

When one of conditions described in *Monitoring the OSI Process* on page 112 has been detected, `sentryd` performs the following tasks:

1. Generates the following surveillance notification:

```
LSMS8037|08:40 Sep 11, 1998|xxxxxxx|Notify:Sys Admin - FAILD: OSI
```

2. Stops all running `npacagent` processes and the Service Assurance process, if it is running.
3. Attempts to restart the OSI process and all `lsmsagent` processes that were previously running. If all processes restart, `sentryd` generates the following Surveillance notifications, where <NPAC_region> is the name of the region served by the `npacagent` process and <CLLI> is the name of the EAGLE 5 ISS:

```
LSMS8038|08:40 Sep 11, 1998|xxxxxxx|Notify:Sys Admin - RECOV: OSI
LSMS6005|08:40 Sep 11, 1998|xxxxxxx|Notify:Sys Admin - RECOV:
eagleagent <CLLI>
LSMS6009|08:40 Sep 11, 1998|xxxxxxx|Notify:Sys Admin - RECOV:
<NPAC_region> agent
```

Continuing Attempts to Restart the OSI Process

If the attempt to restart the OSI process fails, `sentryd` attempts again. After two failed attempts, `sentryd` generates the following Surveillance notification.

```
LSMS8039|08:40 Sep 11, 1998|xxxxxxx|Notify:Sys Admin - RFAILD: OSI
```

If this notification appears, contact the Tekelec *Customer Care Center* on page 5.

Automatically Monitoring and Restarting the Service Assurance Process

The following sections describe the failure conditions for which `sentryd` monitors the optional Service Assurance process (`sacw`) and states that the Surveillance feature restarts `sacw` when it fails.

Monitoring the Service Assurance Process

The `sentryd` process monitors the optional Service Assurance process (`sacw`) so that it can be stopped if the OSI process need to be restarted. It is monitored for the following conditions:

- An unintentional exit or crash during normal operation
- Inability to perform its defined tasks, for example, because it is in an infinite loop

Restarting the Service Assurance Process

The `sentryd` does not attempt to restart the Service Assurance process when it fails. The Surveillance feature performs that function. For more information about the Service Assurance process, see *Understanding the Service Assurance Feature* on page 37.

Automatically Monitoring and Restarting the rmtpmgr Process

The following sections describe the failure conditions for which sentryd monitors the RMTP Manager process (rmtpmgr) and the steps performed in attempts to restart rmtpmgr after failure has been detected.

Monitoring the rmtpmgr Process

The sentryd process monitors rmtpmgr for the following conditions:

- Failure to initialize during automatic system startup
- An unintentional exit or crash during normal operation
- Inability to perform its defined tasks, for example, because it is in an infinite loop

Restarting the rmtpmgr Process

When one of conditions described in *Monitoring the rmtpmgr Process* on page 114 has been detected, sentryd performs the following tasks:

1. Generates the following surveillance notification:

```
LSMS4021|08:40 Sep 11, 1998|xxxxxxx|Notify:Sys Admin - rmtpmgr
failed
```

2. Attempts to stop and restart the process. If the process restarts, no notification is posted. After the sentryd process has restarted the rmtpmgr process, sentryd then attempts to restart the following processes that exited previously due to the rmtpmgr failure:
   - NPAC agents (see *"Restarting NPAC Agent Processes"*)
   - Eagle agents (see *"Restarting an Eagle Agent Process"*)
   - Local Data Manager (see *"Restarting Other Processes"*)

Continuing Attempts to Restart the rmtpmgr Process

If the attempt to restart the rmtpmgr process fails, sentryd attempts again. If the attempt fails again, sentryd generates the LSMS4021 notification again. If this notification appears several times in a row, contact the Tekelec *Customer Care Center* on page 5.

Automatically Monitoring and Restarting the rmtpagent Process

The following sections describe the failure conditions for which sentryd monitors the RMTP Agent process (rmtpagent) and the steps performed in attempts to restart rmtpagent after failure has been detected.

Monitoring the rmtpagent Process

The sentryd process monitors rmtpagent for the following conditions:

- Failure to initialize during automatic system startup
- An unintentional exit or crash during normal operation

- Inability to perform its defined tasks, for example, because it is in an infinite loop

Restarting the `rmtpagent` Process

When one of conditions described in *Monitoring the rmtpagent Process* on page 114 has been detected, `sentryd` performs the following tasks:

1. Generates the following surveillance notification:

```
LSMS4021|08:40 Sep 11, 1998|xxxxxxx|Notify:Sys Admin - rmtpagent failed
```

2. Attempts to stop and restart the process. If the process restarts, no notification is posted. After the `sentryd` process has restarted the `rmtpagent` process, `sentryd` then attempts to restart the following processes that exited previously due to the `rmtpagent` failure:
   - NPAC agents (see *"Restarting NPAC Agent Processes"*)
   - Eagle agents (see *"Restarting an Eagle Agent Process"*)
   - Local Data Manager (see *"Restarting Other Processes"*)

Continuing Attempts to Restart the `rmtpagent` Process

If the attempt to restart the `rmtpagent` process fails, `sentryd` attempts again. If the attempt fails again, `sentryd` generates the `LSMS4021` notification again. If this notification appears several times in a row, contact the Tekelec *Customer Care Center* on page 5.

Automatically Monitoring and Restarting Other Processes

The following sections describe the failure conditions for which `sentryd` monitors the following processes and the steps performed in attempts to restart a process after failure has been detected:

- Local Services Manager (`lsman`)
- Local Data Manager (`supman`)
- Report Manager (`reportman`)
- Logger Server
- Apache Web Server

Monitoring Other Processes

The `sentryd` process monitors each process for the following conditions:

- Failure to initialize during automatic system startup
- An unintentional exit or crash during normal operation
- Inability to perform its defined tasks, for example, because it is in an infinite loop

Restarting Other Processes

When one of conditions described in *"Monitoring Eagle Agent Processes"* has been detected, `sentryd` performs the following tasks:

1. Generates the following surveillance notification, where `<process_name>` is the name of the process:

```
LSMS4021|08:40 Sep 11, 1998|xxxxxxx|Notify:Sys Admin - <process_name>
failed
```

2. Attempts to stop and restart the process. If the process restarts, no notification is posted.

Continuing Attempts to Restart Other Processes

If the attempt to restart the process fails, `sentryd` attempts again. If the attempt fails again, `sentryd` generates the `LSMS4021` notification again. If this notification appears several times in a row, contact the Tekelec Customer Care Center.

Chapter 6

Managing Server States

Topics:

- *Introduction Page 118*
- *Understanding Server States Page 118*
- *Understanding Switchover Page 119*
- *Understanding Automatic Switchover Page 120*
- *Managing Server States Manually Page 123*

This chapter describes the various states that servers can have, the automatic switchover capability for certain failures, and how you can manage the states of the servers manually.

Introduction

This chapter describes the various states that servers can have, the automatic switchover capability for certain failures, and how you can manage the states of the servers manually.

Understanding Server States

The LSMS has two servers for high availability. Usually, the LSMS is in *d uplex* mode, with one server the active server and the other server in a standby state. In duplex mode, the active server is the master MySQL database server, and the standby server acts as the MySQL slave. Any database changes are made on the active server and are replicated to the standby server.

If the active server is not able to run LSMS functions, the standby server can take over to be the active server. The servers are peers; either server can be the active server, but only one server can be active at a time.

When one server is in ACTIVE state and the other server is not in STANDBY state, the LSMS is in *simp lex* mode. When the LSMS is in simplex mode, the non-ACTIVE server should be brought back to STANDBY state as soon as possible (use the procedure described in *Starting a Server* on page 129).

The state of each server is monitored by the LSMS HA (High Availability) utility. *Table 13: LSMS Server States* on page 118 shows the possible states for each server (but only one server at a time can be in the ACTIVE state).

Table 13: LSMS Server States

State	Server Status
ACTIVE	Server is online, running the LSMS application, and acts as the MySQL master.
STANDBY	Server is online and participating in database replication. The server ready to become the active server if automatic switchover is necessary or if manual switchover is performed. The server is not currently running the LSMS application.
UNINITIALIZED "INHIBITED"	Server is online but it is not participating in database replication and no application is running.
Note: Other transitional states may be displayed while a server is changing from one to another of these states.	

Understanding Switchover

Changing active status from one server to another is called *switchover*. The server on which the LSMS is running at a given time is called the *active server*. If the other server is in STANDBY state, it is called the *standby* server. (If the other server is in UNINITIALIZED "INHIBITED" state, the LSMS is said to be running in simplex mode, which means that only one server is currently available to run the LSMS application, and switchover is not possible.) During switchover, the server that was in ACTIVE state changes to UNINITIALIZED "INHIBITED" state and the server that was in STANDBY state changes to ACTIVE state.

What Happens During Switchover?

During a switchover, the following functions occur:

1. The active server shuts down the LSMS application and transitions to UNINITIALIZED "INHIBITED" state.
2. The standby server stops replicating the MySQL database.
3. The standby server starts the LSMS application.

Note: After switchover the state of the previously active server is UNINITIALIZED "INHIBITED", so this server is not ready to act as a standby server. As soon as possible, perform the procedure described in *Starting a Server* on page 129 to put this server in STANDBY state.

The following items describe the results of a switchover:

- Any server-side GUIs (started using the `start_mgui` command) are terminated. This type of GUI must be restarted manually.
- All NPAC associations are terminated and then automatically restarted to connect to the newly active server (for more information, see *LSMS Connectivity* on page 11)
- All EMS associations are terminated and then automatically restarted to connect to the newly active server (for more information, see *LSMS Connectivity* on page 11)
- The VIP (Virtual IP) address is switched from the previously active server to the newly active server. In all types of network configuration, the VIP address is used for the application network, which is used by the following functions:
  - The Service Assurance feature is restarted by the Surveillance feature after the newly active server takes over.
  - After directly-connected Query Servers detect a period of inactivity, they attempt to reconnect. The reconnection is made to the newly active server.
  - Web-based GUIs (if this feature is enabled).

    Note: Although it is possible to start a web-based GUI by specifying server's specific IP address, it is recommended that web-based GUIs use the VIP address. Any web-based GUIs that do not use the VIP address will terminate during switchover.

    Switchover has the following effects on connections on the web-based GUIs that use the VIP address:

    - An alarm that switchover is being initiated is displayed
    - Any user-initiated actions, such as audits or bulk loads, are terminated
    - All web-based GUI sessions automatically reconnect themselves to the newly active server within the GUI refresh interval

- Until the GUI reconnects, no new GUI notifications will be displayed

For some types of failure on the active server, the LSMS automatically attempts to switch over. If automatic switchover is not possible, or at any time you wish, you can manually switch over to the other server. For more information about switching over, see the following:

- *Understanding Automatic Switchover* on page 120
- *Manually Switching Over from the Active Server to the Standby Server* on page 124

What Needs to Happen When Switchover Completes?

When automatic or manual switchover completes, the LSMS is operating in simplex mode, with one server in ACTIVE state and the other server in UNINITIALIZED "INHIBITED" state. Only the server in ACTIVE state is in a condition that is available for running the LSMS application.

As soon as possible, manual intervention is needed to change the state of the non-active server to STANDBY state by performing the procedure described in *Starting a Server* on page 129. When this procedure is performed on a non-active server (while the other server is in ACTIVE state), the following functions are performed:

1. The MySQL binary logs of the active server are copied to the server being started.
2. The server being started takes the MySQL slave role and begins database replication.
3. The server changes to STANDBY state; it is now available if switchover is needed again.

Understanding Automatic Switchover

The LSMS is designed with a number of redundant systems (such as power feeds and CPUs) to enable a server to continue hosting the LSMS application even after some failures. For cases of double-faults or other failure conditions for which there is no designed redundancy, the LSMS is designed to automatically switch over from the active server to the standby server. These failure conditions fall into the following categories:

- Hardware-related failures, such as loss of both power feeds, loss of redundant power feeds, loss of memory controller, and so on
- Database-related failures, such as failed mysqld process
- Network-related failures, if the user has defined certain network interfaces to be critical

Automatic Switchover Due to Hardware-Related Failure

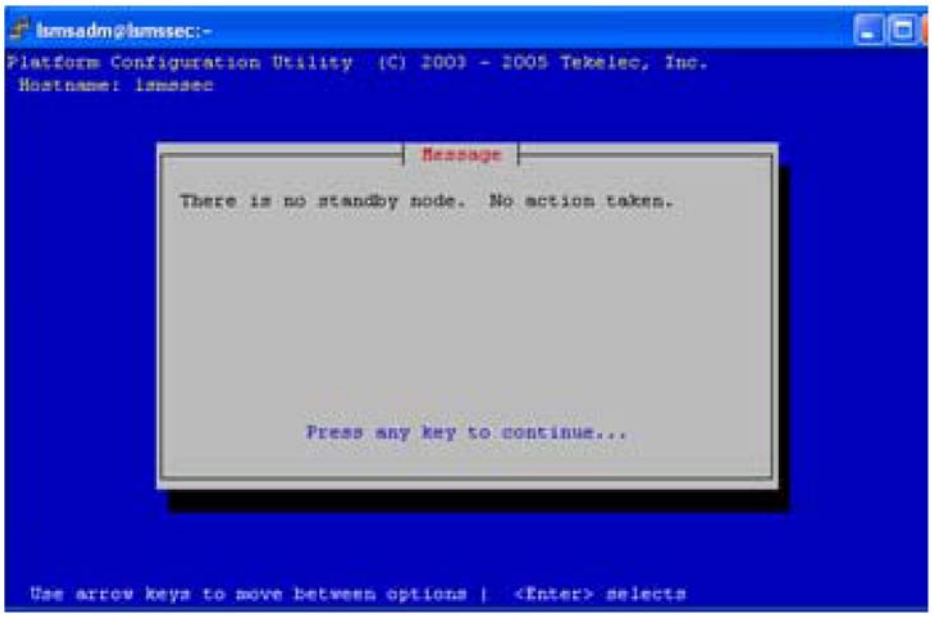
The LSMS HA daemons on the active and standby servers send each other heartbeats once every second. When a server detects a loss of 10 heartbeats in a row, the server concludes that the other server is no longer functional and does the following:

- If the active server detects the loss of 10 heartbeats in a row from the standby server, the active server disqualifies the standby server from either automatic or manual switchover and posts the following notification:

```
LSMS4015|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Heartbeat failure
```

Until the standby server returns to STANDBY state, automatic switchover is not possible, and if manual switchover is attempted, the `lsmsmgr` text interface displays a warning, as shown in *Figure 69: Unable to Switchover to Standby* on page 121.

Figure 69: Unable to Switchover to Standby



- If the standby server detects the loss of 10 heartbeats in a row from the other server, the standby server transitions to ACTIVE state. The results are the same as those described in *What Happens During Switchover?* on page 119.

```
LSMS4015|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Heartbeat failure
```

Automatic Switchover Due to Database-Related Failure

Each server monitors itself for accessibility to its database. In addition, the standby server monitors whether the replication process running and whether its replication of the active server's database is within a configured threshhold (the default is one day).

- If a server finds an error in any of these conditions, it posts the following notification:

```
LSMS4007|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - DB repl error
```

In addition, the server does the following:

- If the active server detects that its database is inaccessible, the active server switches over to the standby server and posts the following notifications:

  ```
  LSMS4000|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Switchover initiated
  ```

  If switchover is successful, the following notification is posted:

  ```
  LSMS4001|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Switchover complete
  ```

  If switchover is not successful, the following notification is posted:

  ```
  LSMS4002|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Switchover failed
  ```

- If the standby server detects that its replication process is not running, its database is inaccessible, or its database is lagging by more than the configured threshhold, the standby server transitions to UNINITIALIZED "INHIBITED" state, and posts one of the following notifications, depending on whether the standby server is Server A (the upper server in the frame, which has the default server name, `lsmspri`) or Server B (the lower server in the frame, which has the default server name, `lsmssec`):

  ```
  LSMS4013|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Primary inhibited
  ```

  ```
  LSMS4014|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Secondary inhibited
  ```

Automatic Switchover Due to Network-Related Failure

Users have the option of defining any network interfaces (NPAC, EMS, and/or Application) as critical. For each network interface that the user defines as critical, the user defines one or more IP addresses to be pinged by each server every minute. (For information about how to define a network interface as critical, refer to the LSMS *Configuration Manual*.)

When a network interface is defined as critical, each server pings the first configured IP address every minute. If the ping fails and only one IP address has been defined for that network interface, the interface is considered to have failed. If the interface has additional IP addresses defined, the interface is not considered to have failed until all IP addresses have been pinged with no response.

When a network interface is considered to have failed, the server posts one of the following notifications that corresponds to the failed interface:

```
LSMS2000|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - NPAC interface failure
```

```
LSMS0001|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - EMS interface failure
```

```
LSMS4004|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - APP interface failure
```

After the server posts the notification of interface failure, it does the following:

- If the active server detects that a critical network interface has failed, the active server determines whether any critical network interfaces are considered to have failed on the standby server:
  - If any critical network interfaces are considered to have failed on the standby server, the active server continues in the ACTIVE state; it does not switch over.

- If all critical network interfaces are responding to pings on the standby server, the active server switches over to the standby server and posts the following notifications:

  ```
  LSMS4000|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Switchover initiated
  ```

  If switchover is successful, the following notification is posted:

  ```
  LSMS4001|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Switchover complete
  ```

  If switchover is not successful, the following notification is posted:

  ```
  LSMS4002|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Switchover failed
  ```

- If the standby server detects that a critical network interface has failed, it continues to operate in STANDBY state. Although automatic switchover is not performed in this case, it is possible to manually switch over to a standby server that has detected a critical network interface has failed.

Managing Server States Manually

The following sections describe how you can manually manage the server states:

- *Determining the Server Status* on page 123
- *Manually Switching Over from the Active Server to the Standby Server* on page 124
- *Inhibiting a Standby Server* on page 127
- *Starting a Server* on page 129

Determining the Server Status

Use either of the following to determine the server status:

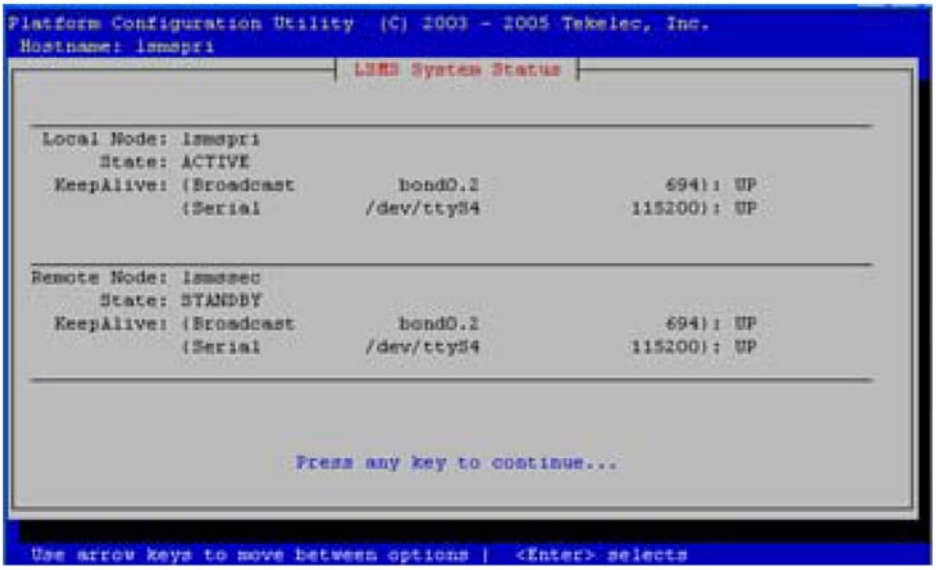
- *Using the lsmsmgr Interface to Determine the Server Status* on page 123
- *Using the hastatus Command to Determine the Server Status* on page 124

Using the `lsmsmgr` Interface to Determine the Server Status

Use the following procedure to determine the status of both servers.

1. Log into either server as the `lsmsmgr` user.
2. From the main `lsmsmgr` interface, select **Maintenance ➤ LSMS Node Status**.

   Figure 70: LSMS Node Status



In *Figure 70: LSMS Node Status* on page 123, the server that was logged into is named `lsmspri` and its state is ACTIVE; the mate server is named `lsmssec` and its state is STANDBY.

3. Press any key to return to the `lsmsmgr` Maintenance menu.

You have now completed this procedure.

Using the `hastatus` Command to Determine the Server Status

To use the command line to determine the state an individual server, perform the following procedure.

1. Log in as the `lsmsadm` or `lsmsall` user to the command line of the server whose state you want to determine.

   (For information about logging in, see *Logging In to LSMS Server Command Line* on page 45.)

2. Enter the following command:

   ```
   $ hastatus
   ```

3. The command line interface displays the status, similar to the following example, and then returns the prompt.

   ```
   ACTIVE

   $
   ```

You have now completed this procedure.

Manually Switching Over from the Active Server to the Standby Server

When there is a failure on the active server, or at other times for testing, you can use the `lsmsmgr` interface to manually switch over to the standby server, as described in the following procedure.

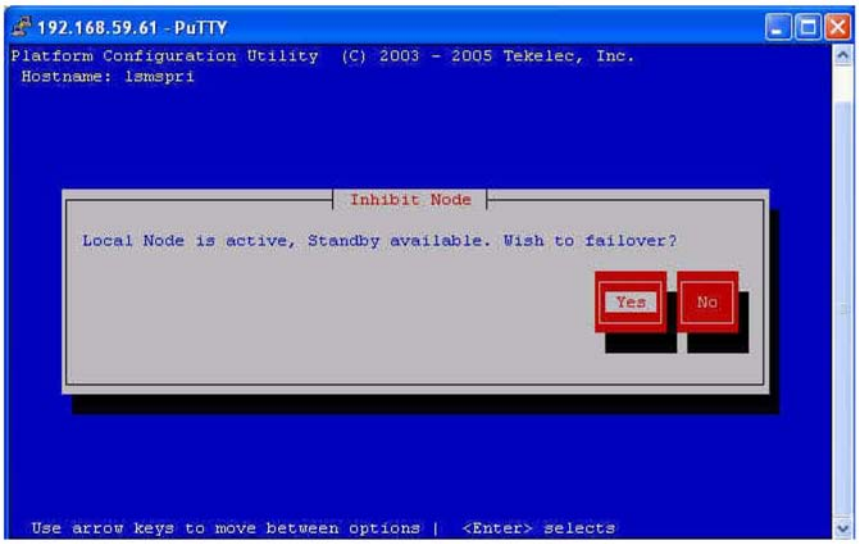
1. Log in as the `lsmsmgr` user to the active server.

   (For information about logging in as `lsmsmgr`, see *Logging In to LSMS Server Command Line* on page 45.)

2. From the main `lsmsmgr` interface, select **Maintenance ➤ Inhibit Node**.

   If the server you logged into is the ACTIVE server, the `lsmsmgr` interface displays information that confirms that the local node (the server you logged into) is active and the mate server is available as a standby (which implies that its state is STANDBY).

   Figure 71: Inhibit Active Node



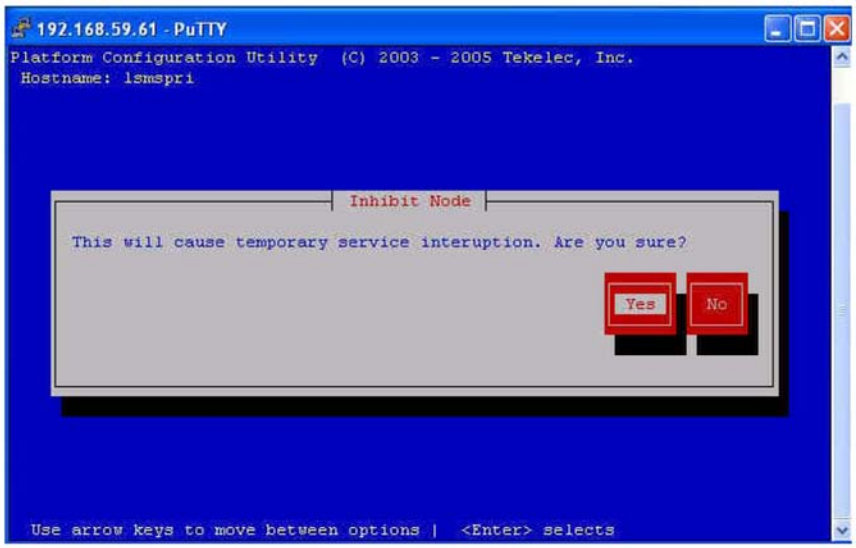
3. Ensure that the **Yes** button is highlighted and press **Enter**.

   A window, as shown in *Figure 72: Check Network Status on Standby Node* on page 125, displays, but no action is needed.

   Figure 72: Check Network Status on Standby Node

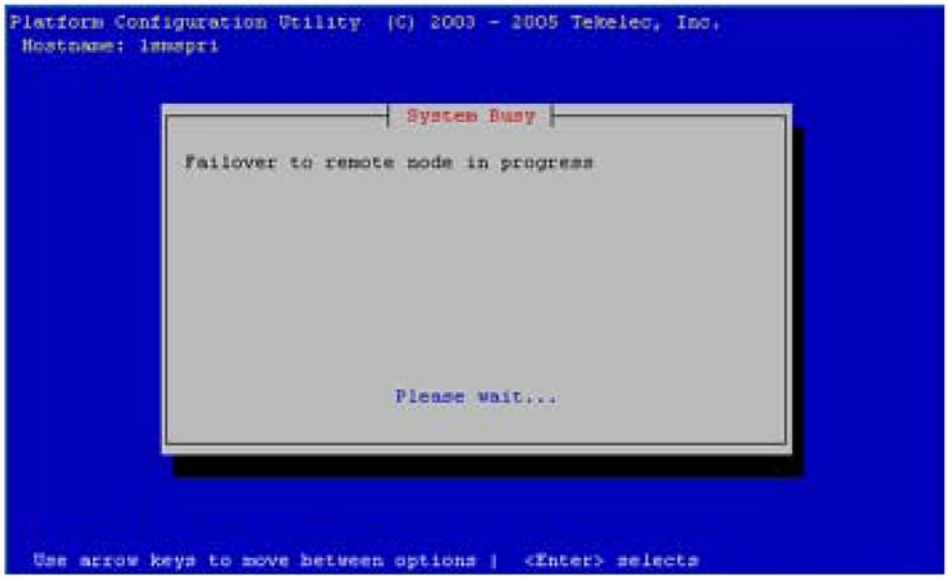
4. Next, a confirmation window displays.

   Figure 73: Confirm Switchover



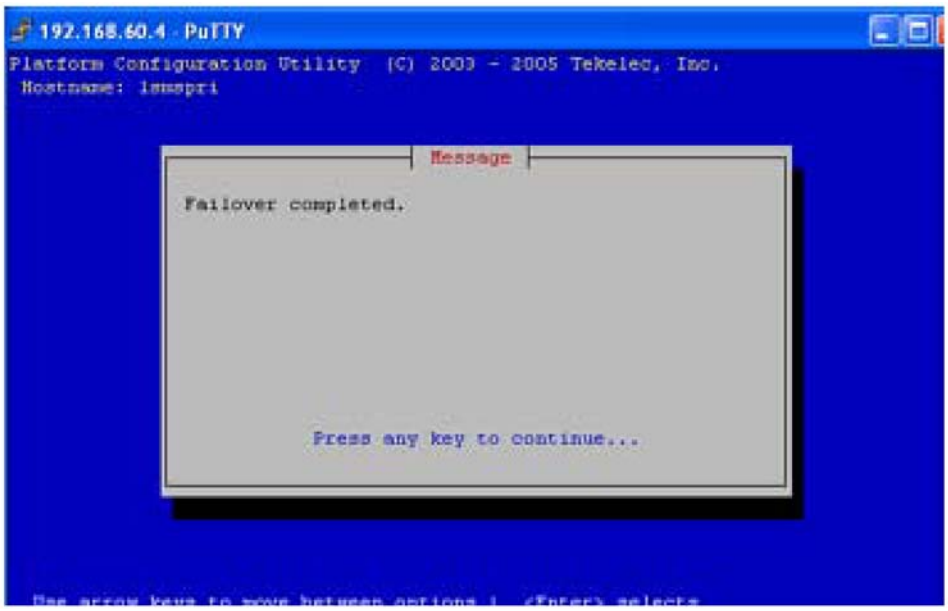
5. Ensure that the **Yes** button is highlighted and press **Enter**.
   The window shown in *Figure 75: Manual Switchover Complete* on page 126 displays.

Figure 74: Manual Switchover In Progress



6. When the switchover is complete, press any key to continue.

Figure 75: Manual Switchover Complete



You have now completed this procedure.

The server that was previously in STANDBY state is now in ACTIVE state, and the server that was previously in ACTIVE state is now in UNINITIALIZED "INHIBITED" state.

Note: As soon as possible, perform the procedure described in *Starting a Server* on page 129 to change the state of the server that is in UNINITIALIZED "INHIBITED" state to STANDBY state so that it is available if automatic switchover is needed or if manual switchover is desired.

Inhibiting a Standby Server

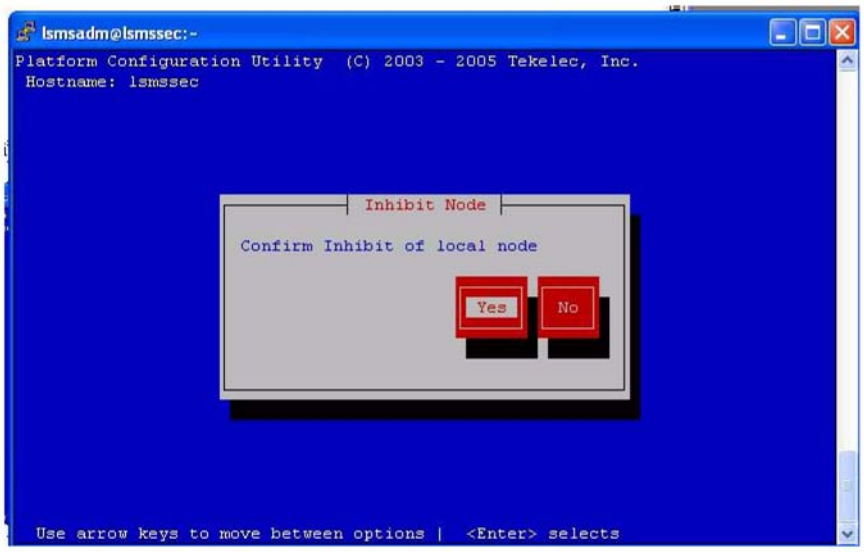
Occasionally (for example, before powering down), it may be necessary to inhibit the standby server.

Note: Inhibiting the active server results in switchover, as described in *Manually Switching Over from the Active Server to the Standby Server* on page 124.

Use the following procedure to inhibit the standby server.

1. Log in as the `lsmsmgr` user to the standby server.
   (For information about logging in as `lsmsmgr`, see *Logging In to LSMS Server Command Line* on page 45.)
2. From the main `lsmsmgr` interface, select **Maintenance ➤ Inhibit Node**.
   The `lsmsmgr` interface displays the window shown in *Figure 76: Inhibit a Non-Active Server* on page 127.

   Figure 76: Inhibit a Non-Active Server



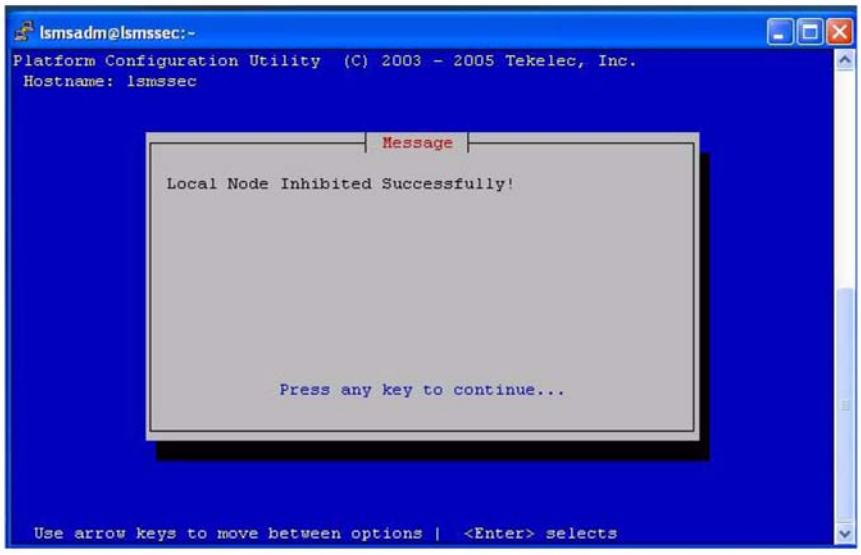
3. Ensure that the **Yes** button is highlighted and press **Enter**.

   While the server is being inhibited, the `lsmsmgr` interface disappears and the following text is displayed on the command line, where `<hostname>` is the name of the server:

   ```
   Inhibiting node <hostname>...
   ```

4. When the server has been completely inhibited, the `lsmsmgr` interface appears again. Press any key to continue.

   Figure 77: Node Successfully Inhibited



   The `lsmsmgr` main menu is displayed again.

You have now completed this procedure.

Note: Do not allow this server to remain in UNINITIALIZED "INHIBITED" state any longer than necessary. As soon as possible, perform the procedure described in perform the procedure described in *Starting a Server* on page 129 to change the state of the server to STANDBY state so that it is available if automatic switchover is needed or if manual switchover is desired.

Starting a Server

A server in UNINITIALIZED "INHIBITED" state cannot run the LSMS application and is not available as a standby server. Use the following procedure to change the state of a server from UNINITIALIZED "INHIBITED" to a state where it is available to run the LSMS application.

During the starting process on a given server, the LSMS HA utility checks to see if the other server is in ACTIVE state. Therefore, the state of the server at the end of this procedure will be one of the following:

- If the other server is not in the ACTIVE state, this server will transition to ACTIVE state.
- If the other server was in the ACTIVE state, this server will perform the following functions:
  - Copy the MySQL binary logs from the active server
  - Take a snapshot of the active server's database
  - Transition to STANDBY state
  - Configure its MySQL to be a slave to the active server's master
  - Start performing MySQL replication

1. Log in as the `lsmsmgr` user to the appropriate server, depending on the server states, as follows (for information about logging in as `lsmsmgr`, see *Logging In to LSMS Server Command Line* on page 45):
   - If both servers are in UNINITIALIZED "INHIBITED" state, log into the server that you want to make active.

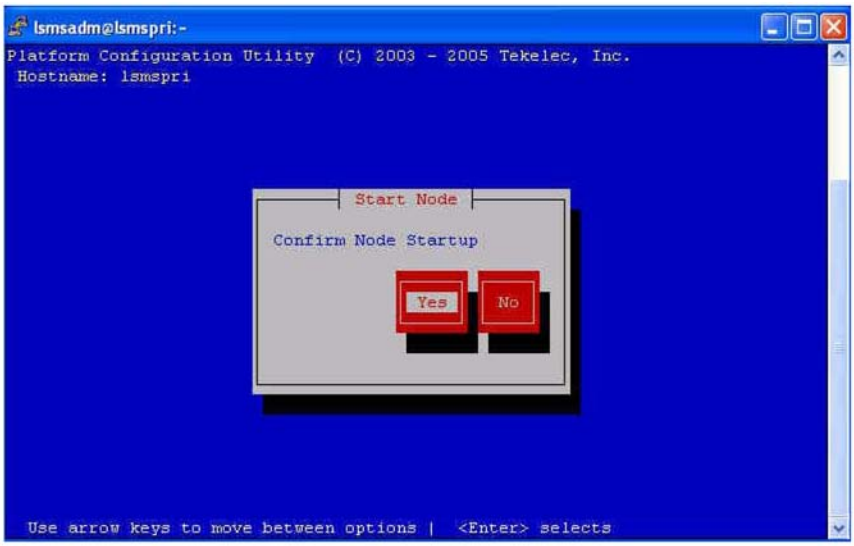
     After you have finished this procedure on that server, repeat this procedure for the other server.
   - If one server is in ACTIVE state, log into the server that is not active.

     Note: Do not attempt to change the state of the server while any of the following processes are running on the active server: backups (automatic or manual), running the `import` command, running the `lsmsdb quickaudit` command, or creating query server snapshots, all of which use temporary storage space. If you attempt to change the state of the server while any of these processes are running, you may not have enough disk space to complete the process. Since backups can be run automatically, perform the procedure described in *Checking for Running Backups* on page 93 to ensure that no backups are running.

2. From the main `lsmsmgr` interface, select **Maintenance ➤ Start Node**.

   The `lsmsmgr` interface displays.

   Figure 78: Starting a Server



3. Ensure that the **Yes** button is highlighted and press Enter.

   While the server is being started, the `lsmsmgr` interface disappears and text similar to the following is displayed on the command line when this procedure is being performed on a server (lsmssec in this example) in UNINITIALIZED "INHIBITED" state while the other server is in ACTIVE state:

```
LSMS starting up on lsmssec...
Checking status from active mate...
Running status on lsmspri node
Copying DB from active mate. Local node will become standby.
  This may take a while
LSMS shutting down lsmssec...
Syncing mate:/mnt/snap/ to /var/TKLC/lsms/db/
Sync'ed
LSMS starting up on lsmssec...
Unihibiting node lsmssec...
Startup of local node successful

Press enter to continue...
```

   Note: The text that displays is different when this procedure is being performed when both servers were originally in UNINITIALIZED "INHIBITED" state, but the condition when both servers are in UNINITIALIZED "INHIBITED" state happens only during upgrade.

4. Press any key.

   The `lsmsmgr` main menu is displayed again.

You have now completed this procedure.

The state of the server will be as described in the beginning of this section. To display the server state, use the procedure described in *Determining the Server Status* on page 123.

Chapter 7

Recovering from Site Failures

Topics:

- *Introduction Page 132*
- *Choosing a Disaster Backup Strategy Page 132*
- *Synchronizing Data Between the Main LSMS and Shadow LSMS Page 135*
- *Preparing for a Disaster Situation Page 136*
- *Determining When to Switch to Shadow LSMS Page 136*
- *Disaster Recovery Procedure Overview Page 137*
- *Performing Disaster Recovery with an Active Shadow LSMS Page 143*
- *Performing Disaster Recovery with an Inactive Shadow LSMS Page 144*
- *Performing Disaster Recovery without a Shadow LSMS Page 146*
- *Returning Operation from Shadow LSMS to Main LSMS Page 148*
- *Restoring LSMS Data from Backup Tape Page 152*
- *Resynchronizing After an Outage Between an NPAC and the LSMS Page 152*
- *Reconnecting Network Elements Page 153*

This chapter describes and compares various disaster backup strategies and describes how to prepare for disaster recovery. For each disaster recovery strategy, this chapter also describes the recovery procedures and a list of assumptions.

Introduction

The LSMS system administrator needs to plan a recovery strategy for situations when both the LSMS active and the standby server are unable to receive data from the NPAC. This occurs when the LSMS hardware is unable to operate, perhaps due to a fire or a natural disaster.

This chapter describes and compares various disaster backup strategies and describes how to prepare for disaster recovery. For each disaster recovery strategy, this chapter also describes the recovery procedures and a list of assumptions.

Choosing a Disaster Backup Strategy

Choose one of the following backup strategies, in which a shadow LSMS is defined to be an entire LSMS, with its own service provider ID, located in a separate geographical location from the main LSMS:

- Active shadow
- Inactive shadow
- No shadow

The various backup strategies provide different methods for ensuring that the shadow LSMS contains the same data as the main LSMS.

Note: Whenever you must manually enter locally provisioned data at the shadow LSMS, be sure that you use the same service provider identifier (SPID) that was used to enter the same locally provisioned data at the main LSMS. For more information, see *Synchronizing Data Between the Main LSMS and Shadow LSMS* on page 135.

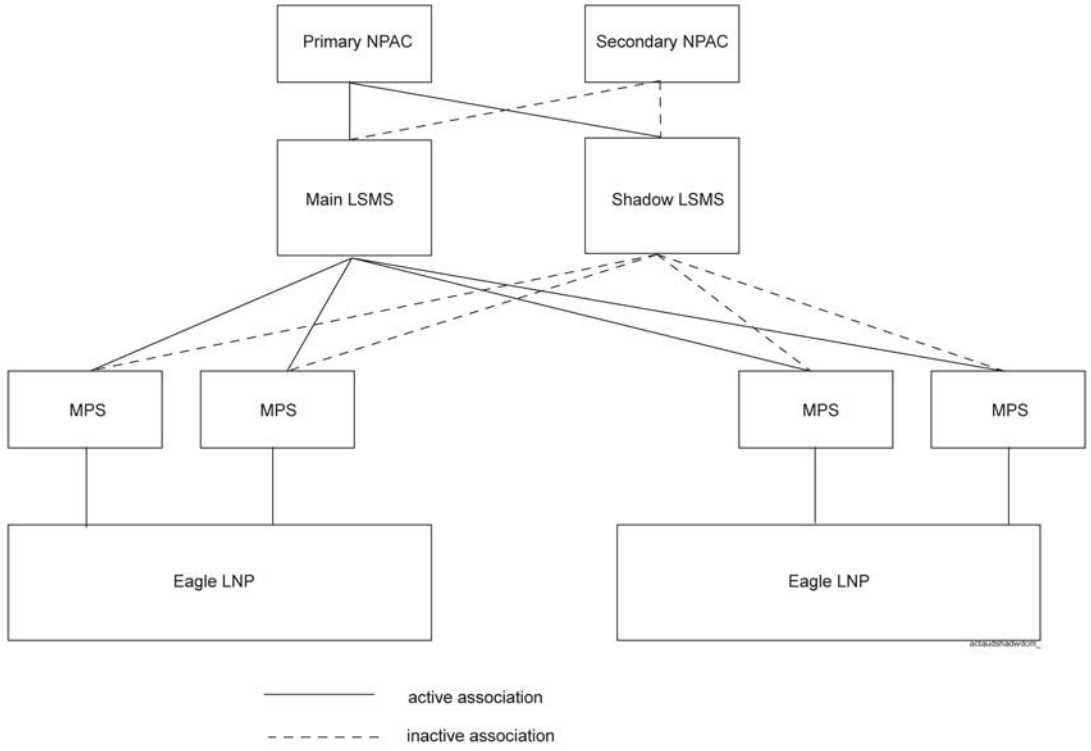
The following sections provide an overview of each strategy. Detailed descriptions or recovery procedures for each strategy are described in *Performing Disaster Recovery with an Active Shadow LSMS* on page 143 through *Returning Operation from Shadow LSMS to Main LSMS* on page 148 .

Using an Active Shadow

Figure 79: Overview of Main LSMS and Active Shadow LSMS on page 132 shows the configuration of a main LSMS that uses an active shadow as its backup.

An active shadow LSMS is an entire LSMS that is active and has active associations with each NPAC from which the LSMS needs data (only one NPAC is shown in *Figure 79: Overview of Main LSMS and Active Shadow LSMS* on page 132).

Figure 79: Overview of Main LSMS and Active Shadow LSMS



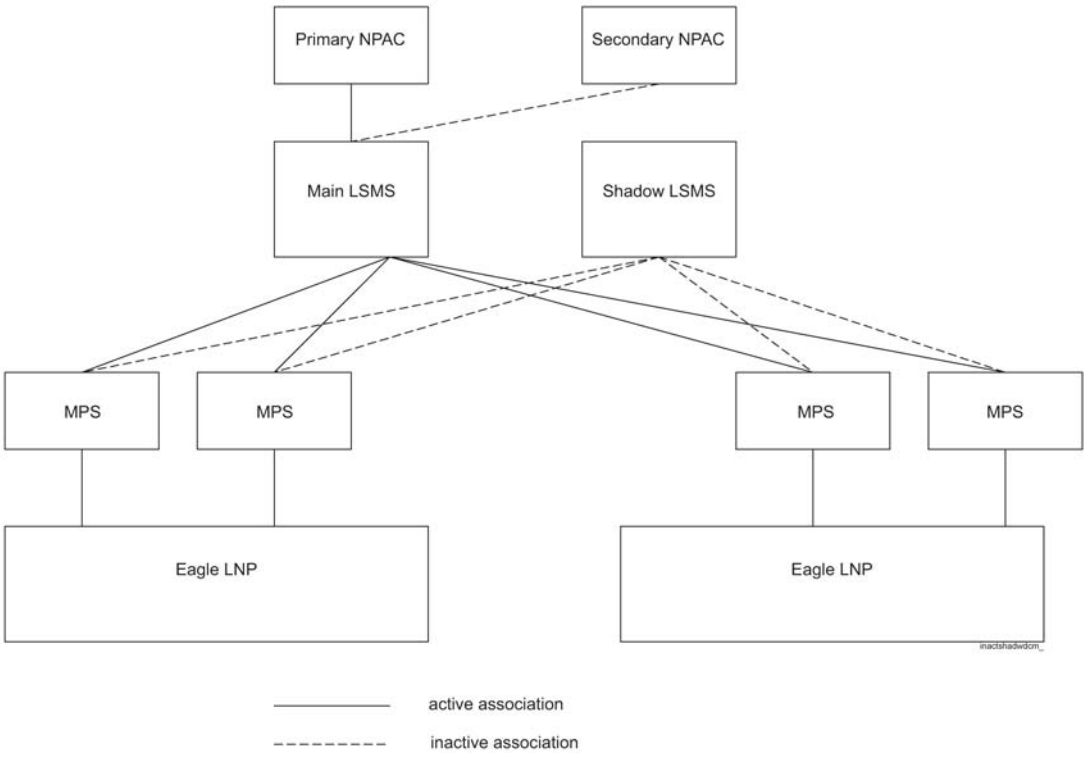
The disaster recovery backup strategy for this configuration provides the least out-of-service time for the LSMS. The recovery procedures for this strategy are described in *Performing Disaster Recovery with an Active Shadow LSMS* on page 143.

Using an Inactive Shadow

Figure 81: Overview of Main LSMS without a Shadow LSMS on page 134 shows the configuration of a main LSMS that uses an inactive shadow as its backup.

The shadow LSMS does not maintain active connections with the NPACs that supply data to the main LSMS. However, disaster recovery is still more feasible than using no shadow, especially for disaster situations in which the physical site of the main LSMS is damaged (such as fire or natural disaster).

Figure 80: Overview of Main LSMS and Inactive Shadow LSMS



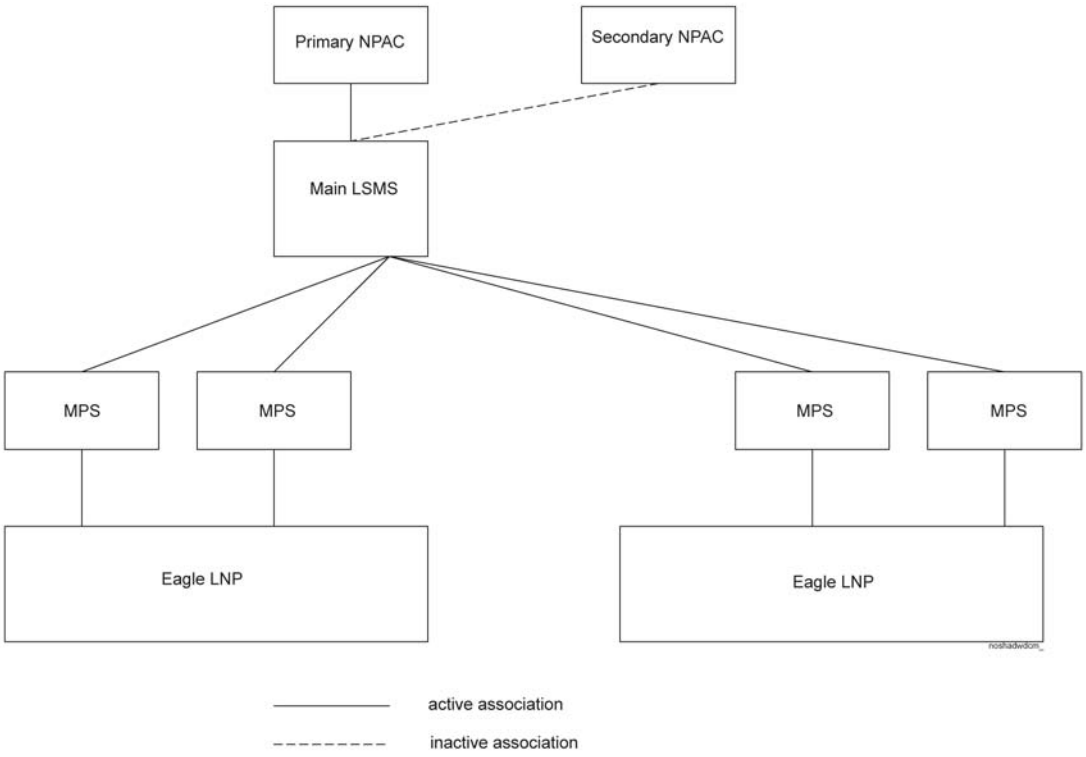
With this configuration, during disaster recovery you need to restore all databases from a backup tape made at the main LSMS. The recovery procedures are described in *Performing Disaster Recovery with an Inactive Shadow LSMS* on page 144.

Using No Shadow

Figure 81: Overview of Main LSMS without a Shadow LSMS on page 134 shows the configuration of a main LSMS that has no shadow as its backup.

When no shadow LSMS exists, disaster recovery requires immediate repair of the main LSMS and of its physical site. All databases must be restored from backup tapes that have been made before the disaster occurred.

Figure 81: Overview of Main LSMS without a Shadow LSMS



With this configuration, during disaster recovery you need to repair the main LSMS and then restore all databases from a backup tape made at the main LSMS. The recovery procedures are described in *Performing Disaster Recovery without a Shadow LSMS* on page 146.

Synchronizing Data Between the Main LSMS and Shadow LSMS

Both NPAC data and locally provisioned data need to be synchronized between the main and shadow LSMS so that the shadow can take over when the main LSMS fails.

- NPAC data synchronization occurs in one of the following ways:
  - With an active shadow, active connections from both main and active shadow to the NPACs allow transmission of the same NPAC data to both LSMSs.
  - With an inactive shadow, NPAC data is synchronized by loading files from a backup tape and/or downloading files from the NPAC to the inactive shadow LSMS.
- Locally provisioned data must be manually entered at both the main LSMS and shadow LSMS.

  Note: When you log in to manually enter any locally provisioned data, always use the same service provider ID (SPID) at both the main LSMS and the shadow LSMS. Locally provisioned data is correlated with a SPID . In order for the data to be the same at the main LSMS and shadow LSMS, it must be entered with the same SPID at both LSMSs. The main LSMS and shadow LSMS must use different NPAC-assigned SPIDs for their association with the NPAC. You can create SPIDs used just for entering data, or you can use the main LSMS's NPAC-assigned SPID for entering locally provisioned data at both the main LSMS and shadow LSMS.

For information about manually entering locally provisioned data, refer to the LSMS Database *Administration Manual*.

Preparing for a Disaster Situation

For all recovery strategies, prepare for disaster situations by doing the following:

- Make sure that the following conditions are true:
  - The main LSMS, any restored LSMS, and the shadow LSMS have the required software licenses. Use the procedure described in *Verifying the Processes Running on the Active Server* on page 159 for each server on each LSMS; licenses are required for processes to run.
  - Hardware and software versions on the main and shadow LSMS are identical.
  - Any optional features are installed and configured on both the main and shadow LSMS.
- Make sure the following items are always available and easy to locate:
  - The most recent database backup tape
  - TPD (Tekelec Platform Distribution) CD-ROM
  - LSMS application CD-ROM
  - Completed Disaster Recovery sheet, as shown in *Recovery Preparation Worksheet* on page 392.

In addition, if you use an active shadow LSMS, make sure the following conditions are true:

- The shadow LSMS hardware has received the same required maintenance as the main LSMS. (See *LSMS Preventive Maintenance Schedule* on page 81 for the necessary maintenance procedures.)
- You have the ability to connect to the shadow LSMS using `ssh` (Secure Shell).
- You have the ability to display LSMS applications on your workstation.
- The network connections from the network elements to the shadow LSMS, which are critical during a disaster, have been periodically tested. Networks are often subject to frequent changes, and these changes can affect your connection between the shadow LSMS and the network elements.
- Any data you have added, modified, or deleted on the main LSMS has also been added, modified, and deleted on the shadow LSMS.

At least annually, your site should prepare a drill in which the key personnel perform the disaster recovery procedure. This ensures that any potential problems or questions can be addressed in a nonemergency situation.

Determining When to Switch to Shadow LSMS

Switching to a shadow LSMS is the obvious solution in cases of fire or other destruction of the main LSMS site. In addition to these cases, some problems with the main LSMS may warrant switching to the shadow LSMS. These situations can be determined with the Surveillance feature.

If the Surveillance feature is active, it posts a notification every five minutes. If the Surveillance feature has detected an error, it posts a notification reporting the error. If no errors have been

detected, the Surveillance feature posts the following "keep alive" message to indicate that the Surveillance feature is running, where <Host Name> indicates the host name of the server that is reporting the notification.

```
LSMS8000|14:58 Jun 22, 2000|<Host Name>|Keep alive
```

Absence of "keep alive" messages is an indication that a potential problem exists. Contact the Tekelec Customer Care Center (see page 1-8) for help in determining whether the problems warrants switching to the shadow LSMS.

For more information about the Surveillance feature, see *Understanding the Surveillance Feature* on page 34. For more information about Surveillance notifications, see *Automatic Monitoring of Events* on page 247

Disaster Recovery Procedure Overview

Table 14: Comparison of Recovery Procedures to Perform on page 138 provides an overview comparison of the procedures you should perform and the order in which to perform them, according to the disaster backup strategy you are using. Following sections describe each disaster backup strategy in more detail and list any conditions assumed.

