IBM Parallel System Support
Programs for AIX

Installation and Migration Guide

GC23-3898-04

IBM Parallel System Support
Programs for AIX

Installation and Migration Guide

GC23-3898-04

Note!

Before using this information and the product it supports, be sure to read the general information under “Notices” on page xiii.

| **Fourth Edition (October 1997)**

This is a major revision of GC23-3898-03.

This edition applies to Version 2 Release 3 of IBM Parallel System Support Programs for AIX (5765-529), which runs on the IBM RS/6000 SP, and to all subsequent releases and modifications until otherwise indicated in new editions. Significant changes or additions to the text and illustrations are indicated by a vertical line (|) to the left of the change.

| This edition also contains information about support for the SP Switch Router Adapter that was added as a PTF to PSSP 2.3.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for readers' comments may be provided at the back of this publication, or you may address your comments to the following address:

International Business Machines Corporation
Department 55JA, Mail Station P384
522 South Road
Poughkeepsie, NY 12601-5400
United States of America

FAX: (United States and Canada) 1+914+432-9405
FAX: (Other Countries). Your international Access Code +1+914+432+9405

IBMLink (United States customers only): KGNVMC(MHVRCFS)
IBM Mail Exchange: USIB6TC9 at IBMMAIL
Internet: mhvrcfs@vnet.ibm.com
World Wide Web: http://www.rs6000.ibm.com (select Parallel Computing)

If you would like a reply, be sure to include your name, address, telephone number, or FAX number.

Make sure to include the following in your comment or note:

- Title and order number of this book
- Page number or topic related to your comment

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© **Copyright International Business Machines Corporation 1995, 1997. All rights reserved.**
Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Notices xiii
Trademarks xiii
Publicly Available Software xiv

About This Book xv
Who Should Use This Book xvi
How This Book Is Organized xvi
Typographic Conventions xvii
Accessing Online Information xvii
Obtaining Documentation xvii
Interface Instructions xvii
Starting and Using Perspectives xviii
Related Publications xviii
RS/6000 SP Publications xviii
Parallel System Support Programs for AIX Publications xviii
IBM Virtual Shared Disk and IBM Recoverable Virtual Shared Disk Publication xix
Performance Monitor Publication xix
General Parallel File System for AIX Publication xix
LoadLeveler Publications xix
Parallel Environment for AIX Publications xix
PVMe for AIX Publications xx
Client Input Output/Sockets (CLIO/S) Publications xx
Parallel I/O File System Publications xx
Network Tape Access and Control System for AIX (NetTAPE) Publications xx
Other IBM Publications xx
International Technical Support Organization Publications (Red Books) . . . xx
AIX and RS/6000 Publications xx
Service xxi
Network Queueing System/MVS (NQS/MVS) xxi
Network Connectivity xxii
Adapters xxii
Non-IBM Publications xxiii
Parallel Computing xxiii
Tcl xxiii
Ascend GRF xxiii
Manual Pages for Public Code xxiii

Chapter 1. Overview of the Installation and Migration Processes 1
What's New in PSSP and AIX? 1
Using Perspectives and the System Monitor Graphical User Interface 2
Installing Your SP System 2
Terminology 3
Prepare and Install the Control Workstation 3
Enter Node and Configuration Information 3
Install SP on the Nodes (Externals) 4
Install SP on the Nodes (Internals) 5
Migrating Your SP System 6
Working With the Basic AIX Image 6
Building a New AIX Image 7

© Copyright IBM Corp. 1995, 1997

Changing the Node's Install Image Attributes . . . 7
Detailed Overview of Network Installation of a Node . . . 8
NIM Specific Terminology and Concepts . . . 8
Network Installation . . . 9
Customization for Network Install . . . 9
Boot Processing . . . 10
Configuring Boot/Install Servers as NIM Masters . . . 10

Chapter 2. Installing and Configuring a New RS/6000 SP System . . . 13
Finding Related Installation Information . . . 13
Task A. Prepare the Control Workstation . . . 14
Step 1: Update the root User Path . . . 14
Step 2: Verify the Control Workstation Requirements . . . 14
Step 3: Verify Network Requirements . . . 16
Step 4: Connect Frames to Your Control Workstation . . . 16
Step 5: Configure RS-232 Control Lines . . . 16
Step 6: Tune the Control Workstation Network Adapters . . . 16
Step 7: Configure Control Workstation Ethernet Adapters . . . 17
Step 8: Verify Control Workstation Interfaces . . . 18
Step 9: Ensure Necessary Daemons are Running on the Control Workstation 18
Step 10: Change Control Workstation root Maximum Default Processes . . . 19
Step 11: Change Control Workstation Tunables and Tunable Values . . . 19
Step 12: Define Space for NIM Boot Images . . . 20
Step 13: Define Space for the /spdata Directory . . . 20
Step 14: Create Required /spdata Directories . . . 23
Step 15: Copy the AIX LPP Images and Other Required AIX LPPs . . . 24
Task B. Install PSSP on the Control Workstation . . . 26
Step 16: Copy the PSSP Images . . . 26
Step 17: Copy a Basic AIX (mksysb) Image . . . 27
Step 18: Install PSSP on the Control Workstation . . . 27
File Sets Installed on the Control Workstation . . . 28
Installation without AIX Preinstalled . . . 29
PSSP Installation Instructions . . . 30
Step 19: Initialize RS/6000 SP Authentication Services . . . 31
Step 20: Complete System Support Installation on the Control Workstation 39
Step 21: Run SDR and System Monitor Verification Tests . . . 40
Task C. Enter Site Environment, Frame, Node, and Switch Information . . . 41
Step 22: Enter Site Environment Information . . . 41
Step 23: Enter Frame Information and Reinitialize the SDR . . . 42
Step 24: Verify System Monitor Installation . . . 43
Step 25: Verify Frame Information . . . 44
Step 26: Update the State of the Supervisor Microcode . . . 44
Step 27: Enter Required Node Information . . . 45
Step 28: Acquire Hardware Ethernet Addresses . . . 47
Step 29: Verify Ethernet Addresses Were Acquired . . . 49
Step 30: Configure Additional Adapters for Nodes . . . 50
Step 31: Configure Initial Host Names for Nodes . . . 53
Step 32: Add Extension Node . . . 54
Step 33: Start System Partition-Sensitive Subsystems . . . 54
Step 34: Verify System Partition-Sensitive Subsystems Have Started . . . 55
Step 35: Restart System Monitor GUI or Perspectives . . . 56
Step 36: Set Up Nodes to Be Installed . . . 56
Step 37: Verify All Node Information . . . 58
Step 38: Verify Extension Node Information . . . 59

Step 39: Change the Default Network Tunable Values 59
Step 40: Configure Control Workstation as Boot/Install Server 62
Task D. Customize the Nodes 63
Step 41: Perform Additional Node Customization 63
Step 42: Verify the System Management Tools Were Correctly Installed . . 64
Step 43: Set Up the Switch 64
Step 44: Verify the Switch Primary and Primary Backup Node 67
Step 45: Set Switch Clock Source for All Switches 68
Step 46: Set Up System Partitions 69
Task E. Power On and Install the Nodes 71
Step 47: Network Boot Optional Boot/Install Servers 71
Step 48: Verify that System Management Tools Were Correctly Installed . . 76
Step 49: Network Boot the Remaining RS/6000 SP Nodes 76
Step 50: Verify Node Installation 77
Step 51: Run Verification Tests on All Nodes 79
Step 52: Start the Optional Switch 79
Step 53: Verify the Switch Was Installed Correctly 80
Step 54: Tune the Network Adapters 81
Install Extension Nodes 82
Control Workstation Steps 83
Extension Node Steps 83
Activate Extension Node Step 84
Extension Node Verification Steps 84
Run Post-Installation Procedures 85

Chapter 3. Installing and Configuring the High Availability Control Workstation 87
Finding Related Information 88
Task A: Prepare the Control Workstations 89
Step 1: Understand the Procedure 89
Step 2: Plan Network Configuration 89
Step 3: Install the SP System 89
Step 4: Install AIX on the Backup Control Workstation 89
Step 5: Back Up the Control Workstations 89
Step 6: Set Up the Hardware 90
Step 7: Configure RS-232 Control Lines 90
Task B. Update SP Authentication Services on Primary Control Workstation . 91
Step 8: Add the Kerberos Principal 91
Step 9: Add Kerberos rcmd Service Key 92
Step 10: Install PSSP on the Backup Control Workstation 92
Step 11: Configure the Backup Control Workstation as a Secondary Authentication Server or Client 92
Step 12: Keep Kerberos Keys the Same 95
Step 13: Verify Kerberos Data 96
Task C. Install Software 97
Step 14: Install HACMP on Both Control Workstations 97
Step 15: Verify Cluster Software 97
Step 16: Install the HACWS Image on Both Control Workstations 97
Step 17: Stop the Primary Control Workstation 97
Step 18: Configure Serial Network 97
Step 19: Configure the Network 97
Step 20: Migrate Internal File System 97
Step 21: Set Up External File System 98
Step 22: Complete Administration Tasks 99

Task D. Configure High Availability Cluster Multi-Processing 100
Step 23: Define the Cluster Environment 100
Step 24: Configure the HACWS Application Server 102
Step 25: Define the Resource Group 102
Step 26: Verify the Cluster and Node Environment 103
Task E. Set Up and Test HACWS 103
Step 27: Make Each Control Workstation Addressable by its Hostname . 103
Step 28: Set Up the HACWS Configuration 103
Step 29: Customize Cluster Event Processing 104
Step 30: Add IP Address Aliases 104
Step 31: Verify the HACWS Configuration 104
Step 32: Verify the Hardware Connections 105
Step 33: Reboot Control Workstations 105
Step 34: Start Cluster Services on the Primary Control Workstation 105
Step 35: Verify HACWS Installation 105

Chapter 4. Migrating to the Latest Level of PSSP 107
High-Level Migration Steps 107
Preparing to migrate 107
Applying PTFs to nodes 107
Migrating the control workstation to AIX 4.2.1 or later and PSSP 2.3 . . . 107
Partitioning your system, if necessary 108
Migrating a test node to AIX 4.2.1 and PSSP 2.3 108
Migrating the boot/install servers to AIX 4.2.1 and PSSP 2.3 108
Migrating the nodes to AIX 4.2.1 and PSSP 2.3. 108
Performing Post-Migration Activity 108
Preparing to Migrate 109
Step 1: Read the RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment 109
Step 2: Understand Coexistence Issues with PSSP 2.3 109
Step 3: Understand System Partitioning Issues 110
Step 4: Verify Control Workstation Requirements 110
Step 5: Verify Boot Install Server Requirements 111
Step 6: Reserve Port Numbers 111
Step 7: Back Up Your Control Workstation 111
Step 8: Back Up Your Nodes 112
Step 9: Archive the System Data Repository (SDR) 113
Step 10: Quiesce Your System 113
Step 11: Understand Amd/Automount Issues 113
Step 12: Understand Print Management Issues 114
Step 13: Understand System Reconfiguration Issues 114
Step 14: Understand Virtual Shared Disk (VSD) Issues 114
Paths to Migrate the Control Workstation to PSSP 2.3 and AIX 4.2.1 115
Migrate the Control Workstation from PSSP 1.2 to PSSP 2.3 117
Step 1: Prepare AIX 3.2.5 Boot/Install and /usr Servers 117
Using /usr Clients 118
Step 2: Prepare to Migrate and Verify Requirements 118
Step 3: Migrate to AIX 4.2.1 118
Step 3a: Perform Control Workstation BOS Migration Install 119
Step 3b: BOS Overwrite Install 119
Step 4: Verify AIX Migration 120
Step 5: Verify Control Workstation Interfaces 120
Step 6: Define Space for NIM Boot Images 120
Step 7: Define Space for the /spdata Directory 121

Step 8: Create Required /spdata Directories 121
Step 9: Copy the AIX 4.2.1 LPP Images 121
Step 10: Verify (Install/Copy) Correct Level of PAIDE (perfagent) 122
Step 11: Copy the PSSP Images 122
Step 12: Install (Copy) the Basic AIX (mksysb) Image 122
Step 13: Install PSSP on the Control Workstation 123
Step 14: Authenticate as the Administrative Principal 123
Step 15: Complete PSSP Installation on the Control Workstation 123
Step 16: Run SDR and System Monitor Verification Test 123
Step 17: Configure PSSP Services and Set Up Site Environment 123
Step 18: Start System Partition-Sensitive Subsystems and Verify 124
Step 19: Start Quiesced Applications 124
Step 20: Configure Control Workstation as Boot/Install Server 124
Step 21: Run Verification Tests 125
Step 22: Validate the Control Workstation 125
Migrate the Control Workstation from PSSP 2.1 to PSSP 2.3 126
Step 1: Prepare to Migrate and Verify Requirements 126
Step 2: Migrate to AIX 4.2.1 126
Step 2a: Perform Control Workstation BOS Migration Install 126
Step 2b: BOS Overwrite Install 127
Step 3: Verify AIX Migration 127
Step 4: Verify Control Workstation Interfaces 127
Step 5: Review Space Requirements for NIM Boot Images 128
Step 6: Review Space Requirements for /spdata 128
Step 7: Create Required /spdata Directories 128
Step 8: Copy the AIX 4.2.1 LPP Images 128
Step 9: Move the Existing LPP Images 129
Step 10: Verify (Install/Copy) Correct Level of PAIDE (perfagent) 129
Step 11: Copy the PSSP Images for PSSP 2.3 130
Step 12: Move the PSSP Images for PSSP 2.1 130
Step 13: Install (Copy) the Basic AIX (mksysb) Image 130
Step 14: Stop Daemons on the Control Workstation and Verify 130
Step 15: Install PSSP on the Control Workstation 131
Step 16: Authenticate as the Administrative Principal 132
Step 17: Complete PSSP Installation on the Control Workstation 132
Step 18: Run SDR and System Monitor Verification Test 132
Step 19: Configure PSSP Services and Set Up Site Environment 132
Step 20: Start System Partition-Sensitive Subsystems and Verify 133
Step 21: Start Quiesced Applications 133
Step 22: Unconfigure the NIM Master 133
Step 23: Configure Control Workstation as Boot/Install Server 134
Step 24: Run Verification Tests 134
Step 25: Validate the Control Workstation 135
Migrate the Control Workstation from PSSP 2.2 to PSSP 2.3 136
Step 1: Prepare to Migrate and Verify Requirements 136
Step 2: Migrate to AIX 4.2.1 136
Step 2a: Upgrade 136
Step 2b: Perform Control Workstation BOS Migration Install 136
Step 2c: BOS Overwrite Install 137
Step 3: Verify AIX Migration 137
Step 4: Verify Control Workstation Interfaces 137
Step 5: Review Space Requirements for NIM Boot Images 138
Step 6: Review Space Requirements for /spdata 138
Step 7: Create Required /spdata Directories 138

Step 8: Copy the AIX 4.2.1 LPP Images 139
Step 9: Verify (Install/Copy) Correct Level of PAIDE (perfagent) 139
Step 10: Copy the PSSP Images for PSSP 2.3 140
Step 11: Install (Copy) the Basic AIX (mksysb) Image 140
Step 12: Stop Daemons on the Control Workstation and Verify 140
Step 13: Install PSSP on the Control Workstation 141
Step 14: Authenticate as the Administrative Principal 141
Step 15: Complete PSSP Installation on the Control Workstation 141
Step 16: Run SDR and System Monitor Verification Test 141
Step 17: Configure PSSP Services and Set Up Site Environment 142
Step 18: Start System Partition-Sensitive Subsystems and Verify 142
Step 19: Start Quiesced Applications 142
Step 20: Configure Control Workstation as Boot/Install Server 143
Step 21: Run Verification Tests 143
Step 22: Validate the Control Workstation 144
Paths to Migrate the Nodes to PSSP 2.3 and AIX 4.2.1 145
Migration Install of Nodes to AIX 4.2.1 and PSSP 2.3 147
Step 1: Enter Node Configuration Data 147
Step 2: Verify Installation Settings 147
Step 3: Run setup_server to Configure the Changes 148
Step 4: Refresh System Partition-Sensitive Subsystems 148
Step 5: Disable Node From the Switch 148
Step 6: Shut Down the Node 148
Step 7: Network Boot the Node 148
Step 8: Run Verification Tests 149
mksysb Install of Nodes 150
Step 1: Enter Node Configuration Data 150
Step 2: Verify Installation Settings 150
Step 3: Run setup_server to Configure the Changes 151
Step 4: Refresh System Partition-Sensitive Subsystems 151
Step 5: Disable Node From the Switch 151
Step 6: Shut Down the Node 152
Step 7: Network Boot the Node 152
Step 8: Run Verification Tests 152
Migrate or Upgrade Nodes to AIX 4.2.1 or Later 153
Migrate 153
Upgrade 153
Upgrade Nodes to AIX 4.2.1 and PSSP 2.3 154
Step 1: Apply AIX 4.2.1 Upgrade on Node 154
Step 2: Verify AIX Migration 154
Step 3: Enter Node Configuration Data 154
Step 4: Verify Installation Settings 155
Step 5: Run setup_server to Configure the Changes 155
Step 6: Refresh System Partition-Sensitive Subsystems 155
Step 7: Disable Node From the Switch 156
Step 8: Copy the PSSP 2.3 pssp_script to Nodes' /tmp 156
Step 9: Execute the pssp_script on the Node 156
Step 10: Reboot the Node 156
Step 11: Start System Partition-Sensitive Subsystems 157
Step 12: Run Verification Tests 157
Perform Control Workstation Overwrite/Preservation Install 158
Step 1: Save spdata File System 158
Step 2: Save PSSP-Related Files 158
Step 3: Optionally, Save Additional Control Workstation Files 159

Step 4: Perform Control Workstation BOS Overwrite/Preservation 160
Step 5: Restore spdata File System 161
Step 6: Restore Control Workstation Files 161
Step 7: Configure RS-232 Control Lines 162
Step 8: Configure Ethernet Adapters 162
Step 9: Verify Step 163
HACWS Migration Strategy 164
High-Level HACWS Migration Instructions 165
Backing Up Your HACWS Configuration 165
AIX Migration Considerations 165
HACMP Migration Considerations 166
PSSP Migration Steps 167
Migrate an HACWS Configuration from PSSP 2.1 to PSSP 2.3 168
Prerequisites 168
Step 1: Verify Network Tunable Values 168
Step 2: Review Space Requirements for NIM Boot Images 168
Step 3: Review Space Requirements for /spdata 168
Step 4: Create Required /spdata Directories 169
Step 5: Copy the AIX 4.2.1 LPP Images 169
Step 6: Move the Existing LPP Images 169
Step 7: Verify (Install/Copy) Correct Level of PAIDE (perfagent) 169
Step 8: Copy the PSSP Images for PSSP 2.3 169
Step 9: Move the PSSP Images for PSSP 2.1 169
Step 10: Install (Copy) the Basic AIX (mksysb) Image 169
Step 11: Start Control Workstation Services on Primary Control Workstation 169
Step 12: Stop Control Workstation Services While HACMP is Running . . 169
Step 13: Install PSSP on Both Control Workstations 170
Step 14: Authenticate as the Administrative Principal 170
Step 15: Complete PSSP 2.3 Installation on Both Control Workstations . 170
Step 16: Verify the HACWS Configuration 171
Step 17: Run SDR and System Monitor Verification Test 171
Step 18: Configure PSSP Services and Set Up Site Environment 171
Step 19: Unconfigure the NIM Master 171
Step 20: Restart Control Workstation Services 172
Step 21: Run Verification Tests 172
Step 22: Validate the Control Workstation 172
Migrate an HACWS Configuration from PSSP 2.2 to PSSP 2.3 173
Prerequisites 173
Step 1: Verify Network Tunable Values 173
Step 2: Review Space Requirements for NIM Boot Images 173
Step 3: Review Space Requirements for /spdata 173
Step 4: Create Required /spdata Directories 174
Step 5: Copy the AIX 4.2.1 LPP Images 174
Step 6: Verify (Install/Copy) Correct Level of PAIDE (perfagent) 174
Step 7: Copy the PSSP Images for PSSP 2.3 174
Step 8: Install (Copy) the Basic AIX (mksysb) Image 174
Step 9: Start Control Workstation Services on Primary Control Workstation 174
Step 10: Stop Control Workstation Services While HACMP is Running . . 174
Step 11: Stop the amd Daemon on Both Control Workstations 174
Step 12: Install PSSP on Both Control Workstations 174
Step 13: Authenticate as the Administrative Principal 175
Step 14: Complete PSSP 2.3 Installation on Both Control Workstations . 175
Step 15: Verify the HACWS Configuration 176
Step 16: Run SDR and System Monitor Verification Test 176

Step 17: Configure PSSP Services and Set Up Site Environment 176
Step 18: Restart Control Workstation Services 176
Step 19: Run Verification Tests 176
Step 20: Validate the Control Workstation 176
Post-Migration Activity 177
Remove Obsolete Files and Resources 177
Recovery Procedures 178

Chapter 5. Reconfiguring the RS/6000 SP System 181
Adding a Frame 181
Step 1: Connect Frames to Your Control Workstation 182
Step 2: Power On Frames and Switches 182
Step 3: Configure the RS-232 Control Line 182
Step 4: Configure the Ethernet Adapter (Optional) 182
Step 5: Enter Frame Information and Reinitialize the SDR 182
Step 6: Verify Frame Information 183
Step 7: Update the State of the Supervisor Microcode 183
Step 8: Add Nodes to the System 183
Step 9: Refresh System Partition-Sensitive Subsystems 183
Step 10: Stop and Restart the Resource Manager in all Affected Partitions 183
Deleting a Frame 184
Step 1: Stop the Resource Manager Server 184
Step 2: Shut Down All the Nodes in the Frame 184
Step 3: Delete Frame Information from the SDR 185
Step 4: Reconfigure the System Partitions (Optional) 185
Step 5: Refresh System Partition-Sensitive Subsystems 186
Step 6: Restart the SP System Monitor GUI and Perspective 186
Step 7: Restart the Resource Manager Server 186
Adding Nodes 186
Step 1: Connect New Nodes to the Frame 187
Step 2: Update the State of the Supervisor Microcode 187
Step 3: Set Up, Power, and Configure the Nodes 187
Step 4: Refresh System Partition-Sensitive Subsystems 187
Step 5: Restart System Monitor GUI or Perspectives 188
Step 6: Stop and Restart the Resource Manager Server 188
Deleting Nodes 188
Step 1: Stop the Resource Manager Server 188
Step 2: Shut Down the Nodes 189
Step 3: Disconnect the Node from the Frame 189
Step 4: Delete Node Information From the SDR 189
Step 5: Refresh System Partition-Sensitive Subsystems 190
Step 6: Restart the Resource Manager Server 190
Replacing a Node with an Equivalent Node 190
Step 1: Shut Down the Node and Power It Off 191
Step 2: Replace the Old Node with the New One and Power It On 191
Step 3: Update the State of the Supervisor Microcode 191
Step 4: Delete NIM Client 191
Step 5: Acquire the Hardware Ethernet Address 192
Step 6: Set Up Nodes To Be Installed 192
Step 7: Restart Perspectives or the System Monitor GUI 192
Step 8: Network Boot the New SP Node 192
Step 9: Run Post—installation Procedures 193
Replacing a Node with a Different Type of Node 193
Step 1: Shut Down the Node and Power It Off 194

Step 2: Disconnect the Node From the Frame . . . 194
Step 3: Stop the Resource Manager Server . . . 194
Step 4: Delete Node Information From the SDR . . . 195
Step 5: Replace the Old Node with the New One and Power It On . . . 195
Step 6: Delete NIM Client . . . 195
Step 7: Update the State of the Supervisor Microcode . . . 195
Step 8: Set Up, Power, and Configure the Nodes . . . 195
Step 9: Refresh System Partition-Sensitive Subsystems . . . 196
Step 10: Restart the Resource Manager Server . . . 196
Step 11: Restart System Monitor GUI or Perspectives . . . 196
Adding a Switch . . . 196
Adding a Switch to a Switchless System . . . 197
Adding a Switch to a System With Existing Switches . . . 199
Reconfiguring Your System for Use with the SP Switch . . . 200
Prerequisites to Transferring Switches . . . 200
Step 1: Prepare for the Switch Transfer . . . 200
Step 2: Shut Down All Nodes and Clean Up the Control Workstation . . . 201
Step 3: Replace the High Performance Switch and Switch Adapters . . . 202
Step 4: Reconfigure the Hardware Monitor to Recognize New Hardware . . . 202
Step 5: Update the State of the Supervisor Microcode . . . 203
Step 6: Update the System Data Repository . . . 203
Step 7: Annotate a Switch Topology File . . . 203
Step 8: Set the Switch Primary and Primary Backup Nodes . . . 204
Step 9: Set Switch Clock Source for All Switches . . . 205
Step 10: Set Up Nodes to Customize . . . 206
Step 11: Power On the Nodes . . . 207
Step 12: Verify SP Switch Adapters . . . 207
Step 13: Start the Switch . . . 208
Step 14: Run Verification Test on the Switch . . . 208
Step 15: Reapply System Partition Configuration . . . 209
Replacing the Frame Supervisor . . . 209
Step 1: Install the New Frame Supervisor Card . . . 209
Step 2: Reconfigure the Hardware Monitor to Recognize New Hardware . . . 209
Step 3: Update the State of the Supervisor Microcode . . . 209
Step 4: Issue Eannotate . . . 209
Step 5: Issue Eclock . . . 209
Step 6: Issue Estart . . . 210
Replacing a Fixed Disk . . . 210
Step 1: Power Off the Node . . . 210
Step 2: Replace the Disk . . . 210
Step 3: Install the System Image on the Disk . . . 210
Step 4: Network Boot the Node . . . 211
Replacing a Disk Not in rootvg . . . 211
Step 1: Power Off the Node . . . 211
Step 2: Replace the Failing Fixed Disk . . . 212
Step 3: Power On the Node . . . 212
Step 4: Restore Any Data Previously Backed-Up . . . 212
Replacing an I/O Planar Card in a Thin Node or an Ethernet Adapter . . . 212
Step 1: Power Off the Node . . . 212
Step 2: Replace the Card . . . 213
Step 3: Delete NIM Client . . . 213
Step 4: Obtain the New Hardware Ethernet Address . . . 213
Step 5: Recreate NIM Client Definition . . . 213

Chapter 6. Performing Software Maintenance 215
Installing Program Updates 215
Which Approach is Right for You? 216
Working With Nodes That Are Down 216
Reinstalling PSSP 216
Updating the css Option 217
Adding mksysb Images to the Control Workstation 217
Restoring the Control Workstation from a mksysb Image 217
Restoring the Node from a mksysb Image 217
Updating the Print Subsystem 217
Installing Updates on a Per Node Basis 218
Installing Updates through Reinstallation 218
Build an Installation Image 219
Test Your Image on a Single Node 220
Propagate Your Installation Image 221
Applying PTFs to the System 221
Task A: Prepare the Control Workstation 221
Task B: Apply PTFs on One SP Node and Verify Correct Operation . . . 222
Task C: Apply PTFs to All Nodes 222
Task D: Commit PTFs on Node and Control Workstation 222
Task E: Update the State of the Supervisor Microcode 223
Task F: Create New mksysb Images 223
Restoring a Control Workstation from mksysb Image 223

Appendix A. SP Perspectives and System Monitor GUI Tasks 225
Starting and Using Perspectives 225
Starting and Using the System Monitor Graphical User Interface 225

Appendix B. Directory Information 229

Appendix C. Sample script.cust File 231

Appendix D. Sample tuning.cust File 237

Appendix E. SAGE Job Descriptions 239
Core Templates Defined by SAGE 239
Junior System Administrator 239
Intermediate/Advanced System Administrator 240
Additional Skill Areas 240

Appendix F. Boot/Install Server Configuration Commands 243

Appendix G. Reserving Ports 245
Procedures 245
Considerations for Network Information Service (NIS) 245
Resolving Port Number Conflicts 246

Glossary of Terms and Abbreviations 247

Index 255

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
USA

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Mail Station P300
522 South Road
Poughkeepsie, NY 12601-5400
USA
Attention: Information Request

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

AIX
ESCON
HACMP/6000
IBM
IBMLink
LoadLeveler
Micro Channel
NQS/MVS
POWERparallel
POWERserver
POWERstation
RISC System/6000

© Copyright IBM Corp. 1995, 1997

RS/6000
Scalable POWERparallel Systems
System/370
System/390
TURBOWAYS

Microsoft, Windows, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names, which may be denoted by a double asterisk (**), may be trademarks or service marks of others.

Publicly Available Software

This product includes software that is publicly available:

expect Programmed dialogue with interactive programs

Kerberos Provides authentication of the execution of remote commands

NTP Network Time Protocol

Perl Practical Extraction and Report Language

SUP Software Update Protocol

Tcl Tool Command Language

TclX Tool Command Language Extended

Tk Tcl-based Tool Kit for X-windows

This book discusses the use of these products only as they apply specifically to the RS/6000 SP system. The distribution for these products includes the source code and associated documentation. (Kerberos does not ship source code.) **/usr/lpp/ssp/public** contains the compressed **tar** files of the publicly available software. (IBM has made minor modifications to the versions of Tcl and Tk used in the SP system to improve their security characteristics. Therefore, the IBM-supplied versions do not match exactly the versions you may build from the compressed **tar** files.) All copyright notices in the documentation must be respected. You can find version and distribution information for each of these products that are part of your selected install options in the **/usr/lpp/ssp/README/ssp.public.README** file.

About This Book

This book provides information to help you install, configure, maintain, and migrate the RS/6000 SP. It includes concepts and instructions pertaining to:

- Installing and configuring the IBM Parallel System Support Programs for AIX
- Installing on an existing RS/6000 SP system
- Reconfiguring the system
- Performing system maintenance
- Migrating the system

Other books that help you administer and use the SP system include:

- The *IBM RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment* book helps you plan for the SP system. It tells you how to prepare for software installation and provides considerations for integrating it into your existing computing network.
- The *IBM Parallel System Support Programs for AIX: System Administration Guide* provides information to help you understand and perform SP System administration. It includes concepts and instructions including performing routine system administration tasks, making the system secure, managing sets of nodes, and monitoring the system.
- The *IBM Parallel System Support Programs for AIX: Diagnosis and Messages* book provides information to help you diagnose SP system problems and describes error messages, their meaning, and appropriate actions to take to recover from problems.
- The *IBM Parallel System Support Programs for AIX: Command and Technical Reference* provides detailed syntax and parameter information for all commands you can use to install, customize, and maintain the SP system.

This book applies to PSSP Version 2 Release 3. To find out what version of PSSP is running on your control workstation, enter the following:

```
SDRGetObjects SP code_version
```

In response, the system displays something similar to:

```
code_version
PSSP-2.3
```

If the response indicates **PSSP-2.3**, this book applies to the version of PSSP that is running on your system.

To find out what version of PSSP is running on the nodes on your system, enter the following:

```
splst_versions -G -t
```

In response, the system displays something similar to:

```
1 PSSP-2.3
3 PSSP-2.3
7 PSSP-2.2
8 PSSP-2.3
```

© Copyright IBM Corp. 1995, 1997

If you are running mixed levels of PSSP, be sure to maintain and refer to the appropriate documentation for whatever versions of PSSP you are running.

Who Should Use This Book

This book is intended for system administrators responsible for installing, configuring, and maintaining the RS/6000 SP system. It assumes the administrators have a working knowledge of AIX* or Unix** and experience with network systems.

The System Administrators Guild of USENIX (SAGE), has developed a classification for skills required for system administrators. Administrators of RS/6000 SP systems are expected to have level II skills (Junior System Administrator) or greater depending on the complexity of your site and system. See Appendix E, "SAGE Job Descriptions" on page 239 for more information on these job skills.

How This Book Is Organized

- Chapter 1, "Overview of the Installation and Migration Processes" on page 1 explains what happens when you perform the installation and customization procedure.
- Chapter 2, "Installing and Configuring a New RS/6000 SP System" on page 13 provides the information you need to get the RS/6000 SP system functioning in your environment.
- Chapter 3, "Installing and Configuring the High Availability Control Workstation" on page 87 explains how to setup and configure your optional High Availability Workstation (HACWS).
- Chapter 4, "Migrating to the Latest Level of PSSP" on page 107 describes how to migrate your system to the latest levels of AIX and PSSP.
- Chapter 5, "Reconfiguring the RS/6000 SP System" on page 181 discusses adding and replacing hardware components.
- Chapter 6, "Performing Software Maintenance" on page 215 provides information on updating installation images, LPPs, and support programs.
- Appendix A, "SP Perspectives and System Monitor GUI Tasks" on page 225 provides instructions for completing common tasks using SP Perspectives and the System Monitor graphical user interface.
- Appendix B, "Directory Information" on page 229 contains a list of the directories created when you install the RS/6000 SP LPP image.
- Appendix C, "Sample script.cust File" on page 231 contains a sample boot customization file (**script.cust**).
- Appendix D, "Sample tuning.cust File" on page 237 contains a sample tuning customization file (**tuning.cust**)
- Appendix E, "SAGE Job Descriptions" on page 239 contains system administrator job descriptions defined by SAGE.
- Appendix G, "Reserving Ports" on page 245 contains information on reserving port numbers.

This book also includes a glossary and index.

Typographic Conventions

This book uses the following typographic conventions:

Typographic	Usage
Bold	• **Bold** words or characters represent system elements that you must use literally, such as commands, flags, and path names. • **Bold** words also indicate the first use of a term included in the glossary.
Italic	• *Italic* words or characters represent variable values that you must supply. • *Italics* are also used for book titles and for general emphasis in text.
`Constant width`	Examples and information that the system displays appear in `constant width` typeface.
[ ]	Brackets enclose optional items in format and syntax descriptions.
{ }	Braces enclose a list from which you must choose an item in format and syntax descriptions.
|	A vertical bar separates items in a list of choices. (In other words, it means “or.”)
< >	Angle brackets (less-than and greater-than) enclose the name of a key on the keyboard. For example, <**Enter>** refers to the key on your terminal or workstation that is labeled with the word Enter.
...	An ellipsis indicates that you can repeat the preceding item one or more times.
<**Ctrl-***x***>**	The notation <**Ctrl-***x***>** indicates a control character sequence. For example, <**Ctrl-c>** means that you hold down the control key while pressing <**c>**.

Accessing Online Information

In order to use the IBM Parallel System Support Programs for AIX (PSSP) man pages or access the PSSP online (HTML) publications, the ssp.docs file set must first be installed. To view the PSSP online publications, you also need the following:

- Access to a common HTML document browser (such as Netscape, WebExplorer, or Mosaic).
- The location of the HTML index file provided with the ssp.docs file set. Contact your system administrator or installer for this location.

Obtaining Documentation

You can view this book or download a PostScript version of it from the IBM RS/6000 web site at **http://www.rs6000.ibm.com**. At the time this manual was published, the full path was **http://www.rs6000.ibm.com/resource/aix_resource/sp_books**. However, the structure of the RS/6000 web site can change over time.

Interface Instructions

Some sections of this book give step-by-step instructions for performing tasks with a graphical user interface. The instructions use a format that distinguishes between the user action and the system response.

User actions appear in uppercase bold type.

PRESS Cancel

Selections from a menu bar are indicated with an →.

SELECT SP → Topology

Starting and Using Perspectives

Perspectives is a graphical user interface you can use to manage and monitor the SP system. Complete instructions for using Perspectives appear in the on-line help information.

You can use Perspectives during the installation and migration process to perform a variety of tasks including installing software and verifying executed steps.

To start Perspectives, type **perspectives &**

Note that many of the steps require you to use SMIT. You can use SMIT directly by issuing SMIT commands or you can access SMIT using Perspectives. Often used SMIT fast-paths, such as **smit_verify**, are available from the Perspectives Launch Pad.

When launching Perspectives, you get the following message which should be ignored:

```
Warning: locale not supported by C library, locale unchanged
```

Related Publications

RS/6000 SP Publications

- *IBM RS/6000 SP: Planning, Volume 1, Hardware and Physical Environment*, GA22-7280
- *IBM RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment*, GA22-7281
- *IBM RS/6000 SP: Maintenance Information, Volume 1, Installation and CE Operations*, GC23-3903
- *IBM RS/6000 SP: Maintenance Information, Volume 2, Maintenance Analysis Procedures and Parts Catalog*, GC23-3904

Parallel System Support Programs for AIX Publications

- *IBM Parallel System Support Programs for AIX: Administration Guide*, GC23-3897
- *IBM Parallel System Support Programs for AIX: Diagnosis and Messages Guide*, GC23-3899
- *IBM Parallel System Support Programs for AIX: Command and Technical Reference*, GC23-3900

- *IBM Parallel System Support Programs for AIX: Event Management Programming Guide and Reference*, SC23-3996
- *IBM Parallel System Support Programs for AIX: Group Services Programming Guide and Reference*, SC28-1675
- *IBM Parallel System Support Programs for AIX: Licensed Program Specification*, GC23-3901

As an alternative to ordering the individual books, you can use SBOF-8587 to order the entire SP software library.

IBM Virtual Shared Disk and IBM Recoverable Virtual Shared Disk Publication

- *IBM Parallel System Support Programs for AIX: Managing Shared Disks*, SA22-7279

Performance Monitor Publication

- *IBM Performance Toolbox Parallel Extensions for AIX: Guide and Reference*, SC23-3997

General Parallel File System for AIX Publication

- *IBM General Parallel File System for AIX: Installation and Administration Guide*, SA22-7278

LoadLeveler Publications

- *Using and Administering LoadLeveler*, SC23-3989
- *IBM LoadLeveler: Licensed Program Specification*, GH23-0040

Parallel Environment for AIX Publications

- *IBM Parallel Environment for AIX: Hitchhiker's Guide*, GC23-3895
- *IBM Parallel Environment for AIX: Operation and Use, Volume 1*, SC28-1979
- *IBM Parallel Environment for AIX: Operation and Use, Volume 2*, SC28-1980
- *IBM Parallel Environment for AIX: Installation Guide*, GC28-1981
- *IBM Parallel Environment for AIX: Messages*, GC28-1982
- *IBM Parallel Environment for AIX: MPL Programming and Subroutine Reference*, GC23-3893
- *IBM Parallel Environment for AIX: MPI Programming and Subroutine Reference*, GC23-3894
- *IBM Parallel Environment for AIX: Licensed Program Specification*, GC23-3896

As an alternative to ordering the individual books, you can use SBOF-8588 to order the entire Parallel Environment for AIX library.

PVMe for AIX Publications

- *IBM PVMe for AIX: Fact Sheet*, GC23-3907
- *IBM PVMe for AIX: User's Guide and Reference*, GC23-3884
- *IBM PVMe for AIX: Licensed Program Specification*, GC23-3885

Client Input Output/Sockets (CLIO/S) Publications

- *IBM CLIO/S General Information*, GC23-3879
- *IBM CLIO/S Licensed Program Specification*, GC23-3789
- *IBM CLIO/S User's Guide and Reference*, GC28-1676

Parallel I/O File System Publications

- *IBM AIX Parallel I/O File System: Fact Sheet*, G325-0649
- *IBM AIX Parallel I/O File System: Installation, Administration, and Use*, SH34-6065
- *IBM AIX Parallel I/O File System: Licensed Program Specification*, GH34-6066

Network Tape Access and Control System for AIX (NetTAPE) Publications

- *IBM NetTAPE General Information*, GC23-3990
- *IBM NetTAPE User's Guide and Reference*, available from your IBM representative

---

Other IBM Publications

International Technical Support Organization Publications (Red Books)

- *IBM International Technical Support Centers Implementing High Availability on RS/6000 SP*, SG24-4742
- *IBM International Technical Support Centers RS/6000 SP High Availability Infrastructure*, SG24-4838
- *IBM International Technical Support Centers RS/6000 SP PSSP 2.2 Technical Presentation*, SG24-4868
- *IBM International Technical Support Centers RS/6000 SP PSSP 2.3 Technical Presentation*, SG24-2080

AIX and RS/6000 Publications

- *IBM AIX Version 4 Getting Started*, SC23-2527
- *IBM AIX General Concepts and Procedures for RS/6000*, GC23-2202
- *IBM AIX Version 4 Files Reference*, SC23-2512
- *IBM AIX Version 4 System Management Guide: Communications and Networks*, SC23-2526
- *IBM AIX Version 4.1 Installation Guide*, SC23-2550
- *IBM AIX Version 4.2 Installation Guide*, SC23-1924

- *IBM AIX Version 4 Commands Reference*, SBOF-1851 (all volumes)
- *IBM AIX Versions 3.2 and 4 Performance Tuning Guide*, SC23-2365
- *IBM AIX Version 4 Messages Guide and Reference*, SC23-2641
- *IBM AIX Version 4.1 Network Installation Management Guide and Reference*, SC23-2627
- *IBM AIX Version 4.2 Network Installation Management Guide and Reference*, SC23-1926
- *IBM AIX Version 4 System Management Guide: Operating System and Devices*, SC23-2525
- *IBM AIX Version 4 General Programming Concepts: Writing and Debugging Programs*, SC23-2533
- *IBM AIX Version 4 Communications Programming Concepts*, SC23-2610
- *Diskless Workstation Management Guide*, SC23-2433
- *C++ for AIX/6000: Language Reference*, SC09-1606
- *C++ for AIX/6000: Standard Class Library Reference*, SC09-1604
- *C++ for AIX/6000: User's Guide*, SC09-1605
- *IBM Performance Toolbox 1.2 and 2 for AIX: Guide and Reference*, SC23-2625

Service

- *IBM AIX Version 3.2 Problem Solving Guide and Reference*, SC23-2204
- *IBM AIX Version 4 Problem Solving Guide and Reference*, SC23-2606
- *Information Manual for Diagnostics Micro Channel Bus*, SA23-2765
- *7012 300 Series Operator Guide*, SA23-2623
- *7012 300 Series Installation and Service Guide*, SA23-2624
- *7013 500 Series Operator Guide*, SA38-0530
- *7013 500 Series Installation and Service Guide*, SA38-0531
- *Electrical Safety for IBM Customer Engineers*, S229-8124
- *Service Information Binder*, SX33-6060
- *7015 Model R30 CPU Enclosure Operator Guide*, SA23-2742
- *7015 Model R30 CPU Enclosure Installation and Service Guide*, SA23-2743
- *Supplemental Information for 7012 G Series Models, 7013 J Series Models, 7015 Models R30 and R40* (No order number — this book comes as part of the ship group with the SP hardware)

Network Queueing System/MVS (NQS/MVS)

- *IBM NQS/MVS Installing and Administering*, SC23-0232
- *IBM NQS/MVS Client User's Guide*, SC23-0231
- *IBM NQS/MVS General Information*, GC23-3684
- *IBM NQS/MVS Licensed Program Specifications*, GC23-0233

Network Connectivity

- *IBM LAN Cabling System Planning and Installation Guide*, GA27-3361
- *IBM Cabling System Optical Fiber Planning and Installation Guide*, GA27-3943
- *IBM 8250/8260/8285 Planning and Site Preparation Guide*, GA33-0285
- *IBM 6611 Network Processor: Introduction and Planning Guide*, GK2T-0334

Adapters

- *SP Switch Router Adapter Guide*, GA22-7310
- *FDDI Introduction and Planning Guide*, GA27-3892
- *FDDI User's Guide and Programming Reference*, SC28-2823
- *Planning for Fiber Optic Channel Links*, GA23-0367
- *IBM Token-Ring Network Introduction and Planning Guide*, GA27-3677
- *RS/6000 Token Ring Adapter Card*, G511-1681
- *HiPPI User's Guide and Programmer's Reference*, SA23-0369 and SA23-2488
- *AIX Parallel and ESCON Channel Tape Attachment/6000 Installation and User's Guide*, GA32-0311
- *9334 SCSI Expansion Units Operator Guide*, GA33-3232
- *9334 Models 010 and 011 SCSI Expansion Units: Installation and Service Guide*, SY33-0165
- *9334 Models 500 and 501 SCSI Expansion Units: Installation and Service Guide*, SY33-0167
- *SCSI-2 Fast/Wide Adapter*, SC23-2646
- *IBM SCSI-2 Fast/Wide Adapter/A Technical Reference*, S83G-7545
- *Turboways 100 User's Guide ATM*, GA27-4057
- *9333 Model 010 and 011 High-Performance Disk-Drive Subsystem Operator Guide*, GA33-3208
- *9333 Model 010 and 011 High-Performance Disk-Drive Subsystem Installation and Service Guide*, SY33-0161
- *9333 Model 010 and 011 High-Performance Disk-Drive Subsystem Hardware Technical Information*, SA33-3209
- *9333 Model 500 and 501 High-Performance Disk-Drive Subsystem Operator Guide*, GA33-3234
- *9333 Model 500 and 501 High-Performance Disk-Drive Subsystem Installation and Service Guide*, SY33-0168
- *9333 Model 500 and 501 High-Performance Disk-Drive Subsystem Hardware Technical Information*, SA33-3235
- *IBM SCSI Tape Drive, Medium Changer, and Library Device Drivers Installation and User's Guide*, GC35-0154

Non-IBM Publications

Parallel Computing

- Almasi, G., Gottlieb, A., *Highly Parallel Computing*, Benjamin-Cummings Publishing Company, Inc., 1989.
- Gropp, W., Lusk, E., Skjellum, A., *Using MPI*, The MIT Press, 1994.
- Message Passing Interface Forum, MPI: *A Message-Passing Interface Standard*. Version 1.1, University of Tennessee, Knoxville, Tennessee, June 6, 1995.
- Foster, I., *Designing and Building Parallel Programs*. Addison-Wesley, 1995.
- Pfister, Gregory, F., *In Search of Clusters*. Prentice Hall, 1995.

Tcl

- Ousterhout, John K., *Tcl and the Tk Toolkit*, Addison-Wesley, Reading, MA, 1994, ISBN 0-201-63337-X.

Ascend GRF

Order according to your Ascend GRF IP switch model:

- *Getting Started*
- *Configuration Guide*
- *Reference Guide*

You can order the Ascend GRF as the IBM 9077.

Manual Pages for Public Code

The following manual pages for public code are available in this product:

SUP	/usr/lpp/ssp/man/man1/sup.1
NTP	/usr/lpp/ssp/man/man8/xntpd.8
	/usr/lpp/ssp/man/man8/xntpdc.8
Perl (Version 4.036)	/usr/lpp/ssp/perl/man/perl.man
	/usr/lpp/ssp/perl/man/h2ph.man
	/usr/lpp/ssp/perl/man/s2p.man
	/usr/lpp/ssp/perl/man/a2p.man
Perl (Version 5.003)	Man pages are in the /usr/lpp/ssp/perl5/man/man1 directory

Manual pages and other documentation for Tcl, TclX, Tk, and expect can be found in the compressed **tar** files located in **/usr/lpp/ssp/public**.

Chapter 1. Overview of the Installation and Migration Processes

This chapter provides an overview of the installation and migration processes. Before you install the SP system, you must perform several planning activities. These activities include completing worksheets or checklists that reflect your decisions regarding, but not limited to, the following:

- System partitioning
- Node and switch configuration
- System management options
- Boot/install servers and node relationships
- Location and type of authentication servers

It is essential that you plan your system carefully before attempting to install it. Refer to the *RS/6000 SP: Planning, Volume 1, Hardware and Physical Environment* and the *RS/6000 SP: Planning Volume 2, Control Workstation and Software Environment* books for planning details.

What's New in PSSP and AIX?

- **PSSP 2.3**

  The new function in PSSP 2.3 requires AIX level 4.2.1 or greater.

- **Extension Node Support**

  Extension nodes are non-standard nodes that extend your system's capabilities or scope, but they cannot be used in all the same ways as standard SP nodes. They are attached to the system via an extension node adapter.

- **The SPIMG Tape**

  The PSSP spimg tape contains a minimal mksysb image for AIX 4.2.1.

- **Amd Replacement**

  An automounter transparently mounts a file system at the time a user accesses it and unmounts it when there has been no activity for a specified amount of time. The Amd automounter, public domain code, was previously available with PSSP but for PSSP 2.3, it has been replaced with Automount, which is packaged with all levels of PSSP.

- **Print Removal**

  The Print Management function, previously packaged with PSSP, is no longer available in PSSP 2.3. Nodes in an SP system running releases of PSSP prior to PSSP 2.3, can still use Print Management. For nodes running PSSP 2.3, you can choose to use the Printing Systems Manager packaged with AIX.

- **PSSP Level Coexistence Support**

  PSSP 2.3 supports multiple levels of AIX and PSSP in the same system partition. Refer to the migration chapter in this book for more detailed information.

- **Extended Migration Support**

© Copyright IBM Corp. 1995, 1997

You can now migrate to PSSP 2.3 and AIX 4.2.1 from several starting points. Refer to the migration chapter in this book for more detailed information.

- **New Tuning Files**

  PSSP 2.3 now provides three additional customization files that allow you to tune your system to meet specific organization needs. One file is geared for the commercial environment, one is for the development environment, and one is for the scientific environment.

Using Perspectives and the System Monitor Graphical User Interface

Perspectives is a graphical user interface you can use to manage and monitor the SP system. Complete instructions for using Perspectives appear in the on-line help information.

You can use Perspectives during the installation and migration process to perform a variety of tasks including installing software and verifying executed steps.

To start Perspectives, type **perspectives &**

Note that many of the installation steps require you to use SMIT. You can use SMIT directly by issuing SMIT commands or you can access SMIT using Perspectives. Often used SMIT fast-paths, such as **smit_verify**, are available from the Perspectives Launch Pad.

When launching Perspectives using the **install_cw** command or from the command line, you get the following message which should be ignored:

```
Warning: locale not supported by C library, locale unchanged
```

In addition to Perspectives, you can use the System Monitor graphical user interface to manage and monitor the SP system. Complete instructions for using this interface appear in the System Administration Guide. Note that support is not available for the extension node when using the System Monitor GUI.

To start the System Monitor GUI, type **spmon -g**.

Installing Your SP System

This section discusses some common terminology, as well as the major sections of the installation process.

Installation involves the following major steps:

1. Prepare (install or migrate) the control workstation with PSSP and AIX.
2. Enter configuration information for nodes that are new to the system.
3. Install and customize the nodes.

You complete all installation and configuration steps centrally from the control workstation.

Terminology

Before installing your system, become familiar with the following terminology used throughout this book. The definitions provide you with an overview only. For more detailed discussions, refer to the appropriate section in this book or the remainder of the PSSP library:

- Overwrite Install

  This type of installation writes a new version of AIX to the hard drive without saving any information on the system.

- Migration Install

  This type of installation preserves all filesystems except /**tmp**.

- Coexistence

  Coexistence occurs when you mix different releases of PSSP software within an SP. There may also be a mixture of AIX software that supports the PSSP level.

- Network Installation Manager (NIM)

  NIM is an AIX component that assists in installing workstations (nodes) over communication networks.

- NIM Master

  In the NIM environment, a NIM master is an AIX system that can install one or more NIM clients. A system must be defined as a NIM master before any NIM clients are defined. A NIM master must be at the latest AIX level with the NIM master file sets installed. A NIM master manages the configuration database containing the information for the NIM clients.

- NIM Client

  A NIM client is a system installed and managed by a NIM master. SP supports the stand-alone type of NIM client.

Prepare and Install the Control Workstation

The first step in installing the SP system is preparing the control workstation. This involves connecting your frame's RS-232 lines to the serial ports of your control workstation, configuring the Ethernet connections on your control workstation, and verifying name resolution. Other steps include installing AIX 4.2 software with required PTFs.

Enter Node and Configuration Information

After preparing the control workstation, you can begin configuring the nodes. To configure them, you can use PSSP commands or the Software Management Interface Tool (SMIT) interface to enter information into the System Data Repository (SDR). The information you enter is based on the planning worksheets you completed. If you have not yet completed these worksheets, turn to the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* and understand the information presented there before you begin installing your system. (Both configuration methods are described throughout the detailed installation information.)

Install SP on the Nodes (Externals)

SP node installation consists of these phases:

- Network installation
- Customization
- Boot processing

In the network installation phase, PSSP uses the AIX Network Installation Management (NIM) support to restore an AIX mksysb image created with the **mksysb** command. It can also perform an AIX migration install to the hard disk of the node. During the customize phase, PSSP personalizes the node with host names, default routes, and TCP/IP network adapter information from the SDR. AIX reboots the node. Final customization takes place after the node reboots, during boot processing.

Use the **spbootins** command to change the **bootp_response** attribute of the Node object in the SDR. You can set this attribute to **install**, **customize**, or **migrate**. For more information on these attributes, refer to the *Command and Technical Reference Guide*.

Network Installation

To install the nodes, netboot the nodes over the network. Boot/install servers on the same network respond by installing the AIX image on the nodes.

Customization

Customization involves the following:

- Updating the node's host name and default route
- Defining the network adapters
- Installing the PSSP LPP options on the node
- Running the **script.cust** you updated for your site-specific customization
- Running the **tuning.cust** you updated for your site-specific customization
- Running cloning support for all nodes.

You customize your system after installing it. You can also customize a node that already has AIX and PSSP installed at any time. Situations that would call for a customize-only step include:

- You have added or changed the networking or routing for one or more nodes.
- You have changed your authentication servers or reinitialized them, invalidating the Kerberos service keys stored on the nodes.

You can do additional customization in one of three ways:

- By copying the **/usr/lpp/ssp/samples/script.cust** and **/usr/lpp/ssp/samples/tuning.cust** files on the control workstation to the **/tftpboot** directory and by tailoring these files to meet your needs. Commands in these files are run after the mksysb installation and PSSP customization and before the reboot of each node. IBM suggests you use **script.cust** to complete your installation and **tuning.cust** to set initial network performance values.

- By selecting one of the IBM supplied tuning files to set your performance parameters. One file is for the commercial environment, one is for the development environment, and one is for the scientific environment. For more information on these files, refer to chapter 2 of this book or the tuning section in the PSSP System Administration Guide.
- By not selecting any existing files. If you choose this method, PSSP automatically uses the **tuning.default** file to set your initial performance parameters.

Before the initial boot of a node, the required RS/6000 SP options (such as **ssp.clients**, **ssp.basic**, and **ssp.sysctl**) are installed if they are not part of the AIX 4.2 image already on the node.

Boot Processing

After PSSP completes installation and customization, AIX reboots the node. PSSP can do additional configuration during the node reboot depending upon the choices you made in SMIT Site Environment panel or with the **spsitenv** command.

Install SP on the Nodes (Internals)

The previous section titled "Install SP on the Nodes (Externals)" provided a high-level discussion of the installation process. This section provides a more-detailed discussion of the process and is intended to provide you with additional, in-depth information.

AIX 4.2 provides the NIM environment to install AIX on the nodes. PSSP defines the control workstation as a NIM master. If a system is larger than one frame, boot/install servers are defined as NIM masters so they can install nodes. In a multi-frame system, the first node in each frame, by default, is a NIM master for its frame. You can change this by using the **spbootins** command. You can define other nodes as boot/install servers and have PSSP make them NIM masters. This section discusses the parts of NIM exploited by the SP system. For more detailed information about the NIM environment, see the IBM AIX Version 4.2 Network Installation Management Guide and Reference.