Table 14: Comparison of Recovery Procedures to Perform

Recovery Procedure **Note: This table is for comparison; for detailed procedures by strategy, see *Table 15: Recovery Procedures When LSMS Shadow Is Active* on page 143 through *Table 17: Recovery Procedures When No LSMS Shadow Exists* on page 147.**	**Active Shadow**[a]	**Inactive Shadow**[a]	**No shadow**[b]	**Restoring Operations to the Main LSMS After Running on Active Shadow**[b]	**Restoring Operations to the Main LSMS After Running on Inactive Shadow**[b]
Repair or replace the LSMS			1	1	1
Recovery acceptance test	1	1	2	2	2
Restore LSMS data from backup tape		2	3		3
Contact each NPAC from which the LSMS needs data to request download files		3	4		4
Contact each NPAC from which the LSMS needs data to		4		3[c]	5

Recovery Procedure **Note: This table is for comparison; for detailed procedures by strategy, see *Table 15: Recovery Procedures When LSMS Shadow Is Active* on page 143 through *Table 17: Recovery Procedures When No LSMS Shadow Exists* on page 147.**	**Active Shadow**[a]	**Inactive Shadow**[a]	**No shadow**[b]	**Restoring Operations to the Main LSMS After Running on Active Shadow**[b]	**Restoring Operations to the Main LSMS After Running on Inactive Shadow**[b]
provide it with the IP address with which to establish association to the mate LSMS					
FTP data from NPAC and import it into the LSMS		5	5[c]	4[c]	6[c]
Start LSMS GUI		6	6	5	7
Add locally provisioned data that had been entered since last backup (or not already entered on mate LSMS)	2	7	7	*	*

Recovery Procedure **Note: This table is for comparison; for detailed procedures by strategy, see *Table 15: Recovery Procedures When LSMS Shadow Is Active* on page 143 through *Table 17: Recovery Procedures When No LSMS Shadow Exists* on page 147.**	**Active Shadow**[a]	**Inactive Shadow**[a]	**No shadow**[b]	**Restoring Operations to the Main LSMS After Running on Active Shadow**[b]	**Restoring Operations to the Main LSMS After Running on Inactive Shadow**[b]
Reconnect network elements	3	8	8	6	8
If the disaster outage has lasted 7 days or less, perform a time range audit and reconcile to network elements and a full-range audit of DGTT, OGTT, and NPA-Splits (otherwise perform a bulk download to network elements and then reassociate	4	9	9[c]	7[c]	9[c]

Recovery Procedure Note: This table is for comparison; for detailed procedures by strategy, see *Table 15: Recovery Procedures When LSMS Shadow Is Active* on page 143 through *Table 17: Recovery Procedures When No LSMS Shadow Exists* on page 147.	Active Shadow[a]	Inactive Shadow[a]	No shadow[b]	Restoring Operations to the Main LSMS After Running on Active Shadow[b]	Restoring Operations to the Main LSMS After Running on Inactive Shadow[b]
network elements)					
If query servers are installed, stop all directly connected query servers	5	10		8	10
If query servers are installed, configure each directly connected query server to use the IP address of the mate LSMS for its master host	6	11		9	11
If query servers are installed, reload each	7	12	10	10	12

Recovery Procedure **Note: This table is for comparison; for detailed procedures by strategy, see *Table 15: Recovery Procedures When LSMS Shadow Is Active* on page 143 through *Table 17: Recovery Procedures When No LSMS Shadow Exists* on page 147.**	**Active Shadow[a]**	**Inactive Shadow[a]**	**No shadow[b]**	**Restoring Operations to the Main LSMS After Running on Active Shadow[b]**	**Restoring Operations to the Main LSMS After Running on Inactive Shadow[b]**
directly connected query server from the mate LSMS					
Run on the shadow LSMS until main LSMS is restored	8	13			
Return operations to restored main LSMS	9[d]	14[d]			

[a] Perform these procedures on the shadow LSMS.

[b] Perform these procedures on the main LSMS.

[c] Perform only as required.

[d] As described in *Table 18: Procedures to Return Operations from Shadow LSMS to Main LSMS* on page 149 (and summarized in the rightmost columns of this table).

[*] Backups should always be scheduled immediately before switching from the shadow LSMS to the main LSMS; no additional data should have been locally provisioned.

Performing Disaster Recovery with an Active Shadow LSMS

In this configuration, an entire LSMS is active and has active associations with each NPAC from which the LSMS needs data. This disaster recovery backup strategy provides the least out-of-service time for the LSMS.

In addition to the assumptions listed in *Preparing for a Disaster Situation* on page 136, the following conditions are assumed:

- Both the main LSMS and shadow LSMS are associated with each NPAC (up to eight) from which the LSMS needs data, and both the main LSMS and the shadow LSMS are receiving automatic updates. Each regional NPAC database at both LSMS sites is synchronized with the NPACs.
- A network connection from each serviced network element to the shadow LSMS exists, but the network element is not associated with the shadow LSMS at the time the main LSMS fails.
- Users, groups, and passwords are identically configured at the main LSMS and shadow LSMS.
- Any data locally provisioned at the main LSMS is also locally provisioned at the shadow LSMS.

Perform the procedures shown in *Table 15: Recovery Procedures When LSMS Shadow Is Active* on page 143 on the shadow LSMS when a disaster occurs on the main LSMS.

Table 15: Recovery Procedures When LSMS Shadow Is Active

Active	In the order shown, perform the following recovery procedures:
1	(Optional) Recovery acceptance test on active server of shadow LSMS: **1.** *Verifying the State of the Servers* on page 159 **2.** *Verifying the Processes Running on the Active Server* on page 159 (with primary server as active server) **3.** *Verifying the GUI Operability on the Active Server* on page 160 (with primary server as active server) **Note:** Do not switch over to the shadow LSMS's standby server until all EMSs have been resynchronized because all queued subscription data would be immediately flushed.
2	Add any locally provisioned data that may have been added to the main LSMS before it failed and has not yet been added to the active shadow.
3	Perform the procedures in *Reconnecting Network Elements* on page 153 (start with *Step 4* on page 155 and use the main LSMS as the source and the shadow LSMS as the destination).

Active	In the order shown, perform the following recovery procedures:
4	For each network element, perform a time-range audit (specify the start time to be one hour before the outage occurred) and a full-range audit of DGTT, OGTT, and NPA Splits. For information about performing audits, refer to "Audit and Optional Reconcile from the LSMS GUI" in the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual*.
5, 6, 7	If any query servers are installed: **1.** Stop the directly connected query servers. **2.** Configure each directly connected query server to use the shadow LSMS as its master host (refer to the procedure described in "MySQL Replication Configuration for Query Servers" in the LSMS *Configuration Manual*). **3.** For each directly connected query server, perform the procedure in *Reload a Query Server Database from the LSMS* on page 402.
8	Run on the shadow LSMS until the main LSMS is restored.
9	*Returning Operation from Shadow LSMS to Main LSMS* on page 148.

Performing Disaster Recovery with an Inactive Shadow LSMS

In this disaster recovery strategy, you have a complete LSMS system installed at a geographically remote site, but it is not running and does not receive updates from the NPAC until you perform the procedures described in this section. This strategy requires a much longer recovery period than having an active shadow requires, but is still much safer than having no shadow. Having no shadow can result in a very long recovery period in serious disaster situations, such as fire or natural disaster.

In addition to the assumptions listed in *Preparing for a Disaster Situation* on page 136, the following conditions are assumed:

- At the shadow site, all hardware and software components have already been installed and passed an acceptance test.
- At the main LSMS, valid backups exist for all data. These backups are ready to be shipped to the shadow LSMS.
- A network connection exists between the shadow LSMS and each network element and each NPAC. At the time of failure, the shadow LSMS is not associated with any of the network elements or NPACs.

Perform the procedures shown in *Table 16: Recovery Procedures When LSMS Shadow Is Inactive* on page 145 on the shadow LSMS when a disaster occurs on the main LSMS.

Table 16: Recovery Procedures When LSMS Shadow Is Inactive

Inactive	In the order shown, perform the following recovery procedures:
1	Recovery acceptance test on inactive shadow LSMS: **1.** *Verifying the State of the Servers* on page 159 **2.** *Verifying the Processes Running on the Active Server* on page 159 (with primary server as active server) **3.** *Verifying the GUI Operability on the Active Server* on page 160 (with primary server as active server) **4.** *Manually Switching Over from the Active Server to the Standby Server* on page 124 **5.** *Verifying the Processes Running on the Active Server* on page 159 (with secondary server as active server) **6.** *Verifying the GUI Operability on the Active Server* on page 160 (with secondary server as active server) **7.** *Manually Switching Over from the Active Server to the Standby Server* on page 124
2	*Restoring LSMS Data from Backup Tape* on page 152.
3, 4	Contact each NPAC from which the LSMS needs data to: • Provide them with the IP address with which to establish association to the shadow LSMS. • Request which files will be needed to download to the shadow LSMS. It is recommended that the request be for all NPAC files dated from one hour before the time shown on the backup tape.
5	FTP data from the NPAC and import it into the LSMS (see *Downloading Files from an NPAC to the LSMS* on page 369).
6	Start the LSMS GUI (association with each NPAC is automatically attempted).
7	At shadow, manually enter any locally provisioned data that had been entered at the main since the last backup tape was made.

Inactive	In the order shown, perform the following recovery procedures:
8	Perform the procedures described in *Reconnecting Network Elements* on page 153.
9	If the disaster outage has lasted for 7 days or less, for each network element, perform a time-range audit (specify the start time to be one hour before the outage occurred) and a full-range audit of DGTT, OGTT, and NPA Splits. For information about performing audits, refer to "Audit and Optional Reconcile from the LSMS GUI" in the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual.* (If the disaster outage has lasted more than 7 days, perform a complete bulk download from the shadow LSMS to each network element. For information about performing bulk downloads to network elements, refer to the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual*.)
10, 11, 12	If any query servers are installed: **1.** Stop the directly connected query servers. **2.** Configure each directly connected query server to use the shadow LSMS as its master host (refer to the procedure described in "MySQL Replication Configuration for Query Servers" in the LSMS *Configuration Manual*. **3.** For each directly connected query server, perform the procedure in *Reload a Query Server Database from the LSMS* on page 402.
13	Run on the shadow LSMS until the main LSMS is restored.
14	After main LSMS has been repaired, *Returning Operation from Shadow LSMS to Main LSMS* on page 148.

Performing Disaster Recovery without a Shadow LSMS

In this disaster backup strategy, you have no physical backup for the LSMS. In a disaster situation, you must restore the main LSMS. Having no shadow can result in a very long recovery period in serious disaster situations, such as fire or natural disaster.

In addition to the assumptions listed in *Preparing for a Disaster Situation* on page 136, the following conditions are assumed for this procedure:

- The main LSMS is restored at the same physical site. If another site is used, you must perform site survey and preparation as you do for any initial LSMS installation. For more information about installing LSMS, refer to the *T1100* Application Server *Hardware Manual*.
- A network connection exists between the restored main LSMS and each NPAC and network element.

Perform the procedures shown in *Table 17: Recovery Procedures When No LSMS Shadow Exists* on page 147 to restore the main LSMS when a disaster occurs.

Table 17: Recovery Procedures When No LSMS Shadow Exists

No shadow	In the order shown, perform the following recovery procedures:
1, 2	Contact the Tekelec Customer Care Center to arrange repair or replacement of the LSMS. Tekelec will dispatch technicians who will perform repairs, return the LSMS to operational status, and perform recovery acceptance tests.
3	*Restoring LSMS Data from Backup Tape* on page 152.
4	Contact each NPAC from which the LSMS needs data to request which files will be needed to download to the shadow LSMS. It is recommended that the request be for all NPAC files dated from one hour before the time shown on the backup tape.
5	FTP data from NPAC and import it into the LSMS (see *Downloading Files from an NPAC to the LSMS* on page 369).
6	Start the LSMS GUI (association with each NPAC is automatically attempted).
7	If any locally provisioned data needs to be added, add it.
8	Perform the procedures in *Reconnecting Network Elements* on page 153.
9	If the disaster outage has lasted for 7 days or less, for each network element, perform a time-range audit (specify the start time to be one hour before the outage occurred) and a full-range audit of DGTT, OGTT, and NPA Splits. For information about performing audits, refer to "Audit and Optional Reconcile from the LSMS GUI" in the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual*. (If the disaster outage has lasted more than 7 days, perform a complete bulk download to each network element. For

No shadow	In the order shown, perform the following recovery procedures:
	information about performing bulk downloads to network elements, refer to the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual*.)
10	If any query servers are installed, for each directly connected query server, perform the procedure in *Reload a Query Server Database from the LSMS* on page 402.

Returning Operation from Shadow LSMS to Main LSMS

Use the procedures described in this section to return operations from the shadow LSMS to the main LSMS after the main LSMS has been restored. Do not take the shadow LSMS out of service until you have completed this procedure, including the resynchronization of LNP data with the NPAC and network elements. If any problem occurs during the restoration of operations to the main LSMS, you can return to using the shadow LSMS.

In addition to the assumptions listed in *Preparing for a Disaster Situation* on page 136, the following conditions are assumed:

- The main LSMS is restored at the same physical site. If another site is used, you must perform site survey and preparation as you do for any initial LSMS installation. For more information about installing LSMS, refer to the *T1100* Application Server *Hardware Manual*.
- A network connection exists between the restored main LSMS and each NPAC and network element.
- Encryption keys have been exchanged between the NPAC and the restored main LSMS.
- License keys are valid for the main LSMS.
- At the main LSMS, valid backups exist for all data.
- At a previously inactive shadow LSMS, valid backups exist for all data. A complete backup should be scheduled immediately before the scheduled return to the main LSMS, so that no locally provisioned data is entered after the switch back to the main LSMS.

Perform the procedures shown in *Table 18: Procedures to Return Operations from Shadow LSMS to Main LSMS* on page 149 to restore the main LSMS.

Table 18: Procedures to Return Operations from Shadow LSMS to Main LSMS

Restoring Operations to the Main LSMS After Running on Active Shadow Main LSMS	Restoring Operations to the Main LSMS After Running on Previously Inactive Shadow	In the order shown in the appropriate column, perform the following recovery procedures:
1	1	Contact the Tekelec Customer Care Center to arrange repair or replacement of the LSMS. Tekelec will dispatch technicians who will perform repairs and return the LSMS to operational status.
2	2	Recovery acceptance test or manufacturing acceptance test, depending on the severity of original failure (performed by technicians).
3	3	After the Tekelec Customer Care personnel have performed an acceptance test, if desired, customers may wish to perform the following tests to verify that the restored main LSMS is fully functional: **1.** *Verifying the State of the Servers* on page 159 **2.** *Verifying the Processes Running on the Active Server* on page 159 (with primary server as active server) **3.** *Verifying the GUI Operability on the Active Server* on page 160 (with primary server as active server) **4.** *Manually Switching Over from the Active Server to the Standby Server* on page 124 **5.** *Verifying the Processes Running on the Active Server* on page 159 (with secondary server as active server)

Restoring Operations to the Main LSMS After Running on Active Shadow Main LSMS	Restoring Operations to the Main LSMS After Running on Previously Inactive Shadow	In the order shown in the appropriate column, perform the following recovery procedures:
		6. *Verifying the GUI Operability on the Active Server* on page 160 (with secondary server as active server) 7. *Manually Switching Over from the Active Server to the Standby Server* on page 124
	4	Create a backup tape on the shadow LSMS (see *Storing Backup Tapes Off-Site* on page 84).
	5	Contact the Tekelec Customer Care Center to arrange for them to restore data from the backup tape (made at the shadow LSMS) to the newly restored main LSMS.
3	6	If any NPAC data may be updated during the period of time between when you plan to disconnect the shadow LSMS and connect with the main LSMS, contact each NPAC from which the LSMS needs data and request download files for that time period.
	7	If returning from a shadow LSMS that was previously inactive, contact each NPAC from which the LSMS needs data to provide them with the IP address with which to establish association to the main LSMS.
4	8	If any download files were requested from any NPAC

Restoring Operations to the Main LSMS After Running on Active Shadow Main LSMS	Restoring Operations to the Main LSMS After Running on Previously Inactive Shadow	In the order shown in the appropriate column, perform the following recovery procedures:
		above, FTP the files and import them into the LSMS (see *Downloading Files from an NPAC to the LSMS* on page 369).
5	9	Start the LSMS GUI (see *Starting an LSMS GUI Session* on page 47).
6	10	Perform the procedures in *Reconnecting Network Elements* on page 153, where the source LSMS is the shadow LSMS, and the destination LSMS is the main LSMS.
7	11	For each network element, perform a time-range audit (specify the start time to be one hour before the outage occurred) and a full-range audit of DGTT, OGTT, and NPA Splits. For information about performing audits, refer to "Audit and Optional Reconcile from the LSMS GUI" in the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual.*
8, 9, 10	12, 13, 14	If any query servers are installed: **1.** Stop the directly connected query servers. **2.** Configure each directly connected query server to use the main LSMS as its master host (refer to the procedure described in "MySQL Replication Configuration for Query

Restoring Operations to the Main LSMS After Running on Active Shadow Main LSMS	Restoring Operations to the Main LSMS After Running on Previously Inactive Shadow	In the order shown in the appropriate column, perform the following recovery procedures:
		Servers" in the LSMS *Configuration Manual*. 3. For each directly connected query server, perform the procedure in *Reload a Query Server Database from the LSMS* on page 402.

Restoring LSMS Data from Backup Tape

To restore LSMS data from backup tapes, contact the Tekelec Customer Care Center.

Resynchronizing After an Outage Between an NPAC and the LSMS

When an outage between the LSMS and NPAC occurs, the LSMS attempts to resynchronize automatically as soon as the association is reestablished. The NPAC then resends to the LSMS all transactions that were missed by the LSMS.

Automatic Resynchronization between the NPAC and the LSMS

Whenever association is reestablished between the NPAC and the LSMS, the NPAC and the LSMS automatically resynchronize their databases. The time required for automatic resynchronization between an NPAC and the LSMS is directly proportional to the number of transactions that need to be sent. If you believe you have a lot of subscription version records, you can choose to perform a manual NPAC/LSMS recovery, as described in *Downloading Files from an NPAC to the LSMS* on page 369.

If the NPAC and the LSMS are unable to complete automatic recovery, one of the following notifications will display on the LSMS console window, where either PRIMARY or SECONDARY indicates the NPAC for which recovery is underway:

```
[Critical] 2018: 99-07-05 12:55:56 NPAC [<PRIMARY|SECONDARY>]  Recovery Failed
```

or

```
[Critical] 2019: 99 -07-05 12:55:56 NPAC [<PRIMARY|SECONDARY>]  Recovery Partial
 Failure
```

If you receive one of these messages, perform the procedure described in *Downloading Files from an NPAC to the LSMS* on page 369 using the example for performing a bulk download of files from the NPAC.

Reconnecting Network Elements

The following procedures explain how to reconnect the LSMS with network element software that manages database updates from the LSMS. Reconnecting is required in one of the following situations:

- When you switch from the main LSMS to the shadow LSMS after a disaster has occurred
- When you switch from the shadow LSMS back to the main LSMS after the main LSMS has been restored
- When you restore an LSMS that had no shadow

Perform the procedures described in the following sections. (In these procedures, the "source LSMS" is the LSMS you switch from and the "destination LSMS" is the LSMS you switch to.)

1. *"Preparing to Reconnect Network Elements"* on page 153
2. *Reconnecting Network Elements Procedures* on page 155

   These procedures will be followed by automatic resynchronization as described in *Automatic Resyncronization after Reconnect* on page 156.

Preparing to Reconnect Network Elements

1. Locate the completed Disaster Recovery Sheet, a current system backup tape, and a current database backup tape.
2. Alert the Tekelec Customer Care Center that you are switching to the destination LSMS.

   The Tekelec Customer Care Center will remain online to provide support during this procedure.
3. From the network element, enter the following command to verify that the destination LSMS is reachable, where <LSMS_IP_Address> is the IP address of the LSMS:

   ```
   > ping <LSMS_IP_Address>
   ```
4. From the destination LSMS, enter the following command to verify that the network element (NE) is reachable:

   ```
   # ping <ELAP_IP_Address>
   ```

5. If the destination LSMS is not already running, log in as a user in the `lsmsadm` group to the destination LSMS and start an LSMS GUI session.

   Verify that the destination LSMS is in stable condition by checking the following:

   a) Verify that there are no active alarm conditions.

      Because the destination LSMS is not connected with the EMS, there are always error messages regarding the network element queue level alarms and its connection with the LSMS. For a destination LSMS, these messages are normal. If the Surveillance feature is active, these normal messages will be notifications `LSMS 0004` and `LSMS 8003` or `LSMS 8004`. (For more information, see *Automatic Monitoring of Events* on page 247)

   b) Verify that the NPACs are connected to the LSMS by examining the NPAC status area on a graphical user interface; verify that the NPAC icon for each supported NPAC displays green.

   c) Use following method to verify that no LSMS hardware failure indications are present:

      If the Surveillance feature is active, verify that no hardware failure notifications (`LSMS 4003`, `LSMS 2000`, `LSMS 0001`, `LSMS 4004`, `LSMS 4005`, `LSMS 4006`, `LSMS 4007`, or `LSMS 4009`) have been posted. For more information about these notifications, see *Automatic Monitoring of Events* on page 247

   d) Verify that the LSMS is not currently in recovery mode with any NPAC by ensuring that none of the following GUI notifications have been posted for any NPAC, where <PRIMARY|SECONDARY> indicates whether the NPAC to be connected is the primary NPAC or the secondary NPAC:

```
[Critical]: <Timestamp> 2006: NPAC <PRIMARY|SECONDARY> Bind Timed Out -
Auto retry after 2 min
[Critical]: <Timestamp> 2007: NPAC <PRIMARY|SECONDARY> Connection Aborted
 by PEER - Auto retry same host
after 2 min
[Critical]: <Timestamp> 2008: NPAC <PRIMARY|SECONDARY> Connection Aborted
 by PEER - Auto retry other host
after 2 min
[Critical]: <Timestamp>: 2009 NPAC <PRIMARY|SECONDARY> Connection Aborted
 by Provider - Auto retry same
host after 2 min
[Critical]: <Timestamp> 2010: NPAC <PRIMARY|SECONDARY> Connection Aborted
 due to recovery failure - Auto
retry after 2 min
[Critical]: <Timestamp> 2012: NPAC <PRIMARY|SECONDARY> Connection Attempt
 Failed : Access Control Failure
[Critical]: <Timestamp> 2014: NPAC <PRIMARY|SECONDARY> Connection Attempt
 Failed : Access Denied
[Critical]: <Timestamp> 2015: NPAC <PRIMARY|SECONDARY> Connection
disconnected by NPAC
[Critical]: <Timestamp> 2018: NPAC iiii Recovery Failed
[Critical]: <Timestamp> 2019: NPAC iiii Recovery Partial Failure
[Critical]: <Timestamp> 2020: NPAC iiii Security Violation. Association
aborted
```

      Also, if the Surveillance feature is active, verify that none of the following Surveillance notifications have been posted for any NPAC, where `xxxxxxx` is the hostname of the server reporting the notification, <PRIMARY|SECONDARY> indicates the primary or secondary NPAC, <NPAC_cust_ID> is a numeric indicator for the NPAC region, and <NPAC_IP_address> is the IP address of the NPAC:

```
LSMS2000|14:58 Jul 22, 1997|xxxxxxx|Notify:Sys Admin - NPAC interface
failure
```

```
LSMS2001|14:58 Jul 22, 1997|xxxxxxx|Notify:Sys Admin - NPAC=
<PRIMARY|SECONDARY> - <NPAC_cust_ID>
LSMS2002|14:58 Jul 22, 1997|xxxxxxx|Notify:Sys Admin - NPAC=
<NPAC_IP_address>
```

If any of these notifications has been posted, verify that the following GUI notifications have been posted for the same NPAC:

```
[Cleared] 2025: <Timestamp>: NPAC <PRIMARY|SECONDARY> Connection Successfully
 established
[Cleared] 8055: <Timestamp>: NPAC <PRIMARY|SECONDARY> Recovery Complete
```

You have now completed this procedure. Continue with the next procedure.

Reconnecting Network Elements Procedures

Perform the following procedure:

1. At the source LSMS, log in as `lsmsadm` on the active server.
2. Enter the following command to display the status of all `eagleagent` processes:`eagle status`

   Scan the output for the names of all active Eagle agents, similar to the values shown in **bold** in the following example:

```
CLLI        Pid   State       Resync        Conn A  Conn B  DCM     EBDA
Debug Queue
Memory  CPU  Timestamp 1190801
     13622 A_ACTIVE    COMPLETE      ACTIVE  STANDBY NONE    IDLE     OFF
 0 %   71
M  0.1 % 13:00:40
```

3. At the source LSMS, for each Eagle agent process that is running, enter the following command to stop the Eagle agent processes (`<CLLI>` is the Common Language Location Identifier for the EAGLE 5 ISS node):

   `$LSMS_DIR/eagle stop <CLLI>`

   For the example shown in step 2, you would enter the following commands:

   `$LSMS_DIR/eagle stop 1190801`

4. At the destination LSMS, for each network element serviced by the LSMS, do one of the following:

   - In an inactive shadow configuration, create the EMS for the given network element (refer to the LSMS *Configuration Manual*, "Creating an EMS Configuration Component"). When you finish creating the EMS, `sentryd` process automatically starts the Eagle agent.
   - In an active shadow configuration, modify the EMS for the given network element (refer to the LSMS *Configuration Manual*, "Modifying an EMS Configuration Component"). Next, stop and restart the Eagle agent for the given CLLI using the following commands, then go to *"Automatic Resyncronization after Reconnect"* on page 156.

     `$LSMS_DIR/eagle stop <CLLI>`

     `$LSMS_DIR/eagle start <CLLI>`

You have now completed this procedure. Next, the LSMS and the network elements will automatically resynchronize as described in *"Automatic Resyncronization after Reconnect"* on page 156.

Automatic Resyncronization after Reconnect

When the LSMS and MPS are reconnected, the LSMS automatically starts an automatic resynchronization of the databases. For more information, see "Automatic Resynchronization Process" in the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual*. If the LSMS cannot complete automatic resynchronization, it posts a notification to the LSMS GUI. For more information, see "Notifications that Database Maintenance Is Required" in the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual*.

If the Surveillance feature is active, the following Surveillance notification is also posted, where <Host Name> is the hostname and <CLLI> is the 11-character CLLI code of the network element:

```
LSMS8001|14:58 Jul 22, 1997|<Host Name>|Notify:Sys Admin - NE CLLI=<CLLI>
```

Chapter 8

Verifying Recovery

Topics:

- *Introduction Page 158*
- *Verifying that the LSMS Is Fully Functional Page 158*

This chapter describes procedures used to verify the status of the LSMS after performing recovery procedures.

Introduction

This chapter describes procedures used to verify the status of the LSMS after performing recovery procedures.

Verifying that the LSMS Is Fully Functional

Perform the tests in the order shown in *Table 19: Recovery Acceptance Tests* on page 158 to verify that the LSMS is fully functional following file system restoration. If any of these tests fail, contact the Tekelec Customer Care Center.

Table 19: Recovery Acceptance Tests

	Condition to Verify	Test to Perform
1	One server is in ACTIVE state and the other server is in STANDY state	*Verifying the State of the Servers* on page 159
2	The appropriate software processes are running on the primary server	*Verifying the Processes Running on the Active Server* on page 159
3	The GUI process can be started on the primary server	*Verifying the GUI Operability on the Active Server* on page 160
4	Switchover can be performed from the active server to the standby server	*Manually Switching Over from the Active Server to the Standby Server* on page 124
5	The appropriate software processes can be run on the newly active server	*Verifying the Processes Running on the Active Server* on page 159
6	The GUI process can be started on the newly active server	*Verifying the GUI Operability on the Active Server* on page 160
7	Switchover can be performed from the active server to the standby server	*Manually Switching Over from the Active Server to the Standby Server* on page 124
8	The appropriate software processes can be run on the newly active server	*Verifying the Processes Running on the Active Server* on page 159
9	The GUI process can be started on the newly active server	*Verifying the GUI Operability on the Active Server* on page 160

Verifying the State of the Servers

Use the TPD HA (Tekelec Platform Distribution High Availability) utility to verify that one server is in ACTIVE state and the other server is in STANDBY state. See *Determining the Server Status* on page 123.

Verifying the Processes Running on the Active Server

1. Log in to the active server as `root`.
2. Display the status of all processes that are configured to run on the active server by entering each of the following commands and examining their outputs:

   ```
   # /usr/TKLC/plat/bin/syscheck -v proc run
   ```

   ```
   # /usr/TKLC/plat/bin/syscheck -v lsmshc proc
   ```

   The following sample output from `syscheck -v proc run` indicates which processes are configured to be running on the active server and that all expected instances of the processes are running:

```
Running modules in class proc...
       run: Checking supman...
       run: Found 1 instance(s) of the supman process.
       run: Checking lsman...
       run: Found 1 instance(s) of the lsman process.
       run: Checking npacagent...
       run: Found 1 instance(s) of the npacagent process.
       run: Checking eagleagent...
       run: Found 2 instance(s) of the eagleagent process.
       run: Checking rmtpmgr...
       run: Found 1 instance(s) of the rmtpmgr process.
       run: Checking rmtpagent...
       run: Found 1 instance(s) of the rmtpagent process.
       run: Checking reportman...
       run: Found 1 instance(s) of the reportman process.
       run: Checking lsmslogd...
       run: Found 1 instance(s) of the lsmslogd process.
       run: Checking sentryd...
       run: Found 1 instance(s) of the sentryd process.
       run: Checking survMon...
       run: Found 1 instance(s) of the survMon process.
       run: Checking smartd...
       run: Found 1 instance(s) of the smartd process.
       run: Checking atd...
       run: Found 1 instance(s) of the atd process.
       run: Checking crond...
       run: Found 1 instance(s) of the crond process.
       run: Checking sshd...
       run: Found 7 instance(s) of the sshd process.
       run: Checking syscheck...
       run: Found 1 instance(s) of the syscheck process.
       run: Checking syslogd...
       run: Found 1 instance(s) of the syslogd process.
Return string: "OK"
                                    OK
```

```
The log is available at:
  -->/var/TKLC/log/syscheck/fail_log
```

If you see FAILURE (similar to the following example) for any process except the GUI process, contact the Tekelec *Customer Care Center* on page 5:

```
run: Only 0 instance(s) of  lsmslogd running. 1 instance(s) required.
```

The following sample output from `syscheck -v lsmshc proc` indicates which processes are configured to be running on the active server and that all expected instances of the processes are running:

```
Running modules in class lsmshc...
      proc: Node active, checking
      proc: Checking supman...
      proc: Found 1 instance(s) of the supman process.
      proc: Checking lsman...
      proc: Found 1 instance(s) of the lsman process.
      proc: Checking npacagent...
      proc: Found 1 instance(s) of the npacagent process.
      proc: Checking eagleagent...
      proc: Found 1 instance(s) of the eagleagent process.
      proc: Checking rmtpmgr...
      proc: Found 1 instance(s) of the rmtpmgr process.
      proc: Checking rmtpagent...
      proc: Found 1 instance(s) of the rmtpagent process.
      proc: Checking reportman...
      proc: Found 1 instance(s) of the reportman process.
      proc: Checking lsmslogd...
      proc: Found 1 instance(s) of the lsmslogd process.
      proc: Checking sentryd...
      proc: Found 1 instance(s) of the sentryd process.
Return string: "OK"
                                  OK
The log is available at:
  -->/var/TKLC/log/syscheck/fail_log
```

You have now completed this procedure.

Verifying the GUI Operability on the Active Server

Perform the following procedure to verify that the LSMS graphical user interface will open:

1. Perform the procedure described in *Logging In to LSMS Server Command Line* on page 45 using the hostname of the active server.
2. Perform the procedure described in *Starting an LSMS GUI Session* on page 47, using an NPAC-provided Service Provider ID.
3. Select **Exit/Logout** from the **User/Session** menu on the LSMS Console window.

   The console logout window displays. Click **OK** to complete the logout.

You have now completed this procedure.

Appendix A

Commands

Topics:

- *Introduction Page 162*
- *Entering LSMS and Third-Party Application Commands Page 165*
- *Using lsmsclaa Commands Page 230*
- *ABORT Page 235*
- *ASSOCIATE Page 237*
- *AUDIT Page 239*
- *EXIT Page 241*
- *HELP Page 242*
- *SYNCH Page 242*

This appendix shows you the syntax and usage of LSMS commands

Introduction

You access most LSMS database administration and configuration functions through the LSMS graphical user interface (GUI). For more information about using the GUI for these functions, refer to the LSMS Database *Administration Manual*, the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual*, and the LSMS *Configuration Manual*.

In addition, you can use commands to manage some LSMS functions. This appendix shows you the syntax and usage of LSMS commands.

This appendix describes the following types of commands:

- LSMS and third-party application commands, entered at a command-line prompt, that control LSMS or third-party applications—for more information, see *Overview of LSMS Application Commands Entered at the Command-Line Prompt* on page 162.
- With the optional LSMS Command Line Application Administration (`lsmsclaa`) feature, actions entered at the `lsmsclaa` prompt, that enable you to administer certain LSMS functions through the command line instead of through the graphical user interface (GUI)—for more information, see *Using lsmsclaa Commands* on page 230.

Overview of LSMS Application Commands Entered at the Command-Line Prompt

Table 20: LSMS Application Functions and Third-Party Commands Available at the command-line Prompt on page 162 summarizes the LSMS application and third-party application commands that are entered at the command-line prompt. These commands are described in this appendix. For information about the notation used in the command descriptions, see *Entering LSMS and Third-Party Application Commands* on page 165.

Table 20: LSMS Application Functions and Third-Party Commands Available at the command-line Prompt

Function	Command
Display, add, or delete remote locations and scheduled transfers	*autoxfercfg* on page 166
Select the last change time for the specified region	*chglct* on page 168
Verify that EMS Routing is set up properly	*chkfilter* on page 170
Control an `eagleagent` process	*eagle* on page 172
Import data from NPAC files into LSMS databases	*import* on page 177

Function	Command
Load, delete, or display keys for NPAC associations	*keyutil* on page 182
Control a regional `npacagent`	*lsms* on page 184
Obtain information about a database	*lsmsdb* on page 187
Start, stop, or show status of the SNMP Agent process	*lsmsSNMP* on page 191
Control the Surveillance process	*lsmssurv* on page 192
Perform mass update of SPID for LRN, NPA-NXX, and NPA-NXX-X	*massupdate* on page 195
Print measurement pegs to the display	*measdump* on page 200
Create or remove a regional NPAC database	*npac_db_setup* on page 202
Import specific files into a regional database	*npacimport* on page 204
Generate a report about one or more databases	*report* on page 206
Create or remove the resynchronization database	*resync_db_setup* on page 212
Control the Service Assurance agent	*SAagent* on page 214
Associate usernames with SPIDs	*spidsec* on page 220
Start the LSMS Command Line Application Administration (`lsmsclaa`) application, which enables users to enter text commands to control certain LSMS application functions otherwise available through the GUI	*start_cmdLine* on page 222
Start the LSMS GUI	*start_mgui* on page 224
Control the Local Services Manager and the Local Data Manager processes	*sup* on page 225
Create or remove the Supported database	*sup_db_setup* on page 226

Function	Command
Use to send a customer-defined notification	*survNotify* on page 229
Detect, diagnose, or display a summary of the overall health of the LSMS	*syscheck* on page 230

Overview of `lsmsclaa` Commands

The optional LSMS Command Line Application Administration (`lsmsclaa`) feature enables you to administer certain LSMS functions through the command line instead of through the graphical user interface (GUI). *Table 21: LSMS Functions Available Through lsmsclaa and Through GUI* on page 164 shows the LSMS functions that can be accessed through the `lsmsclaa` application as well as through the LSMS GUI.

For information about how to start the `lsmsclaa` application, see *start_cmdLine* on page 222. For more information about how to enter these commands, see *Using lsmsclaa Commands* on page 230. The specific actions are listed alphabetically starting at page A-89.

Table 21: LSMS Functions Available Through `lsmsclaa` and Through GUI

Function	`lsmsclaa` Action	GUI Description
Create an association with an NPAC	*ASSOCIATE* on page 237	"Creating an NPAC Association" in the LSMS *Configuration Manual*
Abort an association with an NPAC	*ABORT* on page 235	"Aborting an NPAC Association" in the LSMS *Configuration Manual*
Resynchronize data between the NPAC and the LSMS for: • Individual TN • Range of TNs • All TNs modified or created within a time range • Individual NPB • Range of NPBs	*SYNCH* on page 242	"Resynchronizing an Individual TN," "Resynchronizing a Range of TNs," "Resynchronizing for a Defined Period of Time", "Resynchronizing an Individual NPB", and "Resynchronizing a Range of NPBs" in the LSMS Database *Administration Manual*
Compare subscription version data between the LSMS regional database and the corresponding data at a specified network element	*AUDIT* on page 239	"Auditing Network Element Data" in the LSMS Database *Administration Manual*

Entering LSMS and Third-Party Application Commands

This appendix describes LSMS and certain third-party application commands used to manage the LSMS. Third-party commands identify their software source. All other commands in this appendix are LSMS commands.

All commands in this appendix are case-sensitive and are entered at the command-line prompt. After entering a command, you must press the Enter key. When the command has executed, you can enter another command.

Notation

This appendix uses the following syntax notational conventions for commands entered at the command-line prompt:

- *Keywords* - identify the principal action to be performed by the system.
- *Permission* - identifies the group to which the user must belong to execute the command, or for certain commands, whether the user must be logged in with a particular user name. The possible groups are `lsms` as primary group, or secondary groups `lsmsadm`, `lsmsuser`, `lsmsuext`,`lsmsview`, and `lsmsall` (all users defined to be a member of one of these secondary groups should have `lsms` defined as their primary group). For more information about primary and secondary group definitions, see *Managing User Accounts* on page 62.
- *Restrictions* - note restrictions or limitations applying to the use of the command.
- *Syntax* - identifies the command's keywords, options (if any), parameters, and their proper order. In syntax, the following symbols are used:
  - <xxx> indicates a variable
  - [xxx] indicates a parameter or option that is optional
  - {xxx|yyy} indicates a mandatory parameter; you must specify one of the values shown (in this case xxx or yyy)
- *Options* - tell the operating system how to perform a command. Options are also known as switches.
- *Parameters* - further define the command's operation.
- *Sample Output* - is an example of typical output produced by the command.
- *Environment* - identifies any special environment variables or condition that must exist on the system for the process to execute. All commands use only default environment variables, with the exception of `start_mgui`, which requires setting the $DISPLAY environment variable.
- *Response Notes* - identifies any pertinent command performance information.
- *Related Commands* - identifies other commands or programs related to this command.
- *Files* - identifies, describes, and provides the location of the configuration files required for proper execution of this command.

Command Example

The following is an example of an LSMS command entry:

```
$ $LSMS_DIR/resync_db_setup create
```

The environment variable is `$LSMS_DIR`, the directory containing the LSMS software. It is followed by the keyword `resync_db_setup` (command for creating or removing the resynchronization database). A single parameter is given for this command, `create` (indicates the resynchronization database is to be created). This command has no options.

autoxfercfg

Automatic File Transfers

Displays, adds, and deletes remote locations and scheduled transfers.

Keyword

`autoxfercfg`

Permission

The user must be defined as a member of the secondary group `lsmsadm`.

Syntax

```
$LSMS_DIR/autoxfercfg [-h]
```

Options

None.

Parameters

None.

Sample Output

```
Tekelec Automatic File Transfer Configuration Utility v1.0
Copyright 2000, Tekelec
Select one of the following menu options:
1) Display valid remote locations
2) Add new remote location
3) Remove remote location
4) Display all scheduled transfers
5) Add new scheduled transfer
6) Remove scheduled transfer
7) Exit
```

For more information about using this menu, see one of the following:

- *Displaying Remote Locations Used for Automatic File Transfers* on page 100
- *Adding a New Remote Location for Automatic File Transfers* on page 101
- *Deleting a Remote Location for Automatic File Transfers* on page 102
- *Displaying Previously Scheduled Automatic File Transfers* on page 103
- *Scheduling an Automatic File Transfer* on page 104

- *Removing a Scheduled Automatic File Transfer* on page 105

CAUTION: The `.netrc` file (see *Files* on page 167) contains the `ftp` account login information and is readable by root.

Possible Errors

Table 22: Error Messages: autoxfercfg

Exit Code	Message	Cause	Suggested Recovery
1	`Feature not enabled`	The Automatic File Transfer feature is not installed.	Contact Tekelec to schedule installation and activation of the feature.
2	`Only user 'lsmsadm' can run this program`	The user that tried to run this program was not the user `lsmsadm`.	Change user to `lsmsadm`.
3	`Configuration utility already running`	The `autoxfercfg` command has already been entered, but not yet exited.	No action necessary.
4	`Unable to open <home>/.netrc (where <home> is the home directory of the user)`	The file permissions for `$HOME/.netrc` are not set correctly.	Change permissions on the `$HOME/.netrc` file.

Files

The following files associated with the `autoxfercfg` command.

Table 23: Files: autoxfercfg

Filename	Type	Location
`.netrc`	Autologin resource file for `ftp`	`$HOME`
`crontab`	List of scheduled cron jobs	`$HOME`
`autoxfer.cfg`	Configuration file	`/usr/TKLC/lsms/config`

chglct

Change Last Change Time

Manually sets the Last Change Time (LCT) for the database belonging to the specified region.

In each regional database, the LSMS updates the LCT when the LSMS receives transactions from that NPAC. When the LSMS automatically recovers from a temporary loss of association with an NPAC, it uses the LCT to determine the time range for which to request that the NPAC resend transactions.

Use this command to manually set the LCT when performing a bulk download of files from the NPAC (see *NPAC-LSMS Download Procedure* on page 376, *Step 32* on page 387

Keyword

`chglct`

Permission

The user must be logged in with the user name `lsmsadm`.

Syntax

```
$LSMS_TOOLS_DIR/chglct -h -r <region> [-d|-s <YYYYMMDDhhmmss>]
```

Options

`-h` Displays help information

`-r <region>` Display or set the LCT (in Greenwich Mean Time) for the region specified by <*region*>. Possible values for <*region*> are:

```
Canada
Midwest
MidAtlantic
Southeast
Southwest
Northeast
```

```
Western
WestCoast
```

-d Display the current value of the LCT (in GMT) value for the specified region. The value has 14 characters in the form YYYYMMDDhhmmss which has the format shown in *Table 24: Time Value for chglct* on page 169.

-s <YYYYMMDDhhmmss> Set the value of the last change timestamp (in GMT) value for the specified region to the value indicated by the specified character string, which has 14 characters in the form YYYYMMDDhhmmss.

Table 24: Time Value for `chglct`

Characters	Meaning	Range
YYYY	Year	Any four digits
MM	Month	01–12
DD	Day	01–31
hh	Hour	00–23
mm	Minute	00–59
ss	Second	00–59

Sample Output

```
Display the last changed timestamp for the Midwest region
$ chglct -d -r Midwest

Midwest last changed timestamp: 20011107113017
Local Time: 11/7/2001 6:30:17
GMT Time: 11/7/2001 11:30:17
$
```

Related Commands

None.

Response Notes

None.

Possible Errors

Table 25: Error Messages: chglct

Exit Code	Error Message	Cause	Suggested Recovery
-1	`Syntax error`	User entered command with incorrect syntax.	Try the command again with correct syntax.
1	`DbError`	Database exception.	Contact the Tekelec Customer Care Center.
2	`InvalidUser`	A user with a username other than `lsmsadm` attempted to run this command.	Log in as `lsmsadm` and try the command again.
3	`UnknownError`	Contact Tekelec.	Contact the Tekelec Customer Care Center.

Files

None.

chkfilter

Check EMS Routing Filters

Run this command to verify that EMS Routing is set up properly. This command reviews all the TN (telephone number) and NPB (number pool block) transactions that were received from NPACs in the past 24 hours and determines whether any of these TNs and NPBs were not forwarded to any EAGLE 5 ISS. If any are found, a file `$LSMS_DIR/../logs/trace/LsmsSubNotFwd.log.<MMDD>` (where `<MMDD>` indicates the month and day the `chkfilter` command was run) is created and those TNs and NPBs are stored in this file.

Keyword

`chkfilter`

Permission

The user must be logged in with the user name `lsmsadm`.

Syntax

```
$LSMS_TOOLS_DIR/chkfilter
```

Options

None.

Sample Output

```
$ chkfilter

$
```

Related Commands

None.

Files

Table 26: Files: chkfilter

Filename	Type	Location
LsmsSubNotFwd.log.<MMDD>		$LSMS_DIR/../logs/trace/

Response Notes

None.

Possible Errors

Table 27: Error Messages: chkfilter

Exit Code	Error Message	Cause	Suggested Recovery
-1	`Syntax error`	User entered command with incorrect syntax.	Try the command again with correct syntax.
1	`DbError`	Database exception.	Contact the Tekelec Customer Care Center.
2	`InvalidUser`	A user with a username other than `lsmsadm` attempted to run this command.	Log in as `lsmsadm` and try the command again.
3	`EnvNotSet`	The LSMS_DIR env variable is not set.	Verify the environment variables.
4	`FileError`	Unable to open output file, check directory and permission	Contact the Tekelec Customer Care Center.
5	`UnknownError`	Not known.	Contact the Tekelec Customer Care Center.

eagle

Eagle Agent Control

Used to start, stop, or display status of an `eagleagent` process.

Keyword

`eagle`

Permission

The user must be logged in with the user name `lsmsadm`.

Syntax

```
$LSMS_DIR/eagle <Action> <CLLI>
```

Options

None.

Parameters

`Action` The function to be performed on the `eagleagent` process. This mandatory parameter has the following values:

```
start
stop
status
```

`<CLLI>` Common Language Location Identifier for the network element associated with this `eagleagent` process. This parameter is required when `Action` is `start` or `stop`. When `Action` is `status`, this parameter is optional; if not specified, the status for all `eagleagent` processes is displayed.

Sample Output

Stop the Eagle Agent for the network element whose CLLI is STPM1

```
$ $LSMS_DIR/eagle stop STPM1
```

```
eagle: Stopping...
eagle: eagleagent STPM1 stopped at Thu Mar  7 17:21:05 2002
```

Verify that Eagle Agent has stopped

```
$ $LSMS_DIR/eagle status STPM1
```

```
eagle: eagleagent STPM1 is not running.
```

Restart the Eagle Agent for the network element whose CLLI is STPM1

```
$ $LSMS_DIR/eagle start STPM1
```

```
eagle: Starting...
eagle: eagleagent STPM1 started at Thu Mar  7 17:17:36 2002
```

Check the status of the Eagle Agent for the network element whose CLLI is STPM1

```
$ $LSMS_DIR/eagle status STPM1
```

```
eagleagent:
               CLLI = STPM1
                Pid = 72
              State = NONE_ACTIVE
             Resync = NO_CONNECTION
       Connection A = DOWN
       Connection B = DOWN
     DCM connection = NONE
               EBDA = IDLE
      Debug logging = OFF
      Pending queue = 0 of 2000000 bytes (0%)
 Keepalive timestamp = Thu Mar  7 17:19:02 EST 2002
     Virtual memory = 14392 K bytes
          CPU usage = 1.1 %
```

Check the status of all Eagle Agents

```
$ $LSMS_DIR/eagle status
```

```
CLLI        Pid   State       Resync        Conn A  Conn B  DCM     EBDA    Debug
 Queue  Memory  CPU  Timestamp
STPM0        ---   not running
STPM1        72    NONE_ACTIVE NO_CONNECTION DOWN    DOWN    NONE    IDLE     OFF
    0 %   14 M  0.4 % 17:19:25
STPM2        449   B_ACTIVE    IN_PROGRESS   DOWN    ACTIVE  NONE    RUNNING  OFF
    0 %   12 M  1.0 % 17:19:23
STPO3        20179 A_ACTIVE    COMPLETE      ACTIVE  STANDBY OK      IDLE     OFF
    0 %   14 M  0.3 % 17:19:27
```

Related Commands

None.

Response Notes

None.

Files

None.

Possible Errors

Table 28: Exit Codes: eagle

Exit Code	Cause	Suggested Recovery
1	Incorrect syntax.	Correct the syntax.
2	Invalid command for current state.	No action necessary.
3	Error in environment.	Verify the environment variables.
4	Unable to create socket.	Contact the Tekelec Customer Care Center.
5	Unable to bind socket.	Contact the Tekelec Customer Care Center.
6	Fatal application error.	Contact the Tekelec Customer Care Center.
7	Operation failed.	Contact the Tekelec Customer Care Center.

Exit Code	Cause	Suggested Recovery
This command is usually run by scripts; scripts should search for exit codes. When the command is run from the command line, the output indicates suggested recovery.		

hastatus

Display LSMS HA Status

Allows user to display the High Availability status of the server on which the command is run.

Keyword

`hastatus`

Permission

The user can be logged in as any user.

Syntax

`/usr/TKLC/plat/bin/hastatus`

Required Flags

None.

Sample Output

```
$ hastatus

ACTIVE
```

Related Commands

None.

Response Notes

None.

Possible Errors

Table 29: Error Messages: hastatus

Exit Code	Error Message	Cause	Suggested Recovery
0	Success	n/a	n/a

Exit Code	Error Message	Cause	Suggested Recovery
1	Failure	Varies	Contact the Tekelec Customer Care Center
2	Query No Match	Querying the status of a component, based on a condition, did not result in a match. Following are the most common causes, which are dependent upon the particular query.	

		• If the query was returned while querying for keepalive status, keepalive may be unconfigured or misconfigured	• Customer or field engineers should:
			  • Verify network configuration and network cabling
			  • Verify serial configuration and cabling if serial keepalive is configured
			  • If the problem persists, Contact the Tekelec Customer Care Center

		• If the query was returned while querying for ping status, there may be a network problem	• Customer or field engineers should:
			  • Verify the network configuration and connection, especially the uplink to the customer's network
			  • Check keepalive status
			  • If the problem persists, Contact

Exit Code	Error Message	Cause	Suggested Recovery
			the Tekelec Customer Care Center

		• If the query was returned while querying for node status, there may be a problem with keepalive	• Customer or field engineers should:
			  • Check keepalive status
			  • If the problem persists, Contact the Tekelec Customer Care Center

		• All others	• Contact the Tekelec Customer Care Center
6	UnknownError	Not known	Contact the Tekelec Customer Care Center

import

Upload to MySQL Database

Imports data from NPAC files into LSMS databases. This command performs all parameter checking, and validates or creates the NPAC directory if required.

Note: Do not run the `import` command while any of the following processes are also running: backups, starting a standby node (to change its state from UNINITIALIZED "INHIBITED" to STANDBY), running the `lsmsdb quickaudit` command, and creating query server snapshots, all of which use temporary storage space. If you try to run the `import` command while any of these processes are running, you may not have enough disk space to complete the process. Since backups can be run automatically, perform the procedure described in *Checking for Running Backups* on page 93 to ensure that no backups are running.

Keyword

`import`

Permission

The user must be defined as a member of the primary group `lsms`.

Syntax

```
$LSMS_DIR/import [-c] [-o [-d <dir>]] <region> [<filename>...]
```

Provided the `import` command is prefaced by the `$LSMS_DIR` environment variable, it can be performed from any directory location.

Options

`-c`	If an error occurs, continue with the next record in the file. Errors are recorded in a file named <filename>_FAILED, where <filename> has the same value as was entered in the command.
`-o`	Generate a Response file for SV and NPB imports.
`-d <dir>`	Put the Response file(s) in the specified directory (defaults to the same directory as each SV/NPB import file).

Parameters

`<region>`	Name of the NPAC region: Midwest, MidAtlantic, Northeast, Southeast, Southwest, Western, WestCoast, Canada. This is a required parameter.
`<filename>`	The name of the NPAC downloadfile in `npacftp/<region>`. This is an optional parameter. If you do not specify a `<filename>`, a list displays that includes all the valid import files from the `npacftp/<region>` directory for the NPAC region specified (the region is a required parameter).

Note: Filenames must adhere to the following formats:

```
LRN.<create>.<start>.<end> NPANXX.<create>.<start>.<end>
NPANXXX.<create>.<start>.<end> SPID.<create>
<npanxx>-<npanxx>.<create>.<start>.<end>
<npanxxx>-<npanxxx>.<create>.<start>.<end>
```

Where:

`<create>` is the file creation timestamp: `<DD-MM-YYYYhhmmss>`

`<start>` is the start of the time-range: `<DD-MM-YYYYhhmmss>`

`<end>` is the end of the time-range: `<DD-MM-YYYYhhmmss>`

Note: For Active (not time-range) files,

```
<start> is 00-00-0000000000 and             <end> is 99-99-9999999999
```

Note: SPID files are always Active.

Note: Active files with filenames in the old format, with only a creation timestamp, are still supported.