The NIM environment includes a NIM master, a network, and its clients. The NIM master contains the information necessary to install its NIM clients.

Installing and Migrating Nodes (NIM Clients)

After PSSP configures the NIM masters and the NIM clients, you can begin installing the nodes. If you have a single-frame system, the control workstation installs the nodes. If you have a multi-frame system, the PSSP default is for the first node in each frame to install other nodes in that frame. You may select other SP nodes to be the NIM masters. This depends upon the physical layout of the installation network configuration.

When the node is network booted, the NIM master completes the installation and migration steps as follows:

1. Installs the AIX mksysb image for installation or performs an AIX migration install for migration.
2. Runs **pssp_script** on the node to do the following:
   a. Defines the host name and the primary adapter interface

b. Defines the network adapters specified in the SDR for this NIM client

c. Installs necessary AIX and PSSP file sets if they are not already installed

d. Runs **script.cust** if it exists in the boot/install server's /**tftpboot**

e. Runs **tuning.cust** if it exists in the boot/install server's /**tftpboot**

3. Reboots the node for more PSSP configuration.

Migrating Your SP System

Chapter 4 of this book discusses how to migrate your system to the latest level of AIX and PSSP. You should also refer to the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* to understand how to plan your migration. In general, you can migrate to PSSP 2.3 and AIX 4.2 from several starting points as shown in the list that follows. Note that you do not have to migrate your entire system at once. You can choose to migrate your system all at once or several nodes at a time.

- PSSP 2.2 and AIX 4.1.4, 4.1.5, 4.2.x
- PSSP 2.1 and AIX 4.1.3, 4.1.4, 4.1.5
- PSSP 1.2 and AIX 3.2.5

To migrate a node, the node to migrate must have an AIX 4.2.1 boot/install server and the server must be running PSSP 2.3. The NIM master must be at the latest level of AIX and PSSP to which you want to migrate the node. You can use the **spbootins** command to perform the following functions:

- Change the boot/install server.
- Change the node to migrate or customize.
- Change the **lppsource_name.**
- Change the **code_version.**

Working With the Basic AIX Image

The **spimg** installp image contains a mksysb of an AIX system. You can use this image to install AIX on the nodes in your system after you have successfully installed and configured your control workstation. The PSSP 2.3 spimg medium contains several mksysb images which you can install into /**spdata**/**sys1**/**install**/**images** directory. These images contain the supported AIX LPPs and files to install the SP nodes. The minimal system is made of up of the following:

- The basic operating system
- Extensions
- Networking
- Basic utilities

IBM provides the image as a base for getting your system up and running quickly. You can customize this image to meet the needs of your production environment.

See the *Memo to Users* for details on the supported AIX levels (APARs) that are contained in the SPIMG.

Building a New AIX Image

When you are installing your system for the first time, you can generate a mksysb image and install that on your nodes during the initial installation. To generate this image, do either of the following:

- Generate a mksysb on a node after you have installed the node using the basic image and additional LPPs required for your configuration. You first should install the SP node using the base spimg and the PSSP LPPs. IBM does not support using a boot/install server node to generate the mksysb image because the boot/install node contains additional files that are not wanted in the mksysb image. Then you can use **script.cust** to install additional LPPs and service your system requires. At this point, you can test the node with applications specific to your users' needs to make sure it meets your environment requirements. When you are satisfied this node has all of the LPPs and service, you can make a mksysb image from it by using the SMIT mksysb menu.
- Use a standalone workstation (either the control workstation or a different standalone workstation).

  If you use the control workstation to create the mksysb image, the image should be created before defining the space for the /spdata directory. After you have completed "Step 19: Initialize RS/6000 SP Authentication Services", you cannot use the control workstation to build a new image. Running the **setup_authent** command on any workstation makes the workstation unsuitable for generating a mksysb image for a node. This is because **setup_authent** sets up authentication databases which are unique to the machine.

The control workstation (or a different standalone workstation) must be at the correct level of the AIX RS/6000 operating system and must have all required PTFs applied. See the *Memo to Users* for the list of required AIX operating system level and PTFs. One way to ensure this is to install the mksysb image that resides in the spimg installp image on its installation media.

After the image is created, you must copy it to the**/spdata/sys1/install/images** directory on the control workstation. This directory is the starting point for all the mksysb images used for the RS/6000 SP system. Make sure the directory has permissions `rwxr-sr-x` and the images have permissions `rw-r--r--`.

Changing the Node's Install Image Attributes

After creating and copying a new image to the control workstation, you are ready to update the System Data Respository (SDR) with the name of the new image for the nodes you want to install. To define a new image, you can use the **spbootins** command or the SMIT **server_dialog** interface to do the following:

- Redefine the node's attributes in the SDR.
- Create new installation and configuration files for the boot/install server.
- Copy the new image to the boot/install server for the nodes to be reinstalled.

Detailed Overview of Network Installation of a Node

The information in this section is optional. Read this section if you want to understand the details of the network installation described in "Install SP on the Nodes (Externals)".

NIM Specific Terminology and Concepts

- NIM Master

  A site may have more than one NIM master, but these NIM masters and their clients are considered to be separate NIM environments. NIM does not provide any services to share information across these separate environments.

  As a default, the control workstation is the NIM master for a single frame system. If you have more than one frame, the default configuration is different: the control workstation installs the first node in each frame and defines it as a NIM master. Then, each NIM master installs the rest of the nodes in its frame. You can change the default by using SMIT **server_dialog** or the **spbootins** command.

  Whether you use the default configuration or define your own, you use **spbootins** to define the boot/install server. The **spbootins** command updates the SDR with the information specified with the command and invokes the **setup_server** function on the boot/install servers to define them as NIM masters.

  The **setup_server** function configures and defines the NIM master, resources, and clients that allow the nodes to be installed using the NIM environment.

- NIM Objects

  NIM stores information about the NIM environment as objects in the NIM database. The types of objects defined for the SP system are:

  – Network
  – Machine
  – Resource

  Network objects represent information about the network interfaces required for installing a client. The SP system uses the en0 Ethernet interface on the client for the NIM installation.

  Although the SP System may support multiple Ethernet networks depending upon the physical and defined subnets for your system, only the client's en0 interface is supported for the NIM installation.

  Machine objects represent the machine configuration for a NIM client. Each machine object contains attributes which define it. Examples of machine attributes are:

  – Type of machine (standalone)
  – Hardware address of the client's network installation interface (en0)
  – TCP/IP host name of the client
  – Name of the network object defining the network to which the client is connected
  – Type of processor - Uniprocessor (UP) or Multiprocessor (MP).

Resource objects represent available resources in the NIM environment. All operations on a client in a NIM environment require one or more resources to be allocated. Examples of resources available in a NIM environment are:

- SPOT - Shared Product Object Tree (SPOT)
- mksysb - AIX mksysb image
- script - Scripts run as part of the NIM customization on the client
- lppsource - Directory of installable LPP images
- bosinst_data - Prompt, noprompt, and migrate installation information

See the AIX Network Installation Management Guide and Reference for a complete list and descriptions of the resource objects.

The SP system supports installation of mksysb images only through NIM mksysb resource objects.

Network Installation

When a node boots over the network, it issues a **bootp** request on that network specifying its network device hardware address. (For the RS/6000 SP, this is the node's en0 Ethernet). The boot/install server has a list of nodes it boots and their associated hardware Ethernet addresses.

The **bootp** daemon on the boot/install server gets the request and looks in its table (/**etc**/**bootptab**) for this node's hardware Ethernet address. If it finds the address in its table, it responds by sending the node's IP address.

The node's IPL Read-Only Storage (ROS) requests a boot image transferred to the node using **tftp**. The boot image is run, the rootvg gets created, and NIM performs the installation of the mksysb image. After the mksysb installation is complete, NIM invokes the **pssp_script** script resource which transfers the install information files from the boot/install server to the node and performs the customization. These install files contain information necessary to successfully complete the netinstall.

Customization for Network Install

pssp_script transfers the following netinstall information files from the boot/install server to the node and then performs the customization:

- /**tftpboot**/*node_name*.**install_info**
- /**tftpboot**/*node _name*.**config_info**

Fields in the **install_info** file contain the following information:

- Client en0 IP address and host name
- SP system and node related data from the System Data Repository (SDR)
- Netinstall server IP address and host name
- Control workstation IP information and host name
- lppsource
- PSSP code version

Fields in the **config_info** file contain the following information:

- Node number

- Switch node information
- Default route
- Initial host name
- Control workstation IP information and host name
- An entry for each adapter defined in the SDR, listing the following:
  - Adapter name
  - Adapter IP address host name
  - Netmask
  - ring_speed (for token ring)
  - Cable type (DIX/BNC/TP)

After a node is installed, pssp_script gets a copy of the **config_info** file from its master. The information in the **config_info** file is used to define the adapters, set the hostname, define the default route, and to customize the adapters with information like host name and default route. This file is transferred from the server to the node during customization. The file is read at this time and the node is configured.

The PSSP file sets **ssp.basic**, **ssp.perlpkg**, **ssp.sysctl**, **ssp.ha** and **ssp.clients** are installed if they are not already installed. At this time the **ssp.sysman** option is installed if you have selected any of the additional system management options. The **ssp.css** is always installed on systems with a switch. The **ssp.jm** option is installed if the node's boot/install server has it installed.

As part of completing the network install, NIM modifies the boot/install server's **/etc/bootptab** file so that the node does not perform a netinstall again on the next boot. PSSP changes the SDR node object **bootp_response** attribute to **disk**.

Boot Processing

After customization, a bootable image is written to the node's disk. The node is then shut down and rebooted. When it is rebooted, PSSP checks the SDR to determine if any of the PSSP Site Environment options were chosen. If an option is selected, the node configuration for that system management option is performed now. When the node reboots, if it is a boot/install server, **setup_server** is run.

Configuring Boot/Install Servers as NIM Masters

When you run **/usr/lpp/ssp/bin/setup_server** to configure a boot/install server, it does the following:

- Creates **/tftpboot/***node_name***.install_info** and **/tftpboot/***node_name***.config_info** for all its client nodes.
- Configures the server as a NIM master
- Defines among other items, the spot, mksysb, script, lppsource, bosinst NIM resources
- Defines nodes to be installed or booted in diagnostics or maintenance as NIM clients
- Allocates NIM resources to the NIM clients as needed

- Copies the mksysb images (if any of its nodes need to be installed) to the boot/install server that services the nodes.
- Creates required authentication files, /**tftpboot**/ *hostname***-new-srvtab**
- Executes the NIM **bos_inst** command which allocates the NIM boot and NIM script resources, updating /**etc**/**bootptab**

Chapter 2. Installing and Configuring a New RS/6000 SP System

This chapter describes how to install the IBM Parallel System Support Programs for AIX (PSSP), configure your control workstations, servers and processor nodes, and initialize the system.

Notes:

- Perform the steps in this chapter only if you are installing a new system or if you are doing a complete reinstall. Do not perform the steps if you are migrating from one level of PSSP to another level. For migration steps, refer to the migration chapter in this book.
- Make sure you have your configuration worksheets complete and available before you proceed with installation. During the procedure you are prompted for network, host name, and configuration data. It is easier to install the system if you plan your configuration beforehand. Refer to the *IBM RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment* for planning information.
- You can install your system by using either the System Management Interface Tool (SMIT) or PSSP commands. SMIT is a graphical menu-driven interface to enter information into the System Data Repository (SDR). Experienced users may prefer to issue the PSSP commands directly. Throughout this chapter, instructions for all methods are given. Use default options unless instructed to do otherwise.
- Note - Systems with Default Options Installed or Preloaded Systems

  One of the decisions you must make prior to installing your system is how you want to receive the SP. You have the option of purchasing your SP with the default software installed or you can purchase one that IBM has preloaded with software to meet your organization's specific needs. For more detailed information on these preloaded options, refer to Chapter 1 of the *RS/6000 SP: Planning Volume 2, Control Workstation and Software Environment*.
- Note — Reserving Port Numbers

  Some of the subsystems managed by Syspar Controller (syspar_ctrl) allocate port numbers from the range 10000 to 10100, inclusive. Therefore, if any customer subsystem, such as DB2, uses port numbers in this range, such port numbers must be reserved in /**etc**/**services**. For details, refer to Appendix G, “Reserving Ports” on page 245.

Finding Related Installation Information

To find out more information, refer to the following manuals:

- *IBM General Concepts and Procedures for RISC System/6000*
- *AIX Network Installation Management Guide and Reference*
- *IBM AIX for RISC System/6000 Commands Reference*

© Copyright IBM Corp. 1995, 1997

Task A. Prepare the Control Workstation

This section describes the steps you take to prepare the control workstation. Note that it is a prerequisite for the control workstation to already have the correct level of AIX installed.

Step 1: Update the root User Path

You must run all installation tasks from root on the control workstation, except where indicated. All of the SP commands in this chapter are in **/usr/lpp/ssp/bin**, except where indicated in the following list:

- /usr/lib/instl - inurid
- /usr/sbin - no, mklv, crfs, mount, chfs
- /usr/lpp/ssp/kerberos/bin - klist

To avoid entering the complete path name each time you want to invoke a command, add the path statement to the root user path in root's **.profile** file. The following is an example of the root's user path statement:

```
PATH=$PATH:/usr/lpp/ssp/bin:/usr/lpp/ssp/kerberos/bin
```

In order for this path statement to take effect, you first have to execute **.profile**.

To verify that this step completed successfully, issue:

```
echo $PATH
```

Step 2: Verify the Control Workstation Requirements

Ensure that the following requirements are met:

1. Refer to the document, *Memo to Users*, that accompanies the PSSP installation media for the latest information for supported AIX release and PTF levels.
2. The RISC System/6000 you use as the control workstation must have the following software installed:
   - AIX Version 4.2.1 or later Base Operating System
   - bos.net (TCP/IP and NFS)
   - perfagent.server fileset, which is part of the Performance Aide for AIX (PAIDE) feature of the Performance Toolbox for AIX (PTX)

     This product provides the capability to monitor your SP system's performance, collects and displays statistical data for SP hardware and software, and simplifies run-time performance monitoring of a large number of nodes.

     PAIDE (perfagent.server) must be installed on the control workstation of any SP that has one or more nodes at PSSP 2.2 or greater. The level of PAIDE installed on the control workstation must match the level of AIX installed on the control workstation.

     PAIDE (perfagent.server) must be copied to the lppsource directory on the control workstation of any SP that has one or more nodes at PSSP 2.2 or greater. The level of PAIDE copied to the lppsource directory must match the level of AIX in the lppsource directory.

     The installation image of the perfagent.server should be *perfagent.server.xxx* where *xxx* is the version name. It can also be

perfagent41 if it is a preinstalled system. Also, note that only PTFs are named perfagent.server and perfagent.tools.

PAIDE and AIX levels - there are two PAIDE features of PTX: one for AIX 4.1 and one for AIX 4.2. However, the perfagent.server within PAIDE is related to the AIX level, as follows:

perfagent.server 2.2.w.x required for AIX 4.2.w.y

The perfagent.server file set, which is part of the Performance Aide for AIX (PAIDE) comes in a separate media. However, if you have a preinstalled system, the file set perfagent.server should already be installed on your system and saved in your system's mksysb. If you want to reinstall or upgrade the level of perfagent, install perfagent* from your system mksysb or from the PAIDE media to install all the necessary perfagent components.

3. The control workstation requires one serial port available per frame for the RS-232 cable that supports hardware monitoring and control. If your system has more than two frames, you may need an asynchronous adapter card to provide the extra ports if your control workstation does not already have them.
4. The control workstation must have ample disk space for the boot/install server files. See the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment* for detailed information about space requirements.

Notes:

1. After installing the AIX BOS Product on the control workstation, check to see if the **inurid -r** command was run by issuing:

   ```
   /usr/lib/instl/inurid -q ; echo $?
   ```

   If you executed the **inurid -r** command, some data would have been removed from the /**usr**/**lpp**/**ssp**/**inst_root** directory. This means that the system cannot be used as a SPOT server, which, in turn, does not allow the control workstation to become a NIM master for installing the nodes.

   If the return code=1, the control workstation needs to be reinstalled with an image without the **inurid -r** command being run.

   Some possible reasons which may have caused the **inurid -r** command to be run include:

   - The control workstation was installed with a non-mksysb NIM installation with a bosinst resource which had the RM_INST_ROOT variable set to `yes`.
   - The control workstation was installed with a mksysb image that had **inurid** command run on it prior to the creation of the image.
   - The **inurid** command was issued on this system manually.
2. All names and addresses of all IP interfaces on SP nodes must be resolvable on the control workstation before you install and configure the SP.
3. After you have set the host names and IP addresses on the control workstation, you should not change them for the duration of the installation.

Step 3: Verify Network Requirements

Using your node worksheets, check all SP Ethernet and additional adapter information to ensure that you have assembled the correct host name, IP address, and netmask data for installation.

Step 4: Connect Frames to Your Control Workstation

Connect RS-232 and Ethernet cables from the SP system frames to the control workstation according to your SP Control Workstation Worksheet. The IBM Customer Engineer will perform this step for you. See the *Maintenance Information Volume 1* for instructions.

Step 5: Configure RS-232 Control Lines

Each frame in your system requires a serial port on the control workstation configured to accommodate the RS-232 line. For example, if you have two frames, configure two tty terminals.

If using:	Do this:
SMIT	**TYPE** **smit tty** • The TTY menu appears **SELECT** Add a TTY **SELECT** RS-232 Asynchronous Terminal **SELECT** An appropriate serial port (parent adapter) connection. For example, **sa0**. • A data entry window appears. **PRESS** **List** to show the available port numbers. Select a port number. For example, **s1**, **s2**, **s3**, or **s4**. **PRESS** **Do** to configure the line.

mkdev	Enter a command similar to this example, which defines and configures an RS-232 line for parent adapter sa0 on port serial port 1:
	`mkdev -c tty -t tty -s rs232 -p sa0 -w s1`
	This example configures a second port of a two-frame system:
	`mkdev -c tty -t tty -s rs232 -p sa1 -w s2`

You can accept the default baud rate of 9600. The internal system daemon called **hardmon** changes the rate to 19200.	

Step 6: Tune the Control Workstation Network Adapters

Various models of the network adapters can have different values for transmit queue sizes. For PCI, set the queue size to 256. For micro-channel adapters running AIX 4.1.x, the maximum value is allowed. For micro-channel adapters running AIX 4.2, set the queue size to 512.

You can set these values using SMIT or the **chdev** command. If the adapter you are changing is also the adapter for the network you are logged in through, you will have to make the changes to the database only. Then reboot the control workstation for the changes to become effective.

If using:	Do this:
SMIT	**TYPE** **smit devices** • The Devices menu appears **SELECT** Communication • The Communication menu appears **SELECT** The adapter you want to reset (for example, `Ethernet Adapter`) • The Ethernet Adapter menu appears **SELECT** Adapter • The Adapter menu appears **SELECT** Change / Show Characteristics of an Ethernet Adapter • An Ethernet Adapter window appears **SELECT** An adapter from the list shown • The Change / Show Characteristics of an Ethernet Adapter window appears **CHANGE** The TRANSMIT queue size to 160 (150 for Ethernet on SP nodes) **CHANGE** `Apply change to DATABASE only` to **yes**. (Press F4 and select yes.) **PRESS** **Do** to apply the changes to the database.
chdev	Enter `chdev -P -l ent0 -a xmt_que_size=150`
You must reboot the control workstation in order for the changes to take effect.	

Step 7: Configure Control Workstation Ethernet Adapters

Use SMIT or the **chdev** command to configure each Ethernet adapter connecting your frames to the control workstation. For details on the correct use of **chdev**, see the *AIX Commands Reference*, the man pages, or the online information database.

Refer to your SP Control Workstation Worksheet in the *RS/6000 SP: Control Workstation and Software Environment*.

If the adapter is not yet defined or configured, use **smit mkinet** or the **mkdev** command instead of **smit chinet** or **chdev** to specify new IP host name and netmask values. If you are adding an extension node to your system, you may want to configure the adapters now. For more information, refer to “Install Extension Nodes” on page 82.

If using:	Do this:
SMIT	**TYPE** **smit chinet** **SELECT** The Ethernet interface to be configured **ENTER** IP interface and netmask information from worksheet. **TYPE** **up** in the `current STATE` option **PRESS** **Do** to complete operation
chdev	Enter a command similar to this example, which configures an en0 adapter. `chdev -l en0 -a netaddr=129.33.41.1 -a netmask=255.255.255.0 -a state=up`

mkdev	Enter a command similar to this example, which defines and configures an en0 adapter.
	`mkdev -c if -s EN -t en -a netaddr=129.33.34.1 \`
	`netmask=255.255.255.0 state=up -q -w en0`

Step 8: Verify Control Workstation Interfaces

Verify the configuration for each Ethernet adapter in the control workstation. You can verify that the adapter is installed even if it is not cabled to the SP system yet.

Verify each Ethernet adapter by *pinging* its IP address and seeing if you get a proper response. If you do not receive a response, debug the network problem, and reconfigure the adapter.

For example:

```
ping -c 1 129.33.34.1
```

Step 9: Ensure Necessary Daemons are Running on the Control Workstation

1. Check to see if the System Resource Controller (SRC) is running by issuing the following:

   ```
   lssrc -a
   ```

   If you get an error message similar to the following, then SRC is not running:

   ```
   The System Resource Controller daemon is not active
   ```

   To start SRC, uncomment or add the srcmstr entry in the file called **/etc/inittab** and reboot the control workstation using the **shutdown -Fr** command.

   In **/etc/inittab** the srcmstr entry should look like:

   ```
   srcmstr:2:respawn:/usr/sbin/srcmstr # System Resource Controller
   ```

2. Check to see if the bootps and tftp entries are uncommented in the file called **/etc/inetd.conf**. If they are commented (a leading pound sign designates a comment), uncomment the two entries in the file and issue the following:

   ```
   refresh -s inetd
   ```

Step 10: Change Control Workstation root Maximum Default Processes

When you first install your system, the number of processes the non-root user can have is set to **40**, an AIX 4.2 default. You will not be able to continue installing your system with this default value—you must increase the number. IBM suggests changing the maximum number to 256.

If using:	Do this:
SMIT	**TYPE** smit system • The System Environment menu appears. **SELECT** Change / Show Characteristics of Operating System **ENTER** 256 for the maximum number of processes allowed per user. **PRESS** Enter
chdev	Enter: `chdev -l sys0 -a maxuproc='256'`

Step 11: Change Control Workstation Tunables and Tunable Values

When you first install your system, the network tunable values are set to AIX 4.2 defaults. (A **tunable** is a performance parameter you can set to a value that makes your system run its workload most efficiently.) Your system may not run efficiently with the default values. Use the **no** command to display these values. This command and all its parameters are described in the *IBM AIX Commands Reference*.

When you install PSSP on your control workstation, change the network tunables on the control workstation interface to the suggested values in the following table.

Table 1. Control Workstation Tunables

Tunable	Suggested Initial Value	Description
thewall	16384	The upper bound on the amount of real memory that can be used by the communications subsystem. The units are in 1 KB increments.
sb_max	163840	Upper limit on the size of the TCP and UDP buffers in mbufs of allocated space to a connection.
ipforwarding	1	Specifies whether the kernel should forward packets. A value of **1** forwards packets when they are not for the local system; a value of **0** prevents forwarding.
tcp_sendspace	65536	The default size of the TCP send window.
tcp_recvspace	65536	The default size of the TCP receive window.
udp_sendspace	32768	The default size of the UDP send buffer. The effective maximum is 65536 (64K).
udp_recvspace	65536	The default size of the UDP receive buffer.
tcp_mssdflt	1448	Maximum package size for remote network.

Using the no Command

To display network tunable values, enter:

```
no -a
```

To change the value of **thewall**, enter:

```
no -o thewall=16384
```

When you change the network tunables, they take effect immediately. However, they are not preserved across a boot. To make the changes to the tunables effective across boots, add the **no -o** commands you used to change the network tunables to the bottom of the file **/etc/rc.net**.

Step 12: Define Space for NIM Boot Images

Before creating an AIX boot/install server, ensure that there is sufficient space in the root (/) file system or create a separate file system for **/tftpboot** to manage the space required for the boot images (approximately 25 megabytes per lppsource level supported) created by NIM.

Step 13: Define Space for the /spdata Directory

The **/spdata** directory contains, among other items, mksysb and installp file sets. IBM suggests you create a separate volume group for the **/spdata** file system. These file sets require a minimum of 2 GB of disk space. You may require additional disk space if you need to support multiple AIX and PSSP release levels, and multiple mksysb images. If you have not done so already, use the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment* to help you estimate how much space you need to define.

To define space for the **/spdata** directory, refer to the following table to determine which steps to follow. Do either Procedure A, B1, or B2. Do not perform more than one procedure.

Procedure	To:	Follow these steps:.
A	Define a new volume group	1. Do “Step 13.1: Define a Volume Group” on page 21 2. Do “Step 13.2: Create the Logical Volume for /spdata” on page 22 3. Do “Step 13.3: Create the File System for spdata” on page 22 4. Do “Step 13.4: Mount the /spdata File System” on page 23 5. Do “Step 14: Create Required /spdata Directories” on page 23
B1	Use an existing volume group (such as rootvg) and define a new file system.	1. Do “Step 13.2: Create the Logical Volume for /spdata” on page 22 2. Do “Step 13.3: Create the File System for spdata” on page 22 3. Do “Step 13.4: Mount the /spdata File System” on page 23 4. Do “Step 14: Create Required /spdata Directories” on page 23
B2	Use an existing volume group (such as rootvg) and expand on an existing file system.	1. Do “Step 13.5: Expand an Existing File System” on page 23 2. Do “Step 14: Create Required /spdata Directories” on page 23

Step 13.1: Define a Volume Group

The logical volume manager (LVM) configuration you define can also include placing the /spdata file system in its own volume group rather than using the default volume group **rootvg**.

You cannot create a separate volume group if all control workstation disks are in use or the control workstation has only one physical volume. When working with larger disks that are greater than 4 GB, you must specify the physical partition size to be 8 MB or more for the spdata volume group.

If using:	Do this:
SMIT	**TYPE** **smit vg** • The Volume Groups menu appears **SELECT** Add a Volume Group • The Add a Volume Group window appears **TYPE** The volume group name (for example, **spdatavg**). **TYPE** The physical volume name (press F4 and select a volume). **PRESS** **Do** to create the volume group. SMIT automatically varies on the volume group.

mkvg	The following command will create a new logical volume named **spdatavg**, using **hdisk1** as the physical volume.
	`mkvg -f -y spdatavg hdisk1`
	After you create the new volume group **spdatavg**, vary on the volume group on your control workstation using the **varyonvg** command.
	`varyonvg spdatavg`

Step 13.2: Create the Logical Volume for /spdata

To create the logical volume called spdata_lv with 2 GB, assuming 4 MB physical partition size, use the **mklv** command:

```
mklv -y spdata_lv -x 512 spdatavg 500
```

Step 13.3: Create the File System for spdata

You now need to create the /**spdata** file system on the control workstation. The file system must be mounted as /**spdata**.

If using:	Do this:
SMIT	**TYPE** **smit crfs** **SELECT** Add a Journaled File System on a Previously Defined Logical Volume **SELECT** Add Standard Journal File System **SELECT** Your logical volume (press F4 and select a volume). **SPECIFY** /**spdata** as mount point **SELECT** **yes** for `Mount AUTOMATICALLY at system restart?` **PRESS** **Do** to create the file system.
crfs	To create a file system /**spdata** within the newly created logical volume **spdata_lv**, use the **crfs** command. The following example creates the /**spdata** file system, using logical volume **spdata_lv** and mount point /**spdata**. It also adds the /**spdata** into the /**etc**/**filesystems** to be automatically mounted at system restart. `crfs -v jfs -d spdata_lv -m /spdata -A yes -p rw -t no`

Step 13.4: Mount the /spdata File System

After you create the new /**spdata** file system, you need to mount it on the control workstation. Use the AIX command **mount**.

The following example mounts the /**spdata** file system.

```
mount /spdata
```

Step 13.5: Expand an Existing File System

IBM does not suggest the expanded root file system configuration because of possible performance and backup considerations with the control workstation.

You can choose not to create a logical volume and file system for /**spdata** and increase your current root / file system to hold the required LPP file sets, AIX mksysb images, and installp file sets.

If using:	Do this:
SMIT	**TYPE** **smit chfs** **SELECT** Change / Show Characteristics of a Journaled File System **SELECT** / **SPECIFY** The size in 512-byte blocks to increase the file system
chfs	The following example increases the root file system by 400 MB, which is equal to 781250 512-byte blocks. `chfs -a size=+781250 /`

Step 14: Create Required /spdata Directories

Make sure you mount the new /**spdata** file system before you create the /**spdata** directories. The SP requires you create sub-directories on the /**spdata** file system for storing critical PSSP data. Make sure the directories have the permissions `rwxr-sr-x`. Table 2 on page 24 lists the required directories.

Table 2. Required /spdata Directories

Directory	Description	mkdir Command
/spdata/sys1	Main directory for SDR, spmon, Log Mgt, and Installation	mkdir -P /spdata/sys1
/spdata/sys1/install	Main directory for PSSP installation	mkdir /spdata/sys1/install
/spdata/sys1/install/<name>/lppsource	Location of required AIX file sets.	mkdir -p \ /spdata/sys1/install/<name>/lppsource
/spdata/sys1/install/images	Location of all required AIX mksysb images	mkdir /spdata/sys1/install/images
/spdata/sys1/install/pssplpp/<code_version>	Location of all SP installp file sets.	mkdir -p \ /spdata/sys1/install/pssplpp/<code_version>
/spdata/sys1/install/pssp	Location of NIM configuration data files	mkdir /spdata/sys1/install/pssp

<name> is the new lpp_source name for the nodes (such as aix42 if that is what you called the subdirectory with the AIX 4.2 lpp source). Keep in mind that the setup_server program looks for this name later on during the installation process. By default, it is set to the string "default", so that if you use that as your subdirectory name, you don't have to change name here. If you do not provide a name, setup_server assumes the value is *default*.

default is the directory name default.

<code_version> is the version of code of the form PSSP-x.y. (such as, PSSP-2.3)

Step 15: Copy the AIX LPP Images and Other Required AIX LPPs

If you have not done so already, you must now copy the AIX file sets into the **/spdata/sys1/install/<name>/lppsource** directory on your hard disk on the control workstation. You can download all of the AIX file sets (approximately 1.5 GB) or only the minimal required AIX file sets (approximately 450 MB).

The following is the minimal list of AIX file sets required to perform mksysb installations:

bos	bos.up.*
bos.info.*	bos.mp.*
bos.net.*	bos.diag.*
bos.powermgt.*	X11.Dt.*
bos.sysmgt.*	X11.fnt.*
bos.terminfo.*	X11.loc.*
devices.*	X11.motif.*
X11.apps.*	X11.msg.*
X11.base.*	X11.vsm.*
X11.compat.*	xlC.rte.*
perfagent.server	

perfagent.server fileset, which is part of the Performance Aide for AIX (PAIDE) feature of the Performance Toolbox for AIX provides the capability to monitor your SP system's performance, collects and displays statistical data for SP hardware

and software, and simplifies run-time performance monitoring of a large number of nodes. For more information on the perfagent.server fileset, refer to “Step 2: Verify the Control Workstation Requirements” on page 14.

The <*prefix*>.* syntax in this list refers to everything that starts with the <*prefix*>. For example, **devices.*** refers to all of the file sets starting with **devices**.

1. Download the AIX file sets and the required AIX LPPs into **/spdata/sys1/install/**<**name**>**/lppsource**. If you change the path name in any way, the installation fails.
2. Refer to your disk usage planning in the “Combining the Space Requirements” section of the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment* to determine if you have allocated enough space to accomplish this task.
3. Allow at least 1-3 hours for moving all the file sets from media to disk.

Login to the control workstation as root and run **bffcreate** using SMIT or the command line. If you choose not to use **bffcreate**, you need to run the **inutoc** script as follows:

```
cd /spdata/sys1/install/<name>/lppsource
inutoc .
```

If using:	Do this:	
SMIT	**TYPE**	**smit bffcreate**
		• The Copy Software to Hard Disk for Future Installation window appears.
	PRESS	**List** (F4) to show the available devices. Select the device containing the product installation media.
	PRESS	**Do** to display the target parameters.
		• The Copy Software to Hard Disk for Future Installation window appears.
	PRESS	**List** to show the LPP packages to load. Select either all of the file sets to download or only the minimal list.
	TYPE	**/spdata/sys1/install/**<**name**>**/lppsource** in the `DIRECTORY for storing software` field.
	PRESS	**Do** to begin downloading.
bffcreate	This example shows the product media on **rmt0** and selection of all LPPs. Using **all** may load unnecessary file sets into the directory.	
	`bffcreate -qvX -t/spdata/sys1/install/<name>/lppsource -d /dev/rmt0 all`	
The following warning message is issued—ignore it:		

`bffcreate: Warning:`
`important size information is missing`
`from the table of contents file.  Consequently, there`
`may not be enough free file system space to successfully`
`create the bff image(s).  Continuing anyway...`		

Task B. Install PSSP on the Control Workstation

This section describes the steps you take to install PSSP on the control workstation. After you prepare the control workstation, you are ready to install the PSSP software.

Step 16: Copy the PSSP Images

The RS/6000 SP package is comprised of these install images:

Image	Description
pssp	Contains the PSSP install options
ssp.csd	Contains the IBM Virtual Shared Disk
ssp.ptpegui	Contains the spperfmon perspective

Before you install the PSSP images on the control workstation, you first need to copy the images from the installation media to **/spdata/sys1/install/pssplpp/**<**code_version>** directory on your hard disk.

1. Login to the control workstation as root and run **bffcreate** using SMIT or the command line.

If using:	Do this:
SMIT	**TYPE** **smit bffcreate** • The Copy Software to Hard Disk for Future Installation window appears. **PRESS** **List** (F4) to show the available devices. Select the device containing the product installation media. **PRESS** **Do** to display the target parameters. • The Copy Software to Hard Disk for Future Installation window appears. **TYPE** **/spdata/sys1/install/pssplpp/**<**code_version>** in the `DIRECTORY for storing software` field. **PRESS** **Do** to begin the install process.
bffcreate	This example shows the product media on **rmt0**. Enter `bffcreate -d /dev/rmt0 -t /spdata/sys1/install/pssplpp/<code_version -X all`

The following warning message is issued, and you can ignore it:
`bffcreate:`
`Warning: important size information is missing from`
`the table of contents file. Consequently, there may not`
`be enough free file system space to successfully create`
`the bff image(s). Continuing anyway...`	

2. Update the image Table of Contents (.toc)

   When **bffcreate** completes, rename **ssp.usr.2.3.0.0** in **/spdata/sys1/install/pssplpp/**<**code_version>** to **pssp.installp**.

   a. Enter the following:

```
cd /spdata/sys1/install/pssplpp/<code_version>
mv ssp.usr.2.3.0.0 pssp.installp
```

b. Because the installation tools expect the name of the installp image to be **pssp.installp**, and installp places a different image name in its **.toc** file, update that **.toc** file by running the **inutoc** script as follows:

```
cd /spdata/sys1/install/pssplpp/<code_version>
inutoc .
```

Step 17: Copy a Basic AIX (mksysb) Image

Note that there is no root password in the basic (minimal) AIX/6000 SP mksysb image. If you choose to use this image (it is the default) to install your nodes, you should take appropriate steps to make the system more secure. If your site uses NIS, you can use the script.cust file to define the NIS client. If you are not using NIS, you can use the script.cust file to copy the **/etc/passwd** and **/etc/security/passwd** files from the boot/install server. Refer to the example in the **/usr/lpp/ssp/samples/script.cust** file to determine how to copy a file.

The media shipped with the SP hardware contains the spimg installp image which contains multiple mksysb images of the minimal AIX system. PSSP 2.3 only uses the AIX 4.2 mksysb image called bos.obj.ssp.42. If you are not supporting older versions of PSSP, you can discard the other mksysb images from the **/spdata/sys1/install/images** directory.

You can install the AIX image(s) directly from installation media to the appropriate directory.

If you intend to use your own mksysb image, copy it to **/spdata/sys1/install/images/bos.obj.ssp.42** and continue with “Step 18: Install PSSP on the Control Workstation” .

If using:	Do this:
SMIT	**TYPE** **smit install_latest** • The Install New Software Products at Latest Level window appears. **TYPE** The input device (press F4 and select a device). **PRESS** **Do** to begin the install.
installp	Enter: `installp -a -d /dev/rmt0.1 -X spimg`

Step 18: Install PSSP on the Control Workstation

The PSSP images are made up of one or more file sets. Some of these file sets must be installed on the control workstation while others are optional. A subset of the file sets is installed on the individual nodes later in the installation process. Refer to the following table for more information.

File Sets Installed on the Control Workstation

File set	Required on CWS	Description
ssp.clients	Yes	All user authentication commands, ksh services, monitor command line interfaces, logging daemon, Resource Manager client library, and jm_status command.
ssp.basic	Yes	Code for installing and monitoring the SP, including • SP System Monitor • SDR • Centralized Management Interface (CMI—the SMIT panels) • Installation and Configuration Commands
ssp.sysman		SP Management Tools including • User Management Support • File Collections • Accounting Support • NTP
ssp.css	Yes, if switch	Device Drivers and Switch Support
ssp.jm		Resource manager for parallel application scheduling
ssp.public		Tar files for public domain code.
ssp.gui	Yes	SP System Monitor GUI and Perspectives. ssp.gui is required on the CWS for the System Monitor GUI and can optionally be installed on the node to use Perspectives.
ssp.docs		Man Pages and Online Information
ssp.sysctl	Yes	The Sysctl component
ssp.authent		Authentication Server
ssp.top	Yes, if switch	The system partitioning configuration directory and files including the System Partitioning Aid.
ssp.top.gui		Graphical user interface
ssp.st		Low level application programming interface for loading, unloading, and querying the job switch resource table.
ssp.ha	Yes	Availability subsystems which includes hearbeat, group services, and event management. You must install ssp.ha to use the spdspmsg command.
ssp.perlpkg		Perl4 and Perl5
ssp.spmgr		SNMP Manager (required for extension node support)
ssp.pman		Problem Management
ssp.csd.vsd ssp.csd.cmi ssp.csd.hsd ssp.csd.systcl ssp.csd.gui		IBM Virtual Shared Disk. For more information, refer to the RS/6000 SP: Control Workstation and Software Environment Guide.
ssp.hacws		High Availibility Control Workstation Support
ssp.ptpegui		PTPE graphical user interface
ssp.topsvcs	Yes	Topology services.

File set	Required on CWS	Description
spimg		Contains a single file containing a mksysb image of a minimal AIX 4.2 system.

Notes:

1. **ssp.authent** contains the parts required on a system that are used by the authentication server.

   You must install **ssp.authent** if you are using the authentication server. If you are using MIT Kerberos Version 4 or AFS authentication services, **ssp.authent** is not required. You can install **ssp.authent** on any other RISC System/6000 workstation that is an authentication server. You cannot install **ssp.authent** if the system already has an MIT Kerberos Version 4 or AFS authentication implementation installed. If you want to use the SP authentication facilities, you must first remove the other authentication service.

2. **ssp.clients** contains authentication commands and authenticated client services for the SP system.

   You must install **ssp.clients** on the control workstation in all cases, even if you use AFS or the MIT Kerberos Version 4 authentication servers. **ssp.clients** needs to be installed on any other RISC System/6000 workstation that is an authentication server. It is required to perform system management tasks using System Monitor commands, AIX remote commands, or the sysctl remote command execution facility.

3. If you select any SP Management Tools from the **ssp.sysman** option, all tools on that option are automatically installed. See the Site Environment Worksheet in the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment*.

4. If you are planning to set up system partitions, you must install **ssp.top**.

5. **ssp.ha** will fail to install if perfagent is not installed.

6. ssp.spmgr contains an SNMP manager. If you already have an SNMP manager running on the control workstation, UDP port 162 usage by the SP manager included as part of this file set must change. You will need to update the **spmgrd-trap** entry in the **/etc/services** file on the control workstation to specify an unused port. Any new port configured on the control workstation also has to be configured on the SNMP agents supporting dependent nodes.

Installation without AIX Preinstalled

Because your system may not have AIX 4.2.1 preinstalled on the nodes, you should add an install image to your list of installation options. You can install **spimg**, (**bos.obj.ssp.42**) shipped with the PSSP package.

Or if you prefer, you can provide your own AIX image for installation on the nodes.

PSSP Installation Instructions

Login to the control workstation as root and follow one of the procedures described in the following table:

If using:	Do this:
SMIT	**TYPE** **smit install_latest** • The Install New Software Products at Latest Level window appears. **ENTER** **/spdata/sys1/install/pssplpp/<code_version>** for Input Device **PRESS** **Do** to display the default install parameters. **PRESS** **List** to show options. **SELECT** One or more program options, or select the header file (called **ssp** with **ALL** on the far right side) to do the full installation. **PRESS** **Do** to complete option selection and to begin installation. When the installation is complete, check the SMIT log file for the installation status. If errors occur, see the *IBM RISC System/6000 Problem Solving Guide*.

installp	You can use **installp** to install multiple filesets. For example, to install all of the filesets, enter:
	`installp -a -d /spdata/sys1/install/pssplpp/<code_version> -X ssp.*`
	Note - In AIX 4.2, **installp** automatically commits the packaging file set when you specify the **-a** option.
	To list all of the options for **ssp**, enter:
	`installp -l -d /spdata/sys1/install/pssplpp/<code_version>/pssp.installp`

Customizing the ssp.docs HTML Files

The **ssp.docs** fileset includes HTML files that contain online versions of the PSSP publications.

Making the HTML Files Accessible to Your Browser: Once you have installed the **ssp.docs** fileset, the PSSP HTML files will be located at **/usr/lpp/ssp/html**. However, depending on how your online browser's **httpd** is set up, your browser may or may not be able to access HTML files at this location. Therefore, you may need to copy the PSSP HTML files to another location or make symbolic links to them to enable the browser to access them.

Note: You must ensure that the PSSP HTML files are in a directory or location defined to your browser's **httpd** as one where HTML files may reside and will be accessible to the browser.

Making the HTML Files Accessible to Users: After you have determined where the PSSP HTML files should reside and have placed them there, you will need to direct users to the correct location for each online book. A sample index file, **/usr/lpp/ssp/html/psspbooks.html**, has been provided as a way of helping you do this.

This sample HTML file shows how you can set up a single launching point from which users can access all of the online books. You can modify this file or incorporate it into another HTML file, as needed, to point to the actual location where each book resides.

Step 19: Initialize RS/6000 SP Authentication Services

Prior to performing this step, you must have decided what type of authentication server to use: RS/6000 SP, AFS, or another MIT Kerberos Version 4 implementation. In preparation, you should have completed the checklist in the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide.* See that book for more information.

RS/6000 SP authentication provides a program, **/usr/lpp/ssp/bin/setup_authent**, to initialize RS/6000 SP authentication services on RISC System/6000 workstations (including the control workstation) for authentication servers and authentication client systems. This program defines instances of the **hardmon** and **rcmd** authenticated services, and does one of the following:

1. Creates a primary authentication server and database, or
2. Creates a secondary authentication server and database, after the primary server has been initialized, or
3. Initializes the control workstation or other RISC System/6000 workstation to use AFS authentication, or
4. Creates an authentication client system

The procedure for completing this step varies, depending on the authentication configuration you select. Each configuration includes an example where the **setup_authent** command is invoked. Review the examples. Substitute the principal names and passwords on your system for the *DescriptiveTerms* shown in the examples, and use them to initialize the authentication services on your system.

If initializing as:	**Refer to:**
Primary Authentication Server	"Step 19.1: Initializing as the Primary Authentication Server" on page 32
Secondary Authentication Server	"Step 19.2: Initializing as a Secondary Authentication Server" on page 34
Authentication Client System	"Step 19.3: Initializing as an Authentication Client System" on page 36
Use AFS Authentication	"Step 19.4: Initializing to use AFS Authentication" on page 37
Select only one authentication step to follow. Do not perform the steps for the authentication server you did not choose.	

Note the following:

- <screenclear> shows where **setup_authent** clears the screen before displaying an explanation of the next part of the initialization procedure.
- *root* refers to the administration ID. It can be **root** or any name you choose. It must be a user in the system.

  The Kerberos administrator should be separate from the root user, and be used for installing and monitoring the PSSP spmon and authentication files. Some AIX commands require the root (uid 0) privilege in order to run, but the administrator can lock out and reassign root-based privileges as necessary.

Step 19.1: Initializing as the Primary Authentication Server

Follow this procedure to initialize your primary authentication server on the RS/6000 SP control workstation or another RISC System/6000 workstation:

1. Create a **/etc/krb.conf** file, unless you want **setup_authent** to create a default configuration file with one authentication server for the default local realm name.
2. Create a **/etc/krb.realms** file, if you need to map any domains to the local realm name.
3. Run the **/usr/lpp/ssp/bin/setup_authent** program.
4. Issue the **/usr/lpp/ssp/kerberos/bin/klist** command to make sure a ticket exists for the account.

The following example shows the interaction you can expect when you run **setup_authent** when initializing the primary authentication server.

```
#
setup_authent
<screenclear>
********************************************************************
Creating the Kerberos Database

Invoking the kdb_init and kstash utilities to create the database.

You must decide on a master password for the database. You will be
prompted to enter it twice.  Save this password in a very secure
place, since it is used to encrypt all keys in the database and you
will need it for other administrative tasks.

After you complete this task, the Kerberos daemons will be started:
Kerberos for ticket-granting services, kadmind for administration.

For more information see the kdb_init and kstash man pages.
********************************************************************
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.

Enter Kerberos master key:  YourDatabasePassword

Enter Kerberos master key:  YourDatabasePassword

0513-004 The Subsystem or Group, Kerberos, is currenctly inoperative
0513-083 Subsystem has been Deleted
0513-071 The Kerberos Subsystem has been added
0513-059 The Kerberos Subsystem has been started.  Subsystem PID is 18394
<screenclear>
********************************************************************
Defining an Administrative Principal to Kerberos

The kdb_edit utility is used to define the initial Kerberos users.
You must define a user whose UID is 0 as a Kerberos database
administrator. This user will have to login to Kerberos with this name
prior to performing installation tasks that result in execution of the
setup_server command, during installation or whenever network
interfaces have been added or renamed in the SP system configuration.

kdb_edit prompts you separately for the name and the instance. First
enter the user name, specifying the login name of the user who will be
the primary Kerberos administrator for the local realm. When you are
prompted for the instance, you must enter admin.  You must assign a
Kerberos password for this user and enter it twice (you may use the
AIX login password). To take default values on other options, hit
<Enter>.

You may create any number of other Kerberos principals at this time.
To exit kdb_edit, hit <Enter> when prompted for another
principal name.
```

```
For more information see the kdb_edit man page.

Opening database...
Previous of default values are in [brackets],
enter return to leave the same, or new value.
Principal name:
  root
 Instance: admin <Not found>, Create [y]?
 <Enter> Principal: root, Instance: admin, kdc_key_ver&c
  New Password: rootPassword
Verifying, please re-enter New Password :
 rootPassword
 Principal's new key version = 1 Expiration date (enteryyyy-mm-d
 <Enter> Max ticket lifetime (*5 minutes) [ 255 ] ?
 <Enter> Attributes [ 0 ] ?
 <Enter> Edit O.K. Principal name:
 <Enter> <screenclear>
 ********************************************************************
Logging into Kerberos as an admin user
You must assume the role of a Kerberos administrator <user> admin
to complete the initialization of Kerberos on the local system.  The
kinit command is invoked and will prompt you for the password.  If you
are setting up your primary server here, you just defined it.  If you
have defined multiple administrative principals, or if your primary
authentication principal is on another system, you must first enter the
name of an administrative principal who has root privilege (UID 0).
You need to be authenticated as this administrator so that this program
can create the principals and service key files for the authenticated
services that run on the SP system.  For more information, see the
kinit man page.
Kerberos Initialization for "root.admin"
Password: rootPassword
Expires
Principal Nov 11 16:26:11 Dec 12 16:26:11
krbtgt.XYZ.ABC.COM@XYZ.ABC.COM # #
<end_of_example>
```

Step 19.2: Initializing as a Secondary Authentication Server

- To do this step, the primary authentication server must already be initialized.
- Ensure clock synchronization between the primary and secondary authentication servers.

Follow this procedure to initialize a secondary authentication server on the control workstation or another RISC System/6000 workstation.

1. Copy the **/etc/krb.conf** file from the primary authentication server to this secondary server system.
2. Add a line to the **/etc/krb.conf** file, listing this system (by its full host name) as a secondary server for the local authentication realm.

   For example, to add **sp2cw.xyz.com** as a secondary server for the authentication realm **XYZ.COM**, add this line to **/etc/krb.conf**:

   ```
   XYZ.COM sp2cw.xyz.com
   ```
3. Copy the **/etc/krb.realms** file from the primary server to this secondary server system.

4. Run the **setup_authent** program.

   setup_authent requires you to login to the authentication service using the same administrative principal name that was defined for the primary server. The remainder of the initialization of authentication services on this secondary local system takes place automatically.

5. After **setup_authent** completes, add an entry for the new server to the **/etc/krb.conf** file on all SP systems on which you have already initialized authentication.

6. On the primary server, if this is the first secondary server, you should create a root **crontab** entry that invokes the script **/usr/kerberos/etc/push-kprop** to periodically propagate database changes.

7. Issue the **/usr/lpp/ssp/kerberos/bin/klist** command to make sure a ticket exists for the account.

The following example shows the interaction you can expect when you run **setup_authent** when initializing as a secondary authentication server:

```
#setup_authent
<screenclear>
********************************************************************
Logging into Kerberos as an admin user

You must assume the role of a Kerberos administrator <user>.admin
to complete the initialization of Kerberos on the local system.
The kinit command is invoked and will prompt you for the password.
If you are setting up your primary server here, you just defined it.
If your primary server is on another system, you must first enter
the user name of an administrative principal defined on that server.

You need to be authenticated as an administrator so that this
program can create the service principals required by the
authenticated services that are included in the ssp package.

hardmon - for the System Monitor facilities
rcmd    - for sysctl and Kerberos-authenticated rsh and rcp

For more information, see the kinit man page.
********************************************************************
setup_authent: Enter name of admin user: root
 Kerberos Initialization for "root.admin"
Password: rootPassword
backup.abc.com: success.backup.abc.com:  Succeeded
#
```

The last two messages shown in the previous example are issued by the programs that transfer the database from primary to secondary servers, to indicate that the backup database has been installed.

```
# klist
Ticket file:    /tmp/tkt0
Principal:  root.admin@XYZ.ABC.COM

Issued           Expires          Principal
Nov 11 16:26:11  Dec 12 16:26:11  krbtgt.XYZ.ABC.COM@XYZ
#
<end_of_example>
```

Step 19.3: Initializing as an Authentication Client System

To do this step, the primary authentication server must already be initialized.

Follow this procedure to initialize the control workstation or another RISC System/6000 workstation as an authentication client system.

1. Copy the /**etc**/**krb.conf** file from the primary authentication server to this system.
2. Copy the /**etc**/**krb.realms** file from the primary server.

   If the new workstation is outside the realm of the primary server, you must add this new workstation to the /**etc**/**krb.realms** file on the primary server before you copy the /**etc**/**krb.realms** file from the primary server to the new workstation. Otherwise, the next step will fail.
3. Run the **setup_authent** program.

   setup_authent requires you to login to the authentication service using the same administrative principal name that was defined when the primary server was set up. The remainder of the initialization of authentication services on the local system takes place automatically.
4. The root **.klogin** file on a client workstation contains just the administrative principal name you used to install authentication. You may want to edit the **.klogin** file to add other principals in your configuration.
5. Issue the /**usr**/**lpp**/**ssp**/**kerberos**/**bin**/**klist** command to make sure a ticket exists for the account.

The following example shows the interaction you can expect when you run **setup_authent** when initializing as an authentication client system. The initial warning message shown in the example is issued if you have installed the **ssp.authent** option on a system configured as a client rather than a server.

```
#setup_authent
setup_authent: This system is not listed as a Kerberos server in /etc/krb.
Continuing setup as a Kerberos client system only.
<screenclear>
********************************************************************
Logging into Kerberos as an admin user

You must assume the role of a Kerberos administrator <user>.admin
to complete the initialization of Kerberos on the local system.
The kinit command is invoked and will prompt you for the password.
If you are setting up your primary server here, you just defined it.
If your primary server is on another system, you must first enter
the user name of an administrative principal defined on that server.

You need to be authenticated as an administrator so that this
program can create the service principals required by the
authenticated services that are included in the ssp package.

hardmon - for the System Monitor facilities
rcmd    - for sysctl and Kerberos-authenticated rsh and rcp

For more information, see the kinit man page.
********************************************************************

setup_authent: Enter name of admin user: root
Kerberos Initialization for "root.admin"

Password: rootPassword
# klist
Ticket file:    /tmp/tkt0
Principal:  root.admin@XYZ.ABC.COM

Issued           Expires          Principal
Nov 11 16:26:11  Dec 12 16:26:11  krbtgt.XYZ.ABC.COM@XYZ
#
 # <end_of_example>
```

Step 19.4: Initializing to use AFS Authentication

To do this step, the AFS primary authentication server must already be initialized.

Follow this procedure to initialize using AFS authentication servers.

1. If the AFS configuration files (**ThisCell, CellServDb**) are not in /**usr**/**vice**/**etc**, you must create a symbolic link from /**usr**/**vice**/**etc** to the directory containing those files:
2. If the **kas** command is not installed in /**usr**/**afsws**/**etc**, create a symbolic link from /**usr**/**afsws**/**etc** to the directory containing the **kas** command.
3. If you are using AFS Version 3.4, you must reconcile the conflicting port assignments used by the kaserver and RISC/6000 SP authentication commands, as described in the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* and the *Administration Guide*.
4. Run the **setup_authent** program.

setup_authent requires you to enter the name and password of the AFS administrator.

5. Issue the /**usr**/**afsws**/**bin**/**tokens.krb** command to make sure a ticket exists for the account. The **klist** command does not work at this point in the process yet. You need to issue the AFS **tokens.krb** command to make sure that a ticket exists for the administrator account being used.