Example 1:

```
<npanxx>-<npanxx>.<create>.<start>.<end>:

303123-303125.02-11-1998133022.12-10-1998080000.13-10-1998133022
```

Example 2:

```
LRN.<create>.<start>.<end> [Active (not time-range) file]:

LRN.02-10-2001102201.00-00-0000000000.99-99-9999999999
```

Sample Output

```
NPAC FTP directory: /var/TKLC/lsms/free/data/npacftp/Midwest
The following NPAC download file(s) are available for import:
            LRN.11-07-2001145342           NPANXX.11-07-2001145342
        NPANXX.11-07-2001145342             SPID.11-07-2001145342
  000000-999999.11-07-2001145342     0000000-9999999.11-07-2001145342
Import LRN.11-07-2001145342 (Yes/No/All/Quit)?all
The following NPAC download files have been chosen to be imported:
           SPID.11-07-2001145342          NPANXX.11-07-2001145342
         NPANXX.11-07-2001145342              LRN.11-07-2001145342
  000000-999999.11-07-2001145342  0000000-9999999.11-07-2001145342
Do you want to continue (Yes/No)?yes
Beginning Delete Process for SPID.11-07-2001145342
Delete Process Completed for SPID.11-07-2001145342
Beginning Download Process for SPID.11-07-2001145342
1000 ServiceProvNetwork instance updates in MidwestDB
2000 ServiceProvNetwork instance updates in MidwestDB
2351 ServiceProvNetwork instance updates in MidwestDB
Import completed successfully.
Download Process Completed for SPID.11-07-2001145342
Beginning Delete Process for NPANXXX.11-07-2001145342
Delete Process Completed for NPANXXX.11-07-2001145342
Beginning Download Process for NPANXXX.11-07-2001145342
1000 ServiceProvNPA_NXX_X instance updates in MidwestDB
2000 ServiceProvNPA_NXX_X instance updates in MidwestDB
3000 ServiceProvNPA_NXX_X instance updates in MidwestDB
4000 ServiceProvNPA_NXX_X instance updates in MidwestDB
30000 ServiceProvNPA_NXX_X instance updates in MidwestDB
30860 ServiceProvNPA_NXX_X instance updates in MidwestDB
Import completed successfully.
Download Process Completed for NPANXXX.11-07-2001145342
Beginning Delete Process for NPANXX.11-07-2001145342
Delete Process Completed for NPANXX.11-07-2001145342
Beginning Download Process for NPANXX.11-07-2001145342
90 ServiceProvNPA_NXX instance updates in MidwestDB
1090 ServiceProvNPA_NXX instance updates in MidwestDB
Import completed successfully.
Download Process Completed for NPANXX.11-07-2001145342
Beginning Delete Process for LRN.11-07-2001145342
Delete Process Completed for LRN.11-07-2001145342
Beginning Download Process for LRN.11-07-2001145342
1000 ServiceProvLRN instance updates in MidwestDB
2000 ServiceProvLRN instance updates in MidwestDB
3000 ServiceProvLRN instance updates in MidwestDB
4000 ServiceProvLRN instance updates in MidwestDB
4700 ServiceProvLRN instance updates in MidwestDB
5700 ServiceProvLRN instance updates in MidwestDB
Import completed successfully.
Download Process Completed for LRN.11-07-2001145342
Beginning Delete Process for 000000-999999.11-07-2001145342
All Subscription Version instances deleted from Midwest
Delete Process Completed for 000000-999999.11-07-2001145342
Beginning Download Process for 000000-999999.11-07-2001145342
1000 SubscriptionVersion instance updates in MidwestDB
2000 SubscriptionVersion instance updates in MidwestDB
3000 SubscriptionVersion instance updates in MidwestDB
4000 SubscriptionVersion instance updates in MidwestDB
4500 SubscriptionVersion instance updates in MidwestDB
Import completed successfully.
Download Process Completed for 000000-999999.11-07-2001145342
Beginning Delete Process for 0000000-9999999.11-07-2001145342
All Subscription Version instances deleted from Midwest
Delete Process Completed for 0000000-9999999.11-07-2001145342
```

```
Beginning Download Process for 0000000-9999999.11-07-2001145342
1000 NumberPoolBlock instance updates in MidwestDB
2000 NumberPoolBlock instance updates in MidwestDB
Import completed successfully.
Download Process Completed for 0000000-9999999.11-07-2001145342
Script completed.
```

Files

Table 30: Files: import on page 180 shows the files for the `import` command.

Table 30: Files: import

Filename	Type	Location
`<filename>`	Download file	`/var/TKLC/lsms/free/data/npacftp/<region>`
`<filename>_FAILED`	Error file, created if errors occur during import. If the -c option was not specified, the file will contain at most one entry.	`/var/TKLC/lsms/free/data/npacftp/<region>`
`<filename>-<spid>`	Response file	`/var/TKLC/lsms/free/data/npacftp/<region>`

Error Messages

Table 31: Error Messages: import

Exit Code	Message	Cause	Suggested Recovery
7	• Delete process failed for `BulkLoadFile : retCode` • Delete process failed for `BulkLoadFile : delete coredump from signal SigValue`	Delete utility failed	Contact the Tekelec Customer Care Center.
8	• Download process failed for `BulkLoadFile : retCode` • Download process failed for `BulkLoadFile : dnld coredump from signal SigValue`	DNLD utility failed	Contact the Tekelec Customer Care Center.

Exit Code	Message	Cause	Suggested Recovery
99	`Insufficient arguments Usage: import <region> [<filename>...] where <region> is the name of the NPAC region database: Canada, Midwest, MidAtlantic, Northeast, Southeast, Southwest, Western, WestCoast <filename> name of the NPAC download file: SPID .dd-mm-yyyyhhmmss LRN .dd-mm-yyyyhhmmss NPANXX .dd-mm-yyyyhhmmss npanxx-npanxx.dd-mm-yyyyhhmmss`	Invalid number of parameters supplied	Try the command again with correct syntax.
1	`Invalid NPAC Region. Usage: import <region> [<filename>...] where <region> is the name of the NPAC region: database: Canada, Midwest, MidAtlantic, Northeast, Southeast, Southwest, Western, WestCoast <filename> name of the NPAC download file: SPID.dd-mm-yyyyhhmmss LRN.dd-mm-yyyyhhmmss NPANXX.dd-mm-yyyyhhmmss npanxx-npanxx.dd-mm-yyyyhhmmss`	Invalid NPAC region supplied	Supply valid region name for command.
2	LSMS_DIR environment variable is not set/defined.	LSMS_DIR environment variable is not set	Verify the environment variables or contact the Tekelec Customer Care Center.
9	`/var/TKLC/lsms/free/data/npacftp/<region>` does not contain any download files.	NPAC directory for `<region>` does not contain any download files	No action necessary.
3	`/var/TKLC/lsms/free/data/npacftp/<region>` NPAC directory does not exist.	NPAC FTP directory for `<region>` cannot be located	Contact the Tekelec Customer Care Center.
5	The npacagent process is currently running for the <region> region. It must be stopped prior to importing by executing the following command: **`$LSMS_DIR/lsms stop <region>`**	The `npacagent` process is running for specified region	Stop the `npacagent` process for this region and try the command again.

keyutil

Process Keys

Allows user to view security key status, load keys, or delete keys for NPAC associations.

Keyword

`keyutil`

Permission

The user must be logged in with the user name `lsmsadm`.

Syntax

```
$LSMS_TOOLS_DIR/keyutil -r <region> -k {public|private} [-d] [-l
<filename>] [-x <listid>] [-s <listid>, <keyid>] [-y]
```

Required Flags

`-r <region>` Perform the function specified by another option for keys for the specified region, where `<region>` has one of the following values:

```
Canada
Midwest
MidAtlantic
Southeast
Southwest
Northeast
Western
WestCoast
```

`-k {public|private}` Perform the function specified by another option for keys of either public type or private type.

One of the following options must be specified:

`-d` Display all keys.

`-l <filename>` Load keys from the specified `<filename>`.

`-x <listid>` Delete keys in the specified list.

`-s <listid>, <keyid>` Set the active key. All private keys for the specified region that occur in the specified list before the specified key are expired; all private keys for that region that occur in the specified list after the specified key are made valid.

Optional flags:

-y Make changes without prompting.

Sample Output

```
$ keyutil -r Midwest -k public -l ../../TKLC.1.public.key

Customer ID: TKLC
List ID: 1
Ok to make changes? y
$
```

Related Commands

None.

Response Notes

None.

Possible Errors

Table 32: Error Messages: keyutil

Exit Code	Error Message	Cause	Suggested Recovery
-1	SyntaxError	The command was entered with incorrect syntax.	Try the command again with correct syntax.
1	FileError	The key file to be opened could not be found.	Verify the file path. If necessary, correct the path and try the command again. If the problem persists, contact the Tekelec Customer Care Center.
2	SaidNo	User answered no when prompted for changes.	No action necessary.
3	NoKeysFound	User specified keys to delete, but those keys were not found.	Contact the Tekelec Customer Care Center.
4	DbError	Database exception occurred; contact Tekelec.	Contact the Tekelec Customer Care Center.

Exit Code	Error Message	Cause	Suggested Recovery
5	`InvalidUser`	A user who is not `lsmsadm` attempted to run this command.	Contact the Tekelec Customer Care Center
6	`UnknownError`	Not known.	Contact the Tekelec Customer Care Center.

lsms

NPAC Agent Control

Lets you start, stop, or display status of an instance of the NPAC Agent for a particular region.

Keyword

`lsms`

Permission

The user must be logged in with the user name `lsmsadm`.

Restrictions

Do not start an NPAC agent unless you have already created a regional database for it (see *npac_db_setup* on page 202).

Syntax

```
$LSMS_DIR/lsms <Action> <Region>
```

Options

None.

Parameters

`Action` Function to perform on `npacagent` process. This is a mandatory parameter with the following values:

```
start
stop
status
```

`Region` NPAC region associated with this `npacagent` process. This is a mandatory parameter with the following values:

```
Canada
```

```
Midwest
MidAtlantic
Southeast
Southwest
Northeast
Western
WestCoast
```

Sample Output

```
# Stop the NPAC Agent for the Canada NPAC
$ $LSMS_DIR/lsms stop Canada
Checking if npacagent is running....Yes.

Stopping npacagent....
OK.

npacagent stopped:   Wed Nov 30  16:28:26 2005

Command complete.
$
# Verify that NPAC Agent has terminated
$ $LSMS_DIR/lsms status Canada
Checking if npacagent is running. .. .No.
Command Complete.
# Restart the NPAC Agent for the Canada NPAC
>
$ $LSMS_DIR/lsms start Canada
Checking if npacagent is already running....No

Starting npacagent....

Verifying....OK.

npacagent started:   Wed Nov 30  16:29:45 2005
```

```
Command complete.
```

Possible Errors

Table 33: Error Messages: lsms

Exit Code	Message	Cause	Suggested Recovery
1	`Checking if npacagent is already running....Yes. npacagent is already running`	Operator tried to start `npacagent` when it was already running	No action necessary.
1	`Checking if npacagent is running....No. npacagent is not running.`	Operator tried to stop `npacagent` when it was already stopped	No action necessary.
3	`lsms: bind: errornumber`	Attempt to bind UDP socket failed. *errornumber* is the error returned by bind.	Contact the Tekelec Customer Care Center.
3	`lsms: exec: errornumber`	Attempt to exec `npacagent` process failed. *errornumber* is the error returned by exec.	Contact the Tekelec Customer Care Center.
1	`lsms: Failed to start npacagent`	Execution of `npacagent` failed	Contact the Tekelec Customer Care Center.
1	`lsms: Failed to stop npacagent`	Attempt to stop `npacagent` failed	Contact the Tekelec Customer Care Center.
2	`lsms:LSMS_DIR is not defined`	LSMS_DIR environment variable is not set	Verify the environment variables.
3	`lsms: send: errornumber`	Attempt to send command to agent failed. *errornumber* is the error returned by send.	Contact the Tekelec Customer Care Center.
3	`lsms: socket: errornumber`	Attempt to open UDP socket failed. *errornumber* is the error returned by socket.	Contact the Tekelec Customer Care Center.

Exit Code	Message	Cause	Suggested Recovery
2	`npacagent: Permission denied for npacagent or executable not found.`	Operator does not have permission to execute this command or executable could not be found. The operator must be an `lsmsadm` user.	Change user to `lsmsadm` or `lsmsall` and try the command again. If the error persists, contact the Tekelec Customer Care Center.

2	`Unknown region ==>< region name > must be one of the following:`
	`Canada`
	`MidAtlantic`
	`Midwest`
	`Northeast`
	`Southeast`
	`Southwest`
	`WestCoast`
	`Western`
		Invalid NPAC region specified	Try the command again with a valid region name.

2	`Usage: lsms [ start | stop ] <region>`	Invalid action specified	Try the command again with correct syntax.

lsmsdb

Database Maintenance Utility

The LSMS Database Command-Line Utility (a MySQL client), `$LSMS_TOOLS_DIR/lsmsdb`, provides the capability of obtaining information and performing maintenance operations on the LSMS database. Additionally, the `lsmsdb` command is used to provide information and perform operations to configure query servers.

The syntax for lsmsdb as used within this document is as follows:

Keyword

`lsmsdb`

Permission

The user can be `root` or be defined as a member of the primary group `lsms`.

Syntax

```
$LSMS_TOOLS_DIR/lsmsdb -c <command> [-b <basedir>] [-d <database>] [-h
<hostname>] [-p <password>] [-u <username>]
```

-c <*command*> Options

adduser Creates TPD and MySQL users, both with the same password. Must be run as root.When the `adduser` command option is specified, the `-u <username>` option is required.

addrepluser Sets up a special replication user at the LSMS with privileges and permission that a query server can use to access the LSMS and perform database replication. When the `addrepluser` command option is specified, the `-h <hostname>` and `-p <password>` options are required. SECURITY NOTE: The combination of username and password is unique to replication use and only provides read access to the resynchronization binary log on the LSMS system. Additionally, access to this user account is restricted to the hostname specified. maximum number of supported EAGLE 5 ISSs from the LSMS. If the maximum number of EAGLE 5 ISSs supported would be exceeded, the command terminates with the following error:

```
"Failed: The maximum number of eagles supported has been reached."
```

chguserpw Allows modification of the TPD and MySQL passwords. Can be run as root, or as the user who wants to change the password. When the `chguserpw` command option is specified, the `-u <username>` option is required.

Note: The `lsmsdb - c chguserpw - u <username>` command must be run on both the primary and the secondary servers to completely change the password.

counts Displays counts of records in specified database.

dblist Displays list of databases (if the `-d` option is specified, it is ignored).

features Displays current settings of all optional features.

users Lists all defined LSMS GUI users.

masterstatus Displays status information (log name and position) on the binary log of the master server (LSMS).

ping Pings the `mysql` daemon.

queryservers Displays the connection status of all query servers that are directly connected to the LSMS. The connection status for each query server (denoted by hostname and IP address) is displayed as `Connected`, `Disconnected`, `Not Reachable`, or `Hostname not associated with IP address`.

quickaudit Performs a quick comparison of the number of rows in all of the database tables on both the active and standby servers. It returns "0" if the comparison on the active and standby servers results in a match; it returns various error numbers and error messages if the comparison does not produce a match or if a problem was encountered.

Note: Do not specify this option when the LSMS is performing bulk download. In addition, do not specify this option when any of the following processes are running, due to the possibility of disk space shortage: backups, starting a standby node (to change its state from UNINITIALIZED "INHIBITED" to STANDBY), running the `import` command, and creating query server snapshots. Since

backups can be run automatically, perform the procedure described in *Checking for Running Backups* on page 93 to ensure that no backups are running.

This option:

- Takes about 5 seconds to run.
- Must be run from the active server.
- Checks first to see if the standby server is more than 5 seconds behind the active server; if it is, an error message is generated and quickaudit does not proceed.

rmrepluser Removes a replication user at the LSMS. When the `rmrepluser` command option is specified, the `-h <hostname>` option is required.

rmuser Deletes TPD and MySQL users. Must be run as root. When the `rmuser` command option is specified, the `-u <username>` option is required.

shutdown Stops `mysql` (if the `-d` option is specified, it is ignored).

snapshot Creates a snapshot of the LSMS LNP database to be used to setup query servers and/or for disaster recovery.When the `snapshot` command option is specified, the `-b <basedir>` option is optional.

During the creation of a snapshot of the LSMS LNP database, the following occurs:

- A read lock will be obtained
- Table information is flushed
- Binary logs (if already existing) are removed and a new one started (with log numbered 1)
- MySQL server performs a shutdown
- All LSMS database tables are archived as compressed files, `mysql-snapshot-supDB.tar.gz` and `mysql-snapshot-<regionDB>.tar.gz` (by default in `/var/TKLC/lsms/db`, although the `-b` option changes this base directory)
- MySQL server is restarted
- The read lock is released

start Starts `mysql` (if the `-d` option is specified, it is ignored).

syspwexp Modifies the system level defaul password timeout interval.

usrpwexp Modifies the user level defaul password timeout interval, the `-u <username>` option is required.

Options

-b basedir Base directory for storing snapshots.

-d database Run the command on the database specified by this option. If the `-d` option is not specified, the command is run on all databases.

-h hostname Name of the host.

-p password	User's password.
-u username	LSMS user's username.

Note: The `-c` flag is required.

Sample Input and Output

```
$ ./lsmsdb -c features
```

```
             Y  AFT
             Y  EDR
             Y  ENHANCED_FILTERS
             Y  IP_GUI
            16  MAX_EAGLES
            32  MAX_SPIDS
             8  MAX_USERS
             Y  QUERY_SERVER
             Y  REPORT_GEN
             0  REPORT_GEN_QUERY_ACTIVE
             Y  SNMP
             Y  SPID_SECURITY
             Y  WSMSC
             N  WSMSC_TO_EAGLE
```

```
$ ./lsmsdb -c counts -d NortheastDB
```

```
1 ............. NortheastDB.NumberPoolBlock
1 ............. NortheastDB.ServiceProvLRN
0 ............. NortheastDB.ServiceProvNPA_NXX
0 ............. NortheastDB.ServiceProvNPA_NXX_X
1 ............. NortheastDB.ServiceProvNetwork
39,756 ........ NortheastDB.SubscriptionVersion
```

```
$ $LSMS_TOOLS_DIR/lsmsdb -c addrepluser -h queryserver1 -p password
```

```
$ $LSMS_TOOLS_DIR/lsmsdb -c masterstatus
```

```
Lsmspri-bin.001 73
```

```
$LSMS_TOOLS_DIR/lsmsdb -c queryservers
```

```
queryserver1 (10.25.60.28) Connected
queryserver2 (10.25.60.45) Disconnected
queryserver3 (10.25.60.31) Not Reachable
queryserver4 (Unknown) Hostname not associated with IP address
```

```
$LSMS_TOOLS_DIR/lsmsdb -c rmrepluser -h queryserver1 -p password
```

```
$LSMS_TOOLS_DIR/lsmsdb -c snapshot
```

```
WARNING: For the duration of this command, traffic being sent from the NPAC to
```

```
connected network elements and local LSMS provisioning will be INTERRUPTED.
Do you want to continue? [Y/N] Y
```

lsmsSNMP

SNMP Agent Process Control

Lets you start, stop, or show status of the SNMP Agent process. For more information about the SNMP agent process, see *Understanding the SNMP Agent Process* on page 40.

Keyword

`lsmsSNMP`

Permission

The user must be `root`.

Restrictions

The LSMS_DIR environment variable must be set.

Syntax

```
$LSMS_DIR/lsmsSNMP <Action>
```

Options

None.

Parameters

`Action` Function to perform on the SNMP agent. This is a mandatory parameter with the following values:

`start`
`stop`
`status`

Sample Output

```
 #Stop the SNMP Agent
> $LSMS_DIR/lsmsSNMP stop
LSMS SNMP Agent stopped: Fri Mar 10 09:50:47 2000 #Start the SNMP Agent
 > $LSMS_DIR/lsmsSNMP start
LSMS SNMP Agent started: Fri Mar 10 10:50:47 2000 #Determine the SNMP Agent
status
> $LSMS_DIR/lsmsSNMP status
LSMS SNMP AGENT PROCESS STATUS:
TOTAL SUCCESSFUL TRAP REQUEST= 12
TOTAL FAILED TRAP REQUEST = 2
   == IP-ADDRESS ==   == STATUS ====
```

```
177.88.34.7         Failed
198.77.39.2         Connected
```

Files

Table 34: Files: lsmsSNMP on page 192 shows the files for the `lsmsSNMP` command.

Table 34: Files: lsmsSNMP

Filename	Type	Location
`snmp.cfg`	Configuration file	`/usr/TKLC/plat/etc/snmp`

Possible Errors

Table 35: Exit Codes: lsmsSNMP

Exit Code	Cause	Suggested Recovery
1	Failed operation.	Contact the Tekelec Customer Care Center.
2	Operation not required.	No action necessary.
3	Usage error.	Correct the syntax.
4	Fatal application error	Contact the Tekelec Customer Care Center.
5	Server not active.	Execute the command on the active server.
6	LSMS software not running.	Start the LSMS.
This command is usually run by scripts; scripts should search for exit codes. When the command is run from the command line, the output indicates suggested recovery.		

lsmssurv

Surveillance Monitor Control

Starts, stops, and retrieves the status of the Surveillance Monitor.

The notification output from the Surveillance Monitor is written to Serial Port 1 on each server. The non-active server, whether its state is STANDBY or UNINITIALIZED "INHIBITED", sends surveillance notifications only for platform events that it detects on itself. It also forwards those notifications to the active server.

- The active server sends surveillance notifications for:
  - All platform events that the active server detects on itself
  - All platform notifications received from the non-active server (the active server inserts the hostname of the non-active server before the event text for these notifications)
  - Some applications events (not all application events generate surveillance notifications; for more information, see *Automatic Monitoring of Events* on page 247).

By default, all notification output that is sent to Serial Port 1 on a given server is written also to the log file on that server, `/var/TKLC/lsms/logs/survlog.log`. (See *Files* on page 194.)

Keyword
`lsmssurv`

Permission

The user must be `root` to specify the `start` or `stop` for `<Action>`.

Syntax
```
# $LSMS_DIR/lsmssurv <Action>
```

Options

None.

Parameters

`Action` Specifies the action to be performed on the Surveillance Monitor. This is a mandatory parameter with the following values:

```
start
stop
status
last
```

Sample Output

```
 # Start LSMS Surveillance Process
 # $LSMS_DIR/lsmssurv start
 LSMS Surveillance feature started  # Request LSMS Surveillance Process status
 $ $LSMS_DIR/lsmssurv status
 LSMS Surveillance feature is currently started
LSMS Surveillance feature is currently stopped  # Stop LSMS Surveillance Process

 # $LSMS_DIR/lsmssurv stop
 LSMS Surveillance feature stopped  # Return LSMS Surveillance Process to last
valid state. The following # output indicates that the process ran been running
 prior to termination
```

```
# $LSMS_DIR/lsmssurv last
LSMS Surveillance feature started #
```

Files

Table 36: Files: lsmssurv on page 194 shows the files for the `lsmssurv` command.

Table 36: Files: lsmssurv

Filename	Type	Location
`lsmsSurv.log`	Error/Debug log file	`/var/TKLC/lsms/logs/`
`survlog.log`	Notification log file	`/var/TKLC/lsms/logs/`

Response Notes

The designated response will not occur for five to ten seconds after execution.

Possible Errors

Table 37: Error Messages: lsmssurv

Exit Code	Message	Cause	Suggested Recovery
1	`LSMS Surveillance feature is currently running.`	LSMS Surveillance feature is running	No action necessary.
1	`LSMS Surveillance feature is not currently running.`	LSMS Surveillance feature is not running	No action necessary.
1	`LSMS Surveillance feature did not start successfully Please review log file: /var/TKLC/lsms/logs/lsmsSurv.log for errors`	Socket communication problems, hang on opening of console/serial ports	Contact the Tekelec Customer Care Center.
1	`Must be root to start the LSMS Surveillance feature`	User ID must be root to start the LSMS Surveillance feature	Change user to `root`.

massupdate

SPID Mass Update

The optional mass update utility provides the ability to migrate subscription version, number pool block, and network data from one Service Provider ID (SPID) to another based on an input file downloaded from the NPAC. The mass update utility reads SIC-SMURF files for LRN, NPA-NXX, and NPA-NXX-X, performs the required database updates and, in the case of LRN data, forwards an appropriate Update Override GTT message to the EAGLE 5 ISS.

Keyword
`massupdate`

Permission

The user must be logged in with the user name `lsmsadm`.

Syntax

```
$LSMS_DIR/massupdate [-v] [-p] [-n <npacRegion>] <filename>
```

Note: Stop the `npacagent` process for the region in question when the `-n` option is used. It is not necessary to stop the `npacagent` processes for all eight regions when the `-n` option is used.

Optional flags:

`-v`	Provides verbose output.
`-p`	Perform "pre-check" but make no database updates.
`-n`	Perform the mass update only for the region named by the `<npacRegion>` parameter. Only one NPAC region may be entered after the `-n` option

Parameters

`<npacRegion>`	The name of the region to perform the mass update for.
`<filename>`	The name of the SIC-SMURF file to process.

Note: The filename must be in the following format:

SIC-SMURF-[LRN | NPANXX | NPANXXX].OldSpid.NewSpid.DD-MM-YYYYHH24MISS

Example: `SIC-SMURF-NPANXX.0001.0002.25-12-1996081122`

Sample Output

```
$ $LSMS_DIR/massupdate SIC-SMURF-LRN.1234.9876.15-03-2002121530

One or more npacagents processes are currently running.  They must be
Stopped prior to mass spid updates by executing the following command:
/lsms stop <region>
Massupdate: exiting.
```

```
$ $LSMS_DIR/massupdate SIC-SMURF-LRN.1234.9876.15-03-2002121530

WARNING: The supman, lsman or an eagleagent process is currently running. It is
 recommended that all of these processes be stopped prior to mass spid updates
to prevent modifications of GTT data during execution of this command.
Do you wish to continue [N]?
Massupdate: exiting.
```

```
$ $LSMS_DIR/massupdate -v SIC-SMURF-LRN.1234.9876.15-03-2002121530

Using SIC-SMURF File: SIC-SMURF-LRN.1234.9876.15-03-2002121530
Performing Mass Update of SPIDs for LRN data...
Updating LRN 2223334000 from SPID 1234 to SPID 9876...
5 OverrideGtt object(s) updated in supported database
1 ServiceProvLRN object(s) updated in Southeast region
4 NumberPoolBlock object(s) updated in Southeast region
Updating LRN 2224441000 from SPID 1234 to SPID 9876...
0 OverrideGtt object(s) updated
1 ServiceProvLRN object(s) updated in Southeast region
10 NumberPoolBlock object(s) updated in Southeast region
Updating LRN 2225550000 from SPID 1234 to SPID 9876...
4 OverrideGtt object(s) updated
0 ServiceProvLRN object(s) updated in Southeast region
4 NumberPoolBlock object(s) updated in Southeast region
```

```
Updating SubscriptionVersion tables (this may take a while)...
790 SubscriptionVersion object(s) updated in Southeast region
Command stats
-------------
Lines processed: 3
Successful:      3
Failed:          0
Command complete.
$
```

```
$ $LSMS_DIR/massupdate -p SIC-SMURF-LRN.TKLC.SP05.06-30-2004101010
```

```
WARNING: The supman, lsman or an eagleagent process is currently running. It is
 recommended that all of these processes be stopped prior to mass spid updates
to prevent modifications of GTT data during execution of this command.
Do you wish to continue [N]? Y

START Mass update command: Thu Nov  8 13:41:57 EST 2007

Precheck mode: Makes NO CHANGES, but reports everything as if updating.

Executing mass update for all regions...
 {Precheck only}
Reading SIC-SMURF File: SIC-SMURF-LRN.TKLC.SP05.06-30-2004101010

Performing Mass Update of SPIDs for LRN data... {Precheck only}

Command stats {Precheck only}
-------------
Lines processed: 1
Successful:      1
Failed:          0

Mass update command complete: Thu Nov  8 13:41:57 EST 2007
```

Table 38: Tables/Fields Affected By SIC-SMURF Processing on page 197 identifies the database tables and fields that are updated after invoking `massupdate` for the various SIC-SMURF files.

For each table/field that is affected, the field that is checked for a match is listed under the appropriate SIC-SMURF filename. Under the Table/Field column, the database containing the object to be updated (for example, SupDB), the table to be updated (for example, OverrideGTT), and the field to be updated (for example, spid) are listed.

Under each SIC-SMURF file type, the field to be used for the match (for example, lrn) is listed for each Table/Field impacted by the update. For example, for LRN SIC-SMURF files, the SupDB OverrideGTT table's spid is updated if the lrn is matched.

Table 38: Tables/Fields Affected By SIC-SMURF Processing

Table/Field	LRN SIC-SMURF	NPA-NXX SIC-SMURF	NPA-NXX-X SIC-SMURF
supDB.OverrideGtt.spid	lrn		
supDB.LsmsServiceProvider.spid (create if required)	spid		
supDB.GttGroupSpid.spid (create if required)	spid		

Table/Field	LRN SIC-SMURF	NPA-NXX SIC-SMURF	NPA-NXX-X SIC-SMURF
<regionDB>.ServiceProvLRN.serviceProviderId	lrn		
<regionDB>.ServiceProvNPA_NXX.serviceProvId		npanxx	
<regionDB>.ServiceProvNPA_NXX_X.service-ProvId			npanxx_x
<regionDB>.ServiceProvNetwork.serviceProvId (create if required)	spid	spid	spid
<regionDB>.SubscriptionVersion.newCurrentSp	lrn		
<regionDB>.NumberPoolBlock.newCurrentSp	lrn		

If an Override GTT entry is modified and there is no LSMS Service Provider with the NewSpid, then one is created. If that LSMS Service Provider SPID is not a member of the GTT group for a modified Override GTT, then that membership is added by creating a GTT Group SPID table entry.

If a ServiceProvLRN, ServiceProvNPA_NXX, or ServiceProvNPA_NXX_X object is modified and there is no ServiceProvNetwork object with the NewSpid, then one is created.

LsmsServiceProvider Limit

The mass update utility creates LsmsServiceProvider objects, if needed, even if creating them exceeds the maximum number of SPIDs supported (as recorded in the MAX_SPIDS field in the DbConfig entry.) However, the fact that the limit has been exceeded is recorded in the log file and the limit remains in force otherwise.

Mass Update Log File

To record information or errors during the mass update or the precheck, the mass update utility appends to a log file named `massupdate.log.MMDD`, located in the `$LSMS_DIR/../logs/massupdate` directory. The `.MMDD` suffix is the month and day the massupdate excution begins. If the massupdate runs past midnight, it will keep all output from one massupdate execution in one file, so the file will not be split across days but continue in the same file it started in. The following information is written to the log file by the mass update utility:

- The path name of the mass update input file being used
- The time and date for the start and stop of utility execution
- Identifying information for all automatically created objects, whether ServiceProvNetwork or LsmsServiceProvider, including the adding of a (possibly already existing) LsmsServiceProvider to a GttGroup and noting if a newly created LsmsServiceProvider is over the MAX_SPIDS limit
- Identifying information for any LsmsServiceProvider objects that are no longer used in any OverrideGtt as a result of the mass update and therefore could be removed

- Output from the precheck
- Any kind of processing problem or error
- A summary showing the number of lines actually processed successfully for each invocation of the utility (not needed for precheck mode)

Error Codes

Table 39: Error Codes: massupdate

Error Code	Cause	Suggested Corrective Action
0	Success	None required.
1	Command syntax error	Rerun the command with the proper syntax.
2	Feature not enabled	Enable optional feature.
3	SIC-SMURF file not found	Verify path and filename for SIC-SMURF file.
4	Unable to open SIC-SMURF file	Verify permissions on SIC-SMURF file.
5	Incorrect file format	Supply valid SIC-SMURF file for processing.
6	massupdate already running	Do not attempt to execute more than one massupdate process at the same time.
7	npacmassupdate executable not found	Define environment variable LSMS_DIR or contact the Tekelec Customer Care Center.
8	Database error	Make sure the database server is running.
9	User chose to stop	None needed.
10	`npacagent` running	If massupdate is run for all regions, stop all `npacagent` processes. If massupdate is run for a single region, stop the `npacagent` for that region only.

Error Code	Cause	Suggested Corrective Action
11	Unable to write	Remove `<filename>_FAILED` file and verify directory permissions.
12	Invalid user	Rerun as user `lsmsadm`.

measdump

Print Measurement Information

Lets you print measurement information (contained in databases) to the display.

Keyword
`measdump`

Permission

The user must be logged in with the user name in the `lsmsuser`, `lsmsuext`, `lsmsview`, or `lsmsall`, group.

Syntax
`$LSMS_TOOLS_DIR/measdump {-r <region>|-c <CLLI> [-n]`

Required Flags

Specify one of the following flags:

`-r <region>` NPAC region associated with this `npacagent` process. This is a mandatory parameter with the following values:

```
Canada
Midwest
MidAtlantic
Southeast
Southwest
Northeast
Western
WestCoast
```

`-c <CLLI>` Common Language Location Identifier for the network element for which you wish to display measurements.

Optional Flags

Optionally specify one of the following flags:

-l Lets you create measurement logs (a <region>.meas.<MMDD> file for each NPAC region and a <clli>.meas.<MMDD> file for each network elements) for compatibility with previous releases of the LSMS.

-n Number of days before current day for which measurements are to be displayed, where n can have one of the values shown in *Table 40: Measurement Pegs Date* on page 201 (if this option is not specified, the default value is 0):

Table 40: Measurement Pegs Date

Value	Print Measurement Pegs for the Date of:
0	Today
1	Yesterday
2	Two days before current date
3	Three days before current date
4	Four days before current date
5	Five days before current date
6	Six days before current date

Sample Output

```
$ measdump -r Midwest -2

measdump: There is no measurement data available for the requested day.

$ measdump -r Midwest

Hour     Binds     SuccessOps     FailedOps
   0         0              0             0
   1         0              0             0
   2         0              0             0
   3         0              0             0
   4         0              0             0
   5         0              0             0
   6         0              0             0
   7         0              0             0
   8         0              0             0
   9         0              0             0
  10         1              0             0
  11         0              0             0
  12         0              0             0
  13         0              0             0
  14         0              0             0
  15         0              0             0
  16         0              0             0
  17         0              0             0
```

```
18          0               0               0
19          0               0               0
20          0               0               0
21          0               0               0
22          0               0               0
23          0               0               0
```

Possible Errors

Table 41: Error Messages: measdump

Exit Code	Error Message	Cause	Suggested Recovery
-1	`Syntax error`	User entered command with incorrect syntax.	Try the command again with the correct syntax.
1	`DbError`	Database exception. Contact Tekelec.	Contact the Tekelec Customer Care Center.
2	`EnvNotSet`	The LSMS_DIR env variable is not set.	Verify the environment variables.
3	`NoData`	No measurement data available for the specified day (the agent was never started)	No action necessary.
4	`UnknownError`	Not known.	Contact the Tekelec Customer Care Center.

npac_db_setup

NPAC Database Maintenance

Creates or removes the regional NPAC database.

Keyword
`npac_db_setup`

Permission

The user must be logged in with the user name `lsmsadm`.

Restrictions

- This command must be run on each server.
- If a database is in use by a regional LSMS agent, it cannot be removed.

- If a regional database has already been created, it must be removed before it can be created again.

Syntax

```
$LSMS_DIR/npac_db_setup <Action> <Region>
```

This command must be run from the $LSMS_DIR directory and run only from the primary server.

Options

None.

Parameters

`Action` Specifies the action to be performed on the database. This is a mandatory parameter with the following values:

```
create
remove
```

`Region` NPAC region associated with this `npacagent`. This is a mandatory parameter with the following values:

```
Canada
Midwest
MidAtlantic
Southeast
Southwest
Northeast
Western
WestCoast
```

Sample Output

Create NPAC database for Canada region for the first time

```
> $LSMS_DIR/npac_db_setup create Canada
```

```
------------------------------------------------------------------------
Npac Region Database Setup Script
The Region Database Name is CanadaDB
Initializing regional database...CanadaDB
The regional database CanadaDB was created successfully.
>
```

```
> $LSMS_DIR/npac_db_setup remove Northeast
```

Remove NPAC database for Northeast Region

```
------------------------------------------------------------------------
Npac Region Database Setup Script
The Region Database Name is NortheastDB
Warning: NPAC region database CanadaDB is about to be removed.
```

```
  All data in the database will be lost.

  Do you want to continue? [Y/N]Y
Removing regional database...CanadaDB
>
```

Response Notes

This command takes approximately 35 to 40 seconds to execute.

Possible Errors

Table 42: Error Messages: npac_db_setup

Exit Code	Cause	Suggested Recovery
1	Syntax was incorrect	Use correct syntax.
2	MySQL command failed	Contact Tekelec.
7	User attempted to create a database that already exists	None needed.
9	User attempted to remove a database that is in use	Stop indicated processes before attempting to remove the database.
10	The root user cannot execute this command	Change users to `lsmsadm`.
12	User attempted to remove database for an active region	Make region inactive and retry command.

npacimport

Import Specific Files into a Regional Database

Allows user to import specific files into the regional NPAC database.

Keyword
`npacimport`

Permission

The user must be logged in with the user name `lsmsadm`.

Restrictions

This command must be run from the $LSMS_DIR directory and run only from the primary server.

Syntax

```
$LSMS_TOOLS_DIR/npacimport [-h] -r <region> -i <type> [-u] [-y] [-t
<number>] [-c <number>] <filename>
```

Required Flags

`-r <region>` Specifies the region whose database the imported files are intended for. This is a mandatory parameter with the following values:

```
Canada
MidAtlantic
Midwest
Northeast
Southeast
Southwest
WestCoast
Western
```

`-i <type>` Specifies the type of the file to be imported into the database. This is a mandatory parameter with the following values:

```
SubscriptionVersion
NumberPoolBlock
ServiceProvNetwork
ServiceProvLRN
ServiceProvNPA-NXX
ServiceProvNPA-NXX-X
```

Parameters

`<filename>` Specifies the input file of pipe delimited records to be used.

Optional Flags

`-h` Display Help text and quit.

`-u` Time-range update: May modify or delete and does not purge object range first. Not valid for ServiceProvNetwork.

`-y` Continue on if a record update fails.

`-t` Specify number of threads to use (maximum number is 10).

`-c` Specify number of records in each batch to a thread (default is 1000).

Exit Codes

Table 43: Exit Codes: npacimport on page 206 lists the exit codes generated by the `npacimport` command.

Table 43: Exit Codes: npacimport

Exit Code	Cause	Suggested Recovery
-1	Invalid syntax	Correct the syntax.
1	Database error	Contact the Tekelec Customer Care Center.
2	File access error	Contact the Tekelec Customer Care Center.
3	Invalid record in the input file	Correct the file entry or contact the Tekelec Customer Care Center.
4	Invalid user	Change user to `lsmsadm`.
5	Unknown error	Contact the Tekelec Customer Care Center.
This command is usually run by scripts; scripts should search for exit codes. When the command is run from the command line, the output indicates suggested recovery.		

report

Report Generation

Generates reports for regional NPAC databases and supplemental databases.

Keyword

`report`

Permission

The user must be defined as a member of the primary group `lsms`.

Syntax

```
$LSMS_DIR/report <OutputFile> <ReportType>
[<SP>|<LRN>|<DPC>|<Region>|<SplitStatus>] [<StartTN>] [<EndTN>]
[<StartNPB>] [<EndNPB>]
```

Options

None.

Parameters

OutputFile The filename for the file in which to store the report. This is a mandatory parameter whose value is the filename. The filename is appended with the value specified for <ReportType> and the file is stored in the directory where the command is run.

ReportType The type of report to create. This is a mandatory parameter; use one of the following values:

SPA - Service Provider Administrative Report

SPN - Service Provider Network Report

EMR - Element Management Report

6DT - Six Digit Translation Report

10DT - Ten Digit Translation Report

SPL - NPA Split Data by Status Report

SBL - Subscription Report by LRN

SBS - Subscription Report by Service Provider ID

SBT - Subscription Report by TN

NBL - Number Pool Block Report by LRN

NBS - Number Pool Block Report by Service Provider ID

NBN - Number Pool Block Report by NPA-NXX-X

SPD - Service Provider Data Report

SP Four-character alphanumeric string to specify Service Provider ID. This is a mandatory parameter when <ReportType> is set to SBS or NBS; optional when <ReportType> is set to 6DT, 10DT, EMR, or SPN; otherwise not allowed.

LRN Ten-digit string (values 0000000000–9999999999) to specify Location Routing Number. This is a mandatory parameter when <ReportType> is set to SBL or NBL; otherwise not allowed.

DPC Eleven-character string of format xxx-xxx-xxx (where each xxx can have a value 000 to 256) to specify Destination Point Code. This is an optional parameter when <ReportType> is set to 6DT or 10DT; otherwise not allowed.

Region NPAC region. This is an optional parameter when <ReportType> is set to SPL; otherwise not allowed. Use one of the following values:

MidAtlantic

```
Midwest
Northeast

Southeast

Southwest

Western

Westcoast

Canada
```

SplitStatus NPA-NXX split status. This is an optional parameter when <ReportType> is set to SPL; otherwise not allowed. Use one of the following values:

```
Active

Pending

Error
```

StartTN Starting telephone number in a range of telephone numbers. This is a mandatory parameter when <ReportType> is set to SBT. Valid values are 10 digits from 0000000000 to 9999999999.

EndTN Ending telephone number in a range of telephone numbers. This is a mandatory parameter when <ReportType> is set to SBT. Valid values are 10 digits from 0000000000 to 9999999999.

StartNPB Starting value in a range of number pool blocks. This is a mandatory parameter when <ReportType> is set to NBN. Valid values are 7 digits from 0000000 to 9999999.

EndNPB Ending value in a range of number pool blocks. This is a mandatory parameter when <ReportType> is set to NBN. Valid values are 7 digits from 0000000 to 9999999.

Sample Commands

```
 # Generate SPA report for MidAtlantic NPAC
 $ $LSMS_DIR/report MidAtlanticDB supDB report.output SPA
   # Generate SBL report for MidAtlantic NPAC for LRN 9194605500
 $ $LSMS_DIR/report MidAtlanticDB supDB report.output SBL 9194605500
 # Generate SPL report
> $LSMS_DIR/report MidAtlanticDB supDB report.out SPL
# Generate SBS report for Midwest NPAC for all Subscriptions having a service
provider of TKLC and a TN in the range of 9194600000 to 9195600000
$ $LSMS_DIR/report MidwestDB supDB report.out SBS TKLC 9194600000 9195600000
# Generate SBT report for Western NPAC for all Subscriptions having a TN in the
 range of 9194600000 to 9195600000
$ $LSMS_DIR/report WesternDB supDB report.out SBT 9194600000 9195600000
```

Files

Table 44: Files: report on page 209 shows the files for the report command.

Table 44: Files: report

Filename	Type	Location
`Output`	Report Output File	Directory where command is run

Response Notes

The `report` command can process approximately 300-500 records per second, depending upon the type of report.

To view the report, change directory to the directory where the command was run and use any text editor to open the file named in the command. If you run the command from the `$HOME/LSMSreports` directory, you can also view the report through the graphical user interface; for information, refer to the LSMS Database *Administration Manual*.

Possible Errors

Table 45: Error Messages: report

Exit Code	Message	Cause	Suggested Recovery
1	`DATABASE <name> NOT FOUND`	Specified database could not be found	Verify that the database exists and try the command again.
1	`disk space check failed`	Attempt to check available disk space failed	Remove unnecessary reports from disk.
1	`End TN must be greater than Start TN value.`	The start TN is greater than the end TN in the range of TNs to generate an LSMS subscription report	Try the command again using the correct syntax and supplying all required arguments.
1	`Insufficient disk space available to generate report. N bytes of disk space required: n bytes of disk space available`	Insufficient disk space to save report	Remove unnecessary reports from disk.
1	`Invalid End TN value - <EndTN>`	The last TN in the range of TNs to generate an LSMS subscription report is out of range. The valid range of values for a telephone number is 0000000000...9999999999.	Try the command again using the correct syntax and supplying all required arguments.
1	`Invalid Report Type Specified <Report Type>`	The value specified for the ReportType parameter is not valid.	Try the command again using the correct syntax and supplying all required arguments.
1	`Invalid Start TN value - <StartTN>`	The first TN in the range of TNs to generate an LSMS subscription report is out of range. The valid range of values for a telephone number is 0000000000...9999999999.	Try the command again using the correct syntax and supplying all required arguments.
1	`LRN argument is required for SBL/NBL`	If <ReportType> parameter is specified as	Try the command again using the correct syntax

Exit Code	Message	Cause	Suggested Recovery
	`report`	SBL or NBL, the <LRN> parameter must also be specified	and supplying all required arguments.
3	`LRN argument must be exactly 10 numeric digits`	An <LRN> parameter that had less than 10 digits, more than 10 digits, or non-numeric characters was specified	Try the command again using the correct syntax and supplying all required arguments.
1	`Missing mandatory arguments`	The command was specified with an insufficient number of arguments.	Try the command again using the correct syntax and supplying all required arguments.
1	`NO ACCESS RIGHTS TO DATABASE`	Requesting operator does not have access rights to the database	Change user to a username that has access rights to the database.

Exit Code	Message	Cause	Suggested Recovery
4	`Service Provider argument must have from 1 to 4 characters`	The <SP> parameter was specified with more than 4 characters	Try the command again using the correct syntax and supplying all required arguments.
1	`Service Provider argument required for SBS/NBS report`	If <ReportType> parameter is specified as SBS or NBS, the <SP> parameter must also be specified	Try the command again using the correct syntax and supplying all required arguments.
1	`StartNPB argument is required for NBN report`	If <ReportType> parameter is specified as NBN, the <StartNPB> parameter must also be specified	Try the command again using the correct syntax and supplying all required arguments.
1	`StartTN argument is required for SBT report`	If <ReportType> parameter is specified as SBT, the <StartTN> parameter must also be specified	Try the command again using the correct syntax and supplying all required arguments.
1	`Unable to determine home directory of user - report could not be generated`	Report could not be stored in home directory of user	Contact the Tekelec Customer Care Center.
1	`Unable to open <filename> - report could not be generated`	Could not open the file in which to save the report	Contact the Tekelec Customer Care Center.
1	`Usage: report <regional_database_name sup_database_name> output file <report_type>[LRN|SP]`	Operator did not supply the correct number of arguments	Try the command again using the correct syntax and supplying all required arguments.
1	`Wrong number of arguments for Split report`	The <ReportType> parameter was specified as SPLA or SPLR, but the wrong number of parameters was specified	Try the command again using the correct syntax and supplying all required arguments.

resync_db_setup

Resynchronization Database Maintenance

Creates or removes the resynchronization database.

Keyword
`resync_db_setup`

Permission

The user must be logged in with the user name `lsmsadm`.

Restrictions

- This command must be run on each server.
- If the resynchronization database has already been created, it must be removed before it can be created again.

Syntax
`$LSMS_DIR/resync_db_setup <Action>`

This command must be run from the $LSMS_DIR directory and run only from the primary server.

Options

None.

Parameters

`Action` Specifies the action to be performed on the database. This is a mandatory parameter with the following values:

```
create
remove
```

Response Notes

This command takes approximately 35 to 40 seconds to execute.

Files

None.

Possible Errors

Table 46: Exit Codes: resync_db_setup

Exit Code	Cause	Suggested Recovery
1	Missing arguments.	Use the correct syntax and supply all required arguments.

Exit Code	Cause	Suggested Recovery
3	Executing command from wrong directory.	Change directory to $LSMS_DIR.
6	Invalid action argument.	Use the correct syntax and supply a valid action argument.
7	Database already exists.	No action necessary.
8	Database exists on another host.	No action necessary.
9	Database in use by process.	Stop the process that is using the database.
10	User is not authorized to use this command.	Change user to `lsmsadm`.
11	Command executed on secondary server.	Execute command on the primary server.
This command is usually run by scripts; scripts should search for exit codes. When the command is run from the command line, the output indicates suggested recovery.		

SAagent

Service Assurance Agent Control

Starts, stops, inhibits automatic restart, allows automatic restart, and retrieves the status of the Service Assurance Agent.

The SA Agent can be prevented from starting by inhibiting the process. This action allows you to control whether or not the Surveillance feature automatically starts the agent when it detects that it is not running.

NOTE: If the SA agent is running, the inhibit action does not take effect until the agent has stopped.

Keyword
`SAagent`

Permission

The user must be defined as a member of the secondary group `lsmsadm`.

Syntax

```
$LSMS_DIR/SAagent <Action>
```

Options

None.

Parameters

`Action` Specifies the action to be performed on the Service Assurance Agent. This is a mandatory parameter with the following values:

`start`

`stop`

`inhibit`

`allow`

`status`

Sample Output

```
#  Start the process
 $ $LSMS_DIR/SAagent start
 Checking if SA Agent is already running...No Starting SA
Agent...Started...Verifying... SAagent started:   1997 Sept 04  12:13:14 EST  #
 Stop the process, allow Surveillance to restart it.
 $ $LSMS_DIR/SAagent stop
 Checking if SA Agent is already running...Yes Stopping SA Agent... SAagent
stopped:   1997 Sept 04  12:13:24 EST  # Stop the process but keep Surveillance
 or the user from starting it. # This case assumes it was stopped.
 $ $LSMS_DIR/SAagent inhibit
 Saagent inhibited: 1997 Sept 04  12:13:34 EST  # Now restart the process after
 it had be inhibited.
 $ $LSMS_DIR/SAagent allow
 Saagent allowed:   1997 Sept 04  12:13:44 EST $ $LSMS_DIR/SAagent start Checking
 if SA Agent is already running...No Starting SA Agent...Started...Verifying...
 SAagent started:   1997 Sept 04  12:13:45 EST  # Request status
 $ $LSMS_DIR/SAagent status
 Checking if SA Agent is already running...Yes
SA Agent: GPL=012-000-000  : mem= 5176 kbytes : pcpu = 0.0 % TOTAL QUERIES=0
         : TOTAL TNs=0

THERE ARE CURRENTLY NO SERVICE ASSURANCE ASSOCIATIONS
```

Files

Table 47: Files: SAagent on page 216 shows the files for the `SAagent` command.

Table 47: Files: SAagent

Filename	Type	Location
`sa.cfg`	Configuration file	`$LSMS_DIR/config`

Command Usage

Table 48: SAagent Command Usage on page 216 gives several examples of typical command usage sequence.

Table 48: SAagent Command Usage

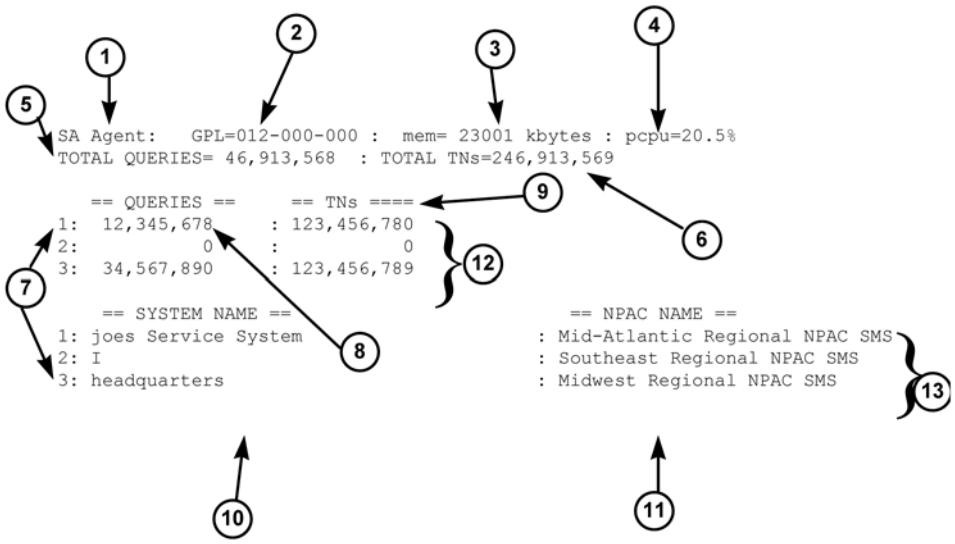
Case	Action	Command Sequence
1	Start the process.	`$LSMS_DIR/SAagent start`
2	Stop the process, allow Surveillance to restart it.	`$LSMS_DIR/SAagent stop`
3	Stop the process but keep Surveillance or the user from starting it. This case assumes it was already started.	`$LSMS_DIR/SAagent stop` `$LSMS_DIR/SAagent inhibit`
4	Start the process after it was stopped as in Case #3.	`$LSMS_DIR/SAagent allow` `$LSMS_DIR/SAagent start`

Understanding Status Output

The association status shows each association established for that pairing. The association is designated with a number (1..4) in the left-most column. The number is a tag to coordinate with the statistics that precede the association status.

Figure 82: Example of SA Agent Status Output on page 216 shows an example in which there are three active associations. The first is handling 10 TNs per query, the second is associated but no traffic has been sent across the interface, and the third is handling an average of 3.5 TNs per query.

Figure 82: Example of SA Agent Status Output



The following numbered items correspond to the numbers in *Figure 82: Example of SA Agent Status Output* on page 216:

1. Name of the process (SA Agent)
2. GPL number of the SA Agent process
3. Number of bytes used by the SA Agent process, in kilobytes as decimal number
4. Ratio of the CPU time used by the SA Agent to the CPU time available during the same time period
5. Total number of queries received by the SA Agent since it was last started
6. Total number of TNs in the queries
7. Tag that correlates the association statistics to the System Name and the NPAC database to which it is connected. Only the systems that are currently associated are shown
8. Total number of queries received by the SA Agent on that association since the association was established
9. Total number of TNs received by the SA Agent on that association since the association was established
10. SystemName of SA Manager
11. lnpNPAC-SMS-Name
12. Association statistics block. Values of zero indicate that no queries or TNs have been sent across the association.
13. Association status

The examples below show the status as the user sees it when the SA Agent is in various conditions. *Figure 83: Example -- No Associations Status Output* on page 217 shows the SA Agent running without any associations.

Figure 83: Example -- No Associations Status Output

```
Checking if SA Agent is running....Yes.

SA Agent: GPL=012-000-000    : mem= 5176 kbytes : pcpu = 0.0 %
TOTAL QUERIES=0              : TOTAL TNs=0

THERE ARE CURRENTLY NO SERVICE ASSURANCE ASSOCIATIONS
------------------------------------------------------------------------
```

Figure 84: Example -- Marked Inhibited Status Output on page 218 shows example output that indicates that the SA Agent was inhibited after it was started.

Figure 84: Example -- Marked Inhibited Status Output

```
SA agent : is inhibited.
Checking if SA Agent is running....Yes.

SA Agent: GPL=012-000-000    : mem= 5176 kbytes : pcpu = 0.1 %
TOTAL QUERIES=0              : TOTAL TNs=0

THERE ARE CURRENTLY NO SERVICE ASSURANCE ASSOCIATIONS
------------------------------------------------------------------------
```

Figure 85: Example -- Active Associations Status Output on page 218 shows example output that indicates that the SA Agent is inhibited and has active associations.

Figure 85: Example -- Active Associations Status Output

```
SA agent : is inhibited.
Checking if SA Agent is running....Yes.

SA Agent: GPL=012-000-000  : mem= 6904 kbytes : pcpu = 0.6 %
TOTAL QUERIES=16           : TOTAL TNs=15

    == QUERIES ==           == TNs ==
1:            4     :              4
2:            4     :              4
3:            4     :              3
4:            4     :              4


    == SYSTEM NAME ==                          == NPAC NAME ==
0: SAM1                                 : Midwest Regional NPAC SMS
1: SAM2                                 : Southeast Regional NPAC SMS
2: SAM3                                 : Southwest Regional NPAC SMS
3: SAM4_123456789012345678901234567890123 45 : West Regional NPAC SMS
```

Response Notes

It takes 15 seconds to start the SA agent. If the SA agent is not running, the results of a status request will not appear for at least five seconds.