The following example shows the interaction you can expect when you run **setup_authent** when initializing to use AFS authentication. The message always appears when the workstation has AFS installed, either as a client or server:

```
#setup_authent
<screenclear>
************************************************************************
Option to Use AFS

Because this system is configured for use of AFS, you may choose to
use the AFS authentication servers instead of installing RS/6000 SP
authentication servers or using other Kerberos Version 4 servers.

The choice of AFS indicates that you will be using AFS authentication
servers exclusively in your RS/6000 SP system's local realm.

Do you want to set up authentication services to use AFS servers?
************************************************************************

Enter y or n: y


afs_add_principal: Enter afs admin principal name [login-name] user-name
Password: UserNamePassword

# klist
Ticket file:    /tmp/tkt0
Principal:  root.admin@XYZ.ABC.COM

Issued           Expires          Principal
Nov 11 16:26:11  Dec 12 16:26:11  krbtgt.XYZ.ABC.COM@XYZ
#
 # <end_of_example>
```

Note: Once you have set up your authentication environment using **setup_authent**, you may use the PSSP authenticated remote commands between the other workstations on which you have performed this step. To do so, you will need to obtain a Kerberos ticket using the **kinit** command. However, if you have chosen AFS as your authentication method, and have not yet completed Step 21, **kinit** will fail. The proper way to get authenticated at this point is to use the **klog.krb** command. This is described in the *Administration Guide*, Chapter 3, "Using SP Credentials". With AFS authentication, **kinit** will work properly after completing step 21.

Step 20: Complete System Support Installation on the Control Workstation

This step does the following:

- Configures the control workstation
- Installs PSSP SMIT Panels
- Starts SP daemons
- Configures the SDR
- Updates /**etc**/**inittab** and /**etc**/**services**
- Sets **node_number** for the control workstation to 0 in the Object Data Management (ODM) databases
- Creates the **hardmon hmacls** file with the administrator's ACL
- Configures the system as one system partition. There is one system partition corresponding to the name of the control workstation in the SP object. It's called the **default** or **persistent** system partition because it always exists.

Using install_cw

To finish installing PSSP on the control workstation, enter the following command:

```
install_cw
```

Note: At this point, you can bring up the Perspectives GUI for use in the rest of the installation. The launch panel will let you bring up SMIT menus, issue commands, and launch the **sphardware** perspective for monitoring and controlling nodes. See Appendix A, “SP Perspectives and System Monitor GUI Tasks” on page 225 for more information on using Perspectives. If you do not wish Perspectives for the install steps, you can to use SMIT, the spmon GUI, and the command line.

To bring up the Perspectives Launch Pad, make sure your DISPLAY environment variable is set correctly and enter the following command:

```
perspectives &
```

You may receive the following message which you can ignore:

```
Warning: locale not supported by C library, locale unchanged.
```

Step 21: Run SDR and System Monitor Verification Tests

If using:	Do this:
Perspectives	**SELECT** **smit SP_verify** from Launch Pad • The RS/6000 SP Installation/Configuration Verification Menu appears. From this point, you can follow the rest of the SMIT steps described in the next row of this table.
SMIT	**TYPE** **smit SP_verify** • The RS/6000 SP Installation/Configuration Verification Menu appears. **SELECT** System Data Repository **PRESS** **Do** to run the tests **SELECT** System Monitor Installation **PRESS** **Do** to run the tests

SDR_test
spmon_itest
	Enter:
	`SDR_test`
	`spmon_itest`

After the tests are run, the system creates logs in **/var/adm/SPlogs** called **spmon_itest.log** and **SDR_test.log**.

See the *Commands and Technical Reference* for more information about what these tests do.

Task C. Enter Site Environment, Frame, Node, and Switch Information

This section describes the steps you take to enter the information defining the SP configuration. After you prepare the control workstation and install the PSSP software, you are ready to enter the data to define your SP configuration.

Step 22: Enter Site Environment Information

If you changed the lppsource <name> to something other than the default (you would have changed the name in “Step 14: Create Required /spdata Directories” on page 23), you must perform this step.

If you do not want to change any of the default site environment variables, skip this step.

Use Perspectives, SMIT or the **spsitenv** command to enter information about your site environment. Use the worksheet in the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* to enter site environment values.

The site environment data is written to the SDR. Before you run any of the installation scripts, you must enter the following data on the control workstation. Refer to the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* for additional explanation.

Site environment data includes:

- The name of the default network install image
- Your method of time service, the name of your time servers, and the version of NTP in use
- Whether you want to have the SP services configure and manage the Automounter.
- User Admin information
- How you want to use RS/6000 SP User Management
- Whether you want RS/6000 SP File Collection Management installed and where the daemon will run
- Whether you want to use RS/6000 SP Accounting
- Whether you use the default lppsource directory as the location of the AIX file sets. If you changed the lppsource name from the default, you also need to change it in the Site Environment Data label.

You can enter the site environment information using SMIT or the **spsitenv** command. Whichever method you chose, keep in mind that you can easily change these options at any time after installation is complete.

If you prefer to issue commands directly, refer to the *Commands and Technical Reference* for **spsitenv** syntax and parameter information.

If using:	Do this:
Perspectives	**SELECT** **smit config_data** from the Launch Pad • The SP Configuration Database Management menu appears. **SELECT** Enter Database Information • The Enter Database Information menu appears. From this point, you can follow the rest of the SMIT steps described in the next row of this table.
SMIT	**TYPE** **smit enter_data** • The Enter Database Information menu appears. **SELECT** Site Environment Information • The Site Environment Information window appears. **TYPE** Your environment choices. Refer to the Site Environment Worksheet. **PRESS** **Do** to complete operation • If you do not make any changes to the information already in the window, SP displays a usage information message. This is normal—continue on.

spsitenv	This example configures NTP service as consensus and specifies that file collection be installed.
	`spsitenv ntp_config=consensus filecoll_config=true`
	This example specifies that the control workstation lppsource directory be **/spdata/sys1/install/aix42/lppsource** for you installation configuration.
	`spsitenv cw_lppsource_name=aix42`

Step 23: Enter Frame Information and Reinitialize the SDR

This step creates frame objects in the SDR for each frame in your system. At the end of this step, the SDR is reinitialized, resulting in the creation of node objects for each node attached to your frames.

You can enter information about your frames using Perspectives, SMIT, or the **spframe** command. You must be an authenticated administrative user to issue this command. You can issue the **klist** command to validate the authenticated ticket-granting-ticket (tgt). If not authenticated, issue **kinit** to obtain authentication.

If frames are not contiguously numbered, repeat this step for each series of contiguous frames. To save time, do not specify reinitialization of SDR until you are entering the final series of contiguous frames.

If using:	Do this:
Perspectives	**SELECT** **smit config_data from the Launch Pad** • The SP Configuration Database menu appears. **SELECT** Enter Database Information • The Enter Database Information menu appears. From this point, you can follow the rest of the SMIT steps described in the next row of this table.
SMIT	**TYPE** **smit enter_data** • The Enter Database Information menu appears. **SELECT** Frame Information • The Frame Information window appears. **TYPE** The number of frames in the Frame Count field. (Start Frame defaults to **1**.) The starting frame tty port defaults to dev/tty0. You may need to change this depending upon your configuration. **SELECT** **yes** or **no** next to `Re-initialize the System Data Repository`, as follows: **no** if you have more (noncontiguous) frame entries to make in this panel. **yes** if you are entering only one series of contiguous frames, or entering the last series of noncontiguous frames. **PRESS** **Do** to enter frame data to the SDR.
spframe	Specify **spframe** command with **-r yes** to reinitialize the SDR (when running the command for final series of frames), a starting frame number, a frame count, and the starting frame's tty port. The following example enters information for four frames (frame 1 to frame 4) and indicates that frame 1 is connected to /**dev**/**tty0**, frame 2 to /**dev**/**tty1**, and so on, and reinitializes the SDR. `spframe -r yes 1 4 /dev/tty0`

Step 24: Verify System Monitor Installation

Perform this step to verify that the System Monitor and Perspectives have been correctly installed.

If using:	Do this:
Perspectives	**SELECT** **smit SP_verify** from the Launch Pad • The Installation/Configuration Verification Menu appears. From this point, you can follow the rest of the SMIT steps described in this table.
SMIT	**TYPE** **smit SP_verify** • The Installation/Configuration Verification Menu appears. **SELECT** System Monitor Configuration
spmon	Enter: `spmon_ctest`

After the tests are run, the system creates a log in **/var/adm/SPlogs** called **spmon_ctest.log**.

See the section on diagnosing RS/6000 SP problems in the *Diagnosis and Messages Guide* if the verification test fails.

Step 25: Verify Frame Information

All frames must be powered up and connected to the control workstation so that the nodes are automatically detected and added to the SDR.

If using:	Do this:
Perspectives	**SELECT** the Manage/Control Hardware icon by double clicking • The Hardware Perspectives appears with the Nodes Pane showing by default. The number of frames and assignment of nodes within the frames should match your configuration. If you had the Hardware Perspective up before you added the frame information, you should delete and re-add the Nodes pane.
System Monitor GUI	From the System Monitor pop-up window: **SELECT** SP **SELECT** All Node Summary Display • The selection screen for node variables appears. **SELECT** 3DigitDisplay from the list of variables **PRESS** Display all-node summary • The 3-Digit Display Summary appears.
spmon	Enter: `spmon -d`

You should see the frames represented with thin, wide, or 604 high nodes, depending on your configuration. If your frames are not correctly represented, you may have a hardware problem, such as a misplugged RS-232 cable. See the chapter on diagnosing RS/6000 SP problems in the *Diagnosis and Messages Guide* for help in correcting the error. If an error occurred, the frame must be deleted, using the **spdelfame** command, prior to reissuing the **spframe** command. After updating the RS-232 connection to the frame, you should reissue the **spframe** command.

Step 26: Update the State of the Supervisor Microcode

This step is required if any of the following conditions are true:

- You performed “Step 20: Complete System Support Installation on the Control Workstation” on page 39. As a result, on the control workstation, you may have installed supervisor microcode files that are at a later level than those installed on the supervisor cards.
- You have added or replaced a frame, node, or switch as defined in the Reconfiguration chapter in this book. As a result, you may have installed supervisor hardware that is at a previous microcode level than that of the supervisor microcode files installed on the control workstation.

- You are installing program updates as defined in the Reconfiguration chapter in this book and you have just performed "D: Commit PTF's on Node and Control Workstation" of the "Applying PTF's to the SP System" section. As a result, you may have installed on the control workstation, supervisor microcode files that are at a later level than those installed on the supervisor cards.

If using:	Do this:
Perspectives	**SELECT** **smit supervisor** from the Launch Pad. • The RS/6000 SP Supervisor Manager menu appears. From this point, you can follow the rest of the SMIT steps described in the next row of this table.
SMIT	**TYPE** **smit supervisor** • The RS/6000 SP Supervisor Manager menu appears. The first five selections on the menu allow you to query the state of the microcode on the supervisor cards. Once you have determined whether a supervisor requires an action, based on the displayed state, continue with these steps. The following SMIT options interface with hardware supervisors that support supervisor microcode download and provide the ability to: • Check for supervisors that require action. • List the status of supervisors. • Update the supervisors to the most current available code level. Supervisor hardware that currently supports microcode download include: • Dual-ported Frame Supervisor card • 604 high node Supervisor card • SP Switch Enter the SMIT fastpath command **smit supervisor** and use the Help Key (F1) for more information. To update all of the supervisors, SELECT Update "All" Supervisors That Require Action. To update a subset of supervisors, SELECT Update Selectable Supervisors That Require Action.
spsvrmgr	Issue the **spsvrmgr** command. Refer to the *Commands and Technical Reference* for more information.

Step 27: Enter Required Node Information

- Verify that the node objects have been created by issuing **splstdata -n** and verify that there is an entry for each node in your system.
- Be sure to have your node configuration worksheet on hand with all the node information completed before attempting to perform this step. The *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* explains how to fill out your worksheet.
- If multiple IP interfaces map to the same host name on the starting node, you must enter the Ethernet IP address for the starting node. Do not enter its host name.

This step adds IP address-related information to the node objects in the SDR. It also creates adapter objects in the SDR for the en0 adapters on your nodes. This information is used during node customization and configuration.

Enter information about your nodes attached to each Ethernet adapter using Perspectives, SMIT, or the **spethernt** command.

If using:	Do this:
Perspectives	**SELECT** **smit config_data** from the Launch Pad. • The SP Configuration Database Management menu appears. **SELECT** Enter Datbase Information • The Enter Database Information menu appears: From this point, you can follow the rest of the SMIT steps described in the next row of this table.
SMIT	**TYPE** **smit node_data** • The Node Database Information Menu appears. **SELECT** SP Ethernet Information • The SP Ethernet window appears: If you have wide nodes which occupy two node slots each in your system, entering **yes** next to `Skip IP Address for Unused Slots?` can be useful in assigning IP addresses that correspond to the slots in the frame, with each wide node address incrementing by 2, each thin node address incrementing by 1, and each 604 high node node incrementing by 4. You can avoid skipping IP addresses for the empty slots by entering **no** next to `Skip IP Address for Unused Slots?` In this way IP addresses are assigned consecutively for both thin and wide nodes. The distribution of your IP addresses determines how many times you perform this step. You may have to do it more than once if: • There are gaps in your IP addresses that are not caused by wide or 604 high nodes • You want to set up alternate default routes or netmasks for certain IP address ranges Enter the following information for each consecutive block of nodes. 1. Start Frame, Start Slot, and Node Count **OR** Node Group (See the Administration Guide for more information on Node Groups) **OR** Node List 2. Starting Node's en0 Host name or IP Address 3. Netmask 4. Default Route IP Address or Host name 5. Skip IP Addresses for Unused Slots? If you specify nodes with a node list, you cannot specify **yes** for `Skip IP Addresses for Unused Slots?` **TYPE** Data in the fields as required. Refer to your worksheet. **PRESS** **Do** to store the data.

<table>
<tr><th>If using:</th><th>Do this:</th></tr>
<tr><td colspan="2">Starting Slot is always relative to the frame and not to the system. This means that the first slot in the second, third, and fourth frames is still slot 1 rather than slots 17, 33, and 49. For example, for the first frame you might enter:

Start Frame 1
Start Slot 1

and for a second frame, you might enter:

Start Frame 2
Start Slot 1

Node List is used to specify a group of node numbers separated by commas. Node numbers can be referenced for systems with more than one frame. (Node number 17 would be used for frame 2 slot 1.) For example:

1,5,7,9,15,17,19

You can also specify a file that contains a single line of data containing the node list, separated by commas. Enter the full-path name, unless the file is in your current directory. For example, if you have a list of nodes in /tmp/node_list, enter the following in the Node List field:

/tmp/node_list</td></tr>
<tr><td>spethernt</td><td>This example configures an en0 network of 16 nodes with IP addresses ranging from 129.33.32.1 to 129.33.32.16, a netmask of 255.255.255.192, and a default route of 129.33.32.200.

spethernt -s no 1 1 16 129.33.32.1 255.255.255.192 129.33.32.200

If you are using twisted-pair Ethernet instead of the default BNC adapter, you need to use the -t tp option with the spethernt command. This example configures an en0 network of 16 nodes with IP addresses ranging from 129.33.32.1 to 129.33.32.16, a netmask of 255.255.255.192, and a default route of 129.33.32.200, using twisted-pair Ethernet.

spethernt -t tp -s no 1 1 16 129.33.32.1 255.255.255.192 129.33.32.200</td></tr>
</table>

If you are adding an extension node to your system, you may want to enter required node information now. For more information, refer to “Install Extension Nodes” on page 82.

Step 28: Acquire Hardware Ethernet Addresses

- Do not do this step on a production running system because it shuts down the nodes.
- If you are adding a node, select only the new node. All the nodes you select are powered off and back on.
- The nodes for which you are obtaining Ethernet addresses must be physically powered on when you perform this step. No ttys can be open in write mode.

This step gets hardware Ethernet addresses for the en0 adapters for your nodes, either from a file or from the nodes themselves, and puts them into the Node Objects in the SDR. That information is used to set up the /**etc**/**bootptab** files for your boot/install servers.

If you know the hardware Ethernet addresses, you can speed this process by putting the addresses in the /**etc**/**bootptab.info** file as follows:

- Create a file named /**etc**/**bootptab.info** (if it does not already exist), listing your RS/6000 SP nodes by node number, followed by a blank and the hardware

Ethernet address. For example, a file containing addresses for a frame might look like this:

- 1 02608C2E48D9
- 3 02608C2D6712
- 5 02608C2E49A4
- 7 02608C2E465D
- 9 02608C2E28AC
- 10 02608C2E6822
- 11 02608C2E688A
- 12 02608C2E424E
- 13 02608C2E1824
- 14 02608C2E440A
- 15 02608C2E602D
- 16 02608C2E3128

The **/etc/bootptab.info** file is not required. If you do not know your hardware Ethernet addresses, and the **/etc/bootptab.info** file does not exist, use **sphrdwrad** to access the SP node and retrieve the hardware Ethernet address for you. (This makes **sphrdwrad** take longer to run.)

If using:	Do this:
Perspectives	**SELECT** **smit config_data** from the Launch Pad. • The SP Configuration Database Management menu appears. **SELECT** Enter Database Information • The Enter Database Information menu appears. **SELECT** Node Database Information • The Node Database Information menu appears. **SELECT** Get Hardware Ethernet Addresses From this point, you can follow the rest of the SMIT steps described in the next row of this table.
SMIT	**TYPE** **smit node_data** • The Node Database Information menu appears. **SELECT** Get Hardware Ethernet Addresses • The Get Hardware Ethernet Addresses window appears. **TYPE** The starting frame, slot, and node count (the number of nodes for each consecutive series of nodes), and node group. **or** The node list. Type the node numbers (separated by commas) or the file containing the list (for example, /**tmp**/**node_list**) **PRESS** **Do** to get the data.

sphrdwrad	This example gets all hardware Ethernet addresses for a RS/6000 SP system.
	`sphrdwrad 1 1 rest`
	This example gets all hardware Ethernet addresses for the nodes specified in the node list (the **-l** flag):
	`sphrdwrad -l 10,12,17`

If this step fails, look for the node conditioning instructions in the *Diagnosis and Messages Guide*.

Step 29: Verify Ethernet Addresses Were Acquired

This step verifies that Ethernet addresses were placed in the SDR node object.

If using:	Do this:
Perspectives	**SELECT** **smit config_data** from the Launch Pad • The SP Configuration Database Management menu appears. **SELECT** List Database Information • The List Database Information menu appears. From this point, you can follow the rest of the SMIT steps described in the next row of this table.
SMIT	**TYPE** **smit list_data** • The List Database Information menu appears. **SELECT** List Node Database Information • The List Node Database Information menu appears. **SELECT** List Node Configuration Information • A window appears listing the node ethernet information. **TYPE** The Start Frame, Start Slot, and Node Count *or* Node List **PRESS** **Do**.
splstdata	**Attention:** If your system is large, **splstdata** returns great quantities of data. You may want to pipe the command output through a filter to reduce the amount of data you see. To display SDR boot/install data, enter: `splstdata -a`

Step 30: Configure Additional Adapters for Nodes

Perform this step if you have a switch or if you require any additional adapters.

Be sure to have your switch configuration worksheet on hand with all the switch information completed before attempting to perform this step. The *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* explains how to fill out your worksheet.

This step creates adapter objects in the SDR for each node. The data in the adapter objects is used during the customization or installation steps to configure the adapters on the nodes. You can configure the following adapters with this procedure:

- en1
- fi0
- fi1
- tr0
- tr1
- css0 (applies to both the High Performance Switch and the SP Switch)

To configure adapters such as ESCON and PCA, you must configure the adapter manually on each node, using **dsh**, or modify the **script.cust** file.

Configuring the Switches

To configure your switch adapters for use with the RS/6000 SP System, use SMIT or issue the **spadaptrs** command. The *IBM RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* contains additional information on IP addressing for the switch.

If using:	Do this:
Perspectives	**SELECT** **smit config_data** from the Launch Pad. • The SP Configuration Database Management menu appears. **SELECT** Enter Datbase Information • The Node Database Information menu appears. From this point, you can follow the rest of the SMIT steps described below.
SMIT	**TYPE** **smit node_data** • The Node Database Information menu appears **SELECT** Additional Adapter Information • The Additional Adapter Information window appears. **TYPE** The data in the fields. Refer to your worksheet as needed. **PRESS** **Do** to store the data. **PRESS** **Cancel** to exit SMIT. The default **css0** adapter attributes are: • `Skip IP Addresses for Unused Slots? no` • `Enable ARP for the css0 Adapter? no` • `Use Switch Node Numbers for css0 IP Addresses? yes` If you want to select **yes** next to `Skip IP Addresses for Unused Slots?`, you must set the `Use Switch Node Numbers` to **no**. If you set `Enable ARP` to **yes**, you must set the `Use Switch Node Numbers` to **no**. For **css0** adapters, you must use the `Start Frame`, `Start Slot`, and `Node Count` fields. `Start Slot` must be set to **1**. Enter the following information for each consecutive block of nodes. 1. Start Frame, Start Slot, and Node Count **OR** Node Group **OR** Node List 2. Adapter Name 3. Starting Node's IP Address or Host name 4. Netmask 5. Token Ring Data Rate (required only when configuring a token-ring adapter.) 6. Skip IP Addresses for Unused Slots? 7. Enable ARP for the css0 Adapter? 8. Use Switch Node Numbers for css0 IP Addresses?

If using:	Do this:

Starting Slot is always relative to the frame and not to the system. This means that the first slot in the second, third, and fourth frames is still slot 1 rather than slots 17, 33, and 49. For example, for the first frame you might enter:
`Start Frame 1`
`Start Slot 1`
and for a second frame, you might enter:
`Start Frame 2`
`Start Slot 1`
Node List is used to specify a group of node numbers separated by commas. Node numbers can be referenced for systems with more than one frame. (Node number 17 would be used for frame 2 slot 1.) For example:
1,5,7,9,15,17,19
You can also specify a file that contains a single line of data containing the node list, separated by commas. Enter the full-path name, unless the file is in your current directory. For example, if you have a list of nodes in /**tmp/node_list**, enter the following in the **Node List** field:
/tmp/node_list	

spadaptrs	This example adds SDR information for a **css0** (High Performance Switch) network of 30 nodes (frame 1 slot 1 to frame 2 slot 16, with a wide node as the first node in each frame and the rest thin nodes, and a switch on each frame) with IP addresses from 129.33.34.1 to 129.33.34.30, and a net mask of 255.255.255.0. The IP addressing corresponds to the slots in the frame, with each wide node incrementing by 2 and each thin node incrementing by 1, and each 604 high node by 4. If you specify the **-s** flag to skip IP addresses when you are setting the **css0** switch addresses, you must also specify **-n no** to not use switch numbers for IP address assignment, and **-a yes** to use ARP. `spadaptrs -s yes -n no -a yes 1 1 30 css0 129.33.34.1 255.255.255.0`

Configuring Other Additional Adapters

To configure other additional adapters, for example Ethernet (en1), token ring (tr0), or FDDI (fi0), you must select the `Additional Adapter Database Information`. For these adapters you can select either the Start Frame, Start Slot, and Node Count fields, or the Node List field.

Notes:

1. When using the token ring (tr0) adapter, you must select the token ring rate (4 MB or 16 MB).
2. For best results, exit and get back into this panel for each different type of adapter. This clears any extraneous values left behind in the panel.

The distribution of your IP addresses determines how many times you perform this step. You may have to do it more than once if:

- There are gaps in your IP addresses not caused by wide nodes or 604 high nodes.
- You want to set up alternate default routes or netmasks for certain IP address ranges

If using:	Do this:
Perspectives	**SELECT** **smit config_data** from the Launch Pad. • The SP Configuration Database Management menu appears. **SELECT** Enter Datbase Information • The Node Database Information menu appears. From this point, you can follow the rest of the SMIT steps described below.
SMIT	**TYPE** **smit node_data** • The Node Database Information menu appears. **SELECT** Additional Adapter Information • The Additional Adapter Information window appears. **TYPE** The data in the fields. Refer to your worksheet as needed. **PRESS** **Do** to store the data. **PRESS** **Cancel** to exit SMIT. `Start Slot` must be set to **1**. Enter the following information for each consecutive block of nodes. 1. Start Frame, Start Slot, and Node Count **OR** Node List 2. Adapter Name 3. Starting Node's IP Address or Host name 4. Netmask 5. Token Ring Data Rate (required only when configuring a token-ring adapter.)

spadaptrs	This example adds SDR information for an fi0 (FDDI adapter) network of 30 nodes (frame 1 slot 1 to frame 2 slot 16, with a wide node as the first node in each frame and the rest thin nodes) with IP addresses from 129.33.34.1 to 129.33.34.30, and a net mask of 255.255.255.0. The IP addressing corresponds to the slots in the frame, with each wide node incrementing by 2 and each thin node incrementing by 1.
	`spadaptrs -s yes 1 1 30 fi0 129.33.34.1 255.255.255.0`
	This example adds SDR information for a tr0 (token ring adapter) for node 1 with IP address 129.33.35.1 and a net mask of 255.255.255.0, and references the node list field.
	`spadaptrs -l 1 -r 16 tr0 129.33.35.1 255.255.255.0`

Step 31: Configure Initial Host Names for Nodes

Do this step if:

- You do not want the default host name to match the en0 adapter name. The en0 name is the default.
- You are using short host names. The default is long host names.

This step changes the default hostname information in the SDR Node Objects used during customization to set up the host name on each node, and allows you to indicate how you want to name your RS/6000 SP nodes. The default is the long form of the en0 host name, which is how the **spethernt** command processes defaulted host names.

You can indicate an adapter name other than en0 for the node host names to be used, as well as whether the long or short form should be used.

If using:	Do this:
Perspectives	**SELECT** **smit config_data** from the Launch Pad. • The SP Configuration Database Management menu appears. **SELECT** Enter Database Information • The Enter Database Information menu appears **SELECT** Node Database Information • The Node Database Information menu appears **SELECT** Hostname Information From this point, you can follow the rest of the SMIT steps described in the next row of this table.
SMIT	**TYPE** **smit node_data** • The Node Database Information menu appears. **SELECT** Hostname Information • The Hostname Information window appears. **TYPE** Frame, starting slot, and node count **or** Node List. Also type the adapter name and whether you are using short or long host names. **PRESS** **Do** to store the data.
sphostnam	This command indicates that the host name of each node is the long (fully qualified) form of the host name of the **css0** adapter, for a system with two frames and 32 nodes. `sphostnam -a css0 1 1 32`

Step 32: Add Extension Node

At this point, you can optionally add an extension node to you system. Refer to "Install Extension Nodes" on page 82 for more information.

Step 33: Start System Partition-Sensitive Subsystems

The PSSP 2.3 installation code sets up a single default system partition that includes all nodes in the system. This system partition is created automatically and is called the default or persistent partition because it always exists.

At this time you need to add and start the partition-sensitive subsystems. Topology Services (hats), heartbeat (hb), host response (hr) are examples of partition-sensitive subsystems. Partition-sensitive subsystems are managed by the **syspar_ctrl** command and are listed in the file **/usr/lpp/ssp/config/cmi/syspar_subsystems**. For a more complete description of partition-sensitive subsystems, refer to the section "Managing Partition-Sensitive Subsystems" in the *Administration Guide*.

If using:	Do this:
Perspectives	**SELECT syspar_ctrl -A** • The **syspar_ctrl -A** command is run.
syspar_ctrl	Enter: `syspar_ctrl -A`

Step 34: Verify System Partition-Sensitive Subsystems Have Started

If using:	Do this:
Perspectives	**SELECT syspar_ctrl -E on CWS** • The **syspar_ctrl -E** command is run.
syspar_ctrl	Enter: `syspar_ctrl -E`

Note that if you did not purchase PTPE, you get the following message which you can ignore:

```
Invalid Entry: spdmd /usr/lpp/ptpe/bin/spdmdctrl
Examine failed.  The subsystem control script either does not exist or
cannot be read or executed.
```

Before continuing with the install, verify that the following subsystems have been started and have an 'active' state.

- hats
- hb
- hags
- haem
- hr

To see if these subsystems have been successfully started, issue the following command:

```
lssrc -a | grep <default_syspar_name>
```

For example, If your default system partition name is k22s, issue:

```
lssrc -a | grep k22s
```

The preceding command returns the following output:

```
hags.k22s        hags             17134   active
hats.k22s        hats             22266   active
hr.k22s          hr               18228   active
haem.k22s        haem             21128   active
hb.k22s          hb               22720   active
hagsglsm.k22s    hags             21338   active
```

To continue with the install, the subsystems hags, hats, hr, haem, hb should all be active. If the subsystems are inactive, they should become active in a few minutes.

If a single subsystem is inactive, simply try adding and starting that particular subsystem by issuing:

```
syspar_ctrl -A <subsystem_name>
```

If more than one subsystem is inactive, stop and delete all of the partition-sensitive subsystems by issuing:

```
syspar_ctrl -D
```

Then try to add and start all of the partition-sensitive subsystems by issuing:

```
syspar_ctrl -A
```

If you still have inactive partition-sensitive subsystems, refer to the *Diagnosis and Messages Guide* for further information.

Step 35: Restart System Monitor GUI or Perspectives

To restart the SP System Monitor GUI, enter:

```
spmon –g
```

To restart perspectives, enter:

```
perspectives &
```

Step 36: Set Up Nodes to Be Installed

- Do this step if you want to change the default installation settings for any of the nodes.
- Be aware that the root password is not set if you are installing from a minimal mksysb. For more information on setting a root password when installing from a minimal mksysb, refer to “Step 41: Perform Additional Node Customization” on page 63.
- If the boot/install server will be forwarding packets from the control workstation to a client node, the boot/install server is acting as a gateway to the control workstation. Therefore, ipforwarding must be correctly enabled. To turn ipforwarding on, issue:

  ```
  /usr/sbin/no -o ipforwarding=1
  ```

- If running a PSSP 2.1 node, you cannot export /**usr** or any directories below /**usr**. If you have exported any directories, you must unexport them using the **exportfs -u** command before running **setup_server**. You need to do this because NIM attempts to issue **exportfs** /**usr** during setup_server processing and if you have exported any /**usr** subdirectories, you will see an error.

  If you are running a PSSP 2.2 or later node, this issue does not apply.
- SP node installation when external disk has been selected as the target install disk is currently not supported.

This step does the following:

- Changes the default boot/install information for the node objects in the SDR so that you can indicate a different boot/install server configuration to the RS/6000 SP system

- Allows you to specify an alternate disk or disks to use when installing AIX on nodes

The default installation assumes one of the following:

- You have only one frame and the control workstation is configured to act as the boot/install server.
- You have multiple frames, the control workstation, and the first node in each frame is configured to act as boot/install server.

The default installation assumes your nodes have not been preinstalled. If you want to have them installed with your own install image, you must specify the following:

- Which nodes you are installing with your own install image
- The name of the installation image you are using if you do not want to use the default image, **bos.obj.ssp.42**

If you want different nodes to be installed by a different boot/install server, you must specify the target nodes and which node will serve as the boot/install server.

There are two ways you can specify the disk or disks to use for installation. The first way is the device names format. To specify a single device name, enter:

```
hdisk0
```

or enter multiple device names separated by commas:

```
hdisk0,hdisk1
```

The second format is called the hardware location format. For example, to specify a SCSI drive, you could issue:

```
00-00-00-0,0
```

It is much safer to use the hardware location format. The relative location of hdisks may change depending on hardware installed or possible hardware failures. The hardware location targets a specific disk at a specific location. When changing the default location, IBM strongly suggests using the hardware location format. Installation on external disk drives is not supported.

If using:	Do this:
Perspectives	**SELECT** **smit config_data on CWS** from the Launch Pad. • The SP Configuration Database Management menu appears. **SELECT** Enter Database Information • The Enter Database Information menu appears **SELECT** Node Database Information • The Node Database Information menu appears **SELECT** Boot/Install/usr Server Information From this point, you can follow the rest of the SMIT steps described in the following table.

If using:	Do this:
SMIT	**TYPE** **smit node_data** • The Node Database Information Window appears. **SELECT** Boot/Install/usr Server Information • The Boot/Install Server Information window appears. **TYPE** The data in the fields. Refer to your worksheet as needed. In addition to the node range, you must supply the boot/install server node identifier. If you are not using the default image, you must supply the network install image name. To specify an alternate installation disk or disks, fill in the Destination Hard Disks field, using device names. **PRESS** **Do** to store the data. The distribution of the nodes to be served and the number of different servers you want determines how many times you must perform this step. You may have to do it more than once if you want to define more than one server for different groups of nodes.

spbootins	If you are issuing the **spbootins** command more than once, you can use the **-s no** option to keep **spbootins** from running **setup_server**. For example, the following command specifies the physical volumes **hdisk1** and **hdisk2** as comprising the root volume group for nodes 10 through 16:
	`spbootins -s no -h hdisk1,hdisk2 1 10 7`
	If you are issuing the **spbootins** command using the hardware location format for disk locations 00-07-00-0,0 and 00-07-00-1,0, in this installation for node 9: For example:
	`spbootins -s no -h 00-07-00,0:00-07-00-1,0 -1 9`
	In a two-frame system with all thin nodes, the following command specifies that a network install be performed on nodes 17 through 32 when they reset:
	`spbootins -s no -r install 2 1 16`
	If you need to change "lppsource_name" from default to a new lppsource_name such as aix42 for nodes 1 through 16.
	`spbootins -s no -v aix42 1 1 16`
	If you need to change the PSSP code_version level from PSSP-2.2 to PSSP-2.3 on nodes 17,18,21,22, you may execute
	`spbootins -s no -p PSSP-2.3 -l 17,18,21,22`
	If you are issuing the **spbootins** command for the last time in this install, have it run **setup_server** (the **-s yes** flag). For example:
	`spbootins -s yes -r install 2 1 16`

Note that hdisk0 is the default.	

Step 37: Verify All Node Information

This step verifies that all the node information has been correctly entered into the SDR.

If using:	Do this:
Perspectives	**SELECT** **smit config_data on CWS** from the Launch Pad. • The SP Configuration Database Management menu appears. **SELECT** List Database Information. From this point, you can follow the rest of the SMIT steps described in the next row of this table.
SMIT	Check each of the List Database panels for correct information. If you find any incorrect data, return to the following steps to make corrections: **Data** — **Step** **Frame data** — "Step 23: Enter Frame Information and Reinitialize the SDR" on page 42 **Node data** — "Step 27: Enter Required Node Information" on page 45 **Additional adapters** — "Step 30: Configure Additional Adapters for Nodes" on page 50 **TYPE** **smit list_data** • The List Database Information Window appears. **SELECT** Each panel listed. Verify all information is correct. **PRESS** **Done** to exit SMIT.

splstdata	To display SDR:	Enter:
	Site environment data	`splstdata -e`
	Frame data	`splstdata -f`
	Node data	`splstdata -n`
	Adapter data	`splstdata -a`
	Boot/install data	`splstdata -b`
	Switch data	`splstdata -s`
If your system is large, **splstdata** returns great quantities of data. You may want to pipe the command output through a filter to reduce the amount of data you see.		

Step 38: Verify Extension Node Information

At this point, you can optionally verify extension node information. Refer to "Install Extension Nodes" on page 82 for more information.

Step 39: Change the Default Network Tunable Values

When a node is installed, migrated, or customized (set to "customize" and rebooted), and that node's boot/install server does not have a /tftpboot/tuning.cust file, a default file of system performance tuning variable settings in **/usr/lpp/ssp/install/config/tuning.default** is copied to **/tftpboot/tuning.cust** on that node. You can override these values by following one of the methods described in the following list:

1. Select an IBM-Supplied Alternate Tuning File

   IBM supplies three alternate tuning files which contain initial performance tuning parameters for three different SP environments:

a. **/usr/lpp/ssp/install/config/tuning.commercial** contains initial performance tuning parameters for a typical commercial environment.

b. **/usr/lpp/ssp/install/config/tuning.development** contains initial performance tuning parameters for a typical interactive/development environment.

c. **/usr/lpp/ssp/install/config/tuning.scientific** contains initial performance tuning parameters for a typical engineering/scientific environment.

To select one of these files for use throughout the nodes in your system, use SMIT or issue the **cptuning** command. When you select one of these files, it is copied to **/tftpboot/tuning.cust** on the control workstation and is propagated from there to each node in the system when it is installed, migrated, or customized. Each node inherits its tuning file from its boot/install server. Nodes which have as their boot/install server another node (other than the control workstation) obtain their tuning.cust file from that server node so it is necessary to propagate the file to the server node before attempting to propagate it to the client node. The settings in the **/tftpboot/tuning.cust** file are maintained across a boot of the node.

2. Create and Select Your Own Alternate Tuning File

   The following steps enable you to create your own customized set of network tunable values and have them propagated throughout the nodes in your system. These values are propagated to each node's/**tftpboot/tuning.cust** file from the node's boot/install server when the node is installed, migrated, or customized and are maintained across the boot of the node.

   a. On the control workstation, create the file **/tftpboot/tuning.cust**. You can choose to begin with a copy of the file located in **/usr/lpp/ssp/samples/tuning.cust** which contains a template of performance tuning settings which have been commented out. Or you may prefer to begin with a copy of one of the IBM supplied alternate tuning files.

   b. Select the tunable values that are best for your system. Refer to the table that follows for more information on tuning values.

   c. Edit the **/tftpboot/tuning.cust** file by ensuring the appropriate lines are uncommented and that the tunable values have been properly set.

Using SMIT,

SELECT SP System Management

SELECT SP Cluster Management

SELECT the desired tuning file.

Table 3. Initial Values for AIX 4.2 Ethernet-Based Performance

Tunable	Ethernet No Switch	Ethernet Thin Node	Ethernet Wide and 604 high node Nodes	Ethernet* Switch
sb_max	163840	442368	475236	655360
rfc1323	1	1	1	1
thewall	16384	16384	16384	16384
subnetsarelocal	1	1	1	1
tcp_sendspace	65536	221184	237568	262144
tcp_recvspace	65536	221184	237568	262144
udp_sendspace	32768	59392	59392	65536
udp_recvspace	65536	221184	237568	655360
tcp_mssdflt	1448	1448	1448	Varies

*These values are designed to optimize the performance of the switch at the expense of the performance of Ethernet.

If you have additional network adapters in your nodes and you want to optimize the network performance for these adapters, use the initial suggested settings in Table 4.

Table 4. Initial Values for Other AIX 4.2 Network Types

Tunable	Token Ring	FDDI	ATM Adapter Card
sb_max	655360	1302528	655360
rfc1323	1	1	1
thewall	16384	16384	16384
subnetsarelocal	1	1	1
tcp_sendspace	262144	196608	262144
tcp_recvspace	262144	196608	262144
udp_sendspace	65536	65536	65536
udp_recvspace	655360	655360	655360

As you set up the network tunables for your environment, it is important to tune for the type of data transfer your site has. If you transfer mainly large blocks of data or buffer sizes of 4 KB or greater, the tunable settings can be different than when you send files or buffers less than 932 bytes. See the *Administration Guide* for more information.

Once you have updated **tuning.cust**, continue installing the nodes. After the nodes are installed and customized, on all subsequent boots, the tunable values in **tuning.cust** will be automatically set on the nodes.

Note that each of the supplied network tuning parameter files, including the default tuning parameter file, contains the line **/usr/sbin/no —o ipforwarding=1**. IBM suggests that on non-gateway nodes, you change this line to read **/usr/sbin/no —o ipforwarding=0**. After a non-gateway node has been installed, migrated, or customized, you can make this change in the **/tftpboot/tuning.cust** file on that node.

Step 40: Configure Control Workstation as Boot/Install Server

Do this step if you have not run **setup_server** already using the SMIT Boot/Install Server Information window or the **spbootins** command.

This step uses the information entered in the previous steps to set up the control workstation and optional boot/install servers on nodes. It configures the control workstation as a boot/install server and configures the following options (when selected in your site environment):

- Automounter
- File Collections
- NTP
- User Management
- Accounting

You can perform this step more than once. If you encounter any errors, see the *Diagnosis and Messages Guide* for further explanation. After you correct your errors, you can start the task again.

In previous releases of PSSP, most of the installation function which configured boot/install servers and clients was performed in the single program called **setup_server** which you could run by issuing the **setup_server** command. This is still the suggested way for configuring the control workstation. For more experienced system administrators, IBM has provided a set of Perl scripts you can issue to also configure the control workstation that enable you to diagnose how the **setup_server** program is progressing. For more information on these scripts, refer to Appendix F.

If using:	**Do this:**
Perspectives	**SELECT** **smit cluster_mgmt** from the Launch Pad. • The RS/6000 SP Cluster Management menu appears. **SELECT** Run setup_server Command
SMIT	**TYPE** **smit enter_data** • The Enter Database Information window appears. **SELECT** Run setup_server Command
setup_server	Enter: `setup_server` with no parameters.
The first time **setup_server** runs, depending upon your configuration, it can take a significant amount of time to configure the control workstation as a NIM master.	

Task D. Customize the Nodes

Step 41: Perform Additional Node Customization

Do this step if you want to perform additional customization such as:

- Adding **installp** images
- Configuring host names
- Setting up NFS, AFS, or NIS
- Configuring adapters that are not configured automatically

Be aware that the root password is not set if you are installing from a minimal mksysb image. If you want to have the root password set, you can do one of the following:

- Modify the **script.cust** file by uncommenting the portion of the code to copy the user information from the server to the node.
- If you did not copy the user management files over, then immediately after the node is up without a password, login to the node as root and set the password either through the SMIT panels under Security & Users or with the **passwd** command.

Use **script.cust** for AIX 4.2 nodes. Do the following tasks:

1. Examine the sample **script.cust** file located in **/usr/lpp/ssp/samples** to determine whether any lines are appropriate to your installation.
2. Copy the file to **/tftpboot/script.cust** and uncomment or edit any necessary lines. Don't forget to change the permissions on the file so that it is world-readable. If you forget to do this, your script will not run.

Name resolution of the control workstation host name is required on the nodes. **script.cust** shows how to copy **/etc/resolv.conf** or **/etc/hosts**, and how to define the node to NIS if that is being used. If you have created a **mksysb** image to install on the nodes, and it already has name resolution defined in it, you do not need to do anything additional.

Commands in this script run after the **mksysb** installation and PSSP customization, and before the reboot of each node.

Step 42: Verify the System Management Tools Were Correctly Installed

This step directs you to run a verification test that checks for correct installation of the System Management tools on the control workstation.

If using:	Do this:
Perspectives	**SELECT** **smit SP_verify on CWS** from the Launch Pad. . • The Installation/Configuration Verification menu appears. From this point, you can follow the rest of the SMIT steps described in the next row of this table.
SMIT	**TYPE** **smit SP_verify** • The RS/6000 Installation/Configuration Verification Menu appears. **SELECT** System Management
sysman	Enter: `SYSMAN_test`

After the tests are run, the system creates a log in **/var/adm/SPlogs** called **SYSMAN_test.log**.

See the *Diagnosis and Messages Guide* for information about what this test does and what to do if the verification fails.

Step 43: Set Up the Switch

If you do not have a switch, proceed to step 44.

If you do have a switch and you want to partition your system, proceed to step 44.

If you do have a switch and you do not want to partition your system, proceed to step 41.

The optional switch connects all the nodes in the system to increase the speed of internal system communications. It supports the high volume of message passing that occurs in a parallel environment with increased bandwidth and low latency.

The switch includes software called the **Worm** which verifies the actual switch topology against an anticipated topology as specified in the switch topology file. This file tells the Worm how many nodes in your configuration ha switch. You create this file by copying one of the default topology files provided for each SP configuration.

The Worm verifies the switch connections beginning at a node designated as the primary node. By default, the primary node is node 1 in frame 1. You can override the default and designate another node as the primary node. You *must* do this if node 1 is not operational.

If you have an SP Switch, a primary backup node exists that will take over for the primary node when it detects that the primary node is no longer functional. The primary backup node passively listens for activity from the primary node. When the primary backup node detects that it has not been contacted by the primary node for a specified amount of time, it assumes the role of the primary node. This takeover involves nondisruptively reinitializing the switch fabric, selecting another primary backup, and updating the System Data Repository (SDR). By default, a node is

selected from a frame that is different from the primary node. If no other frame exists (for example, a single frame system), a node is selected from a switch chip that is different from the primary node. If no other switch chip is available, any available node on the switch is selected. By default, the backup node is the last node in the system or the partition.

Step 43.1: Select a Topology File

Select the correct switch topology file by counting the number of node switch boards (NSBs) and intermediate switch boards (ISBs) in your system, then apply these numbers to the naming convention. The switch topology files are in the /**etc**/**SP** directory on the control workstation.

NSBs are switches mounted in frames containing nodes. ISBs are switches mounted in the switch expansion frame. ISBs are used in large systems, where more than four switch boards exist, to connect many processor frames together.

The topology file naming convention is as follows:

expected.top. nsb. isb

Where:

- *NSBnum* is the number of NSBs in the configuration
- *ISBnum* is the number of ISBs in the configuration
- *type* is the type of topology. The default type is 0.

The exceptions to this naming convention are the topology files for the High Performance Switch-LC8 configuration, which is **expected.top.1nsb_8.0isb.0**, and the topology file for the SP Switch-8 configuration, which is **expected.top.1nsb_8.0isb.1**.

For a description of the topology file names, see the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide.*

Step 43.2: Managing the Switch Topology Files

The switch topology file must be stored in the SDR. The switch initialization code uses the topology file stored in the SDR when starting the switch (**Estart**). When the switch topology file is selected for your system's switch configuration, it must be annotated with **Eannotator**, then stored in the SDR with **Etopology**. The switch topology file stored in the SDR can be overridden by having an **expected.top** file in /**etc**/**SP** on the primary node. **Estart** always checks for an **expected.top** file in /**etc**/**SP** before using the one stored in the SDR.

SP Switch Notes:

1. Be aware that **Estart** distributes the topology file to all the nodes in the system partition on the SP Switch. In the case of **expected.top**, this is significant because if the topology file is left on a node and the primary is changed to that node, the topology file will be used. Therefore, if you are using an **expected.top** bypass file, ensure that it is removed from all nodes when it is no longer needed.
2. Depending upon your configuration, the first **Estart** of the SP Switch may take longer than subsequent **Estart**s.

Step 43.3: Annotating a Switch Topology File

Annotate a switch topology file before storing it in the SDR. Refer to the following table for instructions.

If using:	Do this:
Perspectives	**SELECT** The **smit cluster_mgmt** icon • The RS/6000 SP Cluster Management menu appears. From this point, you can pick up with the SMIT steps listed in the next row of this table.
SMIT	**TYPE** **smit cluster_mgmt** • The RS/6000 SP Cluster Management menu appears. **SELECT** Perform Switch Operations • The Perform Switch Operations menu appears. **SELECT** Topology File Annotator • The Topology File Annotator menu appears. **PRESS** **Do** **TYPE** The data in the fields, as follows: • The fully-qualified name of the topology file (for example, **/etc/SP/expected.top.2nsb.0isb.0**) • The fully-qualified name of the file in which you want to store the annotated topology file (for example, **/etc/SP/expected.top.annotated**) • **yes** to store the topology file in the SDR **PRESS** **Do**
Eannotator	Use **Eannotator** to update the switch topology file's connection labels with their correct physical locations. Use the **-O yes** flag to store the switch topology file in the SDR. Using **Eannotator** makes the switch hardware easier to debug because the switch diagnostics information is based on physical locations. For example, to annotate a two-switch or maximum 32-node system, enter: `Eannotator -F expected.top.2nsb.0isb.0 -f expected.top.annotated -O yes`

Step 43.4: Storing the Switch Topology File in the SDR

If you entered **Eannotator -O yes** or **yes** on the Topology File Annotator menu in "Step 43.3: Annotating a Switch Topology File," skip this step.

If using:	Do this:
Perspectives	**SELECT** the **smit cluster_mgmt** icon • The SP Cluster Management menu appears. From this point, you can pick up with the SMIT steps listed in the next row of this table.
SMIT	**TYPE** **smit cluster_mgmt** • The RS/6000 Cluster Management menu appears. **SELECT** Perform Switch Operations • The Perform Switch Operations menu appears. **PRESS** **Do** **SELECT** Fetch/Store Topology Files • The Fetch/Store Topology Files menu appears. **PRESS** **Do** **SELECT** Store a Topology File • The Store a Topology File menu appears. **PRESS** **Do** **TYPE** The fully-qualified path name of the topology file. **PRESS** **Do**
Etopology	Use **Etopology** to store the switch topology file in the SDR and make sure that it has been annotated. For example, to store a two-switch or maximum 32-node configuration, enter: `Etopology expected.top.2nsb.0isb.0.annotated`

Step 44: Verify the Switch Primary and Primary Backup Node

Frame 1, node 1 is the default primary node for the High Performance Switch. Frame 1, node 1 is the default oncoming primary node for the SP Switch.

A node type exists called the primary backup node for the SP Switch. The primary backup node passively listens for activity from the primary node. When the primary backup node detects that it has not been contacted by the primary node for a specified amount of time, it assumes the role of the primary node. This takeover involves nondisruptively reinitializing the switch fabric, selecting another primary backup, and updating the System Data Repository (SDR). The default is the last node in the frame, not the last node slot. For partitions, the default primary is the first node, the default backup is the last node in the partition. You must override this selection if the node slot is not operational. Use SMIT or the **Eprimary** command to verify this node or change the primary to another node.

If using:	Do this:
Perspectives	**SELECT** the **smit cluster_mgmt** icon • The SP Cluster Management menu appears. From this point, you can pick up with the SMIT steps listed in the next row of this table.
SMIT	**TYPE** **smit cluster_mgmt** • The RS/6000 Cluster Management Menu appears. **SELECT** Perform Switch Operations • The Perform Switch Operations Menu appears. **SELECT** Set Primary/Primary Backup Nodes • The Set Primary and Primary Backup Node Menu appears. **PRESS** **Cancel** to keep defaults **or** **ENTER** A different primary node **PRESS** **Do**
Eprimary	Enter: `Eprimary`

This command, without any parameters, returns the node number of the current primary node, the primary backup node, the oncoming primary node, and the oncoming primary backup node.

The current primary backup, the oncoming primary node, and the oncoming primary backup nodes are valid only for the SP Switch.

Step 45: Set Switch Clock Source for All Switches

Use SMIT or the **Eclock** command to initialize the Switch's Clock Source. The SMIT and **Eclock** interfaces require that you know the number of Node Switch Boards (NSBs) and Intermediate Switch Boards (ISBs) in your RS/6000 SP system.

Select the Eclock topology file from the control workstation's /**etc**/**SP** subdirectory, based on these numbers. For example, if your RS/6000 SP system has six node switch boards and four intermediate switch boards, you would select /**etc**/**SP**/**Eclock.top.6nsb.4isb.0** as an Eclock topology file.

See the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* for the Eclock topology file names.

If using:	Do this:
Perspectives	**SELECT** the **smit cluster_mgmt** icon • The SP Cluster Management menu appears. **SELECT** Perform Switch Operations From this point, you can pick up with the SMIT steps listed in the next row of this table.
SMIT	**TYPE** **smit cluster_mgmt** • The RS/6000 Cluster Management Menu appears. **SELECT** Perform Switch Operations • The Perform Switch Operations Menu appears. **PRESS** **Do** **SELECT** Change/Show Switch Clock Source Settings • The Change/Show Switch Clock Source Settings Menu appears. **PRESS** **Do** **SELECT** Initialize Switch Clock Source Settings • The Initialize Switch Clock Source Settings Menu appears. **PRESS** **Do** **PRESS** List **SELECT** the correct Eclock file **PRESS** **Do**

Eclock	Use the **Eclock** command to set the switch's clock source for all switches.
	For example, if your RS/6000 SP system has six node switch boards and four intermediate switch boards, select **/etc/SP/Eclock.top.6nsb.4isb.0** as an Eclock topology file. Enter:
	`Eclock -f /etc/SP/Eclock.top.6nsb.4isb.0`
	This command sets the proper clock source settings on all switches within a 96-way (6 nsb, 4 isb) RS/6000 SP system.
	Attention: Be careful when using **Eclock** after the switch is initialized. **Eclock** modifies the switch clocking, and can cause the High Performance Switch adapter to lose its clock source.
	To verify the switch configuration information, enter:
	`splstdata -s`

Step 46: Set Up System Partitions

This step is optional. The PSSP 2.3 installation code sets up a default system partition configuration to produce an initial, single-system partition including all nodes in the system. This system partition is created automatically. If you do not want to divide your system into partitions, continue with “Step 47: Network Boot Optional Boot/Install Servers” on page 71.

If you want to partition your system, you can select an alternate configuration from a predefined set of system partitions to implement before booting the nodes or you can use the System Partitioning Aid to generate and save a new layout. Follow the procedure described in the Managing System Partitions chapter in the *Administration Guide* and refer to information regarding the System Partitioning Aid.

You do not have to partition your system now as part of this installation. You can partition it later.

Task E. Power On and Install the Nodes

This section describes the steps you take to power on the nodes to be installed.

Step 47: Network Boot Optional Boot/Install Servers

If you have set up system partitions, do this step in each partition.

Follow the instructions in the following table to network boot the optional boot/install servers which install and customize the nodes you selected. You can check installation progress by checking the node's console. To open a console, issue:

```
s1term <frame_number> <node_number>
```

Depending on the size of the image you are installing and the capacity of your Ethernet network, you should network boot (or reboot) eight nodes per boot/install server at a time.

If using:	Do this:
Perspectives	**SELECT** the Manage/Control Hardware icon by double clicking on it. **SELECT** the Nodes pane **SELECT** Actions → Nodes → 3-digit display • The 3 digit display appears. **SELECT** Nodes to be netbooted **SELECT** Actions → Nodes → Network Boot **SELECT** Apply • All selected nodes are booted and the Network Boot dialog box appears to display status. If you had the Hardware Perspective up before you added the required node information, you should delete and re-add the Nodes Pane. If you had the Hardware Perspective up before you partitioned your system, you should delete and re-add the CWS/System/Syspars Pane and then delete and re-add the Nodes Pane.
System Monitor	From the System Monitor main window: **SELECT** SP → Global Controls • The Global Controls panel appears with all the nodes deselected. **SELECT** Node(s) to Network Boot **SELECT** Net Boot **PRESS** **Do** • All selected nodes network boot and the network boot status window appears **SELECT** SP → All Node Summary Display • The selection screen for node variables appears. **SELECT** 3DigitDisplay from list of variables **PRESS** Display all-node summary • The 3DigitDisplay summary appears.

nodecond	Enter:
	`nodecond frame_number node_number &`
	Enter:
	`spled -n cws_name &`
	to display the 3 digit display.

Network Installation Progress

When a network installation is in progress, the LED for the nodes involved show various values. These values indicate the installation stage. Since the node installation process can be long, it is hard to determine where you are in that process.

Table 5 on page 73 lists the sequence of LED values a node goes through. The table is only a sample list of LED values, and a node may not show all values listed. Depending on the adapters installed on the node, there may be additional values displayed. The table also lists the approximate time, after you start to install a node, when the LED values may be shown. Since the elapsed time to reach a specific LED value can vary, you should use these times as a gauge to determine

the installation progress of the node. The factors that can affect the actual time it takes a node to reach a specific LED value include the following:

- The number of nodes being installed
- The size of the network installation image you are using
- The amount of traffic on the Ethernet
- The amount of activity on the node

Places in the node installation where a single LED value is displayed for an extended period of time are as follows:

1. c40
2. c54

These values are periods of high volumes of network traffic and are only a problem on a node when the value does not change for a very extended period of time. You can use Table 5 as a debugging tool when a node is stuck on a specific LED value.