Possible Errors

Table 49: Error Messages: SAagent

Exit Code	Message	Cause	Suggested Recovery
4	`bind: errormsg`	The bind command failed. *errormsg*is the error message.	Contact the Tekelec Customer Care Center.
3	`SA Agent: executable missing`	**sacw** executable could not be found	Contact the Tekelec Customer Care Center.
1	`SA Agent: Failed to start`	Start action failed	Contact the Tekelec Customer Care Center.
1	`SA Agent: Failed to stop SA Agent`	Stop action failed	Contact the Tekelec Customer Care Center.
2	`SA Agent: is already allowed`	Allow action failed since SA Agent is already in Allow state	No action necessary.
3	`SA Agent: is already inhibited`	Inhibit action failed because the SA Agent is already inhibited	No action necessary.
2	`SA Agent is already started`	Could not start SA Agent since it is already executing	No action necessary.
2	`SA Agent is not running`	Status or stop performed when SA Agent was not running	No action necessary.
3	SA Agent: log directory $logdir does not exist	Logfile directory does not exist	Contact the Tekelec Customer Care Center.
3	`SA Agent: LSMS_DIR is not defined`	LSMS_DIR environment variable not set	Verify the environment variables.
3	`SA Agent: Permission Denied`	Cannot start SA Agent because it has been inhibited	Perform `SAagent allow` and then retry this command.

Exit Code	Message	Cause	Suggested Recovery
4	`socket: errormsg`	The socket command failed. *errormsg* is the error message.	Contact the Tekelec Customer Care Center.
3	`Usage: SAagent [ status | start | stop | inhibit | allow ]`	Invalid action specified	Try the command again using the correct syntax.

spidsec

Authorize Users to Access SPIDs

When the SPID Security feature is enabled, this command allows a user logged in as `lsmsadm` to associate specified users to access data belonging to specified Service Provider ID (SPID).

Keyword
`spidsec`

Permission

The user must be logged in with the user name `lsmsadm`.

Syntax
`$LSMS_TOOLS_DIR/spidsec [-h] [-a -r -d] -u <user> -s{<spid>|GOLDEN}`

Required Flags

`-u <user>`	Specify a username that has already been defined on the LSMS (see *Managing User Accounts* on page 62).
`-s {<spid>|GOLDEN}`	Specify a SPID that has been defined (for more information, refer to the LSMS *Configuration Manual*) or specify `GOLDEN` to apply to all defined SPIDs.

One of the following options must be specified:

`-a`	Authorize user for the specified SPID.
`-d`	Display user's authorization information.
`-r`	Remove SPID authorization from given user (optionally specify a username with the `-u` flag; if no username is specified, all usernames that have been defined on the LSMS are displayed).

Sample Output
```
# Display the SPID security for the username lsmsadm
```

```
$ spidsec -d -u lsmsadm

lsmsadm GOLDEN
```

```
# Authorize the username thomas to access the SPID TKLC

$ spidsec -a -u thomas -s TKLC
```

No output is displayed.

```
# Display the SPID security for all usernames

$ spidsec -d

lsmsadm GOLDEN
lsmsall GOLDEN
lsmsuser GOLDEN
lsmsuext GOLDEN
lsmsview GOLDEN
```

thomas TKLC

Related Commands

None.

Possible Errors

Table 50: Exit Codes: spidsec

Exit Code	Cause	Suggested Recovery
-1	Usage error.	Correct the syntax.
1	File access error.	Contact the Tekelec Customer Care Center.
2	Database error.	Contact the Tekelec Customer Care Center.
3	Invalid user.	Change user to `lsmsadm`.
4	Unknown error.	Contact the Tekelec Customer Care Center.
This command is usually run by scripts; scripts should search for exit codes. When the command is run from the command line, the output indicates suggested recovery.		

start_cmdLine

Start LSMS Command Line Application Administration

Starts the LSMS Command Line Application Administration (`lsmsclaa`) application, an optional feature that enables users to enter text commands to control certain LSMS application functions otherwise available through the GUI. Entering this command allows one or more actions to be entered until the application is exited. For more information about the `lsmsclaa` application and the actions that can be entered (including HELP), see *Using lsmsclaa Commands* on page 230.

Restrictions

The `lsmsclaa` application is designed to be used only on the active server.

Each instance of starting the `lsmsclaa` application is counted as a terminal in the GUI usage restrictions. For more information about the maximum number of GUIs and `lsmsclaa` applications that can be running concurrently, see *Support of Multiple Users* on page 44.

Keyword

```
start_cmdLine
```

Permission

The user must be defined as a member of the primary group `lsms`. The secondary group to which the user belongs determines which actions are allowed. For information about permissions required for each action, see the descriptions of actions starting. For information about assigning users to groups, see *Adding a User* on page 70.

Syntax

```
$LSMS_DIR/start_cmdLine <SPID> <Region> [COMMANDFILE]
```

Options

None.

Parameters

`SPID` Mandatory four-character parameter that specifies Service Provider ID.

`Region` Mandatory parameter that specifies NPAC region associated with this command. Enter one of the following values:

```
Canada

Midwest

MidAtlantic

Southeast

Southwest
Northeast
```

```
Western

WestCoast
```

COMMANDFILE Optional parameter that specifies the full name of a text file that contains a series of actions to be executed by `lsmsclaa`. If included, enter from 1 to 256 characters. For more information about the possible actions that can be included in this file, see *Using lsmsclaa Commands* on page 230.

Sample Output

The following sample output shows that the `lsmsclaa` utility starts, the `ASSOCIATE` action is performed, `lsmsclaa` exits, and the command-line prompt returns.

```
 # Start the lsmsclaa application for the Midwest NPAC
 $ $LSMS_DIR/start_cmdLine TKLC Midwest
 Enter command ->ASSOCIATE PRIMARY
Already connected
Enter command ->EXIT
$
```

Files

You can create a command file that contains a series of actions. You can store this file in any directory. For more information, see the description of the `COMMANDFILE` parameter.

Usage Notes

For information about using the `lsmsclaa` utility, see *Using the lsmsclaa Application Interactively* on page 231.

Response Notes

The command-line prompt does not return until `lsmsclaa` is exited. For more information about exit conditions, see *Exiting the lsmsclaa Application* on page 231.

Error Messages Generated by the start_cmdLine Command

Table 51: Error Messages: start_cmdLine on page 224 lists the error messages and return codes that can be generated by the `start_cmdLine` command.

If the `start_cmdLine` command is entered without the `COMMANDFILE` parameter, only the message appears. If the `start_cmdLine` command is entered with the `COMMANDFILE` parameter, the return code and the message are generated, except as noted in the table. For a complete list of return codes that can be generated while `lsmsclaa` is running, see *Return Codes Generated While Running lsmsclaa* on page 232.

Table 51: Error Messages: start_cmdLine

Message	Cause	Return Code	Exit?
`Invalid argument list passed to lsmsclaa`	A required parameter (`SPID` or `REGION` or both) was not specified or was specified with a value that was not valid.	1	Yes
`Could not open the command file <x>`	The command file specified in the argument list could not be opened. It may not exist or it may not have the correct file permissions.	3	Yes
`Could not read from the command file <x>`	The command file specified in the argument list could not be read from.	3	Yes
`Error processing command file line: <x>`	The action specified on the indicated line of the command file could not be performed.	Note	Yes
Note: Returns the return code for the last action executed or attempted. For more information about return codes for actions, see *Return Codes Generated While Running lsmsclaa* on page 232.			

start_mgui

Start LSMS GUI

Starts the LSMS GUI for the specified NPAC region.

Keyword

`start_mgui`

Permission

The user must be defined as a member of the primary group `lsms`. The secondary group to which the user belongs determines which GUI functions are accessible. For more information about assigning users to groups, see *Adding a User* on page 70. For more information about which GUI

functions are available to which permission groups, see *Non-Configurable Permission Groups* on page 64.

Environment

$DISPLAY

Syntax
`$LSMS_DIR/start_mgui`

Options

None.

Parameters

None.

Sample Output

This command has no output.

sup

Control of Local Services Manager and Local Data Manager

Used to start, stop, or display status of the Local Services Manager (`lsman`) and Local Data Manager (`supman`).

Keyword
`sup`

Permission

The user must be logged in with the user name `lsmsadm`.

Syntax
`$LSMS_DIR/sup <Action>`

Options

None.

Parameters

`Action` The function to be performed on the `lsman` and `supman` processes. This mandatory parameter has the following values:

`start`

`stop`

```
status
```

Sample Output

```
# Stop the lsman and supman currently running
$ $LSMS_DIR/sup stop

supman stopped
lsman stopped
# Restart the lsman and supman
$ $LSMS_DIR/sup start
```

This command has no output.

```
# Check the status of the lsman and supman
$ $LSMS_DIR/sup status

0 reports in progress
0 LNP database synchronization operations in progress
6 GUIs connected
lsman: mem= 23480 kbytes : pcpu = 0.1 %
supman: mem= 41216 kbytes : pcpu = 0.2 %
reportma: mem= 14072 kbytes : pcpu = 0.1 %
```

Possible Errors

Table 52: Exit Codes: sup

Exit Code	Cause	Suggested Recovery
1	Usage error.	Correct the syntax.
This command is usually run by scripts; scripts should search for exit codes. When the command is run from the command line, the output indicates suggested recovery.		

sup_db_setup

Supplemental Database Setup

Creates or removes the supplemental database.

Note:

See *Special Procedure to Remove EMSs from Shared Memory* on page 228 for information about removing EMSs from shared memory when removing supDB.

Keyword
`sup_db_setup`

Permission

The user must be logged in with the user name `lsmsadm`.

Syntax

```
$LSMS_DIR/sup_db_setup <Action>
```

This command must be executed from the $LSMS_DIR and must be run on the both servers. The operator must respond to a prompt to verify removal or creation of the database when a version already exists.

Options

None.

Parameters

`Action`	The function to be performed on the database. This mandatory parameter has the following values:
	`create`
	`remove`

Sample Output

To create a new Supplemental Database:

```
$ $LSMS_DIR/sup_db_setup create
```

```
Supplemental Database Setup Script The Supplemental Database name is supDB
Initializing Supplemental Database...supDB
The supplemental database supDB was created successfully.
```

To remove the current Supplemental Database

```
$ $LSMS_DIR/sup_db_setup remove
```

```
Supplemental Database Setup Script
WARNING: Supplemental Database supDB is about to be removed.
         All data in this database will be lost.
         Do you want to continue? [Y/N] Y
Removing Supplemental Database...supDB
$
```

Response Notes

The create action requires 20 or more seconds to create the database and respond.

Possible Errors

Table 53: Error Messages: sup_db_setup

Exit Code	Cause	Suggested Recovery
1	Syntax was incorrect	Use correct syntax.
2	MySQL command failed	Contact Tekelec.
7	User attempted to create a database that already exists	None needed.
9	User attempted to remove a database that is in use	Stop indicated processes before attempting to remove the database.
10	The root user cannot execute this command	Change users to `lsmsadm`.

Special Procedure to Remove EMSs from Shared Memory

Note:

Beginning with LSMS Release 6.0, Sentry information for LSMS processes is stored in shared memory, not the database. As a result, use of the sup_db_setup command to remove the supDB leaves Sentry in the state that it still monitors/restarts EagleAgents for EMS that were previously defined in the supDB. Therefore, Sentry will continually attempt to restart the EagleAgents for these EMS's and will continue to display their status. To eliminate this problem, perform the following procedure:

Procedure:

1. Delete all EMS Components using the LSMS GUI. (For more information, refer to the LSMS *Configuration Manual*, Chapter 3, "Deleting an EMS Configuration Component.")
2. Deactivate all NPAC Regions using the LSMS GUI. (For more information, refer to the LSMS *Configuration Manual*, Chapter 3, "Modifying LSMS Configuration Components.")
3. Shutdown the LSMS using Sentry. Log in to the active server as `root`, and execute the `sentry shutdown` command:

   ```
   # sentry shutdown
   ```
4. Delete the supDB. Log in to the active server as `lsmsadm`, and execute the `sup_db_setup remove` command:

   ```
   $ $LSMS_DIR/sup_db_setup remove
   ```

You have now completed this procedure.

survNotify

Surveillance Notification Command

Use this command to send a customer-defined notification.

Keyword

`survNotify`

Permission

The user must be defined as a member of the primary group `lsms`.

Syntax

```
$LSMS_DIR/survNotify <MsgNo> SET <Text>
```

Options

None.

Parameters

`MsgNo` Unique identifier for a customer-defined message. When the `Action` parameter has the value `SET`, this parameter is mandatory and must have a value in the range 9000-9999. When the `Action` parameter has any value other than `SET`, this parameter is not allowed.

`SET` Send a surveillance notification which has the number specified by the `MsgNo` parameter and the text specified by `Text` parameter.

`Text` The message text for a customer-defined notification. This parameter can contain up to 39 characters. If the text contains spaces, the text should begin and end with a double quote character. This parameter is optional.

Sample Output

```
# Notify the Surveillance Monitor that a new customer-defined event has occurred

$ $LSMS_DIR/survNotify 9001 SET "Job completed"

Response Notes
```

This command has no output other than the prompt.

Possible Errors

Table 54: Exit Codes: survNotify

Exit Code	Cause	Suggested Recovery
1	Socket open error.	Contact the Tekelec Customer Care Center.

Exit Code	Cause	Suggested Recovery
2	Usage error.	Correct the syntax.
3	Unknown operation argument.	Supply a valid operation argument.
This command is usually run by scripts; scripts should search for exit codes. When the command is run from the command line, the output indicates suggested recovery.		

syscheck

Check System Health

Detects, diagnoses, and displays a summary of the overall health of the LSMS.

Keyword

`syscheck`

Permission

The user must be `root`.

Syntax

The syscheck command resides in the `/usr/TKLC/plat/bin` directory. Use only the syntax specified in procedures in this manual. For all other uses, contact the Tekelec Customer Care Center.

Additional Information

For additional information about the syscheck command, access the man page from the LSMS by typing the following:

```
man syscheck
```

Using lsmsclaa Commands

The `lsmsclaa` application is an optional LSMS feature that allows the certain functions to be invoked through the command line as an alternative to invoking them through the LSMS graphical user interface (GUI). The `lsmsclaa` application allows the actions shown in *Table A-36* to be:

- Accessed interactively, through remote connections that have text-only interfaces (the GUI requires an X-Windows server for display)
- Grouped in a shell script that can be started locally or remotely

This section describes how to start and exit the `lsmsclaa` application, how to specify the actions to be performed with `lsmsclaa` along with their input parameters, and possible return codes and outputs. (Scripts that contain `lsmsclaa` commands may need to parse the output.)

Using the lsmsclaa Application Interactively

Starting the lsmsclaa Application Interactively

To use the `lsmsclaa` application interactively, enter the `start_cmdLine` command without a `COMMANDFILE` parameter (for more information, see *start_cmdLine* on page 222). If the command executes successfully, the following `lsmsclaa` prompt displays:

```
Enter command ->
```

This prompt indicates that the `lsmsclaa` utility is ready to process actions described in *Actions Available Through lsmsclaa* on page 232. You can initiate as many actions as are required to fulfill a task. The prompt appears at the conclusion of each action entered until you enter `EXIT`. A blank line always precedes the prompt.

If an error occurs during interactive processing, an error message appears. Except when the cause of the error is loss of connection to the regional LSMS agent, the error message is followed by the `lsmsclaa` prompt. If you want to end the `lsmsclaa` application, enter the `EXIT` action. For information about the specific error messages that can appear for each action, refer to the *"LSMS Application Functions and Third-Party Commands Available at the command-line Prompt"* on page 162.

Exiting the lsmsclaa Application

If the `lsmsclaa` application is started interactively, it exits only under the following conditions:

- Losing connection to the regional LSMS agent
- Processing an `EXIT` action

Using the lsmsclaa Application with a Script File

Starting the `lsmsclaa` Application with a Script File

To use a script to execute multiple actions, enter the `start_cmdLine` command with a `COMMANDFILE` parameter (for more information, see *start_cmdLine* on page 222). Using a script also enables you to direct standard output to the standard input for `lsmsclaa`.

The `lsmsclaa` prompt is not displayed during the processing of the command file. The `lsmsclaa`application displays the `lsmsclaa`prompt after all the actions in the file have been processed if none of the conditions shown in *Exiting the lsmsclaa Application* on page 231 occur.

Exiting the `lsmsclaa` Application

If the `lsmsclaa` application is started with the `COMMANDFILE` parameter, it exits only under the following conditions:

- Failing to startup (see return codes 1 through 5 in *Table 56: Return Codes Generated While Running lsmsclaa* on page 233)

- Losing connection to the regional LSMS agent (see return code 112 in *Table 56: Return Codes Generated While Running lsmsclaa* on page 233)
- Processing an `EXIT` action in the command file
- Processing an End-of-File character in the command file
- Encountering certain errors during processing of a command file, as shown in *Table 56: Return Codes Generated While Running lsmsclaa* on page 233.

When the `lsmsclaa` application exits, it returns a return code that reflects the success or failure of the last action executed or attempted before exiting. In addition, it prints a text message to standard output. Some of the messages are extensive. Any encapsulating script that needs the results of a particular action, must parse the output for strings shown in the Possible Output columns of *Table 57: Possible Output and Return Codes Generated by ABORT* on page 236 through *Table 60: Possible Output and Return Codes Generated by SYNCH* on page 245 .

Actions Available Through `lsmsclaa`

Table 55: LSMS Functions Available Through lsmsclaa on page 232 lists the actions can be entered at the `lsmsclaa` prompt or included in a `COMMANDFILE`.

Table 55: LSMS Functions Available Through lsmsclaa

`lsmsclaa` Action
ABORT on page 235
ASSOCIATE on page 237
AUDIT on page 239
EXIT on page 241
HELP on page 242
SYNCH on page 242

For information about how these functions can also be managed using the GUI, see *Table 21: LSMS Functions Available Through lsmsclaa and Through GUI* on page 164 .

Return Codes Generated While Running lsmsclaa

Table 56: Return Codes Generated While Running lsmsclaa on page 233 summarizes the return codes that can be generated while `lsmsclaa` is running. For specific causes according to action, see the description of the relevant action starting.

A return code of 0 does not necessarily imply that all aspects of the operation were successful. Examine the output text for results of the operation.

Table 56: Return Codes Generated While Running `lsmsclaa`

Return Code	Cause	Exit?	ABORT	ASSOCIATE	AUDIT	SYNCH
1	Invalid parameter list passed to `lsmsclaa`.	Yes†	X	X	X	X
2	Environment error.	Yes†	X	X	X	X
3	File error including the command file.	Yes†	X	X	X	X
4	Configuration error.	Yes†	X	X	X	X
5	Reconcile running.	Yes†	X	X	X	X
102	An invalid value was specified for a parameter. Formatting error.	File*		X	X	X
103	Missing a required parameter.	File*		X	X	X
104	Constraint violation. Certain parameters have limits on their values based on other provided	File*			X	X

Return Code	Cause	Exit?	ABORT	ASSOCIATE	AUDIT	SYNCH
	parameter values.					
105	Invalid permission. Each action requires the user to be a member of certain groups.	File*	X	X	X	X
106	Invalid or unknown command: <xxx>	File*				
107	The LSMS is already associated, or is currently attempting to associate, with the NPAC.	No		X		
108	No association exists for aborting; association retry timer cancelled.	No	X			
109	Could not log in.	File*				
110	Operation failed; text is generated that describes the error.	File*	X	X	X	X

Return Code	Cause	Exit?	ABORT	ASSOCIATE	AUDIT	SYNCH
111	Too many parameters for the specified action.	File*	X	X	X	X
112	Connection to the regional LSMS agent has been severed.	Yes	X	X	X	X
0	The operation is behaving as it would if entered through the GUI. Examine the command output for the results of the operation.	No	X	X	X	X

† An error message is generated to indicate the reason for the exit.

* The process exits only if it is processing commands from a command file.

ABORT

Abort Association to NPAC

This action attempts to abort an association with the NPAC whose region was specified in the `start_cmdLine` command. The application sends an abort command to the NPAC that is associated (either the Primary NPAC or the Secondary NPAC). Occasionally, the attempt to abort can fail if the LSMS agent is waiting for a response from the NPAC.

An association with the NPAC can also be aborted through the GUI (refer to "Aborting an NPAC Association" in the LSMS *Configuration Manual*).

Permission

The user must have authorization as defined by the permission group of which the user is a member.

Syntax

Enter command -> `ABORT`

Parameters

None.

Return Codes

Table 57: Possible Output and Return Codes Generated by ABORT on page 236shows the possible output and return codes that can be generated by the `ABORT` action. If the `lsmsclaa` application was started interactively, only the output appears. If the `lsmsclaa` application was started with a command file, the output appears and the return code is returned. For a complete list of return codes that can be generated by the `lsmsclaa` application, see *Table 56: Return Codes Generated While Running lsmsclaa* on page 233 .

Table 57: Possible Output and Return Codes Generated by ABORT

Possible Output	Cause	Return Code	Exit?
`Invalid permission. Only authorized users may execute the ABORT command.`	Action entered by a user who is not a member of an authorized permission group.	105	File*
`No association to abort. Association retry timer cancelled.`	No association exists for aborting; association retry timer cancelled.	108	No
`<text that describes error>`	Operation failed.	110	File*
`Too many arguments`	User specified more parameters than are supported by this action.	111	File*

Possible Output	Cause	Return Code	Exit?
	Connection to the regional LSMS agent has been severed.	112	Yes
`<text as would appear on the GUI>`	The operation is behaving as it would if entered through the GUI.	0	No
* The process exits only if it is processing commands from a command file.			

ASSOCIATE

Create Association to NPAC

This action attempts to create an association with the NPAC whose region was specified in the `start_cmdLine` command. The operation returns after the first association (bind) attempt; therefore, the operation may be complete before the association is established.

To verify whether the association has been established, exit `lsmsclaa` and enter the following command, where `<region>` has the same value as was entered on the `start_cmdLine` command:

```
$LSMS_DIR/lsms status <region>
```

For more information about the `lsms` command, see *lsms* on page 184.

An association with the NPAC can also be created through the GUI (refer to "Creating an NPAC Association" in the LSMS *Configuration Manual*).

Permission

The user must have authorization as defined by the permission group of which the user is a member.

Syntax

```
Enter command -> ASSOCIATE <NPAC>
```

Parameters

NPAC Mandatory parameter to specify NPAC with which association is desired. Enter one of the following values:

```
PRIMARY
SECONDARY
```

Return Codes

Table 58: Possible Output and Return Codes Generated by ASSOCIATE on page 238 shows the possible output and return codes that can be generated by the `ASSOCIATE` action. If the `lsmsclaa` application was started interactively, only the output appears. If the `lsmsclaa` application was started with a command file, the output appears and the return code is returned. For a complete list of return codes that can be generated by the `lsmsclaa` utility, see *Table 56: Return Codes Generated While Running lsmsclaa* on page 233 .

Table 58: Possible Output and Return Codes Generated by ASSOCIATE

Possible Output	Cause	Return Code	Exit?
`Invalid value <x>`	A parameter value <x> contained characters that were not valid.	102	File*
`Missing argument <x>`	The mandatory parameter <x> was missing.	103	File*

`Invalid permission.`
`• Only authorized users may execute the ASSOCIATE command.`
`• Only authorized users may execute the RECONCILE command.`
	Action entered by a user who is not a member of an authorized permission group.	105	File*

`Already connected`	The LSMS is already associated, or is currently attempting to associate, with the NPAC.	107	No
`<text that describes error>`	Operation failed.	110	File*
`Too many arguments`	User specified more parameters than are supported by this action.	111	File*
	Connection to the regional LSMS agent has been severed.	112	Yes

Possible Output	Cause	Return Code	Exit?
<text as would appear on the GUI>	The operation is behaving as it would if entered through the GUI.	0	No
* The process exits only if it is processing commands from a command file.			

AUDIT

Audit, and Optionally Reconcile, Subscription Versions

This action performs a comparison between the subscription version data for a set of TNs in a particular NPA-NXX in the database at the network element specified by this action and in the LSMS database that corresponds to the region specified in the `start_cmdLine` command.

Subscription version information can also be audited and reconciled through the GUI (refer to the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual*).

Only one audit of a given network element can occur at a time, whether the audit was started by a GUI or a command-line session.

Permission

To perform this action when the optional `MODE` parameter is specified as `RECONCILE`, the user must have authorization as defined by the permission group of which the user is a member.

Syntax

```
Enter command ->  AUDIT <CLLI> <STARTTN> [MODE] [DETAILS]
```

Parameters

`CLLI` Mandatory parameter to specify Common Language Location Identifier of the network element to be audited. Enter 1 to 11 characters.

`STARTTN` Mandatory parameter to specify complete telephone number (TN) that serves as the starting point for the audit. Enter 10 digits.

`MODE` Optional (mandatory when a value is specified for the `DETAILS` parameter) parameter that specifies whether to perform an audit only or an audit with reconcile. Enter one of the following values (the default is `AUDIT`):

`AUDIT` Perform an audit and generate a report.

`RECONCILE` Perform an audit, generate a report, and reconcile the differences between the LSMS and the NE by sending data to the NE.

DETAILS Optional parameter that specifies where to send the audit summary in addition to sending it to the standard output. If this parameter is specified, the MODE parameter must also be specified. Enter up to 255 characters with one of the following values:

NONE	Do not generate an audit summary.
SCREEN	Send the audit summary to the screen.
FILE <filename>	Send the audit summary to a file and specify the full path name for the file.
BOTH <filename>	Send the audit summary both to the screen and to a file (specify the full path name for the file).

Successful Completion

If the action completes successfully, typically the string AUDIT COMPLETED is displayed to standard output to indicate that the next command may be entered.

Return Codes

Table 59: Possible Output and Return Codes Generated by AUDIT on page 240shows the possible output and return codes that can be generated by the AUDIT action. If the lsmsclaa application was started interactively, only the output appears. If the lsmsclaa application was started with a command file, the output appears and the return code is returned. For a complete list of return codes that can be generated by the lsmsclaa utility, see *Table 56: Return Codes Generated While Running lsmsclaa* on page 233 .

Table 59: Possible Output and Return Codes Generated by AUDIT

Possible Output	Cause	Return Code	Exit?
Invalid value <x>	A parameter value <x> contained formatting or characters that were not valid.	102	File*
Missing argument <x>	The mandatory parameter <x> was missing.	103	File*

Possible Output	Cause	Return Code	Exit?
Constraint violation <x> must be between <a> and <b>	The value specified for `ENDTN` was less than the value specified for `STARTTN`.	104	File*
`Invalid permission.• Only authorized users may execute the AUDIT command.• Only authorized users may execute the RECONCILE operation.`	Action entered by a user who is not a member of an authorized permission group.	105	File*
`<text that describes error>`	Operation failed.	110	File*
`Too many arguments`	User specified more parameters than are supported by this action.	111	File*
	Connection to the regional LSMS agent has been severed.	112	Yes
Audit results are displayed to standard output, and also as defined by the value of the `DETAILS` parameter.	The operation is behaving as it would if entered through the GUI.	0	No

* The process exits only if it is processing commands from a command file.

EXIT

Exit the `lsmsclaa` Application

This action exits the `lsmsclaa` application and returns the prompt to the standard command-line prompt.

Permission

Any user can perform this action.

Syntax

```
Enter command -> EXIT
```

Return Codes

This action has no affect on the return code from the application. The return code will be the return code from the last operation performed before the exit.

HELP

Display Syntax for the `lsmsclaa` Application

This action displays the syntax for each of the actions supported by the `lsmsclaa` application.

Permission

Any user can perform this action.

Syntax

```
Enter command -> HELP
```

Return Codes

This action has no affect on the return code from the application. The return code will be the return code from the last operation performed before the exit.

SYNCH

Synchronize Telephone Numbers and Number Pool Blocks Between the LSMS and NPAC

This action causes a download from the NPAC specified by the `start_cmdLine` command to the LSMS of all subscription information for one of the following categories:

- An individual TN
- A range of TNs
- All TNs modified or created within a time range. This category can also optionally resynchronize network data.
- An individual NPB
- A range of NPBs

Telephone numbers can also be resynchronized through the GUI (refer to “Resynchronizing an Individual TN,” “Resynchronizing a Range of TNs,” “Resynchronizing for a Defined Period of

Time", "Resynchronizing an Individual NPB", and "Resynchronizing a Range of NPBs" in the LSMS Database *Administration Manual*).

Permission

The user must have authorization as defined by the permission group of which the user is a member.

Syntax

Use one of the following syntaxes:

- To resynchronize an individual TN:

```
Enter command -> SYNCH <TN>
```

- To resynchronize a range of TNs:

```
Enter command -> SYNCH <STARTTN> <ENDTN>
```

- To resynchronize all TNs modified or created within a time range:

```
Enter command -> SYNCH <STRTHOUR> <STARTMINUTE> [<STRTSECOND>] [<STRTDAY>]
[<STRTMONTH>] [<ENDHOUR>] [<ENDMINUTE>] [<ENDSECOND>] [<ENDDAY>]
[<ENDMONTH>] [<DNLDYPE>]
```

This syntax has many optional parameters, and order is significant. A parameter can be skipped by entered the character X in its place.

- To resynchronize an individual NPB:

```
Enter command -> SYNCH <NPA_NXX_X>
```

- To resynchronize a range of NPBs:

```
Enter command -> SYNCH <NPA_NXX_X NPA_NXX_X>
```

Parameters

TN	Mandatory parameter that specifies the telephone number whose subscription version needs to be updated on the LSMS. Enter 10 digits.
NPA_NXX_X	Mandatory parameter that specifies the number pool block whose subscription version needs to be updated on the LSMS. Enter seven digits.
STARTTN	Mandatory parameter that specifies the complete telephone number that is the starting value for a range of TNs whose subscription versions need to be updated on the LSMS. Enter 10 digits.
ENDTN	Mandatory parameter that specifies the final four digits of the telephone number that is the ending value for a range of TNs whose subscription versions need to be updated on the LSMS. Enter four digits, which must be greater than the final four digits of the STARTTN parameter.
STRTHOUR	Mandatory parameter that specifies the starting hour for synchronizing all TNs modified or created within a time range. Enter a value from 1 to 23.
STRTMINUTE	Mandatory parameter that specifies the starting minute for synchronizing all TNs modified or created within a time range. Enter a value from 0 to 59.

STRTSECOND Optional parameter that specifies the starting second for synchronizing all TNs modified or created within a time range. Enter a value from 0 to 59; the default is 0.

STRTDAY Optional parameter that specifies the starting day for synchronizing all TNs modified or created within a time range. Enter a value from 1 to 31; the default is the current day.

STRTMONTH Optional parameter that specifies the starting month for synchronizing all TNs modified or created within a time range. Enter a value from 1 to 12; the default is the current month.

STRTYEAR Optional parameter that specifies the starting year for synchronizing all TNs modified or created within a time range. Enter four digits; the default is the current year.

ENDHOUR Optional parameter that specifies the ending hour for synchronizing all TNs modified or created within a time range. Enter a value from 1 to 23; the default is one hour greater than the value of the STRTHOUR parameter. If the calculated default value would be greater than 24, the defaults for the ENDDAY, ENDMONTH, and ENDYEAR parameters change as appropriate.

ENDMINUTE Optional parameter that specifies the minute for the ending range for synchronizing all TNs modified or created within a time range. Enter a value from 0 to 59; the default is equal to the value of the STRTMINUTE parameter.

ENDSECOND Optional parameter that specifies the second for the ending range for synchronizing all TNs modified or created within a time range. Enter a value from 0 to 59; the default is equal to the value of the STRTSECOND parameter.

ENDDAY Optional parameter that specifies the day for the ending range for synchronizing all TNs modified or created within a time range. Enter a value from 1 to 31; the default is equal to the value of the STRTDAY parameter.

ENDMONTH Optional parameter that specifies the month for the ending range for synchronizing all TNs modified or created within a time range. Enter a value from 1 to 12; the default is equal to the value of the STRTMONTH parameter.

ENDYEAR Optional parameter that specifies the year for the ending range for synchronizing all TNs modified or created within a time range. Enter four digits; the default is equal to the value of the STRTYEAR parameter.

DNLDTYPE Optional parameter that specifies the type of download. Enter one of the following values (default is SUBSCRIBER):

SUBSCRIBER	Download only subscriber data.
NETWORK	Download only network data.
ALL	Download both subscriber data and network data.

Return Codes

Table 60: Possible Output and Return Codes Generated by SYNCH on page 245 shows the possible output and return codes that can be generated by the SYNCH action. If the lsmsclaa application was started interactively, only the output appears. If the lsmsclaa application was started with a command file, the output appears and the return code is returned. For a complete list of return

codes that can be generated by the `lsmsclaa` utility, see *Table 56: Return Codes Generated While Running lsmsclaa* on page 233.

Table 60: Possible Output and Return Codes Generated by SYNCH

Possible Output	Cause	Return Code	Exit?
`Invalid value <x>`	A parameter value <x> contained characters that were not valid.	102	File*
`Missing argument <x>`	The mandatory parameter <x> was missing.	103	File*
`Constraint violation <x> must be between <a> and <b>`	A parameter's value was out of range. The values specified for ending values are constrained by the values specified for starting values.	104	File*
`Invalid permission. Only authorized users may execute the SYNCH command.`	Action entered by a user who is not a member of an authorized permission group.	105	File*
`<text that describes error>`	Operation failed.	110	File*
`Too many arguments`	User specified more parameters than are supported by this action.	111	File*
	Connection to the regional LSMS agent has been severed.	112	Yes
`<text as would appear on the GUI>`	The operation is behaving as it would if entered through the GUI.	0	No

* The process exits only if it is processing commands from a command file.

Appendix B

Automatic Monitoring of Events

Topics:

- *Introduction Page 248*
- *Overview of Monitored Events Page 248*
- *Overview of GUI Notifications Page 250*
- *Overview of Surveillance Notifications Page 256*
- *Overview of Traps Page 259*
- *Event Descriptions Page 261*
- *Platform Alarms Page 358*

This appendix contains overviews of monitored events, GUI and surveillance notifications, and traps.

Introduction

This appendix contains:

- *Overview of Monitored Events* on page 248, which describes how the LSMS monitors itself for events and alarms and how it reports them.
- *Overview of GUI Notifications* on page 250, which describes the display, format, and logging of notifications that appear on the graphical user interface.
- *Overview of Surveillance Notifications* on page 256, which describes the display, format, and logging of Surveillance notifications.
- *Overview of Traps* on page 259, which describes the transmission, format, and logging of SNMP *traps*.
- A listing of all events, in numerical order, starting on page B-18. For each event, this appendix includes:
  - Explanation of the probable cause for the event
  - Suggested recovery
  - Indication of whether the event results in a GUI notification, Surveillance notification, *trap*, or some combination of these.

Overview of Monitored Events

This section describes:

- *Types of Events and Alarms Reported* on page 248
- *How Servers Report Alarms and Events* on page 249

Types of Events and Alarms Reported

The LSMS monitors itself for the types of events and alarms shown in *Table 61: Notification Event Number Categories* on page 249 . When one of these events occurs, the LSMS does one or more of the following:

- Displays a notification on the graphical user interface (GUI notification)
- Posts a Surveillance notification at a certain frequency to the administration console by default, or to the second serial port if so configured
- Sends a *trap* to a Network Management System (NMS) if you have installed the optional Remote Monitoring feature

Every GUI notification and Surveillance notification contains its associated event number. Traps contain a trap ID, which is explained in *Overview of Traps* on page 259.

Table 61: Notification Event Number Categories

Event Number Range	Category	Description
0000–1999	EMS	Events that pertain to an Element Management System (EMS). The EMS is a process that runs on the Multi-Purpose Server (MPS) at a network element.
2000–3999	NPAC	Events that pertain to a Number Portability Administration Center (NPAC)
4000–5999	Platform and switchover (some of these events do not produce GUI notifications)	Events that pertain to system resources, such as disks, hardware, memory, central processing unit (CPU) utilization and to switchover functions
6000–7999	Main LSMS processes	Events that pertain to one of the following main LSMS processes: `lsman`, `supman`, `npacagent`, or `eagleagent`
8000–8999	Applications	Events that pertain to LSMS applications that are feature or application dependent, such as LNP Database Synchronization, Service Assurance, or NPA Split Administration

How Servers Report Alarms and Events

The LSMS 9.0 servers perform the following functions to monitor and report events:

- The standby server:
  - Monitors itself only for:
    - Platform events (see *Platform Alarms* on page 358)
    - Switchover-readiness events, such as those that describe database replication or critical network interfaces
  - Controls the appropriate Alarm LED (Critical, Major, or Minor) on the front of the server by illuminating the LED when one or more platform alarm in that category exists and turning off the LED when no platform alarms in that category exist
  - Sends any notification to its Serial Port 1 and logs the notification in its Surveillance log

- Sends the notification to the active server

- The active server performs the following functions:
  - Monitors itself for both platform events and application events
  - Controls the appropriate Alarm LED (Critical, Major, or Minor) on the front of the server by illuminating the LED when one or more platform alarm in that category exists and turning off the LED when no platform alarms in that category exist
  - Sends all platform events for itself, events reported from the standby server, and appropriate application events for itself to its Serial Port 1 and also logs the event as appropriate in its Surveillance log (some event notifications are reported repeatedly; for more information about which events are reported repeatedly, see the individual event descriptions)
    - Alarms that originate from the active server contain the alarm text with no hostname
    - Alarms that originate from the standby server contain the alarm text preceded by the standby server's hostname

    Note: Although all events are reported through SNMP traps and all platform alarms are reported through Surveillance notifications, not all application alarms are reported both through the GUI and through Surveillance notifications; for more information about which alarms are reported in which way, see the individual event descriptions.

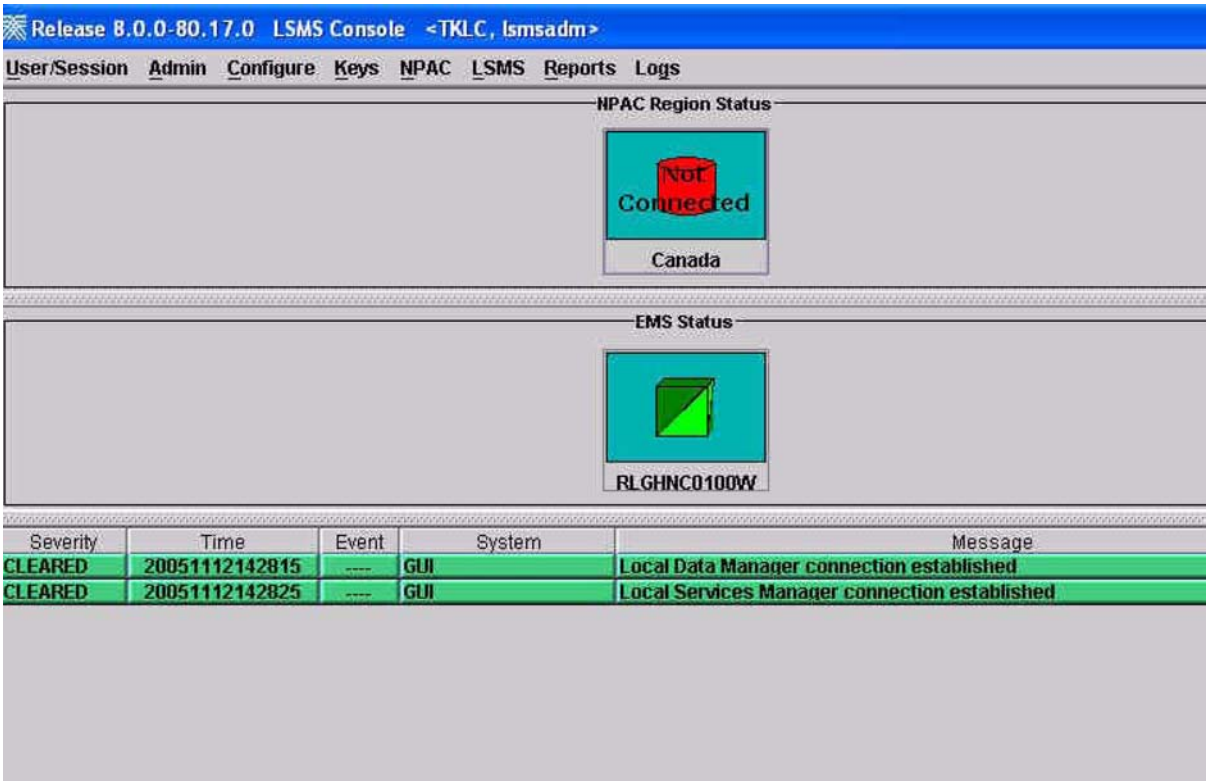
  - Displays one time on the GUI each platform or application event for itself and each platform event received from the standby server:
    - Alarms that originate from the active server display the alarm text with no hostname
    - Alarms that originate from the standby server display the alarm text preceded by the standby server's hostname
  - Sends one SNMP (Simple Network Management Protocol) trap for each platform or application event for itself and for each platform event received from the standby server. Each trap contains the IP address of the server from which the notification originated.

Overview of GUI Notifications

Displaying GUI Notifications

GUI notifications are displayed on the GUI only if the GUI is active when the reported event occurs, but all GUI notifications are logged in an appropriate log as described in *Logging GUI Notifications* on page 255. *Figure 86: GUI Notifications* on page 250shows an example of notifications displayed on the GUI.

Figure 86: GUI Notifications



Format of GUI Notifications

This section describes the general format used for most GUI notifications, as well as additional fields used for GUI event notifications (used to report information only) and for EMS GUI notifications. The formats are expressed as an ordered sequence of variables. Variables are expressed with the name of the variable enclosed by angle brackets; for example, <Severity> indicates a variable for the severity assigned to a GUI notification. *Variables Used in GUI Notification Format Descriptions* on page 252shows the variables used in GUI notification formats.

General Format for GUI Notifications

The format for most GUI notifications is:

```
[<Severity>]:<Time Stamp> <Event Number> <Message Text String>
```

In addition, the following types of GUI notifications contain additional fields:

- EMS GUI notifications contain information about the EMS for which they are reporting status (see *Format for EMS GUI Notifications* on page 252)
- Notifications that have the severity EVENT can contain additional event data fields (see *Format for GUI Notifications with EVENT Severity* on page 252)

Format for EMS GUI Notifications

EMS GUI notifications (event numbers in the range 0000–1999) contain a <CLLI> value to indicate the Common Language Location Identifier for the network element where the EMS resides. The format for EMS GUI notifications is:

```
[<Severity>]:<Time Stamp> <Event Number> <CLLI>: <Message Text String>
```

Format for GUI Notifications with EVENT Severity

Notifications that have the severity EVENT can contain additional event data fields. The format for GUI notifications with severity EVENT is:

```
[EVENT]:<Time Stamp> <Event Number> <EventType>:<EventData1>, [<EventData2>],...
```

Variables Used in GUI Notification Format Descriptions

Table 62: Variables Used in GUI Notifications on page 252 shows the possible values and meanings for each of the variables shown in format definitions for GUI notifications.

Table 62: Variables Used in GUI Notifications

Field	Description		
<Severity>	Indicates seriousness of event, using both text and color, as follows:		
	Text	Color	Meaning
	[Critical]	Red	Reports a serious condition that requires immediate attention
	[Major]	Yellow	Reports a moderately serious condition that should be monitored, but does not require immediate attention
	[Cleared]	Green	Reports status information or the clearing of a condition that caused previous posting of a [Critical] or [Major] GUI notification
	[EVENT]	White	For information only

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><Time Stamp></td><td>Indicates time that the event was detected, in format:
YYYY-MM-DD hh:mm:ss where fields are as follows:
<table>
<tr><th>Field</th><th>Meaning</th><th>Possible Values</th></tr>
<tr><td>YYYY</td><td>Year</td><td>Any four digits</td></tr>
<tr><td>MM</td><td>Month</td><td>01 through 12</td></tr>
<tr><td>DD</td><td>Day</td><td>01 through 31</td></tr>
<tr><td>hh</td><td>Hour</td><td>00 through 23</td></tr>
<tr><td>mm</td><td>Minute</td><td>00 through 59</td></tr>
<tr><td>ss</td><td>Second</td><td>00 through 59</td></tr>
</table></td></tr>
<tr><td><Event Number></td><td>Four-digit number that identifies the specific GUI notification (also indicates the type of GUI notification, as shown in Table 61: Notification Event Number Categories on page 249).</td></tr>
<tr><td><Message Text String></td><td>Text string (which may contain one or more variables defined in Table 63: Variables Used in Message Text of GUI Notifications on page 254) that provides a small amount of information about the event. For more information about the event, look up the corresponding event number in this appendix; for each event number, this appendix shows the text string as it appears in a GUI notification, as well as a more detailed explanation and suggested recovery.</td></tr>
<tr><td><CLLI></td><td>Used in all EMS GUI notifications to indicate the Common Language Location Identifier for the network element where the EMS resides.</td></tr>
<tr><td><EventType>: <EventData1>, [<EventData2>],...</td><td>Optional event data fields, as indicated by square brackets around the field, included in GUI notifications with severity [EVENT]. If no data is available for a given field, the field is empty. If other fields follow an empty field, the empty field is indicated by consecutive commas with no intervening data. One of the optional fields in an event notification is an effective timestamp field. This field indicates the time that the event actually occurred. When present, it uses the ASN.1 Generalized Time format.</td></tr>
</table>

Variables Used in Message Text String of GUI Notifications

Table 63: Variables Used in Message Text of GUI Notifications on page 254 shows the variables that can appear in the message text of a GUI notification.

Table 63: Variables Used in Message Text of GUI Notifications

Symbol	Possible Values and Meanings	Number of Characters
<PRIMARY|SECONDARY>	PRIMARY=Primary NPAC SECONDARY=Secondary NPAC	7 or 9
<retry_interval>	Time, in minutes, between retries of a request sent to an NPAC after it sent a failure response	1-10
<retry_number>	Number of times the LSMS will retry to recover from a failure response sent by NPAC	1-10
<YYYYMMDDhhmmss>	Year, month, day, hour, minute, second	14
<NPAC_region_ID>	CA = Canada MA = MidAtlantic MW = Midwest NE = Northeast SE = Southeast SW = Southwest WE = Western WC = WestCoast	2

Examples of GUI Notifications

Example of General Format GUI Notifications

Following is an example of a general GUI notification (for a description of its format, see *"General Format for GUI Notifications"*):

```
[Critical]:1998-07-05 11:49:56 2012 NPAC PRIMARY-NE Connection Attempt Failed:
Access Control Failure
```

Example of an EMS GUI Notification

Following is an example of an EMS GUI notification (for a description of its format, see *"Format for EMS GUI Notifications"*). In this example, `<CLLI>` has the value `LNPBUICK`:

```
[Critical]:1998-07-05 11:49:56 0003 LNPBUICK: Primary Association Failed
```

Example of GUI Notification with EVENT Severity Level

Following is an example of a GUI notification with severity `[EVENT]`. For a description of its format, see *"Format for GUI Notifications with EVENT Severity"*:

```
[EVENT]: 2000-02-05 11:49:56 8069 LNPBUICK: Audit LNP DB Synchronization Aborted
```

Logging GUI Notifications

When an event that generates a GUI notification occurs, that notification is logged in the file created for those events. *Table 64: Logs for GUI Notifications* on page 255 shows the types of log files used for each of these file names, where `<mmdd>` indicates the month and day the event was logged.

Table 64: Logs for GUI Notifications

Event Type	Log File
EMS Alarms, NPAC Alarms, and Main LSMS Process Alarms	`/var/TKLC/lsms/logs/alarm/LsmsAlarm.log.<mmdd>`
Non-alarm Events	`/var/TKLC/lsms/logs/<region>/LsmsEvent.log.<mmdd>`, where `<region>` indicates the region of the NPAC that generated the information

For information about the format of the logs and how to view the logs, refer to the LSMS Database *Administration Manual*.

Overview of Surveillance Notifications

Surveillance notifications are created by the Surveillance feature. These notifications can report status that is not available through the GUI notifications and report status that can be monitored without human intervention.

Displaying Surveillance Notifications

Surveillance notifications are sent to Serial Port 1 on each server.

Format of Surveillance Notifications

All Surveillance notifications reported on the same server where the event occurred have the following format:

```
<Event Number>|<Time Stamp>|<Message Text String>
```

Surveillance notifications that originated from the non-active server and are reported on the active server where the event occurred have an additional field that shows the hostname of the server where the event occurred, as shown in the following format:

```
<Event Number>|<Time Stamp>|<Host Name>|<Message Text String>
```

Variables Used in Surveillance Notification Format Descriptions

Table 65: Variables Used in Surveillance Notifications on page 256 shows the possible values and meanings for each of the variables shown in format definition for Surveillance notifications.

Table 65: Variables Used in Surveillance Notifications

Field	Description
`<Event Number>`	Four-digit number that identifies the specific Surveillance notification and also indicates the type of Surveillance notification, as shown in *Table 62: Variables Used in GUI Notifications* on page 252 .
`<Time Stamp>`	Indicates time that the event was detected, in format: `hh:mm Mon DD, YYYY` where fields are as follows:

Field	Meaning	Possible Values
`hh`	Hour	00 through 23
`mm`	Minute	00 through 59

Field	Description		
	Mon	Month	First three letters of month's name
	DD	Day	01 through 31
	YYYY	Year	Any four digits
<Host Name>	First seven letters of the name of the host (one of two redundant servers) that noted the event. (In addition, the documentation of the individual event includes information about whether the event is reported by the active server or inactive server, or both servers.)		
<Message Text String>	Text string (which may contain one or more variables defined in *Table 66: Variables Used in Message Text of Surveillance Notifications* on page 257) that provides a small amount of information about the event. For more information about the event, look up the corresponding event number in this appendix; for each event number, this appendix shows the text string as it appears in a Surveillance notification, as well as a more detailed explanation and suggested recovery.		

Variables Used in Message Text String of Surveillance Notifications

Table 66: Variables Used in Message Text of Surveillance Notifications on page 257 shows the variables that can appear in the message text of a Surveillance notification.

Table 66: Variables Used in Message Text of Surveillance Notifications

Symbol	Possible Values and Meanings	Number of Characters
<CLLI>	Common Language Location Identifier for the network element	11
<PRIMARY|SECONDARY>	PRIMARY=Primary NPAC SECONDARY=Secondary NPAC	7 or 9
<NPAC_cust_ID>	0000 = Midwest 0001 = MidAtlantic 0002 = Northeast 0003 = Southeast 0004 = Southwest	4

Symbol	Possible Values and Meanings	Number of Characters
	0005 = Western 0006 = WestCoast 0008 = Canada	
<NPAC_IP_Address>	IP address of the NPAC	10
<process_name>	First 12 characters of process name	12
<region>	Midwest MidAtlantic Northeast Southeast Southwest Western WestCoast Canada	6 to 12
<return_code>	Return code	1 or 2
<Service_Assurance_Manager_name>	System name of machine that implements the Service Assurance Manager	12
<volume_name>	Name of disk volume, for example: a01	3
<volume_name_of_disk_partition>	Name of disk volume, for example: a01	3

Example of a Surveillance Notification

Following is an example of a Surveillance notification:

```
LSMS8088|14:58 Mar 10, 2000|lsmspri|Notify: sys Admin - Auto Xfer Failure
```

Logging Surveillance Notifications

In addition to displaying Surveillance notifications, the Surveillance feature logs all Surveillance notifications in the file survlog.log in the/var/ TKLC /lsms/logs directory.

If the LSMS Surveillance feature becomes unable to properly report conditions, it logs the error information in a file, named `lsmsSurv.log`, in the /var/TKLC/lsms/logs directory on each server's system disk. When the size of `lsmsSurv.log` exceeds 1MB, it is copied to a backup file, named `lsmsSurv.log.bak`,in the same directory. There is only one LSMS Surveillance feature backup log file, which limits the amount of log disk space to approximately 2MB.

Overview of Traps

The optional Remote Monitoring feature provides the capability for the LSMS to report certain events and alarms to a remote location, using the industry-standard Simple Network Management Protocol (SNMP). The LSMS implements an SNMP agent.

Customers can use this feature to cause the LSMS to report events and alarms to another location, which implements an SNMP Network Management System (NMS). An NMS is typically a standalone device, such as a workstation, which serves as an interface through which a human network manager can monitor and control the network. The NMS typically has a set of management applications (for example, data analysis and fault recovery applications).

For more information about the LSMS implementation of an SNMP agent, see *Understanding the SNMP Agent Process* on page 40.

SNMP Version 1 Trap PDU Format

Following is an overview of the format of the SNMP version 1 *trap* request. For more information about SNMP message formats, refer to SNMP, SNMPv2, SNMPv3, *and* RMON *1 and 2*, Third Edition, William Stallings, Addison Wesley, ISBN 0-201-48534-6, 1999.

Each SNMP message consists of the following fields:

- SNMP authentication header, which consists of:
  - Version identifier, used to ensure that both the sender and receiver of the message are using the same version of the SNMP protocol. Currently, the LSMS supports only version 1, which has a version identifier of 0 (zero).
  - Community name, used to authenticate the NMS. The SNMP agent uses this field as a password to ensure that the sender of the message is allowed to access the SNMP agent's information. The LSMS supports only *trap* requests, which originate at the LSMS; therefore, this field is not significant.
- Protocol data unit (PDU), which for a *trap* request consists of:
  - Enterprise field, which identifies the device generating the message. For the Tekelec LSMS SNMP agent, this field is 323.
  - Agent address field, which contains the IP address of the host that runs SNMP agent. For the Tekelec LSMS SNMP agent, this field contains the IP address of the LSMS active server.
  - Generic *trap* type, which can be set to any value from 0 through 6. Currently, the LSMS supports only the value 6, which corresponds to the *enterpriseSpecific* type of *trap* request.
  - Time stamp, which indicates how many hundredths of a second have elapsed since the last reinitialization of the host that runs the SNMP agent.
  - One or more variables bindings, each of which contains an object field followed by a value field. The object and value fields together specify information about the event being reported.

Logging SNMP Agent Actions

When the LSMS SNMP agent process starts, stops, or sends a *trap* request, it logs information about the action in a log file. The log file is named `lsmsSNMP.log.<MMDD>`, where `<MMDD>` represents the current month and day. The log file is stored in the directory `/var/TKLC/lsms/logs/snmp`.

Table 67: Information Logged by the LSMS SNMP Agent on page 260 shows the actions and information logged by the LSMS SNMP agent.

Table 67: Information Logged by the LSMS SNMP Agent

Action	Information Logged
The SNMP agent starts	Action, followed by day, date, time, and year; for example: `LSMS SNMP agent started: Thu Mar 09 09:02:53 2000`
The SNMP agent stops	Action, followed by day, date, time, and year; for example: `LSMS SNMP agent stopped: Thu Mar 09 15:34:50 2000`

The SNMP agent sends a *trap* request	The following fields, delimited by pipe characters:
	• Timestamp, recorded as YYYYMMDDhhmmss (year, month, date, hour, minute, second)
	• trap_ID, a unique numeric identifier that corresponds to the specific *trap* request sent.
	• For each NMS configured (up to five allowed):
	  • The NMS's IP address
	  • Status (either of the following):
	  • `S` to indicate that the LSMS SNMP agent succeeded in sending the *trap* request. (Even if the LSMS SNMP agent successfully sends the *trap* request, there is no guarantee that the NMS receives it.)
	  • `F` to indicate that the LSMS SNMP agent failed in sending the *trap* request.
	
	Following is a sample entry logged when a *trap* is sent (in this entry, a *trap* with a trap_ID of 3 is sent to two NMSs):
	`20000517093127|3|10.25.60.33|S|10.25.60.10|S`

Event Descriptions

0001

Explanation

The EMS Ethernet interface has a problem. The `ping` utility did not receive a response from the interface associated with the EMS.

Recovery

Consult with your network administrator.

Event Details

Table 68: Event 0001 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - EMS interface failure
Source	Both servers
Frequency	Every 2.5 minutes as long as condition exists
Trap	
Trap ID	16
Trap MIB Name	emsInterfaceFailure

0002

Explanation

The EMS, which is indicated in the System field on the GUI or whose CLLI has the value that replaces `<CLLI>` in the Surveillance notification text, requires a resynchronization with the LSMS that cannot be accomplished by automatic resynchronization between the LSMS and the EMS.

Recovery

Perform one of the synchronization procedures described in the LSMS-EAGLE *5* ISS LNP Database *Synchronization Manual*.

Event Details

Table 69: Event 0002 Details

GUI Notification	
Severity	Critical
Text	DB Maintenance Required
Surveillance Notification	
Text	Notify:Sys Admin - NE CLLI=<CLLI>
Source	Active server
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
Trap	
Trap ID	33
Trap MIB Name	emsRequiresResynchWithLSMS

0003

Explanation

The LSMS has lost association with the primary EMS of the network element, which is indicated in the System field on the GUI or whose CLLI has the value that replaces <CLLI> in the Surveillance notification text; the association with the secondary EMS is established.

Recovery

Determine why the primary association failed (connectivity problem, EMS software problems, NE software problem, etc.). Correct the problem. Association will be automatically retried.

Event Details

Table 70: Event 0003 Details

GUI Notification	
Severity	Major

Text	Primary Association Failed
Surveillance Notification	
Text	Notify:Sys Admin - NE CLLI=<CLLI>
Source	Active server
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
Trap	
Trap ID	5
Trap MIB Name	primaryEMSAssocLostSecEstablished

0004

Explanation

The LSMS has lost association with the primary EMS of the network element, which is indicated in the System field on the GUI or whose CLLI has the value that replaces <CLLI> in the Surveillance notification text; the association with the secondary EMS is not established.

Recovery

Determine why the primary association failed (connectivity problem, EMS software problems, NE software problem, etc.). Correct the problem, and then reestablish the association with the primary EMS.

Event Details

Table 71: Event 0004 Details

GUI Notification	
Severity	Critical
Text	Primary Association Failed
Surveillance Notification	
Text	Notify:Sys Admin - NE CLLI=<CLLI>
Source	Active server

Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
Trap	
Trap ID	36
Trap MIB Name	primaryEMSAssocLostNoSec

0006

Explanation

The pending queue used to hold transactions to be sent to the EMS/NE, which is indicated in the System field on the GUI or whose CLLI has the value that replaces <CLLI> in the Surveillance notification text, is full. To help ensure that no updates are lost, the `eagleagent` will abort associations with both the primary EMS and secondary EMS. Updates will be queued in a resynchronization log until the EMS reassociates.

Recovery

Determine why the EMS/NE is not receiving LNP updates, and correct the problem.

Event Details

Table 72: Event 0006 Details

GUI Notification	
Severity	Critical
Text	All Association(s) Aborted: Pending Queue Full
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	97
Trap MIB Name	emsAssociationAbortedQueueFull

0007

Explanation

The network element, which is indicated in the System field on the GUI or whose CLLI has the value that replaces `<CLLI>` in the Surveillance notification text, is busy and is sending 'retry later' in response to a message sent by the `eagleagent`. The `eagleagent` has already tried resending the same message the maximum number of times. The `eagleagent` has aborted associations with both the primary EMS and secondary EMS.

Recovery

Correct the problem at the network element. When the EMS reconnects with the LSMS, the LSMS will automatically resynchronize the network element's LNP database.

Event Details

Table 73: Event 0007 Details

GUI Notification	
Severity	Critical
Text	All Association(s) Aborted: Retries Exhausted
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	98
Trap MIB Name	emsAssocAbortedMaxResend

0008

Explanation

The LSMS has lost association with the secondary EMS which is indicated in the System field on the GUI or whose CLLI has the value that replaces `<CLLI>` in the Surveillance notification text. The association with the primary EMS is still up.

Recovery

Determine why the secondary association failed (connectivity problem, EMS software problems, NE software problem, etc.) and then reestablish the association with the secondary EMS.

Event Details

Table 74: Event 0008 Details

GUI Notification	
Severity	Major
Text	Secondary Association Failed
Surveillance Notification	
Text	Notify:Sys Admin - NE CLLI=<CLLI>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	130
Trap MIB Name	secondaryEMSAssocLost

0009

Explanation

The LSMS has established the first association with the network element (NE) which is indicated in the System field on the GUI or whose CLLI has the value that replaces <CLLI> in the Surveillance notification text. The first association established is called the primary association. This EMS is called the primary EMS.

Recovery

No action required; this notification is for information only.

Event Details

Table 75: Event 0009 Details

GUI Notification	
Severity	Cleared
Text	Primary Association Established
Surveillance Notification	

Text	None
Source	
Frequency	
Trap	
Trap ID	8
Trap MIB Name	primaryEMSAssocEstablished

0010

Explanation

The LSMS has established the second association with the network element (NE) which is indicated in the System field on the GUI or whose CLLI has the value that replaces <CLLI> in the Surveillance notification text. The association is established only if a primary association already exists. This EMS is called the secondary EMS.

Recovery

No action required; this notification is for information only.

Event Details

Table 76: Event 0010 Details

GUI Notification	
Severity	Cleared
Text	Secondary Association Established
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	134

Trap MIB Name	secondaryEMSAssocEstablished

0011

Explanation

The primary association for the EMS/NE, which is indicated in the System field on the GUI or whose CLLI has the value that replaces <CLLI> in the Surveillance notification text, is either down or is inhibited, such that transactions sent to the primary EMS will not be received by the NE. Transactions are being sent to the secondary EMS instead of the primary EMS.

Recovery

Determine why the primary association failed (connectivity problem, EMS software problem, NE software problem, or other problem). Correct the problem. Association will be automatically retried. When the association is reestablished, it will be a secondary association, and the EMS will be the secondary EMS.

Event Details

Table 77: Event 0011 Details

GUI Notification	
Severity	Cleared
Text	Successful Switchover Occurred to Secondary EMS
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	139
Trap MIB Name	transactionToSecondary

2000

Explanation

The NPAC Ethernet interface has a problem. The `ping` utility did not receive a response from the interface associated with the NPAC.

Recovery

Consult with your network administrator.

Event Details

Table 78: Event 2000 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - NPAC interface failure
Source	Both primary and secondary servers
Frequency	Every 2.5 minutes as long as condition exists
Trap	
Trap ID	15
Trap MIB Name	npacInterfaceFailure

2001

Explanation

The association with the NPAC identified by <NPAC_region_ID> has been disconnected by the user.

Recovery

Examine additional GUI notifications to determine whether the LSMS is retrying the association. Follow the recovery actions described for the GUI notification.

Event Details

Table 79: Event 2001 Details

GUI Notification	
Severity	Critical

Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Connection Disconnected
Surveillance Notification	
Text	Notify:Sys Admin - NPAC=<PRIMARY|SECONDARY>-<NPAC_region_ID>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	37
Trap MIB Name	lostNPACAssoc

2002

Explanation

The LSMS is not able to confirm the physical connectivity with the NPAC, which is specified in the System field on the GUI or is indicated by `<NPAC_region_ID>` in the Surveillance notification.

Recovery

Check the physical connection between the LSMS and the NPAC. The problem may be in the network, a router, or both.

Event Details

Table 80: Event 2002 Details

GUI Notification	
Severity	Critical
Text	LSMS Physical Disconnect with NPAC
Surveillance Notification	
Text	Notify:Sys Admin - NPAC=<NPAC_region_ID>
Source	Active server
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists

Trap	
Trap ID	45
Trap MIB Name	failedNPACConnectivity

2003

Explanation

The NPAC (`PRIMARY` or `SECONDARY`, as indicated) identified by `<NPAC_region_ID>` rejected the association because it received a message from the LSMS that failed security checks. This can be due to one of the following:

- The CMIP departure time is more than five minutes out of synchronization with the NPAC servers.
- The security key is not valid.
- The CMIP sequence number is out of sequence (messages must be returned to the NPAC in the same order in which they were received).

Recovery

Do the following:

1. Log in as `lsmsadm` to the active server.
2. Enter the following command to determine what the LSMS system time is:
   ```
   $ date
   ```
3. Contact the NPAC administrator to determine what the NPAC time is. If the NPAC time is more than five minutes different from the LSMS time, reset the LSMS system time on both servers and on the administration console using one of the procedures described in *Managing the System Clock* on page 59.
4. After you have verified that the NPAC and LSMS times are within five minutes of each other, cause a different security key to be used by stopping and restarting the regional agent. Enter the following commands, where `<region>` is the name of the region in which this notification occurred:
   ```
   $LSMS_DIR/lsms stop <region> $LSMS_DIR/lsms start <region>
   ```
5. Start the GUI again by performing the procedure described in *Starting an LSMS GUI Session* on page 47.
6. Attempt to reassociate with the NPAC. For information about associating with an NPAC, refer to the LSMS *Configuration Manual*.
7. If the problem persists, contact Tekelec Technical Service.

Event Details

Table 81: Event 2003 Details

GUI Notification

Severity	Critical
Text	NPAC [<PRIMARY | SECONDARY>-<NPAC_region_ID>] Connection Aborted by PEER: Access Control Failure
Surveillance Notification	
Text	Notify:Sys Admin - NPAC=<PRIMARY | SECONDARY>-<NPAC_region_ID>
Source	Active server
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
Trap	
Trap ID	95
Trap MIB Name	npacRejectedAssocAccessCtrlFail

2004

Explanation

The primary or secondary NPAC, identified by <NPAC_region_ID>, rejected the association because it received data that was not valid.

Recovery

Contact the NPAC administrator.

Event Details

Table 82: Event 2004 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY | SECONDARY>-<NPAC_region_ID>] Connection Aborted by PEER: Invalid Data Received
Surveillance Notification	
Text	Notify:Sys Admin - NPAC= <PRIMARY | SECONDARY>-<NPAC_region_ID>

Source	Active server
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
Trap	
Trap ID	96
Trap MIB Name	npacRejectedAssocInvalidData

2005

Explanation

The LSMS has lost association with the primary or secondary NPAC identified by <NPAC_region_ID> because the user aborted the association.

Recovery

Reassociate with the NPAC when the reason for aborting the association no longer exists. For information about associating with an NPAC, refer to the LSMS *Configuration Manual*.

Event Details

Table 83: Event 2005 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>]-<NPAC_region_ID> Association Aborted by User
Surveillance Notification	
Text	Notify:Sys Admin - NPAC= <PRIMARY|SECONDARY>-<NPAC_region_ID>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	9

Trap MIB Name	npacAbortByUser

2006

Explanation

The LSMS did not receive an association response from the NPAC within the timeout period. The LSMS will attempt the association with the NPAC again after an interval that defaults to two minutes, but can be configured to a different value by Tekelec.

Recovery

Determine whether there is a network connection problem and/or contact the NPAC administrator to determine whether the NPAC is up and running.

Event Details

Table 84: Event 2006 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Bind Timed Out - Auto Retry After NPAC_RETRY_INTERVAL
Surveillance Notification	
Text	Notify:Sys Admin - NPAC= <PRIMARY|SECONDARY>-<NPAC_region_ID>
Source	Active server
Frequency	As soon as condition occurs, and at two-minute intervals as long as condition exists
Trap	
Trap ID	100
Trap MIB Name	assocRespNPACTimeout

2007

Explanation

The NPAC association attempt was rejected by the NPAC, and the LSMS was informed to attempt the NPAC association again to the same NPAC host after an interval that defaults to two minutes, but can be configured to a different value by Tekelec.

Recovery

No action required; the LSMS will automatically try to associate again.

Event Details

Table 85: Event 2007 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Connection Aborted by PEER - Auto Retry Same Host After NPAC_RETRY_INTERVAL
Surveillance Notification	
Text	Notify:Sys Admin - NPAC=< PRIMARY|SECONDARY>-<NPAC_region_ID>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	101
Trap MIB Name	assocRejectedRetrySameHost

2008

Explanation

The NPAC association attempt was rejected by the NPAC, and the LSMS was informed to attempt the NPAC association again to the other NPAC host after an interval that defaults to two minutes, but can be configured to a different value by Tekelec.

Recovery

No action required; the LSMS will automatically try to associate again.

Event Details

Table 86: Event 2008 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>]-<NPAC_region_ID>- Connection Aborted by PEER - Auto Retry Other Host After NPAC_RETRY_INTERVAL
Surveillance Notification	
Text	Notify:Sys Admin - NPAC= <PRIMARY|SECONDARY>-<NPAC_region_ID>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	102
Trap MIB Name	assocRejectedRetryOtherHost

2009

Explanation

A problem exists in the network connectivity. The LSMS will attempt the association with the NPAC again after an interval that defaults to two minutes, but can be configured to a different value by Tekelec.

Recovery

Check the network connectivity for errors. Verify the ability to `ping` the NPAC from the LSMS.

Event Details

Table 87: Event 2009 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Connection Aborted by PROVIDER - Auto Retry Same Host After NPAC_RETRY_INTERVAL

Surveillance Notification	
Text	Notify:Sys Admin - NPAC= <PRIMARY|SECONDARY>-<NPAC_region_ID>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	103
Trap MIB Name	nwtkProblemRetryNPACAssoc

2010

Explanation

The LSMS received three consecutive responses from the NPAC with a download status of failure from a recovery action request. The LSMS has aborted the association and will attempt to associate again after a retry interval that defaults to five minutes, but can be configured to a different value by Tekelec. The LSMS will retry the recovery action after the association is reestablished.

Recovery

No action required; the LSMS will automatically try to associate again.

Event Details

Table 88: Event 2010 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Connection Aborted Due to Recovery Failure - Auto Retry After NPAC_RETRY_INTERVAL
Surveillance Notification	
Text	Notify:Sys Admin - NPAC= <PRIMARY|SECONDARY>-<NPAC_region_ID>
Source	Active server

Frequency	Once, as soon as condition occurs
Trap	
Trap ID	104
Trap MIB Name	lsmsAbortedNPACassocDowRecFail

2011

Explanation

The LSMS has disconnected the association with the NPAC region in question due to the lack of a response to heartbeat messages from the LSMS to the NPAC.

Recovery

Contact Tekelec Customer Care Center.

Event Details

Table 89: Event 2011 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Connection Disconnected by Heartbeat
Surveillance Notification	
Text	Notify:Sys Admin - NPAC= <PRIMARY|SECONDARY>-<NPAC_region_ID>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	111
Trap MIB Name	lostNPACAssoc

2012

Explanation

The NPAC (`primary` or `secondary`, as indicated) identified by <NPAC_region_ID> rejected the association because of an access control failure. This can be due to one of the following:

- The OSI Presentation Address is incorrect.
- The Service Provider ID in the regional configuration file is incorrect.
- The CMIP departure time is more than five minutes out of synchronization with the NPAC servers.
- The security key is not valid.

Recovery

Do the following:

1. Verify that the correct PSEL, SSEL, TSEL, and NSAP values have been configured for the OSI Presentation Address (for more information, refer to "Viewing a Configured NPAC Component" in the LSMS *Configuration Manual)*. If you need to change the values, use the procedure described in "Modifying an NPAC Component" in the LSMS *Configuration Manual.*
2. Verify that the configured Service Provider ID (SPID) is the same as the SPID assigned by the NPAC. For more information about this configuration file, refer to "Modifying LSMS Configuration Components" in the LSMS *Configuration Manual*.
3. Verify that the configured NPAC_SMS_NAME is the same as the value assigned by the NPAC (this field is case-sensitive). For more information about this configuration file, refer to "Modifying an NPAC Component" in the LSMS *Configuration Manual*.
4. Log in as `lsmsadm` to the active server.
5. Enter the following command to determine what the LSMS system time is:

   ```
   $ date
   ```
6. Contact the NPAC administrator to determine what the NPAC time is. If the NPAC time is more than five minutes different from the LSMS time, reset the LSMS system time on both servers and on the administration console by performing one of the procedures described in *Managing the System Clock* on page 59.
7. After you have verified that the NPAC and LSMS times are within five minutes of each other, cause a different security key to be used by stopping and restarting the regional agent. Enter the following commands, where `<region>` is the name of the region in which this notification occurred:

   ```
   $ $LSMS_DIR/lsms stop <region> $ $LSMS_DIR/lsms start <region>
   ```
8. Start the GUI again by performing the procedure described in *Starting an LSMS GUI Session* on page 47.
9. Attempt to reassociate with the NPAC.
10. If the problem persists, contact Tekelec Technical Service.

Event Details

Table 90: Event 2012 Details

GUI Notification

Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Connection Attempt Failed: Access Control Failure
Surveillance Notification	
Text	Notify:Sys Admin - NPAC= <PRIMARY|SECONDARY>-<NPAC_region_ID>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	106
Trap MIB Name	assocRejDueToAccessControl

2014

Explanation

The userInfo value in the cmipUserInfo portion of the NPAC association response CMIP message is not valid.

Recovery

Contact the NPAC administrator to determine why the NPAC is sending an invalid association response.

Event Details

Table 91: Event 2014 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Connection Attempt Failed: Invalid Data Received
Surveillance Notification	
Text	Notify:Sys Admin - NPAC=

	<PRIMARY|SECONDARY>-<NPAC_region_ID>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	108
Trap MIB Name	npacConnFailedCMIP

2015

Explanation

The NPAC association was terminated gracefully by the NPAC.

Recovery

According to the NANC specifications, this should never occur; if this message is seen, contact the NPAC administrator for the reason for the association unbind.

Event Details

Table 92: Event 2015 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Connection Disconnected by NPAC
Surveillance Notification	
Text	Notify:Sys Admin - NPAC= <PRIMARY|SECONDARY>-<NPAC_region_ID>
Source	Active server
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
Trap	
Trap ID	109

Trap MIB Name	npacAssocGracefullyTerminated

2018

Explanation

The LSMS was unable to properly resynchronize (with the NPAC) the data that was lost while the LSMS was not associated with the NPAC.

Recovery

Do the following:

1. Abort the NPAC association (refer to the LSMS *Configuration Manual).*
2. Attempt to reassociate with the NPAC (refer to the LSMS *Configuration Manual).*
3. If the reassociation is not successful, contact the NPAC and contact the Tekelec Customer Care Center.

Event Details

Table 93: Event 2018 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Recovery Failed
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	112
Trap MIB Name	lsmsDataLostBadResynch

2019

Explanation

The LSMS data lost during the resynchronization time was not resynchronized properly with the NPAC.

Recovery

Do the following:

1. Abort the NPAC association (refer to the LSMS *Configuration Manual).*
2. Reestablish the NPAC association (refer to the LSMS *Configuration Manual).*
3. Determine whether notification *8055* on page 333 `NPAC <PRIMARY|SECONDARY> Recovery Complete` is posted. If instead notification `2019` reappears, perform a resynchronization for a period of time starting one hour before the `2019` notification first appeared, using either the GUI (refer to "Resynchronizing for a Defined Period of Time Using the GUI" in the *LSMS Database Administration Manual*) or the *SYNCH* on page 242 command.
4. If `2019` continues to appear, contact the Tekelec Customer Care Center.

Event Details

Table 94: Event 2019 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Recovery Partial Failure
Surveillance Notification	
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Recovery Failure
Source	Active server
Frequency	Once , as soon as condition occurs
Trap	
Trap ID	113
Trap MIB Name	badNPACresynchTime

2020

Explanation

The LSMS aborted the NPAC association because the LSMS received a message from the NPAC that did not have the correct LSMS key signature.

Recovery

Verify that the correct keys are being used by both the NPAC and the LSMS.

Event Details

Table 95: Event 2020 Details

GUI Notification	
Severity	Critical
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Security Violation. Association Aborted. Retrying
Surveillance Notification	
Text	Notify:Sys Admin - NPAC= <PRIMARY|SECONDARY>-<NPAC_region_ID>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	114
Trap MIB Name	assocAbortedBadKeys

2021

Explanation

An associate retry timer was in effect. The retry attempt was canceled because a GUI user issued an Associate, Abort or Disconnect request. If an Associate request was issued, the association is attempted immediately.

Recovery

No action required; for information only.

Event Details

Table 96: Event 2021 Details

GUI Notification	
Severity	Major
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Automatic Association Retry Canceled

Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	122
Trap MIB Name	npacAutoAssociationRetryCanceled

2022

Explanation

Either the LSMS did not receive any response from the NPAC before a timeout expired or the LSMS received a response from the NPAC with a download status of failure from a recovery action request. The NPAC is unable to process the recovery action due to a temporary resource limitation. The LSMS will retry the request for the number of times indicated by `<retry_number>` with the interval between each retry indicated by `<retry_interval>` minutes. If recovery is not successful after the indicated number of retries, the LSMS will abort the association and post the following notification:

```
[Critical]: <Timestamp>  2010
:  NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Connection Aborted Due to Recovery
 Failure - Auto Retry After NPAC_RETRY_INTERVAL
```

Recovery

No action required; for information only.

Event Details

Table 97: Event 2022 Details

GUI Notification	
Severity	Major
Text	NPAC [<PRIMARY | SECONDARY>-<NPAC_region_ID>] Fail/No Response from NPAC Recovery - Auto Retry <retry_number> Times in <retry_interval> Minutes
Surveillance Notification	

Text	None
Source	
Frequency	
Trap	
Trap ID	123
Trap MIB Name	npacRecoveryFailureResourceLimit

2023

Explanation

The NPAC association will be down for the specified period of time (from the first time field shown in the notification to the second time field shown in the notification) due to NPAC-scheduled down time.

Recovery

When the scheduled down time is over, manually reestablish the NPAC association. For information about aborting and reestablishing an association, refer to the LSMS *Configuration Manual*.

Event Details

Table 98: Event 2023 Details

GUI Notification	
Severity	Major
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] ScheduleDownTime from [<YYYYMMDDhhmmss>] to [<YYYYMMDDhhmmss>]
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	124

Trap MIB Name	npacAssocPeriodDown

2024

Explanation

An Associate request has been sent to the NPAC after a retry timer expired.

Recovery

No action required; for information only.

Event Details

Table 99: Event 2024 Details

GUI Notification	
Severity	Major
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Timer Expired - Resending Association Request
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	125
Trap MIB Name	npacAssocRequestSentAfterRetryTimer

2025

Explanation

The NPAC association was successfully established.

Recovery

No action required; for information only.

Event Details

Table 100: Event 2025 Details

GUI Notification	
Severity	Cleared
Text	NPAC [<PRIMARY|SECONDARY>-<NPAC_region_ID>] Connection Successfully Established
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	7
Trap MIB Name	npacAssocEstablished

4000

Explanation

The active server has initiated an automatic switchover to the inactive server.

Recovery

No action required; for information only.

Event Details

Table 101: Event 4000 Details

GUI Notification	
Severity	Event
Text	Switchover Initiated
Surveillance Notification	
Text	Notify:Sys Admin - Switchover initiated

Source	Active server
Frequency	Once, soon as condition occurs.
Trap	
Trap ID	11
Trap MIB Name	switchOverStarted

4001

Explanation

LSMS service has been switched over.

Recovery

No action required; for information only.

Event Details

Table 102: Event 4001 Details

GUI Notification	
Severity	Event
Text	Switchover complete
Surveillance Notification	
Text	Notify:Sys Admin - Switchover complete
Source	Active server
Frequency	Once, soon as condition occurs.
Trap	
Trap ID	12
Trap MIB Name	switchOverCompleted

4002

Explanation

LSMS service could not be switched over to the inactive server; the inactive server was not able to start LSMS service.

Recovery

Contact the Tekelec Customer Care Center.

Event Details

Table 103: Event 4002 Details

GUI Notification	
Severity	Event
Text	Switchover Failed
Surveillance Notification	
Text	Notify:Sys Admin - Switchover Failed
Source	Active server
Frequency	Once, as soon as condition occurs.
Trap	
Trap ID	13
Trap MIB Name	switchOverFailed

4004

Explanation

The Ethernet interface used to connect to the application network has a problem. This interface usually connects to network-connected workstations. The `ping` utility did not receive a response from the interface associated with the application network.

Recovery

Consult with your network administrator.

Event Details

Table 104: Event 4004 Details

GUI Notification	
Severity	None

Text	
Surveillance Notification	
Text	Notify:Sys Admin - APP interface failure
Source	Either server
Frequency	Every 2.5 minutes as long as condition exists
Trap	
Trap ID	17
Trap MIB Name	appsInterfaceFailure

4007

Explanation

Database replication has failed.

Recovery

Contact the Tekelec Customer Care Center.

Event Details

Table 105: Event 4007 Details

GUI Notification	
Severity	Critical
Text	DB Repl Err - <dbReplErr>
Surveillance Notification	
Text	Notify:Sys Admin - DB repl error
Source	Active server
Frequency	Every five minutes as long as condition exists.
Trap	

Trap ID	21
Trap MIB Name	dataReplError

4008

Explanation

The database replication process monitor has failed.

Recovery

Contact the Tekelec Customer Care Center.

Event Details

Table 106: Event 4008 Details

GUI Notification	
Severity	Critical
Text	DB Proc Mon Err - <dbMonErr>
Surveillance Notification	
Text	Notify:Sys Admin - DB monitor failure
Source	Active server
Frequency	Every five minutes as long as condition exists.
Trap	
Trap ID	22
Trap MIB Name	dbMonitorFail

4009

Explanation

The server has an internal disk error.

Recovery

Contact the Tekelec Customer Care Center.

Event Details

Table 107: Event 4009 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - Internal Disk Error
Source	Either server
Frequency	Within five minutes of the condition occurring and at five-minute intervals as long as condition exists
Trap	
Trap ID	23
Trap MIB Name	internalDiskError

4011

Explanation

This notification indicates that LSMS database replication is delayed.

Recovery

No action required.

Event Details

Table 108: Event 4011 Details

GUI Notification	
Severity	N/A
Text	DB Repl Info
Surveillance Notification	
Text	Notify:Sys Admin - DB repl info

Source	Either server
Frequency	Within five minutes of the condition occurring and at five-minute intervals as long as condition exists.
Trap	
Trap ID	25
Trap MIB Name	dataReplInfo

4012

Explanation

A process specified by <process_name> is utilizing 40 percent or more of the LSMS's CPU resource and the <second_ID> indicates a specific instance of the process, as follows:

- When the <process_name> is eagleagent, the <second_ID> specifies the Common Language Location Indicator (CLLI) of the network element
- When the <process_name> is npacagent, the <second_ID> specifies the name of the region
- When the <process_name> is not eagleagent or npacagent , the <second_ID> specifies the process ID (PID) of the process.

Recovery

Because this notification is posted every five minutes as long as the condition exists, you may choose to ignore this notification the first time that it appears. However, if this notification is repeated several times in a row, do one of the following:

1. If the <process_name> is not npacagent, go to step 4. Otherwise, determine whether the npacagent is still using 40% or more of the CPU resource by entering the following command, where <region> can be optionally specified (it is the name of the region as displayed at the end of the notification text):

   ```
   $ ps -eo pid,pcpu,args | grep npacagent | grep <region>
   ```

2. If the npacagent is still using 40% or more of the CPU resource, enter the following commands to stop the npacagent and restart it, where <region> is the name of the NPAC region whose npacagent is using 40% or more of the CPU resource:

   ```
   $ cd $LSMS_DIR

   $ lsms stop <region>

   $ lsms start <region>
   ```

3. Repeat step 1. If the npacagent you tried to stop is still using 40% or more of the CPU resource, contact the Tekelec Customer Care Center.

4. If the <process_name> is not eagleagent, go to step 7. Otherwise, determine whether the eagleagent is still using 40% or more of the CPU resource by entering the following command, where <CLLI> can be optionally specified (it is the name of the network element as displayed at the end of the notification text):

```
$ ps -eo pid,pcpu,args | grep eagleagent | grep <CLLI>
```

5. If the `eagleagent` is still using 40% or more of the CPU resource, enter the following commands to stop the `eagleagent` and restart it, where `<CLLI>` is the Common Language Location Indicator (CLLI) of the network element whose `eagleagent` is using 40% or more of the CPU resource:

   ```
   $ cd $LSMS_DIR
   ```

   ```
   $ eagle stop <CLLI>
   ```

   ```
   $ eagle start <region>
   ```

6. Repeat step 1. If the process you tried to stop is still using 40% or more of the CPU resource, contact the Tekelec Customer Care Center.
7. If the `<process_name>` is not `eagleagent` or `npacagent`, contact the Tekelec Customer Care Center.

Event Details

Table 109: Event 4012 Details

GUI Notification	
Severity	Major
Text	Process [<process_name>-<second_ID>] Utilizing High Percentage of CPU
Surveillance Notification	
Text	Notify:Sys Admin - [<process_name>-<second_ID>]
Source	Either server
Frequency	Every five minutes as long as condition exists
Trap	
Trap ID	26
Trap MIB Name	cpuUtilitzationOver39

4013

Explanation

The upper server in the LSMS frame has been inhibited (this server has a default hostname of `lsmspri`).

Recovery

As soon as possible, start the server by performing the procedure described in *Starting a Server* on page 129.

Event Details

Table 110: Event 4013 Details

GUI Notification	
Severity	Major
Text	Primary Server Inhibited
Surveillance Notification	
Text	Notify:Sys Admin - Primary inhibited
Source	Upper server in frame
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
Trap	
Trap ID	27
Trap MIB Name	primaryServerInhibited

4014

Explanation

The lower server in the LSMS frame has been inhibited (this server has a default hostname of `lsmssec`).

Recovery

As soon as possible, start the server by performing the procedure described in *Starting a Server* on page 129.

Event Details

Table 111: Event 4014 Details

GUI Notification	
Severity	Major

Text	`Secondary Server Inhibited`
Surveillance Notification	
Text	`Notify:Sys Admin - Secondary inhibited`
Source	Lower server in frame
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
Trap	
Trap ID	28
Trap MIB Name	secondaryServerInhibited

4015

Explanation

A heartbeat link is down.

Recovery

Contact the Tekelec Customer Care Center.

Event Details

Table 112: Event 4015 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - Heartbeat failure
Source	Both servers
Frequency	Once, as soon as condition occurs
Trap	

Trap ID	29
Trap MIB Name	heartbeatLinkDown

4020

Explanation

The server's swap space has exceeded the critical usage threshold (default = 95%).

Recovery

If the problem persists, contact the Tekelec Customer Care Center.

Event Details

Table 113: Event 4020 Details

GUI Notification	
Severity	Critical
Text	Swap space exceeds Critical
Surveillance Notification	
Text	Notify:Sys Admin - Swap space Critical
Source	Either server
Frequency	Every five minutes as long as condition exists
Trap	
Trap ID	39
Trap MIB Name	swapSpaceCritical

4021

Explanation

The LSMS application or system daemon whose name has `<process_name>` as the first 12 characters is not running.

Recovery

No user action is necessary. The Surveillance process automatically restarts the Service Assurance process (`sacw`) and the `sentryd` process automatically restarts other processes.

Event Details

Table 114: Event 4021 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - <process_name> failed
Source	Active server
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
Trap	
Trap ID	40
Trap MIB Name	lsmsAppsNotRunning

4022

Explanation

The backup of the LSMS database has completed successfully.

Recovery

No action required; for information only.

Event Details

Table 115: Event 4022 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	

Text	DATABASE backup complete
Source	Standby server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	41
Trap MIB Name	backupCompleted

4023

Explanation

The backup of the LSMS database has failed.

Recovery

Review backup output to determine why backup failed, correct the problems, and run backup script again manually.

Note: Determine whether the NAS can be reached using the ping command. If the NAS cannot be reached, restart the NAS. To restart the NAS turn the power off, then turn the power on. If the NAS can be reached, contact the Tekelec Customer Care Center for assistance.

Event Details

Table 116: Event 4023 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - DATABASE backup failed
Source	Standby server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	42

Trap MIB Name	backupFailed

4024

Explanation

The primary LSMS server (Server 1A) is not providing the LSMS service.

Recovery

No action required; for information only.

Event Details

Table 117: Event 4024 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - Primary not online
Source	Both primary and secondary servers
Frequency	Every five minutes as long as condition exists
Trap	
Trap ID	63
Trap MIB Name	primaryServerNotOnline

4025

Explanation

The standby server is not prepared to take over LSMS service.

Recovery

Contact the Tekelec Customer Care Center.

Event Details

Table 118: Event 4025 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - Can't switch to standby
Source	Standby server
Frequency	Every five minutes as long as condition exists
Trap	
Trap ID	64
Trap MIB Name	standbyNotReadyForSwitchover

4026

Explanation

The secondary LSMS server (Server 1B) is currently providing the LSMS service.

Recovery

No action required; for information only.

Event Details

Table 119: Event 4026 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - Secondary online
Source	Both primary and secondary servers

Frequency	Every five minutes as long as condition exists
Trap	
Trap ID	65
Trap MIB Name	secServerProvidingLSMSService

4027

Explanation

The standby LSMS server cannot determine the availability of the LSMS service on the active server.

Recovery

Determine if the other server is working normally. Also, verify that the heartbeat connections (`eth12`, `eth91`, and the serial cable) are connected and functioning properly

Event Details

Table 120: Event 4027 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - Primary status unknown
Source	Standby server
Frequency	Every five minutes as long as condition exists
Trap	
Trap ID	66
Trap MIB Name	secServerCannotDeterminePrimAvailability

4030

Explanation

The server's swap space has exceeded the major usage threshold (default = 80%).

Recovery

If the problem persists, contact the Tekelec Customer Care Center.

Event Details

Table 121: Event 4030 Details

GUI Notification	
Severity	Major
Text	`Swap Space Warning`
Surveillance Notification	
Text	`Notify:Sys Admin - Swap space warning`
Source	Both servers
Frequency	Every five minutes as long as condition exists
Trap	
Trap ID	190
Trap MIB Name	swapSpaceWarning

4031

Explanation

A database replication error that was reported earlier by the 4007 event has now been cleared.

Recovery

No action necessary.

Event Details

Table 122: Event 4031 Details

GUI Notification	
Severity	Cleared

Text	Database Replication cleared - <dbReplErr>
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	195
Trap MIB Name	dataReplClear

4032

Explanation

A database process monitor error that was reported earlier by the 4008 event has now been cleared.

Recovery

No action necessary.

Event Details

Table 123: Event 4032 Details

GUI Notification	
Severity	Cleared
Text	Database Replication cleared - <dbMonErr>
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	

Trap ID	196
Trap MIB Name	dbMonitorCLear

4033

Explanation

The LSMS database failed count operation, which suggests a corrupt MySQL index.

Recovery

Contact Tekelec Customer Care Center.

Event Details

Table 124: Event 4033 Details

GUI Notification	
Severity	Critical
Text	Database Corrupt Index
Surveillance Notification	
Text	None
Source	Both servers
Frequency	Every 30 minutes.
Trap	
Trap ID	200
Trap MIB Name	dbCorruptIndex

4100

Explanation

One or more platform alarms in the minor category exists. To determine which minor platform alarms are being reported, see *How to Decode Platform Alarms* on page 359. When the active server reports minor platform alarms that originated on the other server, the hostname of the other server is inserted before the alarm string.

Recovery

Contact Tekelec Customer Care Center.

Note: If you received Event 4100 in response to an snmpget error, contact the Tekelec Customer Care Center to have the NAS snmp daemon stopped and restarted.

Event Details

Table 125: Event 4100 Details

GUI Notification	
Severity	Minor
Text	Minor Platform Alarm [hostname]: <alarm_string>
Surveillance Notification	
Text	Notify:Sys Admin - ALM <alarm_string>
Source	Both servers
Frequency	Every five minutes as long as condition exists
Trap	
Trap ID	191
Trap MIB Name	minorPlatAlarmMask

4101

Explanation

All platform alarms in the minor category have been cleared. When the active server reports that all minor platform alarms have cleared on the other server, the hostname of the other server is inserted before the alarm string.

Recovery

No action necessary.

Event Details

Table 126: Event 4101 Details

GUI Notification	
Severity	Cleared

Text	Minor Platform Alarms Cleared
Surveillance Notification	
Text	Notify:Sys Admin - Minor Plat alrms clear
Source	Both servers
Frequency	Every five minutes as long as condition exists
Trap	
Trap ID	197
Trap MIB Name	minorPlatAlarmClear

4200

Explanation

One or more platform alarms in the major category exists. To determine which major platform alarms are being reported, see *How to Decode Platform Alarms* on page 359. When the active server reports major platform alarms that originated on the other server, the hostname of the other server is inserted before the alarm string.

Recovery

Contact Tekelec Customer Care Center.

Event Details

Table 127: Event 4200 Details

GUI Notification	
Severity	Major
Text	Major Platform Alarm [hostname]: <alarm_string>
Surveillance Notification	
Text	Notify:Sys Admin - ALM <alarm_string>
Source	Both servers
Frequency	Every five minutes as long as condition exists

Trap	
Trap ID	192
Trap MIB Name	majorPlatAlarmMask

4201

Explanation

All platform alarms in the major category have been cleared. When the active server reports that all major platform alarms have cleared on the other server, the hostname of the other server is inserted before the alarm string.

Recovery

No action necessary.

Event Details

Table 128: Event 4201 Details

GUI Notification	
Severity	Cleared
Text	Major Platform Alarms Cleared
Surveillance Notification	
Text	Notify:Sys Admin - Major Plat alrms clear
Source	Both servers
Frequency	Once
Trap	
Trap ID	198
Trap MIB Name	majorPlatAlarmClear

4300

Explanation

One or more platform alarms in the critical category exists. To determine which critical platform alarms are being reported, see *How to Decode Platform Alarms* on page 359. When the active server

reports critical platform alarms that originated on the other server, the hostname of the other server is inserted before the alarm string.

Recovery

Contact Tekelec Customer Care Center.

Event Details

Table 129: Event 4300 Details

GUI Notification	
Severity	Critical
Text	Critical Platform Alarm [hostname]: <alarm_string>
Surveillance Notification	
Text	Notify:Sys Admin - ALM <alarm_string>
Source	Both servers
Frequency	Once
Trap	
Trap ID	193
Trap MIB Name	criticalPlatAlarmMask

4301

Explanation

All platform alarms in the major category have been cleared. When the active server reports that all major platform alarms have cleared on the other server, the hostname of the other server is inserted before the alarm string.

Recovery

No action necessary.

Event Details

Table 130: Event 4301 Details

GUI Notification

Severity	Cleared
Text	Critical Platform Alarms Cleared
Surveillance Notification	
Text	Notify:Sys Admin - Crit Plat alrms clear
Source	Both servers
Frequency	Once
Trap	
Trap ID	199
Trap MIB Name	criticalPlatAlarmClear

6000

Explanation

The `eagleagent` process has been started.

Recovery

No action required; for information only.

Event Details

Table 131: Event 6000 Details

GUI Notification	
Severity	Cleared
Text	Eagleagent <CLLI> Has Been Started
Surveillance Notification	
Text	Notify:Sys Admin - <CLLI> started
Source	Active server
Frequency	Once, as soon as condition occurs

Trap	
Trap ID	1
Trap MIB Name	eagleAgentStarted

6001

Explanation

The `eagleagent` process has been stopped by the `eagle` script.

Recovery

No action required; for information only.

Event Details

Table 132: Event 6001 Details

GUI Notification	
Severity	Critical
Text	Eagleagent <CLLI> Has Been Stopped by User
Surveillance Notification	
Text	Notify:Sys Admin - <CLLI> norm exit
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	2
Trap MIB Name	eagleAgentStoppedbyscript

6002

Explanation

The `npacagent` for the region indicated by < NPAC_region_ID > has been started.

Recovery

No action required; for information only.

Event Details

Table 133: Event 6002 Details

GUI Notification	
Severity	Cleared
Text	NPACagent Has Been Started
Surveillance Notification	
Text	Notify:Sys Admin - <NPAC_region_ID> NPACagent started
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	3
Trap MIB Name	NPACAgentStarted

6003

Explanation

The `npacagent` for the region indicated by `<region>` has been stopped using the `lsms` command.

Recovery

No action required; for information only. If you desire to restart the agent, do the following:

1. Log in to the active server as `lsmsadm`.
2. Enter the following commands to start the `npacagent` where `<region>` is the name of the NPAC region:

```
$ cd $LSMS_DIR
$ lsms start <region>
```

Event Details

Table 134: Event 6003 Details

GUI Notification

Severity	Critical
Text	NPACAgent Has Been Stopped by User
Surveillance Notification	
Text	Notify:Sys Admin - <NPAC_region_ID> norm exit
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	4
Trap MIB Name	lsmsCommandStoppedNPACAgent

6004

Explanation

The `eagleagent` process for the network element identified by <CLLI> has failed. The `sentryd` process will attempt to restart.

Recovery

No action required; the `sentryd` process will attempt to restart the `eagleagent` process.

Event Details

Table 135: Event 6004 Details

GUI Notification	
Severity	Critical
Text	Eagleagent [<CLLI>] Has Failed
Surveillance Notification	
Text	Notify:Sys Admin - FAILD: <CLLI>
Source	Active server
Frequency	Once, as soon as condition occurs

Trap	
Trap ID	74
Trap MIB Name	lsmsEagleAgentFailed

6005

Explanation

The `eagleagent` process for the network element identified by <CLLI> has been successfully restarted by the `sentryd` process.

Recovery

No action required.

Event Details

Table 136: Event 6005 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - RECOV: <CLLI>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	75
Trap MIB Name	lsmsEagleAgentRestarted

6006

Explanation

The `sentryd` process was unable to restart the `eagleagent` process for the network element identified by `<CLLI>`.

Recovery

Contact the Tekelec Customer Care Center.

Event Details

Table 137: Event 6006 Details

GUI Notification	
Severity	Critical
Text	Failure Restarting Eagleagent [<CLLI>]
Surveillance Notification	
Text	Notify:Sys Admin - RFAILD: <CLLI>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	76
Trap MIB Name	failureToRestartEagleAgent

6008

Explanation

The `npacagent` process for the region specified by <NPAC_region_ID> has failed. The `sentryd` process will attempt to restart.

Recovery

No action required; the `sentryd` process will attempt to restart the `npacagent` process.

Event Details

Table 138: Event 6008 Details

GUI Notification	
Severity	Critical
Text	NPACagent [<NPAC_region_ID>] Failure
Surveillance Notification	

Text	Notify:Sys Admin - FAILD: <NPAC_region_ID> agent
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	78
Trap MIB Name	NPACagentForRegionFailure

6009

Explanation

The `npacagent` process for the region specified by <NPAC_region_ID> has been successfully restarted by the `sentryd` process.

Recovery

No action required. Any active LSMS GUI processes will automatically reconnect.

Event Details

Table 139: Event 6009 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - RECOV: <NPAC_region_ID> agent
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	79

Trap MIB Name	NPACagentForRegionRestarted

6010

Explanation

The `sentryd` process was unable to restart the `npacagent` process for the region specified by `<NPAC_region_ID>`.

Recovery

Contact the Tekelec Customer Care Center.

Event Details

Table 140: Event 6010 Details

GUI Notification	
Severity	Critical
Text	Failure Restarting NPACagent [<NPAC_region_ID>]
Surveillance Notification	
Text	Notify:Sys Admin - RFAILD: <NPAC_region_ID> agent
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	80
Trap MIB Name	failureToRestartNPACagentRegion

6020

Explanation

The `npacagent` process has been stopped due to a fault in accessing the regional database.

Recovery

A database error has occurred. Contact the Tekelec *Customer Care Center* on page 5.

Event Details

Table 141: Event 6020 Details

GUI Notification	
Severity	Critical
Text	NPACagent Has Been Shut Down - Database Access Error
Surveillance Notification	
Text	Notify:Sys Admin - <NPAC_region_ID> DB error
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	189
Trap MIB Name	NPACagentStopRegDBaccessFault

8000

Explanation

The LSMS Surveillance feature is in operation.

Recovery

No action required; for information only.

Event Details

Table 142: Event 8000 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	`Keep alive`

Source	Both primary and secondary servers
Frequency	Every five minutes as long as condition exists
Trap	
Trap ID	19
Trap MIB Name	survFeatureOn

8001

Explanation

The network element resynchronization database contains more than 1 million entries.

Recovery

Each day, as part of a cron job, the LSMS trims the resynchronization database so that it contains 768,000 entries. The occurrence of this event means that more than 232,000 transactions have been received since the last cron job. If this event occurs early in the day, contact the Tekelec Customer Care Center.

Event Details

Table 143: Event 8001 Details

GUI Notification	
Severity	Major
Text	ResyncDB Contains 1 Mil Entries
Surveillance Notification	
Text	Notify:Sys Admin - ResyncDB 1 Mil
Source	Active server
Frequency	Once
Trap	
Trap ID	34
Trap MIB Name	resynchLogMidFull

8003

Explanation

The pending queue, used to hold the transactions to send to the network element (which is indicated in the System field on the GUI or whose CLLI has the value that replaces <CLLI> in the Surveillance notification text), is over half full.

Recovery

No recovery is required. Informational only.

Event Details

Table 144: Event 8003 Details

GUI Notification	
Severity	Major
Text	EMS Pending Queue Is Half full
Surveillance Notification	
Text	Notify:Sys Admin - CLLI=<CLLI>
Source	Active server
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
Trap	
Trap ID	43
Trap MIB Name	ensPendingQueueHalfFull

8004

Explanation

The pending queue, used to hold the transactions to send to the network element (which is indicated in the System field on the GUI or whose CLLI has the value that replaces <CLLI> in the Surveillance notification text), is completely full. The association to that EMS will be broken.

Recovery

No manual recovery required. The LSMS will automatically re-establish the association to the EMS and synchronization will take place.

Event Details

Table 145: Event 8004 Details

GUI Notification	
Severity	Critical
Text	EMS Pending Queue Is Full
Surveillance Notification	
Text	Notify:Sys Admin - CLLI=<CLLI>
Source	Active server
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
Trap	
Trap ID	44
Trap MIB Name	emsPendingQueueMaxReached

8005

Explanation

There was a data error in a record that prevented the LSMS eagleagent from sending the record to the network element.

Recovery

Both the error and the ignored record are written to the file `/var/TKLC/lsms/logs/trace/LsmsTrace.log.<mmdd>`, where `<mmdd>` indicates the month and day the error occurred. Examine the log file for the month and day this error was reported to determine what the error was. Enter the data manually or send it again.

Event Details

Table 146: Event 8005 Details

GUI Notification	
Severity	Minor
Text	Eagleagent <CLLI> Ignoring Record: <DataError>

Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	84
Trap MIB Name	eagleAgentIgnoredRecord

8024

Explanation

The Service Assurance agent has started successfully.

Recovery

No action required; for information only.

Event Details

Table 147: Event 8024 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	67

Trap MIB Name	serviceAssuranceAgentStarted

8025

Explanation

Association with the Service Assurance Manager, identified by `<Service_Assurance_Manager_Name>`, has been established successfully.

Recovery

No action required; for information only.

Event Details

Table 148: Event 8025 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - <Service_Assurance_Manager_Name>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	68
Trap MIB Name	establishServAssuranceMgrAssoc

8026

Explanation

Association with the Service Assurance Manager, identified by `<Service_Assurance_Manager_Name>`, has been stopped or disconnected.

Recovery

Contact the Service Assurance system administrator to determine the cause of disconnection, then have Service Assurance system administrator reassociate the Service Assurance Manager to the Service Assurance Agent.

Event Details

Table 149: Event 8026 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - <Service_Assurance_Manager_Name>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	69
Trap MIB Name	servAssuranceMgrAssocBroken

8027

Explanation

The Service Assurance agent is not currently running.

Recovery

No action required; the Service Assurance agent should be restarted automatically.

Event Details

Table 150: Event 8027 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	

Text	Notify:Sys Admin
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	70
Trap MIB Name	servAssuranceAgentNotRunning

8037

Explanation

The OSI process has failed. The `sentryd` process will attempt to restart.

Recovery

No action required; the `sentryd` process will attempt to restart the failed process.

Event Details

Table 151: Event 8037 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - FAILD: OSI
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	88
Trap MIB Name	osiDaemonFailure

8038

Explanation

The OSI process has been successfully restarted by the `sentryd` process.

Recovery

No action required. The `sentryd` process will attempt to restart the `npacagent` processes for all active regions. Any active LSMS GUI processes will automatically reconnect.

Event Details

Table 152: Event 8038 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - RECOV: OSI
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	89
Trap MIB Name	osiDaemonRestarted

8039

Explanation

The `sentryd` process was not able to restart the OSI process.

Recovery

Contact the Tekelec Customer Care Center.

Event Details

Table 153: Event 8039 Details

GUI Notification

Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - RFAILD: OSI
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	90
Trap MIB Name	osiDaemonRestartFailure

8040

Explanation

The Surveillance feature has detected that the `sentryd` process is no longer running.

Recovery

No action required; the LSMS HA software will attempt to restart the `sentryd` process.

Event Details

Table 154: Event 8040 Details

GUI Notification	
Severity	None
Text	
Surveillance Notification	
Text	Notify:Sys Admin - FAILD: sentryd
Source	Active server
Frequency	Once, as soon as condition occurs

Trap	
Trap ID	91
Trap MIB Name	sentrydFailure

8049

Explanation

The EMS/NE has rejected the NPANXX GTT creation, deletion, or modification transaction, and the NPANXX value in the transaction could not be determined.

Recovery

Look in the transaction log file, `/var/TKLC/lsms/logs/<CLLI>/LsmsTrans.log.MMDD`, and locate the NE's response to the NPANXX GTT command to determine why the command failed. Re-enter the NPANXX GTT data correctly, which will cause the LSMS to try to command again.

Event Details

Table 155: Event 8049 Details

GUI Notification	
Severity	Major
Text	<CLLI>: NPANXX GTT <type_of_operation> Failed
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	126
Trap MIB Name	npanxxGTTValueNotFound

8050

Explanation

The EMS/NE has rejected the NPANXX GTT creation, deletion, or modification transaction for the specified NPANXX value.

Recovery

Look in the transaction log file, `/var/TKLC/lsms/logs/<CLLI>/LsmsTrans.log.MMDD`, and locate the NE's response to the NPANXX GTT command to determine why the command failed. Re-enter the NPANXX GTT data correctly, which will cause the LSMS to try to command again.

Event Details

Table 156: Event 8050 Details

GUI Notification	
Severity	Major
Text	<CLLI>: NPANXX GTT <type_of_operation> Failed for NPANXX <NPANXX_value>
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	127
Trap MIB Name	npanxxGTTValueRejected

8051

Explanation

The EMS/NE has rejected the Override GTT creation, deletion, or modification transaction, and the LRN value in the transaction could not be determined.

Recovery

Look in the transaction log file, `/var/TKLC/lsms/logs/<CLLI>/LsmsTrans.log.MMDD`, and locate the NE's response to the Override GTT command to determine why the command failed. Re-enter the Override GTT data correctly, which will cause the LSMS to try to command again.

Event Details

Table 157: Event 8051 Details

GUI Notification	
Severity	Major
Text	<CLLI>: Override GTT <type_of_operation> Failed
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	128
Trap MIB Name	overrideGTTValueNotFound

8052

Explanation

The EMS/NE has rejected the Override GTT creation, deletion, or modification transaction for the specified LRN value.

Recovery

Look in the transaction log file, `/var/TKLC/lsms/logs/<CLLI>/LsmsTrans.log.MMDD`, and locate the NE's response to the Override GTT command to determine why the command failed. Re-enter the Override GTT data correctly, which will cause the LSMS to try to command again.

Event Details

Table 158: Event 8052 Details

GUI Notification	
Severity	Major
Text	<CLLI>: Override GTT <type_of_operation> Failed for LRN <LRN_value>

Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	129
Trap MIB Name	overrideGTTValueRejected

8053

Explanation

The LSMS was not able to complete the automatic synchronization with the EMS/NE. Possible reasons include:

- The network failed temporarily but not long enough to cause the association with the EMS to fail.
- The EMS/NE rejected the data because it is busy updating its databases.

Recovery

Verify the connection between the LSMS and the EMS; then reinitialize the MPS. If this notification appears again, perform one of the bulk download procedures in the LSMS *with* EAGLE *5* ISS LNP Database *Synchronization Manual*.

Event Details

Table 159: Event 8053 Details

GUI Notification	
Severity	Major
Text	Short Synchronization Failed
Surveillance Notification	
Text	None
Source	

Frequency	
Trap	
Trap ID	131
Trap MIB Name	unableToCompleteAutoResynch

8054

Explanation

The LSMS has started its automatic synchronization with the EMS/NE.

Recovery

No action required; for information only.

Event Details

Table 160: Event 8054 Details

GUI Notification	
Severity	Major
Text	Short Synchronization Started
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	132
Trap MIB Name	autoResynchNEStarted

8055

Explanation

The automatic resynchronization of databases after an outage between the LSMS and the NPAC has completed successfully.

Recovery

No action required; for information only.

Event Details

Table 161: Event 8055 Details

GUI Notification	
Severity	Cleared
Text	Recovery Complete
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	133
Trap MIB Name	dbResynchCompleted

8059

Explanation

The LSMS has completed its automatic synchronization with the EMS/NE.

Recovery

No action required; for information only.

Event Details

Table 162: Event 8059 Details

GUI Notification	
Severity	Cleared
Text	Short Synchronization Complete
Surveillance Notification	

Text	None
Source	
Frequency	
Trap	
Trap ID	138
Trap MIB Name	emsShortSynchCompleted

8060

Explanation

The EMS pending queue used to hold the transactions to send to the EMS/NE identified by <CLLI> in the Survellance notification, has fallen sufficiently below the halfway full point.