Table 5 (Page 1 of 4). Sample NIM Installation Trace

Time (min:sec)	LED Value	Description
0:00		Various hardware LEDs
1:30	231	Attempting a normal mode IPL from Ethernet specified in IPL ROM.
2:30	Blank	
	606	Running the **if_config** command to bring up network interface.
	610	Attempting to NFS mount a remote file system.
	299	IPL ROM passed control to the loaded program code.
	608	Attempting to tftp the **.info** file from client's SPOT server.
	612	Accessing remote configuration files.
	622	Returning control to the **/sbin/rc.boot** program.
	520	Running bus configuration.
	890	SCSI-2 differential fast/wide adapter.
	620	Updating special device files.
3:00	890	SCSI-2 differential fast/wide adapter.
	570	Configuring virtual SCSI devices.
3:30	622	Returning control to the **/sbin/rc.boot** program
4:00	811	Identifying or configuring processor complex.

Table 5 (Page 2 of 4). Sample NIM Installation Trace

Time (min:sec)	LED Value	Description
	Blank	
	570	Configuring virtual SCSI devices.
	727	Identifying or configuring unknown asynchronous device.
	538	The configuration manager is invoking a configuration method.
	622	Returning control to the /**sbin**/**rc.boot** program.
	c40	Restoring configuration files.
8:00		
	c42	Extracting data from diskette.
	c33	Selecting a tty terminal attached to serial ports S1 or S2.
	c44	Initializing installation database with target disk info.
8:30		
	c46	Normal installation processing.
	Blank	
9:00		
	c50	Creating root volume group on target disks.
	c46	Normal installation processing.
10:30		
	c54	Installing either BOS or additional packages.
19:00		
	c52	Changing from RAM environment to disk environment.
21:30		
	c46	Normal installation processing.
	570	Configuring virtual SCSI devices.
22:00		
	c46	Normal installation processing.
	731	Identifying or configuring PTY.
	539	The configuration method has terminated, returning to config.
	811	Identifying or configuring processor complex.
	538	The configuration manager is invoking a configuration method.
	570	Configuring virtual SCSI devices.

Table 5 (Page 3 of 4). Sample NIM Installation Trace

Time (min:sec)	LED Value	Description
22:30		
	Blank	
23:00		
	u78	Running rsh to complete node processing on boot/install server.
	u60	Creating **/etc/ssp/server_name** and updating **/etc/hosts**.
	u68	Copying Kerberos realms file from boot/install server
	u59	Running **config_node** to define adapters.
27:00		
	u65	SSP completing the **install/customize/maint**. Issuing shutdown.
27:30		
	c46	Normal installation processing.
28:00		
	292	Running SCSI POST.
	298	Attempting a software IPL.
	291	Running standard I/O POST.
	299	IPL ROM passed control to the loaded program code.
	Blank	
	890	SCSI-2 differential fast/wide adapter.
	820	
	538	The configuration manager is invoking a configuration method.
	570	Configuring Virtual SCSI devices.
28:30		
29:00		
	551	Running IPL varyon.
	517	Mounting client remote file system during network IPL.
29:30		
	553	IPL phase 1 is complete.
	570	Configuring virtual SCSI devices.
	538	The configuration manager is invoking a configuration method.
	c33	Selecting a tty terminal attached to serial ports S1 or S2.
30:00		
	Blank	
33:00		
	762	Configuring the SP Switch adapter card.
	83u	Running SSP configuration method for TB2 card.

Table 5 (Page 4 of 4). Sample NIM Installation Trace

Time (min:sec)	LED Value	Description
34:00		
	570	Configuring virtual SCSI devices.
	538	The configuration manager is invoking a configuration method.
34:30		
	Blank	

Step 48: Verify that System Management Tools Were Correctly Installed

Now that the boot/install servers are powered up, run the verification test from the control workstation to check for correct installation of the System Management tools on these nodes.

If using:	Do this:
Perspectives	**SELECT** smit SP_verify from the Launch Pad. At this point, you can follow the SMIT steps discussed in the row of this table.
SMIT	**TYPE** **smit SP_verify** • The Installation/Configuration Menu appears **SELECT** System Management
sysman	Enter: `SYSMAN_test`

After the tests are run, the system creates a log in **/var/adm/SPlogs** called **SYSMAN_test.log**.

See the section on diagnosing RS/6000 SP problems in the *Diagnosis and Messages Guide* for information on what this test does and what to do if the test fails.

Step 49: Network Boot the Remaining RS/6000 SP Nodes

If you have set up system partitions, do this step in each partition.

Repeat the procedure used in "Step 47: Network Boot Optional Boot/Install Servers" on page 71 to network boot and install, or customize the remaining nodes. You may need to ensure that all setup_server processes have completed on the boot/install nodes prior to issuing a network boot on the remaining nodes. Refer to the **/var/adm/SPlogs/sysman/**<**node>.console.log** file on the boot/install node to see if **setup_server** has completed.

If any of your boot/install servers have more than eight clients on a single Ethernet segment, you should Network Boot those nodes in groups of eight or less. See the tuning considerations chapter in the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* for more information.

Using a Token Ring-Bridge Gateway

If you are using a token ring through a bridge as your default gateway to your nodes and the token ring bridge is not on the same segment as your LAN, you must change the value of the broadcast field in the ODM for each node. The default value is set to **No** (confine broadcast to local token-ring) each time you install or customize a node. However, when you boot the nodes with this bridge setup, the network is unusable.

If using:	Do this:
SMIT	**TYPE** **smit chinet** • The Available Network Interfaces menu appears. **SELECT** tr0 token ring network interface **TYPE** `Yes` in the Confine broadcast to LOCAL Token-ring field.
chdev	Enter: `chdev -P -l tr0 -a allcast=off`

Step 50: Verify Node Installation

If you have set up system partitions, select a global view to do this step.

Check hostResponds and powerLED indicators for each node.

If using:	Do this:
Perspectives	**SELECT** the Manage/Control Hardware icon by double clicking on it. • The Hardware Perspectives appears. **SELECT** the Nodes Pane **SELECT** View → Monitor • The Set Monitoring for Nodes dialog box appears. **SELECT** the hostResponds condition **PRESS** Apply • The nodes should now be colored green. Check the node icons. All node icons should be solid green. If any are not, see the section in the *Diagnosis and Messages Guide* **PRESS** the Stop Monitoring button in the Set Monitoring for Nodes dialog box. **PRESS** APPLY • The node icons will turn black. **SELECT** the powerLED condition in the Set Monitoring for Nodes dialog box. **PRESS** APPLY • The nodes should now be colored green.
System Monitor GUI	**SELECT** SP **SELECT** Global Controls **SELECT** SP **SELECT** All Node Summary Display • The selection screen for node variables appears. **SELECT** hostResponds from the list of variables **PRESS** Display all-node summary. • The hostResponds Summary appears. Check the indicators for hostResponds. All indicators should be solid green. If not, see the section on diagnosing RS/6000 SP problems in the *Diagnosis and Messages Guide*. **PRESS** Window → Exit **SELECT** powerLED on the selection screen for node variables. **PRESS** Display all-node summary. • The powerLED Summary appears. Check the indicators for PowerLED. All indicators should be solid green. If not, see the section on diagnosing RS/6000 SP problems in the *Diagnosis and Messages Guide*. **PRESS** Window → Exit
spmon	Enter: `spmon -d -G`

Step 51: Run Verification Tests on All Nodes

If you have set up system partitions, do this step in each partition.

This step directs you to run a series of verification tests that check for correct installation of your selected options on all the nodes.

If using:	Do this:
Perspectives	**SELECT** smit SP_verify from the Launch Pad. From this point, follow the SMIT steps discussed in the next row of this table.
SMIT	**TYPE** **smit SP_verify** • The Installation/Configuration Menu appears **SELECT** System Management
SYSMAN_test	Enter: `SYSMAN_test`

After the tests are run, the system creates a log in **/var/adm/SPlogs** called **SYSMAN_test.log**.

See the section on diagnosing RS/6000 SP problems in the *Diagnosis and Messages Guide* if the verification test fails.

Step 52: Start the Optional Switch

- Do this step if you have installed a switch.
- If you have set up system partitions, you will need to initialize the switch from within each partition.
- Rerun the **Eannotator** command if installing the SP Switch to update connector information.

If using:	Do this:
Perspectives	**SELECT** The **smit cluster_mgmt** icon • The SP Cluster Management menu appears. **SELECT** Perform Switch Operations From this point, you can pick up with the SMIT steps listed in the next row of this table.
SMIT	**TYPE** **smit switch_ops** • The Perform Switch Operations Menu appears. **SELECT** Start Switch
Estart	Enter: `Estart`

Step 53: Verify the Switch Was Installed Correctly

- Do this step if you have installed a switch.
- If you have set up system partitions, verify the switch from within each partition.
- Check all connectors for miscabling and node communications.

Run a verification test to ensure that the switch is installed completely.

If using:	Do this:
Perspectives	**SELECT** smit SP_verify from the Launch Pad. At this point, follow the SMIT steps discussed in the next row of this table.
SMIT	**TYPE** **smit SP_verify** • The Installation/Configuration Menu appears **SELECT** The Communication Subsystem option **PRESS** Enter.

CSS_test	Enter:
	`CSS_test`
	Enter:
	`spmon -G -d`
	to make sure the switch_responds indicates a "yes" value for SP nodes.

After the tests are run, the system creates a log in **/var/adm/SPlogs** called **CSS_test.log**.

If the verification test fails, see the section on diagnosing RS/6000 SP problems in the *Diagnosis and Messages Guide*.

Check switchResponds and powerLED indicators for each node.

If using:	Do this:
Perspectives	**SELECT** the Manage/Control Hardware icon by double clicking on it. **SELECT** the Nodes Pane • The Nodes Pane receives focus. **SELECT** View → Monitor • The Set Monitoring for Nodes dialog box appears. **SELECT** the switch_responds condition **PRESS** Apply • The nodes should now be colored green. Check the node icons. All node icons should be solid green. If they are not, refer to the *Diagnosis and Messages Guide* for further information.
System Monitor GUI	From the main window: **SELECT** SP **SELECT** Global Controls **SELECT** SP **SELECT** All Node Summary Display • The selection screen for node variables appears. **SELECT** switchResponds from the list of variables **PRESS** Display all-node summary. • The switchResponds Summary appears. Check the indicators for switchResponds. All indicators should be solid green. If not, see the section on diagnosing RS/6000 SP problems in the *Diagnosis and Messages Guide*.
spmon	Enter: `spmon -d -G`

Step 54: Tune the Network Adapters

Various models of the network adapters can have different values for transmit queue sizes. To get peak performance out of the network adapters, increase the transmit and receive queue sizes to their maximum. For all adapters on nodes running AIX 4.2 (except for built-in Ethernet adapters) set the transmit queue size to 160. Set the built-in Ethernet adapters to 150 and set the FDDI adapter queue limit to 250.

If the adapter you are changing is also the adapter for the network you are logged in through, you will have to make the changes to the database only. Then reboot the node for the changes to become effective.

If using:	Do this:
Perspectives	**SELECT** **smit devices** from the Launch Pad. • The Devices menu appears From this point, you can follow the rest of the SMIT steps described in the next row of this table.
SMIT	**TYPE** **smit devices** • The Devices menu appears **SELECT** Communication • The Communication menu appears **SELECT** The adapter you want to reset (for example, `Ethernet Adapter`) • The Ethernet Adapter menu appears **SELECT** Adapter • The Adapter menu appears **SELECT** Change / Show Characteristics of an Ethernet Adapter • An Ethernet Adapter window appears **SELECT** An adapter from the list shown • The Change / Show Characteristics of an Ethernet Adapter window appears **CHANGE** The TRANSMIT queue size to 160 (150 for Ethernet on SP nodes) **CHANGE** `Apply change to DATABASE only` to **yes**. (Press F4 and select yes.) **PRESS** **Do** to apply the changes to the database.
chdev	Enter `chdev -P -l ent0 -a xmt_que_size=160`
You must reboot the node in order for the changes to take effect.	

Install Extension Nodes

The information in this section is optional unless you plan on installing an extension node.

Extension nodes are non-standard nodes that extend your system's capabilities or scope, but can't be used in all the same ways as standard SP nodes. Extension nodes are attached to the system via an *extension node adapter*.

A specific type of extension node is a *dependent node*. A dependent node depends on SP nodes for certain functions, but implements much of the switch-related protocol that standard nodes use.

You can use the command line interface or SMIT to add, delete, or modify the extension node information in the SDR. This information consists of both an extension node and an extension node adapter definition.

To add an extension node, there are several steps to follow. You perform some of these steps on the extension node. Most of the steps, however, must be performed on the control workstation. You will have to login to the extension node, either directly or via a telnet session to perform the steps required on the extension node.

This section provides a high-level discussion of the steps you must perform on the control workstation and on the extension node. For more specific information, refer to the following documents:

- *PSSP System Administration Guide*
- *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment*
- *SP Switch Router Adapter Guide* which comes with the SP Switch Rou
- All related Ascend documentation.

Control Workstation Steps

Perform the following steps on the control workstation:

1. Install the **ssp.spmgr** File Set

   If the file set **ssp.spmgr** is not already installed on the control workstation, install it now by issuing the following commands:

   ```
   installp ssp.spmgr
   ```

2. Verify Port Information

   Once **ssp.spmgr** is installed on the control workstation, UDP port 162 becomes reserved for SNMP traffic between the SP Extension Node SNMP Manager and the SNMP Agent on the extension node. This port is the default SNMP trap port for any SNMP Manager. If another LPP which includes an SNMP Manager is configured on the control workstation, there is a conflict which you would need to resolve by modifying the entry for **spmgrd-trap** in **/etc/services** on the control workstation to specify an unused UDP port number.

3. Define the Extension Node

   Issue the **endefnode** command to add an extension node definition in the SDR. You need to issue this command for each extension node you want to configure. For more information on this command, see the *PSSP Commands and Technical Reference*.

4. Define the Extension Node Adapter

   Issue the **endefadapter** command to add an extension node adapter definition in the SDR. You need to issue this command for each extension node adapter you want to configure.

Extension Node Steps

Perform the following steps on the extension node:

1. Optionally, Define the Extension Node and Extension Node Adapter

   IBM requires that you define the extension node and the extension node adapter on the control workstation, as discussed in the previous section. In addition, you can optionally define these items on the extension node.

   Once the items have been defined, the extension node is configured automatically. The SNMP Agent on the extension node polls the SPMGR Manager running on the control workstation for the information at a designated interval. The SPMGR Manager looks for the information for the extension node adapter specified and passes back the configuration information. Once the extension node and extension node adapter information has been added to the

SDR, the SPMGR Manager is able to respond with the configuration information.

For more information, refer to the *SP Switch Router Adapter Guide*.

2. Configure the SNMP Agent to communicate with the extension node SNMP Manager on the control workstation. See the *SP Switch Router Adapter Guide* for further information.
3. Install the Ascend extension node IP router and all IP interfaces connected to it.

   For more information, refer to the *SP Switch Router Adapter Guide*.

Activate Extension Node Step

Issue the **Estart** command on the control workstation to reconfigure the switch to recognize the new extension nodes.

Extension Node Verification Steps

There are several ways to verify that the extension node has been successfully installed and is operating correctly. Perform steps 1, 2, and 3. You can optionally perform step 4:

1. Issue the following command to verify the definition of the extension node:

   ```
   splstnodes -t dependent node_number reliable_host_name \
   management_agent_hostname extension_node_identifier snmp_community_name
   ```

2. Issue the following command to verify the definition of the extension node adapter:

   ```
   splstadapters -t node_number netaddr netmask
   ```

3. Issue the following command to verify that the extension node is connected to the switch:

   ```
   SDRGetObjects switch_responds
   ```

   You should receive output similar to the following:

   ```
   node_number switch_responds autojoin  isolated     adapter_config_status
   1           0               0         0            css_ready
   3           0               0         0            css_ready
   4           0               0         0            css_ready
   5           0               0         0            css_ready
   6           0               0         0            css_ready
   7           0               0         0            css_ready
   ```

4. Use the Perspectives GUI to verify the definitions of the extension node and extension node adapter, and to verify that the extension node is connected to the switch.

   Issue **perspectives &** to bring up Perspectives as a background process.

   SELECT Hardware Perspective

   SELECT IP node

   The notebook associated with the node appears. Review the node information to ensure it is operating correctly.

Run Post-Installation Procedures

Now that your RS/6000 SP System is installed and ready to run, you can set up any additional tools you want to use to manage your parallel environment.

You can find procedures for setting up these facilities as follows:

Table 6. Information About RS/6000 SP Facilities

For RS/6000 SP Facility	**Refer to:**
Error Log	Error logging information in the *Diagnosis and Messages Guide*.
Resource Manager	Managing RS/6000 SP resources chapter in the *Administration Guide*
Login Control	Managing user accounts chapter in the *Administration Guide*
IBM Virtual Shared Disk	Virtual Shared Disk chapter in the *Managing Shared Disks Guide*
DTMS	Distributed Tape Management System chapter in the *Administration Guide*
Sysctl	Sysctl chapter in the *Administration Guide*

Chapter 3. Installing and Configuring the High Availability Control Workstation

This chapter discusses how to install and configure the High Availability Control Workstation (HACWS). The information in this chapter is optional—you do not have to install HACWS in order to run your SP system. Before you begin, you should carefully plan your HACWS installation. This will help make your installation more efficient and successful. For more information about planning for HACWS installation, see the *IBM RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment.*

Install HACWS if you want to do any of the following:

- Continue running your SP system after a control workstation failure.
- Shutdown the control workstation for deferred hardware and software maintenance without having a system outage.
- Maintain the SP system function and reliability when the control workstation fails.
- Fail over the control workstation to a backup.

You can add an HACWS configuration at any time in the life of your SP system.

Part of the HACWS installation procedure involves installing the High Availability Cluster Multi-Processing/6000 (HACMP/6000) on the primary and backup control workstations. (See “Task D. Configure High Availability Cluster Multi-Processing” on page 100.) You may use any level of HACMP 4.2 or greater that is supported with the level of AIX that you are using. Refer to the appropriate HACMP documentation to determine which levels of HACMP are supported with the level of AIX that you are using.

HACMP runs on two control workstations in a two-node rotating resource configuration. There are external disks and a dual RS-232 frame supervisor card with a connection from each control workstation to each SP frame. The DASD is not accessed concurrently. The control workstation configuration provides automated detection, notification, and recovery of control workstation failures. For more information about HACMP, see *AIX HACMP/6000 Concepts and Facilities.*

Keep these points in mind as you install HACWS:

- You must install your SP system with a regular control workstation first. (The original control workstation becomes the primary control workstation in your HACWS configuration.)
- You must install HACMP on both control workstations.
- HACWS supports only a single backup control workstation.
- Resource Manager does not participate in HACWS. You must start it manually after a fail over or reintegration. For more information on the Resource Manager, refer to the PSSP System Administration Guide.
- Standby adapters on the primary control workstation are *not* required.
- The external file system can be mounted over either the /**spdata** or the /**spdata**/**sys1** directories.

© Copyright IBM Corp. 1995, 1997

Finding Related Information

You can find more information about HACMP and HACWS in the following books:

- *AIX HACMP/6000 Concepts & Facilities*
- *AIX HACMP/6000 Planning Guide*
- *AIX HACMP/6000 Installation Guide*
- *AIX HACMP/6000 Administration Guide*
- *IBM RS/6000 SP: Planning, Volume 2, Control Workstation and System Environment*
- *IBM Parallel System Support Programs for AIX: Administration Guide*
- *Implementing High Availability on RISC/6000 SP (Redbook)* SG24-4742.

Task A: Prepare the Control Workstations

This section describes the steps you take to prepare the control workstation.

Step 1: Understand the Procedure

Read and become familiar with the following publications:

- *AIX HACMP/6000 Concepts & Facilities*
- *AIX HACMP/6000 Planning Guide*
- *AIX HACMP/6000 Installation Guide*
- *AIX HACMP/6000 Administration Guide*
- *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment*
- *Administration Guide*

You must be familiar with HACMP terminology, including the following:

- Service address
- Boot address
- Network interface

Step 2: Plan Network Configuration

Planning for your High Availability Control Workstation is essential before proceeding with the installation steps. Be sure to read the section on planning for the High Availability Control Workstation in chapter 4 of the *IBM RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment*.

Step 3: Install the SP System

If you have not done so already, install your SP system (single control workstation, frames, and nodes) as described in Chapter 2, “Installing and Configuring a New RS/6000 SP System” on page 13). The SP system must be completely installed and operating correctly before beginning HACWS installation.

After you complete the rest of the instructions in this chapter, the original control workstation will become the primary control workstation, and the backup control workstation will be added to your system.

Step 4: Install AIX on the Backup Control Workstation

If you have not done so already, install base AIX on the backup control workstation. For more information, refer to the *IBM AIX Installation Guide*.

Step 5: Back Up the Control Workstations

Create mksysb images of both the primary control workstation and the backup control workstation, and keep them on hand in case the HACWS installation fails. **Restoring a mksysb image is the only way you can recover from a failed HACWS installation**.

Also backup the /**spdata** file system if it is not located on the root volume group.

Step 6: Set Up the Hardware

Perform all hardware setup. Refer to the *IBM RS/6000 SP: Planning, Volume 1, Hardware and Physical Environment* for instructions. The use of a serial network with HACMP is strongly suggested. The serial connection can be either a SCSI-2 Differential bus using target mode SCSI, or a raw RS-232 serial line. Refer to the *AIX HACMP/6000 Installation Guide* for full details.

To set up the external disks, follow the shared disk installation instructions in Chapter 5 of the *AIX HACMP/6000 Installation Guide*.

Step 7: Configure RS-232 Control Lines

Each frame in your SP system requires a serial port on the control workstation configured to accommodate the RS-232 line.

You already performed this step on the primary control workstation. You need to perform the same step on the backup control workstation. Each frame must be connected to the exact same tty port on both control workstations. If not cabled correctly, the hardware monitor will not bring all of the frames online.

Refer to “Step 5: Configure RS-232 Control Lines” on page 16 for more instructions.

Task B. Update SP Authentication Services on Primary Control Workstation

This section describes the steps you take to update Kerberos on the control workstations.

Step 8: Add the Kerberos Principal

Use this procedure to add principals for all the primary boot addresses (if the principals do not already exist.)

Some of the network interfaces configured on a regular control workstation become service addresses in the HACWS configuration. For example, a control workstation named **sp_cws** would have a network interface by the same name. When the SP system becomes an HACWS configuration, **sp_cws** becomes a service address. Since the service addresses in a rotating configuration rotate with their resource groups, the **sp_cws** network interface moves back and forth between the primary and backup control workstations.

When the **sp_cws** network interface is on the backup control workstation, the network adapter on the primary control workstation is known by an alternate name, such as **sp_cws_bt**. This alternate name is the boot address. The primary boot addresses need to be identified to Kerberos so the backup control workstation can access authenticated services on the primary while the backup control workstation is acting as the system control workstation.

This example shows the procedure you should follow to add the Kerberos principal **rcmd**, instance *sp_cws_bt* on the primary control workstation. Run the **/usr/kerberos/etc/kdb_edit** program as follows:

```
Opening database...

Enter Kerberos master key: kerberosMasterPassword


Previous or default values are in [brackets] ,
enter return to leave the same, or new value.

Principal name: rcmd

Instance: sp_cws_bt

<Not found>, Create [y] ? <Enter>
Principal: rcmd, Instance: sp_cws_bt, kdc_key_ver: 1

New Password: rcmdPassword Verifying, please re-enter New Password:
rcmdPassword
Principal's new key version = 1
Expiration date (enter yyyy-mm-dd) [ 1999-12-31 ] ?
<Enter>
Max ticket lifetime (*5 minutes) [ 255 ] ? <Enter>
Attributes [ 0 ] ? <Enter>
Edit O.K.
Principal name: <Enter>
#
```

```
# <end_of_example>
```

Step 9: Add Kerberos rcmd Service Key

This example shows the procedure you should follow to add the Kerberos **rcmd** service key for each primary control workstation boot address.

Run the **/usr/lpp/ssp/kerberos/bin/ksrvutil add** command as follows:

```
Name: rcmd

Instance: sp_cws_bt

Realm: XYZ.COM

Version number: 1

New principal: rcmd.sp_cws_bt@XYZ.COM; version 1

Is this correct? (y,n) <Enter>

Password: RcmdPassword Verifying, please re-enter Password: RcmdPassword

Key successfully added.

Would you like to add another key? (y,n) n

Old keyfile in /etc/krb-srvtab.old. # # <end_of_example>
```

Step 10: Install PSSP on the Backup Control Workstation

You must now install the PSSP file sets on the backup control workstation to match the PSSP software that is already installed on the primary control workstation. Refer to "Task B. Install PSSP on the Control Workstation" on page 26 for descriptions of the PSSP file sets. You can perform file set installation from the command line by issuing the **installp** command or you can use SMIT by issuing the **smit install_latest** command. Refer to the *AIX Installation Guide* for more details on how to use these commands.

Note: You will complete the installation of PSSP later, so do not run any PSSP configuration commands. (Do not run the **install_cw** command).

Note: You should not install the **ssp.hacws** file set at this time. You will do this later in "Step 16: Install the HACWS Image on Both Control Workstations" on page 97.

Step 11: Configure the Backup Control Workstation as a Secondary Authentication Server or Client

If the primary control workstation is either a primary or secondary Kerberos authentication server, then the backup control workstation must be configured as a secondary authentication server. If the primary control workstation is an authentication client, the backup control workstation must also be configured as an authentication client.

Follow the instructions in “Step 11.1: Initializing as a Secondary Authentication Server” on page 93 or in “Step 11.2: Initializing as an Authentication Client System” on page 94 to configure the backup control workstation as either a second authentication server or as an authentication client.

Step 11.1: Initializing as a Secondary Authentication Server

Note: If you perform this step, do not perform “Step 11.2: Initializing as an Authentication Client System” on page 94.

The following example illustrates the procedure you should follow to initialize the backup control workstation as a secondary authentication server.

1. Copy the **/etc/krb.conf** file from the primary authentication server to the backup control workstation.
2. Add a line to the **/etc/krb.conf** file, listing the backup control workstation (by its full host name) as a secondary server for the local authentication realm.

   For example, to add **sp2cw.xyz.com** as a secondary server for the authentication realm **XYZ.COM**, add this line to **/etc/krb.conf**:

   ```
   XYZ.COM sp2cw.xyz.com
   ```
3. Copy the **/etc/krb.realms** file from the primary server to the backup control workstation.
4. On the backup control workstation, run the **setup_authent** program.

   setup_authent requires you to login to the authentication service using the same administrative principal name that was defined when the primary server was set up. The remainder of the initialization of authentication services on this secondary local system takes place automatically.

   The following example shows the interaction you can expect when you run **setup_authent** when initializing as a secondary authentication server.

   ```
   #setup_authent
   <screenclear>
   ********************************************************************
   Logging into Kerberos as an admin user

    You must assume the role of a Kerberos administrator <user>. to
    complete the initialization of Kerberos on the local system. The kinit
    command is invoked and will prompt you for the password. If you are
    setting up your primary server here, you have just defined it. If you
    have defined multiple administrative principals, or if your primary
    authentication server is on another system, you must first enter the
    name of an administrative principal who has root privilege (UID 0). You
    need to be authenticated as this administrator so that this program
    can create the principals and service key files for the authenticated
    services that run on the SP system.

    For more information, see the kinit man page.
    ********************************************************************

   setup_authent: Enter name of admin user: root

   Kerberos Initialization for "root.admin"

   Password: rootPassword sp2cw.xyz.com: success.
   ```

```
sp2cw.xyz.com:  Succeeded
#
```

Note: The last two messages shown in the example above are issued by the programs that transfer the database from primary to secondary servers, to indicate that the backup database has been installed.

```
# klist
Ticket file:    /tmp/tkt0
Principal:  root.admin@XYZ.COM

Issued           Expires          Principal
Nov 11 16:26:11  Dec 12 16:26:11  krbtgt.XYZ.COM@XYZ.COM
#
<end_of_example>
```

5. After **setup_authent** completes, add an entry for the secondary authentication server to the **/etc/krb.conf** file on all SP nodes on which you have already initialized authentication.
6. If this is the first secondary authentication server, you should create a root **crontab** entry on the primary authentication server that invokes the script **/usr/kerberos/etc/push-kprop**. This periodically propagates database changes from the primary to the secondary authentication server.

Step 11.2: Initializing as an Authentication Client System

Note: If you perform this step, do not perform “Step 11.1: Initializing as a Secondary Authentication Server” on page 93.

The following example illustrates the procedure you should follow to initialize the backup control workstation as an authentication client.

1. Copy the **/etc/krb.conf** file from the primary authentication server to this system (the backup control workstation).
2. Copy the **/etc/krb.realms** file from the primary server.

   Note: If the new workstation is outside the realm of the primary server, you must add this new workstation to the **/etc/krb.realms** file on the primary server before you copy the **/etc/krb.realms** file from the primary server to the new workstation. Otherwise, the next step will fail.
3. Run the **setup_authent** program.

   setup_authent requires you to login to the authentication service using the same administrative principal name that was defined when the primary server was set up. The remainder of the initialization of authentication services on the local system takes place automatically.
4. The root **.klogin** file on a client workstation contains just the administrative principal name you used to install authentication. You may want to edit the **.klogin** file to add other principals in your configuration.
5. Enter the **/usr/lpp/ssp/kerberos/bin/klist** command to make sure a ticket exists for the account.

The following example shows the interaction you can expect when you run **setup_authent** when initializing as an authentication client system.

Note: The initial warning message shown in the example is issued if you have installed the **ssp.authent** option on a system configured as a client rather than a server.

```
#setup_authent
<screenclear>
********************************************************************
Logging into Kerberos as an admin user

You must assume the role of a Kerberos administrator <user>.admin to
complete the initialization of Kerberos on the local system. The kinit
command is invoked and will prompt you for the password. If you are
setting up your primary server here, you have just defined it. If you
have defined multiple administrative principals, or if your primary
authentication server is on another system, you must first enter the
name of an administrative principal who has root privilege (UID 0). You
need to be authenticated as this administrator so that this program
can create the principals and service key files for the authenticated
services that run on the SP system.

 For more information, see the kinit man page.
********************************************************************

setup_authent: Enter name of admin user: root

Kerberos Initialization for "root.admin"

Password: rootPassword

# klist
Ticket file:    /tmp/tkt0
Principal:  root.admin@XYZ.COM

Issued           Expires          Principal
Nov 11 16:26:11  Dec 12 16:26:11  krbtgt.XYZ.COM@XYZ.COM
#

 # <end_of_example>
```

Step 12: Keep Kerberos Keys the Same

When control workstation services move back and forth between the two control workstations, the Kerberos service keys must remain the same. The **krb_srvtab** file should be the same on both the primary and secondary authentication servers.

Enter the following commands on the backup control workstation:

```
/usr/lpp/ssp/rcmd/bin/rcp -p <primary_name> :/etc/krb-srvtab /etc/
cp -p /etc/krb-srvtab /etc/krb-srvtab.backup
cat /etc/krb-srvtab.primary >>/etc/krb-srvtab
```

Repeat this procedure whenever you change Kerberos service keys on either of the two control workstations.

Step 13: Verify Kerberos Data

Make sure a Kerberos principal and rcmd service key exist for the network address that matches the host name of the backup control workstation.

Run the **/usr/lpp/ssp/kerberos/bin/kadmin** command on the backup control workstation as follows:

```
Welcome to the Kerberos Administration Program, version 2
Type "help" if you need it.

admin: get_entry rcmd.BackupControlWorkstation

Admin password:

Info in Database for rcmd.BackupControlWorkstation:
Max Life: 255   Exp Date: Fri Dec 31 22:59:59 1999

Attribs: 00  key: 0 0
admin:  q
Cleaning up and exiting.
 # <end_of_example>
```

Run the **/usr/lpp/ssp/kerberos/bin/ksrvutil list** command on the backup control workstation and the system will display information similar to the following:

```
Version    Principal
2     rcmd.k21sha@PPD.POK.IBM.COM
2     hardmon.k21sha@PPD.POK.IBM.COM
2     rcmd.k21shacw@PPD.POK.IBM.COM
2     hardmon.k21shacw@PPD.POK.IBM.COM
1     hardmon.k21cw@PPD.POK.IBM.COM
1     rcmd.k21cw@PPD.POK.IBM.COM
1     rcmd.k21s@PPD.POK.IBM.COM
1     hardmon.k21s@PPD.POK.IBM.COM
1     rcmd.k21cw_bt@PPD.POK.IBM.COM
1     rcmd.k21s_bt@PPD.POK.IBM.COM
#
 # <end_of_example>
```

Task C. Install Software

Step 14: Install HACMP on Both Control Workstations

Follow the instructions in Chapter 8 of the *AIX HACMP/6000 Installation Guide* to install the HACMP software.

Step 15: Verify Cluster Software

Follow the instructions in Chapter 10 of the *AIX HACMP/6000 Installation Guide* to verify the cluster software.

Step 16: Install the HACWS Image on Both Control Workstations

Install **ssp.hacws** on both control workstations using SMIT.

TYPE **smit install_latest**

•The Install New Software Products at Latest Level window appears .

SELECT The input device (press F4 and select a device) and the **ssp.hacws** fileset.

PRESS **Do** to complete the action.

Step 17: Stop the Primary Control Workstation

Stop control workstation services on the primary control workstation by entering the following command:

```
/usr/sbin/hacws/spcw_apps -d
```

Step 18: Configure Serial Network

Configure the target mode SCSI connection or the raw RS-232 serial line which is to be used as the HACMP serial network. Refer to chapter 4 of the *AIX HACMP/6000 Installation Guide* for instructions.

Step 19: Configure the Network

You need to configure each control workstation to use its boot addresses after it reboots. (You should have identified the boot addresses in “Step 2: Plan Network Configuration” on page 89.) To do this, enter the following command:

```
smit chinet
```

The Internet Address field should contain the IP address corresponding to the boot address. Do this for each boot address on both control workstations.

Note: Do not reboot until you are instructed to do so in Step 33: Reboot Control Workstations.

Step 20: Migrate Internal File System

If not previously done, the /**spdata** directory needs to reside in an external volume group so both control workstations can access it. You can accomplish this by migrating the /**spdata** files from a separate file system in an internal volume group to the external volume group.

Complete the following procedure:

1. Determine which file system contains the /**spdata** directory by entering the following command:

   ```
   df /spdata
   ```

   If the file system is separate, the mount point will be /**spdata**.
2. Unmount the /spdata file system by entering the following command:

   ```
   umount /spdata
   ```
3. Enter:

   ```
   smit chjfs
   ```
4. Select /**spdata**.
5. Set the new mount point to /**spdata.old**. Set `mount automatically at system restart` to **no**.
6. Mount the file system at its new mount point by entering the following command:

   ```
   mount /spdata.old
   ```

Step 21: Set Up External File System

The following list illustrates how the HACMP terminology maps to your HACWS setup:

HACMP Term	HACWS Equivalent
Source node	Primary control workstation
Destination node	Backup control workstation

If you have not already set up an external file system, refer to the shared logical volume configuration instructions in Chapter 6 of the *AIX HACMP/6000 Installation Guide*. Follow the instructions for non-concurrent access. Use the following list with the shared logical volume configuration instructions:

1. Create a volume group on the primary control workstation. The volume group can have any name—it does not have to be **spvg**. (**spvg** is used in the examples.) Be sure to use a major number that is available on both control workstations.
2. Follow the instructions to create a file system in the new volume group.
3. Follow the instructions to rename the logical volumes. After you rename the logical volumes, check the /**etc**/**filesystems** file to make sure the **dev** and **log** attributes reflect the changes. If they do not, edit /**etc**/**filesystems** and update these attributes to reflect the changes.
4. Follow the instructions to add copies to the logical volume on the source node (primary control workstation).
5. Mount the new /**spdata** file system. Enter the following command:

   ```
   mount /spdata
   ```
6. Copy the /**spdata** files from the old /**spdata** file system to the new file system. Enter the following command:

   ```
   cp -Rph /spdata.old/* /spdata
   ```
7. Unmount both spdata file systems. Enter the following commands:

```
umount /spdata.old
umount /spdata
```

8. Follow the instructions in the remainder of non-concurrent access section to do the following:
   a. Vary off the volume group on the primary control workstation.
   b. Import the volume group on the backup control workstation. (Make sure to use the same major number you used on the primary control workstation.)
   c. Change the volume group so it remains dormant on the backup control workstation. If the volume group is mirrored three ways, then answer **Yes** to the `quorum required` question. Otherwise, answer **No** to the question. Refer to the HACMP publications for more information about quorum in an HACMP cluster.
   d. Vary off the volume group on the backup control workstation.
9. Make the /**spdata** file system available on the primary control workstation.
   a. Vary on the volume group on the primary. Enter the following command:

      ```
      varyonvg spvg
      ```

   b. Mount the /**spdata** file system. Enter the following command:

      ```
      mount /spdata
      ```

10. Issue the SMIT **chvg** command to make sure quorum status on the primary control workstation matches the quorum status that you specified for the backup control workstation.

Step 22: Complete Administration Tasks

Follow the AIX administration instructions in Chapter 7 of the *AIX HACMP/6000 Installation Guide*. Use the following list with the installation instructions:

1. The **install_hacws** command you will use in “Step 28: Set Up the HACWS Configuration” on page 103 sets I/O pacing to the HACMP suggested starting points. If you **install_hacws** set these values, skip the set I/O pacing step.
2. The /**etc**/**hosts** file should contain both short and long host names for each network interface, so both types of references (for example, **sp_cws_bt** and **sp_cws_bt.xyz.com**) can be resolved.

Task D. Configure High Availability Cluster Multi-Processing

This section describes the steps you take to setup High Availability Cluster Multi-Processing (HACMP) to work with HACWS.

Step 23: Define the Cluster Environment

Follow the instructions in Chapter 11 of the *AIX HACMP/6000 Installation Guide* to define the cluster environment. You must configure HACMP to use hardware address swapping in conjunction with IP address takeover on any service adapter belonging to the SP Ethernet network or whose name matches the hostname of the primary control workstation.

The service adapter *dutchess.xyz.com* from the sample scenario, (see Planning, Volume 2) falls into both categories. Chapter 3 of the *AIX HACMP/6000 Planning Guide* explains hardware address swapping.

As you define your cluster environment, you may find it helpful to read the following examples which reference the example configuration discussed in Planning, Volume 2.

Step 23.1: Define the Cluster ID and Name

Follow the instructions in the *AIX HACMP/6000 Installation Guide*.

Step 23.2: Define Nodes to HACMP

In the sample scenario discussed in Planning, Volume 2, the hostnames of the control workstations are *dutchess.xyz.com* and *ulster.xyz.com*. HACMP does not care whether you use the short or long hostnames, so use the short hostnames. The sample scenario short hostnames are `dutchess` and `ulster`. Follow the instructions in the AIX HACMP/6000 Installation Guide to define the cluster nodes to HACMP.

Step 23.3: Define Adapters to HACMP

In the sample scenario discussed in Planning, Volume 2, the service address is *dutchess.xyz.com*. The node *dutchess* has the boot address *dutchess_bt.xyz.com* and the node *ulster* has the boot address *ulster_bt.xyz.com*. The screens in the following figures show how the sample scenario adapters would be defined to HACMP. Refer to these figures as you follow the instructions in the AIX HACMP/6000 Installation Guide to define the adapters to HACMP.

```
Add an Adapter

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Entry Fields
* Adapter IP Label                                    dutchess_bt
* Network Type                                        ether                +
* Network Name                                        hacws_en0            +
* Network Attribute                                    public              +
* Adapter Function                                     boot                +
Adapter Identifier                                  129.40.60.21
Adapter Hardware Address
Node Name                                           dutchess               +
```

Figure 1. Adding an Adapter—Primary Boot Address

```
Add an Adapter

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Entry Fields
* Adapter IP Label                                    ulster_bt
* Network Type                                        ether                +
* Network Name                                        hacws_en0            +
* Network Attribute                                    public              +
* Adapter Function                                     boot                +
Adapter Identifier                                  129.40.60.22
Adapter Hardware Address
Node Name                                           ulster               +
```

Figure 2. Adding an Adapter—Backup Boot Address

```
Add an Adapter

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

Entry Fields
* Adapter IP Label                                    dutchess
* Network Type                                        ether                +
* Network Name                                        hacws_en0            +
* Network Attribute                                    public              +
* Adapter Function                                     service             +
Adapter Identifier                                  129.40.60.99
Adapter Hardware Address                            0x02608c2d2a10
Node Name                                                                  +
```

Figure 3. Adding an Adapter—Service Address. Note the Node Name field is blank, and the adapter hardware address field has been completed.

Step 23.4: Configure Network Modules

Follow the instructions in the *AIX HACMP/6000 Installation Guide*.

Step 23.5: Synchronize the Cluster Definition on All Nodes

Follow the instructions in the *AIX HACMP/6000 Installation Guide*.

Step 24: Configure the HACWS Application Server

Follow the instructions in Chapter 12 of the *AIX HACMP/6000 Installation Guide* to configure the HACWS application server. Use the following definitions:

Server Name (Specify a unique name)

Start Script **/usr/sbin/hacws/spcw_apps -ua**

Stop Script **/usr/sbin/hacws/spcw_apps -di**

Step 25: Define the Resource Group

Follow the instructions in Chapter 12 of the *AIX HACMP/6000 Installation Guide* to define the resource group.

Adding a Resource Group

Use the following options:

ENTER **hacws_group1** for Resource Group Name

SELECT **rotating** for Node Relationship

ENTER the node names of the primary control workstation and backup control workstation for Participating Node Names

PRESS **Do** to complete option selection.

Configuring a Resource Group

Use the following options:

ENTER the service addresses identified to HACMP for Service IP Label. You identified these service addresses to HACMP in "Step 23: Define the Cluster Environment" on page 100 (`dutchess` in Figure 3 on page 101).

This field can contain multiple network interfaces. You may have to type them out in order to get the SMIT screen to accept them all. You must have at least one network interface name matching the host name of the primary control workstation.

ENTER the name of your external file system for Filesystems (/**spdata** or /**spdata**/**sys1**).

ENTER the name of the volume group containing the /**spdata** or /**spdata**/**sys1** file system for Volume Groups.

ENTER the server name you used in "Step 24: Configure the HACWS Application Server" for Application Servers.

PRESS **Do** to complete option selection.

Complete the rest of the instructions in Chapter 12 of the *AIX HACMP/6000 Installation Guide*.

Step 26: Verify the Cluster and Node Environment

Follow the instructions in Chapter 13 of the *AIX HACMP/6000 Installation Guide* to verify the cluster and node environment.

Task E. Set Up and Test HACWS

This section describes the steps you take to customize HACWS and verify its function.

Step 27: Make Each Control Workstation Addressable by its Hostname

"Step 28: Set Up the HACWS Configuration" requires each control workstation be addressable by its hostname. If the name of the primary control workstation is *dutchess.xyz.com*, the backup control workstation must be able to communicate with the primary control workstation using the name *dutchess.xyz.com*. If the name of the backup control workstation is *ulster.xyz.com*, the primary control workstation must be able to communicate with the backup control workstation using the name *ulster.xyz.com*.

If either control workstation is not addressable by its hostname, you need to enter the appropriate **ifconfig** command to cause the required name to be temporarily configured as a network interface.

Note: Do not use SMIT for this step. Using SMIT causes the change to be permanent.

An example of an **ifconfig** command is as follows:

```
ifconfig en0 dutchess.xyz.com netmask 255.255.255.192 up
```

The **ifconfig** options you need to use are specific to your site. Refer to the **ifconfig** man page for more information.

Step 28: Set Up the HACWS Configuration

Configure the primary and backup control workstation as an HACWS configuration.

Note: Do this step from the primary control workstation.

If using:	Do this:.
SMIT	**TYPE** **smit hacws** • The High Availability Control Workstation Management window appears. **SELECT** **Install and Configure HACWS**. **ENTER** the node names of the primary control workstation and backup control workstation in the HOSTNAME fields. **SELECT** **yes** for Execute on both primary and backup?. **PRESS** **Do** to complete option selection and install HACWS.
install_hacws	Enter: `/usr/sbin/hacws/install_hacws -p \` *`primary_hostname`* `-b` *`backup_hostname`* `-s`

Step 29: Customize Cluster Event Processing

Identify the HACMP pre- and post-event scripts provided by HACWS to HACMP.

If using:	Do this:.
SMIT	**TYPE** **smit hacws** • The High Availability Control Workstation Management window appears. **SELECT** **Identify Event Scripts to HACMP**. **PRESS** Enter to continue.
spcw_addevents	Enter: `/usr/sbin/hacws/spcw_addevents`

If you want to further customize cluster event processing, follow the instructions in Chapter 5 of the *PSSP Administration Guide*.

Step 30: Add IP Address Aliases

In "Step 2: Plan Network Configuration" on page 89 you planned the network configuration for both control workstations. If your configuration requires IP address aliases, you need to provide the appropriate commands to HACWS. If these commands already existed somewhere else before you installed HACWS, remove them from the old location.

If you need to use an IP address alias to configure the hostname of the backup control workstation as a network interface, edit the **/etc/rc.backup_cw_alias** script on the backup control workstation. This script only runs on the backup control workstation. See the comments in the script for more details. If you make any changes to the **/etc/rc.backup_cw_alias** script, you must also edit the **/etc/rc.net** script so **/etc/rc.backup_cw_alias** runs when the backup control workstation boots. Use an editor to add the following line near the end of the **/etc/rc.net** file:

```
/etc/rc.backup_cw_alias
```

If you need to use an IP address alias to configure a network interface for an SP system partition, or if you need to configure an IP address alias on the active control workstation for some other reason, edit the **/spdata/sys1/hacws/rc.syspar_aliases** script. This script runs on the active control workstation before it starts the control workstation services. See the comments in the script for more details.

Step 31: Verify the HACWS Configuration

Verify the HACWS configuration.

If using:	Do this:.
SMIT	**TYPE** **smit hacws** • The High Availability Control Workstation Management window appears. **SELECT** **Verify HACWS Installation and Configuration**.
hacws_verify	Enter: `/usr/sbin/hacws/hacws_verify`

Step 32: Verify the Hardware Connections

Verify the connections between the backup control workstation and the frame. Run this step from the backup control workstation.

If using:	Do this:.
SMIT	**TYPE** **smit hacws** • The High Availability Control Workstation Management window appears. **SELECT** **Verify Frame to Control Workstation Cabling**.
spcw_verify_cabling	Type: `/usr/sbin/hacws/spcw_verify_cabling`

Step 33: Reboot Control Workstations

Reboot the primary control workstation. After it finishes booting, reboot the backup control workstation.

Step 34: Start Cluster Services on the Primary Control Workstation

Follow the instructions in Chapter 2 of the HACMP Administration Guide to start cluster services on the primary control workstation.

Using SMIT:

TYPE **smit clstart**

•The Start Cluster Services menu is displayed.

SELECT **now** for Start now option.

SELECT **true** for Startup Cluster Information Daemon? option.

PRESS **Do** to complete option selection.

Step 35: Verify HACWS Installation

To make sure you installed HACWS correctly, verify control workstation services exist and can move between the primary and backup control workstations.

Verify Control Workstation Services

Make sure control workstation services come up on the primary control workstation. Use the following procedure to test them:

1. Service addresses should be configured on the primary control workstation. Try to telnet to a service address.
2. /**spdata** should be mounted on the primary control workstation. To verify this, use the following command:

   ```
   df /spdata
   ```

3. The SDR should be available. To verify this, use the following command:

   ```
   /usr/lpp/ssp/bin/SDRGetObjects SP
   ```

The test is successful if you receive output. You can tell whether the startup of the control workstation services has completed by issuing the command:

```
grep  /tmp/hacmp.out SPCW_APPS COMPLETE
```

Once control workstation services have completely started on the primary control workstation, start cluster services on the backup control workstation by following the procedure described in “Step 34: Start Cluster Services on the Primary Control Workstation” on page 105.

Cause a Failover

After cluster services have started on the primary control workstation, direct HACMP to move control workstation services to the backup control workstation.

Using SMIT:

TYPE **smit clstop**

•The Stop Cluster Services menu is displayed.

SELECT **now** for Stop now option.

SELECT **takeover** for Shutdown mode option.

PRESS **Do** to complete option selection.

This should stop cluster services on the primary control workstation and move control workstation services to the backup control workstation. Make sure control workstation services move to the backup. On the backup control workstation, follow the procedure described in “Verify Control Workstation Services” on page 105.

When you are finished testing, restart cluster services on the primary control workstation by following “Step 34: Start Cluster Services on the Primary Control Workstation” on page 105.

Note: The first time you start control workstation services on the backup control workstation, the **spcw_apps** command runs and takes about a half hour to complete. You must wait for it to complete before you move control workstation services back to the primary control workstation. You can tell whether the **spcw_apps** command completed by issuing the following command:

```
grep  /tmp/hacmp.out SPCW_APPS COMPLETE
```

Once the startup of the control workstation services has completed on the backup control workstation, you can restart cluster services on the primary control workstation and then move control workstation services back to the primary control workstation. When you have completed testing, make sure to restart cluster services on both control workstations.

Chapter 4. Migrating to the Latest Level of PSSP

This chapter describes how you can migrate your system to PSSP 2.3 and AIX 4.2.1. Note that minimum PTF levels are recommended depending from where you migrate. Refer to the *Memo to Users* for information on required AIX file sets and PTFs.

Migrating your control workstation and nodes is a complex task. Thorough planning should be completed prior to attempting to migrate your SP to a new level of AIX and/or PSSP. The best technique for simplifying the complexity of the task is to divide the migration of your SP system into smaller steps, where you verify that each step was successfully completed before proceeding to the next step. This technique of simplifying the complexity of the task helps to ensure the successful completion of your migration, or if necessary, allows you to recover from unexpected problems should they arise.

High-Level Migration Steps

The process of migrating your system includes the following high-level steps. Read the high-level steps first, then refer to the appropriate section in this chapter to perform the actual steps. Once you perform the steps, refer back to this section to determine which step to address next.

Preparing to migrate

Preparing to migrate your system is a very important activity that you should not skip. It involves planning the migration carefully by examining your current configuration and the desired future configuration. Reading the migration information in the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment* is a prerequisite.

Refer to “Preparing to Migrate” on page 109.

Applying PTFs to nodes

Before migrating your control workstation, you must apply specific PTFs to any node at PSSP 2.2, PSSP 2.1, or PSSP 1.2. Refer to the *Memo to Users* for a list of required PTFs.

Migrating the control workstation to AIX 4.2.1 or later and PSSP 2.3

Prior to migrating any of your nodes, you must migrate your control workstation to the latest level of AIX and PSSP of any node you wish to serve. Therefore, if you plan to migrate any node to AIX 4.2.1 and PSSP 2.3, the control workstation must first be migrated to AIX 4.2.1 and PSSP 2.3.

To simplify the migration process, a "crossover" migration path from PSSP 2.2 to PSSP 2.3 has been provided. This allows you to separate the AIX migration from the PSSP migration and perform each operation in a timely manner. If your control workstation is currently at AIX 4.1.x and PSSP 2.2, you should first migrate just the AIX level on your control workstation to AIX 4.2.1 or later. Wait an appropriate amount of time for this to stabilize. Then, as a second step, migrate the control workstation from PSSP 2.2 to PSSP 2.3. This minimizes the risk you take when migrating your control workstation.

© Copyright IBM Corp. 1995, 1997

If your control workstation is currently at AIX 3.2.5 and PSSP 1.2 or AIX 4.1.x and PSSP 2.1, you must migrate your control workstation to both AIX 4.2.1 and PSSP 2.3 within the same service window.

To perform your control workstation migration, refer to “Paths to Migrate the Control Workstation to PSSP 2.3 and AIX 4.2.1” on page 115.

Partitioning your system, if necessary

When you read the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* and the Preparing to Migrate section is this chapter, one of the issues you needed to consider is whether you will need to partition your system. If you determined that you wanted to partition your system due to coexistence limitations, migration test purposes, or for any other reason, you should partition your system at this time. Refer to the System Partitioning chapter of the *PSSP System Administration Guide* for instructions on how to partition your system. Make sure your system is working correctly before continuing.

Refer to “Step 3: Understand System Partitioning Issues” on page 110 for more information.

Migrating a test node to AIX 4.2.1 and PSSP 2.3

If possible, you should migrate a single node (such as a test node) to AIX 4.2.1 and PSSP 2.3 before migrating all or a group of your nodes. This will allow you to gain experience with the migration, resolve any problem that might occur due to the migration, and help you determine how much time you will need to migrate all or a group of your nodes. You should use the control workstation as the boot/install server for this test node.

Refer to “Paths to Migrate the Nodes to PSSP 2.3 and AIX 4.2.1” on page 145 for more information.

Migrating the boot/install servers to AIX 4.2.1 and PSSP 2.3

You first must migrate the boot/install servers to the latest level of AIX and PSSP before you migrate the nodes they serve.

Refer to “Paths to Migrate the Nodes to PSSP 2.3 and AIX 4.2.1” on page 145 for more information.

Migrating the nodes to AIX 4.2.1 and PSSP 2.3.

Migrating the nodes is the final activity in the migration process.

Refer to “Paths to Migrate the Nodes to PSSP 2.3 and AIX 4.2.1” on page 145 for more information.

Performing Post-Migration Activity

This section discusses the activities you should perform after a successful migration. It also discusses recovery procedures you should perform if the migration process was not successful.

Refer to “Post-Migration Activity” on page 177 for more information.

Preparing to Migrate

Step 1: Read the RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment

Read the migration information in the *IBM RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment*. You should know the current system configuration and which nodes will reside in each system partition. You must know which boot/install server nodes will service the SP nodes. You should have worksheets that define the boot/install information for each node that is being migrated to PSSP 2.3.

Generally, completing the configuration worksheets found in the planning manual is not necessary when migrating. However, if you are going to use partitioning or coexistence to implement your migration strategy, you may find completing the worksheets helpful.

Step 2: Understand Coexistence Issues with PSSP 2.3

PSSP 2.3 supports multiple levels of AIX and PSSP in the same system partition. This function provides additional migration and upgrade flexibility. Installations that may benefit from coexistence include those running diverse application workloads and those planning to add new nodes to existing production systems. For more information to determine if coexistence is appropriate for your installation, refer to the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide*. Note that minimum service levels are required for coexistence support. See the Memo to Users for the most up-to-date information on service levels. PSSP 2.3 and AIX 4.2.1 must be installed on the control workstation to support coexistence configuration for SP nodes at PSSP 2.3.

Supported Coexistence Configurations

PSSP 2.3 provides support for coexistence of SP nodes running at different levels of PSSP in the same system partition, thus building on the PSSP 2.2 introduction of that mechanism. Remember, that an unpartitioned system is viewed as having one default system partition. As in PSSP 2.2, all the combinations of the PSSP levels are supported **except** the one allowing nodes with PSSP 1.2 and PSSP 2.1 to run in the same system partition.

The following levels of PSSP are supported in a system partition:

- PSSP 1.2 and PSSP 2.2
- PSSP 2.1 and PSSP 2.2
- PSSP 1.2, PSSP 2.2, and PSSP 2.3
- PSSP 2.1, PSSP 2.2, and PSSP 2.3
- PSSP 1.2 and PSSP 2.3
- PSSP 2.1 and PSSP 2.3
- PSSP 2.2 and PSSP 2.3

Each PSSP level corresponds to a supported level of AIX. Note that PSSP 1.2 and PSSP 2.1 continue to be supported in the same system, but they must be in separate system partitions. The result of subsequent repartitioning is subject to the same restrictions and considerations.

Coexistence and Related LPPs

Restrictions exist for some of the Licensed Program Products (LPPs) and PSSP components when coexisting in the same system partition. If you are running any of the following LPPs or PSSP components on your system, refer to the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment*. for more information.

- VSD and IBM Recoverable VSD (RVSD)
- LoadLeveler
- PIOFS, CLIO/S, NetTAPE
- General Parallel File System (GPFS)
- Parallel Application Products (such as PESSL, PVME, PE)
- High Availability Group Services API (GSAPI)
- The Switch (CSS) Support
- Extension node Support

Tuning

Note that there may be tuning considerations with regard to coexistence. Consider the other characteristics that influence performance for your specific configuration, making trade-offs if necessary. Then, as with any performance tuning strategy, make refinements based on your results or as your migration strategy progresses. Refer to the *PSSP Administration Guide* for more information on tuning.

Step 3: Understand System Partitioning Issues

There are two reasons why you may want to create one or more system partitions. First, as an option, you can create a production system partition with your current AIX and PSSP level software and a test system partition with AIX 4.2.1 and PSSP 2.3 level software. In this way, you can test AIX 4.2.1/PSSP 2.3 while running your existing AIX/PSSP production environment.

Second, you may also want to partition your system due to coexistence limitations.

For more information on system partitions, consult the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment* and the *PSSP Administration Guide*.

Step 4: Verify Control Workstation Requirements

Ensure that the following requirements are met for the control workstation:

- Refer to the *Memo to Users* for the latest information on supported AIX release and PTF levels.
- Install adequate serial ports and RS-232 cables to support all frames.
- Allocate adequate disk space for rootvg, paging, and installation. IBM requires a minimum of 4 GB of DASD made available on the control workstation. IBM suggests allocating 2 GB for rootvg, and 2 GB for the /spdata file system. If you plan to support mixed levels of PSSP and AIX, you may require more than 2 GB of /spdata file system.
- Ensure that all host names and IP addresses are resolvable on the control workstation. You should not change them for the duration of the migration.

- You must run all migration tasks from root on the control workstation. IBM suggests that you add the following directory paths in your .profile to avoid incomplete path names:

  ```
  /usr/lpp/ssp/bin
  /usr/sbin
  /usr/bin
  /usr/lpp/ssp/kerberos/bin
  ```

  The following is an example of root user path in the .profile.

  ```
  PATH=/usr/lpp/ssp/bin:/usr/sbin:/usr/lpp/ssp/kerberos/bin:/usr/bin
  ```

Step 5: Verify Boot Install Server Requirements

Ensure that the following requirements are met for the boot/install server(s):

- If there will be any nodes remaining at PSSP 1.2, you must have a boot/install server for those nodes prior to any migration. IBM suggests that you have at least two PSSP 1.2 boot/install servers.
- The boot install server node must be at the highest level of AIX and PSSP to which it will serve.
- Allocate adequate disk space for rootvg on the boot/install server nodes taking into consideration the size of your mksysb image(s), the pssp.installp image(s), and SPOT resources.

Step 6: Reserve Port Numbers

Some of the subsystems managed by the Syspar Controller (syspar_ctrl) allocate port numbers from the range 10000 to 10100, inclusive. Therefore, if any customer subsystem, such as DB2, uses port numbers in this range, such port numbers must be reserved in /**etc**/**services**. For details, refer to Appendix G, “Reserving Ports” on page 245.

Step 7: Back Up Your Control Workstation

Before you migrate your system, you should always make a backup of your existing system. The following list provides you with a basic set of instructions for backing up your system:

1. Create a mksysb image of your existing root volume group of the control workstation using one of the following commands:
   - mkszfile and mksysb - Used with AIX 3.2.5 systems
   - mksysb - Used with AIX 4.x systems
   - smit mksysb - Supported SMIT interface

   For example:

   ```
   /bin/mksysb -i /dev/rmt0
   ```

2. Backup files and file systems with critical data

   You should keep backup copies of critical files and file systems that have configuration data in them. For example, you should backup the /spdata file system. Use the **tar** command to save critical files and use the **backup** command to save file systems.

Command	Example
tar	`/bin/tar -cvf /dev/rmt0 <files>`
backup	`/usr/sbin/backup <file_system>`

For AIX 4.1 and later systems, you may choose to backup the volume group by issuing the **savevg** command. For example, to save the spdatavg volume group, you could issue the following command:

```
savevg -f /dev/rmt0 -i spdatavg
```

3. Export Non-Root Volume Groups

   You may want to export your non-root volume groups immediately prior to the AIX migration. This will undefine the volume group from the system during the AIX migration. For example, you may want to export the spdatavg volume group by issuing the following commands:

   ```
   umount      /spdata   (unmount the file system)
   varyoffvg   spdatavg  (vary off volume group)
   exportvg    spdatavg  (export volume group)
   ```

   Once the AIX migration is complete, you will need to import any volume group that you previously exported. For example, to import the spdatavg volume group, issue the following command:

   ```
   importvg -y spdatavg -V <major #> <hdisk>
   ```

   Note: If you are migrating from AIX 3.2.5 to AIX 4 and you exported any non-rootvg volume groups, once you import your non-rootvg volume groups using AIX 4, you will not be able to return back to AIX 3.2.5 and reimport these non-rootvg. Therefore, ensure that you back up all non-rootvg prior to migrating AIX.

4. Verify Your Backups

   Whether you made the backup to a file or a tape, verify that the file exists on the medium.

Step 8: Back Up Your Nodes

After backing up the control workstation in the last step, you should make a backup of your nodes. The following list provides you with a basic set of instructions for backing up your nodes.

1. Create a mksysb image file of your node. You must save the mksysb file to a tape, media, or to a file system on another workstation, using one of the following commands:
   - mkszfile and mksysb - Used with AIX 3.2.5 systems.
   - mksysb - Used with AIX 4.x systems
   - smit mksysb - Supported SMIT interface
2. Verify your backups. Whether you make the backup to a file or a tape, verify that the file exists on the medium.

Step 9: Archive the System Data Repository (SDR)

If you have a PSSP 2.1 or later system, you should archive the SDR at its current level by issuing the **SDRArchive** command:

```
SDRArchive <append_string>
```

where <append_string> is the name you want to use for this archive. If you specified the <append_string>, it is appended to the name of the backup file **/spdata/sys1/sdr/archives/backup.JULIANdate.HHMM.appendstring**.

Step 10: Quiesce Your System

Be sure to quiesce your system as follows:

- All users are logged off nodes
- No jobs are running
- Batch submission queues, such as LoadLeveler queues, should be shutdown or quiesced and the migrating node should be removed from the queue.
- Quiesce the High Performance Switch or SP Switch
- LoadLeveler Interactive Session Support should not be routing interactive traffic.
- The Resource Manager should be stopped.
- Crontab files should be inspected and processes that could start during the migration should be disabled from starting.
- Jobs started via the **at** command or any other job initiator command should be disabled from starting.
- If local applications have been enabled by adding entries into the **/etc/inittab** file, consider preventing these applications from automatically starting up during the migration.

  Note: When migrating from AIX 3.2.5 to AIX 4.x, **/etc/inittab** is replaced. Your AIX 3.2.5 file is saved in **/tmp/bos/etc/inittab**.

Step 11: Understand Amd/Automount Issues

PSSP 2.3 replaces its use of the public domain Amd automount daemon with the AIX automount daemon, which is available as part of NFS in the Network Support Facilities of the AIX Base Operating System (BOS) Runtime. Amd uses map files to define the automounter control. These map files are not compatible with the AIX automounter and must be converted.

If your current installation has the Amd configuration turned on and is using the SP User Management Services (SP site environment variables *amd_config* and *usermgmt_config* are both **true**), the PSSP maintains a user home directory map file for the **/u** file system. The PSSP System Management Software will automatically convert the **/etc/amd/amd-maps/amd.u** map file for you when migrating to PSSP 2.3.

If you have modified the **/etc/amd/amd-maps/amd.u** Amd map file, added your own map files, or in any other way customized your Amd installation, you will need to consider the impact of the automounter conversion in planning your migration to PSSP 2.3. You will need to manually convert your Amd map files to AIX Automount map files. Refer to the AIX publications for information on the AIX automounter and

map file format. Also, refer to the Automount chapter in the *PSSP System Administration Guide* for more information.

Step 12: Understand Print Management Issues

The SP Print Management System is removed from PSSP 2.3. That is, the SP Print Management System cannot be configured on nodes running PSSP 2.3. IBM suggests the use of Printing Systems Manager (PSM) for AIX as a more general solution to managing printing on the SP system.

However, if you are running earlier versions of PSSP on some of your nodes, the SP Print Management System is still supported on those nodes. The **print_config** routine running on the control workstation will configure the SP Print Management System on nodes running versions of PSSP earlier than PSSP 2.3.

Step 13: Understand System Reconfiguration Issues

Note that you should not reconfigure your system in any way during the migration process. For example, do not add a frame, switch, node, or any other piece of hardware to your system until after the migration process has completed. In addition, you should not add or delete any hostnames or IP addresses until after the migration process has completed. This will help to ensure a successful migration. For more information on reconfiguring your system, refer to Chapter 5, “Reconfiguring the RS/6000 SP System” on page 181.

Step 14: Understand Virtual Shared Disk (VSD) Issues

If you are migrating from PSSP 1.2 or PSSP 2.1 to PSSP 2.3, you must first deinstall VSD code. Also, refer to *IBM Parallel System Support Programs for AIX: Managing Shared Disks*, SA22-7279 for additional information.

Paths to Migrate the Control Workstation to PSSP 2.3 and AIX 4.2.1

After preparing to migrate, you now need to migrate the control workstation to AIX 4.2.1. Once you have migrated the AIX level, you then migrate the PSSP level.

Keep in mind that you should always make a mksysb of your control workstation before proceeding with the migration process. For information on making a mksysb, refer to "Step 7: Back Up Your Control Workstation" on page 111.

You need to select the control workstation migration procedure that is most appropriate for your environment. Your choice of procedures is based on the current AIX and PSSP level of the control workstation. You also have choices on the method used to migrate the AIX level to AIX 4.2.1. The following list identifies the supported migration choices:

- **Migration Install (BOS/Migration Install)**

  This method preserves all file systems except /tmp, as well as the root volume group, logical volumes, and system configuration files. This method migrates the control workstation using AIX media (tape, CDROM) or NIM software. IBM suggests using AIX BOS Migration Installation when migrating AIX versions or releases (for example, AIX 4.1.4 to AIX 4.2.1).

- **BOS Overwrite/Preservation Install**

  You will need to save many of the PSSP related files when choosing to do this type of migration since the rootvg / (root), /var, and /usr file systems will be recreated. The majority of the files deal with the SDR, installation, and authentication files working with Kerberos database. For more information refer to "Perform Control Workstation Overwrite/Preservation Install" on page 158.

  You may choose this method if you want to clean up files in rootvg.

- **Upgrade**

  For AIX 4.2.0 based systems, you should install the AIX PTF service for AIX 4.2.1. The application of PTF service is similar to a BOS migration, where rootvg is preserved. IBM suggests installing PTF service when upgrading AIX modification levels. You do have the choice to execute a BOS Overwrite installation, but you should install PTF service whenever available.

  The option of applying the PTFs apply only when migrating to PSSP 2.3 from PSSP 2.2 where the AIX level is 4.2.0.

  You need to install the latest AIX 4.2.1 service to support PSSP 2.3. This requires you to install the AIX PTFs by issuing the **installp** command. You may install the AIX PTFs directly from media (tape or CD-ROM) or you can load the required PTFs into the lppsource directory, then install from the lppsource directory.

The following table identifies the supported migration paths. First determine your starting point by selecting the AIX and PSSP level of your current system. Then select the appropriate method from the **Installation Method Choice** column. This choice is used later during the migration steps. Finally, refer to the appropriate section in this chapter and follow the steps to migrate the nodes.

Table 7. Migration paths for control workstation.

AIX Starting Point	PSSP Starting Point	Target Point	Installation Method Choice	Refer to:
AIX 3.2.5	PSSP 1.2	AIX 4.2.1, PSSP 2.3	Migration Install Overwrite/Preservation Install	“Migrate the Control Workstation from PSSP 1.2 to PSSP 2.3” on page 117
AIX 4.1.3 AIX 4.1.4 AIX 4.1.5	PSSP 2.1	AIX 4.2.1, PSSP 2.3	Migration Install Overwrite/Preservation Install	“Migrate the Control Workstation from PSSP 2.1 to PSSP 2.3” on page 126
AIX 4.1.4 AIX 4.1.5	PSSP 2.2	AIX 4.2.1, PSSP 2.2 AIX migration only.	Migration Install	“Migrate the Control Workstation from PSSP 2.2 to PSSP 2.3” on page 136 Do steps 1 - "Verify AIX Migration" Step.
AIX 4.2.0	PSSP 2.2	AIX 4.2.1, PSSP 2.2 AIX migration only.	Upgrade	“Migrate the Control Workstation from PSSP 2.2 to PSSP 2.3” on page 136 Do steps 1 - "Verify AIX Migration" Step.
AIX 4.1.4 AIX 4.1.5	PSSP 2.2	AIX 4.2.1, PSSP 2.3	Migration Install Overwrite/Preservation Install	“Migrate the Control Workstation from PSSP 2.2 to PSSP 2.3” on page 136
AIX 4.2.0 AIX 4.2.1	PSSP 2.2	AIX 4.2.1, PSSP 2.3	Upgrade	“Migrate the Control Workstation from PSSP 2.2 to PSSP 2.3” on page 136
AIX 4.2.1	PSSP 2.3	AIX 4.2.x, PSSP 2.3 AIX migration only.	Upgrade	“Migrate the Control Workstation from PSSP 2.2 to PSSP 2.3” on page 136 Do steps 1 - "Verify AIX Migration" Step.

Note: If you are migrating your HACWS, refer to “HACWS Migration Strategy” on page 164.

Migrate the Control Workstation from PSSP 1.2 to PSSP 2.3

Follow the steps in this section if you have chosen to migrate the control workstation from PSSP 1.2 to PSSP 2.3.

Step 1: Prepare AIX 3.2.5 Boot/Install and /usr Servers

This step is required if any nodes will remain at AIX 3.2.5 and PSSP 1.2.

Select one of the remaining PSSP 1.2 nodes to act as the new boot/install server for other PSSP 1.2 nodes. You will need to have at least one node that can support the reinstallation or customization at PSSP 1.2 levels in case of hardware or software failures. This is because the upgraded control workstation at PSSP 2.3 does not support the PSSP 1.2 node installation code.

IBM suggests that you first create a new AIX mksysb image of one of the current PSSP 1.2 nodes. This PSSP 1.2 node should have all of the necessary LPPs and PTFs that have been listed as required to support the PSSP 2.3 control workstation. You may issue the **mkszfile** command or use **smit mksysb** to create the new AIX mksysb image file. This mksysb image does not contain a bootable image as part of mksysb.

You should then copy the new mksysb image file to the control workstation directory /**usr**/**sys**/**inst.images**/**ssp** as bos.obj.xxx.yyy (install image name). It is now necessary to update the SDR to reflect the new boot/install server information using the **spbootins** command. To reference the new mksysb installation image name, and a new boot/install server for the SP nodes issue the following:

```
spbootins -i <install_image_name> -n <boot_server_node_number> \
-l <node_list>
```

The **spbootins** command updates the SDR on the control workstation and executes the **setup_server** command on the target boot/install node. This command properly sets up the PSSP 1.2 installation code on the new boot/install node.

IBM suggests that you create a second boot/install server in the production system partition as a backup to the primary boot/install server. If you don't have a second boot/install server, ensure that you have a mksysb image of the boot/install server and have an alternate way of backing up the boot/install server.

To change the boot/install server for a group of nodes, use the following command:

```
spbootins -n boot_server_node_number -l node_list
```

This causes the node indicated by *boot_server_node_number* to become the boot/install server for the nodes in *node_list*.

Caution: When you migrate the last boot/install server PSSP 1.2 node to PSSP 2.3, the server resources (mksysb images, ssp.installp) are deleted from the node. You should backup the PSSP 1.2 server node prior to executing the node migration in case you want to restore back to the PSSP 1.2 environment for the node.

Using /usr Clients

If you are using /**usr** clients, you may have some additional preparation work. If some of the nodes you select for the test partition are /**usr** clients, their designation in the SDR as /**usr** clients must be changed before you apply the system partition configuration. If you try to change the attribute after the partition configuration is applied, **spbootins** sends a message that /**usr** clients are not supported in a PSSP 2.3 partition.

To change the attribute, issue the following command before you apply the system partition configuration:

```
spbootins -u local -l node_list
```

where *node_list* is a list of the /**usr** client nodes moving to the PSSP 2.3 system partition.

Note: You cannot migrate nodes that are /usr clients. You must change the /usr server to local for the nodes using the previous command and then do a complete reinstall of AIX and PSSP in order to upgrade them.

Step 2: Prepare to Migrate and Verify Requirements

Before beginning, refer to “Preparing to Migrate” on page 109 for information on verifying control workstation requirements and quiescing your system.

Step 3: Migrate to AIX 4.2.1

You need to upgrade the control workstation to AIX 4.2.1. Determine which of the following methods you want to follow based upon the information described at the beginning of this chapter:

BOS Migration Install: The control workstation is currently at AIX 3.2.5. Use this method to preserve the current files in the / (root), /var, /usr, and user based file systems. For more information, see “Step 3a: Perform Control Workstation BOS Migration Install” on page 119.

BOS Overwrite Install: You may choose to reinstall the control workstation to AIX 4.2.1. This method does not preserve the files in the / (root), /var, /usr, and user file systems and it requires multiple steps to first save, and then later restore necessary PSSP files. See “Step 3b: BOS Overwrite Install” on page 119.

Notes:

- Reference the /**.klogin** file on the control workstation to make sure that the (rcmd) principal for the control workstation has been included.

  .klogin file of the Kerberos Administrative Principal in PSSP 2.3 contains an entry not always included in the PSSP 1.2 **.klogin** file. If the entry is not already part of your Kerberos Administrative Principal's **.klogin** file, add it now.

  If the **.klogin** file of the Administrative Principal has no remote command (**rcmd**) principal for the control workstation, add one. For example, suppose your control workstation is `spctrl`, your authentication realm is `XYZ.ABC.COM`, and root is your Kerberos Administrative Principal. In this example, you would add the following line to /**.klogin**:

  ```
  rcmd.spctrl@XYZ.ABC.COM
  ```

- If you executed the **inurid -r** command, some data would have been removed from the **/usr/lpp/ssp/inst_root** directory. This means that the system cannot be used as a SPOT server, which, in turn, does not allow the control workstation to become a NIM master for installing the nodes.

  After installing the AIX 4.2.1 BOS Product on the control workstation, check to see if the **inurid -r** command was run by issuing:

  /usr/lib/instl/inurid -q ; echo $?

  If the return code=1, the control workstation needs to be reinstalled with an image without the **inurid -r** command being run. Some possible reasons which may have caused the **inurid -r** command to be run include:

  - The control workstation was installed with a non-mksysb NIM installation with a bosinst resource which had the RM_INST_ROOT variable set to yes.
  - The control workstation was installed with a mksysb image that had **inurid -r** command run on it prior to the creation of the image.
  - The **inurid -r** command was issued on this system manually.

Step 3a: Perform Control Workstation BOS Migration Install

This method preserves all file systems except /tmp, as well as the root volume group, logical volumes, and system configuration files. This activity provides installp updates and installs necessary AIX LPPs to the control workstation. You must have all the necessary AIX file sets and PTFs listed in the *Memo to Users* available by CD-ROM, tape, or from the NIM master.

Refer to the AIX Installation Guide in chapters 1-3 for more information. The following list provides some hints:

- Boot off your AIX CD-ROM or tape or setup the control workstation as a NIM client from an AIX 4.2.1 NIM master.
- Select option 2 "Change/Show Installation Settings and Install". Always verify that it has been set to *migrate* and that the correct target disk is assigned for root volume group.
- Select option 1 "System Settings" on Installation and Settings menu
- Select option 3 "Migration Install" on the Change Method of Installation menu.
- Select the proper hdisk(s) being used for rootvg. You may want to update the hdisk configuration for the control workstation.
- Customize your control workstation based on the documented PSSP requirements. This includes required AIX LPPs and PTFs being installed.

Step 3b: BOS Overwrite Install

See “Perform Control Workstation Overwrite/Preservation Install” on page 158 for instructions.

After completing that procedure, proceed to “Step 4: Verify AIX Migration” on page 120.

Step 4: Verify AIX Migration

Verify that the control workstation has successfully been migrated to AIX 4.2.1 by issuing the following command:

```
oslevel
```

If the output of this command does not indicate AIX 4.2.1, issue the following command to return a list of AIX files not migrated to AIX 4.2.1. You may need to install AIX PTFs to migrate those file sets to AIX 4.2.1.

```
oslevel -l 4.2.1.0
```

Step 5: Verify Control Workstation Interfaces

Verify the configuration for each Ethernet adapter in the control workstation by *pinging* its IP address and seeing if you get a response. For example:

```
ping -c 1 129.33.34.1
```

Reconfigure the adapter if you did not receive a response.

Changing User Process Limits

When you first install your system, the number of processes the root user can have is set to **40**, an AIX 4.2.1 default. You will not be able to continue installing your system with this default value—you must increase the number to 256.

To change the value, enter the following command:

```
chdev -l sys0 -a maxuproc='256'
```

Tunables and Tunable Values

You need to validate the network tunables on the control workstation. Use the **no** command to view and change the network values. To list the values, enter:

```
/usr/sbin/no -a
```

To modify the value of **thewall**, enter:

```
/usr/sbin/no -o thewall=16384
```

The following are the PSSP defaults you should use:

```
thewall          16384
sb_max          163840
ipforwarding         1
tcp_sendspace    65536
tcp_recvspace    65536
udp_sendspace    32768
udp_recvspace    65536
tcp_mssdflt       1448
```

You need to update the /**etc**/**rc.net** file so that these changes will take affect.

Step 6: Define Space for NIM Boot Images

Before creating an AIX 4.2.1 boot/install server, ensure that there is sufficient space in the root (/) file system or create a separate file system for /**tftpboot** to manage the space required for the boot images (approximately 25 megabytes per lppsource level supported) created by NIM.

Step 7: Define Space for the /spdata Directory

You need to define a large amount of disk space to be allocated for the /spdata file system. IBM suggests disk space of 2 GB, and that you place the spdata file system into its own volume group (spdatavg). The following are steps required to create a separate volume group, and the spdata file system.

Create the spdata volume group named **spdatavg** on 2 GB hdisk1, then vary on the new spdata volume group.

```
mkvg -f -y spdatavg  hdisk1
varyonvg spdatavg
```

Create the logical volume named **spdata_lv** for 2 GB. The number of logical partitions is based on a physical partition size of 4Meg.

```
mklv  -y spdata_lv -x 512 spdatavg 512
```

Create the /spdata file system using the logical volume **spdata_lv**, and then mount the /spdata file system on control workstation.

```
crfs -v jfs -d spdata_lv -m /spdata -A yes -p rw -t no
mount /spdata
```

Refer to “Step 13: Define Space for the /spdata Directory” on page 20 for more information.

Step 8: Create Required /spdata Directories

You need to create the proper PSSP directory structure for PSSP 2.3 by creating the following directories:

- mkdir -p /spdata/sys1/install/images

  This is the location of all required AIX mksysb images.

- mkdir /spdata/sys1/install/pssp

  This is the location of NIM configuration data files.

- mkdir -p /spdata/sys1/install/<name>/lppsource

  This is the location of required AIX 4.2.1 file sets.

- mkdir -p /spdata/sys1/install/pssplpp/PSSP-2.3

  This is the location of installp file sets for the code version PSSP 2.3. If the control workstation will be the NIM server for nodes at other PSSP code levels, other subdirectories will be created under pssplpp with the code versions for those levels.

Note: Make sure you mount the new /**spdata** file system before you create the /**spdata** directories.

Step 9: Copy the AIX 4.2.1 LPP Images

You must copy all required AIX 4.2.1 based file sets (LPPs) into the /**spdata**/**sys1**/**install**/<**name**>/**lppsource** directory on the control workstation. This includes the **xlC.rte**, **perfagent**, most of the **bos**, some of the **X11**, and all of the **devices** file sets. You also need to copy any AIX PTFs that were listed in the *Memo to Users* to the lppsource directory. You can use the **bffcreate** command to copy the LPPs.

```
bffcreate -qvX -t /spdata/sys1/install/<name>/lppsource \
-d /dev/rmt0 all
```

Create a **toc** file by issuing the following command:

```
inutoc /spdata/sys1/install/<name>/lppsource
```

Step 10: Verify (Install/Copy) Correct Level of PAIDE (perfagent)

The Performance Toolbox for AIX, Agent Component (PAIDE) is required starting with PSSP 2.2. The correct level of AIX PAIDE (perfagent) needs to be installed on the control workstation and copied to the lppsource directory. The level of perfagent required is dependent upon the level of AIX:

- AIX 4.1.4 - perfagent 2.1.4.x
- AIX 4.1.5 - perfagent 2.1.5.x
- AIX 4.2.0 - perfagent 2.2.0.x
- AIX 4.2.1 - perfagent 2.2.1.x

For more details regarding PAIDE, refer to the *Memo to Users*.

If the correct level of perfagent is not installed on the control workstation, it needs to be installed at this time. To verify whether the correct level of perfagent is installed on the control workstation, issue the following command:

```
lslpp -l perfagent.server
```

The correct level of perfagent must also be copied to the lppsource directory. You now need to copy the correct level of perfagent to the lppsource directory associated with the corresponding level of AIX (for example, perfagent 2.2.1.x for AIX 4.2.1).

Step 11: Copy the PSSP Images

The RS/6000 SP package consists of several file sets which must be copied into the **/spdata/sys1/install/pssplpp/PSSP-2.3** directory using the **bffcreate** command. Then, rename the pssp package to **pssp.installp** and create the .toc file.

```
bffcreate -qvX -t /spdata/sys1/install/pssplpp/PSSP-2.3  -d /dev/rmt0 all
cd /spdata/sys1/install/pssplpp/PSSP-2.3
mv  ssp.usr.2.3.0.0 pssp.installp
inutoc .
```

Refer to “Step 16: Copy the PSSP Images” on page 26 for complete instructions.

Step 12: Install (Copy) the Basic AIX (mksysb) Image

The RS/6000 SP media provides a basic AIX 4.2.1 minimal image. You need to properly load in the base AIX 4.2.1 mksysb image to the **/spdata/sys1/install/images** directory using the **installp** command. You then may remove any mksysb images you no longer need.

```
installp  -aXd  /dev/rmt0.1  spimg
```

Refer to “Step 17: Copy a Basic AIX (mksysb) Image” on page 27 for more information.

Step 13: Install PSSP on the Control Workstation

You now need to install the PSSP 2.3 level code on the control workstation. The PSSP 2.3 file sets are packaged to be installed on top of previously supported releases. IBM suggests that you install all file sets made available in the pssp.installp package using the **installp** command.

```
installp  -aXd /spdata/sys1/install/pssplpp/PSSP-2.3/pssp.installp all
```

Step 14: Authenticate as the Administrative Principal

Issue the **kinit** command to properly authenticate as the administration user to the Authentication database.

```
/usr/lpp/ssp/kerberos/bin/kinit  <admin_user>
```

where <admin_user> is the name of the administrator. For default SP Kerberos based systems *root.admin* is the Kerberos administrator.

Note: If the PSSP Authentication services was not properly restored, you must run **setup_authent** to recreate your Kerberos database. You then need to *customize* all older PSSP nodes to distribute the new krb-srvtab files to the nodes. This is accomplished using the **spbootins -r customize** command in a later step.

Step 15: Complete PSSP Installation on the Control Workstation

To properly setup the PSSP 2.3 control workstation for SDR, Hardmon, and other SP related services, issue the following command:

```
install_cw
```

Step 16: Run SDR and System Monitor Verification Test

In this step, run verification tests that check for correct installation of the SDR, correct installation and configuration of the System Monitor.

```
SDR_test (SDR verification)
spmon_itest (SP mon verification)
```

It may be necessary to reinitialize the SP frame connection to the SDR by issuing the **spframe** command to reset the hardmon connection.

```
spframe -r yes 1 1 /dev/tty0
```

Step 17: Configure PSSP Services and Set Up Site Environment

You must set the proper LPP source name variable **cw_lppsource_name** to the appropriate name. This name is based on the <name> directory you selected in directory /**spdata**/**sys1**/**install**/<**name>**/**lppsource**. The <name> environment is set to the string *default*. To change **cw_lppsource_name** or other site environment variables, issue:

```
spsitenv cw_lppsource_name=<name>
```

The system management environments on the control workstation are started by running **services_config**. Issue the following command:

```
/usr/lpp/ssp/install/bin/services_config
```

If the Site Environment variable **amd_config** is set to true, **services_config** will configure automounter directories and files. If the Site Environment variable

usermgmt_config is also set to true, the file **/etc/auto/maps/auto.u** will be created to control the **/u** file system containing user home directories. Since the use of Amd has been replaced with the AIX automount daemon in PSSP 2.3, **services_config** will automatically convert the existing **/etc/amd/amd-maps/amd.u** map file to **auto.u**. If you had an **amd.u** map file that was not generated by PSSP, or if you had modified the entries in that file in any way, this conversion process may fail. See the Managing the Automounter chapter in the *PSSP Administration Guide* for more details on the migration conversion process and what to do fails.

If you had other file systems that were under Amd control, you may wish to convert those map files at this time. See the Managing the Automounter chapter in the *PSSP Administration Guide* for more details on managing other file systems with the automount daemon.

Step 18: Start System Partition-Sensitive Subsystems and Verify

There are system partition-sensitive subsystems that you need to add to the system. Even if you are not partitioning your system, you need to do this since you still have one default partition. Do the following:

1. Remove old subsystems (for example, hr, hb) by issuing the following command:

   ```
   syspar_ctrl -c
   ```

2. Add new subsystems (for example, hats, hags) by issuing the following command:

   ```
   syspar_ctrl -A -G
   ```

To verify that the System Partition Sensitive Subsystems have been properly started, refer to “Step 34: Verify System Partition-Sensitive Subsystems Have Started” on page 55.

Step 19: Start Quiesced Applications

Any of the applications that you quiesced prior to migrating your control workstation should be started now if they have not already been automatically started. For example, if you have a switch, issue the following command to restart your switch:

```
Estart
```

Step 20: Configure Control Workstation as Boot/Install Server

Verify that the SDR node attribute value for **code_version**, **lppsource_name**, and **next_install_image** are appropriately set. Issue the following command:

```
splstdata -b -G
```

- Each node's PSSP **code_version** should be set to the level of PSSP currently installed on the node.
- Each node's **lppsource_name** should indicate the level of AIX currently installed on the node. The **lppsource_name** value must correspond to the directory name where you chose to place the lppsource files in **/spdata/sys1/install/**<**name**>**/lppsource** (for all nodes running PSSP-2.1 or greater).
- Each node's **install_image** should indicate the mksysb image that is installed on the node. Each mksysb image should be stored in the directory **/spdata/sys1/install/images** except for AIX 3.2.5/PSSP 1.2 node mksysb

images which should be stored in the directory **/usr/sys/inst.images/ssp**. If the value is *default* then verify the SDR Syspar and SP attribute value for **install_image** is appropriately set.

If necessary, you can issue the **spbootins** command to change the node's attribute values or **spsitenv** command to change SP attribute values. Issue the appropriate command specifying the options associated with the attributes that you want changed:

```
spbootins -s no -p <code_version> -i <install_image_name> \
-v <lppsource_name> -l <node_list>
```

```
spsitenv install_image=<install_image_name>
```

The **setup_server** command must be run to properly set up NIM on the control workstation by issuing the command:

```
setup_server 2>& | tee /tmp/setup_server.out
```

The output will be saved in a log file called **setup_server.out**. This may take a while since it will be creating the NIM master.

Step 21: Run Verification Tests

You should validate that the PSSP 2.3 software has been properly installed on the control workstation by issuing the following commands:

```
SYSMAN_test
spmon_ctest
CSS_test                * run only if you have a switch
spverify_config         * run only if your system is partitioned
jm_install_verify       * run only if using Resource Manager
jm_verify               * run only if using Resource Manager
```

Verify **host_responds** and **switch_responds**, if you have a switch, are set to *yes* by issuing the following command:

```
spmon -d -G
```

Step 22: Validate the Control Workstation

Your control workstation should now function at PSSP 2.3 level. All PSSP 2.2, PSSP 2.1, and PSSP 1.2 nodes should now be able to communicate to the PSSP 2.3 control workstation, if the proper level of PTF service has been applied to the PSSP nodes.

There are occasions based on customer changes made to the SDR and Authentication services, that may require the PSSP nodes to be rebooted and possibly recustomized by the boot/install server (BIS) nodes.

You can now add other AIX, PSSP, and customer owned LPPs and files on to the control workstation. Be careful to make sure that older applications and LPPs will work properly with AIX 4.2 and PSSP 2.3.

Note: At this point, refer back to “High-Level Migration Steps” on page 107 to determine your next step in the migration process.

Migrate the Control Workstation from PSSP 2.1 to PSSP 2.3

Follow the steps in this section if you have chosen to migrate the control workstation from PSSP 2.1 to PSSP 2.3.

Step 1: Prepare to Migrate and Verify Requirements

Before beginning, refer to “Preparing to Migrate” on page 109 for information on verifying control workstation requirements and quiescing your system.

Step 2: Migrate to AIX 4.2.1

You need to upgrade the control workstation to AIX 4.2.1. Determine which of the following methods you want to follow based upon the information described at the beginning of this chapter:

BOS Migration Install: The control workstation is currently at AIX 4.1.x. Use this method to preserve the current files in the / (root), /var, /usr and user based file systems. For more information see “Step 2a: Perform Control Workstation BOS Migration Install” .

BOS Overwrite Install: You may choose to reinstall the control workstation to AIX 4.2.1. This method does not preserve the files in the / (root), /var, /usr and user file systems and it requires multiple steps to first save and then later restore necessary PSSP files. See “Step 2b: BOS Overwrite Install” on page 127.

Step 2a: Perform Control Workstation BOS Migration Install

This method allows the current rootvg file systems to be preserved. This activity provides installp updates and installs necessary AIX LPPs to the control workstation. You must have all the necessary AIX file sets and PTFs listed in the *Memo to Users* available by CD-ROM, tape, or the NIM master.

Refer to the AIX Installation Guide in chapters 1-3, for more information. The following list provides some hints:

- Boot off your AIX CD-ROM or tape or setup the control workstation as a NIM client from an AIX 4.2.1 NIM master.
- Select option 1 "Change/Show Installation Settings. Always verify that it has been set to migrate and the correct target disk has been specified for root volume group.
- Select option 1 "System Settings" on Installation and Settings menu.
- Select option 3 "Migration Install" on the Change Method of Installation menu.
- Select the proper hdisk(s) being used for rootvg. You may want to update the hdisk configuration for the control workstation.
- Customize your control workstation based on the documented PSSP requirements. This includes required AIX LPPs and PTFs being installed.

Step 2b: BOS Overwrite Install

See “Perform Control Workstation Overwrite/Preservation Install” on page 158 for instructions.

After completing that procedure, proceed to “Step 3: Verify AIX Migration.”

Step 3: Verify AIX Migration

Verify that the control workstation has successfully been migrated to AIX 4.2.1 by issuing the following command:

```
oslevel
```

If the output of this command does not indicate AIX 4.2.1, issue the following command to return a list of AIX files not migrated to AIX 4.2.1. You may need to install AIX PTFs to migrate those file sets to AIX 4.2.1.

```
oslevel -l 4.2.1.0
```

Step 4: Verify Control Workstation Interfaces

Verify the configuration for each Ethernet adapter in the control workstation.

You can verify each Ethernet adapter by *pinging* its IP address and seeing if you get a response. For example:

```
ping -c 1 129.33.34.1
```

Reconfigure the adapter if you did not receive a response.

Changing User Process Limits

When you first install your system, the number of processes the root user can have is set to 40, an AIX 4.2 default. You will not be able to continue installing your system with this default value—you must increase the number to 256.

To change the value, enter the following command:

```
chdev -l sys0 -a maxuproc='256'
```

Tunables and Tunable Values

To validate the network tunables on the control workstation, use the **no** command to view and change the network values. To list the values, enter:

```
/usr/sbin/no -a
```

To modify the value of **thewall**, enter:

```
/usr/sbin/no -o thewall=16384
```

The following list provides the PSSP defaults to use:

```
thewall          16384
      sb_max           163840
      ipforwarding         1
      tcp_sendspace    65536
      tcp_recvspace    65536
      udp_sendspace    32768
      udp_recvspace    65536
      tcp_mssdflt      1448
```

You need to update the /**etc**/**rc.net** file so that these changes will take affect.

Step 5: Review Space Requirements for NIM Boot Images

Before creating an AIX 4.2.1 boot/install server, ensure that there is sufficient space in the root (/) file system or create a separate file system for /**tftpboot** to manage the space required for the boot images (approximately 25 megabytes per lppsource level supported) created by NIM.

Step 6: Review Space Requirements for /spdata

The /**spdata** directory contains mksysb images and installp file sets. IBM suggests you create a separate volume group for the /**spdata** file system. These file sets are large and need much space (up to 2 GB per lppsource level supported). If you have not done so already, use the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* to help you estimate how much space you need to define.

Step 7: Create Required /spdata Directories

You need to validate the proper PSSP directory structure for PSSP 2.3. Since PSSP 2.3 supports multiple levels of AIX and PSSP, a directory hierarchy was designed to contain different levels of images.

Note: Make sure you mount the /**spdata** file system before you create the /**spdata** directories.

You must create sub-directories on the /**spdata** file system for storing critical PSSP data. Make sure the directories have the permissions `rwxr-sr-x`. Issue the following commands to create the required directories:

- To create /**spdata**/**sys1**/**install**/<**name**>/**lppsource**, issue:

  ```
  mkdir -p /spdata/sys1/install/<name>/lppsource
  ```

  This is the subdirectory for the required AIX 4.2.1 file sets. You can choose any name but the name must not contain any dots (.). If you have multiple lppsources, you should pick more than one name. By default this is set up as the string "default". You might want to pick a more meaningful name, such as aix421 for AIX 4.2.1 level code. If the control workstation will be the NIM server for different levels of AIX, you should create one subdirectory for each level of AIX.

- To create /**spdata**/**sys1**/**install**/**pssplpp**/**PSSP-2.3**, issue:

  ```
  mkdir /spdata/sys1/install/pssplpp/PSSP-2.3
  ```

  This is the location of installp file sets for the code version PSSP-2.3. If the control workstation will be NIM server for nodes at other PSSP code levels, also create subdirectories under pssplpp with the code versions for those levels (PSSP-1.2, PSSP-2.1, PSSP-2.2).

Step 8: Copy the AIX 4.2.1 LPP Images

You must copy all required AIX 4.2.1 based file sets (LPPs) into the directory /**spdata**/**sys1**/**install**/<**name**>/**lppsource** on the control workstation. You also need to copy any AIX PTFs that were listed in the *Memo to Users* to the lppsource directory. You can use the **bffcreate** command to copy the LPPs.

```
bffcreate -qvX -t /spdata/sys1/install/<name>/lppsource  -d /dev/rmt0 al
```

Create a toc file by issuing the following command:

```
inutoc /spdata/sys1/install/<name>/lppsource
```

For more information, refer to “Step 15: Copy the AIX LPP Images and Other Required AIX LPPs” on page 24.

Step 9: Move the Existing LPP Images

PSSP 2.3 now supports more than one SPOT resource on the control workstation. It now implements a non /usr SPOT configuration as part of NIM. There is a new directory structure that is supported under **/spdata/sys1/install**. If you plan to support PSSP 2.1 nodes at the AIX 4.1.x level, you will need to select a new lppsource <*lppsource_name*> to be used to hold the AIX 4.1 file sets. This <*lppsource_name*> will be used as a new directory location at **/spdata/sys1/install/<name>**. You need to move the existing directory **/spdata/sys1/install/lppsource** to the new lppsource directory **/spdata/sys1/install/<name>/lppsource**.

Then, create a symbolic link from the new lppsource directory to the old directory to support PSSP 2.1 customization. For instance if the lppsource is at AIX 4.1.4 <*lppsource_name*>=*aix414*, you could issue the following commands:

```
mkdir /spdata/sys1/install/aix414

mv /spdata/sys1/install/lppsource /spdata/sys1/install/aix414

ln -s /spdata/sys1/install/aix414/lppsource /spdata/sys1/install/lppsource
```

Step 10: Verify (Install/Copy) Correct Level of PAIDE (perfagent)

The Performance Toolbox for AIX, Agent Component (PAIDE) is required starting with PSSP 2.2. The correct level of AIX PAIDE (perfagent) needs to be installed on the control workstation and copied to the lppsource directory. The level of perfagent required is dependent upon the level of AIX:

- AIX 4.1.4 - perfagent 2.1.4.x
- AIX 4.1.5 - perfagent 2.1.5.x
- AIX 4.2.0 - perfagent 2.2.0.x
- AIX 4.2.1 - perfagent 2.2.1.x

For more details regarding PAIDE, refer to the *Memo to Users*.

If the correct level of perfagent is not installed on the control workstation, it needs to be installed at this time. To verify whether the correct level of perfagent is installed on the control workstation, issue the following command:

```
lslpp -l perfagent.server
```

The correct level of perfagent must also be copied to the lppsource directory. You now need to copy the correct level of perfagent to the lppsource directory associated with the corresponding level of AIX (for example, perfagent 2.2.1.x for AIX 4.2.1).

Step 11: Copy the PSSP Images for PSSP 2.3

The RS/6000 SP package consists of several file sets which must be copied into the **/spdata/sys1/install/pssplpp/PSSP-2.3** directory using the **bffcreate** command. Then, rename the pssp package to **pssp.installp** and create the .toc file:

```
bffcreate -qvX -t /spdata/sys1/install/pssplpp/PSSP-2.3  -d /dev/rmt0 all
cd /spdata/sys1/install/pssplpp/PSSP-2.3
mv  ssp.usr.2.3.0.0 pssp.installp
inutoc .
```

Refer to “Step 16: Copy the PSSP Images” on page 26 for more information.

Step 12: Move the PSSP Images for PSSP 2.1

PSSP 2.3 supports more than one PSSP level in the SP system. If you want to continue to support PSSP 2.1 nodes, you need to create the proper directory structure for the PSSP 2.1 file sets and PTFs. You need to create the **/spdata/sys1/install/pssplpp/PSSP-2.1** directory on the control workstation.

If the **/spdata/sys1/install/pssplpp** directory still exists on the control workstation, move the PSSP 2.1 file sets including **pssp.installp** to the new directory **/spdata/sys1/install/pssplpp/PSSP-2.1**. Then, create a symbolic link from the new PSSP 2.1 directory back to the previous directory to support PSSP 2.1 nodes. Issue the following commands to setup the PSSP 2.1 directory:

```
mkdir /spdata/sys1/install/pssplpp/PSSP-2.1

mv /spdata/sys1/install/pssplpp/pssp.installp  \
/spdata/sys1/install/pssplpp/PSSP-2.1/

mv /spdata/sys1/install/pssplpp/<PSSP-2.1 LPP>  \
/spdata/sys1/install/pssplpp/PSSP-2.1/

ln -s /spdata/sys1/install/pssplpp/PSSP-2.1/pssp.installp  \
/spdata/sys1/install/pssplpp/pssp.installp
```

If the **/spdata/sys1/install/pssplpp** directory does not exist on the control workstation, load the PSSP 2.1 file sets from the install media to the new directory **/spdata/sys1/install/pssplpp/PSSP-2.1**.

Step 13: Install (Copy) the Basic AIX (mksysb) Image

The RS/6000 SP media provides a basic AIX 4.2.1 minimal image. You need to properly load in the base AIX 4.2.1 mksysb image to directory **/spdata/sys1/install/images** using the **installp** command.

```
installp  -aXd  /dev/rmt0.1  spimg
```

Step 14: Stop Daemons on the Control Workstation and Verify

Refer to the following table for the commands to issue to stop the daemons from running on the control workstation. You must stop the daemons in the order that they are presented in this table.

To stop this daemon:	Issue this command:
hr daemon	`stopsrc -g hr`
hb daemon	`stopsrc -g hb`
Emonitor daemon	`stopsrc -g emon`
sysctld daemon	`stopsrc -s sysctld`
Amd	`/etc/amd/amq` (See note below)
splogd daemon	`stopsrc -s splogd`
hardmon daemon	`stopsrc -s hardmon`
sdrd daemons	`stopsrc -g sdr`

Issue the **lssrc -a** command to verify that the daemons are no longer running on the control workstation. The SRC objects in the table should now have a status of *inoperative* with no active process ID (PID).

Amd Note:

If the **amq** command returns a response similar to:

```
/    root    "root"                   k22n04:(pid12128)
/u   toplvl  /etc/amd/amd-maps/amd.u  /u
```

the Amd daemon is running. Make sure that no processes are using any directories controlled by Amd (only two entries such as those previously listed appear in the **amq** output). If there is additional **amq** output indicating that directories are in use, stop all processes using those directories and then either wait five minutes to allow Amd to time out and unmount the directories, or force an unmount of the directories with the **amq -u** option.

Stop the daemon by issuing the following command:

```
kill -term <process_id>
```

where <process_id> is the pid value listed in the **amq** output, or which can be determined by issuing the following command:

```
ps -ef | grep amd
```

Do NOT use **kill -kill** or **kill -9** to stop the daemon as this will not allow the Amd daemon to properly shut down its control and may cause the file system to hang.

Step 15: Install PSSP on the Control Workstation

You now need to install the PSSP 2.3 level code on the control workstation. The PSSP 2.3 file sets are packaged to be installed on top of previously supported releases. IBM suggests installing all file sets made available in the pssp.installp package using the **installp** command:

```
installp  -aXd /spdata/sys1/install/pssplpp/PSSP-2.3/pssp.installp all
```

Complete “Step 18: Install PSSP on the Control Workstation” on page 27.

Step 16: Authenticate as the Administrative Principal

Issue the **kinit** command to properly authenticate as the administration user to the Authentication database.

```
/usr/lpp/ssp/kerberos/bin/kinit  <admin_user>
```

where <admin_user> is the name of the administrator. For default SP Kerberos based systems, *root.admin* is the kerberos administrator.

Note: If the PSSP Authentication services was not properly restored, you must run **setup_authent** to recreate your Kerberos database. You then need to *customize* all older PSSP nodes to distribute the new krb-srvtab files to the nodes using the **spbootins -r customize** command in a later step.

Step 17: Complete PSSP Installation on the Control Workstation

To properly setup the PSSP 2.3 control workstation for SDR, Hardmon, and other SP-related services, issue the following command:

```
install_cw
```

For more information, see “Step 20: Complete System Support Installation on the Control Workstation” on page 39.

Step 18: Run SDR and System Monitor Verification Test

In this step, run verification tests that check for correct installation of the SDR, the System Monitor, and the correct configuration of the System Monitor.

```
SDR_test (SDR verification)
spmon_itest (SP mon verification)
```

It may be necessary to reinitialize the SP frame connection to the SDR. You should issue the **spframe** command to reset the hardmon connection.

```
spframe -r yes 1 1 /dev/tty0
```

Complete “Step 21: Run SDR and System Monitor Verification Tests” on page 40 and “Step 24: Verify System Monitor Installation” on page 43.

Step 19: Configure PSSP Services and Set Up Site Environment

You must set the proper LPP Source name variable **cw_lppsource_name** to the appropriate name. This name is based on the <name> directory you selected in directory /**spdata**/**sys1**/**install**/<**name>**/**lppsource**. The <lppsource_name> environment is set to the string *default*. To change any of the site environments, issue the **spsitenv** command:

```
spsitenv cw_lppsource_name=<name>
```

The system management environments on the control workstation are started by running **services_config**. Issue the following command:

```
/usr/lpp/ssp/install/bin/services_config
```

If the Site Environment variable **amd_config** is set to true, **service_config** will configure automounter directories and files. If the Site Environment variable **usermgmt_config** is also set to true, the file /**etc**/**auto**/**maps**/**auto.u** will be created to control the /**u** file system containing user home directories. Since the use of **Amd** has been replaced with the AIX automount daemon in PSSP 2.3, **services_config** will automatically convert the existing /**etc**/**amd**/**amd-maps**/**amd.u** map file to

auto.u. If you had an **amd.u** map file that was not generated by PSSP, or if you had modified the entries in that file in any way, this conversion process may fail. See the Managing the Automounter chapter in the *PSSP Administration Guide* for more details on the migration conversion process and what to do if it fails.

If you had other file systems that were under Amd control, you may wish to convert those map files at this time. See the Managing the Automounter chapter in the *PSSP Administration Guide* for more details on managing other file systems with the automount daemon.

Step 20: Start System Partition-Sensitive Subsystems and Verify

There are system partition-sensitive subsystems that you need to add to the system. Even if you are not partitioning your system, you need to do this since you still have one default partition. Do the following:

1. Remove old subsystems (for example, hr, hb) by issuing the following command:

   ```
   syspar_ctrl -c
   ```

2. Add new subsystems (for example, hats, hags) by issuing the following command:

   ```
   syspar_ctrl -A -G
   ```

To verify that the System Partition Sensitive Subsystems have been properly started, refer to “Step 34: Verify System Partition-Sensitive Subsystems Have Started” on page 55.

Step 21: Start Quiesced Applications

Any of the applications that you quiesced prior to migrating your control workstation should be started now if they have not already been automatically started. For example, if you have a switch, issue the following command to restart your switch:

```
Estart
```

Step 22: Unconfigure the NIM Master

It may be necessary to unconfigure the control workstation as a NIM master. PSSP 2.3 supports multiple non- /usr SPOT resources on the control workstation. Issue the following command to unconfigure NIM.

```
delnimmast -l 0
```

To verify that the control workstation is no longer a NIM master, issue the following command:

```
/usr/sbin/lsnim
```

You should receive an error message similar to the following one that indicates that lsnim is not found:

```
ksh: lsnim:  not found.
```

Step 23: Configure Control Workstation as Boot/Install Server

Verify that the SDR node attribute value for **code_version**, **lppsource_name**, and **next_install_image** are appropriately set. Issue the following command:

```
splstdata -b -G
```

- Each node's PSSP **code_version** should be set to the level of PSSP currently installed on the node.
- Each node's **lppsource_name** should indicate the level of AIX currently installed on the node. The **lppsource_name** value must correspond to the directory name where you chose to place the lppsource files in /**spdata**/**sys1**/**install**/<**name**>/**lppsource** (for all nodes running PSSP-2.1 or greater).
- Each node's **install_image** should indicate the mksysb image that is installed on the node. Each mksysb image should be stored in the directory /**spdata**/**sys1**/**install**/**images** except for AIX 3.2.5/PSSP 1.2 node mksysb images which should be stored in the directory /**usr**/**sys**/**inst.images**/**ssp**. If the value is *default* then verify the SDR Syspar and SP attribute value for **install_image** is appropriately set.

If necessary, you can issue the **spbootins** command to change the node's attribute values or **spsitenv** command to change SP attribute values. Issue the appropriate command specifying the options associated with the attributes that you want changed:

```
spbootins -s no -p <code_version> -i <install_image_name> \
-v <lppsource_name> -l <node_list>
```

```
spsitenv install_image=<install_image_name>
```

The **setup_server** command must be run to properly set up NIM on the control workstation by issuing the command:

```
setup_server 2>& | tee /tmp/setup_server.out
```

The output will be saved in a log file called **setup_server.out**. This may take a while since it will be creating the NIM master.

Step 24: Run Verification Tests

You should validate that the PSSP 2.3 software has been properly installed on the control workstation by issuing the following commands:

```
SYSMAN_test
spmon_ctest
CSS_test                * run only if you have a switch
spverify_config         * run only if your system is partitioned
jm_install_verify       * run only if using Resource Manager
jm_verify               * run only if using Resource Manager
```

Verify **host_responds** and **switch_responds**, if you have a switch, are set to *yes* by issuing the following command:

```
spmon -d -G
```

Step 25: Validate the Control Workstation

Your control workstation should now function at PSSP 2.3 level. All PSSP 2.2, PSSP 2.1, and PSSP 1.2 nodes should now be able to communicate to the PSSP 2.3 control workstation, if the proper level of PTF service has been applied to the PSSP nodes.

There are occasions based on customer changes made to the SDR and Authentication services, that may require the PSSP nodes to be rebooted and possibly recustomized by the boot/install server (BIS) nodes.

You can now add other AIX, PSSP, and customer owned LPPs and files on to the control workstation. Be careful to make sure that older applications and LPPs will work properly with AIX 4.2 and PSSP 2.3.

Note: At this point, refer back to “High-Level Migration Steps” on page 107 to determine your next step in the migration process.

Migrate the Control Workstation from PSSP 2.2 to PSSP 2.3

Follow the steps in this section if you are upgrading your control workstation from PSSP 2.2 to PSSP 2.3.

Step 1: Prepare to Migrate and Verify Requirements

Before beginning, refer to “Preparing to Migrate” on page 109 for information on preparing to migrate and verifying control workstation and system requirements.

Step 2: Migrate to AIX 4.2.1

You need to upgrade the control workstation to AIX 4.2.1. Determine which of the following methods you want to follow based upon the information described at the beginning of this chapter:

Upgrade: Your control workstation may already be at AIX 4.2.0. You should issue the **installp** commands to install the new AIX 4.2.1 PTFs or file sets on top of the the current AIX level to preserve the current files in the / (root), /var/ /usr, and user based file systems. For more information, see “Step 2a: Upgrade.”

BOS Migration Install: The control workstation is currently at AIX 4.1.x. Use this method to preserve the current files in the / (root), /var, /usr and user based file systems. For more information, see “Step 2b: Perform Control Workstation BOS Migration Install.”

BOS Overwrite Install: You may choose to reinstall the control workstation to AIX 4.2.1. This method does not preserve the files in the / (root), /var, /usr and user file systems and it requires multiple steps to first save, and then later restore necessary PSSP files. See “Step 2c: BOS Overwrite Install” on page 137.

Step 2a: Upgrade

Applying PTFs for the control workstation allows the current rootvg file systems to be preserved. This activity provides installp updates and installs necessary AIX LPPs to the control workstation. You must have all the necessary AIX file sets and PTFs listed in the *Memo to Users* available during this PTF upgrade. You will issue the **installp** command where the input source can be a tape, CD-ROM, or a directory (lppsource) that contains the PTFs or file sets. Using the directory requires you to use the **bffcreate** command to copy the AIX 4.2.1 PTFs or file sets into the lppsource directory.