Recovery

No action required; for information only.

Event Details

Table 163: Event 8060 Details

GUI Notification	
Severity	Cleared
Text	EMS Pending Queue Less Than Half Full
Surveillance Notification	
Text	Notify:Sys Admin - CLLI=<CLLI>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	141
Trap MIB Name	pendingQueueHalfFull

8061

Explanation

The EMS pending queue used to hold the transactions to send to the EMS/NE identified by <CLLI> in the Surveillance notification, has fallen sufficiently below the full point.

Recovery

No action required; for information only.

Event Details

Table 164: Event 8061 Details

GUI Notification	
Severity	Cleared
Text	EMS Pending Queue No Longer Full
Surveillance Notification	
Text	Notify:Sys Admin - CLLI=<CLLI>
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	142
Trap MIB Name	pendingQueueNotFull

8064

Explanation

The specified NPA-NXX is opened for portability starting at the value of the `<EffectiveTimestamp>` field.

Recovery

No action required; for information only.

Event Details

Table 165: Event 8064 Details

GUI Notification

Severity	Event
Text	New NPA-NXX: SPID [<SPID>], NPANXX [<NPANXX>], TS [<EffectiveTimestamp>]
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	145
Trap MIB Name	npaNxxOpenedForPortabilityAtTS

8065

Explanation

The first telephone number in the specified NPA-NXX is ported starting at the value of the `<EffectiveTimestamp>` field.

Recovery

No action required; for information only.

Event Details

Table 166: Event 8065 Details

GUI Notification	
Severity	Event
Text	First use of NPA-NXX: SPID [<SPID>], NPANXX [<NPANXX>], TS [<EffectiveTimestamp>]
Surveillance Notification	
Text	None
Source	

Frequency	
Trap	
Trap ID	146
Trap MIB Name	npaNxxPortedAtTS

8066

Explanation

An audit of the network element identified by <CLLI> has begun.

Recovery

No action required; for information only.

Event Details

Table 167: Event 8066 Details

GUI Notification	
Severity	Cleared
Text	Audit LNP DB Synchronization Started
Surveillance Notification	
Text	NE <CLLI> Audit started
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	147
Trap MIB Name	ebdaAuditActive

8067

Explanation

An audit of the network element identified by <CLLI> has completed successfully.

Recovery

No action required; for information only.

Event Details

Table 168: Event 8067 Details

GUI Notification	
Severity	Cleared
Text	Audit LNP DB Synchronization Completed
Surveillance Notification	
Text	NE <CLLI> Audit completed
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	148
Trap MIB Name	ebdaAuditSuccess

8068

Explanation

An audit of the network element identified by `<CLLI>` has failed.

Recovery

Inspect the log file `/var/TKLC/lsms/logs/<CLLI>/LsmsTrans.log.MMDD` for details as to the cause of the error. After clearing the cause of the error, start the audit again.

Event Details

Table 169: Event 8068 Details

GUI Notification	
Severity	Critical
Text	Audit LNP DB Synchronization Failed

Surveillance Notification	
Text	NE <CLLI> Audit failed
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	149
Trap MIB Name	ebdaAuditFailure

8069

Explanation

The user aborted an audit of the network element identified by `<CLLI>` before it had completed.

Recovery

No action required; for information only.

Event Details

Table 170: Event 8069 Details

GUI Notification	
Severity	Cleared
Text	Audit LNP DB Synchronization Aborted
Surveillance Notification	
Text	NE <CLLI> Audit aborted
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	150

Trap MIB Name	ebdaAuditAbortedByUser

8070

Explanation

A reconcile has started at the completion of an audit.

Recovery

No action required; for information only.

Event Details

Table 171: Event 8070 Details

GUI Notification	
Severity	Cleared
Text	Reconcile LNP DB Synchronization Started
Surveillance Notification	
Text	NE <CLLI> Reconcile started
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	151
Trap MIB Name	ebdaReconcileActive

8071

Explanation

A reconcile, which was performed at the end of an audit, has completed.

Recovery

No action required; for information only.

Event Details

Table 172: Event 8071 Details

GUI Notification	
Severity	Cleared
Text	Reconcile LNP DB Synchronization Complete
Surveillance Notification	
Text	NE <CLLI> Reconcile completed
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	152
Trap MIB Name	ebdaReconcileSuccess

8072

Explanation

A reconcile, which was performed at the end of an audit, has failed before it completed.

Recovery

Inspect the log file `/var/TKLC/lsms/logs/<CLLI>/LsmsAudit.log.MMDD` for details as to the cause of the error. After clearing the cause of the error, start the reconcile again.

Event Details

Table 173: Event 8072 Details

GUI Notification	
Severity	Critical
Text	Reconcile LNP DB Synchronization Failed
Surveillance Notification	
Text	NE <CLLI> Reconcile failed

Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	153
Trap MIB Name	ebdaReconcileFailure

8073

Explanation

The user has stopped a reconcile before it completed.

Recovery

No action required; for information only.

Event Details

Table 174: Event 8073 Details

GUI Notification	
Severity	Cleared
Text	Reconcile LNP DB Synchronization Aborted
Surveillance Notification	
Text	NE <CLLI> Reconcile aborted
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	154
Trap MIB Name	ebdaReconcileAbortedByUser

8078

Explanation

A bulk download is currently running.

Recovery

No action required; for information only.

Event Details

Table 175: Event 8078 Details

GUI Notification	
Severity	Cleared
Text	Bulk Load LNP DB Synchronization Started
Surveillance Notification	
Text	NE <CLLI> Bulk load started
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	159
Trap MIB Name	ebdaBulkLoadActive

8079

Explanation

A bulk download has completed successfully.

Recovery

No action required; for information only.

Event Details

Table 176: Event 8079 Details

GUI Notification	
Severity	Cleared
Text	Bulk Load LNP DB Synchronization Complete

Surveillance Notification	
Text	NE <CLLI> Bulk load completed
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	160
Trap MIB Name	ebdaBulkLoadSuccess

8080

Explanation

A bulk download has failed before it completed.

Recovery

Inspect the log file `/var/TKLC/lsms/logs/<CLLI>/LsmsBulkLoad.log.MMDD` for details as to the cause of the error. After clearing the cause of the error, start the bulk download again.

Event Details

Table 177: Event 8080 Details

GUI Notification	
Severity	Critical
Text	Bulk Load LNP DB Synchronization Failed
Surveillance Notification	
Text	NE <CLLI> Bulk load failed
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	161

Trap MIB Name	ebdaBulkLoadFailure

8081

Explanation

The user has stopped a bulk download before it completed.

Recovery

No action required; for information only.

Event Details

Table 178: Event 8081 Details

GUI Notification	
Severity	Cleared
Text	Bulk Load LNP DB Synchronization Aborted
Surveillance Notification	
Text	NE <CLLI> Bulk load aborted
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	162
Trap MIB Name	ebdaBulkLoadAbortedByUser

8082

Explanation

A user-initiated resynchronization is currently running.

Recovery

No action required; for information only.

Event Details

Table 179: Event 8082 Details

GUI Notification	
Severity	Cleared
Text	Re-sync LNP DB Synchronization Started
Surveillance Notification	
Text	NE <CLLI> Re-sync started
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	163
Trap MIB Name	ebdaResyncActive

8083

Explanation

A user-initiated resynchronization has completed successfully.

Recovery

No action required; for information only.

Event Details

Table 180: Event 8083 Details

GUI Notification	
Severity	Cleared
Text	Re-sync LNP DB Synchronization Complete
Surveillance Notification	
Text	NE <CLLI> Re-sync completed
Source	Active server

Frequency	Once, as soon as condition occurs
Trap	
Trap ID	164
Trap MIB Name	ebdaResyncSuccess

8084

Explanation

A user-initiated resynchronization has failed before it completed.

Recovery

Inspect the contents of the file `/var/TKLC/lsms/logs/<CLLI>/LsmsResync.log.MMDD` to determine the cause of the error. After clearing the cause of the error, start the user-initiated resynchronization again.

Event Details

Table 181: Event 8084 Details

GUI Notification	
Severity	Critical
Text	Re-sync LNP DB Synchronization Failed
Surveillance Notification	
Text	NE <CLLI> Re-sync failed
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	165
Trap MIB Name	ebdaResyncFailure

8085

Explanation

The user has stopped a user-initiated resynchronization before it completed.

Recovery

No action required; for information only.

Event Details

Table 182: Event 8085 Details

GUI Notification	
Severity	Cleared
Text	Re-sync LNP DB Synchronization Aborted
Surveillance Notification	
Text	NE <CLLI> Re-sync aborted
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	166
Trap MIB Name	ebdaResyncAbortedByUser

8088

Explanation

A scheduled file transfer has failed.

Recovery

Inspect the error log file/var/TKLC/lsms/logs/`aft/aft.log.MMDD` for details as to the cause of the error.

Event Details

Table 183: Event 8088 Details

GUI Notification	
Severity	Major

Text	Automatic File Transfer Failure - See Log for Details
Surveillance Notification	
Text	Notify:Sys Admin- Auto xfer Failure
Source	Active server
Frequency	Once, as soon as condition occurs
Trap	
Trap ID	171
Trap MIB Name	automaticFileTransferFeatureFailure

8089

Explanation

An NPA-NXX split activation completed successfully.

Recovery

No action required; for information only.

Event Details

Table 184: Event 8089 Details

GUI Notification	
Severity	Cleared
Text	Activate Split Successful OldNPA=<old_NPA> NewNPA=<new_NPA> NXX=<NXX>
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	

Trap ID	10
Trap MIB Name	npaSplitActOk

8090

Explanation

An NPA-NXX split activation failed.

Recovery

Perform and audit and reconcile of NPA Split information at the network element.

Event Details

Table 185: Event 8090 Details

GUI Notification	
Severity	Critical
Text	Activate Split Failed OldNPA=<old_NPA> NewNPA=<new_NPA> NXX=<NXX>
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	172
Trap MIB Name	npaSplitActFailed

8091

Explanation

At least one active NPA-NXX split is past its end date and needs to be deleted.

Recovery

Do the following:

1. View all split objects (for information, refer to the LSMS Database *Administration Manual*) to determine which objects have end dates that have already passed.
2. Delete the objects whose end dates have passed (for information, refer to the LSMS Database *Administration Manual*).

Event Details

Table 186: Event 8091 Details

GUI Notification	
Severity	Major
Text	Active Splits Are Past Their End Dates
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	173
Trap MIB Name	activeSplitsPastEndDates

8096

Explanation

The EMS/NE has rejected the NPANXX Split operation indicated by <operation>, and the NPANXX value in the transaction could not be determined.

Recovery

Look in the transaction log file, `/var/TKLC/lsms/logs/<CLLI>/LsmsTrans.log.MMDD`, and locate the NE's response to the NPANXX Split command to determine why the command failed. Delete and re-enter the NPANXX Split data correctly, which will cause the LSMS to try to command again.

Event Details

Table 187: Event 8096 Details

GUI Notification

Severity	Major
Text	<CLLI>: NPANXX Split <operation> Failed
Surveillance Notification	
Text	None
Source	
Frequency	
Trap	
Trap ID	178
Trap MIB Name	EmsNeRejNpaNxxSplitNotDetermined

8097

Explanation

The EMS/NE has rejected the NPANXX Split operation indicated by <operation> for the indicated NPANXX value.

Recovery

Look in the transaction log file, `/var/TKLC/lsms/logs/<CLLI>/LsmsTrans.log.MMDD`, and locate the NE's response to the NPANXX Split command to determine why the command failed. Delete and re-enter the NPANXX Split data correctly, which will cause the LSMS to try to command again.

Event Details

Table 188: Event 8097 Details

GUI Notification	
Severity	Major
Text	<CLLI>: NPANXX Split <operation> Failed for New NPANXX <NPANXX>
Surveillance Notification	
Text	None

Source	
Frequency	
Trap	
Trap ID	179
Trap MIB Name	EmsNeRejectedNpaNxxSplit

8098

Explanation

The LSMS is not able to confirm the physical connectivity with the directly connected query server identified by `<hostname>`. The problem may be one of the following:

- Physical connectivity issues between the LSMS and directly connected Query Server.
- The query server host name is not associated with the appropriate Internet Protocol (IP) address in `/etc/hosts` file.
- The Internet Protocol (IP) address specified for the special replication user for the for the query server is incorrect.
- The proper TCP/IP ports are not open in the firewall(s) between the LSMS and the query servers.

Recovery

- Check the physical connectivity of the LSMS to the query server.
- Check that the query server hosts name is associated with corresponding Internet Protocol (IP) addresses in `/etc/hosts` file.
- Verify that the IP address for the query server is correct. Display the IP address of all configured query servers by using the `$LSMS_TOOLS_DIR/lsmsdb -c queryservers` command.
- Verify that the firewall TCP/IP port configuration is set correctly for both the LSMS and query servers directly connected to the LSMS (refer to Appendix A, "Configuring the Query Server," of the LSMS *Configuration Manual* for information about port configuration for firewall protocol filtering).

Event Details

Table 189: Event 8098 Details

GUI Notification	
Severity	Major
Text	`Query Server <hostname> Physical Connection Lost`

Surveillance Notification	
Text	`Query Server=<hostname> Physical Conn Lost`
Source	Active Server
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
SNMP Trap	
Trap ID	180
Trap MIB Name	physicalConnectivityWithQueryServerLost

8099

Explanation

The query server identified by `<hostname>` does not have a replication connection established with the LSMS. The problem may be one of the following:

- Query server cannot establish a connection with the master.
- Query server not properly configured to connect to the master.
- A query that succeeded on the master failed on the query server.
- The binary log(s) that are needed by the query server to resynchronize itself to its master no longer exist.
- Data on the query server does not agree with what is on the master when the binary log was started.
- Replication was stopped at the query server by a user.

Recovery

1. At the query server, perform the following substeps:
   a. Start the MySQL command line utility on the slave server:
      ```
      # cd /opt/TKLCplat/mysql/bin
      # mysql -u root -p
      Enter password:
      <Query Server/s MySql root user password>
      ```
   b. Determine whether the query server is running by entering the following command and looking at the Slave_IO_Running and Slave_SQL_Running column values.
      ```
      mysql> SHOW SLAVE STATUS \G;
      ```

- If the Slave_IO_Running and Slave_SQL_Running column values show that the slave is not running, verify the query server's `/usr/mysql1/my.cnf` option file (see "MySQL Replication Configuration for Query Servers," in Appendix A, "Configuring the Query Server," of the LSMS *Configuration Manual*) and check the error log (`/usr/mysql1/<hostname>.err`) for messages.
- If the Slave_IO_Running and Slave_SQL_Running column values show that the slave (query server) is running, enter the following command to verify whether the slave established a connection with the master (LSMS or another query server acting as a master/slave).

  ```
  mysql> SHOW PROCESSLIST;
  ```

  Find the thread with the system user value in the `User` column and none in the `Host` column, and check the `State` column. If the `State` column says "connecting to master," verify that the master hostname is correct, that the DNS is properly set up, whether the master is actually running, and whether it is reachable from the slave (refer to Appendix A, "Configuring the Query Server," of the LSMS *Configuration Manual* for information about port configuration for firewall protocol filtering if the master and slave are connecting through a firewall).
- If the slave was running, but then stopped, enter the following command:

  ```
  mysql> SHOW SLAVE STATUS;
  ```

  Look at the output. This error can happen when some query that succeeded on the master fails on the slave, but this situation should never happen while the replication is active if you have taken a proper snapshot of the master and never modify the data on the slave outside of the slave thread.

2. However, if this is not the case, or if the failed items are not needed and there are only a few of them, try the following:
   a. First see if there is some stray record in the way on the query server. Understand how it got there, then delete it from the query server database and run SLAVE START.
   b. If the above does not work or does not apply, try to understand if it would be safe to make the update manually (if needed) and then ignore the next query from the LSMS.
   c. If you have decided you can skip the next query, enter one of the following command sequences:
      - To skip a query that uses AUTO_INCREMENT or LAST_INSERT_ ID(), enter:

        ```
        mysql> SET GLOBAL SQL_SLAVE_SKIP_COUNTER=2;
        mysql> SLAVE START;
        ```

        Queries that use AUTO_INCREMENT or LAST_INSERT_ ID() take two events in the binary log of the master.
      - Otherwise, enter:

        ```
        mysql> SET GLOBAL SQL_SLAVE_SKIP_COUNTER=1;
        mysql> SLAVE START;
        ```

3. If you are sure the query server database started out perfectly in sync with the LSMS database, and no one has updated the tables involved outside of the slave thread, contact the Tekelec

Customer Care Center (see *"Emergency Response"* on page 5), so you will not have to do the above steps again.

4. If all else fails, read the error log, `/usr/mysql/<hostname>.err`. If the log is big, run the following command on the slave:

   ```
   grep -i slave /usr/mysql1/<hostname>.err
   ```

   (There is no generic pattern to search for on the master, as the only errors it logs are general system errors. If it can, the master will send the error to the slave when things go wrong.)

   - If the error log on the slave conveys that it could not find a binary log file, this indicates that the binary log files on the master have been removed (purged). Binary logs are periodically purged from the master to prevent them from growing unbounded and consuming large amounts of disk resources. However, if a query server was not replicating and one of the binary log files it wants to read is purged, it will be unable to replicate once it comes up. If this occurs, the query server is required to be reset with another snapshot of data from the master or another query server (see *Reload a Query Server Database from the LSMS* on page 402 and *Reload a Query Server Database from Another Query Server* on page 406).
   - When you have determined that there is no user error involved, and replication still either does not work at all or is unstable, please contact the Tekelec Customer Care Center (see *"Emergency Response"* on page 5).

Event Details

Table 190: Event 8099 Details

GUI Notification	
Severity	Major
Text	Query Server <hostname> Replication Connection Lost
Surveillance Notification	
Text	Query Server=<hostname> Replication Conn Lost
Source	Active Server
Frequency	As soon as condition occurs, and at five-minute intervals as long as condition exists
SNMP Trap	
Trap ID	181
Trap MIB Name	queryServerConnectionWithLsmsLost

8100

Explanation

The SV/NPB storage database has exceeded the 90 percent usage threshhold. The usage is currently at the percentage represented in the notification text displayed on the GUI.

Recovery

Contact the Tekelec Customer Care Center to arrange for additional features to support a greater quantity of ported numbers.

Event Details

Table 191: Event 8100 Details

GUI Notification	
Severity	Event
Text	SV/NPB Storage Exceeds 90 percent <%>
Surveillance Notification	
Text	Notify:Sys Admin - SV/NPB threshold 90%
Source	Active server
Frequency	Every 5 minutes
Trap	
Trap ID	194
Trap MIB Name	svNpbLimit90Usage

Platform Alarms

This section describes the following:

- *How Platform Alarms Are Reported* on page 359
- *How to Decode Platform Alarms* on page 359
- *Platform Alarms* on page 360

How Platform Alarms Are Reported

Each server runs `syscheck` periodically and reports any problems found through platform alarms. The severity of platform alarms is one of the following:

- Critical, reported through event 4300
- Major, reported through event 4200
- Minor, reported through event 4100

When one or more problems in a given category has been found, the server reports one corresponding event notification to its Surveillance log and its serial port 1. If the server is not the active server, it also sends the event notification to the active server. The active server reports its own platform events to its own Surveillance log and to its Serial Port 1, and also sends an SNMP trap and displays a GUI notification for either its own platform events or for the non-active server's platform events.

Each of the events 4100, 4200, and 4300 contain a 16-character hexadecimal bitmasked string that indicates all of the platform events in that category that currently exist. To decode which platform events exist, use the procedure described in *How to Decode Platform Alarms* on page 359.

Each time the combination of platform events in a given category changes, a new event is reported. Following is an example of how platform events are reported:

1. At first, only one major platform event is reported on the standby server. A 4200 event with the alarm number of the event is reported.
2. One minute later, another platform event exists on the standby server (and the first one still exists). Another 4200 event is reported, with a bitmasked string that indicates both of the platform events that exist.
3. One minute later, another platform event exists on the standby server (and the previous ones still exist). Another 4200 event is reported, with a bitmasked string that indicates all of the platform events that exist.
4. One minute later, the first platform event is cleared. Another 4200 event is reported, with a bitmasked string that indicates the two platform events that still exist.

How to Decode Platform Alarms

Use the following procedure to determine all the platform alarms that exist in a given category:

1. Look in *Table 192: LSMS Platform Alarms* on page 360 to see if the alarm number is shown there.
   - If the alarm number matches one of the alarms shown in this table, only one alarm (the one that appears in the table) is being reported and you have completed this procedure.
   - If the alarm number does not match one of the alarms shown in this table, perform the remaining steps of this procedure.
2. Log in as any user to either server.
3. Enter the following command to decode the reported hexadecimal alarm string:

   ```
   $ /usr/TKLC/plat/bin/almdecode <alarm_number>
   ```

   The output displays the information about the alarm category and displays the text string for each of the alarms that is represented by the string. For example, if you enter:

   ```
   $ /usr/TKLC/plat/bin/almdecode 3000000000000180
   ```

the following text displays:

```
The string alarm value comes from the Major Platform alarm category.
```

The following alarms are encoded within the hex string:

```
Server Swap Space Shortage FailureServer Provisioning Network Error
```

You have now completed this procedure.

Platform Alarms

Table 192: LSMS Platform Alarms on page 360 shows all the platform alarms that can be reported by LSMS servers. For recovery procedures for these alarms, contact the Tekelec Customer Care Center.

Table 192: LSMS Platform Alarms

Alarm Number	Alarm Text	Category	Indicates:
1000000000000200	Uncorrectable ECC Memory Error	Critical	The T1100 chipset has detected an uncorrectable (multiple-bit) error that the ECC (Error-Correcting Code) circuitry in the memory is unable to correct.
3000000000000001	Server Fan Failure	Major	One or more of the fans in the system has failed.
3000000000000002	Server Internal Disk Error	Major	The server has experienced issues replicating data to one or more of its mirrored disk drives. This could indicate that one of the server's disks has either failed or is approaching failure. The customer should replace the failed disk as soon as possible.

Alarm Number	Alarm Text	Category	Indicates:
3000000000000008	Server Platform Error	Major	A major-class platform error such as a corrupt system configuration or missing files, or indicates that `syscheck` itself is corrupt.
3000000000000010	Server File System Error	Major	`syscheck` was unsuccessful in writing to at least one of the server's file systems.
3000000000000020	Server Platform Process Error	Major	Either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.
3000000000000080	Server Swap Space Shortage Error	Major	The server has less than 10,000 kilobytes of swap space left. The server's swap space is in danger of being depleted. This is usually caused by a process that has allocated a very large amount of memory over time.
3000000000000800	Server Sync Network Error	Major	The sync network between the two servers has lost all connectivity.
3000000000001000	Server Disk Space Shortage Error	Major	One of the following conditions has occurred:

Alarm Number	Alarm Text	Category	Indicates:
			• A filesystem has exceeded a failure threshold, which means that more than 90% of the available disk storage has been used on the filesystem. • More than 90% of the total number of available files have been allocated on the filesystem. • A filesystem has a different number of blocks than it had at install.
3000000000002000	Server Default Route Network Error	Major	The server's default network route is experiencing a problem. Running `syscheck` in verbose mode will provide information about which type of problem.
3000000000004000	Server Temperature Error	Major	The internal temperature of the server is unacceptably high.
3000000000008000	Server Mainboard Voltage Error	Major	One or more of the monitored voltages on the server mainboard have been detected to be out of the normal expected operating range.
3000000000010000	Server Power Feed Unavailable	Major	One of the power feeds to the server has failed.

Alarm Number	Alarm Text	Category	Indicates:
3000000000020000	Server Disk Health Test Error	Major	Either the hard drive has failed or failure is imminent.
3000000000040000	Server Disk Unavailable Error	Major	The `smartd` service is not able to read the disk status because the disk has other problems that are reported by other alarms. This alarm appears only while a server is booting.
3000000000100000	Device Interface Error	Major	A device network interface has a problem. Running `syscheck` in verbose mode will provide information about which type of problem.
3000000000200000	Correctable ECC Memory Error	Major	The chipset has detected a correctable (single-bit) memory error that has been corrected by the ECC (Error-Correcting Code) circuitry in the memory.
3000000000400000	Server Power Supply A Error	Major	Power supply A (feed A) has failed.
3000000000800000	Server Power Supply B Error	Major	Power supply B (feed B) has failed.
3000000001000000	Breaker Panel Feed Error	Major	The server is not receiving information from the breaker panel relays.

Alarm Number	Alarm Text	Category	Indicates:
3000000002000000	Breaker Panel Breaker Error	Major	A power fault has been identified by the power panel.
3000000004000000	Breaker Panel Monitoring Error	Major	The hardware and/or software that monitors the breaker panel has failed. This could mean there is a problem with the file I/O libraries, the serial device drivers, or the serial hardware itself.
3000000008000000	HA Keepalive Error	Major	One or both of the configured HA heartbeat channels (either the serial cable or the sync network) has a problem. Running `syscheck` in verbose mode will provide information about which channel has the problem.
5000000000000001	Server Disk Space Shortage Warning	Minor	One of the following conditions has occurred: • A filesystem has exceeded a warning threshold, which means that more than 80% (but less than 90%) of the available disk storage has been used on the filesystem. • More than 80% (but less than 90%) of the total number

Alarm Number	Alarm Text	Category	Indicates:
			of available files have been allocated on the filesystem.
5000000000000002	Server Application Process Error	Minor	Either the minimum number of instances for a required process are not currently running or too many instances of a required process are running.
5000000000000004	Server Hardware Configuration Error	Minor	One or more of the server's hardware components are not in compliance with Tekelec specifications (refer to the *Tekelec 1100* Application Server *Hardware Manual*).
5000000000000020	Server Swap Space Shortage Warning	Minor	The server has less than 50,000 kilobytes of swap space left. The server's swap space is in danger of being depleted. This is usually caused by a process that has allocated a very large amount of memory over time.
5000000000000080	Server Temperature Warning	Minor	The internal temperature within the server is outside of the normal operating range. A Server Fan Failure may also exist along with the Server Temperature Warning.

Alarm Number	Alarm Text	Category	Indicates:
5000000000000100	Server Core File Detected	Minor	A process has failed and debug information is available.
5000000000000200	Server NTP Daemon Not Synchronized	Minor	The NTP daemon (background process) has been unable to locate a server to provide an acceptable time reference for synchronization.
5000000000000400	Server CMOS Battery Voltage Low	Minor	The CMOS battery voltage has been detected to be below the expected value. This alarm is an early warning indicator of CMOS battery end-of-life failure which will cause problems in the event the server is powered off.
5000000000000800	Server Disk Self Test Warning	Minor	A non-fatal disk issue (such as a sector cannot be read) exists.
5000000000001000	Device Warning	Minor	A device has a network problem. Running `syscheck` in verbose mode will provide information about which type of problem.
5000000000002000	Device Interface Warning	Minor	A device interface has a network problem. Running `syscheck` in verbose mode will

Alarm Number	Alarm Text	Category	Indicates:
			provide information about which type of problem.
5000000000004000	Server Reboot Watchdog Initiated	Minor	The server has been rebooted due to a hardware watchdog.
5000000000008000	Server HA Failover Inhibited	Minor	Server has been either automatically or manually inhibited from switchover and is not ready to become active. The system is running in simplex mode and switchover cannot occur while this condition is present.
5000000000010000	Server HA Active to Standby Transition	Minor	This event is reported by the active server to indicate that switchover is in progress. The server reporting this event is currently shutting down application processes but will remain active until this transition is complete.
5000000000020000	Server HA Standby to Active Transition	Minor	This event is reported by the standby server to indicate that switchover is in progress. The server reporting this event is about to become the active server but will remain standby

Alarm Number	Alarm Text	Category	Indicates:
			until ready to provide service.

Appendix C

Downloading Files from an NPAC to the LSMS

Topics:

- *Overview Page 370*
- *Prerequisite Information Page 371*
- *File Naming Conventions Page 372*
- *NPAC-LSMS Download Procedure Page 376*
- *Copying Files to Other Server If Switchover Occurs Page 388*

This chapter describes how you can manually FTP bulk data download (BDD) files from the NPAC to the LSMS and merge those data files into an LSMS regional database.

Overview

This chapter describes how you can manually FTP bulk data download (BDD) files from the NPAC to the LSMS and merge those data files into an LSMS regional database.

Following are some examples of situations in which you would use the BDD procedure described in this chapter (see *NPAC-LSMS Download Procedure* on page 376):

- To perform a download of NPAC data after an LSMS site failure (for more information about restoring an LSMS site, see *Recovering from Site Failures* on page 131)
- To perform a download of NPAC data when migrating an LSMS
- To update NPA split information as part of a procedure to correct an active NPA Split Entry made in error (for more information about this procedure, refer to "Reversing (Correcting) an NPA Split Entry Made in Error" in the LSMS Database *Administration Manual*)

Time Range BDD and Object BDD/Object Range BDD

Note: Object ranges are used so that potentially very large files can be broken down into smaller files based on NPA-NXX (for SVs) or NPA-NXX-X (for NPBs) ranges. Because of the much smaller number of LRN, NPA-NXX, NPA-NXX-X, or SPID objects, ranges are not supported for these data file types.

If you have installed the optional feature, NANC 3.2 Mass Update of SPID and BDD Enhancements, you can download files either for objects/object ranges or for time ranges (however, time range files are not supported for SPIDs).

Whenever you need to perform a download after a site failure or when migrating an LSMS, determine if it necessary to perform an Object BDD/Object Range BDD, or whether a Time Range BDD would suffice; a Time Range BDD can take many hours less to complete than an Object BDD/Object Range BDD.

Primarily, a Time Range BDD differs from an Object BDD/Object Range BDD in that:

- Each entry in the Time Range BDD file is processed as a create, modify, or delete in the LSMS databases; *no data* is deleted from the LSMS database prior to the import. Each entry in the Object BDD/Object Range BDD file is processed only as a create in the LSMS databases; *all data* in the LSMS database that meets the range criteria is deleted prior to the import.
- A Time Range BDD enables you to download a file from an NPAC that contains porting data for a specific period of time (you can specify begin and end timestamp values); an Object Range BDD does not allow you to specify begin and end timestamp values (the default values, 00-00-0000000000 and 99-99-9999999999, are assumed).

  Note: Time Range SPID BDD files are not supported.

A Time Range BDD is not appropriate for correcting NPA Split information or EDR Conversion data.

NPAC-LSMS Download Procedure Summary

The following procedure is an outline of the detailed procedure shown in *NPAC-LSMS Download Procedure* on page 376.

CAUTION: The following procedure requires the connection between the LSMS and each regional NPAC that needs to have files downloaded be aborted (when you stop the regional agent in *Step 27* on page 381) before the NPAC builds the files to be sent to the LSMS. The connection must be aborted so that data can be properly resynchronized after the download of files completes. Therefore, the normal transmission of NPAC data from the LSMS to the connected NEs will temporarily be precluded during this procedure. It is recommended that you contact the Tekelec *Customer Care Center* on page 5 before performing this procedure.

Note: If an automatic or manual switchover occurs while files are being downloaded from the NPAC or between the time files are downloaded from the NPAC and the time they are imported into the LSMS database, perform the appropriate procedure described in *Copying Files to Other Server If Switchover Occurs* on page 388.

Note: Before you start this procedure, it is recommended that you contact the Tekelec Customer Care Center. If you encounter any problems in the procedure, you must call the Tekelec Customer Care Center.

1. Request the appropriate file from the NPAC for a given SPID and region.
2. Use FTP to download that file when the NPAC indicates the file is available.
3. Move to another folder all the files currently residing in the NPAC import folder (`/var/TKLC/lsms/free/data/npacftp/<region>`, where `<region>` is the region that you are importing).
4. Untar the BDD file (Object BDD/Object Range BDD file or Time Range BDD file) in this `<region>` folder using the following command:

   ```
   tar -zxvf filename.tar.gz
   ```

5. Run `/usr/TKLC/lsms/bin/import <region>` for the appropriate region.
6. Answer the questions presented by the import script.

You have now completed this procedure.

Prerequisite Information

Before starting this procedure, obtain the following site-specific information. Record this information on your recovery preparation worksheet (see *Recovery Preparation Worksheet* on page 392).

- A login name and password for each supported NPAC. This login and password have been previously issued by the regional NPAC.
- The FTP IP address of each supported NPAC.
- The FTP directory names where the files are located on each supported NPAC.
- Data file names you need to download. To determine the naming convention for each type of NPAC data file, see *File Naming Conventions* on page 372.
- Contact the NPAC of the region for which data files are required and request that the files you need be copied into the NPAC's FTP directory.

File Naming Conventions

All BDD file names include a creation timestamp, which is represented as **<create>**. Time Range BDD file names also contain start (**<start>**) and end (**<end>**) timestamps. All timestamps are represented as **DD-MM-YYYYhhmmss** where:

DD represents a two-digit day

MM represents a two-digit month

YYYY represents a four-digit year

hh represents a two-digit hour

mm represents a two-digit minute

ss represents a two-digit second

An example timestamp is 11-10-2006123015.

For Object Range BDD files, `<start>` is always 00-00-0000000000 and `<end>` is always 99-99-9999999999. These are the default values.

Table 193: Determining Naming Conventions for NPAC Data Files on page 372 references the pages where you can find information about file naming conventions for each data type:

Table 193: Determining Naming Conventions for NPAC Data Files

Type of Data File	See:
Subscription Version (Object Ranges and Time Ranges are supported)	*Table 194: NPAC File Naming Convention for Subscription Version Data File* on page 373
Number Pool Block (Object Ranges and Time Ranges are supported)	*Table 195: NPAC File Naming Convention for Number Pool Block Data File* on page 374
LRN, NPA-NXX, and NPA-NXXX (Only Objects are supported)	*Table 196: NPAC File Naming Convention for LRN, NPA-NXX, and NPA-NXXX Network Data Files* on page 375
SPID (Only Objects are supported)	*Table 197: NPAC File Naming Convention for SPID Network Data File* on page 376

Note: Object ranges are used so that potentially very large files can be broken down into smaller files based on NPA-NXX (for SVs) or NPA-NXX-X (for NPBs) ranges. Because of the much smaller number of LRN, NPA-NXX, NPA-NXX-X, or SPID objects, ranges are not supported for these data file types.

Subscription Version File Naming Convention

The file name for subscription version files is represented as `<NPANXX-NPANXX>`, which indicates the range of NPA-NXX values contained in the download file. The file extension values depend on whether you are requesting a file for an Object Range BDD or for a Time Range BDD, as shown in *Table 194: NPAC File Naming Convention for Subscription Version Data File* on page 373.

Table 194: NPAC File Naming Convention for Subscription Version Data File

Range Type	Naming Convention
Object Range BDD	`<NPANXX-NPANXX>.<create>`[2] `.00-00-0000000000.99-99-9999999999`
Time Range[1] BDD	`<NPANXX-NPANXX>.<create>.<start>.<end>`[2]

[1] Time Range files are supported only if you have installed the NANC 3.2 feature

[2] For format of `<create>`, `<start>`, and `<end>`, see *File Naming Conventions* on page 372.

Following are examples of uses for subscription version BDD files:

- If you need to bulk download all subscription versions from the NPAC, use the following file name:

  ```
  <000000-999999>.<create>.00-00-0000000000.99-99-9999999999
  ```

- If you need to bulk download all subscription versions for a time period from midnight February 12, 2006 to midnight February 13, 2006 in a file created February 14, 2006 at 9:00 a.m., use the following file name:

  ```
  <000000-999999>.14022006090000.12022006000000.13022006000000
  ```

- If you need files to correct an NPA split, specify three Object Range files that have the same NPANXX values before and after the hyphen:
  - One file with the old NPANXX value
  - One file with the correct new NPANXX value
  - One file with the erroneous new NPANXX value

  For example, if an NPA split was erroneously entered from 909-860 to 123-860 instead of correctly from 909-860 to 124-860, specify the following files:

  - 909860-909860
  - 124860-124860
  - 123860-123860

  Because no file extension is specified in these files, the default values of `00-00-0000000000.99-99-9999999999` are assumed.

Number Pool Block File Naming Convention

The file name for number pool block files is represented as `<NPANXXX-NPANXXX>`, which indicates the range of EDR NPA-NXXX values contained in the download file. The file extension values depend on whether you are requesting a file for an Object Range BDD or for a Time Range BDD, as shown in *Table 195: NPAC File Naming Convention for Number Pool Block Data File* on page 374.

Table 195: NPAC File Naming Convention for Number Pool Block Data File

Range Type	Naming Convention
Object Range BDD	`<NPANXXX-NPANXXX>.<create>`[2] `.00-00-0000000000.99-99-9999999999`
Time Range[1] BDD	`<NPANXXX-NPANXXX>.<create>.<start>.<end>`[2]

[1] Time Range files are supported only if you have installed the NANC 3.2 feature

[2] For format of `<create>`, `<start>`, and `<end>`, see *File Naming Conventions* on page 372.

These file types exist only if the NPAC supports Efficient Data Representation (EDR). Following are examples of uses for number pool block BDD files:

- If you need to bulk download all number pool blocks from the NPAC, use the following file name:

  ```
  <0000000-9999999>.<create>.00-00-0000000000.99-99-9999999999
  ```

- If you need to bulk download all number pool blocks for a time period from midnight February 12, 2006 to midnight February 13, 2006 in a file created February 14, 2006 at 9:00 a.m., use the following file name:

  ```
  <0000000-9999999>.14022006090000.12022006000000.13022006000000
  ```

- If you need files to correct an NPA split, specify three files, each with the NPANXX value followed by a 0 before the hyphen and the NPANXX value followed by a 9 after the hyphen:
  - One file with the old NPANXX value
  - One file with the correct new NPANXX value
  - One file with the erroneous new NPANXX value

  For example, if an NPA split was erroneously entered from 909-860 to 123-860 instead of correctly from 909-860 to 124-860, specify the following files:
  - 9098600-9098609
  - 1248600-1248609
  - 1238600-1238609

Because no file extension is specified in these files, the default values of `00-00-0000000000.99-99-9999999999` are assumed.

LRN, NPA-NXX, and NPA-NXXX File Naming Convention

Note:

In contrast to SVs and NPBs data file types, there are a much smaller number of LRN, NPA-NXX, and NPA-NXX-X objects; therefore, ranges are not supported for these data file types, as shown in *Table 196: NPAC File Naming Convention for LRN, NPA-NXX, and NPA-NXXX Network Data Files* on page 375.

- The file name for LRN files is represented as `<LRN>`, which indicates the LRN value contained in the download file.
- The file name for NPA-NXX files is represented as `<NPANXX>`, which indicates the NPA-NXX value contained in the download file.
- The file name for NPA-NXXX files is represented as `<NPANXX>`, , which indicates the EDR NPA-NXXX value contained in the download file. This file type exists only if the NPAC supports Efficient Data Representation (EDR).

The file extension values depend on whether you are requesting a file for an Object BDD or for a Time Range BDD, as shown in *Table 196: NPAC File Naming Convention for LRN, NPA-NXX, and NPA-NXXX Network Data Files* on page 375.

Table 196: NPAC File Naming Convention for LRN, NPA-NXX, and NPA-NXXX Network Data Files

Type	Naming Convention
Object BDD	`<LRN>.<create>`[2] `.00-00-0000000000.99-99-9999999999`
	`<NPANXX>.<create>`[2] `.00-00-0000000000.99-99-9999999999`
	`<NPANXX>.<create>`[2] `.00-00-0000000000.99-99-9999999999`
Time Range[1] BDD	`<LRN>.<create>.<start>.<end>`[2]
	`<NPANXX>.<create>.<start>.<end>`[2]
	`<NPANXXX>.<create>.<start>.<end>`[2]

[1] Time Range files are supported only if you have installed the NANC3.2 feature

[2] For format of `<create>`, `<start>`, and `<end>`, see *File Naming Conventions* on page 372.

SPID File Naming Convention

Note:

In contrast to SVs and NPBs data file types, there is a much smaller number of SPID objects; therefore, ranges are not supported for this data file type, as shown in *Table 197: NPAC File Naming Convention for SPID Network Data File* on page 376.

The SPID naming convention only applies to Object BDD files; Time Range is not supported. The file name for SPID files is represented as <SPID>, which indicates the SPID value contained in the download file..

Table 197: NPAC File Naming Convention for SPID Network Data File

Type	Naming Convention
Object BDD	<SPID>.<create> [2] .00-00-0000000000.99-99-9999999999
[2] For format of <create>, <start>, and <end>, see *File Naming Conventions* on page 372.	

Only the <create> timestamp field is supported.

Because no file extension is specified in these files, the default values of 00-00-0000000000.99-99-9999999999 are assumed.

NPAC-LSMS Download Procedure

Use the following procedure to perform a download of files from an NPAC to the LSMS. The example output shown in the procedure is for Time Range BDD files that include Number Pooling Efficient Data Representation (EDR). File formats for other download types vary, as described in *File Naming Conventions* on page 372. For more information about EDR, refer to the LSMS Database *Administration Manual*.

Note: Before you start this procedure, it is recommended that you contact the Tekelec Customer Care Center. If you encounter any problems in the procedure, you must call the Tekelec Customer Care Center.

CAUTION: The following procedure requires the connection between the LSMS and each regional NPAC that needs to have files downloaded be aborted (when you stop the regional agent in step 26) before the NPAC builds the files to be sent to the LSMS. The connection must be aborted so that data can be properly resynchronized after the download of files completes. Therefore, the normal transmission of NPAC data from the LSMS to the connected NEs will temporarily be precluded during this procedure. It is recommended that you contact the Tekelec Customer Care Center before performing this procedure.

Note: If an automatic or manual switchover occurs while files are being downloaded from the NPAC or between the time files are downloaded from the NPAC and the time they are imported into the LSMS database, perform the appropriate procedure described in *Copying Files to Other Server If Switchover Occurs* on page 388.

1. Ensure that you have the necessary information, as described in *Prerequisite Information* on page 371.
2. Log in to the LSMS active server as lsmsadm.
3. Change to the directory that contains the current LSMS version:

   ```
   $ cd /var/TKLC/lsms/free/data/npacftp/<region>
   ```

4. Verify that the correct directory was accessed by entering the following command:
   ```
   $ pwd
   ```
   The correct output is:
   ```
   /var/TKLC/lsms/free/data/npacftp/<region>
   ```
5. Determine whether any files are currently contained in this directory:
   ```
   $ ls -l
   ```
6. If the output shows any files, delete them by entering the following command:
   ```
   $ rm *
   ```
   Note: Though the steps in this procedure refer to the use of FTP, you may use SFTP instead.
7. Use FTP to connect to the NPAC by entering the following command, where `<NPAC_IP_address>` is the decimal version of the NPAC's IP address, recorded on your worksheet, as described in *Prerequisite Information* on page 371:
   ```
   $ ftp <NPAC_IP_address>
   ```
   An example command line follows:
   ```
   $ ftp 208.143.38.10
   ```
8. When prompted, enter your NPAC login name and password, recorded on your worksheet, as described in *Prerequisite Information* on page 371.
9. Change to the NPAC's FTP directory by entering the following command, where `<NPAC_FTP_directory>` is the regional directory as recorded on the your worksheet that corresponds to the region selected in *Step 3* on page 376:
   ```
   ftp> cd <NPAC_FTP_directory>
   ```
10. Display the contents of the NPAC's FTP directory by entering the following command:
    ```
    ftp> ls
    ```
    - Output similar to the following appears.
      ```
      200 PORT command successful.
      150 Opening ASCII mode data connection for file list.
      000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
      0000000-9999990.07-11-2004023849.07-10-2004023849.07-11-2004023849
      LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849
      NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
      NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
      SPID.07-11-2000023849
      226 Transfer complete.
      70 bytes received in 0.026 seconds (2.6 Kbytes/s)
      ```
    - If you are converting a regional database to support EDR, output similar to the following appears:
      ```
      200 PORT command successful.
      150 Opening ASCII mode data connection for file list.
      0000000-9999990.07-11-2004023849.07-10-2004023849.07-11-2004023849
      NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
      226 Transfer complete.
      20 bytes received in 0.026 seconds (2.6 Kbytes/s)
      ```

11. Change to noninteractive mode by entering the following command:

```
ftp> prompt
```

Output similar to the following appears:

```
Interactive mode off
```

12. Transfer the files you need as follows:

- If you are downloading files from the NPAC after a site failure, enter the following command to transfer all the files in the NPAC's FTP directory <NPAC_FTP_directory> to the LSMS's regional directory /var/TKLC/lsms/free/data/npacftp/<region>:

  ```
  ftp> mget *
  ```

- If you are reversing an NPA split, enter commands similar to the following commands (these commands use the values from the example) to transfer the subscription files and NPB files for the old NPANXX and the erroneous new NPANXX from the NPAC's FTP directory <NPAC_FTP_directory> to the LSMS's regional directory /var/TKLC/lsms/free/data/npacftp/<region>:

  ```
  ftp> mget 909860*
  ftp> mget 123860*
  ftp> mget 124860*
  ```

- If you are converting a regional database to support EDR, enter the following commands to transfer the EDR files from the NPAC's FTP directory <NPAC_FTP_directory> to the LSMS's regional directory /var/TKLC/lsms/free/data/npacftp/<region>:

  ```
  ftp> mget 0000000-9999999*
  ftp> mget NPANXXX*
  ```

13. Output similar to the following appears (the example shows only Time Range BDD files for downloading):

```
200 PORT command successful.
150 Opening BINARY mode data connection for
000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849 (17979 bytes).
###
226 Transfer complete.
local: 000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
remote: 000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
17979 bytes received in 0.18 seconds (le+02 Kbytes/s)
200 PORT command successful.
150 Opening BINARY mode data connection for
0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
(17979 bytes).
###
226 Transfer complete.
local: 0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
remote: 0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
17979 bytes received in 0.18 seconds (le+02 Kbytes/s)
200 PORT command successful.
150 Opening BINARY mode data connection for LRN.07-10-2000023849
(17979 bytes).
###
226 Transfer complete.
local: LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849
```

```
remote: LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849
17979 bytes received in 0.18 seconds (le+02 Kbytes/s)
200 PORT command successful.
150 Opening BINARY mode data connection for
NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849 (124831 bytes).
################
226 Transfer complete.
local: NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
remote: NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
124831 bytes received in 1 seconds (1.2e+02 Kbytes/s)
200 PORT command successful.
150 Opening BINARY mode data connection for
NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849 (124831 bytes).
################
226 Transfer complete.
local: NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
remote: NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
124831 bytes received in 1 seconds (1.2e+02 Kbytes/s)
200 PORT command successful.
150 Opening BINARY mode data connection for SPID.07-10-2004023849 (479 bytes).
#
226 Transfer complete.
local: SPID.07-10-2004023849 remote: 07-10-2004023849
479 bytes received in 0.018 seconds (27 Kbytes/s)
```

14. Exit FTP by entering the following command:

    ```
    ftp> quit
    ```

15. Ensure that the files just downloaded have appropriate permissions for all users by entering the following command:

    ```
    $ chmod 655 *
    ```

16. Enter the following command to verify that all the files in *Step 12* on page 378 transferred and that they now have read-write permission:

    ```
    $ ls -l
    ```

    Output similar to the following appears (the example shows only Time Range BDD files for downloading):

    ```
    total 3188358
    -rw-r-r-  1 lsmsadm  lsms 1608000001 Jul  11 02:38
    000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
    -rw-r-r-  1 lsmsadm  lsms 1608000001 Jul  11 02:38
    0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
    -rw-r-r-  1 lsmsadm  lsms 780001     Jul  11 02:38
    LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849
    -rw-r-r-  1 lsmsadm  lsms 6440001    Jul  11 02:38
    NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
    -rw-r-r-  1 lsmsadm  lsms 6440001    Jul  11 02:38
    NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
    -rw-r-r-  1 lsmsadm  lsms 239990     Jul  11 02:38 SPID.07-10-2000023849
    ```

    Note: It is recommended that you create a backup of your files before proceeding to the next step. To create a backup, enter the following command:

    ```
    $ mkdir /var/TKLC/lsms/free/data/npacftp/<region>/save
    ```

17. If you need files from another NPAC region, repeat *Step 3* on page 376 through *Step 16* on page 379.

18. If switchover has occurred, perform the appropriate procedure described in *Copying Files to Other Server If Switchover Occurs* on page 388.
19. Untar the BDD file (Object Range BDD file or Time Range BDD file) in the `<region>` folder using the following command:

    ```
    tar –zxvf filename.tar.gz
    ```

20. Enter the following command to display the number of lines in each bulk load file.

    ```
    $ wc -l *
    ```

    Note: Record the line count values (shown in **bold** below) for future reference.

    ```
    1892 000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
       0 000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
     892 0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
       0 0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
     250 LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849
       0 LRN.07-10-2004023849.07-11-2004023849
      23 NPANXX.07-10-2004023849.07-11-2004023849
       0 NPANXX.07-10-2004023849.07-11-2004023849
      12 NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
       0 NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
       0 SPID.07-10-2004023849
    ```

21. BDD files received from the NPAC require conversion before they can be imported into the LSMS database.

    The conversion must be performed by entering the following command for each file:

    ```
    $ cat orig_file_from_NPAC | tr "\015" "\012" > new_file_for_import
    ```

    (The file name must be changed. Tekelec recommends that you append a few characters, such as `.tr`, to the end of the file name. Maintaining most of the file name will make it easier to rename the files to the original file names, as instructed in *Step 23* on page 381) For example:

    ```
    $ cat 000000-999999.07-10-2000023849 | tr "\015" "\012" >
    000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849.tr
    $ cat 0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849 | tr
     "\015" "\012" >
    0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849.tr
    $ cat LRN.07-10-2000023849 | tr "\015" "\012" >
    LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849.tr
    $ cat NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849 | tr "\015"
    "\012" > NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849.tr
    $ cat NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849 | tr "\015"
     "\012" > NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849.tr
    $ cat SPID.07-10-2004023849 | tr "\015" "\012" >
    SPID.07-10-2004023849.tr
    ```

22. After ensuring all files have been converted, delete the original files.

    ```
    $ rm orig_file_from_NPAC
    ```

    For example:

    ```
    $ rm 000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
    $ rm 0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
    $ rm LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849
    $ rm NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
    $ rm NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
    $ rm SPID.07-10-2004023849
    ```

23. Rename each of the files that were converted in *Step 21* on page 380 back to the original NPAC file names by entering the following command for each file:

    ```
    $ mv new_file_for_import orig_filename_from_NPAC
    ```

    For example:

    ```
    $ mv 000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849.tr
     000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
    $ mv 0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849.tr
    0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
    $ mv LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849.tr
    LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849
    $ mv NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849.tr
    NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
    $ mv NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849.tr
    NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
    $ mv SPID.07-10-2004023849.tr SPID.07-10-2004023849
    ```

24. Verify that the files were properly converted by entering the following command:

    ```
    $ file *
    ```

    Properly converted files will be appended with the following information, `: ASCII text`, as shown in the example output below.

    ```
    000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849: ASCII text
    000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849: ASCII text
    0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849: ASCII text
    0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849: ASCII text
    LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849: ASCII text
    LRN.07-10-2004023849.07-11-2004023849: ASCII text
    NPANXX.07-10-2004023849.07-11-2004023849: ASCII text
    NPANXX.07-10-2004023849.07-11-2004023849: ASCII text
    NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849: ASCII text
    NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849: ASCII text
    SPID.07-10-2004023800: ASCII text
    SPID.07-10-2004023849: ASCII text
    ```

    Note: If the files are appended with `: ASCII text, with CR line terminators`, then the conversion performed in *Step 21* on page 380 failed. Contact the Tekelec Customer Care Center.

25. If switchover has occurred, perform the appropriate procedure described in *Copying Files to Other Server If Switchover Occurs* on page 388.
26. If the SWIM feature has been enabled, contact the Tekelec Customer Care Center to turn off SWIM.
27. Perform the following substeps to prevent the NPAC database from being updated while the files are being converted and copied in subsequent steps:
    a) Halt the LSMS agent for the region:

       ```
       $ $LSMS_DIR/lsms stop <region>
       ```

    b) From the LSMS GUI menu, select **Configure>LNP System>NPAC>Modify>Primary** and click the Activate Region checkbox so that is empty.

       For more information about this GUI window, refer to the LSMS *Configuration Manual*. Having this checkbox empty prevents the `sentryd` utility from attempting to automatically restart the regional agent.

28. You are now ready to run the `import` command.

Note: Do not run the `import` command while any of the following processes are also running: backups, starting a standby node (to change its state from UNINITIALIZED "INHIBITED" to STANDBY), running the `lsmsdb quickaudit` command, and creating query server snapshots, all of which use temporary storage space. If you try to run the `import` command while any of these processes are running, you may not have enough disk space to complete the process. Since backups can be run automatically, perform the procedure described in *Checking for Running Backups* on page 93 to ensure that no backups are running.

- If you are performing this procedure as part of reversing an NPA split, converting a regional database to support EDR, importing an incremental download of files from NPAC after a site failure, or importing files for any reason other than a complete regional bulk download, go to *Step 29* on page 382.
- If you are performing a complete regional bulk download from the NPAC, you can save a significant amount of time (which would be required to delete all existing entries in the database) by entering the following commands, where `<region>` is the name of the NPAC region:

  CAUTION: The following commands will delete all data in your regional database.

  Log into the active server and run both of the following commands:

  ```
  $ $LSMS_DIR/npac_db_setup remove <region>
  ```

  ```
  $ $LSMS_DIR/npac_db_setup_create <region>
  ```

29. Import data in the downloaded files into the regional database by entering the following command:

    ```
    $ $LSMS_DIR/import [-c] <region>
    ```

    For example:

    ```
    $ $LSMS_DIR/import -c MidAtlantic
    ```

    The `-c` option allows the import to continue on to the next line of the file even if errors occur. Output similar to the following indicates the progress of the LSMS processing:

    Note: In these examples, … on a line by itself indicates that output occurs, but its contents are not significant to this procedure.

    Note: If you do not specify the `-c` option and a failure, such as a syntax error, occurs during the import process, an error message is displayed and the import utility prompts the user with the following message: `Do you want to continue (Yes/No)?` If `n` is entered, the import utility operation is aborted. If `y` is entered, the import utility aborts its operation for the current download file and continues importing the remaining specified download files.

    If such an error occurs, be sure to perform the substeps shown in *Step 30* on page 385.