To create a list of LPPs on the control workstation, issue:

```
lslpp -l -J   >/tmp/FILE.42
```

To install and apply PTF service from tape media and commit LPPs, issue:

```
installp -acNgd /dev/rmt0 -f /tmp/FILE.42
```

Step 2b: Perform Control Workstation BOS Migration Install

This method preserves all file systems except **/tmp**, as well as the root volume group, logical volumes, and system configuration files. This activity provides installp updates and installs necessary AIX LPPs to the control workstation. You must have all the necessary AIX file sets and PTFs listed in the *Memo to Users* available by CD-ROM, tape, or from the NIM master.

Migration install from tape or CD-ROM is an interactive process. You will be prompted to verify settings, continue the installation, and verify the migration.

Refer to the AIX Installation Guide in chapters 1-3, for more information. The following list provides some hints:

- Boot off your AIX CD-ROM or tape or setup the control workstation as a NIM client from an AIX 4.2.1 NIM master.
- Select option 2 "Change/Show Installation Settings and Install". Always verify that it has been set to *migrate* and that the correct target disk is assigned for root volume group.
- Select option 1 "System Settings" on Installation and Settings menu.
- Select option 3 "Migration Install" on the Change Method of Installation menu.
- Select the proper hdisk(s) being used for rootvg. You may want to update the hdisk configuration for the control workstation.
- Customize your control workstation based on the documented PSSP requirements. This includes required AIX LPPs and PTFs being installed.

Step 2c: BOS Overwrite Install

See “Perform Control Workstation Overwrite/Preservation Install” on page 158 for instructions.

After completing that procedure, proceed to “Step 3: Verify AIX Migration.”

Step 3: Verify AIX Migration

Verify that the control workstation has successfully been migrated to AIX 4.2.1 by issuing the following command:

```
oslevel
```

If the output of this command does not indicate AIX 4.2.1, issue the following command to return a list of AIX files not migrated to AIX 4.2.1. You may need to install AIX PTFs to migrate those file sets to AIX 4.2.1.

```
oslevel -l 4.2.1.0
```

Step 4: Verify Control Workstation Interfaces

Verify the configuration for each Ethernet adapter in the control workstation.

You can verify each Ethernet adapter by *pinging* its IP address and seeing if you get a response. For example:

```
ping -c 1 129.33.34.1
```

Reconfigure the adapter if you did not receive a response.

Changing User Process Limits

When you first install your system, the number of processes the root user can have is set to 40, an AIX 4.2 default. You will not be able to continue installing your system with this default value—you must increase the number to 256.

To change the value, enter the following command:

```
chdev -l sys0 -a maxuproc='256'
```

Tunables and Tunable Values

To validate the network tunables on the control workstation, use the **no** command to view and change the network values. To list the values, enter:

```
/usr/sbin/no -a
```

To modify the value of **thewall**, enter:

```
/usr/sbin/no -o thewall=16384
```

The following list provides the PSSP defaults to use:

```
thewall          16384
sb_max          163840
ipforwarding         1
tcp_sendspace    65536
tcp_recvspace    65536
udp_sendspace    32768
udp_recvspace    65536
tcp_mssdflt       1448
```

You need to update the /**etc**/**rc.net** file so that these changes will take affect.

Step 5: Review Space Requirements for NIM Boot Images

Before creating an AIX 4.2.1 boot/install server, ensure that there is sufficient space in the root (/) file system or create a separate file system for /**tftpboot** to manage the space required for the boot images (approximately 25 megabytes per lppsource level supported) created by NIM.

Step 6: Review Space Requirements for /spdata

The /**spdata** directory contains mksysb images and installp file sets. IBM suggests you create a separate volume group for the /**spdata** file system. These file sets are large and need much space (up to 2 GB per lppsource level supported). If you have not done so already, use the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* to help you estimate how much space you need to define.

Step 7: Create Required /spdata Directories

You need to validate the proper PSSP directory structure for PSSP 2.3. Since PSSP 2.3 supports multiple levels of AIX and PSSP, a directory hierarchy was designed to contain different levels of images.

Note: Make sure you mount the /**spdata** file system before you create the /**spdata** directories.

You must create sub-directories on the /**spdata** file system for storing critical PSSP data. Make sure the directories have the permissions `rwxr-sr-x`. Issue the following commands to create the required directories:

- To create /**spdata**/**sys1**/**install**/<**name**>/**lppsource**, issue:

  ```
  mkdir -p /spdata/sys1/install/<name>/lppsource
  ```

  This is the subdirectory for the required AIX 4.2.1 file sets. You can choose any name but the name must not contain any dots (.). If you have multiple lppsources, you should pick more than one name. By default this is set up as the string "default". You might want to pick a more meaningful name, such as *AIX421* for AIX 4.2.1 level code. If the control workstation will be the NIM

server for different levels of AIX, you should create one subdirectory for each level of AIX.

- To create **/spdata/sys1/install/pssplpp/PSSP-2.3**, issue:

  ```
  mkdir /spdata/sys1/install/pssplpp/PSSP-2.3
  ```

  This is the location of installp file sets for the code version PSSP-2.3. If the control workstation will be NIM server for nodes at other PSSP code levels, also create subdirectories under pssplpp with the code versions for those levels (PSSP-1.2, PSSP-2.1, PSSP-2.2).

Step 8: Copy the AIX 4.2.1 LPP Images

You must copy all required AIX 4.2 file sets (LPPs) into directory **/spdata/sys1/install/**<**name**>**/lppsource** on the control workstation. You also must copy any AIX PTFs that are listed in the Memo to Users to the lppsource directory. Use the **bffcreate** command to copy the LPPs.

```
bffcreate -qvX -t /spdata/sys1/install/<name>/lppsource \
-d /dev/rmt0 all
```

You should then create a .toc file for the AIX 4.2.1 files:

```
inutoc /spdata/sys1/install/<name>/lppsource
```

Refer to “Step 15: Copy the AIX LPP Images and Other Required AIX LPPs” on page 24 for more information.

Step 9: Verify (Install/Copy) Correct Level of PAIDE (perfagent)

The Performance Toolbox for AIX, Agent Component (PAIDE) is required starting with PSSP 2.2. The correct level of AIX PAIDE (perfagent) needs to be installed on the control workstation and copied to the lppsource directory. The level of perfagent required is dependent upon the level of AIX:

- AIX 4.1.4 - perfagent 2.1.4.x
- AIX 4.1.5 - perfagent 2.1.5.x
- AIX 4.2.0 - perfagent 2.2.0.x
- AIX 4.2.1 - perfagent 2.2.1.x

For more details regarding PAIDE, refer to the *Memo to Users*.

If the correct level of perfagent is not installed on the control workstation, it needs to be installed at this time. To verify whether the correct level of perfagent is installed on the control workstation, issue the following command:

```
lslpp -l perfagent.server
```

The correct level of perfagent must also be copied to the lppsource directory. You now need to copy the correct level of perfagent to the lppsource directory associated with the corresponding level of AIX (for example, perfagent 2.2.1.x for AIX 4.2.1).

Step 10: Copy the PSSP Images for PSSP 2.3

The RS/6000 SP package consists of several file sets which must be copied into the **/spdata/sys1/install/pssplpp/PSSP-2.3** directory using the **bffcreate** command. Then, rename the pssp package to **pssp.installp** and create the .toc file:

```
bffcreate -qvX -t /spdata/sys1/install/pssplpp/PSSP-2.3  -d /dev/rmt0 all
cd /spdata/sys1/install/pssplpp/PSSP-2.3
mv  ssp.usr.2.3.0.0 pssp.installp
inutoc .
```

Refer to “Step 16: Copy the PSSP Images” on page 26 for more information.

Step 11: Install (Copy) the Basic AIX (mksysb) Image

The RS/6000 SP media provides a basic AIX 4.2.1 minimal image. You need to properly load in the base AIX 4.2.1 mksysb image to the **/spdata/sys1/install/images** directory using the **installp** command. You then may remove any mksysb images you no longer need.

```
installp  -aXd  /dev/rmt0.1  spimg
```

Refer to “Step 17: Copy a Basic AIX (mksysb) Image” on page 27 for more information.

Step 12: Stop Daemons on the Control Workstation and Verify

Refer to the following table for the commands to issue to stop the daemons from running on the control workstation: You must stop the daemons in the order that they are presented in this table.

To stop this daemon:	Issue this command:
Partition sensitive daemons	`syspar_ctrl -G -k`
sysctld daemon	`stopsrc -s sysctld`
Amd	`/etc/amd/amq` (See note below)
splogd daemon	`stopsrc -s splogd`
hardmon daemon	`stopsrc -s hardmon`
sdrd daemons	`stopsrc -g sdr`

Issue the **lssrc -a** command to verify that the daemons are no longer running on the control workstation. The SRC objects in the table should now have a status of *inoperative* with no active process ID (PID).

Amd Note:

If the **amq** command returns a response similar to:

```
/    root    "root"                    k22n04:(pid12128)
/u   toplvl  /etc/amd/amd-maps/amd.u   /u
```

the Amd daemon is running. Make sure that no processes are using any directories controlled by Amd (only two entries such as those previously listed appear in the **amq** output). If there is additional **amq** output indicating that directories are in use, stop all processes using those directories and then either

wait five minutes to allow Amd to time out and unmount the directories, or force an unmount of the directories with the **amq -u** option.

Stop the daemon by issuing the following command:

```
kill -term <process_id>
```

where <process_id> is the pid value listed in the **amq** output, or which can be determined by issuing the following command:

```
ps -ef | grep amd
```

Do NOT use **kill -kill** or **kill -9** to stop the daemon as this will not allow the Amd daemon to properly shut down its control and may cause the file system to hang.

Step 13: Install PSSP on the Control Workstation

You now need to install the PSSP 2.3 level code on the control workstation. The PSSP 2.3 file sets are packaged to be installed on top of previously supported releases. You should install all file sets made available in the **pssp.install** package using the **installp** command:

```
installp  -aXd /spdata/sys1/install/pssplpp/PSSP-2.3/pssp.installp all
```

Step 14: Authenticate as the Administrative Principal

You need to issue the **kinit** command to properly authenticate as the administration user to the Authentication database.

```
/usr/lpp/ssp/kerberos/bin/kinit <admin_user>
```

where <admin_user> is the name of the administrator. For default SP Kerberos based systems "root.admin" is the kerberos administrator.

Note: If the PSSP Authentication services was not properly restored, you must run **setup_authent** to recreate your Kerberos database. You then need to "customize" all older PSSP nodes to distribute the new krb-srvtab files to the nodes using the **spbootins -r customize** command in a later step.

Step 15: Complete PSSP Installation on the Control Workstation

To properly setup the PSSP 2.3 control workstation for SDR, Hardmon, and other SP related services, issue the following command:

```
install_cw
```

For more information, see “Step 20: Complete System Support Installation on the Control Workstation” on page 39.

Step 16: Run SDR and System Monitor Verification Test

Run verification tests that check for correct installation of the SDR, the System Monitor, and correct configuration of the System Monitor.

```
SDR_test     (SDR verification)
spmon_itest  (SP mon verification)
```

You may have to reinitialize the SP frame connection to the SDR by issuing the following command to reset the hardmon connection:

```
spframe -r yes 1 1 /dev/tty0
```

Step 17: Configure PSSP Services and Set Up Site Environment

You must set the proper LPP source name variable **cw_lppsource_name** to the appropriate name. This name is based on the <name> directory you selected in directory /**spdata**/**sys1**/**install**/<**name**>/**lppsource**. The <name> environment is set to the string *default*. To change **cw_lppsource_name** or other site environment variables, issue:

```
spsitenv cw_lppsource_name=<name>
```

The system management environments on the control workstation are started by running **services_config**. Issue the following command:

```
/usr/lpp/ssp/install/bin/services_config
```

If the Site Environment variable **amd_config** is set to true, **services_config** will configure automounter directories and files. If the Site Environment variable **usermgmt_config** is also set to true, the file /**etc**/**auto**/**maps**/**auto.u** will be created to control the /**u** file system containing user home directories. Since the use of Amd has been replaced with the AIX automount daemon in PSSP 2.3, **services_config** will automatically convert the existing /**etc**/**amd**/**amd-maps**/**amd.u** map file to **auto.u**. If you had an **amd.u** map file that was not generated by PSSP, or if you had modified the entries in that file in any way, this conversion process may fail. See the Managing the Automounter chapter in the *PSSP Administration Guide* for more details on the migration conversion process and what to do if it fails.

If you had other file systems that were under Amd control, you may wish to convert those map files at this time. See the Managing the Automounter chapter in the *PSSP Administration Guide* for more details on managing other file systems with the automount daemon.

Step 18: Start System Partition-Sensitive Subsystems and Verify

There are system partition-sensitive subsystems that you need to add to the system. Even if you are not partitioning your system, you need to do this since you still have one default partition. Do the following:

1. Remove old subsystems (for example, hats, hags) by issuing the following command:

   ```
   syspar_ctrl -c
   ```

2. Add new subsystems (for example, hats, hags) by issuing the following command:

   ```
   syspar_ctrl -A -G
   ```

To verify that the System Partition Sensitive Subsystems have been properly started, refer to “Step 34: Verify System Partition-Sensitive Subsystems Have Started” on page 55.

Step 19: Start Quiesced Applications

Any of the applications that you quiesced prior to migrating your control workstation should be started now if they have not already been automatically started. For example, if you have a switch, issue the following command to restart your switch:

```
Estart
```

Step 20: Configure Control Workstation as Boot/Install Server

Verify that the SDR node attribute value for **code_version**, **lppsource_name**, and **next_install_image** are appropriately set. Issue the following command:

```
splstdata -b -G
```

- Each node's PSSP **code_version** should be set to the level of PSSP currently installed on the node.
- Each node's **lppsource_name** should indicate the level of AIX currently installed on the node. The **lppsource_name** value must correspond to the directory name where you chose to place the lppsource files in /**spdata**/**sys1**/**install**/<**name>**/**lppsource** (for all nodes running PSSP-2.1 or greater).
- Each node's **install_image** should indicate the mksysb image that is installed on the node. Each mksysb image should be stored in the directory /**spdata**/**sys1**/**install**/**images** except for AIX 3.2.5/PSSP 1.2 node mksysb images which should be stored in the directory /**usr**/**sys**/**inst.images**/**ssp**. If the value is *default* then verify the SDR Syspar and SP attribute value for **install_image** is appropriately set.

If necessary, you can issue the **spbootins** command to change the node's attribute values or **spsitenv** command to change SP attribute values. Issue the appropriate command specifying the options associated with the attributes that you want changed:

```
spbootins -s no -p <code_version> -i <install_image_name> \
-v <lppsource_name> -l <node_list>
```

```
spsitenv install_image=<install_image_name>
```

The **setup_server** command must be run to properly set up NIM on the control workstation by issuing the command:

```
setup_server 2>& | tee /tmp/setup_server.out
```

The output will be saved in a log file called **setup_server.out**. This may take a while since it will be creating the NIM master.

Step 21: Run Verification Tests

You should validate that the PSSP 2.3 software has been properly installed on the control workstation by issuing the following commands:

```
SYSMAN_test
spmon_ctest
CSS_test                * run only if you have a switch
spverify_config         * run only if your system is partitioned
jm_install_verify       * run only if using Resource Manager
jm_verify               * run only if using Resource Manager
```

Verify **host_responds** and **switch_responds**, if you have a switch, are set to *yes* by issuing the following command:

```
spmon -d -G
```

Step 22: Validate the Control Workstation

Your control workstation should now function at PSSP 2.3 level. All PSSP 2.2, PSSP 2.1, and PSSP 1.2 nodes should now be able to communicate to the PSSP 2.3 control workstation, if the proper level of PTF service has been applied to the PSSP nodes.

There are occasions based on customer changes made to the SDR and Authentication services, that may require the PSSP nodes to be rebooted and possibly recustomized by the boot/install server (BIS) nodes.

You can now add other AIX, PSSP, and customer owned LPPs and files on to the control workstation. Be careful to make sure that older applications and LPPs will work properly with AIX 4.2 and PSSP 2.3.

Note: At this point, refer back to “High-Level Migration Steps” on page 107 to determine your next step in the migration process.

Paths to Migrate the Nodes to PSSP 2.3 and AIX 4.2.1

You cannot migrate the nodes until you have first migrated the control workstation to AIX 4.2.1 and PSSP 2.3. Remember that the control workstation must always be at the latest level of AIX and PSSP to which you plan to migrate the nodes. Refer to the beginning of this chapter for that information. Keep in mind that you should always make a mksysb of all of your nodes that you want to migrate before proceeding with the migration process. For information on making a mksysb of your nodes, refer to “Step 8: Back Up Your Nodes” on page 112.

You can migrate the nodes to AIX 4.2.1 and PSSP 2.3 in one of the ways identified in the following list:

- Migration Install

  This method preserves all file systems except /**tmp**, as well as the root volume group, logical volumes, and system configuration files. This method requires the setup of AIX NIM on the new PSSP 2.3 control workstation. This applies only to migrations when an AIX version or release is changing (for example, AIX 4.1.x to 4.2.x).

- mksysb install

  This method erases all existence of current rootvg and installs AIX 4.2.1 and PSSP 2.3 using an AIX 4.2.1 mksysb image for the node. This installation requires the setup of AIX NIM on the new PSSP 2.3 control workstation.

- Upgrade

  This method preserves the current rootvg and installs AIX PTF updates using the **installp** command. This method applies only to AIX modification level changes (for example, AIX 4.2.0 to 4.2.1).

Typically, a customer would migrate a node using either the migration install or upgrade methods depending upon the node's current AIX and PSSP levels. If some nodes are identical, you could create a mksysb of the node and then migrate these nodes using the mksysb install method.

The following table identifies the supported migration paths. First determine your starting point by selecting the AIX and PSSP level of your current system. Second, select the target point for AIX and PSSP. Then, select the appropriate method from the **Installation Method Choice** column. Finally, refer to the appropriate section in this chapter and follow the steps to migrate the nodes.

Table 8. Paths to migrate the nodes

AIX Starting Point	PSSP Starting Point	Target Point	Installation Method Choice	Refer to:
AIX 3.2.5	PSSP 1.2	AIX 4.2.1, PSSP 2.3	Migration Install	"Migration Install of Nodes to AIX 4.2.1 and PSSP 2.3" on page 147
			mksysb Install	"mksysb Install of Nodes" on page 150
AIX 4.1.3 AIX 4.1.4 AIX 4.1.5	PSSP 2.1	AIX 4.2.1, PSSP 2.3	Migration Install	"Migration Install of Nodes to AIX 4.2.1 and PSSP 2.3" on page 147
			mksysb Install	"mksysb Install of Nodes" on page 150
AIX 4.1.4 AIX 4.1.5	PSSP 2.2	AIX 4.2.1, PSSP 2.2 AIX migration only.	Migration Install	"Migrate or Upgrade Nodes to AIX 4.2.1 or Later" on page 153
AIX 4.2.0	PSSP 2.2	AIX 4.2.1, PSSP 2.2 AIX migration only.	Upgrade	"Migrate or Upgrade Nodes to AIX 4.2.1 or Later" on page 153
AIX 4.1.4 AIX 4.1.5	PSSP 2.2	AIX 4.2.1, PSSP 2.3	Migration Install	"Migration Install of Nodes to AIX 4.2.1 and PSSP 2.3" on page 147
			mksysb Install	"mksysb Install of Nodes" on page 150
AIX 4.2.0 AIX 4.2.1	PSSP 2.2	AIX 4.2.1, PSSP 2.3	Upgrade	"Upgrade Nodes to AIX 4.2.1 and PSSP 2.3" on page 154
			mksysb Install	"mksysb Install of Nodes" on page 150
AIX 4.2.1	PSSP 2.3	AIX 4.2.x, PSSP 2.3 AIX migration only.	Upgrade	"Migrate or Upgrade Nodes to AIX 4.2.1 or Later" on page 153

Migration Install of Nodes to AIX 4.2.1 and PSSP 2.3

Before proceeding with the steps in this section, be sure you have selected the correct migration path. If you are unsure, refer to Table 8 on page 146.

Step 1: Enter Node Configuration Data

You need to properly set the appropriate SDR node object attributes for **lppsource_name**, **code_version**, and **bootp_response** for each node being migrated. Use the **spbootins** command to update these fields. Run the following **spbootins** command:

```
spbootins -s no -p <code_version> -r migrate -v \
<lppsource_name> -l <node_list>
```

- **-s no** prevents setup_server from running.
- **-p** <**code_version>** sets the node's PSSP level. Use this to indicate the PSSP level to install on the node. The value you choose must match the directory name you choose to place the PSSP installation files under in the **/spdata/sys1/install/pssplpp** directory during installation.
- **-r migrate** sets the node's **bootp_response** value to *migrate* which indicates that you want the server to perform a migration installation on the specified nodes.
- **-v** <**lppsource_name>** sets the node's lppsource name. Use this to indicate the level of AIX to which the node will be migrated. This name is based on the chosen directory that was set during control workstation migration.
- **-l** <**node_list>** specifies the list of nodes you are migrating. Either specify a comma-delimited list of node numbers, or a file containing one line of data which is a comma-delimited list of node numbers. The file can also contain comment lines (preceded by a #) and lines that are all white space. (This is a lowercase l, as in list.)

For example, to migrate nodes 1 and 2 to PSSP 2.3 where lppsource was placed in **/spdata/sys1/install/AIX421/lppsource**, issue the following command:

```
spbootins -s no -p PSSP-2.3 -r migrate -v AIX421 -l 1,2
```

Step 2: Verify Installation Settings

Make sure that the SDR has the appropriate values specified in the following attributes for each of the nodes. Issue the following command to display the values:

```
splstdata -G -b
```

- response

  Nodes being migrated should be set to *migrate*.

- lppsource_name

  The AIX level of the nodes to be migrated. For example, *AIX421*.

- pssp_ver

  The code_version of PSSP should be set to "PSSP-2.3" for nodes you are migrating.

Make sure that **/tftpboot/script.cust** has been properly updated for PSSP 2.3 modifications.

Step 3: Run setup_server to Configure the Changes

The **setup_server** command must be run to properly set up NIM on the control workstation by issuing the following command:

```
setup_server 2>&1 | tee /tmp/setup_server.out
```

The output will be saved in a log file called `setup_server.out`.

If you have a node defined as a boot/install server you must run **setup_server** out on that server node.

```
dsh -w <boot/install_node> /usr/lpp/ssp/bin/setup_server
```

Step 4: Refresh System Partition-Sensitive Subsystems

The SDR has now been updated to reflect the new nodes that will run PSSP 2.3. You now need to refresh the System Partition Sensitive Subsystems on the control workstation and all nodes to pick up these changes. Run **syspar_ctrl** on the control workstation to refresh the subsystems on both the control workstation and on the nodes.

```
syspar_ctrl -r -G
```

Note: You can ignore any messages that you receive from the nodes you are migrating at this point because the migration process is not yet complete. Once the migration is complete, you should no longer receive error messages.

Step 5: Disable Node From the Switch

If you do not have a switch in your SP System, skip this step.

If you want to bring the switch down for all nodes issue the **Equiesce** command. If you use the **Equiesce** command, you will need to later restart the switch using the **Estart** command. Issue the **Estart** command prior to the step where you "Verify the Nodes".

If you are migrating a few nodes, you must disconnect these nodes from the switch (if appropriate, first reassign the Primary Node or Primary Backup Node). To determine if one of the nodes you are migrating is a Primary or Primary Backup Node, or to reassign the Primary or Primary Backup Node, issue the **Eprimary** command. You must then execute the **Efence** command to disconnect nodes from the switch.

```
Efence -G -autojoin <node_number>
```

Step 6: Shut Down the Node

To shut down the node gracefully, issue the following command:

```
cshutdown -F -N <node_number>
```

Step 7: Network Boot the Node

Note: If you have any boot/install servers in your system, you need to migrate them before migrating their clients. You should not netboot more than 8 nodes with the same server at a time.

Network boot each node that you are migrating by using the **nodecond** command or by using **perspectives**.

```
nodecond -G <frame_id> <slot_id> &
```

You should notice that the node has been properly installed when the LED's become blank, and the host_responds is active.

Verify that the **bootp_response** has been set to disk by issuing the following command:

```
splstdata -G -b
```

Step 8: Run Verification Tests

Verify that the nodes are running properly by issuing the following commands:

```
SYSMAN_test
CSS_test                  * run only if you have a switch
spverify_config           * run only if your system is partitioned
jm_install_verify         * run only if using Resource Manager
jm_verify                 * run only if using Resource Manager
```

Verify **host_responds** and **switch_responds**, if you have a switch, are set to *yes* by issuing the following command:

```
spmon -d -G
```

Note: At this point, refer back to “High-Level Migration Steps” on page 107 to determine your next step in the migration process.

mksysb Install of Nodes

Before proceeding with the steps in this section, be sure you have selected the correct migration path. If you are unsure, refer to Table 8 on page 146.

Step 1: Enter Node Configuration Data

You need to properly set the appropriate SDR node object attributes for **lppsource_name**, **code_version**, **bootp_response**, and **next_install_image** for each node being migrated. Use the **spbootins** command to update these fields.

```
spbootins -s no -p <code_version> -r install \
-v <lppsource_name> -i <install_image_name> -l <node_list>
```

- **-s no** prevents setup_server from running.
- **-p** <**code_version>** sets the node's PSSP level. Use this to indicate the PSSP level to install on the node. The value you choose must match the directory name you choose to place the PSSP installation files under in the **/spdata/sys1/install/pssplpp** directory during installation.
- **-r install** sets the node's **bootp_response** value to *install* which indicates that you want the server to perform an install operation on the specified nodes.
- **-v** <**lppsource_name>** sets the node's lppsource name. Use this to indicate the level of AIX to which the node will be migrated. This is based on the chosen directory that was set during the control workstation migration. Use this subdirectory name that you loaded the lppsource into under **/spdata/sys1/install**.
- **-i** <**install_image_name**> specifies the file name of the install image to use for the nodes when they are network-installed. Specify the mksysb image in the **/spdata/sys1/install/images** directory on the control workstation. At installation, the value for each node's install image name is *default*, which means that the default install image name for the system is used for each node. The default install image name for the system is found in the SP object.
- **-l** <**node_list>** specifies the list of nodes you are migrating. Either specify a comma-delimited list of node numbers, or a file containing one line of data which is a comma-delimited list of node numbers. The file can also contain comment lines (preceded by a #) and lines that are all white space. (This is a lowercase l, as in list.)

For example, to migrate nodes 1 and 2 to PSSP 2.3 where lppsource was placed in **/spdata/sys1/install/AIX421/lppsource**, issue the following command:

```
spbootins -s no -p PSSP-2.3 -r install -v AIX421 \
-i bos.obj.ssp.421 -l 1,2
```

Step 2: Verify Installation Settings

Make sure that the SDR has the appropriate values specified in the following attributes for each of the nodes. Issue the following command to display the values:

```
splstdata -G -b
```

- response

  Nodes being migrated should be set to *install*.

- lppsource_name

  The AIX level of the nodes to be migrated, For example, *AIX421*.

- pssp_ver

  The code_version of PSSP should be set to "PSSP-2.3" for nodes you are migrating.

- next_install_image

  Should be set to appropriate AIX 4.2 mksysb image. For example, *bos.obj.ssp.421*.

Make sure that **/tftpboot/script.cust** has been properly updated for PSSP 2.3 modifications.

Step 3: Run setup_server to Configure the Changes

The **setup_server** command must be run to properly set up NIM on the control workstation by issuing the following command:

```
setup_server 2>&1 | tee /tmp/setup_server.out
```

The output will be saved in a log file called `setup_server.out`.

If you have a node defined as a boot/install server you must run **setup_server** out on that server node.

```
dsh -w <boot/install_node> /usr/lpp/ssp/bin/setup_server
```

Step 4: Refresh System Partition-Sensitive Subsystems

The SDR has now been updated to reflect the new nodes that will run PSSP 2.3. You now need to refresh the System Partition Sensitive Subsystems on the control workstation and all nodes to pick up these changes. Run **syspar_ctrl** on the control workstation to refresh the subsystems on both the control workstation and on the nodes.

```
syspar_ctrl -r -G
```

Note: You can ignore any messages that you receive from the nodes you are migrating at this point because the migration process is not yet complete. Once the process is complete, you should no longer receive error messages.

Step 5: Disable Node From the Switch

If you do not have a switch in your SP System, skip this step.

If you want to bring the switch down for all nodes issue the **Equiesce** command. If you use the **Equiesce** command, you will need to later restart the switch using the **Estart** command. Issue the **Estart** command prior to the step where you "Verify the Nodes".

If you are migrating a few nodes, you must disconnect these nodes from the switch (if appropriate, first reassign the Primary Node or Primary Backup Node). To determine if one of the nodes you are migrating is a Primary or Primary Backup Node, or to reassign the Primary or Primary Backup Node, issue the **Eprimary** command. You must then execute the **Efence** command to disconnect nodes from the switch.

```
Efence -G -autojoin <node_number>
```

Step 6: Shut Down the Node

To shut down the node gracefully, issue the following command:

```
cshutdown -F -N <node_number>
```

Step 7: Network Boot the Node

Note: If you have any boot/install servers in your system, you need to migrate them before migrating their clients. You should not netboot more than 8 nodes with the same server at a time.

Network boot each node that you are migrating by using the **nodecond** command or by using **perspectives**.

```
nodecond -G <frame_id> <slot_id> &
```

You should notice that the node has been properly installed when the LED's become blank, and the host_responds is active.

Verify that the **bootp_response** has been set to disk by issuing the following command:

```
splstdata -b
```

Step 8: Run Verification Tests

Verify that the nodes are running properly by issuing the following commands:

```
SYSMAN_test
CSS_test                    * run only if you have a switch
spverify_config             * run only if your system is partitioned
jm_install_verify           * run only if using Resource Manager
jm_verify                   * run only if using Resource Manager
```

Verify **host_responds** and **switch_responds**, if you have a switch, are set to *yes* by issuing the following command:

```
spmon -d -G
```

Note: At this point, refer back to “High-Level Migration Steps” on page 107 to determine your next step in the migration process.

Migrate or Upgrade Nodes to AIX 4.2.1 or Later

PSSP 2.3 and PSSP 2.2 run on AIX 4.2.1. If your system has nodes currently at PSSP 2.2 and AIX 4.1.x and you only want to migrate the AIX level, you can do so without migrating the PSSP level. This way, you can wait until the AIX migration has successfully completed and that your system is stable enough for you to proceed with the PSSP migration.

It is a requirement that the control workstation already be migrated to AIX 4.2.1.

Migrate

Refer to "Migration Install of Nodes to AIX 4.2.1 and PSSP 2.3" on page 147 and complete steps 1-3, and 5-8.

For step 1, you do not have to set the <code_version> option.

For step 2, validate that you have the correct <code_version>.

Upgrade

If your system has nodes at AIX 4.2.0, you can upgrade them to AIX 4.2.1 using the upgrade approach by applying a PTF.

Complete "Step 1: Apply AIX 4.2.1 Upgrade on Node" on page 154 and "Step 2: Verify AIX Migration" on page 154.

Upgrade Nodes to AIX 4.2.1 and PSSP 2.3

Before proceeding with the steps in this section, be sure you have selected the correct migration path. If you are unsure, refer to Table 8 on page 146.

This method is used primarily when your existing configuration is at AIX 4.2.x and PSSP 2.2 and you want to update the nodes to AIX 4.2.1 and PSSP 2.3. This method applies AIX 4.2.1 PTF Service and preserves the current rootvg disk configuration and install/upgrade the AIX BOS file sets to AIX 4.2.1. The **pssp_script** installs and updates the PSSP 2.3 LPPs on top of current PSSP 2.2 LPPs.

Step 1: Apply AIX 4.2.1 Upgrade on Node

Issue the NFS **mount** command from the control workstation using **dsh** to mount the lppsource directory on the control workstation to the node. You can elect not to use **dsh** and issue the **mount** command on the node.

```
dsh -w <node> "/usr/sbin/mount <CWS>:   \
/spdata/sys1/install/<lppsource_name>/lppsource  /mnt"
```

Issue the **lslpp** and **installp** commands to update all listed LPPs on the node with AIX 4.2.1 service found in the lppsource directory. You can issue the commands directly from the node.

```
dsh -w <node> "/usr/sbin/lslpp -l -J  > /tmp/FILE.42"
dsh -w <node> "/usr/sbin/installp -acNgXd /mnt -f /tmp/FILE.42"
```

Step 2: Verify AIX Migration

Verify that the node has successfully been migrated to AIX 4.2.1 by issuing the following command:

```
dsh -w <node> "/bin/oslevel"
```

If the output of this command does not indicate AIX 4.2.1, issue the following command to return a list of AIX files not migrated to AIX 4.2.1. You may need to install AIX PTFs to migrate those file sets to AIX 4.2.1.

```
dsh -w <node> "/bin/oslevel -l 4.2.1.0"
```

Step 3: Enter Node Configuration Data

You need to properly set the appropriate SDR node object attributes for **lppsource_name**, **code_version**, and **bootp_response** for each node being upgraded. Use the **spbootins** command to update these fields.

```
spbootins -s no -p <code_version> -r customize \
-v <lppsource_name> -l <node_list>
```

- **-s no** prevents setup_server from running.
- **-p** <**code_version>** sets the node's PSSP level. Use this to indicate the PSSP level to install on the node. The value you choose must match the directory name you choose to place the PSSP installation files under in the /**spdata**/**sys1**/**install**/**pssplpp** directory during installation.
- **-r customize** sets the node's **bootp_response** value to *customize*.
- **-v** <**lppsource_name>** sets the node's lppsource name. Use this to indicate the level of AIX to which the node will be migrated. The name is based on the chosen directory that was set during the control workstation migration. Use the

subdirectory name that you loaded the lppsource into under **/spdata/sys1/install**.

- **-l** <**node_list**> specifies the list of nodes you are migrating. Either specify a comma-delimited list of node numbers, or a file containing one line of data which is a comma-delimited list of node numbers. The file can also contain comment lines (preceded by a #) and lines that are all white space. (This is a lowercase l, as in list.)

For example, to migrate nodes 1 and 2 to PSSP 2.3 where lppsource was placed in **/spdata/sys1/install/AIX421/lppsource**, issue the following command:

```
spbootins -s no -p PSSP-2.3 -r customize -v AIX421 -l 1,2
```

Step 4: Verify Installation Settings

Make sure that the SDR has the appropriate values specified in the following attributes for each of the nodes. Issue the following command to display the values:

```
splstdata -G -b
```

- response

  Nodes being migrated should be set to *customize*.

- lppsource_name

  The AIX level of the nodes to be migrated. For example, *AIX421*.

- pssp_ver

  The code_version of PSSP should be set to "PSSP-2.3" for nodes you are migrating.

Make sure that **/tftpboot/script.cust** has been properly updated for PSSP 2.3 modifications.

Step 5: Run setup_server to Configure the Changes

The **setup_server** command must be run to properly set up NIM on the control workstation by issuing the following command:

```
setup_server 2>&1 | tee /tmp/setup_server.out
```

The output will be saved in a log file called `setup_server.out`.

If you have a node defined as a boot/install server you must run **setup_server** out on that node.

```
dsh -w <boot/install_node> /usr/lpp/ssp/bin/setup_server
```

Step 6: Refresh System Partition-Sensitive Subsystems

The SDR has now been updated to reflect the new nodes that will run PSSP 2.3. You now need to refresh the System Partition Sensitive Subsystems on the control workstation and all nodes to pick up these changes. Run **syspar_ctrl** on the control workstation to refresh the subsystems on both the control workstation and on the nodes.

```
syspar_ctrl -r -G
```

Note: You can ignore any messages that you receive from the nodes you are migrating at this point because the migration process is not yet complete. Once the process is complete, you should no longer receive error messages.

Step 7: Disable Node From the Switch

If you do not have a switch in your SP System, skip this step.

If you want to bring the switch down for all nodes issue the **Equiesce** command. If you use the **Equiesce** command, you will need to later restart the switch using the **Estart** command. Issue the **Estart** command prior to the step where you "Verify the Nodes".

If you are migrating a few nodes, you must disconnect these nodes from the switch (if appropriate, first reassign the Primary Node or Primary Backup Node). To determine if one of the nodes you are migrating is a Primary or Primary Backup Node, or to reassign the Primary or Primary Backup Node, issue the **Eprimary** command. You must then execute the **Efence** command to disconnect nodes from the switch.

```
Efence -G -autojoin <node_number>
```

Step 8: Copy the PSSP 2.3 pssp_script to Nodes' /tmp

Copy the PSSP 2.3 version of pssp_script from the control workstation to the /**tmp** directory on each of the nodes you are migrating. If you are only updating one node, you can issue **rcp** from the node to copy pssp_script. If you are updating multiple nodes, use a **dsh** command. For example:

```
dsh -w <node> /usr/lpp/ssp/rcmd/bin/rcp <cws>: \
/spdata/sys1/install/pssp/pssp_script /tmp/pssp_script
```

where <*cws*> is the hostname for the control workstation and <*node*> is the hostname of a node.

Step 9: Execute the pssp_script on the Node

Execute the pssp_script that you copied to /**tmp** on all of the nodes you are migrating:

```
dsh -w <node> /tmp/pssp_script
```

You need to wait until the script has completed before proceeding to the next step. To determine if pssp_script is still running on the nodes, monitor the 3 digit LEDs and wait for them to turn blank. Check the **bootp_response** and ensure that it is set to disk by issuing the following command:

```
splstdata -G -b
```

Step 10: Reboot the Node

If your system contains a switch, you must reboot the node at this time so that changes to the kernel can take affect. Any other kernel change that may have occurred when you upgraded AIX would also require that you reboot the node at this time.

IBM suggests that you reboot the node at this time.

Step 11: Start System Partition-Sensitive Subsystems

If you rebooted your node in the last step, you can skip this step because this step would have been automatically performed when the node was rebooted.

To start the subsystems, do the following:

1. Remove the old subsystems by issuing:

   ```
   dsh -w <node> /usr/lpp/ssp/bin/syspar_ctrl -c
   ```

2. Add and start the new subsystems by issuing:

   ```
   dsh -w <node> /usr/lpp/ssp/bin/syspar_ctrl -A
   ```

To verify that the subsystems are running, refer to "Step 34: Verify System Partition-Sensitive Subsystems Have Started" on page 55.

Step 12: Run Verification Tests

Verify that the nodes are running properly by issuing the following commands:

```
SYSMAN_test
CSS_test                  * run only if you have a switch
spverify_config           * run only if your system is partitioned
jm_install_verify         * run only if using Resource Manager
jm_verify                 * run only if using Resource Manager
```

Verify **host_responds** and **switch_responds**, if you have a switch, are set to *yes* by issuing the following command:

```
spmon -d -G
```

Note: At this point, refer back to "High-Level Migration Steps" on page 107 to determine your next step in the migration process.

Perform Control Workstation Overwrite/Preservation Install

Before proceeding with the steps in this section, be sure you have selected the correct migration path. If you are unsure, refer to Table 7 on page 116.

You have selected to reinstall the control workstation by executing an overwrite install. This method causes you to perform manual steps similar to that of a new installation.

Step 1: Save spdata File System

For PSSP 2.1 and later control workstations, you must first save the spdata file system. Refer to "Step 7: Back Up Your Control Workstation" on page 111 for information on the commands to use to properly backup the spdata file system and export the spdata volume group.

Step 2: Save PSSP-Related Files

You need to save many of the PSSP related files since the rootvg / (root), /var, and /usr file systems will be recreated. The majority of the files deal with the SDR, installation, and authentication files working with Kerberos database. The following is the minimum list of PSSP files that you must save. You may also want to save any other AIX or user based files that currently exist on the control workstation.

The following is a minimum list of the files you must save:

- The contents of /**var**/**sdr** - (PSSP 1.2 only)
- The contents of /**var**/**kerberos**
- /**.k**
- /**.klogin**
- /etc/krb-srvtab
- /etc/krb.conf
- /etc/krb.realms
- /etc/hmacls - (PSSP 1.2 only)
- /usr/lpp/ssp/config/hmthresholds - (PSSP 1.2 only)

If you are keeping some AIX 3.2.5 nodes, you must also save the following files to preserve the **netinst** id.

- /etc/group
- /etc/security/group
- /etc/passwd
- /etc/security/passwd

Follow this procedure to save the PSSP files required for migration:

1. Create a file called **MigList** containing the following minimum set of file names:
   - /.k
   - /.klogin
   - /etc/krb-srvtab

- /etc/krb.conf
- /etc/krb.realms
- /etc/hmacls - (PSSP 1.2 only)
- /usr/lpp/ssp/config/hmthresholds - (PSSP 1.2 only)

2. Run the following tar command:

   ```
   tar -cvf PSSP.tar -L MigList /var/sdr /var/kerberos
   ```

   This creates a tar archive of the files listed previously, the SDR, and the Kerberos database. If you prefer saving the files on tape, substitute the name of a device for **PSSP.tar** in the following examples.

   To verify the tar file **PSSP.tar** is readable, run the following tar command:

   ```
   tar -tvf PSSP.tar
   ```

3. Copy **PSSP.tar** to another system or some other safe location before you reinstall AIX 4.2.1 on your control workstation.

Step 3: Optionally, Save Additional Control Workstation Files

In addition to saving the minimal list of files, you may also want to save other customized files to a second tar file in order to restore them to /**tmp** later and integrate your changes into the new system.

To create the tar file **my.archive**, use the tar command using the -cvf options. You then can update the tar file by using the tar command with the -uvf options. You should place all saved AIX based files into /tmp file systems for the tar execution.

```
tar -cvf /tmp/my.archive <target files>
tar -uvf /tmp/my.archive <more target files>
```

You should save the /**tmp**/**my.archive** file to tape, or move it to another workstation during control workstation installation.

Caution: Do not use the "MigList" method shown previously to tar the files, since untarring the files would result in overlaying the new versions of these files. Instead, you could copy the files you want to save to a directory in /tmp to tar. After reinstalling your system, carefully merge the changes with new versions of these files. Do not merely copy the old version of the file onto the new version.

The following is a list of files which will be changed during the migration. If you want to keep them, you can save them to a tar file named, for example, **my.archive**. This list is not a comprehensive list of everything that you could customize on your system, only those that relate to PSSP. There might be other AIX configuration files that you also should save depending on how you have customized your system.

File	Description
/etc/amd/amd-maps/*	Amd map files
/etc/bootptab.info	specified hardware ethernet address for SP nodes
/etc/cshutSeq	customer sequence used with cshutdown
/etc/cstartSeq	customer sequence used with cstartup
/etc/exports	NFS export directory lists
/etc/filesystems	File system information
/etc/group	Basic group attributes
/etc/hosts	name resolution
/etc/inetd.conf	Network TCP/UDP socket services
/etc/inittab	System boot information and execution
/etc/jmd_config.xxx	Configuration file for Resource Manager
/etc/logmgt.acl	Error Log Mgt for ACL priveleges
/etc/motd	Message of the Day
/etc/ncs/glb_site.txt	used with license servers
/etc/ntp.conf	ntp server information
/etc/ntp.drift	ntp time for synchronization
/etc/passwd	Basic user attributes
/etc/rc.tcpip	starts network TCP daemons
/etc/resolv.conf	domain name services
/etc/security/group	Extended group attributes
/etc/security/user	login control
/etc/security/passwd	Password information
/etc/services	network port services
/etc/snmpd.conf	system network manager
/etc/splm.allow	commands with log management
/etc/sysctl.acl /etc/sysctl.rootcmds.acl /etc/sysctl.pman.acl	Sysctl file for ACL priveleges
/etc/sysctl.conf	Sysctl configuration file for sysctl commands
/etc/syslog.conf	system logging daemon
/usr/lpp/ssp/config/hwevents	user exits for hardware state changes

Step 4: Perform Control Workstation BOS Overwrite/Preservation

This step recreates the current rootvg based file systems which removes all AIX based files from / (root), /var, and /usr file systems. It will then "install" new AIX 4.2.1 files and AIX LPP's to the control workstation. The difference between an Overwrite and Preservation installation is that an overwrite also erases user based file systems while a preservation does not effect user based file systems. You must have all the necessary AIX file sets and PTFs listed in the *Memo to Users* available

by AIX CD-ROM, tape, or from the NIM master during the BOS Overwrite/Preservation Installation.

Reference the AIX Installation Guide in chapters 1-3, for more detailed information. The following list provides some BOS Overwrite Installation hints:

- Backup your current system.
- Boot off your AIX CD-ROM or tape or set up the control workstation as a NIM client from a AIX 4.2.1 NIM master.
- Select option 1 "System Settings" on Installation and Settings menu to change for Preservation install. The default is Overwrite install.
- Select option 2 "Preservation Install" on the Change Method of Installation menu for Preservation choice.
- Select the proper hdisk(s) being used for rootvg. You may want to add or change the hdisk configuration for the control workstation.
- Customize your control workstation based on the documented PSSP requirements. This includes required AIX LPPs and PTFs being installed.

Step 5: Restore spdata File System

You may need to restore the spdata file system that was saved earlier by using the **backup** command. Issue the **restore** command to properly restore the spdata file system from the tape media.

```
restore -r q -f /dev/rmt0 -d /spdata -v
```

If you have previously exported the spdata volume group using the **exportvg** command, you may choose to now import the spdata volume group by issuing the **importvg** command:

```
importvg -y spdatavg -V <major #> <hdisk>
```

Step 6: Restore Control Workstation Files

You need to restore the PSSP related files on the control workstation. You should have saved these files using the tar command either to tape or to a tar file called PSSP.tar. Place the tape or the saved PSSP.tar file on the control workstation. Use the tar command to restore the PSSP files.

```
tar -xvf PSSP.tar
```

or

```
tar -xvf /dev/rmt0
```

You may have also saved other AIX or user based files from the PSSP control workstation configuration. It is best to save these files in /tmp file system first, and then carefully integrate updates or changes to AIX 4.2.1 based files. Place the tape or saved tar file /**tmp**/**my.archive** on the control workstation and use the tar command to extract the user based files on the control workstation.

To extract the information from a file where `my.archive` is the name of the file, issue:

```
tar -xvf /tmp/my.archive
```

To extract the information from a tape, issue:

```
tar -xvf /dev/rmt0
```

Note: When you restore the PSSP 1.2 SDR files on the control workstation, the PSSP 2.3 software will detect a migration activity. It updates the SDR files into the proper directory locations.

Step 7: Configure RS-232 Control Lines

Each frame in your system requires a serial port on the control workstation configured to accommodate the RS-232 line. For example, if you have two frames, configure two tty serial ports.

Enter a command similar to this example, which defines and configures an RS-232 line for parent adapter sa0 on port serial port 1:

```
mkdev -c tty -t tty -s rs232 -p sa0 -w s1
```

This example configures a second port of a two-frame system:

```
mkdev -c tty -t tty -s rs232 -p sa1 -w s2
```

Note: You can accept the default baud rate of 9600. When the System Monitor starts, it changes the rate to 19200.

Step 8: Configure Ethernet Adapters

Use **smit chinet** or the **chdev** command to configure each Ethernet adapter connecting your frames to the control workstation. For details on the correct use of **chdev**, see the AIX Commands Reference. the man pages, or the online information database.

Refer to your Control Workstation Worksheet in the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment*. for the IP addresses and netmask values of your Ethernet adapters.

Note: If the adapter is not yet defined or configured, use **smit mkinet** or the **mkdev** command instead of **smit chinet** or **chdev** to specify new IP host name and netmask values. This chapter discusses only the command line.

If using **chdev**, enter a command similar to this example, which configures an en0 adapter.

```
chdev -l en0 -a netaddr=129.33.41.1 -a \
netmask=255.255.255.0 -a state=up
```

If using **mkdev**, enter a command similar to this example, which defines and configures an en0 adapter.

```
mkdev -c if -s EN -t en -a netaddr=129.33.34.1 \
netmask=255.255.255.0 state=up -q
```

You can set values with transmit queue sizes for the network adapters. You should set the queue sizes based on the different adapter types.

- Ethernet and token ring - set to 160
- built-in Ethernets (node) - set to 150

Use the following command to modify TANSMIT Queue sizes.

```
chdev -P -l ent0 -a xmt_que_size=160
```

Step 9: Verify Step

Refer to the following table to proceed to the next step:

If you are migrating the control workstation from:	Proceed to:
PSSP 1.2 to PSSP 2.3	"Step 4: Verify AIX Migration" on page 120.
PSSP 2.1 to PSSP 2.3	"Step 3: Verify AIX Migration" on page 127.
PSSP 2.2 to PSSP 2.3	"Step 3: Verify AIX Migration" on page 137.

HACWS Migration Strategy

An HACWS configuration at the PSSP 2.3 level requires the following software on both control workstations:

- PSSP 2.3 (including the ssp.hacws 2.3.0.0 file set).
- Any level of AIX 4.2.1 or greater that is supported with PSSP 2.3. Refer to the *Memo to Users* to determine what levels of AIX are supported with PSSP 2.3.
- Any level of HACMP 4.2 or greater that is supported with the level of AIX that you are using. Refer to the appropriate HACMP documentation to determine what levels of HACMP are supported with the level of AIX that you are using or considering.

Whether or not you need to upgrade all three of these at the same time depends on your software levels before migration. You can choose to upgrade your HACWS configuration a little at a time, stopping along the way to run your system long enough to become confident that it is stable before proceeding to the next phase, as long as you run your HACWS configuration with a combination of AIX, HACMP and PSSP that is supported. For example, if your HACWS configuration currently has AIX 4.1.5, HACMP 4.1.1 and PSSP 2.2, you may choose to first migrate to HACMP 4.2.1 and run with AIX 4.1.5, HACMP 4.2.1 and PSSP 2.2, because that combination of software levels is supported. After you become confident that your system is stable, you can then migrate to AIX 4.2.1 and run with AIX 4.2.1, HACMP 4.2.1 and PSSP 2.2, because that combination of software levels is also supported. Finally, after you become confident that your system is stable, you can then complete your migration by migrating to PSSP 2.3 and run with AIX 4.2.1, HACMP 4.2.1 and PSSP 2.3.

If your HACWS configuration is at the PSSP 2.1 level, you may not migrate directly to PSSP 2.3 without migrating to AIX 4.2.1 or greater at the same time. This is because PSSP 2.1 is not supported with AIX 4.2.1 or greater, and PSSP 2.3 is not supported with anything less than AIX 4.2.1. You also might not have the ability to upgrade HACMP without upgrading AIX at the same time. For example, if you are running AIX 4.1.4 and HACMP 4.1.1, you could not migrate to HACMP 4.2.1 without migrating to AIX 4.1.5 or greater at the same time, because HACMP 4.2.1 is not supported with AIX 4.1.4. In this case (where you are running AIX 4.1.4, HACMP 4.1.1 and PSSP 2.1) you could not migrate to HACMP 4.2.1 without upgrading AIX at the same time, and you could not migrate to AIX 4.2.1 without upgrading both HACMP and PSSP at the same time, and you could not migrate to PSSP 2.3 without upgrading both AIX and HACMP at the same time, so you might plan to upgrade all three software products within the same service window. As an alternative, you could maintain a bit-by-bit upgrade strategy by migrating to PSSP 2.2 as an intermediate step, but you should consider whether it would be worth the additional effort.

If you implement a bit-by-bit HACWS migration strategy (within the rules outlined previously), you may also choose to upgrade AIX and/or HACMP on each control workstation separately and avoid an SP system outage. For example, you might take the backup control workstation offline to upgrade AIX and/or HACMP, while you keep the primary control workstation in production. After you finish migrating the backup control workstation, you could move control workstation services to it, and take the primary control workstation offline to perform the same migration of AIX and/or HACMP. If you use this approach to upgrade HACMP, you should find out whether the old and new HACMP software levels can coexist within the same

HACMP cluster. If they cannot coexist, then you cannot perform a graceful failover to move control workstation services. Instead you have to stop HACMP on the currently active control workstation, and wait for it to stop completely before starting HACMP on the takeover control workstation. Such a coexistence limitation should also encourage you to migrate the second control workstation very soon after the first, or a failure of the currently active control workstation would require manual intervention.

You cannot upgrade the PSSP software level within your HACWS configuration until both control workstations have been migrated to supported levels of both AIX and HACMP, and while you may be able to avoid an SP system outage by upgrading AIX and/or HACMP on each control workstation separately, you cannot use this technique to upgrade PSSP. You must upgrade PSSP on both control workstations at the same time, so there is no way to avoid an SP system outage while you upgrade PSSP.

At this point you should apply these rules to your situation, and plan your own strategy for migrating your HACWS configuration to PSSP 2.3.

High-Level HACWS Migration Instructions

By now you should have read "HACWS Migration Strategy" on page 164 and planned your HACWS migration strategy. If you have not done this, you should read the section now. Refer to the items in this section as you implement your HACWS migration strategy.

Backing Up Your HACWS Configuration

Before you begin your HACWS migration, you should backup the root volume group on each control workstation, and you should also backup the shared volume group which contains the /spdata file system. If anything goes wrong with your HACWS migration, you can recover by restoring the appropriate backup image(s). If you separate your HACWS migration into multiple service windows, then you should backup your HACWS configuration each time, in order to make sure the backup images are current.

You may backup the root volume group by issuing the mksysb command directly, or you may invoke the mksysb command through SMIT by issuing the command **smit mksysb**. You may backup the shared volume group which contains the /spdata file system by issuing the **savevg** command directly, or you may invoke the savevg command through SMIT by issuing the command **smit savevg**. Refer to the AIX documentation for more detailed instructions.

AIX Migration Considerations

Before you can migrate your HACWS control workstations to PSSP 2.3, you must install any level of AIX 4.2.1 or greater that is supported with PSSP 2.3. "Paths to Migrate the Control Workstation to PSSP 2.3 and AIX 4.2.1" on page 115 describes three different methods for upgrading AIX on a non-HACWS workstation. One of these methods involves saving selected configuration files, performing an overwrite or preservation install of AIX, and restoring the saved configuration files. This method is not suggested for upgrading AIX on an HACWS control workstation. You should upgrade AIX on an HACWS control workstation by either applying AIX

PTF service, if this is possible, or performing a migration install of AIX. Refer to the *AIX Installation Guide* for AIX installation instructions.

Once you have completed the installation procedure, you should verify the migration of AIX by running the following command:

```
oslevel
```

The output of this command is the current AIX software level. If you are not at the level you expected, you can also use this command to get a list of file sets that need to be updated. For example, to find out which file sets must be updated in order to reach AIX 4.2.1, issue the following command:

```
oslevel -l 4.2.1.0
```

You may need to install AIX PTFs in order to migrate those file sets to the desired AIX software level.

Whenever you make a significant change to your HACWS configuration, such as upgrading the AIX software level, you should always run the HACMP **clverify** utility to verify the HACMP cluster upon which your HACWS configuration is based. You should resolve any problems that **clverify** reports before you consider the AIX upgrade to be successful. However, if you are going to upgrade HACMP immediately after you upgrade AIX, then it makes sense to delay running **clverify** until after you upgrade HACMP. Refer to chapters 10 and 13 of the *HACMP Installation Guide* for more information about this utility.

In addition, you can use the **hacws_verify** command to check for problems with your HACWS configuration. You will be asked to run this command when you upgrade PSSP. However, if you upgrade AIX and then put your HACWS configuration back into production before you migrate to PSSP 2.3, then you should run this command after you start control workstation services on the primary control workstation.

If using:	Do this:
SMIT	TYPE smit hacws The High Availability Control Workstation Management window appears. SELECT Verify HACWS Installation and Configuration
hacws_verify	Enter: `/usr/sbin/hacws/hacws_verify`

Note: The **hacws_verify** command requires that the primary control workstation must be the active control workstation, or the one which is currently providing the control workstation services. If control workstation services are being provided by the backup control workstation, you cannot run this command.

HACMP Migration Considerations

Before you can migrate your HACWS control workstations to PSSP 2.3, you must install any level of HACMP 4.2 or greater that is supported with the level of AIX that you are using with PSSP 2.3. Refer to chapter 9 of the *HACMP Installation Guide* for HACMP migration installation instructions.

After you upgrade HACMP on both control workstations, you should run the HACMP **clverify** utility to verify the HACMP cluster upon which your HACWS

configuration is based. You should resolve any problems that **clverify** reports before you consider the HACMP upgrade to be successful. Refer to chapters 10 and 13 of the *HACMP Installation Guide* for more information about this utility.

After you upgrade HACMP on both control workstations, you need to identify to HACMP the HACMP pre- and post-event scripts that are provided by HACWS.

If using:	Do this:
SMIT	TYPE smit hacws The High Availability Control Workstation Management window appears. SELECT Identify Event Scripts to HACMP PRESS Enter to continue.
spcw_addevents	Enter: `/usr/sbin/hacws/spcw_addevents`

You already performed this task, when you originally installed HACWS. However, a new release of HACMP may introduce more cluster events, so you need to repeat this task, so that HACWS-supplied pre- and post-event scripts get defined to HACMP for the newly introduced cluster events. Failure to do this will not hurt the functionality of your HACWS configuration, but it will cause the **hacws_verify** command to fail.

In addition to the HACMP **clverify** utility, you can use the **hacws_verify** command to check for problems with your HACWS configuration. You will be asked to run this command when you upgrade PSSP. However, if you upgrade HACMP and then put your HACWS configuration back into production before you migrate to PSSP 2.3, then you should run the command after you start control workstation services on the primary control workstation.

If using:	Do this:
SMIT	TYPE smit hacws The High Availability Control Workstation Management window appears. SELECT Verify HACWS Installation and Configuration
hacws_verify	Enter: `/usr/sbin/hacws/hacws_verify`

Note: The **hacws_verify** command requires that the primary control workstation must be the active control workstation, or the one which is currently providing the control workstation services. If control workstation services are being provided by the backup control workstation, you cannot run this command.

PSSP Migration Steps

If your HACWS configuration is currently at PSSP 2.1, then proceed to “Migrate an HACWS Configuration from PSSP 2.1 to PSSP 2.3” on page 168. If your HACWS configuration is currently at PSSP 2.2, then proceed to “Migrate an HACWS Configuration from PSSP 2.2 to PSSP 2.3” on page 173.

Migrate an HACWS Configuration from PSSP 2.1 to PSSP 2.3

Follow the steps in this section if you are upgrading an HACWS configuration from PSSP 2.1 to PSSP 2.3.

Prerequisites

Before following the instructions in this section, you should:

1. Read "Preparing to Migrate" on page 109 and follow the instructions which describe how to prepare to migrate your SP system.
2. Read "HACWS Migration Strategy" on page 164 and plan your HACWS migration strategy.
3. Read "High-Level HACWS Migration Instructions" on page 165 and perform all of the tasks that must be done prior to upgrading the PSSP software level of your HACWS configuration.

Step 1: Verify Network Tunable Values

The suggested network tunable values for your control workstations are as follows:

```
thewall           16384
sb_max           163840
ipforwarding          1
tcp_sendspace     65536
tcp_recvspace     65536
udp_sendspace     32768
udp_recvspace     65536
tcp_mssdflt        1448
```

Verify that the network tunable values on both control workstations are correct. Use the **no** command to display these values. To display all of the network tunable values at once, issue the command:

```
/usr/sbin/no -a
```

To change the value of the **thewall** network tunable to 16384, issue the command:

```
/usr/sbin/no -o thewall=16384
```

When you change a network tunable value, the change takes effect immediately. However, the change is not preserved across a reboot. To make the change permanent, add the required no command to the bottom of the **/etc/rc.net** script. Refer to the **no** command man page for more information about changing network tunable values.

Step 2: Review Space Requirements for NIM Boot Images

Follow the instructions in "Step 5: Review Space Requirements for NIM Boot Images" on page 128.

Step 3: Review Space Requirements for /spdata

Follow the instructions in "Step 6: Review Space Requirements for /spdata" on page 128.

Step 4: Create Required /spdata Directories

Follow the instructions in “Step 7: Create Required /spdata Directories” on page 128.

Step 5: Copy the AIX 4.2.1 LPP Images

Follow the instructions in “Step 8: Copy the AIX 4.2.1 LPP Images” on page 128.

Step 6: Move the Existing LPP Images

Follow the instructions in “Step 9: Move the Existing LPP Images” on page 129

Step 7: Verify (Install/Copy) Correct Level of PAIDE (perfagent)

Follow the instructions in “Step 10: Verify (Install/Copy) Correct Level of PAIDE (perfagent)” on page 129.

Step 8: Copy the PSSP Images for PSSP 2.3

Follow the instructions in “Step 11: Copy the PSSP Images for PSSP 2.3” on page 130.

Step 9: Move the PSSP Images for PSSP 2.1

Follow the instructions in “Step 12: Move the PSSP Images for PSSP 2.1” on page 130.

Step 10: Install (Copy) the Basic AIX (mksysb) Image

Follow the instructions in “Step 13: Install (Copy) the Basic AIX (mksysb) Image” on page 130.

Step 11: Start Control Workstation Services on Primary Control Workstation

If you have not already done so, make sure that HACMP is running on both control workstations and the primary control workstation is the active control workstation, or the one that is providing the control workstation services.

Step 12: Stop Control Workstation Services While HACMP is Running

While HACMP is still running, you need to stop the control workstation applications on both control workstations. While the primary control workstation is the active control workstation, the backup control workstation will act as a client of the primary control workstation. You need to turn this off by issuing the following command on the backup control workstation:

```
/usr/sbin/hacws/spcw_apps -d
```

Next, you need to stop control workstation services on the primary control workstation by issuing the same command on the primary control workstation:

```
/usr/sbin/hacws/spcw_apps -d
```

Step 13: Install PSSP on Both Control Workstations

You need to install the PSSP 2.3 file sets on both control workstations. When the PSSP file sets are installed, files are copied into the /**spdata**/**sys1** directory. This requires special consideration for an HACWS configuration, because both control workstations share the same /spdata file system, which resides in a shared volume group. At this point the /spdata file system should be mounted on the primary control workstation, so files copied to the /**spdata**/**sys1** directory on the primary control workstation get written to the shared /spdata file system, and files copied to the /**spdata**/**sys1** directory on the backup control workstation get written to the backup control workstation's / (or root) file system. Since both control workstations share the same /spdata file system, the files that are copied to the backup control workstation are not needed, and they will get removed later by the **install_hacws** command in "Step 15: Complete PSSP 2.3 Installation on Both Control Workstations." In the meantime, you need to make sure there is at least 4 MB of free space in the / (or root) file system on the backup control workstation, or installation on the backup control workstation may fail.

You can install the PSSP 2.3 file sets on the primary control workstation from either the /**spdata**/**sys1**/**install**/**pssplpp**/**PSSP-2.3** directory, which is in the locally mounted /spdata file system, or you can install directly from the installation media. However, IBM suggests that you install the PSSP 2.3 file sets on the backup control workstation directly from the installation media. You should not mount the /spdata file system on the backup control workstation to install PSSP. Now you may proceed to install the PSSP 2.3 file sets on both control workstations. Remember that you must also install the **ssp.hacws 2.3.0.0** file set on both control workstations. You can perform file set installation from the command line by issuing the installp command, or you can use SMIT by issuing the **smit install_latest** command. Refer to the *AIX Installation Guide* for more details on how to use these commands.

Step 14: Authenticate as the Administrative Principal

Follow the instructions in "Step 16: Authenticate as the Administrative Principal" on page 132.

Step 15: Complete PSSP 2.3 Installation on Both Control Workstations

Run the **install_hacws** command.

If using:	Do this:
SMIT	TYPE smit hacws The High Availability Control Workstation Management window appears. SELECT Install and Configure HACWS. ENTER the node names of the primary control workstation and backup control workstation in the HOSTNAME fields. SELECT "yes" for Execute on both primary and backup? PRESS "Do" to complete option selection and install HACWS.
install_hacws	Enter: `/usr/sbin/hacws/install_hacws -p primary_hostname -b backup_hostname -s`

Note: Do this step from the primary control workstation.

Step 16: Verify the HACWS Configuration

Run the **hacws_verify** command.

If using:	Do this:
SMIT	TYPE smit hacws The High Availability Control Workstation Management window appears. SELECT Verify HACWS Installation and Configuration
hacws_verify	Enter: `/usr/sbin/hacws/hacws_verify`

Note: The **hacws_verify** command requires that the primary control workstation must be the active control workstation, or the one which is currently providing the control workstation services. If control workstation services are being provided by the backup control workstation, you cannot run this command.

Step 17: Run SDR and System Monitor Verification Test

Follow the instructions in "Step 18: Run SDR and System Monitor Verification Test" on page 132.

Step 18: Configure PSSP Services and Set Up Site Environment

Follow the instructions in "Step 19: Configure PSSP Services and Set Up Site Environment" on page 132.

Step 19: Unconfigure the NIM Master

Issue the following command on the primary control workstation:

```
delnimmast -l 0
```

To verify that the primary control workstation is no longer a NIM master, issue the following command on the primary control workstation:

```
/usr/sbin/lsnim
```

You should receive an error message which indicates that the lsnim command is not installed.

Since the backup control workstation is not the active control workstation, or the one that is currently providing the control workstation services, you cannot use the **delnimmast** command to unconfigure the backup control workstation as a NIM master. Instead you should issue the following commands on the backup control workstation:

```
/usr/sbin/nim -o remove psspspot
/usr/sbin/nim -o unconfig master
/usr/sbin/installp -u bos.sysmgt.nim.master
/usr/sbin/installp -u bos.sysmgt.nim.spot
```

To verify that the backup control workstation is no longer a NIM master, issue the **/usr/sbin/lsnim** command on the backup control workstation, and the command should fail the same as it did on the primary control workstation.

Step 20: Restart Control Workstation Services

Start control workstation services on the primary control workstation by issuing the following command:

```
/usr/sbin/hacws/spcw_apps -u
```

After this command completes on the primary control workstation, get the backup control workstation to synchronize with the primary control workstation by issuing the same command on the backup control workstation:

```
/usr/sbin/hacws/spcw_apps -u
```

Step 21: Run Verification Tests

Follow the instructions in “Step 24: Run Verification Tests” on page 134.

Step 22: Validate the Control Workstation

Your migration to PSSP 2.3 is now complete. You should test your HACWS configuration by performing a control workstation failover from the primary control workstation to the backup control workstation, and then failover from the backup control workstation back to the primary control workstation. Perform additional failover testing as you desire. Refer to “Step 25: Validate the Control Workstation” on page 135 for additional instructions.

At this point, refer back to “High-Level Migration Steps” on page 107 to determine the next step in your SP system migration process.

Migrate an HACWS Configuration from PSSP 2.2 to PSSP 2.3

Follow the steps in this section if you are upgrading an HACWS configuration from PSSP 2.2 to PSSP 2.3.

Prerequisites

Before following the instructions in this section, you should:

1. Read "Preparing to Migrate" on page 109 and follow the instructions which describe how to prepare to migrate your system.
2. Read "HACWS Migration Strategy" on page 164 and plan your HACWS migration strategy.
3. Read "High-Level HACWS Migration Instructions" on page 165 and perform all of the tasks that must be done prior to upgrading the PSSP software level of your HACWS configuration.

Step 1: Verify Network Tunable Values

The suggested network tunable values for your control workstations are as follows:

```
thewall           16384
sb_max           163840
ipforwarding          1
tcp_sendspace     65536
tcp_recvspace     65536
udp_sendspace     32768
udp_recvspace     65536
tcp_mssdflt        1448
```

Verify that the network tunable values on both control workstations are correct. Use the **no** command to display these values. To display all of the network tunable values at once, issue the command:

```
/usr/sbin/no -a
```

To change the value of the thewall network tunable to 16384, issue the command:

```
/usr/sbin/no -o thewall=16384
```

When you change a network tunable value, the change takes effect immediately. However, the change is not preserved across a reboot. To make the change permanent, add the required **no** command to the bottom of the **/etc/rc.net** script. Refer to the **no** command man page for more information about changing network tunable values.

Step 2: Review Space Requirements for NIM Boot Images

Follow the instructions in "Step 5: Review Space Requirements for NIM Boot Images" on page 138.

Step 3: Review Space Requirements for /spdata

Follow the instructions in "Step 6: Review Space Requirements for /spdata" on page 138.

Step 4: Create Required /spdata Directories

Follow the instructions in “Step 7: Create Required /spdata Directories” on page 138.

Step 5: Copy the AIX 4.2.1 LPP Images

Follow the instructions in “Step 8: Copy the AIX 4.2.1 LPP Images” on page 139.

Step 6: Verify (Install/Copy) Correct Level of PAIDE (perfagent)

Follow the instructions in “Step 9: Verify (Install/Copy) Correct Level of PAIDE (perfagent)” on page 139.

Step 7: Copy the PSSP Images for PSSP 2.3

Follow the instructions in “Step 10: Copy the PSSP Images for PSSP 2.3” on page 140.

Step 8: Install (Copy) the Basic AIX (mksysb) Image

Follow the instructions in “Step 11: Install (Copy) the Basic AIX (mksysb) Image” on page 140.

Step 9: Start Control Workstation Services on Primary Control Workstation

If you have not already done so, make sure that HACMP is running on both control workstations and the primary control workstation is the active control workstation, or the one that is providing the control workstation services.

Step 10: Stop Control Workstation Services While HACMP is Running

While HACMP is still running, you need to stop the control workstation applications on both control workstations. While the primary control workstation is the active control workstation, the backup control workstation will act as a client of the primary control workstation. You need to turn this off by issuing the following command on the backup control workstation:

```
/usr/sbin/hacws/spcw_apps -d
```

Next, you need to stop control workstation services on the primary control workstation by issuing the same command on the primary control workstation.

Step 11: Stop the amd Daemon on Both Control Workstations

You need to stop the amd daemon on both control workstations. Follow the instructions in “Step 12: Stop Daemons on the Control Workstation and Verify” on page 140 which explain how to stop the amd daemon. Disregard the instructuctions relating to the other PSSP daemons, because you already stopped those daemons in the previous step.

Step 12: Install PSSP on Both Control Workstations

You need to install the PSSP 2.3 file sets on both control workstations. When the PSSP file sets are installed, files are copied into the **/spdata/sys1** directory. This requires special consideration for an HACWS configuration, because both control workstations share the same /spdata file system, which resides in a shared volume group. At this point the /spdata file system should be mounted on the primary

control workstation, so files copied to the **/spdata/sys1** directory on the primary control workstation get written to the shared /spdata file system, and files copied to the **/spdata/sys1** directory on the backup control workstation get written to the backup control workstation's / (or root) file system. Since both control workstations share the same /spdata file system, the files that are copied to the backup control workstation are not needed, and they will get removed later by the **install_hacws** command in "Step 14: Complete PSSP 2.3 Installation on Both Control Workstations." In the meantime, you need to make sure there is at least 4 MB of free space in the / (or root) file system on the backup control workstation, or installation on the backup control workstation may fail.

You can install the PSSP 2.3 file sets on the primary control workstation from either the **/spdata/sys1/install/pssplpp/PSSP-2.3** directory, which is in the locally mounted /spdata file system, or you can install directly from the installation media. However, IBM suggests that you install the PSSP 2.3 file sets on the backup control workstation directly from the installation media. You should not mount the /spdata file system on the backup control workstation to install PSSP. Now you may proceed to install the PSSP 2.3 file sets on both control workstations. Remember that you must also install the **ssp.hacws 2.3.0.0** file set on both control workstations. You can perform file set installation from the command line by issuing the installp command, or you can use SMIT by issuing the **smit install_latest** command. Refer to the *AIX Installation Guide* for more details on how to use these commands.

Step 13: Authenticate as the Administrative Principal

Follow the instructions in "Step 14: Authenticate as the Administrative Principal" on page 141.

Step 14: Complete PSSP 2.3 Installation on Both Control Workstations

Run the **install_hacws** command.

If using:	Do this:
SMIT	TYPE smit hacws The High Availability Control Workstation Management window appears. SELECT Install and Configure HACWS. ENTER the node names of the primary control workstation and backup control workstation in the HOSTNAME fields. SELECT "yes" for Execute on both primary and backup? PRESS "Do" to complete option selection and install HACWS.
install_hacws	Enter: `/usr/sbin/hacws/install_hacws -p primary_hostname -b backup_hostname -s`

Note: Do this step from the primary control workstation.

Step 15: Verify the HACWS Configuration

Run the **hacws_verify** command.

If using:	Do this:
SMIT	TYPE smit hacws The High Availability Control Workstation Management window appears. SELECT Verify HACWS Installation and Configuration
hacws_verify	Enter: `/usr/sbin/hacws/hacws_verify`

Note: The **hacws_verify** command requires that the primary control workstation must be the active control workstation, or the one which is currently providing the control workstation services. If control workstation services are being provided by the backup control workstation, you cannot run this command.

Step 16: Run SDR and System Monitor Verification Test

Follow the instructions in "Step 16: Run SDR and System Monitor Verification Test" on page 141.

Step 17: Configure PSSP Services and Set Up Site Environment

Follow the instructions in "Step 17: Configure PSSP Services and Set Up Site Environment" on page 142.

Step 18: Restart Control Workstation Services

Start control workstation services on the primary control workstation by issuing the following command:

```
/usr/sbin/hacws/spcw_apps -u
```

After this command completes on the primary control workstation, get the backup control workstation to synchronize with the primary control workstation by issuing the same command on the backup control workstation.

Step 19: Run Verification Tests

Follow the instructions in "Step 21: Run Verification Tests" on page 143.

Step 20: Validate the Control Workstation

Your migration to PSSP 2.3 is now complete. You should test your HACWS configuration by performing a control workstation failover from the primary control workstation to the backup control workstation, and then failover from the backup control workstation back to the primary control workstation. Perform additional failover testing as you desire. Refer to "Step 22: Validate the Control Workstation" on page 144 for additional instructions.

At this point, refer back to "High-Level Migration Steps" on page 107 to determine the next step in your SP system migration process.

Post-Migration Activity

This section discusses the activities you should perform after a successful migration. It also discusses recovery procedures you should perform if the migration process was not successful.

Remove Obsolete Files and Resources

After migrating the control workstation to PSSP 2.3, you may be supporting nodes at mixed levels of AIX and PSSP for a period of time. Once all the nodes have been migrated to AIX level *n* and PSSP level *p* and none of the PSSP levels that you are still supporting are dependent on AIX level *n-1*, you can remove all NIM resources and files associated with this old level of AIX and PSSP. You may want to back up these files prior to removing them if there is any chance that you may one day need to reinstall nodes at this level of AIX and PSSP. You can remove the files listed in the following list.

- All of the NIM resources associated with AIX level *n-1*; the lppsource, spot, and mksysb.
- All of the AIX files under /**spdata**/**sys1**/**install** associated with AIX level *n-1*.
- All of the PSSP files under /**spdata**/**sys1**/**install**/**pssplpp** associated with PSSP level *p-1*.

For example, if you completed migrating all of your nodes from PSSP 2.1 and AIX 4.1.5 to PSSP 2.3 and AIX 4.2.1 and you do not have any PSSP 2.2 nodes that are running on AIX 4.1.5, you may now remove the following NIM resources and files. Assume that your mksysb image is named **bos.obj.ssp.415** and that your lppsource is stored in the directory named AIX415.

1. Remove the NIM resources associated with AIX 4.1.5; the lppsource, spot, and mksysb. To remove the lppsource resource, issue the command:

   ```
   nim -o remove lppsource_AIX415
   ```

2. Remove the spot and all files that NIM generated for this spot by issuing the following command:

   ```
   nim -o remove spot_AIX415
   ```

3. Remove the mksysb resource by first displaying a list of all resources of type mksysb by issuing the command:

   ```
   lsnim -t mksysb -l
   ```

   Determine which mksysb is associated with bos.obj.ssp.415. For example, if after examining the output of the previous command, you see that bos.obj.ssp.415 is associated with mksysb_x, then remove the mksysb_x resource by issuing the command:

   ```
   nim -o remove mksysb_x
   ```

   If the resource removal fails, you may first need to deallocate the resources from all clients using the **unallnimres** command.

   Then, remove the AIX files associated with AIX 4.1.5 (lppsource, mksysb) and PSSP 2.1 by issuing the following commands:

   ```
   rm -r /spdata/sys1/install/AIX415
   rm -r /spdata/sys1/install/images/bos.obj.ssp.415
   rm -r /spdata/sys1/install/pssplpp/PSSP-2.1
   ```

Recovery Procedures

If you encounter a migration failure which you cannot resolve, you can call an IBM service representative for additional help. In addition, refer to the following list for a basic set of instructions for recovering your system. You may use the backups you made prior to the migration.

Recovering from a PTF Migration Failure

- If you are recovering from a failed PTF installation on the control workstation, clean up the possible failed installation by issuing:

  ```
  /usr/sbin/installp -C
  ```

  and then reject the applied PTFs on the control workstation by issuing:

  ```
  /usr/sbin/installp -r ALL
  ```

- If the PTFs failed on SP nodes, clean up possible failed installation by issuing:

  ```
  dsh -w <node> /usr/sbin/installp -C
  ```

  and reject the applied PTFs on the nodes by issuing:

  ```
  dsh -w <node> /usr/sbin/installp -r ALL
  ```

Recovering from a Control Workstation Migration Failure

If you are recovering from a control workstation migration failure, perform the following steps:

1. Insert the tape, the mksysb backup, that you created in “Step 7: Back Up Your Control Workstation” on page 111.
2. Change the key to the service position. If your control workstation is a PCI-based RS/6000, press the F2 key at boot time. This provides a menu. From this menu, select the tape as boot device and press Enter. If your control workstation is a microchannel-based RS/6000, follow the instructions on the screen.
3. Select the disk(s) to install the rootvg volume group.
4. Re-install the control workstation using the mksysb install option.
5. Wait for the control workstation to reboot.
6. Login as root user after successful completion of the restore.
7. Authenticate as the Administrative Principal by issuing the **kinit** command. For example:

   ```
   kinit root.admin
   ```

8. Complete the PSSP installation on the control workstation by issuing the command:

   ```
   install_cw
   ```

9. Check to see if your SDR is correct by issuing the **spmon -d** command and the **splstdata** command. If the SDR is corrupt, you may restore a previously archived SDR by issuing the command:

   ```
   sprestore_config <SDR_archive_name>
   ```

10. Restore any other files that you may have saved.

Recovering from a Node Migration Failure

If you are recovering from an SP node migration failure, perform the following steps:

1. Place the SP node mksysb image file that you previously saved in “Step 8: Back Up Your Nodes” on page 112. into the directory **/spdata/sys1/install/images**.
2. Update the SDR to match the proper settings for the SP node being restored. Issue the **spbootins** command with the correct options **-r** <**install>**, **-v** <**lppsource_name>**, **-p** <**code_version>**, and **-i** <**old_mksysb_image>** for the node.
3. Network boot the SP node using the **nodecond** command or the GUI. This will reinstall the SP node back to the same AIX and PSSP level of the backup mksysb image.

   ```
   nodecond -G <frame_id> <slot_id> &
   ```

4. Restore any other user volume groups or files that were saved in “Step 8: Back Up Your Nodes” on page 112.

Chapter 5. Reconfiguring the RS/6000 SP System

This chapter explains the tasks necessary to manage your RS/6000 SP hardware. It shows you the SP commands before and after you make hardware changes, and how to expand your system with additional hardware.

Notes:

- It is very important that you consult the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment Guide* prior to reconfiguring your system to understand the implications of adding, deleting, or modifying any hardware.
- You should run the verification test that checks for the correct installation of the SP System Monitor. Note that you can access SMIT using Perspectives by typing **perspectives &** to bring up the Perspectives Launch Pad and then selecting **smit SP_verify** from the Launch Pad.

  If using SMIT:

  – TYPE smit SP_verify

    The RS/6000 SP Installation/Configuration Verification Menu appears.

  – SELECT System Monitor Installation

  – PRESS Do to run the tests

    You should run the verification test that checks for the correct installation of the SP System Monitor. You can run the verification test from SMIT panels or from the command line by issuing **spmon_itest**.

  If using the command line, issue::

  ```
  spmon_itest
  ```

  After the tests are run, the system creates logs in **/var/adm/SPlogs** called **spmon_itest.log**.
- To learn more about the implications of changing IP addresses and host names, refer to the appendix titled "IP Address and Host Name Changes for SP Systems" in the PSSP Administration Guide.

Adding a Frame

When you add a frame to your RS/6000 SP System, you should plan how it fits into your network configuration. Consider the number of new nodes and how many interfaces they will have when planning your network configuration. Record this information in your Frame and Node Configuration Worksheets, located in the *Planning, Volume 2, Control Workstation and Software Environment*. Both the *Planning, Volume 1* and the *Planning, Volume 1* and the *Planning, Volume 2* offer information to help you with these decisions.

If your existing system has multiple partitions defined and you want to add a frame that has a switch, you need to bring the system down to one partition using the **Eunpartition** command before you can add the additional frame.

© Copyright IBM Corp. 1995, 1997

If you are running with system partitions, adding a new frame to an existing system partition or to a new system partition requires a different switch topology file. The system administrator must do the following:

1. Select a new system partitioning configuration.
2. Reconfigure the system partitions.

IBM suggests that you add frames only to the end of your system otherwise you will have to reconfigure the System Data Repository (SDR).

After you plan the configuration, follow these steps to add the frame and its nodes to your RS/6000 SP System, referring to your worksheets as necessary. Many steps include a reference to a previous chapter where it was explained as part of the initial installation and integration process.

Note: Performing this task requires that your identity be authenticated as an authorized user of the system management commands and SP System Monitor GUI interfaces shown in the following steps. You do this by issuing the **kinit** command to obtain a ticket from the RS/6000 SP authentication services, specifying the administrative principle name that was used when authentication was set up.

See the section on using RS/6000 SP authentication services in the *Administration Guide* for more information.

Step 1: Connect Frames to Your Control Workstation

Connect RS-232 and Ethernet cable from the new RS/6000 SP System frame to the control workstation according to your Frame Configuration Worksheet.

Step 2: Power On Frames and Switches

If the frames and switches are not already powered on, turn them on.

Step 3: Configure the RS-232 Control Line

Each frame in your RS/6000 SP system requires a serial port on the control workstation configured to accommodate the RS-232 line. Use SMIT or the **mkdev** command to define a serial port for each frame.

See “Step 5: Configure RS-232 Control Lines” on page 16 for more information.

Step 4: Configure the Ethernet Adapter (Optional)

Use SMIT or the **mkdev** command to configure the Ethernet adapter connecting your SP frame to the control workstation.

See “Step 7: Configure Control Workstation Ethernet Adapters” on page 17 for more information.

Step 5: Enter Frame Information and Reinitialize the SDR

Enter information about your RS/6000 SP frames using SMIT or the **spframe** command.

This step creates frame objects in the SDR for each frame in your SP system. At the end of this step, the SDR is reinitialized if you specify **-r yes** on the **spframe**

command, resulting in the creation of Node Objects for each node attached to your frames. If frames are not contiguously numbered, repeat sequence for each series of contiguous frames. To save time, do not specify reinitialization of System Data Repository until you are entering final series of contiguous frames. After adding a frame, only the userid used to add the frame information can be used to view the added frame information. To use other userids, edit **/spdata/sys1/spmon/hmacls** file to add additional userids. Run **hmadm setacls** to update the hardmon daemon with the additional userids.

See "Step 23: Enter Frame Information and Reinitialize the SDR" on page 42 for more information.

Step 6: Verify Frame Information

All frames must be powered up and connected to the control workstation so that the nodes are automatically detected and added to the SDR. For more information, refer to "Step 25: Verify Frame Information" on page 44.

Step 7: Update the State of the Supervisor Microcode

Refer to "Step 26: Update the State of the Supervisor Microcode" on page 44 for more information.

Step 8: Add Nodes to the System

1. To complete this task, follow installation steps "Step 26: Update the State of the Supervisor Microcode" on page 44 through "Step 23: Enter Frame Information and Reinitialize the SDR" on page 42 and "Step 24: Verify System Monitor Installation" on page 43 and proceeding through the rest of the chapter.

   Note: Because you are adding a new frame, you must do "Step 40: Configure Control Workstation as Boot/Install Server" on page 62.

2. If you are running with system partitions, make sure the SP_NAME environment variable on the control workstation is set to the correct system partition. When you add a node, you must be in the environment of the node's partition. By default, new nodes are added to the default partition.

Step 9: Refresh System Partition-Sensitive Subsystems

To refresh the subsystems, issue the following command on the control workstation:

```
syspar_ctrl -r -G
```

This command refreshes all the subsystems in each partition such as **hats** and **hb** so that they recognize the new hardware.

Step 10: Stop and Restart the Resource Manager in all Affected Partitions

For more information on this step, see the section on managing RS/6000 SP resources in the *Administration Guide*.

Deleting a Frame

When you delete a frame from your system, you should first plan how the change will affect the remainder of your system. Consider the workload and applications currently running on the frame and plan how to transfer the workload and applications to another frame. For example, if the frame you want to delete contains the boot/install server, you may need to configure a new boot/install server in the remaining frames.

In most cases, deleting a frame will require that you select a new topology file and a new partition configuration. For example, if your existing system contains 32 nodes, you are using a 2–switch topology file. If you remove a frame containing 16 nodes, you need to select a 1–switch topology file and you may need to repartition.

IBM suggests that you delete frames only at the end of your system otherwise you will have to reconfigure the System Data Repository (SDR).

Use SMIT or the **spdelfram** command to delete frame information from the SDR.

Note: Performing this task requires that your identity be authenticated as an authorized user of the system management commands and SP System Monitor GUI interfaces shown in the following steps. You do this by issuing the **kinit** command to obtain a ticket from the RS/6000 SP authentication services, specifying the administrative principle name that was used when authentication was set up.

See the section on using RS/6000 SP authentication services in the *Administration Guide* for more information.

Step 1: Stop the Resource Manager Server

Stop the resource manager server in the system partition(s) that the frame belongs to by following one of the procedures described in the following table:

If using:	Do this:.
SMIT	**TYPE** **smit RM_options** **SELECT** Stop the Resource Manager **PRESS** **Do** to complete the operation
jm_stop	Enter: `jm_stop`

For more information, see the section on managing RS/6000 SP resources in the *Administration Guide*.

Step 2: Shut Down All the Nodes in the Frame

Use the SP System Monitor GUI, Perspectives, or the **cshutdown** command to shut down the nodes.

If using:	Do this:.
System Monitor GUI	**SELECT** SP → Display Layouts **SELECT** node to be displayed **SELECT** Node front panel layout **PRESS** Display Node Layout **PRESS** Off **SELECT** Power off options
Perspectives	**SELECT** Hardware Perspective from the Launch Pad **SELECT** Correct current partition **SELECT** Actions → cws/system/syspars → Set Current Partition **SELECT** Nodes Pane **SELECT** all the nodes **SELECT** Actions → Nodes → Power on **PRESS** Power Off icon **PRESS** cshutdown **PRESS** Apply
cshutdown	Enter: `cshutdown`

Step 3: Delete Frame Information from the SDR

If using:	Do this:.
SMIT	**TYPE** **smit delete_data** • The Delete Data Information window appears **SELECT** Delete Frame Information • The Delete Frame Information window appears **TYPE** The start frame and frame count.
spdelfram	This example deletes the last two frames in a four-frame system: `spdelfram -G 3 2`

Step 4: Reconfigure the System Partitions (Optional)

Note: Complete this step if you are running multiple system partitions.

Follow the instructions in the *Administration Guide* to do the following:

1. Select a new system partitioning configuration.
2. Reconfigure the system partitions.

Step 5: Refresh System Partition-Sensitive Subsystems

To refresh the subsystems, issue the following command on the control workstation:

```
syspar_ctrl -r -G
```

This command refreshes all the subsystems in each partition such as **hats** and **hb** so that they recognize the new hardware.

Step 6: Restart the SP System Monitor GUI and Perspective

To restart:	Do this:.
System Monitor GUI	Enter: `spmon -g`
Perspectives &	Enter: `perspectives`

Step 7: Restart the Resource Manager Server

If using:	Do this:.
SMIT	**TYPE** **smit RM_options** **SELECT** Start the Resource Manager **PRESS** **Do** to complete the operation
jm_start	Enter: `jm_start`

Adding Nodes

When you add nodes to an existing frame, you need to know which nodes provide their boot/install service. You can configure a new boot/install server for these nodes or add them to an existing boot/install server as clients. Record this information on your Frame and Node Configuration Worksheets and refer to them as you perform these steps. The worksheets can be found in the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment.*

For more information on adding an extension node, refer to “Install Extension Nodes” on page 82.

Note the following:

- Performing this task requires that your identity be authenticated as an authorized user of the system management commands, SP System Monitor GUI interfaces, and Perspectives. You do this by issuing the **kinit** command to obtain a ticket from the RS/6000 SP authentication services, specifying the administrative principle name that was used when authentication was set up.

  See the section on using RS/6000 SP authentication services in the *Administration Guide* for more information.

- When you add a node, ensure that the switch adapters are compatible with the switch adapters in the rest of your system and ensure that the nodes you are adding are supported by the switch in the system. For example, the SP Switch-8, only handles eight nodes.
- You cannot add a node in a location already defined for a SP Switch Router Adapter node. View the System Partition Map to determine which slots are valid for adding nodes.
- Do these steps in the system partition to which you add the nodes.

Note to High Performance Switch-LC8 and SP Switch-8 Users; Since the switch node numbers for these switches are computed sequentially, it is possible for new nodes to be incorrectly numbered when a group of nodes is added. You can avoid this problem by having the IBM Customer Engineer connect the nodes one at a time in an ascending fashion. Between each node, you should verify that a node object has been created with the proper switch node number.

Step 1: Connect New Nodes to the Frame

Your IBM Customer Engineer (CE) performs this step.

Step 2: Update the State of the Supervisor Microcode

Refer to “Step 26: Update the State of the Supervisor Microcode” on page 44 for more information.

Step 3: Set Up, Power, and Configure the Nodes

To complete this task, follow the installation steps starting at “Step 27: Enter Required Node Information” on page 45 and proceed through the rest of the chapter.

Notes:

1. Only the new node needs to be selected in “Step 27: Enter Required Node Information” on page 45. Any production nodes chosen will be powered off.
2. Only the new node needs to be selected in “Step 28: Acquire Hardware Ethernet Addresses” on page 47. Any production nodes chosen will be powered off and rebooted.
3. If you have a switch and are using system partitions, in “Step 30: Configure Additional Adapters for Nodes” on page 50 the starting node is the first node in the system partition an number of nodes is the number of nodes in the system partition.
4. When you add a node, you must run **setup_server** on the control workstation (see “Step 40: Configure Control Workstation as Boot/Install Server” on page 62) or on the boot/install server.

Step 4: Refresh System Partition-Sensitive Subsystems

To refresh the subsystems, issue the following command on the control workstation:

```
syspar_ctrl -r -G
```

This command refreshes all the subsystems in each partition such as **hats** and **hb** so that they recognize the new hardware.

Step 5: Restart System Monitor GUI or Perspectives

Exit the System Monitor GUI. To restart the SP System Monitor GUI, enter:

```
spmon -g
```

To restart Perspectives, enter:

```
perspectives &
```

Step 6: Stop and Restart the Resource Manager Server

Stop and restart the resource manager server in the system partition. For more information, see the section on managing RS/6000 SP resources in the *Administration Guide*.

Deleting Nodes

Note:

- Performing this task requires that your identity be authenticated as an authorized user of the system management commands and SP System Monitor GUI interfaces shown in the following steps. You do this by issuing the **kinit** command to obtain a ticket from the RS/6000 SP authentication services, specifying the administrative principle name that was used when authentication was set up.

  See the section on using RS/6000 SP authentication services in the *Administration Guide* for more information.

- Do these steps in the system partition from which you delete the nodes.

Note:

If you are deleting an extension node, you need to issue the **enrmnode** command followed by the **enrmadapter** command. For specific instructions, refer to the PSSP System Administration Guide.

Step 1: Stop the Resource Manager Server

Stop the resource manager server in the system partition that the nodes belong to by following one of the procedures described in the following table:

If using:	**Do this:.**
SMIT	**TYPE** **smit RM_options** **SELECT** Stop the Resource Manager **PRESS** **Do** to complete the operation.
jm_stop	Enter: `jm_stop`

Step 2: Shut Down the Nodes

Use the SP System Monitor GUI, Perspectives, or the **cshutdown** command to shut down the nodes.

If using:	Do this:.
System Monitor GUI	**SELECT** SP → Display Layouts **SELECT** node to be displayed **SELECT** Node front panel layout **PRESS** Display Node Layout **PRESS** Off **SELECT** Power off options row.
Perspectives	**SELECT** Hardware Perspective from the Launch Pad **SELECT** Correct current partition **SELECT** Actions → cws/system/syspars → Set Current Partition **SELECT** Nodes Pane **SELECT** all the nodes **SELECT** Actions → Nodes → Power on **PRESS** Power Off icon **PRESS** cshutdown **PRESS** Apply
cshutdown	Enter: `cshutdown`

Step 3: Disconnect the Node from the Frame

Your IBM Customer Engineer performs this step.

Step 4: Delete Node Information From the SDR

Use SMIT or the **spdelnode** command to delete node information from the SDR.

If using:	Do this:.
SMIT	**TYPE** **smit delete_data** • The Delete Data Information window appears **SELECT** Delete Node Information • The Delete Node Information window appears **TYPE** Start Frame, Start Slot, and Node Count **or** The Node List. **PRESS** **Do**
spdelnode	To delete the SDR information for the 16 nodes in frame 3, enter: `spdelnode 3 1 16`

Step 5: Refresh System Partition-Sensitive Subsystems

To refresh the subsystems, issue the following command on the control workstation after deleting the node:

```
syspar_ctrl -r -G
```

This command refreshes all the subsystems in each partition such as **hats** and **hb** so that they recognize that the hardware was deleted.

Step 6: Restart the Resource Manager Server

If using:	Do this:.
SMIT	**TYPE** **smit RM_options** **SELECT** Start the Resource Manager **PRESS** **Do** to complete the operation
jm_start	Enter: `jm_start`

Replacing a Node with an Equivalent Node

Follow the steps in this section to replace a node in one of your frames with an equivalent node. Equivalent nodes have the same adapters and configuration data, and have the same node type. Note that if you are replacing a 604 high node with another 604 high node, you must also ensure that the microcode level of the 604 high node is correct. Refer to “Step 26: Update the State of the Supervisor Microcode” on page 44 for more information.

Replacing a node with an equivalent node means removing one node and adding another in its place. Before you do this, you need to determine what applications are currently running on the node. You may need to plan to transfer these applications to another node on your system. Also, if the node you want to delete serves as the boot/install server or as a primary node, you may need to transfer the responsibilities to one of the remaining nodes.

- Be sure to back up any local data you want to preserve.
- Performing this task requires that your identity be authenticated as an authorized user of the system management commands, SP System Monitor GUI, and Perspectives. You do this by issuing the **kinit** command to obtain a ticket from the RS/6000 SP authentication services, specifying the administrative principle name that was used when authentication was set up.

  See the section on using RS/6000 SP authentication services in the *Administration Guide* for more information.
- Do these steps in the system partition in which you replace the nodes.

Step 1: Shut Down the Node and Power It Off

Prior to shutting down the node, make a list of all the applications and programs running on the node such as the Resource Manager and stop them from running.

Use the SP System Monitor GUI, Perspectives, or the **cshutdown** command to shut down the nodes.

If using:	Do this:.
System Monitor GUI	**SELECT** SP → Display Layouts **SELECT** node to be displayed **SELECT** Node front panel layout **PRESS** Display Node Layout **PRESS** Off **SELECT** Power off options
Perspectives	**SELECT** Hardware Perspective from the Launch Pad **SELECT** Correct current partition **SELECT** Actions → cws/system/syspars → Set Current Partition **SELECT** Nodes Pane **SELECT** all the nodes **SELECT** Actions → Nodes → Power on **PRESS** Power Off icon **PRESS** cshutdown **PRESS** Apply
cshutdown	Enter: `cshutdown`

Step 2: Replace the Old Node with the New One and Power It On

Your IBM Customer Engineer performs this step.

When the node is powered on, the node supervisor contacts the frame supervisor and informs it that it is running. The frame supervisor updates the **hardmon** daemon, running on the control workstation, that a new node has been added to the system.

Step 3: Update the State of the Supervisor Microcode

Perform “Step 26: Update the State of the Supervisor Microcode” on page 44.

Step 4: Delete NIM Client

Delete the NIM client on the boot/install server for the node you are replacing by issuing the **delnimclient** command. For example, to delete the NIM client for node number 3, issue:

```
delnimclient -l 3
```

Step 5: Acquire the Hardware Ethernet Address

This step takes the hardware Ethernet address for your new node (either from the node itself or from a file), puts it in the Node Object of the SDR, and sets up the **/etc/bootptab** file on the boot/install server.

Note: If you have information for the node being replaced in **/etc/bootptab.info**, be sure to remove the old address and then add the new Ethernet address.

Use SMIT or the **sphrdwrad** command to write the hardware Ethernet address to the SDR.

See “Step 28: Acquire Hardware Ethernet Addresses” on page 47 for more information.

Step 6: Set Up Nodes To Be Installed

Use SMIT or issue the **spbootins** command to change the default boot/install information in the Node Objects in the SDR so that you can indicate a different bootp response for nodes to be installed. This step also runs the **setup_server** command on all affected server nodes so that the nodes served is installed accordingly at power-up.

Step 7: Restart Perspectives or the System Monitor GUI

Exit the System Monitor GUI. To restart the SP System Monitor GUI, enter:

```
spmon -g
```

To restart Perspectives, enter:

```
perspectives &
```

Step 8: Network Boot the New SP Node

You can network boot the nodes using either Perspectives or the System Monitor GUI.

If using:	Do this:.
Perspectives	**SELECT** the Nodes Pane of the Hardware Perspective **SELECT** Nodes to network boot **PRESS** Actions → Nodes → Netboot **PRESS** Nodes **Select** Net Boot **PRESS** Apply
System Monitor GUI	**SELECT** SP → Global Commands • The Global Commands panel appears. **SELECT** The new node **SELECT** Net boot **PRESS** **Do** • The SP System Monitor boots the new node. • The network boot status window appears.
Note: See the chapter on using the system monitor and Perspectives in the *Administration Guide* for more information.	

Step 9: Run Post—installation Procedures

Set up the new nodes for any additional tools you use to manage your RS/6000 SP System environment.

See Table 6 on page 85 for a listing of information on the procedures for facilities.

Replacing a Node with a Different Type of Node

Follow the steps in this section to replace a node with a different type of node in one of your frames.

- Be sure to back up any local data you want to preserve from the node.
- Performing this task requires that your identity be authenticated as an authorized user of the system management commands, System Monitor GUI interfaces, and Perspectives. You do this by issuing the **kinit** command to obtain a ticket from the RS/6000 SP authentication services, specifying the administrative principle name that was used when authentication was set up.

  See the section on using RS/6000 SP authentication services in the *Administration Guide* for more information.
- Do these steps in the system partition in which you replace the nodes.

Note to High Performance Switch-LC8 and SP Switch-8 Users; Since the switch node numbers for these switches are computed sequentially, it is possible for new nodes to be incorrectly numbered when a group of nodes is added. You can avoid this problem by having the IBM Customer Enginner connect the nodes one at a time in an ascending fashion. Between each node, you should verify that a node object has been created with the proper switch node number.

Step 1: Shut Down the Node and Power It Off

Use Perspectives, the SP System Monitor GUI, or the **cshutdown** command to shut down the nodes. You will also need to disconnect the node from the switch using the Efence command.

If using:	Do this:.
Perspectives	**SELECT** Hardware Perspective from the Launch Pad **SELECT** Correct current partition **SELECT** Actions → cws/system/syspars → Set Current Partition **SELECT** Nodes Pane **SELECT** all the nodes **SELECT** Actions → Nodes → Power on **PRESS** Power Off icon **PRESS** cshutdown **PRESS** Apply
System Monitor GUI	**SELECT** SP → Display Layouts **SELECT** node to be displayed **SELECT** Node front panel layout **PRESS** Display Node Layout **PRESS** Off **SELECT** Power off options
cshutdown	Enter: `cshutdown`

Step 2: Disconnect the Node From the Frame

Your IBM Customer Engineer performs this step.

Step 3: Stop the Resource Manager Server

Stop the resource manager server in the system partition that the node belongs to by following one of the procedures described in the following table:

If using:	Do this:.
SMIT	**TYPE** **smit RM_options** **SELECT** Stop the Resource Manager **PRESS** **Do** to complete the operation
jm_stop	Enter: `jm_stop`

Step 4: Delete Node Information From the SDR

Use SMIT or the **spdelnode** command to delete node information from the SDR.

If using:	Do this:.
SMIT	**TYPE** **smit delete_data** • The Delete Data Information window appears **SELECT** Delete Node Information • The Delete Node Information window appears **TYPE** Start Frame, Start Slot, and Node Count **or** The Node List **PRESS** **Do**
spdelnode	To delete the SDR information for the 16 nodes in frame 3, enter: `spdelnode 3 1 16`

Step 5: Replace the Old Node with the New One and Power It On

Your IBM Customer Engineer performs this step.

Step 6: Delete NIM Client

Delete the NIM client on the boot/install server for the node you are replacing by issuing the **delnimclient** command. For example, to delete the NIM client for node number 3, issue:

```
delnimclient -l 3
```

Step 7: Update the State of the Supervisor Microcode

Refer to “Step 26: Update the State of the Supervisor Microcode” on page 44 for more information.

If you are replacing a node with an 604 high node, you need to ensure that the microcode level on the 604 high node is correct. For more information, refer to “Step 26: Update the State of the Supervisor Microcode” on page 44.

Step 8: Set Up, Power, and Configure the Nodes

To complete this task, follow the installation steps starting at “Step 27: Enter Required Node Information” on page 45 and proceed through the rest of the chapter.

Note: When you add a node, you must complete “Step 40: Configure Control Workstation as Boot/Install Server” on page 62.

Step 9: Refresh System Partition-Sensitive Subsystems

To refresh the subsystems, issue the following command on the control workstation:

```
syspar_ctrl -r -G
```

This command refreshes all the subsystems in each partition such as **hats** and **hb** so they recognize any node changes.

Step 10: Restart the Resource Manager Server

If using:	Do this:.
SMIT	**TYPE** **smit RM_options** **SELECT** Start the Resource Manager **PRESS** **Do** to complete the operation
jm_start	Enter: `jm_start`

Step 11: Restart System Monitor GUI or Perspectives

Exit the System Monitor GUI. To restart the SP System Monitor GUI, enter:

```
spmon -g
```

To restart Perspectives, enter:

```
perspectives &
```

Adding a Switch

The RS/6000 SP system supports four types of switches. They are listed in the following table:

Switch Type	Description	Feature Code
High Performance Switch	This switch connects all the processor nodes, providing scalable high-performance communication between processor nodes for parallel job execution. This switch contains the High Performance Switch Adapter-2 (feature code 4018). Some older models may contain the High Performance Switch Adapter-1 (feature code 4017).	4010
Scalable POWERparallel Switch (SP Switch)	This switch represents a new level of switch function. Like the High Performance Switch, it connects all the processor nodes, providing enhanced scalable high-performance communication between processor nodes for parallel job execution.	4011
High Performance Switch-LC8	This switch provides high-performance switch functions for small systems (up to 8 total nodes).	4007
Scalable POWERparallel Switch-8 (SP Switch-8)	This switch provides enhanced high-performance switch functions for small systems (up to 8 total nodes).	4008

If you are adding any of these switches, an IBM Customer Engineer installs the switch hardware on your RS/6000 SP System. You must plan your switch configuration and record your information on the Switch Configuration Worksheet, located in the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment*. Both the *RS/6000 SP: Planning, Volume 1, Hardware and Physical Environment.* and the *Planning, Volume 2, Control Workstation and Software Environment* offer information to help you with the worksheet. After you complete the worksheet, follow these steps to install and configure the switch according to your configuration worksheet.

Note the following:

- Performing this task requires that your identity be authenticated as an authorized user of the system management commands, SP System Monitor GUI, and Perspectives. You do this by issuing the **kinit** command to obtain a ticket from the RS/6000 SP authentication services, specifying the administrative principle name that was used when authentication was set up.

  See the section on using RS/6000 SP authentication services in the *Administration Guide* for more information.

- The extension node only communicates with the SP Switch and the SP Switch-8. If you have multiple partitions, and you want the nodes in each partition to use the extension node, you must add an extension node in each partition.

Adding a Switch to a Switchless System

Step 1: Redefine the System to a Single Partition

Refer to the *RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment* for more information.

Step 2: Install the Communication Subsystem Software

Install the Communication Subsystem software that supports the switch you are installing. Ensure that the correct level of **ssp.css** is on the control workstation.

Use SMIT or **installp** to install **ssp.css** on the control workstation. For more information, see “Step 18: Install PSSP on the Control Workstation” on page 27.

Ensure that the proper level of software for the switch has been installed.

Step 3: Install the New Switch

Your Customer Engineer will perform this step for you. This step may include installing the switch adapters and installing a new frame supervisor card.

Step 4: Create the Switch Partition Class

Issue the following command:

```
Eprimary -init
```

Step 5: Configure the Switch Adapters for Each Node

Use SMIT or the **spadaptrs** command to create **css0** adapter objects in the SDR for each new node. Refer to your Switch Configuration Worksheet. Use this data to configure the switch on the nodes.

See “Step 30: Configure Additional Adapters for Nodes” on page 50 for more information.

Step 6: Update the State of the Supervisor Microcode

Refer to “Step 26: Update the State of the Supervisor Microcode” on page 44 for more information.

Step 7: Reconfigure the Hardware Monitor to Recognize the New Switch

To do this, issue the following command:

```
hmcmds -G setid 1:0
```

Step 8: Update the System Data Repository

To update the SDR switch information, issue the following command:

```
hmreinit
```

Step 9: Set Up the Switch

Do installation steps “Step 43: Set Up the Switch” on page 64 through “Step 46: Set Up System Partitions” on page 69. If you have set up system partitions, you need to reconfigure them.

Step 10: Refresh System Partition-Sensitive Subsystems

To refresh the subsystems, issue the following command on the control workstation after adding the switch:

```
syspar_ctrl -r -G
```

This command refreshes all the subsystems in each partition such as **hats** and **hb** so they will recognize the new switch.

Step 11: Set Up Nodes to Customize

Previously, you installed the Communication Subsystem Software (CSS) on the control workstation. Now, you need to install this software on all the nodes in the system. Use SMIT or issue the **spbootins** command to do this by changing the boot/install information for all the Node Objects in the SDR to specify a bootp response of *customize*.

Set the node(s) to *customize* with the following command:

```
spbootins -r customize -l <node_list>
```

Step 12: Reboot All Nodes

1. Reboot all the nodes for node customization..
2. When the nodes have booted and initialized, validate that **hostresponds** is active for the nodes.

Step 13: Start Up and Verify the Switch

1. To complete this step, follow the installation steps starting at “Step 52: Start the Optional Switch” on page 79 and proceed through the rest of the chapter.
2. Exit the SP System Monitor GUI. To restart the SP System Monitor GUI, enter the following command:

   ```
   spmon -g
   ```

   To restart Perspectives, enter the following command:

   ```
   perspectives &
   ```

Adding a Switch to a System With Existing Switches

Step 1: Redefine the System to a Single Partition

Refer to the *IBM RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment* for information on setting up partitions.

Step 2: Install the New Switch

Your Customer Engineer will perform this step for you. This step includes installing the switch adapters and installing new frame supervisors.

Step 3: Update the State of the Supervisor Microcode

Refer to “Step 26: Update the State of the Supervisor Microcode” on page 44 for more information.

Step 4: Configure the Adapters for Each Node

Use SMIT or the **spadaptrs** command to create **css0** adapter objects in the SDR for each new node. Refer to your Switch Configuration Worksheet. Use this data to configure the switch on the nodes.

See “Step 30: Configure Additional Adapters for Nodes” on page 50 for more information.

Step 5: Set Up the Switch

Do installation steps “Step 43: Set Up the Switch” on page 64 through “Step 46: Set Up System Partitions” on page 69. If you have set up system partitions, you need to reconfigure them.

Step 6: Refresh System Partition-Sensitive Subsystems

To refresh the subsystems, issue the following command on the control workstation:

```
syspar_ctrl -r -G
```

This command refreshes all the subsystems in each partition such as **hats** and **hb** will recognize the new switch.

Step 7: Set Up Nodes to Customize

In step 1, you installed the Communication Subsystem Software (CSS) on the control workstation. Now, you need to install this software on all the nodes in the system. Use SMIT or issue the **spbootins** command to do this by changing the boot/install information for all the Node Objects in the SDR to specify a bootp response of *customize*.

Set the node(s) to *customize* by issuing the following command:

```
spbootins -r customize -l  <node_list>
```

Step 8: Reboot All Nodes

1. Reboot all the nodes.
2. Verify the production partition. When the nodes have booted and initialized, the production partition is ready for use.
3. Issue the **Estart** command in each partition.

Step 9: Start Up and Verify the Switch

1. To complete this step, follow the installation steps starting at “Step 52: Start the Optional Switch” on page 79 and proceed through the rest of the chapter.
2. Exit the SP System Monitor GUI. To restart the GUI, enter the following command:

   ```
   spmon -g
   ```

   To restart Perspectives, enter the following command:

   ```
   perspectives &
   ```

Reconfiguring Your System for Use with the SP Switch

This section discusses how to reconfigure your system to remove an existing High Performance Switch, High Performance Switch-LC8, or a SP Switch-8, and replace it with an SP Switch. It does not discuss how to install an SP Switch initially into your system. For this information, refer to Chapter 2, “Installing and Configuring a New RS/6000 SP System” on page 13 or “Adding a Switch” on page 196.