    - Output similar to the following appears as the LSMS deletes subscription versions, NPBs, LRNs, NPANXXs, and SPIDs in the regional LSMS database, reformats the NPAC data file, and places the data from the NPAC data file into the specified regional LSMS database.

      ```
      NPAC FTP directory: /var/TKLC/lsms/free/data/npacftp/Midwest
      The following NPAC download file(s) are available for import:
                  LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849
      ```

```
          NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
       NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849

SPID.07-10-2004023849
  000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
Import LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849
(Yes/No/All/Quit)?all
The following NPAC download files have been chosen to be imported:
          SPID.07-10-2004023849
NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
      NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849

LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849
  000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
Do you want to continue (Yes/No)?yes
Beginning Delete Process for SPID.07-10-2004023849
Delete Process Completed for SPID.07-10-2004023849
Beginning Download Process for SPID.07-10-2004023849
1000 ServiceProvNetwork instances written to MidwestDB
2000 ServiceProvNetwork instances written to MidwestDB
2351 ServiceProvNetwork instances written to MidwestDB

Import completed successfully.
Download Process Completed for SPID.11-07-2001145342

Beginning Delete Process for
NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
Delete Process Completed for
NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849

Beginning Download Process for
NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849

1000 ServiceProvNPA_NXX_X instances written to MidwestDB
2000 ServiceProvNPA_NXX_X instances written to MidwestDB
3000 ServiceProvNPA_NXX_X instances written to MidwestDB
4000 ServiceProvNPA_NXX_X instances written to MidwestDB
…
30000 ServiceProvNPA_NXX_X instances written to MidwestDB
30860 ServiceProvNPA_NXX_X instances written to MidwestDB
Import completed successfully.
Download Process Completed for
NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849

Beginning Delete Process for
NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849

Delete Process Completed for
NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849

Beginning Download Process for
NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849

90 ServiceProvNPA_NXX instances written to MidwestDB
1090 ServiceProvNPA_NXX instances written to MidwestDB
Import completed successfully.
Download Process Completed for
NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849

Beginning Delete Process for
LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849

Delete Process Completed for
```

```
LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849

Beginning Download Process for
LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849

1000 ServiceProvLRN instances written to MidwestDB
2000 ServiceProvLRN instances written to MidwestDB
3000 ServiceProvLRN instances written to MidwestDB
4000 ServiceProvLRN instances written to MidwestDB
4700 ServiceProvLRN instances written to MidwestDB
5700 ServiceProvLRN instances written to MidwestDB
Import completed successfully.
Download Process Completed for
LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849

Beginning Delete Process for
000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849

Will drop instances of:
Drop instances of class `SubscriptionVersion'
DROPPING INSTANCES.
Delete Process Completed for
000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849

Beginning Download Process for
000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849

1000 SubscriptionVersion instances written to MidwestDB
2000 SubscriptionVersion instances written to MidwestDB
3000 SubscriptionVersion instances written to MidwestDB
4000 SubscriptionVersion instances written to MidwestDB
4500 SubscriptionVersion instances written to MidwestDB
Import completed successfully.
Download Process Completed for 000000-999999.11-07-2001145342

Beginning Delete Process for
0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849

Will drop instances of:
Drop instances of class `NumberPoolBlock'
DROPPING INSTANCES.
Delete Process Completed for
0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849

Beginning Download Process for
0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849

1000 NumberPoolBlock instances written to MidwestDB
2000 NumberPoolBlock instances written to MidwestDB
Import completed successfully.
Download Process Completed for
0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
Script completed.
```

- If you are reversing an NPA split, in this step the LSMS deletes all subscription versions and NPBs for the old NPA-NXX and the erroneous new NPA-NXX in the regional LSMS database, reformats the NPAC data file, and places the data from the NPAC data file into the specified regional LSMS database. (Example output is not shown.)
- If you are converting a regional database to support EDR, in this step the LSMS formats the NPAC data file, and places the data from the NPAC data file into the specified regional LSMS database. (Example output is not shown.)

30. If you specified the `-c` option or you answered Y when prompted for any failure, such as syntax error, that occurred during the import process in *Step 29* on page 382, perform the one of the following sets of substeps:

CAUTION: This step requires a working knowledge of the vi editor and detailed understanding of the contents of the files downloaded from the NPAC. It is recommended that the Tekelec Customer Care Center be contacted prior to performing this step.

- If you answered Y when prompted for any failure during the import process in *Step 29* on page 382, perform these substeps:

  1. Examine and correct the files that were not successfully imported by entering the following command:

     ```
     $ vi /var/TKLC/lsms/free/data/npacftp/<region>/<downloaded file>
     ```

     For example:

     ```
     $ vi
     /var/TKLC/lsms/free/data/npacftp/Midwest/SPID.07-10-2000023849
     ```

  2. Delete the `^D` characters added at the end of the file by the vi editor by pressing the Shift and G keys at the same time to go to the end of the file, and then typing `dd` to remove the last line.
  3. For each file corrected by *Step 30* on page 385 a and b, enter the following command to import the corrected file into the regional database:

     ```
     $ $LSMS_DIR/import <region> <bulk load file>
     ```

  4. Go to step 30.

- If you specified the `-c` option in *Step 29* on page 382, perform these substeps:

  1. Examine and correct the files that were not successfully imported by entering the following command:

     ```
     $ vi /var/TKLC/lsms/free/data/npacftp/<region>/<downloaded file>
     ```

     For example:

     ```
     $ vi
     /var/TKLC/lsms/free/data/npacftp/Midwest/SPID.07-10-2000023849_FAILED
     ```

  2. Correct the file as desired, and then import the file into the database by entering the following command, where `<region>` is the name of the NPAC region, `<instance>` is the type of instance to be imported into the database, and `<filename>` is the name of the file to be imported:

     ```
     $ $LSMS_TOOLS_DIR/npacimport -r <region> -i <instance> -y
     <filename>
     ```

31. If you are reversing an NPA split, go to step *Step 34* on page 387.

    Otherwise, perform the following substeps:

Table 198: NPAC Bulk Load Files and LSMS Database Object Classes

NPAC Bulk Load File	LSMS Database Object Class
000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849	SubscriptionVersion
0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849	NumberPoolBlock
LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849	ServiceProvLRN
NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849	ServiceProvNPA_NXX
NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849	ServiceProvNPA_NXX_X
SPID.07-11-2004023849	ServiceProvNetwork

These substeps compare the number of instances of each object type (shown in **bold** in the following examples) contained in the NPAC files and in the LSMS database.

a) Enter the following command to display the number of lines in each bulk load file:

```
$ wc -l *
```

Output similar to the following appears:

- If you are downloading files from the NPAC after a site failure or during migration, output similar to the following appears. This output includes lines (shown in **bold**) used for Efficient Data Representation (EDR). If an NPAC does not support EDR, or if you do not have the EDR feature installed, lines similar to those shown in **bold** will not appear.

```
    1892
  000000-999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
     892
0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
    250
  LRN.07-11-2004023849.07-10-2004023849.07-11-2004023849           23
  NPANXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
      12  NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
     5
  SPID.07-10-2004023849
```

- If you are converting a regional database to support EDR, output similar to the following output appears.

```
 892
  0000000-9999999.07-11-2004023849.07-10-2004023849.07-11-2004023849
12
  NPANXXX.07-11-2004023849.07-10-2004023849.07-11-2004023849
```

b) Enter the following command to display the total number of instances of each class in the regional database:

```
$ lsmsdb -c counts -d <dbname>
```

Output similar to the following appears:

```
$ lsmsdb -c counts -d MidwestDB 892
 .......... MidwestDB.NumberPoolBlock 250
 .......... MidwestDB.ServiceProvLRN 23
 ........... MidwestDB.ServiceProvNPA_NXX 12
 ........... MidwestDB.ServiceProvNPA_NXX_X 5
 ............ MidwestDB.ServiceProvNetwork 1,892
 ......... MidwestDB.SubscriptionVersion
#
```

c) Verify that the numbers of instances indicated in the output of *Step 31* on page 385 b (shown in **bold** in the example) match the numbers included in the output of *Step 31* on page 385 a (shown in **bold** in that example). If they do not match, repeat *Step 28* on page 381 through *Step 30* on page 385

32. If you are converting a regional database to support EDR, go to *Step 34* on page 387.

Otherwise, perform the following command to change the Last Change Time (LCT) of the regional database to match the timestamp embedded in the file name of the files obtained in *Step 16* on page 379.

```
$ chglct -r <region> -s <YYYYMMDDhhmmss>
```

Where `<region>` is the name of the NPAC for which you are performing the download and <YYYYMMDDhhmmss> is the timestamp embedded in the file name as shown in the files displayed in *Step 16* on page 379. For more information about the `chglct` command, see *chglct* on page 168.

33. Once you have verified that the region has received a "Recovery Complete" message from the NPAC, you may remove the "import" files from the system by repeating *Step 2* on page 376 through *Step 6* on page 377 of this procedure.

34. Restart the LSMS agent for the region by doing the following:

From the LSMS GUI menu, select **Configure ➤ LNP System ➤ NPAC ➤ Modify ➤ Primary** and click the Activate Region checkbox so that is checked. For more information about this GUI window, refer to the LSMS *Configuration Manual*. Having this checkbox checked enables the `sentryd` utility to automatically attempt to restart the regional agent.

35. If the SWIM feature was turned off in *Step 26* on page 381, contact the NPAC to have the SWIM list cleared for all imported regions, then contact Tekelec Customer Service to reactivate SWIM.

36. If imports were performed for all active regions, go to *Step 37* on page 387 Otherwise, contact Tekelec Customer Service to determine if time range resynchronizations are needed for regions that were not imported due to SWIM having been turned off temporarily.

If necessary, Tekelec Customer Service will help the customer reassociate LSMS with the NPAC and perform manual time range resynchronizations.

37. Restart the LSMS GUI for the region by entering the following command:

```
$ $LSMS_DIR/start_mgui
```

For example:

```
$ $LSMS_DIR/start_mgui
```

38. Repeat steps *Step 21* on page 380 through *Step 37* on page 387 for each NPAC region for which you have downloaded files.

39. For each network element supported by the LSMS, resynchronize the data that corresponds to the data downloaded from the NPAC, using one of the procedures described in LSMS *with* EAGLE *5* ISS LNP Database *Synchronization Manual*. For example:

    - If you downloaded from the NPAC after a site failure or during migration, perform a time range audit or a bulk download to each supported network element (refer to "Auditing and Reconciling Network Elements from the LSMS" or "Managing Bulk Load from the LSMS").
    - If you have reversed an NPA split, perform an audit and reconcile procedure for subscription versions and NPBs in both the old NPA-NXX and the erroneous new NPA-NXX to each supported network element (refer to "Auditing and Reconciling Network Elements from the LSMS").
    - If you have converted a regional database to support EDR, perform an audit and reconcile procedure for all NPBs to each supported network element (refer to "Auditing and Reconciling Network Elements from the LSMS").

You have now completed this procedure.

Copying Files to Other Server If Switchover Occurs

When switchover (whether automatically or manually initiated) occurs, the standby server, which has been replicating the database on the active server, takes over to be the newly active server. However, any files that have been downloaded from the NPAC exist only on the server to which they were downloaded. If switchover occurs during a BDD procedure, the quickest way to get the files on the newly active server is to perform one of the procedures described in this section.

The following notifications indicate that a switchover has been initiated and completed:

```
LSMS4000|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Switchover initiated
LSMS4001|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Switchover complete
```

Perform one of the following procedures:

- If switchover occurred after all files have been downloaded from the NPAC, perform the procedure described in *Copying All Downloaded Files After Switchover* on page 388
- If switchover occurred while files are being downloaded from the NPAC, perform the procedure described in *Copying Partially Downloaded Files After Switchover* on page 389

Copying All Downloaded Files After Switchover

If switchover is initiated and completed after all the files you need have been downloaded from the NPAC but before you have imported them into the LSMS database, perform the following procedure.

1. If switchover is initiated between the time all the files have been downloaded from the NPAC and the time they are to be imported into the LSMS, wait until the following notification has been reported:

   ```
   LSMS4001|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Switchover complete
   ```

2. Log into the non-active server as `lsmsadm`.
3. Navigate to the directory where files have been downloaded:
   ```
   $ cd /var/TKLC/lsms/free/data/npacftp/<region>
   ```
   Where `<region>` is the name of the NPAC region for which files are being downloaded.
4. Verify that the correct directory was accessed by entering the following command:
   ```
   $ pwd
   ```
   The correct output is:
   ```
   /var/TKLC/lsms/free/data/npacftp/<region>
   ```
5. Use the secure file transfer protocol (`sftp`) to move the files from the previously active server into the `/var/TKLC/lsms/free/data/npacftp/<region>` directory on the newly active server:
   ```
   $ sftp lsmsadm@mate
   ```
   When prompted, enter the `lsmsadm` password. Then the `sftp>` prompt will appear; enter the following commands at the prompt:
   ```
   sftp> cd /var/TKLC/lsms/free/data/npacftp/<region>
   sftp> mput *
   sftp> bye
   ```
6. Proceed with the step you were performing when you were directed to this procedure.

You have now completed this procedure.

Copying Partially Downloaded Files After Switchover

If switchover is initiated and completed while files are being downloaded from the NPAC, some of the files may exist on the previously active server and some may exist on the newly active server. The safest procedure is to repeat the BDD procedure.

However, if you have already downloaded a number of files, you can choose to determine which files exist on which server and use the following procedure to copy the files that exist on the non-active server to the active server.

1. If switchover is initiated while files are being downloaded from the NPAC, wait until the following notification has been reported:
   ```
   LSMS4001|14:58 Oct 22, 2005|xxxxxxx|Notify:Sys Admin - Switchover complete
   ```
2. Log into the non-active server as `lsmsadm`.
3. Navigate to the directory where files have been downloaded:
   ```
   $ cd /var/TKLC/lsms/free/data/npacftp/<region>
   ```
   Where `<region>` is the name of the NPAC region for which files are being downloaded.
4. Verify that the correct directory was accessed by entering the following command:
   ```
   $ pwd
   ```

The correct output is:

```
/var/TKLC/lsms/free/data/npacftp/<region>
```

5. Enter the following command to list which files are stored in this directory:
   `$ ls -l`
6. Log into the active server as `lsmsadm`.
7. Navigate to the directory where files have been downloaded:
   `$ cd /var/TKLC/lsms/free/data/npacftp/<region>`
   Where `<region>` is the name of the NPAC region for which files are being downloaded.
8. Verify that the correct directory was accessed by entering the following command:
   `$ pwd`
   The correct output is:

```
/var/TKLC/lsms/free/data/npacftp/<region>
```

9. Enter the following command to list which files are stored in this directory:
   `$ ls -l`
10. Compare the files listed in *Step 5* on page 390 and *Step 9* on page 390 to determine whether all the files you need have been downloaded to one server or the other.
    If any files you need are missing from both servers, perform the procedure described in *NPAC-LSMS Download Procedure* on page 376 to obtain the missing files from the NPAC.
11. If you desire to copy any files from the non-active server to the active server, perform the remaining steps of this procedure.
12. At the previously active server, use the secure file transfer protocol (`sftp`) to move the files from the standby server into the/var/TKLC/lsms/free/data/npacftp/<region> directory on the newly active server:
    `$ sftp lsmsadm@mate`
    When prompted, enter the `lsmsadm` password. Then the sftp> prompt will appear; enter the following commands at the prompt:
    `sftp> cd /var/TKLC/lsms/free/data/npacftp/<region>`
    `sftp> mput *`
    `sftp> bye`
13. Proceed with the step you were performing when you were directed to this procedure.

You have now completed this procedure.

Appendix D

Worksheets

Topics:

- *Introduction Page 392*
- *Recovery Preparation Worksheet Page 392*

This appendix contains worksheets that you can copy and fill out with your own information.

Introduction

This appendix contains worksheets that you can copy and fill out with your own information.

Complete the worksheet shown in *Table 199: Recovery Preparation Worksheet* on page 392 to record information that you may need during disaster recovery procedures, as described in *Recovering from Site Failures* on page 131.

Recovery Preparation Worksheet

In preparation for possible error situations, including disasters, record the following information, as shown in *Table 199: Recovery Preparation Worksheet* on page 392, and store it in a safe and accessible location, off-site from both the main and shadow LSMS. Rows are provided for up to eight NPACs and up to eight EMSs; your LSMS may serve fewer NPACs or EMSs.

Table 199: Recovery Preparation Worksheet

Information Required	Customer Value
Obtain the following license information from the Tekelec Customer Care Center	
OSI license key for main LSMS upper server	
OSI license key for main LSMS lower server	
OSI license key for shadow LSMS upper server	
OSI license key for shadow LSMS lower server	
Main LSMS Data	
Service Provider Identification (SPID)	
LSMS Version	
`root` password	
`lsmsadm` name	
`lsmsadm` password	
`lsmsuser` name	

Information Required	Customer Value
`lsmsuser` password	
`lsmsuext` name	
`lsmsuext` password	
`lsmsview` name	
`lsmsview` password	
`lsmsall` name	
`lsmsall` password	
Shadow LSMS Data	
Service Provider Identification (SPID)	
primary IP address (decimal)	
primary IP address (hexadecimal)	
secondary IP address (decimal)	
secondary IP address (hexadecimal)	
NPAC Region 1 Name and Information	
FTP IP address (decimal)	
FTP IP address (hexadecimal)	
FTP directory	
FTP file names	
NPAC user ID	
NPAC password	
LSMS key set	

Information Required	Customer Value
NPAC Region 2 Name and Information	
FTP IP address (decimal)	
FTP IP address (hexadecimal)	
FTP directory	
FTP file names	
NPAC user ID	
NPAC password	
LSMS key set	
NPAC Region 3 Name and Information	
FTP IP address (decimal)	
FTP IP address (hexadecimal)	
FTP directory	
FTP file names	
NPAC user ID	
NPAC password	
LSMS key set	
NPAC Region 4 Name and Information	
FTP IP address (decimal)	
FTP IP address (hexadecimal)	
FTP directory	
FTP file names	

Information Required	Customer Value
NPAC user ID	
NPAC password	
LSMS key set	
NPAC Region 5 Name and Information	
FTP IP address (decimal)	
FTP IP address (hexadecimal)	
FTP directory	
FTP file names	
NPAC user ID	
NPAC password	
LSMS key set	
NPAC Region 6 Name and Information	
FTP IP address (decimal)	
FTP IP address (hexadecimal)	
FTP directory	
FTP file names	
NPAC user ID	
NPAC password	
LSMS key set	
NPAC Region 7 Name and Information	
FTP IP address (decimal)	

Information Required	Customer Value
FTP IP address (hexadecimal)	
FTP directory	
FTP file names	
NPAC user ID	
NPAC password	
LSMS key set	
NPAC Region 8 Name and Information	
FTP IP address (decimal)	
FTP IP address (hexadecimal)	
FTP directory	
FTP file names	
NPAC user ID	
NPAC password	
LSMS key set	

Appendix E

Query Server Maintenance Procedures

Topics:

- *Introduction Page 398*
- *LSMS Maintenance Procedures Page 398*
- *Automated System Check Page 409*
- *Query Server Error Log Page 410*
- *Retrieving Information from LNP Database Fields Page 411*
- *LNP Database Tables and Fields Page 413*
- *Query Server Database Structure Page 417*

This appendix contains detailed, step-by-step query server procedures, as well as information about the automated system check feature, the query server error log, and how to retrieve information from the LNP database fields.

Introduction

This appendix contains detailed, step-by-step query server procedures to enable you to do the following:

- *Check Connection Status of Directly Connected Query Servers* on page 400
- *Maintain the Binary Log on Query Servers* on page 400
- *Check MySQL Replication Status on Query Servers* on page 401
- *Start MySQL Replication on Query Servers* on page 401
- *Stop MySQL Replication on Query Servers* on page 402
- *Check for Running Backups* on page 402
- *Reload a Query Server Database from the LSMS* on page 402
- *Reload a Query Server Database from Another Query Server* on page 406
- *Clean Up After Failed or Interrupted Snapshot* on page 408

It also contains information about the automated system check feature, the query server error log, and how to retrieve information from the LNP database fields.

LSMS Maintenance Procedures

Figure 87: Query Server Configuration Scenario on page 398 illustrates a query server configuration scenario depicting how the LSMS might be directly connected to a query server, or indirectly connected to daisy-chained query servers. Refer to this figure when performing the maintenance procedures described in this section.

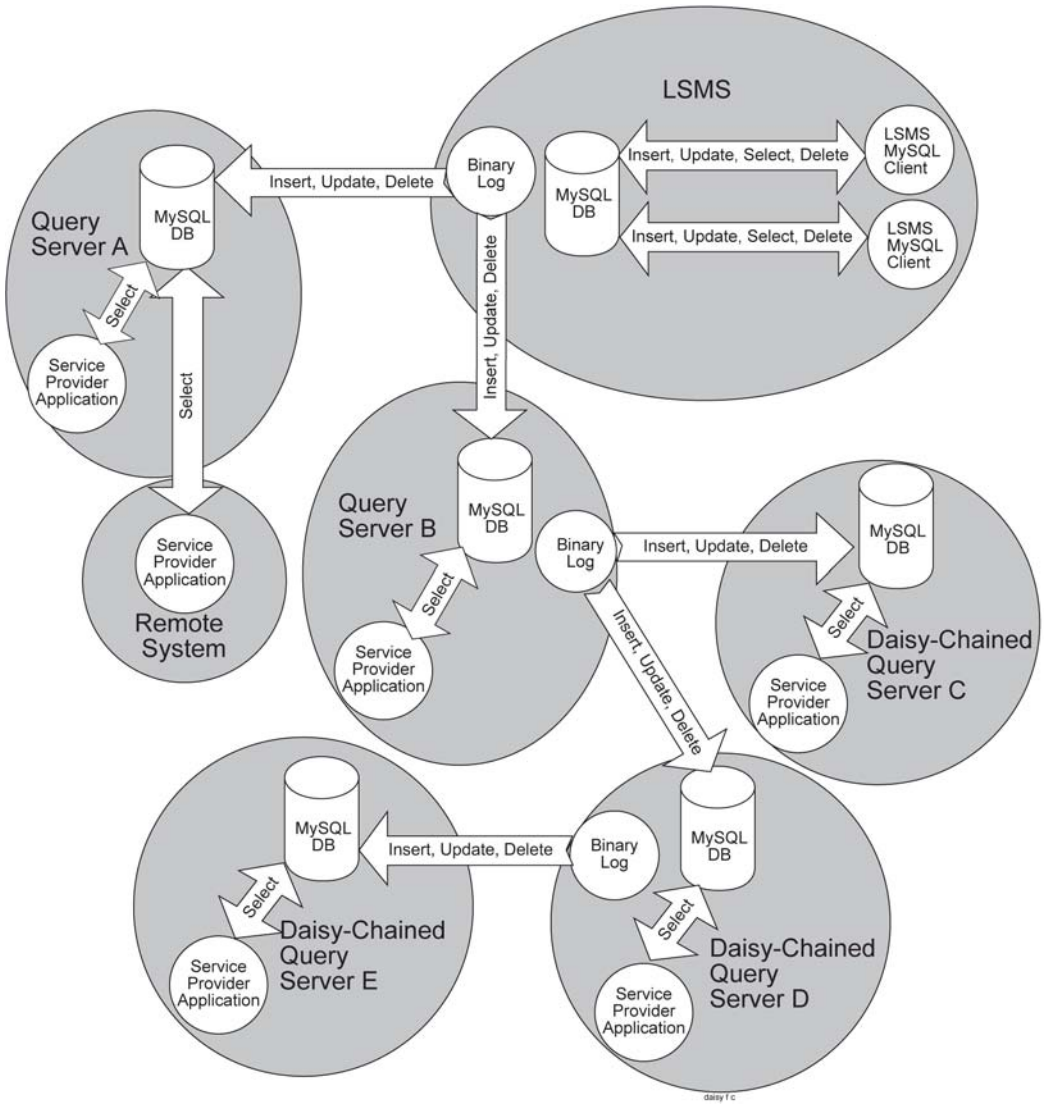
This scenario includes the following:

- One master (LSMS)
- One remote system
- Five query servers:
  - One directly connected slave (Query Server A)
  - One directly connected master/slave (Query Server B)
  - Two daisy-chained slaves (Daisy-chained Query Servers C and E)
  - One daisy-chained master/slave (Daisy-chained Query Server D)

Client applications on each query server represent a non-Tekelec provided Service Provider application that queries the replicated LSMS LNP databases using supported MySQL database APIs.

Note: Process all updates to the query server database through the master.

Figure 87: Query Server Configuration Scenario



Automatic Monitoring of Query Servers

The `lsmsQueryServer` script monitors the connectivity and status of each directly connected query server to ensure that it is replicating the LSMS LNP database. During failure and recovery of the connection with the query servers, the LSMS does one or more of the following:

- Displays a notification on the graphical user interface (GUI notification)
- Posts a Surveillance notification at five-minute intervals to Serial Port 1 used by Surveillance
- Sends a trap to a Network Management System (NMS) if the optional Remote Monitoring feature is installed

For information about the notifications posted, see *8098* on page 354 and *8099* on page 355.

Note: The LSMS does not monitor the connectivity or status of the daisy-chained query servers.

Check Connection Status of Directly Connected Query Servers

You can check the connection status of query servers that are directly connected to the LSMS. The connection status for each query server (denoted by hostname and IP address) is displayed as "Connected", "Disconnected" or "Not Reachable."

To check the connection status, use the following procedure:

1. Log into the active server as the `lsmsadm` user.
   (For information about logging in, see *Logging In to LSMS Server Command Line* on page 45.)
2. Enter the following command:
   ```
   $ lsmsdb -c queryservers
   ```
   Output similar to the following displays:
   ```
   10.25.60.32 (10.25.60.32) Disconnected
   ```
   In this example, only one query server has been configured to directly connect to the LSMS and it is currently disconnected.

You have now completed this procedure.

Maintain the Binary Log on Query Servers

Use this procedure to purge the binary log of a query server platform that will have one or more daisy-chained query servers. (Perform this procedure on Query Servers B and D, as shown in *Figure 87: Query Server Configuration Scenario* on page 398.)

Note: Monitor the binary log size and delete unnecessary binary log files on a weekly basis, following the steps listed below.

1. Use the following commands to identify what log each daisy-chained query server is replicating from and record your findings:
   ```
   # cd /opt/TKLCplat/mysql/bin
   # mysql -u root -p
   ```
   Enter password:
   ```
   <daisy-chained Query Server's MySql root user password
   >mysql> SHOWSLAVESTATUS \G;
   mysql> exit;
   ```
2. From Step 1, find the earliest log among all the daisy-chained query servers (if all the daisy-chained query servers are up-to-date, this is the last log on the list).
   On the query server that has query servers daisy-chained from it, list the binary log files. The target log is the one just before the earliest one in use.
   ```
   # cd /opt/TKLCplat/mysql/bin
   # mysql -u root -p
   Enter password:
   <Query Server's MySql root user password>
   ```

```
mysql> SHOWMASTERLOGS;
```

3. Use the following command to purge the master binary log files on the query server (that has one or more query servers daisy-chained from it) excluding the target log:

```
mysql> PURGE MASTER LOGS TO '<binary_log_file>';
```

You have now completed this procedure.

Check MySQL Replication Status on Query Servers

Use the following procedure to check MySQL replication status on query servers:

1. Start the MySQL command-line utility on the slave server:

```
# cd /opt/TKLCplat/mysql/bin
# mysql -u root -p
Enter password:
<Query Server's MySql root user password>
```

2. Check the replication status using the SHOW SLAVE STATUS command (the status of the slave server is conveyed by the Slave_IO_Running and Slave_SQL_Running column values):

```
mysql> SHOW SLAVE STATUS \G;
```

You have now completed this procedure.

Start MySQL Replication on Query Servers

Use the following procedure to start MySQL replication on the query server:

1. Start the MySQL command-line utility on the query server:

```
# cd /opt/TKLCplat/mysql/bin
# mysql -u root -p
Enter password:
<Query Server's MySql root user password>
```

2. Start MySQL replication:

   When the replication operation resumes, the slave server should connect to the master and catch up on any updates that occurred since the replication operation was terminated.

```
mysql> SLAVE START;
```

3. Verify that MySQL replication is running using the SHOW SLAVE STATUS command (ensure the Slave_IO_Running and Slave_SQL_Running column values are set to **Yes**, and ensure that the log file has a name).

```
mysql> SHOW SLAVE STATUS \G;
```

4. Exit the MySQL command-line utility:

```
mysql> exit;
```

You have now completed this procedure.

Stop MySQL Replication on Query Servers

Use the following procedure to stop MySQL replication on the query server:

1. Start the MySQL command-line utility on the query server:

```
# cd /opt/TKLCplat/mysql/bin
# mysql -u root -p
Enter password:
<Query Server's MySql root user password>
```

2. Stop MySQL replication: (When replication is off, the slave server data is not updated and is not kept in synchronization with the master server.)

```
mysql> SLAVE STOP;
```

3. Verify that MySQL replication is no longer running using the SHOW SLAVE STATUS command (ensure the Slave_IO_Running and Slave_SQL_Running column values are set to **No**).

```
mysql> SHOW SLAVE STATUS \G;
```

4. Exit the MySQL command-line utility:

```
mysql> exit;
```

You have now completed this procedure.

Check for Running Backups

Both database backups and query server snapshots use the same file space on the LSMS. Before creating a snapshot on the LSMS, perform the procedure described in *Checking for Running Backups* on page 93 to ensure that no database backups are running.

CAUTION: If you attempt to create a snapshot while a backup is running, the backup will be interrupted, and the next time a backup is performed, it will take much longer to complete.

The following tasks also use temporary file space (as does a snapshot), so you may run out of file space if you attempt to create a snapshot after you have started but not yet finished any of these tasks:

- Starting the standby server (changing its state from UNINITIALIZED "INHIBITED" to STANDBY) using the procedure described in *Starting a Server* on page 129
- Running the `import` command
- Running the `quickaudit` command

Reload a Query Server Database from the LSMS

This procedure reloads a corrupted or backlevel query server's database by copying the LSMS LNP database. If the LSMS is configured with multiple query servers, reload a query server from another query server (that is currently synchronized with the LSMS) to prevent NPAC-to-network element traffic from being interrupted (see *Reload a Query Server Database from Another Query Server* on page 406).

Note: The following method of reloading a query server may briefly interrupt provisioning on the LSMS while a snapshot of the LNP database occurs. Therefore, choose this method only when other methods for synchronizing the query server are not feasible. The time required to accomplish this procedure depends on the bandwidth of the customer's network and the amount of data to be reloaded. To minimize service interruption, perform this procedure during a scheduled maintenance period.

1. Log into the active server as `root`.

   If you are already logged into the active server as a different user, enter the following command:

   ```
   $ su - root
   ```

   When prompted, enter the root password.

2. Enter both of the following commands to remove all existing snapshots as well as the snapshot information file:

   ```
   # rm /var/TKLC/lsms/free/mysql-snapshot*
   ```

   ```
   # rm /var/TKLC/lsms/free/snapinfo.sql
   ```

3. Ensure that no database backups are in progress by performing the procedure described in *Check for Running Backups* on page 402.

4. Enter the following command to create a snapshot of all the LSMS data.

   CAUTION: Do not create a snapshot while a database backup is occurring. To ensure that a database backup is not occurring, perform the procedure described in *Check for Running Backups* on page 402.

   In addition, do not create a snapshot while any of the following processes are also running: backups, starting a standby node (to change its state from UNINITIALIZED "INHIBITED" to STANDBY), running the `import` command, or running the `lsmsdb quickaudit` command, all of which use temporary storage space. If you try to create a snapshot while any of these processes are running, you may not have enough disk space to complete the process.

   Note: GNU tar (gtar) must be installed on the Query Server prior to any single region exceeding 60 million TNs.

   ```
   # lsmsdb -c snapshot
   ```

   The following output displays:

   ```
   WARNING: This command may cause a brief interruption in traffic being sent
   from the NPAC to connected network elements and local LSMS provisioning may
   be INTERRUPTED.
   Do you want to continue? [Y/N] Y
   ```

5. Type **Y** and press Enter.

   Note: This input is case-sensitive. Be sure to type a capital Y.

   Output similar to the following displays (the line .....: in the example output below represents many lines of information that are displayed about each of the databases that is included in the snapshot).

   ```
   Creating snapshot of the database partition, please wait...
   lvcreate -- WARNING: the snapshot will be automatically disabled once it gets
    full
   lvcreate -- INFO: using default snapshot chunk size of 64 KB for
   ```

```
"/dev/vgapp/dbbackup"
lvcreate -- doing automatic backup of "vgapp"
lvcreate -- logical volume "/dev/vgapp/dbbackup" successfully created
The database is available to the application again.
Disk snapshot created successfully.
mount: block device /dev/vgapp/dbbackup is write-protected, mounting read-only
Snapshot mounted successfully.
Created snapinfo.sql file successfully
............
lvremove -- doing automatic backup of volume group "vgapp"
lvremove -- logical volume "/dev/vgapp/dbbackup" successfully removed
```

When the last two lines shown above (which start with lvremove), the snapshot is complete. However, the database is available to the application before the snapshot is complete, as indicated by the line shown in bold in the example output above. During the creation of a snapshot of the LSMS data, the following occurs:

- A read lock is obtained
- Table information is flushed
- A snapshot is created
- The read lock is released

CAUTION: If the snapshot fails or is interrupted, perform the procedure described in *Clean Up After Failed or Interrupted Snapshot* on page 408 to clean up the file space where snapshot information is temporarily stored. If you do not clean up this file space, future snapshots will fail.

If the compressed snapshot is successfully created, the LSMS data is stored in the following files in the `/var/TKLC/lsms/free` directory:

- `mysql-snapshot-supDB.tar.gz`
- `mysql-snapshot-<region>DB.tar.gz`
- `snapinfo.sql`

6. Use the file transfer protocol (FTP) to move the snapshot data of the master server into the`/usr/mysql1` directory on the query server:

```
# cd /var/TKLC/lsms/free
# ftp <IP address of the Query Server>
ftp> cd /usr/mysql1
ftp> bin
ftp> prompt
ftp> mput mysql-snapshot*.tar.gz snapinfo.sql
ftp> bye
```

7. Shut down the MySQL server on the query server (if it is running):

```
# cd /opt/TKLCplat/mysql/bin
# ./mysqladmin -u root -p shutdown
Enter password:
<Query Server's MySQL user root password>
```

8. On the query server, extract the snapshot data from the archive tar files, `/usr/mysql1 /mysql-snapshot-<db>.tar.gz` of the master server's data.

   Make sure that the privileges on the files and directories are correct. The user that MySQL runs as needs to be able to read and write to them, just as on the master.

   ```
   # cd /usr/mysql1
   # gunzip -c mysql-snapshot-supDB.tar.gz | tar -xvf -
   # rm mysql-snapshot-supDB.tar.gz
   ```

   Now, extract the data for the snapshot files for each of the LSMS regions starting with the largest regions first. Replace <regionDB> with the regional database name (for example, CanadaDB, MidwestDB, and so forth). Be sure to remove the compressed snapshot files after each database is extracted to guarantee that sufficient disk space is available for all databases.

   ```
   # gunzip -c mysql-snapshot-<regionDB>.tar.gz | tar -xvf -
   # rm mysql-snapshot-<regionDB>.tar.gz
   ```

9. Start the MySQL daemon on the query server:

   ```
   # cd /opt/TKLCplat/mysql/bin
   # ./mysqld_safe --skip-slave-start &
   ```

   Note: It is important to start the daemon with the --skip-slave-start option so that replication does not start automatically.

10. On the query server, start the MySQL command line utility:

    ```
    # ./mysql -u root -p
    ```

11. On the query server, reset the configuration information:

    ```
    mysql> reset slave;
    mysql> reset master;
    ```

12. Configure the query server to start replication from the correct position on the master.

    This information is stored in the `snapinfo.sql` file.

    ```
    mysql> source /usr/mysql1/snapinfo.sql
    ```

13. Start replication:

    ```
    mysql> start slave;
    ```

    The query server should connect to the master and catch up on any updates that occurred since the snapshot was taken. When a query server has started replicating, a `master.info` file is stored in the same directory as the error log (for information about where the error log is stored, see *Query Server Error Log* on page 410).

CAUTION: Do not remove or edit the `master.info` file. This file is used by the query server to keep track of how much of the master's binary log it has processed.

You have now completed this procedure.

Reload a Query Server Database from Another Query Server

This procedure reloads a corrupted or backlevel query server's LNP database by copying another query server's LNP database. If the LSMS is configured with multiple query servers and at least one is currently synchronized, it is recommended to reload a query server from another query server (instead of from the LSMS) to prevent NPAC-to-network element traffic from being interrupted.

Note: Replication on the query server may be interrupted while a snapshot of the LNP database occurs. The time required to accomplish this procedure depends on the bandwidth of your network and the amount of data to be reloaded.

Note: *Step 1* on page 406 through *Step 10* on page 407 pertain to the query server that is directly connected to the LSMS. *Step 11* on page 407 through *Step 14* on page 408 pertain to the query server being reloaded.

1. Start the MySQL command-line utility on the query server that is directly connected to the LSMS:

   ```
   # cd /opt/TKLCplat/mysql/bin
   ```

   ```
   # ./mysql -u root -p
   ```

   ```
   Enter password:
   ```

   ```
   <Query Server's MySQL user root password>
   ```

2. Stop MySQL replication: (When replication is off, the query server data is not updated and is not kept in synchronization with the LSMS.)

   ```
   mysql> stop slave;
   ```

3. Obtain a read lock and flush table cache information:

   (The flush writes changes to tables on disk. The read lock prohibits changes to be made to tables but continues to allow other threads to read from them.)

   ```
   mysql> FLUSH TABLES WITH READ LOCK;
   ```

4. Display the file name and current position of the binary log:

   ```
   mysql> SHOW MASTER STATUS;
   ```

   Output similar to the following displays:

   ```
   +---------------+----------+--------------+------------------+
   | File | Position | Binlog_Do_DB | Binlog_Ignore_DB |
   +---------------+----------+--------------+------------------+
   | mysql-bin.003 | 73       | test         | manual,mysql     |
   +---------------+----------+--------------+------------------+
   ```

5. Record the values in the `File` and `Position` columns, which display the file name and current position of the binary log, respectively.

   In the example above, the file name is `mysql-bin.003`, and the current position is `73`. These values are necessary to properly start the slave process on the query server that is being reloaded.

6. Exit the MySQL command-line utility:

   ```
   mysql> exit;
   ```

7. Shutdown the MySQL server on the query server that is directly connected to the LSMS:

```
# ./mysqladmin -u root -p shutdown
Enter password:
<Query Server's MySql root user password>
```

8. Remove all existing compressed snapshot files (if any):

```
# rm /usr/mysql1/mysql-snapshot*
```

9. Create a snapshot of the query server's copy of all the LSMS data.

   Create a compressed snapshot file for the Supplemental database:

   Note: GNU tar (gtar) must be installed on the Query Server prior to any single region exceeding 60 million TNs.

```
# tar -cvf - /usr/mysql1/supDB/* | gzip >
/usr/mysql1/mysql-snapshot-supDB.tar.gz
```

   Create compressed snapshot files for each of the regional databases. Replace <regionDB> with the regional database name (for example, CanadaDB, MidwestDB, and so forth).

```
# tar -cvf - /usr/mysql1/<regionDB>/* | gzip >
/usr/mysql1/mysql-snapshot-<regionDB>.tar.gz
```

10. At the query server that is directly connected to the LSMS, restart the MySQL daemon:

```
# cd /opt/TKLCplat/mysql/bin
# ./mysqld_safe &
```

11. Shut down the MySQL server on the query server being reloaded:

```
# ./mysqladmin -u root -p shutdown
Enter password:
<Query Server's MySQL user root password>
```

12. From the master query server, use the file transfer protocol (FTP) to move the snapshot data of the master server into the`/usr/mysql1` directory on the query server being reloaded:

```
# cd /usr/mysql1
# ftp <IP address of the Query Server being reloaded>
ftp> cd /usr/mysql1
ftp> bin
ftp> prompt
ftp> mput mysql-snapshot*.tar.gz
ftp> bye
```

13. On the query server being reloaded, extract the snapshot data from the archive tar file of the directly connected query server's data.

    Ensure that the privileges on the files and directories are correct. The user which MySQL runs as needs to be able to read and write to them, just as on the master. Perform the following commands:

```
# cd /usr/mysql1
# gunzip -c mysql-snapshot-supDB.tar.gz | tar -xvf -
```

```
# rm mysql-snapshot-supDB.tar.gz
```

Now, extract the data for the snapshot files for each of the LSMS regions starting with the largest regions first. Replace <regionDB> with the regional database name (for example, CanadaDB, MidwestDB, and so forth). Be sure to remove the compressed snapshot files after each database is extracted to guarantee that sufficient disk space is available for all databases:#

```
# gunzip -c mysql-snapshot-<regionDB>.tar.gz | tar -xvf -
```

```
# rm mysql-snapshot-<regionDB>.tar.gz
```

14. Start the MySQL daemon on the query server being loaded.

```
# cd /opt/TKLCplat/mysql/bin
```

```
# ./mysqld_safe --skip-slave-start
```

Note: It is important to start the daemon with the --skip-slave-start option so that replication does not start automatically.

15. Start the `mysql` command-line utility on the query server that is being loaded:

```
# ./mysql -u root -p
```

16. Set the binary log position using information that you recorded in *Step 5* on page 406.

```
mysql> CHANGE MASTER TO
```

```
MASTER_LOG_FILE='<recorded_log_file_name>',
```

```
MASTER_LOG_POS=<recorded_log_position>;
```

For `<recorded_log_file_name>`, use the value you recorded for the file name in *Step 5* on page 406, and for , use the value you recorded for the binary position in *Step 5* on page 406. For example, using the values shown in the example in *Step 4* on page 406, enter the following command to set the binary log position:

```
mysql> CHANGE MASTER TO
```

```
MASTER_LOG_FILE='mysql-bin.003',
```

```
MASTER_LOG_POS=73;
```

17. Start replication on the query server that has been loaded:

```
mysql> start slave;
```

The query server should connect to the master server (LSMS or another query server) and catch up on any updates that occurred since the snapshot was taken.

You have now completed this procedure.

Clean Up After Failed or Interrupted Snapshot

If a snapshot fails or is interrupted, the `/dev/vgapp/dbbackup` volume will remain in the file space that is temporarily used by both backups and snapshot creation. If this volume is present when another snapshot is attempted, the new snapshot will fail.

If a snapshot fails, perform the following procedure to clean up the file space that is used for temporarily storing snapshot information. If this file space is not cleaned up, any future snapshot attempts will fail.

1. If a snapshot has failed, first ensure that no backup is already running by performing the procedure described in *Check for Running Backups* on page 402.
   - If a backup is running, DO NOT perform this procedure. Wait until the backup is complete and retry the snapshot.
   - If a backup is not running, proceed to the next step.
2. Log into the active server as `root`.
   If you are already logged into the active server as a different user, enter the following command:
   ```
   $ su - root
   ```
   When prompted, enter the root password.
3. Enter the following commands:
   ```
   # /bin/umount /mnt/backup
   ```
   ```
   # /sbin/lvremove -f /dev/vgapp/dbbackup
   ```
   The following output will display:
   ```
   lvremove -- doing automatic backup of volume group "vgapp"
   lvremove -- logical volume "/dev/vgapp/dbbackup" successfully removed
   ```

When the last line in *Step 3* on page 409 displays, you have completed this procedure.

Automated System Check

The automated system check feature (`syscheck`) detects, diagnoses, and displays a summary of the overall health of the LSMS server. An LSMS application-specific module, `qs_app` (System Class) reports on the status of query server direct connections with the LSMS. The status of each connection is displayed on the screen as "OK", "WARNING", or "FAILURE".

Manually Checking Query Server Status

Although `syscheck` runs automatically and records output in the syscheck log, users can run the syscheck command to check query server status. To manually check query server status, perform the following procedure:

1. Log into the active server command line as `root`.
   (For information about logging in, see *Logging In to LSMS Server Command Line* on page 45).
2. Enter the following command:
   ```
   # syscheck system qs
   ```
   The possible output examples are explained below.

You have now completed this procedure.

Automated System Check OK Status

When `syscheck` detects no problems with query server direct connections, output similar to the following appears.

Figure 88: Automated System Check Output Example - OK

```
Running modules in class system...
                    OK

The log is available at:
  -->/var/TKLC/log/syscheck/fail_log
```

Automated System Check FAILURE Status

When `syscheck` detects one or more of the following failures, output similar to the following appears.

- The LSMS DB tool, which is utilized to obtain connection status, does not exist.
- The LSMS DB tool fails to connect to the database server.
- The query server hostname is not associated with corresponding Internet Protocol (IP) addresses in the `/etc/hosts` file.
- The platform hosting a query server could not be pinged (Not Reachable). The hostname of the query servers that fail the `ping` check is reported.

Figure 89: Automated System Check Output Example - FAILURE

```
Running modules in class system...
*       qs: FAILURE:: Query Server 10.26.60.136 (10.26.60.136) Not Reachable
One or more module in class "system" FAILED

Failures occured during system check. The failure log is available at:
  -->/var/TKLC/log/syscheck/fail_log
```

Automated System Check WARNING Status

When `syscheck` detects that one or more query servers are not connected and replicating the LSMS database, output similar to the following appears. The hostname of the query servers that fail the connections check is reported.

Figure 90: Automated System Check Output Example - WARNING

```
Running modules in class system...
*       qs: WARNING:: Query Server 10.25.60.32 (10.25.60.32) Disconnected
                                  OK
The log is available at:
  -->/var/TKLC/log/syscheck/fail_log
```

Query Server Error Log

The query server error log (see the example shown in *Figure 91: Query Server Error Log Example* on page 411) contains the following information, if applicable:

- When `mysqld` was started and stopped
- Critical errors found when running `mysqld`
- Replication errors and warnings
- Warnings if `mysqld` detects a table that needs to be automatically checked or repaired

The query server error log is assigned a name based on the name of your host and appended with a `.err` extension (for example, `<hostname>.err`) and is located in one of the following directories:

- On the LSMS, in `/var/TKLC/lsms/db`
- On a query server, in `/usr/mysql1`. On a Windows machine, `mysqld` writes this log directly to `C:\mysql\data\mysql.err`.

  Note: Because the query server error log continuously increases in size, it is the user's responsibility to monitor it. To manually delete the log, first shut down the server. Alternatively, execute the `mysql-log-rotate`script inside your crontab.

Figure 91: Query Server Error Log Example

```
mysqld: ready for connections

020715 14:27:38  Slave thread initialized

020715 14:28:00  Slave thread: error connecting to master: Can't connect
to MySQL server on '192.168.34.98' (183) (0), retry in 60 sec

020715 14:29:21  Slave: connected to master
'lsmsrepl@192.168.34.98:3306',  replication started in log
'192.168.34.98-bin.003' at position 1763
```

Retrieving Information from LNP Database Fields

The LNP database is in table format. Following are the characteristics of the table rows and columns:

- Each column contains a value for each row.
- The table does not contain gaps or short columns.
- Each row is a single entity, and the columns describe the attributes of those entities.
- Each column has a name and a type, such as a string or a number. (See *Table 200: Regional Database Tables and Fields* on page 413 through*Table 202: Supplemental Database Tables and Fields (Part 2)* on page 415 for the LNP database table names and associated fields.)

  To obtain information (name, type, if field contains a Null, key fields, default value, and so forth) for each field of a table on the query server, perform the following steps:

  Note: Example output follows the command syntax in *Step 2* on page 411 through *Step 5* on page 412

1. Start the `mysql` command-line utility on the query server using the following command:

   ```
   # cd /opt/TKLCplat/mysql/bin
   ```

   ```
   # mysql -u root -p
   Enter password:
   ```

   ```
   <Query Server's MySQL user root password>
   ```

2. List the names of the databases on the query server using the following command:

   ```
   mysql> SHOWDATABASES;
   ```

   ```
   mysql> SHOW DATABASES;
   +-----------+
   | Database  |
   +-----------+
   ```

```
| ResyncDB  |
| WesternDB |
| mysql     |
| supDB     |
+-----------+
4 rows in set (0.09 sec)
```

3. Select the name of the database that contains tables from which you want to retrieve information using the following command:

   `mysql> USE <database>;`

   where `<database>` is one of the following: supDB, CanadaDB, MidAtlanticDB, MidwestDB, NortheastDB, SoutheastDB, SouthwestDB, WestCoastDB, WesternDB

```
mysql> USE WesternDB
Database changed
```

4. List the names of the tables in the selected database using the following command:

   `mysql> SHOW TABLES;`

```
mysql> SHOW TABLES;
+----------------------+
| Tables_in_WesternDB  |
+----------------------+
| NumberPoolBlock      |
| ServiceProvLRN       |
| ServiceProvNPA_NXX   |
| ServiceProvNPA_NXX_X |
| ServiceProvNetwork   |
| SubscriptionVersion  |
+----------------------+
6 rows in set (0.01 sec)
```

5. Retrieve column and field information of a database table using the following command:

   `mysql> DESCRIBE <table>;`

   where `<table>` is the name of the database table from the list of tables displayed in *Step 4* on page 412

```
mysql> describe SubscriptionVersion;

Field                Type                Null Key Default      Extra
---------------------------------------------------------------------

versionId            int(11)             NO   PRI
tn                   char(10)            NO   UNI
lrn                  char(10)            NO   MUL
newCurrentSp         char(4)             NO   MUL 0000
activationTimestamp  char(14)           NO      00000000000000     classDPC
             char(9)             NO
classSSN             char(3)             NO
lidbDPC              char(9)             NO
lidbSSN              char(3)             NO
isvmDPC              char(9)             NO
isvmSSN              char(3)             NO
cnamDPC              char(9)             NO
cnamSSN              char(3)             NO
endUserLocationValue char(12)            NO
endUserLocationType  char(2)             NO
billingId            char(4)             NO
lnpType              tinyint(3) unsigned NO       0
```

```
downloadReason       tinyint(3) unsigned NO       0
wsmscDPC             char(9)             NO
wsmscSSN             char(3)             NO
svType               tinyint(4)          NO       -1
alternativeSPID      char(4)             NO

22 rows in set (0.00 sec)
```

You have now completed this procedure.

LNP Database Tables and Fields

The Query Server database consists of replicated copies of the LSMS LNP database tables listed in *Table 200: Regional Database Tables and Fields* on page 413, *Table 201: Supplemental Database Tables and Fields (Part 1)* on page 414, and *Table 202: Supplemental Database Tables and Fields (Part 2)* on page 415.

Note: In the table below, names of regional LNP database tables and fields may be split between lines. This does not imply a space in the name of the table or field.

Table 200: Regional Database Tables and Fields

Regional (<Region>) DB) LNP Database Tables	Fields			
SubscriptionVersion	versionID	tn	lrn	newCurrentSp
	classDPC	classSSN	lidbDPC	lidbSSN
	isvmDPC	isvmSSN	cnamDPC	cnamSSN
	wsmscDPC	wsmscSSN	LnpType	billingId
	endUserLocation Value	endUserLocation Type	activation Timestamp	downloadReason
	SVType	alternativeSPID		
NumberPoolBlock	blockId	npanxx_x	lrn	newCurrentSP
	classDPC	classSSN	lidbDPC	lidbSSN
	isvmDPC	isvmSSN	cnamDPC	cnamSSN
	wsmscDPC	wsmscSSN	activationTimestamp	downloadReason
	SVType	alternativeSPID		
ServiceProvLRN	serviceProviderId	id	lrn	creationTimeStamp
	downloadReason			
ServiceProv NPA_NXX	serviceProviderId	id	npanxx	creationTimeStamp

Regional (<Region>) DB) LNP Database Tables	Fields			
	effectiveTimeStamp	downloadReason		
ServiceProv NPA_NXX_X	serviceProviderId	id	npanxx_x	creationTimeStamp
	effectiveTimeStamp	modifiedTime Stamp	downloadReason	
ServiceProvNetwork	serviceProvId	serviceProvName	serviceProvType	
Where <Region> is one of the following:	Canada	MidAtlantic	Midwest	Northeast
	Southeast	Southwest	WestCoast	Western

Table 201: Supplemental Database Tables and Fields (Part 1)

Supplemental (supDB) LNP Database Tables	Fields			
DefaultGtt	groupName	npanxx	spid	
	ain_set	ain_tt	ain_dpc	ain_ssn
	ain_xlat	ain_ri	ain_ngt	ain_rgta
	in_set	in_tt	in_dpc	in_ssn
	in_xlat	in_ri	in_ngt	in_rgta
	class_set	class_tt	class_dpc	class_ssn
	class_xlat	class_ri	class_ngt	class_rgta
	lidb_set	lidb_tt	lidb_dpc	lidb_ssn
	lidb_xlat	lidb_ri	lidb_ngt	lidb_rgta
	isvm_set	isvm_tt	isvm_dpc	isvm_ssn
	isvm_xlat	isvm_ri	isvm_ngt	isvm_rgta
	cnam_set	cnam_tt	cnam_dpc	cnam_ssn
	cnam_xlat	cnam_ri	cnam_ngt	cnam_rgta
	wsmsc_set	wsmsc_tt	wsmsc_dpc	wsmsc_ssn
	wsmsc_xlat	wsmsc_ri	wsmsc_ngt	wsmsc_rgta
OverrideGtt	groupName	lrn	spid	
	class_set	class_tt	class_dpc	class_ssn
	class_xlat	class_ri	class_ngt	class_rgta

Supplemental (supDB) LNP Database Tables	Fields			
	lidb_set	lidb_tt	lidb_dpc	lidb_ssn
	lidb_xlat	lidb_ri	lidb_ngt	lidb_rgta
	isvm_set	isvm_tt	isvm_dpc	isvm_ssn
	isvm_xlat	isvm_ri	isvm_ngt	isvm_rgta
	cnam_set	cnam_tt	cnam_dpc	cnam_ssn
	cnam_xlat	cnam_ri	cnam_ngt	cnam_rgta
	wsmsc_set	wsmsc_tt	wsmsc_dpc	wsmsc_ssn
	wsmsc_xlat	wsmsc_ri	wsmsc_ngt	wsmsc_rgta
NpaSplit	oldNpa	newNpa	nxx	startPDP
	endPDP	region	status	
LsmsServiceProvider	spid	description	contactInfo	

Table 202: Supplemental Database Tables and Fields (Part 2)

Supplemental (supDB) LNP Database Tables	Fields			
GttGroup	name	description		
	ain_set	ain_tt	ain_dpc	ain_ssn
	ain_xlat	ain_ri	ain_ngt	ain_rgta
	in_set	in_tt	in_dpc	in_ssn
	in_xlat	in_ri	in_ngt	in_rgta
	class_set	class_tt	class_dpc	class_ssn
	class_xlat	class_ri	class_ngt	class_rgta
	lidb_set	lidb_tt	lidb_dpc	lidb_ssn
	lidb_xlat	lidb_ri	lidb_ngt	lidb_rgta
	isvm_set	isvm_tt	isvm_dpc	isvm_ssn
	isvm_xlat	isvm_ri	isvm_ngt	isvm_rgta
	cnam_set	cnam_tt	cnam_dpc	cnam_ssn
	cnam_xlat	cnam_ri	cnam_ngt	cnam_rgta
	wsmsc_set	wsmsc_tt	wsmsc_dpc	wsmsc_ssn
	wsmsc_xlat	wsmsc_ri	wsmsc_ngt	wsmsc_rgta

Supplemental (supDB) LNP Database Tables	Fields			
EmsInterface	clli	emsType	primaryAddress	secondaryAddress
	mateClii	pointCode	matePointCode	capabilityPoint Code
	gttGroup	tnFilter	ownerSpid	componentInfo
	contactInfo	dcmAddress	retryinterval	retryCount
	pingMethod			
TnFilter	spid	name	description	filterType
	regions	npanxxType	npanxxs	
NpacRegion	region	npacSmsName	lsmsPsel	lsmsSsel
	lsmsTsel	lsmsNsap	primaryNpacPsel	primaryNpacSsel
	primaryNpacTsel	primaryNpacNsap	primaryNpac FtpAddress	secondaryNpac Psel
	secondaryNpacSsel	secondaryNpacTsel	secondaryNpac Nsap	secondaryNpac FtpAddress
	active	componentInfo	contactInfo	lastChanged Timestamp
	currentNpac			
<Region>Npac Measurements	yyyydddhh	Binds	SuccessOps	FailedOps
<Clii>Eagle Measurements	yyyydddhh			
	updTnSuccess	updTnFail	DelTnSuccess	DelTnFail
	updDGttSuccess	updDGttFail	DelDGttSuccess	DelDGttFail
	updOGttSuccess	updOGttFail	DelOGttSuccess	DelOGttFail
	updSplitSuccess	updSplitFail	DelSplitSuccess	DelSplitFail
	Binds	LsmsRetries	NERetries	
<Region>PublicKey	id	listId	keyId	status
	exponent	modulus		
<Region>PrivateKey	id	listId	keyId	status
	keyval			
LsmsUser	name	golden	groupName	inactivityTimeout
LsmsUserSpid	lsmsUser	spid		

Supplemental (supDB) LNP Database Tables	Fields			
Where <Region> is one of the following:	Canada	MidAtlantic	Midwest	Northeast
	Southeast	Southwest	WestCoast	Western
Where <Clii> is the Common Language Location Indicator of the EMS/EAGLE to which that LSMS is connected.				

Note: In *Table 202: Supplemental Database Tables and Fields (Part 2)* on page 415, by default, the following Supplemental (SupDB) LNP Database Tables are not replicated. To replicate these tables, see the Note in Step 1 of the topic, "MySQL Replication Configuration for Query Servers" in Appendix A of the *LSMS Configuration Manual*.

- <Region>PublicKey
- <Region>PrivateKey
- LsmsUser
- LsmsUserSpid

  To replicate these tables, see the Note in Step 1 of the topic, "MySQL Replication Configuration for Query Servers" in Appendix A of the LSMS *Configuration Manual*.

Query Server Database Structure

This section contains the database structure needed to develop customer-provided applications on the query servers.

```
--

-- Create NpacRegion table

--

-- One NpacRegion defines the configuration of the primary and secondary
NPAC.

--

CREATE TABLE  NpacRegion

(

    -- Region name

    region              VARCHAR(40)  NOT NULL,


    -- SMS Name defined by NPAC

    npacSmsName         TINYBLOB,
```

```
-- OSI address of LSMS
lsmsPsel              TINYBLOB,
lsmsSsel              TINYBLOB,
lsmsTsel              TINYBLOB,
lsmsNsap              TINYBLOB,

-- OSI address of primary NPAC
primaryNpacPsel       TINYBLOB,
primaryNpacSsel       TINYBLOB,
primaryNpacTsel       TINYBLOB,
primaryNpacNsap       TINYBLOB,

primaryNpacFtpAddress TINYBLOB,

-- OSI address of secondary NPAC
secondaryNpacPsel     TINYBLOB,
secondaryNpacSsel     TINYBLOB,
secondaryNpacTsel     TINYBLOB,
secondaryNpacNsap     TINYBLOB,

secondaryNpacFtpAddress TINYBLOB,

-- Region is active
active               BOOL        NOT NULL DEFAULT 0,

-- Component Info (stored as CSV string)
componentInfo        BLOB        NOT NULL,
-- Contact Info (stored as CSV string)
contactInfo        BLOB          NOT NULL,

-- Last changed timestamp set by npacagent
lastChangedTimestamp CHAR(14)    NOT NULL, -- Default now
```

```
    -- Current npac in use set by npacagent
    currentNpac          ENUM("Primary", "Secondary") DEFAULT "Primary",


    -- Region name is primary key
    PRIMARY KEY (region)
)
TYPE = MyIsam;


INSERT INTO NpacRegion
    (region, npacSmsName,
     lsmsPsel, lsmsSsel, lsmsTsel, lsmsNsap,
     primaryNpacPsel, primaryNpacSsel, primaryNpacTsel, primaryNpacNsap,
primaryNpacFtpAddress,
     secondaryNpacPsel, secondaryNpacSsel, secondaryNpacTsel,
secondaryNpacNsap, secondaryNpacFtpAddress,
     componentInfo, contactInfo, lastChangedTimestamp)
    VALUES ("Canada", "Region8 NPAC Canada",
            "cw7", "cw7", "", "rk6",
            "", "", "", "0x00000000",
            "0.0.0.0",
            "", "", "", "0x00000000",
            "0.0.0.0",
            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',
            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1
234","9195551234"',
            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),
           ("MidAtlantic", "Mid-Atlantic Regional NPAC SMS",
            "cw1", "cw1", "", "rk6",
            "", "", "", "0x00000000",
            "0.0.0.0",
            "", "", "", "0x00000000",
            "0.0.0.0",
            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',
```

```
            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1
234","9195551234"',

            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),

           ("Midwest", "Midwest Regional NPAC SMS",

            "cw0", "cw0", "", "rk6",

            "", "", "", "0x00000000",

            "0.0.0.0",

            "", "", "", "0x00000000",

            "0.0.0.0",

            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',

            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1
234","9195551234"',

            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),

           ("Northeast", "Northeast Regional NPAC SMS",

            "cw2", "cw2", "", "rk6",

            "", "", "", "0x00000000",

            "0.0.0.0",

            "", "", "", "0x00000000",

            "0.0.0.0",

            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',

            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1
234","9195551234"',

            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),

           ("Southeast", "Southeast Regional NPAC SMS",

            "cw3", "cw3", "", "rk6",

            "", "", "", "0x00000000",

            "0.0.0.0",

            "", "", "", "0x00000000",

            "0.0.0.0",

            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',

            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1
234","9195551234"',
```

```
            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),

           ("Southwest", "Southwest Regional NPAC SMS",

            "cw4", "cw4", "", "rk6",

            "", "", "", "0x00000000",

            "0.0.0.0",

            "", "", "", "0x00000000",

            "0.0.0.0",

            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',

            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1
234","9195551234"',

            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),

           ("WestCoast", "WestCoast Regional NPAC SMS",

            "cw6", "cw6", "", "rk6",

            "", "", "", "0x00000000",

            "0.0.0.0",

            "", "", "", "0x00000000",

            "0.0.0.0",

            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',

            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1
234","9195551234"',

            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s")),

           ("Western", "Western Regional NPAC SMS",

            "cw5", "cw5", "", "rk6",

            "", "", "", "0x00000000",

            "0.0.0.0",

            "", "", "", "0x00000000",

            "0.0.0.0",

            '"NPAC","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"',

            '"Lsms Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1
234","9195551234"',

            DATE_FORMAT(NOW(), "%Y%m%d%h%i%s"));



--
```

```
-- Create  LsmsServiceProvider table
--
CREATE TABLE  LsmsServiceProvider
(
    -- The service provider id (Primary Key)
    spid        CHAR(4)   NOT NULL,

    -- Description of the service provider
    description CHAR(80)  NOT NULL,

    -- Contact Info (stored as comma separated value string)
    contactInfo BLOB NOT NULL,

    -- Primary key is the spid
    PRIMARY KEY (spid)
)
TYPE = MyIsam;

--
-- Create  LsmsUser table
--
CREATE TABLE  LsmsUser
(
    -- The user name (Primary Key)
    name    CHAR(64) NOT NULL,

    -- Description of the service provider
    golden  BOOL     NOT NULL DEFAULT 0,

    -- The Assigned permission group
    groupName    CHAR(4) NOT NULL,
```

```
    -- The assigned inactivity timeout
    inactivityTimeout    CHAR(11) NOT NULL DEFAULT '-1',

    -- Primary key is the user name
    PRIMARY KEY (name)
)
TYPE = MyIsam;
-- Create default 'golden' users
INSERT INTO LsmsUser (name, golden)
            VALUES('lsmsadm',1), ('lsmsuser',1), ('lsmsview',1),
                  ('lsmsall',1), ('lsmsuext',1);
--
-- Create  GttGroup table
--
CREATE TABLE  GttGroup
(
    -- The group name (Primary Key)
    name        CHAR(64)   NOT NULL,

    -- Description of the GttGroup
    description CHAR(80)  NOT NULL,

    -- Services in GttGroup are for storing default TT/SSN values
    -- AIN Service
    ain_set  BOOL    NOT NULL DEFAULT 0,
    ain_tt   TINYINT UNSIGNED NOT NULL,
    ain_dpc  CHAR(9) NOT NULL,
    ain_ssn  CHAR(3) NOT NULL,
    ain_xlat TINYINT UNSIGNED NOT NULL,
    ain_ri   TINYINT UNSIGNED NOT NULL,
    ain_ngt  TINYINT UNSIGNED NOT NULL,
    ain_rgta BOOL    NOT NULL,
    -- IN Service
```

```
in_set  BOOL    NOT NULL DEFAULT 0,
in_tt   TINYINT UNSIGNED NOT NULL,
in_dpc  CHAR(9) NOT NULL,
in_ssn  CHAR(3) NOT NULL,
in_xlat TINYINT UNSIGNED NOT NULL,
in_ri   TINYINT UNSIGNED NOT NULL,
in_ngt  TINYINT UNSIGNED NOT NULL,
in_rgta BOOL    NOT NULL,
-- CLASS Service
class_set  BOOL    NOT NULL DEFAULT 0,
class_tt   TINYINT UNSIGNED NOT NULL,
class_dpc  CHAR(9) NOT NULL,
class_ssn  CHAR(3) NOT NULL,
class_xlat TINYINT UNSIGNED NOT NULL,
class_ri   TINYINT UNSIGNED NOT NULL,
class_ngt  TINYINT UNSIGNED NOT NULL,
class_rgta BOOL    NOT NULL,
-- LIDB Service
lidb_set  BOOL    NOT NULL DEFAULT 0,
lidb_tt   TINYINT UNSIGNED NOT NULL,
lidb_dpc  CHAR(9) NOT NULL,
lidb_ssn  CHAR(3) NOT NULL,
lidb_xlat TINYINT UNSIGNED NOT NULL,
lidb_ri   TINYINT UNSIGNED NOT NULL,
lidb_ngt  TINYINT UNSIGNED NOT NULL,
lidb_rgta BOOL    NOT NULL,
-- ISVM Service
isvm_set  BOOL    NOT NULL DEFAULT 0,
isvm_tt   TINYINT UNSIGNED NOT NULL,
isvm_dpc  CHAR(9) NOT NULL,
isvm_ssn  CHAR(3) NOT NULL,
isvm_xlat TINYINT UNSIGNED NOT NULL,
```

```
    isvm_ri   TINYINT UNSIGNED NOT NULL,
    isvm_ngt  TINYINT UNSIGNED NOT NULL,
    isvm_rgta BOOL    NOT NULL,
    -- CNAM Service
    cnam_set  BOOL    NOT NULL DEFAULT 0,
    cnam_tt   TINYINT UNSIGNED NOT NULL,
    cnam_dpc  CHAR(9) NOT NULL,
    cnam_ssn  CHAR(3) NOT NULL,
    cnam_xlat TINYINT UNSIGNED NOT NULL,
    cnam_ri   TINYINT UNSIGNED NOT NULL,
    cnam_ngt  TINYINT UNSIGNED NOT NULL,
    cnam_rgta BOOL    NOT NULL,
     -- WSMSC Service
    wsmsc_set  BOOL    NOT NULL DEFAULT 0,
    wsmsc_tt   TINYINT UNSIGNED NOT NULL,
    wsmsc_dpc  CHAR(9) NOT NULL,
    wsmsc_ssn  CHAR(3) NOT NULL,
    wsmsc_xlat TINYINT UNSIGNED NOT NULL,
    wsmsc_ri   TINYINT UNSIGNED NOT NULL,
    wsmsc_ngt  TINYINT UNSIGNED NOT NULL,
    wsmsc_rgta BOOL    NOT NULL,

    -- Primary key is the group name
    PRIMARY KEY (name)
)
TYPE = MyIsam;


--
-- Create GttGroupSpid table
--
-- This table is used to associate a GttGroup to an authorized
-- LsmsServiceProvider. The many-many relationship between the two
-- is stored by this table a group-spid combinations.
```

```
--
CREATE TABLE  GttGroupSpid
(
    -- Group name
    gttGroup    CHAR(64) NOT NULL,

    -- Spid
    spid        char(4) NOT NULL,

    -- Force GttGroup,LsmsServiceProvider combinations to be unique
    PRIMARY KEY (gttGroup, spid),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (gttGroup) REFERENCES GttGroup(groupName),
    FOREIGN KEY (spid) REFERENCES LsmsServiceProvider(spid)
)
TYPE = MyIsam;

--
-- Create LsmsUserSpid table
--
-- This table is used to associate a LsmsUser to an authorized
-- LsmsServiceProvider. The many-many relationship between the two
-- is stored by this table a group-spid combinations.
--
CREATE TABLE  LsmsUserSpid
(
    -- User name
    lsmsUser    CHAR(64) NOT NULL,

    -- Spid
    spid        CHAR(4) NOT NULL,
```

```
    -- Force LsmsUser,LsmsServiceProvider combinations to be unique
    PRIMARY KEY (lsmsUser, spid),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (lsmsUser) REFERENCES LsmsUser(name),
    FOREIGN KEY (spid) REFERENCES LsmsServiceProvider(spid)
)
TYPE = MyIsam;

--
-- Create DefaultGTT Table
--
CREATE TABLE  DefaultGtt
(
    -- The group this DefaultGtt belongs to
    groupName  CHAR(64) NOT NULL, -- Foreign key

    -- NPA-NXX of the DefaultGtt
    npanxx     CHAR(6) NOT NULL,

    -- The SPID that created the DefaultGtt
    spid       CHAR(4) NOT NULL,

    -- AIN Service
    ain_set  BOOL    NOT NULL DEFAULT 0,
    ain_tt   TINYINT UNSIGNED NOT NULL,
    ain_dpc  CHAR(9) NOT NULL,
    ain_ssn  CHAR(3) NOT NULL,
    ain_xlat TINYINT UNSIGNED NOT NULL,
    ain_ri   TINYINT UNSIGNED NOT NULL,
    ain_ngt  TINYINT UNSIGNED NOT NULL,
    ain_rgta BOOL    NOT NULL,
```

```
-- IN Service
in_set  BOOL    NOT NULL DEFAULT 0,
in_tt   TINYINT UNSIGNED NOT NULL,
in_dpc  CHAR(9) NOT NULL,
in_ssn  CHAR(3) NOT NULL,
in_xlat TINYINT UNSIGNED NOT NULL,
in_ri   TINYINT UNSIGNED NOT NULL,
in_ngt  TINYINT UNSIGNED NOT NULL,
in_rgta BOOL    NOT NULL,
-- CLASS Service
class_set  BOOL    NOT NULL DEFAULT 0,
class_tt   TINYINT UNSIGNED NOT NULL,
class_dpc  CHAR(9) NOT NULL,
class_ssn  CHAR(3) NOT NULL,
class_xlat TINYINT UNSIGNED NOT NULL,
class_ri   TINYINT UNSIGNED NOT NULL,
class_ngt  TINYINT UNSIGNED NOT NULL,
class_rgta BOOL    NOT NULL,
-- LIDB Service
lidb_set  BOOL    NOT NULL DEFAULT 0,
lidb_tt   TINYINT UNSIGNED NOT NULL,
lidb_dpc  CHAR(9) NOT NULL,
lidb_ssn  CHAR(3) NOT NULL,
lidb_xlat TINYINT UNSIGNED NOT NULL,
lidb_ri   TINYINT UNSIGNED NOT NULL,
lidb_ngt  TINYINT UNSIGNED NOT NULL,
lidb_rgta BOOL    NOT NULL,
-- ISVM Service
isvm_set  BOOL    NOT NULL DEFAULT 0,
isvm_tt   TINYINT UNSIGNED NOT NULL,
isvm_dpc  CHAR(9) NOT NULL,
isvm_ssn  CHAR(3) NOT NULL,
```

```
    isvm_xlat TINYINT UNSIGNED NOT NULL,
    isvm_ri   TINYINT UNSIGNED NOT NULL,
    isvm_ngt  TINYINT UNSIGNED NOT NULL,
    isvm_rgta BOOL    NOT NULL,
    -- CNAM Service
    cnam_set  BOOL    NOT NULL DEFAULT 0,
    cnam_tt   TINYINT UNSIGNED NOT NULL,
    cnam_dpc  CHAR(9) NOT NULL,
    cnam_ssn  CHAR(3) NOT NULL,
    cnam_xlat TINYINT UNSIGNED NOT NULL,
    cnam_ri   TINYINT UNSIGNED NOT NULL,
    cnam_ngt  TINYINT UNSIGNED NOT NULL,
    cnam_rgta BOOL    NOT NULL,
     -- WSMSC Service
    wsmsc_set  BOOL    NOT NULL DEFAULT 0,
    wsmsc_tt   TINYINT UNSIGNED NOT NULL,
    wsmsc_dpc  CHAR(9) NOT NULL,
    wsmsc_ssn  CHAR(3) NOT NULL,
    wsmsc_xlat TINYINT UNSIGNED NOT NULL,
    wsmsc_ri   TINYINT UNSIGNED NOT NULL,
    wsmsc_ngt  TINYINT UNSIGNED NOT NULL,
    wsmsc_rgta BOOL    NOT NULL,

    -- DefaultGtt npanxx's are unique within each group
    PRIMARY KEY (groupName, npanxx),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (groupName) REFERENCES GttGroup(name)
)
TYPE = MyIsam;

--
-- Create OverrideGtt Table
```

```
--
CREATE TABLE  OverrideGtt
(
    -- The group this OverrideGtt belongs to
    groupName  CHAR(64) NOT NULL, -- Foreign key

    -- LRN of the OverrideGtt
    lrn        CHAR(10) NOT NULL,

    -- The SPID that created the OverrideGtt
    spid       CHAR(4)  NOT NULL,

    -- CLASS Service
    class_set  BOOL    NOT NULL DEFAULT 0,
    class_tt   TINYINT UNSIGNED NOT NULL,
    class_dpc  CHAR(9) NOT NULL,
    class_ssn  CHAR(3) NOT NULL,
    class_xlat TINYINT UNSIGNED NOT NULL,
    class_ri   TINYINT UNSIGNED NOT NULL,
    class_ngt  TINYINT UNSIGNED NOT NULL,
    class_rgta BOOL    NOT NULL,
    -- LIDB Service
    lidb_set  BOOL    NOT NULL DEFAULT 0,
    lidb_tt   TINYINT UNSIGNED NOT NULL,
    lidb_dpc  CHAR(9) NOT NULL,
    lidb_ssn  CHAR(3) NOT NULL,
    lidb_xlat TINYINT UNSIGNED NOT NULL,
    lidb_ri   TINYINT UNSIGNED NOT NULL,
    lidb_ngt  TINYINT UNSIGNED NOT NULL,
    lidb_rgta BOOL    NOT NULL,
    -- ISVM Service
    isvm_set  BOOL    NOT NULL DEFAULT 0,
```

```
    isvm_tt   TINYINT UNSIGNED NOT NULL,
    isvm_dpc  CHAR(9) NOT NULL,
    isvm_ssn  CHAR(3) NOT NULL,
    isvm_xlat TINYINT UNSIGNED NOT NULL,
    isvm_ri   TINYINT UNSIGNED NOT NULL,
    isvm_ngt  TINYINT UNSIGNED NOT NULL,
    isvm_rgta BOOL    NOT NULL,
    -- CNAM Service
    cnam_set  BOOL    NOT NULL DEFAULT 0,
    cnam_tt   TINYINT UNSIGNED NOT NULL,
    cnam_dpc  CHAR(9) NOT NULL,
    cnam_ssn  CHAR(3) NOT NULL,
    cnam_xlat TINYINT UNSIGNED NOT NULL,
    cnam_ri   TINYINT UNSIGNED NOT NULL,
    cnam_ngt  TINYINT UNSIGNED NOT NULL,
    cnam_rgta BOOL    NOT NULL,
     -- WSMSC Service
    wsmsc_set  BOOL    NOT NULL DEFAULT 0,
    wsmsc_tt   TINYINT UNSIGNED NOT NULL,
    wsmsc_dpc  CHAR(9) NOT NULL,
    wsmsc_ssn  CHAR(3) NOT NULL,
    wsmsc_xlat TINYINT UNSIGNED NOT NULL,
    wsmsc_ri   TINYINT UNSIGNED NOT NULL,
    wsmsc_ngt  TINYINT UNSIGNED NOT NULL,
    wsmsc_rgta BOOL    NOT NULL,

    -- OverrideGtt lrns are unique within each group
    PRIMARY KEY (groupName, lrn),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (groupName) REFERENCES GttGroup(name)
)
TYPE = MyIsam;
```

```
--
-- Create EmsInterface table. A row in the EmsInterface table can
represent
-- either a MpsInterface or a OapInterface object
--
CREATE TABLE  EmsInterface
(
    -- The CLLI (Primary Key)
    clli                CHAR(10)   NOT NULL,

    emsType             ENUM("OAP", "MPS") NOT NULL,

    -- The IP address of the primary interface
    primaryAddress      TINYBLOB   NOT NULL,

    -- The IP address of the secondary interface
    secondaryAddress    TINYBLOB   NOT NULL,

    -- The method to use to verify the presence of the MPS
    pingMethod          ENUM("PING", "SSH", "NONE") NOT NULL,

    -- The mate CLLI
    mateClli            CHAR(10)   NOT NULL,

    -- Point code
    pointCode           CHAR(9)    NOT NULL,

    -- Point code of the mate
    matePointCode       CHAR(9)    NOT NULL,

    -- Capability point code
    capabilityPointCode CHAR(9)    NOT NULL,
```

```
    -- GttGroup assigned to the EmsInteraface
    gttGroup            CHAR(64)   NOT NULL DEFAULT ""
        REFERENCES GttGroup(name),

    -- TnFilter assigned to the EmsInteraface
    tnFilter            CHAR(64)   NOT NULL DEFAULT ""
        REFERENCES TnFilter, -- via FOREIGN KEY (ownerSpid, tnfilter)

    -- ServiceProvider to which this EmsInterface is assigned
    ownerSpid           CHAR(4)    NOT NULL DEFAULT ""
        REFERENCES LsmsServiceProvider(spid),

    -- Component Info (stored as CSV string)
    componentInfo        BLOB        NOT NULL,
    -- Contact Info (stored as CSV string)
    contactInfo        BLOB          NOT NULL,

    -- The last fields are only used when the row represents a
    -- OAP interface. The row is used to construct both OapInterface
    -- objects and MpsInterface objects which are subclasses of
EmsInterface

    -- OAP dcmAddress
    dcmAddress        TINYBLOB NULL DEFAULT NULL,

    -- OAP retry interval
    retryInterval     INTEGER  NULL DEFAULT NULL,

    -- OAP retry count
    retryCount        INTEGER  NULL DEFAULT NULL,

    -- Primary key is the CLLI name
```

```
    PRIMARY KEY (clli),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (ownerSpid, tnFilter) REFERENCES TnFilter
)
TYPE = MyIsam;

--
-- Create TnFilter table. A row in the EmsInterface table can represent
-- either a RegionTnFilter or a NpaNxxTnFilter object
--
CREATE TABLE  TnFilter
(
    -- The LsmsServiceProvider this TnFilter belongs to
    spid           char(4)    NOT NULL,   -- Foreign key

    -- The name of the TnFilter
    name           CHAR(64)   NOT NULL,

    -- Description of the TnFilter
    description CHAR(80)  NOT NULL,

    -- The filter type (NpaNxxTnFilter or RegionalTnFilter)
    filterType     ENUM("Regional", "NpaNxx") NOT NULL,

    -- If RegionalTnFilter, the region to send
    regions        SET("Not Used", "Canada", "MidAtlantic", "Midwest",
"Northeast",
                       "Southeast", "Southwest", "WestCoast", "Western")
NOT NULL,

    -- If NpaNxxTnFilter, the filter type
    npanxxType     ENUM("Include", "Exclude") NOT NULL,
```

```
    -- If NpaNxxTnFilter, the npa-nxxs to send
    npanxxs        LONGBLOB NOT NULL,

    -- TnFilter names are unique within LsmsServiceProvider
    PRIMARY KEY (spid, name),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (spid) REFERENCES LsmsServiceProvider(spid)

)
TYPE = MyIsam;

--
--  Create private and public key tables
--
--  The first four fields define a base class Key in the object interface
--
--         +-- PrivateKey
--  Key <--|
--         +-- PublicKey
--
-- Each subclass and table has the key values for the key type.
--


--
-- Create "Model" PrivateKey table
--
CREATE TEMPORARY TABLE IF NOT EXISTS TempPrivateKey
(
    listId      INT UNSIGNED,
    keyId       INT UNSIGNED,
    status      ENUM("Expired", "Valid", "InUse"),
```

```
    keyval      BLOB -- Max length 1024
)
TYPE = MyIsam;

-- Create CanadaPrivateKey table
CREATE TABLE  CanadaPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPrivateKey;

-- Create NortheastPrivateKey table
CREATE TABLE  NortheastPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPrivateKey;

-- Create MidAtlanticPrivateKey table
CREATE TABLE  MidAtlanticPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPrivateKey;

-- Create MidwestPrivateKey table
CREATE TABLE  MidwestPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPrivateKey;
```

```
-- Create SoutheastPrivateKey table
CREATE TABLE  SoutheastPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPrivateKey;

-- Create SouthwestPrivateKey table
CREATE TABLE  SouthwestPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPrivateKey;

-- Create WestCoastPrivateKey table
CREATE TABLE  WestCoastPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPrivateKey;

-- Create WesternPrivateKey table
CREATE TABLE  WesternPrivateKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPrivateKey;

--
-- Create "Model" PublicKey table
--
CREATE TEMPORARY TABLE IF NOT EXISTS TempPublicKey
(
```

```
    listId      INT UNSIGNED,
    keyId       INT UNSIGNED,
    status      ENUM("Expired", "Valid", "InUse"),
    exponent    TINYBLOB, -- Max length 3
    modulus     TINYBLOB  -- Max length 256
)
TYPE = MyIsam;

-- Create CanadaPublicKey table
CREATE TABLE  CanadaPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPublicKey;

-- Create NortheastPublicKey table
CREATE TABLE  NortheastPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPublicKey;

-- Create MidAtlanticPublicKey table
CREATE TABLE  MidAtlanticPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPublicKey;

-- Create MidwestPublicKey table
CREATE TABLE  MidwestPublicKey
(
```

```
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPublicKey;

-- Create SoutheastPublicKey table
CREATE TABLE  SoutheastPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPublicKey;

-- Create SouthwestPublicKey table
CREATE TABLE  SouthwestPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPublicKey;

-- Create WestCoastPublicKey table
CREATE TABLE  WestCoastPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPublicKey;

-- Create WesternPublicKey table
CREATE TABLE  WesternPublicKey
(
    id INT UNSIGNED NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (id)
) SELECT * FROM TempPublicKey;

--
```

```
-- Create one measurements table for each region
--
-- Create "Model" NpacMeasurements table
CREATE TEMPORARY TABLE IF NOT EXISTS TempNpacMeasurements
(
    yyyydddhh   INT UNSIGNED NOT NULL,
    Binds       INT UNSIGNED NOT NULL DEFAULT 0,
    SuccessOps  INT UNSIGNED NOT NULL DEFAULT 0,
    FailedOps   INT UNSIGNED NOT NULL DEFAULT 0,

    PRIMARY KEY (yyyydddhh)
)
TYPE = MyIsam;

-- Create CanadaNpacMeasurements table
CREATE TABLE  CanadaNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM TempNpacMeasurements;

-- Create NortheastNpacMeasurements table
CREATE TABLE  NortheastNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM TempNpacMeasurements;

-- Create MidAtlanticNpacMeasurements table
CREATE TABLE  MidAtlanticNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM TempNpacMeasurements;
```

```
-- Create MidwestNpacMeasurements table
CREATE TABLE  MidwestNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM TempNpacMeasurements;

-- Create SoutheastNpacMeasurements table
CREATE TABLE  SoutheastNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM TempNpacMeasurements;

-- Create SouthwestNpacMeasurements table
CREATE TABLE  SouthwestNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM TempNpacMeasurements;

-- Create WestCoastNpacMeasurements table
CREATE TABLE  WestCoastNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM TempNpacMeasurements;

-- Create WesternNpacMeasurements table
CREATE TABLE  WesternNpacMeasurements
(
    PRIMARY KEY (yyyydddhh)
) SELECT * FROM TempNpacMeasurements;


--
-- Create DbConfig table
--
```

```
CREATE TABLE  DbConfig

(

    keyType     ENUM("Canada", "MidAtlantic", "Midwest", "Northeast",

                     "Southeast", "Southwest", "WestCoast", "Western",

                     "R9", "R10", "R11", "R12", "R13", "R14",

                     "R15", "R16", "R17", "R18", "R19", "R20", -- Future
Regions

                     "Internal", "Ebda", "Lsms") NOT NULL,

    keyName     TINYBLOB NOT NULL,            -- Max length 256

    description TINYBLOB NOT NULL DEFAULT "", -- Max length 256

    value           BLOB NOT NULL DEFAULT "", -- Max length 64K


    -- keyName is unique within keyType

    PRIMARY KEY (keyType, keyName(255))

)

TYPE = MyIsam;


INSERT INTO DbConfig (keyType, keyName, description, value)

    VALUES

    ("Canada",      "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),

    ("Canada",      "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),

    ("Canada",      "RECOV_RETRY_NUMBER",     "Retry times for NPAC
recovery requests",   "3"),

    ("Canada",      "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),

    ("MidAtlantic", "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),

    ("MidAtlantic", "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),

    ("MidAtlantic", "RECOV_RETRY_NUMBER",     "Retry times for NPAC
recovery requests",   "3"),

    ("MidAtlantic", "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),

    ("Midwest",     "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),
```

```
    ("Midwest",     "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),

    ("Midwest",     "RECOV_RETRY_NUMBER",     "Retry times for NPAC
recovery requests",   "3"),

    ("Midwest",     "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),

    ("Northeast",   "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),

    ("Northeast",   "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),

    ("Northeast",   "RECOV_RETRY_NUMBER",     "Retry times for NPAC
recovery requests",   "3"),

    ("Northeast",   "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),

    ("Southeast",   "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),

    ("Southeast",   "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),

    ("Southeast",   "RECOV_RETRY_NUMBER",     "Retry times for NPAC
recovery requests",   "3"),

    ("Southeast",   "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),

    ("Southwest",   "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),

    ("Southwest",   "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),

    ("Southwest",   "RECOV_RETRY_NUMBER",     "Retry times for NPAC
recovery requests",   "3"),

    ("Southwest",   "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),

    ("WestCoast",   "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),

    ("WestCoast",   "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),

    ("WestCoast",   "RECOV_RETRY_NUMBER",     "Retry times for NPAC
recovery requests",   "3"),

    ("WestCoast",   "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),

    ("Western",     "REQUEST_RETRY_NUMBER",   "Retry times for NPAC
requests",   "3"),

    ("Western",     "REQUEST_RETRY_INTERVAL", "Retry minutes for NPAC
requests", "2"),

    ("Western",     "RECOV_RETRY_NUMBER",     "Retry times for NPAC
recovery requests",   "3"),
```

```
    ("Western",     "RECOV_RETRY_INTERVAL",   "Retry mintues for NPAC
recovery requests", "5"),



    ("Internal", "MAX_SPIDS",     "Maximum Service Providers allowed.",

"32"),

    ("Internal", "EDR",           "Enable Efficient Data Reperesentation
(EDR).",   "N" ),

    ("Internal", "SNMP",          "Enable SNMP Agent.",

"N" ),

    ("Internal", "AFT",           "Enable Automatic File Transfer.",

"N" ),

    ("Internal", "WSMSC",         "Enable wireless service feature.",

"N" ),

    ("Internal", "WSMSC_TO_EAGLE","Enable sending of WSMSA service to
Eagle.",      "N" ),

    ("Internal", "IP_GUI",        "Enable Web based ip gui.",

"N" ),

    ("Internal", "SPID_SECURITY", "Enable SPID based security.",

"N" ),

    ("Internal", "MAX_USERS",     "Maximum Number of Users",

"8" ),

    ("Internal", "ENHANCED_FILTERS","Enable Group and Regional filter
creation.",   "N" ),

    ("Internal", "MAX_EAGLES",    "Maximum number of eagles.",

"16"),

    ("Internal", "REPORT_GEN",    "Enable report generator.",

"N" ),

    ("Internal", "REPORT_GEN_QUERY_ACTIVE","Report generator pid field",

"0" ),

    ("Internal", "QUERY_SERVER",  "Enable Query Server feature",

"N" ),

    ("Internal", "INACTIVITY_TIMEOUT", "Gui and Shell inactivity timeout
feature",  "N" ),

    ("Internal", "SYSTEM_INACTIVITY_TIMEOUT", "System wide GUI and Shell
inactivity timeout value", "15" ),
```

```
    ("Ebda", "CMD_ARGS", "EBDA command line arguments", ""),


    ("Lsms", "NPAC_SPID", "Spid used to connect to NPAC", ""),

    ("Lsms", "CONTACT_INFO", "Spid used to connect to NPAC", '"Lsms
Admin","admin@tekelec.com","5200 Paramount
Parkway","Morrisville","NC","","USA","27560","9194605500","8005551234","1
234","9195551234"'),

    ("Lsms", "COMPONENT_INFO", "Spid used to connect to NPAC",
'"LSMS","TKLC","LSMS","Tekelec, Inc.","6.0","1.0"');



--

-- Create NpaSplit table

--

CREATE TABLE  NpaSplit

(

    -- The old npa

    oldNpa         char(3)    NOT NULL,


    -- The new npa

    newNpa         CHAR(3)    NOT NULL,


    -- The nxx

    nxx            CHAR(3)    NOT NULL,


    -- The start of the permissive dialing period

    startPDP       CHAR(8)    NOT NULL,


    -- The end of the permissive dialing period

    endPDP         CHAR(8)    NOT NULL,


    -- The region the split belongs to

    region      ENUM("Canada", "MidAtlantic", "Midwest", "Northeast",

                     "Southeast", "Southwest", "WestCoast", "Western",

                     "R9", "R10", "R11", "R12", "R13", "R14",
```

```
                    "R15", "R16", "R17", "R18", "R19", "R20"), -- Future
Regions


    -- The status of the npa split

    status      ENUM("NotSet", "Pending", "Active", "Error"),


    -- Old npa, new npa and nxx form primary unique key

    PRIMARY KEY (oldnpa, newnpa, nxx)

)

TYPE = MyIsam;
```

```
--
-- Create SubscriptionVersion table
--
-- The Fields are defined in the order and format that are defined by the
-- NPAC bulk data file. This allows the SQL LOAD DATA command to be used
-- to load tables which is extremely fast.
--
-- Revision History
-- 15-may-07  ARICENT  Feature 110663: NANC 399
--
CREATE TABLE  SubscriptionVersion
(
    -- Required field (Primary key)
    versionId            INT              NOT NULL,

    -- Required field (10 numeric character unique key)
    tn                   CHAR(10)         NOT NULL,

    -- Optional field (10 numeric characters, Empty string means not present)
    lrn                  CHAR(10)         NOT NULL DEFAULT "",

    -- Required field (1-4 characters)
    newCurrentSp         CHAR(4)          NOT NULL DEFAULT "0000",

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    activationTimestamp  CHAR(14)         NOT NULL DEFAULT "00000000000000",

    -- Optional field (9 characters, Empty string means not present)
    classDPC             CHAR(9)          NOT NULL DEFAULT "",

    -- Optional field (1-3 characters, Empty string means not present)
    classSSN             CHAR(3)          NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    lidbDPC              CHAR(9)          NOT NULL DEFAULT "",

    -- Optional field (1-3 characters, Empty string means not present)
    lidbSSN              CHAR(3)          NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    isvmDPC              CHAR(9)          NOT NULL DEFAULT "",

    -- Optional field (1-3 characters, Empty string means not present)
```

```
    isvmSSN              CHAR(3)          NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    cnamDPC              CHAR(9)          NOT NULL DEFAULT "",

    -- Optional field (1-3 characters, Empty string means not present)
    cnamSSN              CHAR(3)          NOT NULL DEFAULT "",

    -- Optional field (1-12 numeric characters, Empty string means not present)

    endUserLocationValue CHAR(12)         NOT NULL DEFAULT "",

    -- Optional field (2 numeric characters, Empty string means not present)
    endUserLocationType  CHAR(2)          NOT NULL DEFAULT "",

    -- Required field (1-4 characters, Empty string means not present)
    billingId            CHAR(4)          NOT NULL DEFAULT "",

    -- Required field (lspp(0), lisp(1), pool(2))
    lnpType              TINYINT UNSIGNED NOT NULL DEFAULT 0,

    -- Required field (new(0), delete(1), modified(2), audit-descrepancy(3)
    downloadReason       TINYINT UNSIGNED NOT NULL DEFAULT 0,

    -- Optional field (9 characters, Empty string means not present)
    wsmscDPC             CHAR(9)          NOT NULL DEFAULT "",

    -- Optional field (1-3 characters, Empty string means not present)
    wsmscSSN             CHAR(3)          NOT NULL DEFAULT "",

    -- Optional field  (wireline(0), wireless(1), voIP(2), voWiFi(3),
sv_type_4(4), sv_type_5(5), sv_type_6(6) )
    svType TINYINT NOT NULL DEFAULT -1,

    -- Optional field (1-4 CHARACTERS)
    alternativeSPIDCHAR(4)         NOT NULL DEFAULT "",

    -- Primay key is the Npac SubscriptionVersion id
    PRIMARY KEY (versionId),

    -- TN must be indexed and unique
    UNIQUE KEY tn (tn),

    -- Index lrn, for LSMS Subscription Version by LRN reports
    INDEX (lrn),

    -- Index lrn, for LSMS Subscription Version by SPID reports
    INDEX (newCurrentSp)

)
TYPE = MyIsam;

--
-- Create NumberPoolBlock table
--
-- The Fields are defined in the order and format that are defined by the
-- NPAC bulk data file. This allows the SQL LOAD DATA command to be used
-- to load tables which is extremely fast.
--
CREATE TABLE  NumberPoolBlock
(
    -- Required field (Primary key)
    blockId              INT              NOT NULL,

    -- Required field (7 numeric characters, Unique key)
```

```
    npanxx_x             CHAR(7)          NOT NULL,

    -- Optional field (10 numeric characters, Empty string means not present)
    lrn                  CHAR(10)         NOT NULL DEFAULT "",

    -- Required field (1-4 characters)
    newCurrentSp         CHAR(4)          NOT NULL DEFAULT "0000",

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    activationTimestamp  CHAR(14)         NOT NULL DEFAULT "00000000000000",

    -- Optional field (9 characters, Empty string means not present)
    classDPC             CHAR(9)          NOT NULL DEFAULT "",
    -- Optional field (1-3 characters, Empty string means not present)
    classSSN             CHAR(3)          NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    lidbDPC              CHAR(9)          NOT NULL DEFAULT "",
    -- Optional field (1-3 characters, Empty string means not present)
    lidbSSN              CHAR(3)          NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    isvmDPC              CHAR(9)          NOT NULL DEFAULT "",
    -- Optional field (1-3 characters, Empty string means not present)
    isvmSSN              CHAR(3)          NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    cnamDPC              CHAR(9)          NOT NULL DEFAULT "",
    -- Optional field (1-3 characters, Empty string means not present)
    cnamSSN              CHAR(3)          NOT NULL DEFAULT "",

    -- Optional field (9 characters, Empty string means not present)
    wsmscDPC             CHAR(9)          NOT NULL DEFAULT "",
    -- Optional field (1-3 characters, Empty string means not present)
    wsmscSSN             CHAR(3)          NOT NULL DEFAULT "",

    -- Required field (new(0), delete(1), modified(2), audit-descrepancy(3)
    -- Changed DEFAULT from "" to 0 when migrated MySQL from 4.1.11 to 5.0.37
    downloadReason       TINYINT UNSIGNED NOT NULL DEFAULT 0,

    -- Optional field  (wireline(0), wireless(1), voIP(2), voWiFi(3),
sv_type_4(4), sv_type_5(5), sv_type_6(6) )
    svType TINYINT NOT NULL DEFAULT -1,

    -- Optional field (1-4 CHARACTERS)
    alternativeSPID     CHAR(4)         NOT NULL DEFAULT "",

    -- Primay key is the Npac NumberPoolBlock id
    PRIMARY KEY (blockId),

    -- TN must be indexed and unique
    UNIQUE KEY npanxx_x (npanxx_x),

    -- Index lrn, for LSMS Number Pool Block by LRN reports
    INDEX (lrn),

    -- Index lrn, for LSMS Number Pool Block by SPID reports
    INDEX (newCurrentSp)
)
TYPE = MyIsam;

--
-- Create ServiceProvNetwork table
--
-- The Fields are defined in the order and format that are defined by the
```

```
-- NPAC bulk data file
--
CREATE TABLE ServiceProvNetwork
(
    -- Required field (Primary key)
    serviceProvId    CHAR(4)       NOT NULL,

    -- Required field (1 - 40 characters)
    serviceProvName  CHAR(40)      NOT NULL DEFAULT "",

     -- Service Provider type
    serviceProvType  ENUM("wireline", "wireless", "non_carrier", "sp_type_3",
"sp_type_4", "sp_type_5") NULL DEFAULT NULL,

    -- Prmary key is the Service Provider ID
    PRIMARY KEY (serviceProvId)
)
TYPE = MyIsam;

--
-- Create ServiceProvLRN table
--
-- The Fields are defined in the order that are defined by the
-- NPAC bulk data file
--
CREATE TABLE ServiceProvLRN
(
    -- Foreign key -> ServiceProvNetwork
    serviceProvId     CHAR(4)   NOT NULL,

    -- Required field (Primary key within each ServiceProvNetwork)
    id                INT       NOT NULL,

    -- Required field (10 numeric characters)
    lrn               CHAR(10)  NOT NULL,

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    creationTimeStamp CHAR(14)  NOT NULL DEFAULT "00000000000000",

    -- Required field (new(0), delete(1), modified(2), audit-descrepancy(3)
    downloadReason    TINYINT   NOT NULL DEFAULT 0,

    -- Primary key is the Npac id within each ServiceProvNetwork
    PRIMARY KEY (serviceProvId, id),

    -- Lrn is unique key within each ServiceProvNetwork
    UNIQUE KEY lrn (serviceProvId, lrn),

    -- Index lrn
    INDEX (lrn),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (serviceProvId) REFERENCES ServiceProvNetwork(serviceProvId)
)
TYPE = MyIsam;

--
-- Create ServiceProvNPA_NXX table
--
-- The Fields are defined in the order defined by the NPAC bulk data file
-- but the npac file formats the npanxx as 'npa-nxx'.
--
CREATE TABLE ServiceProvNPA_NXX
(
    -- Foreign key -> ServiceProvNetwork
```

```
    serviceProvId      CHAR(4)  NOT NULL,

    -- Required field (Primary Unique Key)
    id                 INT      NOT NULL,

    -- Required field (6 numeric characters)
    npanxx             CHAR(6)  NOT NULL,

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    creationTimeStamp  CHAR(14) NOT NULL DEFAULT "00000000000000",

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    effectiveTimeStamp CHAR(14) NOT NULL DEFAULT "00000000000000",

    -- Required field (new(0), delete(1), modified(2), audit-descrepancy(3)
    downloadReason     TINYINT  NOT NULL DEFAULT 0,

    -- Primary key is the Npac id within each ServiceProvNetwork
    PRIMARY KEY (serviceProvId, id),

    -- NpaNxx is unique key within each ServiceProvNetwork
    UNIQUE KEY npanxx (serviceProvId, npanxx),

    -- Index npanxx
    INDEX (npanxx),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (serviceProvId) REFERENCES ServiceProvNetwork(serviceProvId)

)
TYPE = MyIsam;

--
-- Create ServiceProvNPA_NXX_X table
--
-- The Fields are defined in the order defined by the NPAC bulk data file
-- but the npac file formats the npanxx as 'npa-nxx-x'.
--
CREATE TABLE ServiceProvNPA_NXX_X
(
    -- Foreign key -> ServiceProvNetwork
    serviceProvId      CHAR(4)  NOT NULL,

    -- Required field (Primary Unique Key)
    id                 INT      NOT NULL,

    -- Required field (7 numeric characters)
    npanxx_x           CHAR(7)  NOT NULL,

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    creationTimeStamp  CHAR(14) NOT NULL DEFAULT "00000000000000",

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    effectiveTimeStamp CHAR(14) NOT NULL DEFAULT "00000000000000",

    -- Required field (14 characters "YYYYMMDDHHMMSS")
    modifiedTimeStamp  CHAR(14) NOT NULL DEFAULT "00000000000000",

    -- Required field (new(0), delete(1), modified(2), audit-descrepancy(3)
    downloadReason     TINYINT  NOT NULL DEFAULT 0,

    -- Primary key is the Npac id within each ServiceProvNetwork
    PRIMARY KEY (serviceProvId, id),

    -- NpaNxx is unique key within each ServiceProvNetwork
```

```
    UNIQUE KEY npanxx_x (serviceProvId, npanxx_x),

    -- Index npanxx_x
    INDEX (npanxx_x),

    -- Not used by MySql but included for documentation
    FOREIGN KEY (serviceProvId) REFERENCES ServiceProvNetwork(serviceProvId)
)
TYPE = MyIsam;
```

```
-- Create Eagle Measurements Table

-- $S is replaced by CLLI for EMS in Table Name (ie,
STPAEagleMeasurments)

CREATE TABLE $SEagleMeasurements (

        yyyydddhh   INT UNSIGNED NOT NULL,

        UpdTnSuccess    INT UNSIGNED NOT NULL DEFAULT 0,

        UpdTnFail       INT UNSIGNED NOT NULL DEFAULT 0,

        DelTnSuccess    INT UNSIGNED NOT NULL DEFAULT 0,

        DelTnFail       INT UNSIGNED NOT NULL DEFAULT 0,


        UpdDGttSuccess  INT UNSIGNED NOT NULL DEFAULT 0,

        UpdDGttFail     INT UNSIGNED NOT NULL DEFAULT 0,

        DelDGttSuccess  INT UNSIGNED NOT NULL DEFAULT 0,

        DelDGttFail     INT UNSIGNED NOT NULL DEFAULT 0,


        UpdOGttSuccess  INT UNSIGNED NOT NULL DEFAULT 0,

        UpdOGttFail     INT UNSIGNED NOT NULL DEFAULT 0,

        DelOGttSuccess  INT UNSIGNED NOT NULL DEFAULT 0,

        DelOGttFail     INT UNSIGNED NOT NULL DEFAULT 0,


        UpdSplitSuccess INT UNSIGNED NOT NULL DEFAULT 0,

        UpdSplitFail    INT UNSIGNED NOT NULL DEFAULT 0,

        DelSplitSuccess INT UNSIGNED NOT NULL DEFAULT 0,

        DelSplitFail    INT UNSIGNED NOT NULL DEFAULT 0,

        Binds           INT UNSIGNED NOT NULL DEFAULT 0,

        LsmsRetries     INT UNSIGNED NOT NULL DEFAULT 0,
```

```
        NERetries       INT UNSIGNED NOT NULL DEFAULT 0,


        PRIMARY KEY (yyyydddhh)
)
TYPE = MyIsam;";
```

Glossary

A

AC	Alternating Current
ALM	Alarm Card
API	Application Interface
AS	Application Server
Association	An association refers to an SCTP association. The association provides the transport for protocol data units and adaptation layer peer messages.

B

BDD	Bulk Data Download

C

CA	Canada (NPAC Region)
CD	Compact Disk
CLLI	Common Language Location Identifier
CMIP	Common Management Information Protocol
CMISE	Common Management Information Service Element
CMOS	Complementary Metal Oxide Semiconductor

C

Command Class	A set of commands that are assigned to a user or to a terminal port. Command classes are assigned to a user with the `chg-user` or `ent-user` commands to control the commands that user can execute. Command classes are assigned to a terminal port with the `chg-secu-trm` command to control the commands that can be executed on a particular terminal.
CPU	Central Processing Unit
CSR	Customer Service Request

D

daemon	A process that runs in the background and performs a specified operation at predefined times or in response to certain events.
Database	All data that can be administered by the user, including cards, destination point codes, gateway screening tables, global title translation tables, links, LNP services, LNP service providers, location routing numbers, routes, shelves, subsystem applications, and 10 digit telephone numbers.
DB	Database
DC	Direct Current
DD	Detailed Design

D

DO	Derived Object
DVD	Digital Versatile Disk

E

EBDA	Enhanced Bulk Download and Audit
ECC	Error Correction Coded
EDR	Efficient Data Representation
EMS	Element Management System A system used to provide a top level management view of the network elements.
ESD	Electro-Static Discharge

F

FTP	File Transfer Protocol.

G

GB	Gigabyte — 1,073,741,824 bytes
GMT	Greenwich Mean Time
GPL	Generic Program Load
GTT	Global Title Translation
GUI	Graphical User Interface

H

H

HSOP	High Speed Operation Protocol

I

ID	Identity, identifier
IP	Internet Protocol
IP Address	The location of a device on a TCP/IP network. The IP Address is a number in dotted decimal notation which looks something like [192.168.1.1].
ISS	Integrated Signaling System

L

LED	Light Emitting Diode
LNP	Local Number Portability
LRN	Location Routing Number A 10 digit number identifying the new location of the ported 10 digit telephone number.
LSMS	Local Service Management System

M

MA	Mated Application
MIB	Management Information Database
MPS	Multi-Purpose Server

N

N

NANC	North American Numbering Council
NE	Network Element
NMS	Network Management System
NPA	Number Plan Area.
NPAC	Number Portability Administration Center
NPANXX	The area code and office prefix of a telephone number. For example, with the telephone number 919-555-1212, the digits 919 are the area code (NPA) and the digits 555 are the office prefix (NXX).
NPB	Numbering Pool Block
NSAP	Network Service Access Point
NTP	Network Time Protocol

O

OSI	Open System Interconnection

P

PC	Point Code.
PCI	Peripheral Component Interconnect
PDU	Protocol Data Unit

P

PID	Password ID
PSEL	Presentation Selector

R

RAID	Redundant Array of Independent Disks
RAM	Random Access Memory A type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes.
RJ	Registered Jack
RMTP	Reliable Multicast Transport Protocol
ROM	Read Only Memory
Route	A path to another signaling point.

S

SA	Service Action Indicates what service-specific behaviors to execute when processing a digit string.
SAM	Subsequent Address Message
SE	South East
SMS	Short Message Service

S

SNMP	Simple Network Management Protocol.
SP	Service Provider
SPID	Service Provider ID
SSH	Secure Shell
SSL	Secure Socket Layer
SV	Subscription Version
SW	Software

T

TCP/IP	Transmission Control Protocol/Internet Protocol
TN	Telephone Number A 10 digit ported telephone number.
TPD	Tekelec Platform Development

U

UDP	User Datagram Protocol

W

WAN	Wide Area Network
WC	West Coast
WE	Western

X

XML — Extensible Markup Language

Index

A

account types 64
as needed maintenance procedures 82

B

broadcast channel 29

D

database administration user 64
downloading files
    after site failure 370
    to correct NPA split information 370
downloading files, from NPAC 370
duplex mode 118

E

env command 61
external user 64

F

ftp, files from NPAC 370

G

GUI notifications
    severity 252

H

heartbeats
    sent by each server 120

K

keep alive messages, absence of 137

L

LSMS HA
    during starting a server 129
    monitoring server states 118
    sending heartbeats 120
lsmsadm group 64
lsmsall group 64
lsmsuser group 64
lsmsview group 65

M

manual
    audience 2
    scope 2
monthly maintenance procedures 82

N

NPA split information, downloading files from NPAC to correct 370
NPAC 370
    transfer files from 370

O

operating system 26

P

permission groups 64

Q

quarterly maintenance procedures 82
query server
    introduction 398
    maintenance procedures 398

R

Remote Monitoring optional feature 40
Report Manager 30

S

sacw 113
sentryd 108
server 118, 129
    starting 129
Service Assurance feature
    Service Assurance Agent 38
    Service Assurance Manager 38
    terms 38
severity of GUI notifications 252

shadow LSMS
maintaining 136
definition 132
simplex mode 118
software
overview 25
used in the LSMS system 25
SPID, using same at main LSMS and shadow LSMS for locally provisioned data 135
state
monitored by LSMS HA 118
Surveillance feature
error logs 37, 259
overview 30, 34
status 36
system administration user 64
system configuration user 64
system date, setting 61
system time
LSMS 59
NPAC 59

T

traceroute utility 98
transfer files from NPAC 370
troubleshooting
aids 6

V

viewer user 65

W

weekly maintenance procedures 82