Prerequisites to Transferring Switches

Prior to removing the High Performance Switch and replacing it with the SP Switch, you need to do the following:

- Ensure your entire SP system has been migrated to AIX 4.2.1 and PSSP 2.3. For instructions, refer to Chapter 4, “Migrating to the Latest Level of PSSP” on page 107.
- Ensure that you have the PDU or SEPBU twin tailed frame supervisor card with the appropriate supervisor card level installed.

Step 1: Prepare for the Switch Transfer

IBM suggests that your system be configured as a single partition. If your system is a single partition, skip this step and proceed to the next step. If your system has multiple partitions, continue with this step.

Step 1.1: Archive the System Data Repository

Always archive the System Data Repository before partitioning (or repartitioning) your system. If you change your mind once you have committed a system partition configuration, or if applying a system partition configuration fails, you should use the archived SDR to recreate the previous system partition configuration. (To do this, select the Restore System Partition Configuration option from the SMIT menu.)

If using:	Do this:.
SMIT	At the System Partition Configuration menu: **SELECT** Archive System Data Repository
SDRArchive	Enter **SDRArchive**
Note: When you archive the SDR from either SMIT or by using the **SDRArchive** command, the archive produced is in tar format. Issuing **tar -x** for this archive does not restore the system partition configuration. To restore the system partition configuration, always use the SMIT Restore System Partition Configuration option.	

Step 1.2: Return to a Single Partition Environment

Either restore a previous single partition or set up a single partition.

To Restore a Single Partition:	To Set Up a Single Partition:.
Using SMIT **TYPE** smit syspar **SELECT** Restore System Partition Configuration **ENTER** The name of a previously archived system partition configuration or press **List** for a list of choices. **PRESS** Enter to apply the new configuration. **Using the command line** The full pathname of the **sprestore_config** command is: `/usr/lpp/ssp/bin/sprestore_config <archived file>`	**Using SMIT** **TYPE** smit syspar **SELECT** Select System Partition Configuration • A list of system partition configurations appears. **SELECT** a single system partition **Using the command line** Issue the **spapply_config** command.

Note: IBM suggests that your system be in one partition when transferring switches. If this is the case, the IBM Customer Engineer can use the control workstation to diagnose the switch and determine that it is functioning correctly. If there are multiple partitions, however, the Customer Engineer cannot diagnose the switch completely using the control workstation. In this event, ask your Customer Engineer to request that the laptop tool be shipped with the SP Switch Miscellaneous Equipment Specifications (MES).

Step 2: Shut Down All Nodes and Clean Up the Control Workstation

1. Check for any unique switch topology files on nodes and save them.
   a. Issue the following command:

      ```
      dsh -a ls -al /etc/SP/expected.top
      ```

   b. Move any files you find to a new location. For example, (/**tmp**/**expected.top**).
2. Shut down the nodes using either the System Monitor GUI, Perspectives, or the **cshutdown** command.

If using:	Do this:.
Perspectives	**SELECT** Hardware Perspective from the Launch Pad **SELECT** Correct current partition **SELECT** Actions → cws/system/syspars → Set Current Partition **SELECT** Nodes Pane **SELECT** all the nodes **SELECT** Actions → Nodes → Power on **PRESS** Power Off icon **PRESS** cshutdown **PRESS** Apply
System Monitor GUI	**SELECT** SP → Display Layouts **SELECT** node to be displayed **SELECT** Node front panel layout **PRESS** Display Node Layout **PRESS** Off **SELECT** Power off options
cshutdown	Enter: `cshutdown`

Step 3: Replace the High Performance Switch and Switch Adapters

This step involves replacing the switch, switch adapters, frame supervisors, and for some node types, the OCS modules. For more information regarding the instances when OCS module replacement is necessary, refer to the SP Switch Miscellaneous Equipment Specifications (MES) that you received when you ordered the SP Switch.

Your IBM System Engineer will perform this step for you using the instructions found in the Miscellaneous Equipment Specifications (MES) that you received when you ordered the SP Switch.

If your system has multiple partitions, you must run the **Eannotate** command against all switch topology files that are in use for any system partition.

Step 4: Reconfigure the Hardware Monitor to Recognize New Hardware

Once step 3 is complete, you need to reconfigure the hardware monitor to recognize the new hardware.

1. Issue the following command to update the frame supervisors with the frame id:

   ```
   hmcmds -G setid <frame_number> :0
   ```

   For example:

   ```
   hmcmds -G setid 1:0
   ```

Step 5: Update the State of the Supervisor Microcode

Refer to “Step 26: Update the State of the Supervisor Microcode” on page 44 for more information.

Step 6: Update the System Data Repository

To update the SDR switch information, issue the following command:

```
/usr/lpp/ssp/install/bin/hmreinit
```

Step 7: Annotate a Switch Topology File

Annotate a switch topology file before storing it in the SDR.

If using:	Do this:.
SMIT	**TYPE** **smit switch_ops** • The Perform Switch Operations menu appears. **SELECT** Topology File Annotator • The Topology File Annotator menu appears. **TYPE** The data in the fields, as follows: • The fully-qualified name of the topology file (for example, **/etc/SP/expected.top.2nsb.0isb.0**) • The fully-qualified name of the file in which you want to store the annotated topology file (for example, **/etc/SP/expected.top.annotated**) • **yes** to store the topology file in the SDR **PRESS** **Do**
Eannotator	Use **Eannotator** to update the switch topology file's connection labels with their correct physical locations. Use the **-O yes** flag to store the switch topology file in the SDR. Using **Eannotator** makes the switch hardware easier to debug because the switch diagnostics information is based on physical locations. For example, to annotate a two-switch or maximum 32-node system, enter: `Eannotator -F expected.top.2nsb.0isb.0 -f expected.top.annotated -O yes`

Storing the Switch Topology File in the SDR

If you entered **Eannotator -O yes** or **yes** previously when issuing the **Eannotator** command, skip this step.

If using:	Do this:.
Perspectives	**SELECT** the Cluster_Mgmt icon • The SP Cluster Management menu appears. **SELECT** Perform Switch Operations From this point, you can pick up with the SMIT steps listed in the next row of this table.
SMIT	**TYPE** **smit cluster_mgmt** • The RS/6000 Cluster Management menu appears. **SELECT** Perform Switch Operations • The Perform Switch Operations menu appears. **SELECT** Fetch/Store Topology Files • The Fetch/Store Topology Files menu appears. **SELECT** Store a Topology File • The Store a Topology File menu appears. **TYPE** The fully-qualified path name of the topology file. **PRESS** **Do**
Etopology	Use **Etopology** to store the switch topology file in the SDR and make sure that it has been annotated. For example, to store a two-switch or maximum 32-node configuration, enter: **`Etopology expected.top.2nsb.0isb.0.annotated`**

Step 8: Set the Switch Primary and Primary Backup Nodes

Frame 1, node 1 is the default primary node.

If you have an SP Switch, the primary backup node takes over for the primary node when it detects that the primary node is no longer functional. By default, a node is selected from a frame that is different from the primary node. If no other frame exists (for example, a single frame system), a node is selected from a switch chip that is different from the primary node. If no other switch chip is available, any available node on the switch is selected. Use SMIT or the **Eprimary** command to verify this node or change the primary to another node.

If using:	Do this:.
SMIT	**TYPE** **smit cluster_mgmt** • The RS/6000 Cluster Management Menu appears. **SELECT** Perform Switch Operations • The Perform Switch Operations Menu appears. **SELECT** Set Primary and Primary Backup Nodes • The Set Primary and Primary Backup Node Menu appears. **ENTER** A primary and primary backup node **PRESS** **Do**
Eprimary	Enter: **Eprimary** <primary node> -backup <primary backupnode> For example: Eprimary 1 -backup 16

This command, without any parameters, returns the node number of the current primary node, the primary backup node, the oncoming primary node, and the oncoming primary backup node.

Note: The current primary backup, the oncoming primary node, and the oncoming primary backup nodes are valid only for the SP Switch.

Step 9: Set Switch Clock Source for All Switches

Use SMIT or the **Eclock** command to initialize the switch's Clock Source. The SMIT and **Eclock** interfaces require that you know the number of Node Switch Boards (NSBs) and Intermediate Switch Boards (ISBs) in your RS/6000 SP system.

Select the Eclock topology file from the control workstation's /**etc**/**SP** subdirectory, based on these numbers. For example, if your RS/6000 SP system has six node switch boards and four intermediate switch boards, you would select /**etc**/**SP**/**Eclock.top.6nsb.4isb.0** as an Eclock topology file.

See the *IBM RS/6000 SP: Planning, Volume 2, Control Workstation and Software Environment* for the Eclock topology file names.

If using:	Do this:.
Perspectives	**SELECT** the Cluster_Mgmt icon • The SP Cluster Management menu appears. **SELECT** Perform Switch Operations From this point, you can pick up with the SMIT steps listed in the next row of this table.
SMIT	**TYPE** **smit cluster_mgmt** • The RS/6000 Cluster Management Menu appears. **SELECT** Perform Switch Operations • The Perform Switch Operations Menu appears. **SELECT** Change/Show Switch Clock Source Settings • The Change/Show Switch Clock Source Settings Menu appears. **SELECT** Initialize Switch Clock Source Settings • The Initialize Switch Clock Source Settings Menu appears. **SELECT** Automatic Selection of Switch Clock Setting **PRESS** **Do**
Eclock	Use the **Eclock** command to set the switch clock source for all switches. For example, if your RS/6000 SP system has six node switch boards and four intermediate switch boards, select **/etc/SP/Eclock.top.6nsb.4isb.0** as an Eclock topology file. Enter: `Eclock -f /etc/SP/Eclock.top.6nsb.4isb.0` This command sets the proper clock source settings on all switches within a 96-way (6 nsb, 4 isb) RS/6000 SP system.
Note: Be careful when using **Eclock** after the switch is initialized. **Eclock** modifies the switch clocking and is disruptive to the entire system (all system partitions).	

Step 10: Set Up Nodes to Customize

Since there was a switch topology change, you need to install this software on all the nodes in the system. Use SMIT or issue the **spbootins** command to do this by changing the boot/install information for all the Node Objects in the SDR to specify a bootp response of *customize*.

Set the node(s) to *customize* with the following command:

```
spbootins -r customize -l <node_list>
```

Step 11: Power On the Nodes

If using:	Do this:.
Perspectives	From hardware perspective menu bar: **SELECT** Node to be powered on **SELECT** Actions → Nodes → Power On... **SELECT** Power on options **PRESS** Apply or From hardware perspective tool bar: **SELECT** Node to be powered on **PRESS** Power on icon from Tool bar **SELECT** Power on options **PRESS** Apply
System Monitor GUI	**SELECT** SP → Display Layouts **SELECT** Node to be displayed **PRESS** Display Node Layout **PRESS** On **SELECT** Power on options

Step 12: Verify SP Switch Adapters

To verify that the SP Switch adapters are functioning correctly, issue the following command:

```
SDRGetObjects switch_responds
```

If *adapter_config_status* shows other than **css_ready**, such as **diag_fail**, contact your IBM service representative.

Step 13: Start the Switch

This step initializes the optional switch. You can perform this step from SMIT panels, using Perspectives, or from the command line.

If using:	Do this:.
SMIT	**TYPE** **smit switch_ops** • The Perform Switch Operations Menu appears. **SELECT** Start Switch
Perspectives	**SELECT** the Hardware icon by double clicking on it. **SELECT** the Nodes Pane • The Nodes Pane receives focus. **SELECT** View → Monitor • The Set Monitoring for Nodes dialog box appears. **SELECT** the switch_responds condition **PRESS** Apply • The nodes should now be colored green. Check the node icons. All node icons should be solid green. If they are not, refer to the *Diagnosis and Messages Guide* for further informatio
Estart	Enter: `Estart`

Check switchResponds and powerLED indicators for each node. From the SP System Monitor GUI main window:

SELECT SP

SELECT Global Controls

SELECT SP

SELECT All Node Summary Display

• The selection screen for node variables appears.

SELECT switchResponds from the list of variables

PRESS Display all-node summary.

• The switchResponds Summary appears.

Check the indicators for switchResponds. All indicators should be solid green. If not, see the section on diagnosing RS/6000 SP problems in the *Diagnosis and Messages Guide.*

Step 14: Run Verification Test on the Switch

Run a verification test to ensure the installation of the switch is complete. You do this using either SMIT or the command line. You can also use Perspectives to access the SMIT **smit SP_verify** option.

If using:	Do this:.
SMIT	**TYPE** **smit SP_verify** • The Installation/Configuration Menu appears **SELECT** The SSP Communication Subsystem option **PRESS** Enter
CSS_test	Enter: `CSS_test`

If the verification test fails, see the section on diagnosing RS/6000 SP problems in the *Diagnosis and Messages Guide*.

Step 15: Reapply System Partition Configuration

This is an optional step to perform only if you have multiple partitions. To reapply your original system partition configuration, follow Steps 2 through 6 of "Partitioning the SP System" from Chapter 6 of the *Administration Guide*.

Replacing the Frame Supervisor

To replace the frame supervisor with an updated frame supervisor, follow these steps:

Step 1: Install the New Frame Supervisor Card

Your Customer Engineer will perform this step for you.

Step 2: Reconfigure the Hardware Monitor to Recognize New Hardware

Issue the following command to update the frame supervisors with the frame id:

```
hmcmds setid <frame_number>:0
```

For example:

```
hmcmds setid 1:0
```

Step 3: Update the State of the Supervisor Microcode

Refer to “Step 26: Update the State of the Supervisor Microcode” on page 44 for more information.

Step 4: Issue Eannotate

Run **Eannotate** on the topology file for each partition.

Step 5: Issue Eclock

Run **Eclock** to set switch clock sources and use the System Monitor GUI to verify the status in the supervisor cards.

Step 6: Issue Estart

Run **Estart** to restart the switch.

Replacing a Fixed Disk

This procedure applies only to disks that are part of the **rootvg** volume group.

- Performing this task requires that your identity be authenticated as an authorized user of the system management commands, SP System Monitor GUI, and Perspectives. You do this by issuing the **kinit** command to obtain a ticket from the RS/6000 SP authentication services, specifying the administrative principle name that was used when authentication was set up.
- If possible, back up any required data on the disk before replacing it.
- Do these steps in the system partition in which you replace the disk.

Step 1: Power Off the Node

You can use the System Monitor GUI or Perspectives to power off the node.

If using:	Do this:.
Perspectives	**SELECT** the node to power off **PRESS** Power Off icon **SELECT** the power off options **PRESS** Apply
System Monitor GUI	**SELECT** SP → Display Layouts **SELECT** node to be displayed **SELECT** Node front panel layout **PRESS** Display Node Layout **PRESS** Off **SELECT** Power off options

Step 2: Replace the Disk

Your IBM Customer Engineer performs this step. Make sure that the new disk has equivalent or greater disk space available.

Step 3: Install the System Image on the Disk

Use the **spbootins** command to:

1. Select image to be installed, if necessary.
2. Set **bootp_response** to `install`.

Step 4: Network Boot the Node

Use the SP System Monitor GUI or Perspectives to network boot the node.

If using:	Do this:.
Perspectives	**SELECT** the Nodes Pane **Select** Nodes to network boot **PRESS** Actions → Nodes → Netboot **PRESS** Apply
Note: See the chapter on using the system monitor and Perspectives in the *Administration Guide* for more information.	
System Monitor GUI	**SELECT** SP → Global Commands • The Global Commands panel appears. **SELECT** The new node **SELECT** Net boot **PRESS** **Do** • The SP System Monitor boots the new node. • The network boot status window appears.

Replacing a Disk Not in rootvg

To replace disks that are *not* in the **rootvg** volume group:

Step 1: Power Off the Node

You can use the System Monitor GUI or Perspectives to power off the node.

If using:	Do this:.
Perspectives	**SELECT** the node to power off **PRESS** Power Off icon **SELECT** the power off options **PRESS** Apply
System Monitor GUI	**SELECT** SP → Display Layouts **SELECT** node to be displayed **SELECT** Node front panel layout **PRESS** Display Node Layout **PRESS** Off **SELECT** Power off options

Step 2: Replace the Failing Fixed Disk

Your IBM Customer Engineer performs this step for you. Make sure that the new disk has equivalent or greater disk space available.

Step 3: Power On the Node

If using:	Do this:
Perspectives	From hardware perspective menu bar **SELECT** node to be powered on **SELECT** Actions → Nodes → Power On... **SELECT** power on options **PRESS** Apply or From hardware perspective tool bar **SELECT** node to be powered on **PRESS** Power on icon from Tool bar **SELECT** power on options **PRESS** Apply
System Monitor GUI	**SELECT** SP → Display Layouts **SELECT** node to be displayed **PRESS** Display Node Layout **PRESS** On **SELECT** Power on options

Step 4: Restore Any Data Previously Backed-Up

You will need to recreate the volume group and restore any files back into the user based file system.

Replacing an I/O Planar Card in a Thin Node or an Ethernet Adapter

The I/O planar card for a thin node or the en0 adapter for a wide or 604 high node has a hardware address used to network boot the nodes. This procedure updates the SDR hardware Ethernet address.

- A ticket is required to perform some of the commands in this procedure. Run the **kinit** command.
- Do these steps in the system partition in which you replace the card.

Step 1: Power Off the Node

You can use the System Monitor GUI or Perspectives to power off the node.

If using:	Do this:.
Perspectives	**SELECT** the node to power off **PRESS** Power Off icon **SELECT** the power off options **PRESS** Apply
System Monitor GUI	**SELECT** SP → Display Layouts **SELECT** node to be displayed **SELECT** Node front panel layout **PRESS** Display Node Layout **PRESS** Off **SELECT** Power off options

Step 2: Replace the Card

Your IBM Customer Engineer performs this step.

Step 3: Delete NIM Client

Delete the NIM client on the boot/install server for the node you are replacing by issuing the **delnimclient** command from the control workstation. For example, to delete node 3 from the boot/install server, issue:

```
delnimclient -l 3
```

Step 4: Obtain the New Hardware Ethernet Address

If you have ethernet information for the node being replaced in **/etc/bootptab.info**, be sure to remove the old address.

Use the **sphrdwrad** command to get the new hardware Ethernet address.

Step 5: Recreate NIM Client Definition

To recreate the NIM client definition, issue the mknimclient command. For example, to recreate the NIM client for node number 3, issue:

```
mknimclient –l 3
```

Chapter 6. Performing Software Maintenance

This chapter provides information on updating installation images, LPPs, and support programs.

Installing Program Updates

Note: Performing this task requires that your identity be authenticated as an authorized user of the system management commands, the System Monitor GUI interface, and the Perspectives interface shown in the following steps. You do this by issuing the **kinit** command to obtain a ticket from the RS/6000 SP authentication services, specifying the administrative principle name that was used when authentication was set up.

See the section on using RS/6000 SP authentication services in the *Administration Guide* for more information.

There are two approaches to installing program updates.

Approach	Description
Per-node	Apply the maintenance on each node individually. For the per-node approach, you can apply service on all the nodes in one of the following ways: • Logging in to each node and using SMIT for installation • Running the installation command on each node using **dsh**
Reinstall	Install the maintenance on a single node, building an image on that node, and then propagate the changes to all other nodes by reinstalling that image on each node. The reinstall approach requires you install the programs and updates on your maintenance test node using SMIT or **installp** in order to generate an installation image and then place the new image on the control workstation. SMIT or the **spbootins** command enables you to specify all the nodes to be reinstalled with the new image. All that remains is to boot the nodes, which causes the nodes to be reinstalled.

Regardless of which approach you choose, do the following:

1. Apply the desired maintenance to a single test node. This allows you to gauge how long the service takes for a single node and enables you to verify the success of the maintenance before applying the service to the rest of the nodes.
2. Generate a **mksysb** image of your updated system. In the event of a required reinstall, you can use the **mksysb** image instead of reapplying the maintenance to any nodes that need to be reinstalled.

© Copyright IBM Corp. 1995, 1997

Which Approach is Right for You?

How do you know which approach to take? Consider these factors:

- How many nodes you have in your system.
- How long it takes to apply the desired maintenance.
- Whether you have user data on a node in its root volume group. (This data is destroyed on a reinstall.)

If you have fewer than 16 nodes in your system or the maintenance is minor, it may be faster to apply the maintenance directly on each node rather than to reinstall. On the other hand, if you have a large amount of maintenance to do and you have no user data to preserve in the root volume group, it may be faster to install the maintenance once, generate a new installation image, and reinstall all your nodes.

Working With Nodes That Are Down

Regardless of your approach, nodes that were down when service was applied must get updated. This situation is handled differently in the two approaches.

Using the Per-Node Approach

When using the per-node approach, you need to note the nodes that are down and service them when they come back up. You can use the **lslpp** command to help determine what maintenance has been applied on a particular node, and use **dsh** to run the **lslpp** command on a group of nodes.

Using the Reinstall Approach

If you are using the reinstall approach and a node is unavailable when you are reinstalling images, whenever the node comes back up it reinstalls the correct image. To ensure that a node is reinstalled when it comes back up, use the flags of the **spbootins** command to set the **bootp_response** attribute for the node to **install** and the **install_image** attribute to indicate that the new installation image is to be used.

In addition to the **bootp_response** and the **install_image** attributes values, the name of the installation image last used and the date and time of the last install are kept in the Node Object in the SDR for each node and can be examined using the **-b** flag of the **splstdata** command.

Reinstalling PSSP

If you need to apply service to PSSP or reinstall PSSP, you must install the maintenance on the control workstation first. Then proceed to install the maintenance on the nodes depending on which approach you have chosen, as described in “Installing Program Updates” on page 215.

Make sure you read the *Memo to Users* that comes with any updates to PSSP. The *Memo to Users* indicates if there are any updates that would require you to service all nodes in your RS/6000 SP System before continuing to run your system.

Note: If you are restoring from a **mksysb** image, issue the **install_cw** command to initialize the ODM.

Updating the css Option

When reinstalling or updating the **ssp.css** option of PSSP, you must reboot all affected nodes to load changes that affect the kernel extensions.

Adding mksysb Images to the Control Workstation

Changes in system configurations may require you to create additional mksysbs or replace existing ones. To create additional mksysbs, use one of the following commands:

- mkszfile — used with AIX 3.2.5 systems
- mksysb — used with AIX 4.x systems
- smit mksysb — supported SMIT interface

Store the resulting mksysb on the control workstation using a different name from the mksysbs that already exists on the control workstation. If you do not use a different name, you will overwrite the existing mksysb and your changes will not get propogated to boot/install servers or nodes.

To replace an existing mksysb, create a new one and store in on the control workstation using the same name as the existing mksysb.

Restoring the Control Workstation from a mksysb Image

When you need to restore the control workstation from a mksysb image, for example in the case of a disk in the rootvg volume group being replaced, follow the procedure documented in chapter 5 "Installing BOS for a System Backup" of the AIX Version 4.2 Installation Guide. Make sure that the mksysb image you are using is the most recent copy from the control workstation. Otherwise, you may have a version that does not match with the version on the nodes. In addition, once the restoration is complete, issue the **install_cw** command to reinitialize the Object Data Manager (ODM).

Restoring the Node from a mksysb Image

To restore the node from a mksysb image, refer to “Test Your Image on a Single Node” on page 220. Make sure that the mksysb you want to restore on the node is correct one for that node.

Updating the Print Subsystem

If you are applying service to any base AIX print commands and you are using the RS/6000 SP Print Management Utility, you must do the following when applying the service:

1. Use SMIT or the **spsitenv** command to set the **print_config** attribute to **none**. This causes the links to be removed and the original AIX commands to be renamed to the original names.
2. Perform any updates.
3. Use SMIT or the **spsitenv** command to set the **print_config** attribute to **open** or **secure** to reconfigure the Print Management Service.

Installing Updates on a Per Node Basis

Note: A ticket is required to perform some of the commands in this procedure. Run the **kinit** command.

After you have made the service you want to apply available as an image on the control workstation, you can apply service to each node individually by selecting one of the following methods:

- Login to each node and use SMIT for installation.
- Run the installation command on each node using **dsh** from the control workstation. This requires that you know exact syntax of the **installp** command you want to issue. See the *SP Commands and Technical Reference* for **dsh** command syntax. For example, to use **installp** to install the Resource Manager program on every node, issue:

```
dsh -a /usr/sbin/umount /mnt
dsh -a /usr/sbin/mount <cw>:/spdata/sys1/install/pssplpp /mnt
dsh -a /usr/sbin/installp -d /mnt/ssp/pssp.installp  -X ssp.jm
```

Installing Updates through Reinstallation

Performing this task requires that your identity be authenticated as an authorized user of the system management commands, the System Monitor GUI interface, and the Perspectives interface shown in the following steps. You do this by issuing the **kinit** command to obtain a ticket from the RS/6000 SP authentication services, specifying the administrative principle name that was used when authentication was set up.

See the section on using RS/6000 SP authentication services in the *Administration Guide* for more information.

If you choose the reinstall approach, you may want to target particular nodes for maintenance images. For instance, if you have groups of nodes with distinct identities such as:

- Boot/install servers
- Compute nodes
- Interactive nodes

You may want to select one representative node in each group from which to apply maintenance and generate new installation images. The other nodes in the group should always then be reinstalled with the image generated from that node.

Note: For System Partitions:

1. All nodes using the switch must be at the same level of base AIX.
2. The communications subsystem software (**ssp.css**) must be at the same level on each node using the switch.

Build an Installation Image

Note: If you want your machine to be a NIM master, make sure that the image you are building from had not executed the **inurid -r** command. Check to see if this command was run by issuing the following:

```
/usr/lib/instl/inurid -q ; echo $?
```

If the return code=1, the **inurid -r** command was executed. IBM suggests that you not execute the **inurid -r** command on any machine in case you want to use the machine as a boot/install server in the future.

Before building an installation image, install all the LPPs and service to the node on which you intend to create your installation image. Careful planning in selecting LPPs and required service spares you from repeating this process.

After you have installed the LPPs and service required for your nodes, you are ready to make an installation image. Login to the node where you want to create an installation image and enter:

```
smit -C mksysb
```

Enter the file name of the image that you want to create and press Enter.

Note: The installation tools require that the name of this image begin with **bos.obj**. A suggested naming convention for these images is:

bos.obj.<level>.<date>

For example:

```
bos.obj.41.950515
```

You can generate a **mksysb** image to install on your nodes. You can do this on a node after you have installed at least that node, or you can use a standalone workstation (either the control workstation or a different standalone workstation). However, after you have done “Step 19: Initialize RS/6000 SP Authentication Services” on page 31, you cannot use the control workstation for this purpose. Runn **setup_authent** command on any workstation makes the workstation unsuitable for generating a **mksysb** image for a node.

The control workstation (or a different standalone workstation) must be at the right level of the AIX RS/6000 operating system and must have all required PTFs applied. One way to ensure this is to install the **mksysb** image that resides in the **spimg installp** image on its product tape. You can also install any of the RS/6000 SP software options on that machine. After installing extra LPPs or maintenance, you can generate a **mksysb** image of the system and copy it back to **/spdata/sys1/install/images** on the control workstation. You can then use that image to install your nodes.

After you install a node, you can install any RS/6000 SP software options or LPPs, other LPPs, or any maintenance that you need. You can then test your node and generate a **mksysb** image of that node. Before doing this, you may want to remove certain files from the node that you do not want in the image. These include any **mksysb** images in that node's **/spdata/sys1/install/images** directory (if the node is a boot/install server itself).

Do not remove **/home** from the node. If you do so, when you use the **mksysb** image to install a boot/install server node, you cannot create the **netinst** user ID

that is required for network install after you install the image. After you create the **mksysb** image, copy it back to **/spdata/sys1/install/images** on the control workstation and install the rest of your nodes with that image.

Consider the following items prior to creating a mksysb backup:

- Excluding Mounted Filesystems:

  Are there any mounted filesystems from other systems? The mksysb command automatically backs up everything unless you specify what to exclude. Some example of items you might want to exclude are AFS, DFS, or NFS filesystems. You can exclude files by specifying the "-e" flag and creating an **/etc/exclude.rootvg** file with a list of the files to exclude. The file might contain somthing like this:

  ```
  /afs
  /usr/public
  ```

  Where the /afs is an AFS filesystem and the /usr/public is a shared NFS filesystem that is mounted on this system.

  If you specify the "-e" flag with the **/etc/exclude.rootvg** file containing this information, mksysb image will not backup any files in these directories or create the directories.

- Generate a New /image.data file

  The /image.data file in the mksysb image contains information about the operating system level, the logical volumes, the filesystems, and other information. This information may be out of date. Therefore, you should always create the file during the mksysb creation using the "-i" option.

- Create MAP files

  Note: Do not use the "-m" flag on the mksysb command. This flag generates a layout mapping of the logical-to-physical partitions for each logical volume in the volume group. This mapping is used to allocate the same logical-to-physical partition mapping when the image is restored. Do not use this option because it requires that you have the exact same physical disk configurations when restoring the image. This option causes an installation failure if this requirement is not met. The installation process will stop with an LED code of C48 and the installation will automatically switch from a noprompt to a prompt mode.

To create the mksysb image, use the following command to create a /image.date file. It will also expand /tmp if needed:

```
mksysb  -i -X
```

The following command creates a ./image.date file, expands /tmp, and excludes all files listed in /etc/exclude.rootvg.

```
mksysb  -e  -i -X
```

Test Your Image on a Single Node

After you create your netinstall image, you must test the image. Use **ftp** in binary mode or **rcp** to transfer the image to the control workstation. The installation tools require all installation images to reside on the control workstation. Remember that the image must be placed in the **/spdata/sys1/install/images** directory and that the permissions must allow it to be read by **other**.

To test the image, you must reinstall a node with this new image and run your applications to see if it meets your requirements.

Propagate Your Installation Image

After you create the netinstall image and copy it to the control workstation in /**spdata/sys1/install/images**, you are ready to reinstall.

On the control workstation issue the following:

```
/usr/lpp/ssp/bin/spbootins -i install_image_name \
-r install start-slot node-count
```

In the following example:

```
spbootins -i bos.obj.41.940515 -r install 2 3 1
```

would change the SDR information to install the image **bos.obj.41.950515** on node 3 in rack 2 from its boot/install server.

This command automatically issues the **setup_server** on node 3's boot/install server to update its install files with the new information. Note that **setup_server** copies the installation image from the control workstation to the appropriate boot/install servers if the boot/install server is not the control workstation. If the image has to be copied to a boot/insall server, this may take some time. You can now use the System Monitor GUI or Perspectives to reset the node, which causes the netinstall of the test image on the node.

The boot list of a node is set by /**etc/rc.sp** to boot from **hdisk0** only. When the **bootp_response** of a node is changed from **disk** to be some other response, such as "install," the node is sent a boot list command to cause it to boot from **ent0** before **hdisk0**. If a node is down when its **bootp_response** is changed, its boot list is not changed. In order to cause the node to boot over the network, you must use the Network Boot button of the System Monitor display manager.

After the netinstall is complete, the node reboots and you can verify the image runs your applications. When you are satisfied that this image meets your requirements, you can use the **spbootins** command to change the **install_image** attribute and **bootp_response** and reinstall the rest of your nodes.

Applying PTFs to the System

This section outlines a procedure you can follow to install PTFs on your system using the procedure described in “Installing Updates on a Per Node Basis” on page 218.

Task A: Prepare the Control Workstation

1. Create a mksysb backup of the control workstation.
2. Create a mksysb backup of the test node.
3. Copy the PTFs into an appropriate directory on the control workstation, for example:

   ```
   /spdata/sys1/install/pssplpp/ptf2
   ```

4. Run the command **inutoc .** in that directory to build a new .toc file.

5. Verify /**spdata**/**sys1**/**install**/**pssplpp** is exported to all nodes.
6. Apply the PTFs to the control workstation.

   Note: Do *not* commit.
7. Verify the correct operation of all SP and AIX control workstation functions.

   Note: You may want to reboot the control workstation. Check the README in the PTF to see if this is required.

Task B: Apply PTFs on One SP Node and Verify Correct Operation

Some PTFs require you apply them to all the nodes in your system. To do this, set up a test AIX 4.2 partition. See the *Administration Guide* for instructions.

1. Select one node for PTF installation.
2. NFS mount /**spdata**/**sys1**/**install**/**pssplpp** from the control workstation onto that node:

   ```
   /usr/sbin/mount <cw>:/spdata/sys1/install/pssplpp /mnt
   ```
3. Apply PTFs to that node.
4. Reboot the node and verify correct operation.
5. Verify correct installation and operation of the node.
6. Create a mksysb image of this node and store it in an appropriate directory on the control workstation, for example:

   ```
   /spdata/sys1/install/images/bos.obj.ssp.41.ptf2
   ```

   Note: You may want to install one node using the mksysb image you just saved to make sure the image is correct.

Task C: Apply PTFs to All Nodes

You can follow these instructions to install the PTF code from the directory onto each node. You can also install the PTFs by using the mksysb you just saved.

1. Using the **dsh** command, NFS mount /**spdata**/**sys1**/**install**/**pssplpp** onto each node. You can exclude the node you used for testing since it is now at the correct level.

   ```
   dsh -a /usr/sbin/mount <cw>:/spdata/sys1/install/pssplpp /mnt
   ```
2. Use **dsh** to run the appropriate **installp** command to apply PTFs to all nodes.

   ```
   dsh -a /usr/sbin/installp -d /mnt/ssp/pssp.installp -X ssp.jm
   ```

   Note: The **dsh -f** option allows the dsh commands to be fanned out to multiple nodes.
3. Reboot the nodes and verify their correct operation.

Task D: Commit PTFs on Node and Control Workstation

See the README in the PTF to determine if you are required to commit the PTFs. If you are not required to commit, you can skip this task.

1. Using **dsh**, commit the PTFs onto all nodes.
2. Commit the PTFs on the control workstation.

Task E: Update the State of the Supervisor Microcode

Refer to “Step 26: Update the State of the Supervisor Microcode” on page 44 for more information.

Task F: Create New mksysb Images

Create a new **mksysb** backup of the control workstation. The **mksysb** image you created earlier is now the **mksysb** image for all nodes. Store any earlier **mksysb** images you created before you installed the PTFs in case you need to restore your system to its previous maintenance level.

Restoring a Control Workstation from mksysb Image

When a mksysb image is made from an existing control workstation, there are certain ODM attributes that are not saved such as *node_number*. These attributes can be restored by running the **install_cw** command. This should be done before running any of the other PSSP scripts which are dependent on these attributes being defined.

Appendix A. SP Perspectives and System Monitor GUI Tasks

This appendix discusses how to start and use Perspectives and the System Monitor Graphical User Interface (GUI). In addition, a table appears describing how to perform some of the most common administrative tasks.

Starting and Using Perspectives

Perspectives is a graphical user interface you can use to manage and monitor the SP system. Complete instructions for using Perspectives appear in the on-line help information.

You can use Perspectives during the installation and migration process to perform a variety of tasks including installing software and verifying executed steps.

To start Perspectives by bringing up the Launch Pad, first export your display and then type **perspectives &** to run the process in the background. The Launch Pad gives you graphical access to Perspectives applications. To launch an application, either double click on the icon associated with an application or select the icon using the Launch action found under the Actions menu.

In each of the Perspectives, to perform an action, all you need to do is to click on the icon of one or more objects and then click on an action in either the menu bar or the tool bar. If you need more information to complete the action, a dialog box will appear. In addition, each Perspective has online help available from the Help menu selection.

Note that many of the steps require you to use SMIT. You can use SMIT directly by issuing SMIT commands or you can access SMIT using Perspectives. Often used SMIT fast-paths such as **smit_verify** are available from the Perspectives Launch Pad.

Starting and Using the System Monitor Graphical User Interface

In addition to Perspectives, you can use the System Monitor graphical user interface to manage and monitor the SP system. Complete instructions for using this interace appear in the *System Administration Guide*.

To start the System Monitor GUI, first export your display and then type:

```
spmon -g
```

Note that the System Monitor GUI does not support extension nodes.

The following table discusses the most common tasks that you can perform using Perspectives or the System Monitor Graphical User Interface (GUI).

Table 9 (Page 1 of 4). Performing Common Tasks Using SP Perspectives and the System Monitor GUI

Task	Perspectives	System Monitor GUI
Bringing up the GUI	**TYPE perspectives &** to bring up the launch pad	**Enter** spmon -g

© Copyright IBM Corp. 1995, 1997

Table 9 (Page 2 of 4). Performing Common Tasks Using SP Perspectives and the System Monitor GUI

Task	Perspectives	System Monitor GUI
Launching applications	Double click on application icon in Launch Pad or **SELECT** application icon **SELECT** Actions → Launch	Not applicable
Closing the GUI	**SELECT** Window→ Close to close the launch pad	**SELECT** File→ Exit
Closing a window	**SELECT** Cancel button or select Close from the top left of window.	**SELECT** Window→ Exit or select Close from the top left of window.
Powering off one node	From hardware perspective menu bar **SELECT** node to be powered off **SELECT** Actions → Nodes → Power Off... **SELECT** power off options **PRESS** Apply or from hardware perspective tool bar **SELECT** node to be powered off **PRESS** Power off icon from Tool bar **SELECT** power off options **PRESS** Apply	From the SP System Monitor GUI **SELECT** SP → Display Layouts **SELECT** SP → Display Layouts **SELECT** Frame which displays the node. **SELECT** Node Front Panel Layout **PRESS** Display Node Layout **PRESS** Off **SELECT** Power off options
Powering off more than one node	From hardware perspective menu bar **SELECT** nodes to be powered off **SELECT** Actions → Nodes → Power Off... **SELECT** power off options **PRESS** Apply or from hardware perspective menu bar with Node Groups **SELECT** node group to be powered off **SELECT** Actions → Node GroupS → Power Off... **SELECT** power off options **PRESS** Apply or from hardware perspective tool bar **SELECT** nodes to be powered off **PRESS** Power off icon from Tool bar **SELECT** power off options **PRESS** Apply	From the SP System Monitor GUI **SELECT** SP → Global Controls **SELECT** nodes to be powered off **PRESS** Off **SELECT** Power off options
Powering on one node	From hardware perspective menu bar **SELECT** node to be powered on **SELECT** Actions → Nodes → Power On... **SELECT** power on options **PRESS** Apply or From hardware perspective tool bar **SELECT** node to be powered on **PRESS** Power on icon from Tool bar **SELECT** power on options **PRESS** Apply	From the SP System Monitor GUI **SELECT** SP → Display Layouts **SELECT** Frame which contains the nodes. **SELECT** node to be displayed **SELECT** Node Front Panel Layout **PRESS** Display Node Layout **PRESS** On **SELECT** Power on options

Table 9 (Page 3 of 4). Performing Common Tasks Using SP Perspectives and the System Monitor GUI

Task	Perspectives	System Monitor GUI
Powering on more than one node	From hardware perspective menu bar **SELECT** nodes to be powered on **SELECT** Actions → Nodes → Power On... **SELECT** power on options **PRESS** Apply or From hardware perspective menu bar with Node Groups **SELECT** node groups to be powered on **SELECT** Actions → Node GroupS → Power On... **SELECT** power on options **PRESS** Apply or From hardware perspective tool bar **SELECT** nodes to be powered on **PRESS** Power on icon from Tool bar **SELECT** power on options **PRESS** Apply	From the SP System Monitor GUI **SELECT** SP → Global Controls **SELECT** nodes to be powered on **PRESS** On **SELECT** power on options
Verifying node status for many nodes: hostResponds, powerLED, switchResponds, and 3 digit display	From hardware perspective menu bar **Click** on the Nodes pane **SELECT** View→ Monitor **SELECT** hostResponds **PRESS** Apply Repeat these steps for individual viewing of node powerLED and switchResponds status, or select all three. Check to see if any node icons do not turn green. If a red X is showing, then there is a problem with that node. Three digit display is always displayed in it's own window. Bring up the 3 digit display: **SELECT** the Nodes pane **SELECT** Actions→ Nodes→ 3 digit display	From the SP System Monitor GUI **SELECT** SP → All Node Summary Display **SELECT** variable to be displayed **PRESS** Display all-node summary Repeat these steps for individual viewing of each variable. Each variable is displayed in a separate window.
Verifying node status for one node: hostResponds, powerLED, and switchResponds.	From hardware perspective node notebook **SELECT** a node by double clicking on it. **SELECT** Node Status tab To verify the status of an extension node: **SELECT** the extension node by double clicking on it. Once the notebook appears, check that the switchresponds variable is running. The Node Status page does not display the value of the 3 digit display for the node.	From the SP System Monitor GUI **SELECT** SP → Display Layouts **SELECT** Frame Number **SELECT** Node number **SELECT** Node Front Panel Layout **PRESS** Display Node Layout The Node Front panel shows both powerLED and hostResponds. SwitchResponds is not shown on the Node Front panel.
Viewing node information	**SELECT** a node by double clicking on it. **SELECT** Tab corresponding to desired page	SDR via smit

Table 9 (Page 4 of 4). Performing Common Tasks Using SP Perspectives and the System Monitor GUI

Task	Perspectives	System Monitor GUI
Changing to the system (global) view	From hardware perspective menu bar **SELECT** System icon **SELECT** Actions→CWS/System/Syspars→Set Current Partition	From the SP System Monitor GUI **SELECT** SP→Global Controls
Changing to a partition (syspar) view	From hardware perspective menu bar **SELECT** Syspar icon **SELECT** Actions→CWS/System/Syspars→ Set Current Partition	From the SP System Monitor GUI **SELECT** View → syspar This action can also be taken anywhere the View menu bar appears. **SELECT** indicates clicking on an icon or a menu choice. **PRESS** indicates a button press. → indicates a menu item sequence

Appendix B. Directory Information

The following table lists the directories created when you install the RS/6000 SP LPP image.

Table 10 (Page 1 of 2). RS/6000 SP LPP Images Directories

Directory	Contents
//etc/auto	automounter files
/etc/amd	amd files
/etc/ssp/css	css user space library
/spdata/sys1/st	Switch table API data files.
/spdata/sys1/err_methods	
/spdata/sys1/logtables	Sample service collection tables
/spdata/sys1/sdr	SDR database files
/spdata/sys1/spmon	hardmon internal security and threshold tables
/spdata/sys1/syspar_configs	System partition configuration files
/spdata/sys1/vsd	Partitioning data with regard to vsds
/usr/lpp/ssp/lib	ssp libraries.
/usr/lpp/ssp	Package files
/usr/lpp/ssp/amd	amd/amq files
/usr/lpp/ssp/bin	ssp command files
/usr/lpp/ssp/config	Setup file for switch, and so on.
/usr/lpp/ssp/config/admin	User mgmt SMIT stanzas
/usr/lpp/ssp/config/cmi	Cluster setup/management SMIT stanzas
/usr/lpp/ssp/css	Communication subsystem (css) files
/usr/lpp/ssp/css/diags	css diagnosis files
/usr/lpp/ssp/filec	File collection installation files
/usr/lpp/ssp/info	InfoExplorer setup files
/usr/lpp/ssp/inst_root	Root package files
/usr/lpp/ssp/install/bin	Configuration scripts
/usr/lpp/ssp/install/config	Install/config data and templates
/usr/lpp/ssp/lib	ssp libraries
/usr/lpp/ssp/perspectives	Perspectives files
/usr/lpp/ssp/kerberos/bin	Kerberos user commands
/usr/lpp/ssp/kerberos/etc	Kerberos daemons and privileged administrative commands
/usr/lpp/ssp/man	man page files
/usr/lpp/ssp/perl/bin	perl translation commands
/usr/lpp/ssp/perl/lib	perl functions and headers
/usr/lpp/ssp/perl/lib/sys	c headers converted to perl

© Copyright IBM Corp. 1995, 1997

Table 10 (Page 2 of 2). RS/6000 SP LPP Images Directories	
Directory	**Contents**
/usr/lpp/ssp/config/spmgrd	MIB files for SNMP manager
/usr/lpp/ssp/perl/man	perl man page files
/usr/lpp/ssp/rcmd/bin	Kerberos-authenticated remote commands
/usr/lpp/ssp/rcmd/etc	RS/6000 SP command daemon
/usr/lpp/ssp/public	Public tar files
/usr/lpp/ssp/samples	Sample scripts
/usr/lpp/ssp/sysctl/bin	Supported client code
/var/adm/acct	Created when accounting is configured on nodes.
/var/adm/cacct	Cluster consolidated accounting data
/var/adm/SPlogs	Logs and other run time data collectors
/var/adm/SPlogs/amd	amd logs
/var/adm/SPlogs/cs	Cluster startup/shutown logs
/var/adm/SPlogs/css	css logs
/var/adm/SPlogs/filec	File collection logs
/var/adm/SPlogs/kerberos	Kerberos server logs
/var/adm/SPlogs/sdr	System Data Repository logs
/var/adm/SPlogs/SPconfig	Vital product data information
/var/adm/SPlogs/spmon	SP System Monitor logs
/var/adm/SPlogs/sysctl	Sysctl server log file
/var/adm/SPlogs/sysman	Installation, configuration, and console logs
/var/adm/SPlogs/jm	Resource Manager logs.
/var/adm/SPlogs/st	Switch table API logs.
/var/adm/SPlogs/spmgr	Trace file for SNMP manager
/var/kerberos/database	Kerberos server database and other files

Appendix C. Sample script.cust File

This appendix contains a sample **script.cust** file, located in **/usr/lpp/ssp/samples**.

```
#!/bin/ksh
#####################################################################
#
# Module: <script.cust>
#
#--------------------------------------------------------------------
#
# Description: This script is a sample which is designed to be used
#   by the user as a guide for some functions that might be performed
#   after a node has been netinstalled, but before it boots for the
#   first time.
#
# If you want  to use some of the examples in this file, then you need
# to either copy the entire script to /tftpboot/script.cust and
# edit the lines you want to execute, or just copy over the portions
# of this sample that you want executed to /tftpboot/script.cust
#
#
#####################################################################

PATH=/bin:/usr/bin:/etc:/usr/sbin:/usr/bin/X11:/var/sysman
/etc:/etc/amd:/usr/lpp/ssp/bin:/usr/lpp/ssp/install/bin:
SSPDIR=/usr/lpp/ssp
SERVER= cat /etc/ssp/server_hostname | cut -d" " -f3
#
# Set the time zone
# use smit chtz to see the choices for time zones
# (EST5)           Eastern U.S.; Colombia  - daylight time unobserved
# (EST5EDT)        Eastern U.S.; Colombia  - daylight time observed
#chtz EST5EDT
#
#####################################################################
# Importing existing volume groups
#####################################################################
#
#importvg -y uservg hdisk1
#
# To activate a volume group use varyonvg.
#varyonvg uservg
#
#####################################################################
# if you are mirroring rootvg volume group, uncomment the following
# in order to preserve the disabling of volume group quorum across
# an install (using a mksysb image with rootvg mirrored).
#
# /usr/sbin/chvg -Qn rootvg
#
#
```

© Copyright IBM Corp. 1995, 1997

```
# defining name resolution
# name resolution is required on the nodes. If you have not created an
# image that contains a method for resolving hostnames and addresses,
# then one of these methods must be selected.
#############################################################################
#
#############################################################################
# To perform kerberos authenticated rcp use the ssp rcmdtgt to obtain
# a Kerberos ticket first.
#############################################################################
#
# Define the file that will store the ticket
#export KRBTKFILE=/tmp/tkt_rcmd$$
#
# Get the Kerberos ticket
#/usr/lpp/ssp/rcmd/bin/rcmdtgt
#
# If you are using /etc/resolv.conf to resolve hostnames and addresses
# then use this to copy the /etc/resolv.conf file from the boot/install
# server.
# Perform Kerberos authenticated rcp
#/usr/lpp/ssp/rcmd/bin/rcp $SERVER:/etc/resolv.conf /etc/resolv.conf
#
# If you are using the /etc/hosts file to resolve hostnames and addresses
# then use the following commands to copy and append the /etc/hosts
# file from the boot/install server
#
# Perform Kerberos authenticated rcp
#/usr/lpp/ssp/rcmd/bin/rcp $SERVER:/etc/hosts /tmp/hosts
#/bin/cat /tmp/hosts >>/etc/hosts
#/bin/rm /tmp/hosts
#
# Remove the ticket file
#/bin/rm $KRBTKFILE
#
# If you are using NIS to resolve hostnames and addresses then use the
# next section to define you NIS environment
#
#############################################################################
# defining nis domains, and clients
#############################################################################
#
# To set the NIS domainname use the domainname command.
# To list the NIS domainname, issue domainname with no parameters and it
# will list the NIS domainname.
#
#/usr/etc/yp/chypdom '-B' <NIS domainname>
#
#
# Configuring NIS servers is not possible during install because
# the srcmstr daemon is not running and therefore cannot start
# the required yp daemons for NIS servers at the time script.cust runs.
#
#
```

```
# Make this node an NIS client at next boot (not now)
#
#mkclient -I
#
#########################################################################
# installing other lpp's
# If you installed other lpp's on your system, made a mksysb image of
# that system, and are planning to install /usr clients from that mksysb
# image, you do not need to issue any installp commands here related to
# those lpp's.  The /usr parts will be available on your /usr server
# (assuming you installed the server with the same mksysb image), and the
# root parts will get updated automatically by the finishrclient script,
# which is run automatically after every /usr client is installed.
#########################################################################
#
# To install Fortran on a node create a backup image of the installp in
# the /usr/sys/inst.images/ssp directory of the control workstation and
# name it xlf.installp (make sure the installp image has read and execute
# permissions by all - chmod +rx xlf.installp).
#
# Check to see if fortran is already installed on this system
# if [[ -z  lslpp -h | grep xlf  ]]
# then
#  # Fortran not installed - Mount the installp image and perform the
# installp
# /usr/sbin/mount <control workstation address>:/usr/sys/inst.image
# [[ -f /mnt/pssp.installp ]] && installp -ac
#
#  # Unmount the installp image
#  /usr/sbin/unmount /mnt
#fi
#
#########################################################################
# Modifying page space
#########################################################################
#
# To make a new logical volume mypage for page space with 5 logical
# partitions (4 MB per partition - 20 MB total) on the volume group vg04,
# issue the mklv command.
# -t specifies the logical volume type (jfs, jfslog, or paging)
# -y specifies the name of the logical volume to be used instead of
# the system generated logical volume name(pagelvXX - where XX starts
# at 00 an  d increase by one).
# Use lsps -a to list all available paging space and its status.
#
#mklv -t paging -y mypage vg04 5
#
# To cause the /dev/mypage device to become available, use the swapon
# command.
#
#swapon /dev/mypage
#
# To change page space to be active on the next and subsequent reboots
# us the chps command.
```

```
# -a specifies to use page spae at next reboot
# y specifies to use page space at subsequent reboots
#
#chps -a y mypage
#
# Change the paging space - to add 100 logical partitions (400 MB )
# to mypage page space
# note: The default logical partition size is 4 MB.
# note: To use smit to change page space issue: smit chps
#
# Sample check to see if we are greater than what we are asking for
# NOTE: read comments for increasing logical volume space below
#
#num_pps_tox=100                # number of PPs to extend page space by
#
## determine cur size of mypage in PPs
#pps= /usr/sbin/lsps -c mypage | tail +2 | cut -d":" -f4
#if (( pps < num_pps_tox ))
#then
# chps -s$num_pps_tox mypage
#fi
#
# Create a 40 logical partition (default 4 MB partions - 160 MB) page
# space on the root volume group
# -a option actviates page space on subsequent reboots
# -n option actviates page space immediately
# -s option is the size of the page space in partitions
#
#mkps -s'40' -n -a rootvg
#
#########################################################################
# increasing logical volume space
#
# Code below is a sample test for increasing LV one time and for a large
# amount... If you need to extend for small amounts, uncomment just
# the extendlv command line or do the extend manually, but remember to
# comment it out for subsequent customizes; otherwise the LV will be
# extended by that amount on ALL customizes.
#
# Assumption: LV is a minimal size (4MB = 1PPs) and want it to be
# 160MB at initial install time ...
#########################################################################
#
## increasing logical volume space 40 logical partition (default 4 MB
## partions - 160 MB) pps -> physical partitions equate to logical
## partitions when LV is COPY=1
#
#num_pps_tox=100                  # number of PPs to extend LV by
#
## determine current number PPs in hd3
#cur_pps_str= lslv hd3 | grep "¬LPs" | cut -d":" -f2
#cur_pps=${cur_pps_str%%PP*}
#
#if (( num_pps_tox >= cur_pps ))   # already that big
```

```
#then
# extendlv hd3 $num_pps_tox        # extend by 100
#fi
#
#
#######################################################################
# increasing a filesystem size
#################################################################   ###
# NOTE: read comments above on increasing logical volume space ...
#
## increasing the /var filesystem by 4 MB
#
##check to see if we did the increase once, by checking size >
##extend amount
#
#increase=8192    # specified in 512 byte blocks; represents 4M increase
#fssize= /usr/sbin/lsfs -c /var | tail +2 | cut -d":" -f6
#if (( fssize < increase ))
#then
# chfs -a size=+$increase /var
#fi
#
#######################################################################
# changing the maximum number of of users that can be concurrently logged
# in according to the one-time AIX license fee for the system. The
# change is put into effect after the next restart of the system.
#######################################################################
#
#chlicense -u30
#
#######################################################################
#
# To set the allcast attribute of a Token Ring Network Interface to
# not confine broadcast to the local LAN:
#
# chdev -l tr0 -a allcast=off -P
#####################################################################
#
# Copy user management files from server to node.
# These are only some of the files that are copy over.
# The server address is gotten from the /etc/ssp/server_hostname file.
# If the server can not get to the correct files (passwd, group, etc)
# then place the correct ip address of where those files are in place
# of $SERVER.
#   (e.g.) /usr/bin/rcp -p 129.40.62.11:/etc/passwd /etc/passwd
# Check the /var/adm/SPlogs/sysman/<hostname>.config.log log
# file for errors
#####################################################################
#
# /usr/bin/rcp -p $SERVER:/etc/passwd /etc/passwd
# /usr/bin/rcp -p $SERVER:/etc/group /etc/group
# /usr/bin/rcp -p $SERVER:/etc/security/passwd /etc/security/passwd
# /usr/bin/rcp -p $SERVER:/etc/security/group /etc/security/group
# /usr/bin/rcp -p $SERVER:/etc/security/user /etc/security/user
```

Appendix D. Sample tuning.cust File

This appendix contains a sample **tuning.cust** file, located in **/usr/lpp/ssp/samples**. Additional IBM-supplied tuning files are available to set your performance parameters. One file is for the commercial environment, one is for the development environment, and one is for the scientific environment. For more information on these files, refer to the tuning section in the PSSP Administration Guide.

```
#!/bin/ksh
#"@(#)96 1.2.1.2 src/ssp/samples/tuning.cust, sysman, ssp_rloc 7/24/96
#####################################################################
#
# Module: <tuning.cust>
#--------------------------------------------------------------------
#
# Description: This script is a sample which is designed to be used
# by the user as a guide to change the network options for TCP/IP and
# UDP/IP communications on the SP system
#
# If you want to use some of the examples in this file, then you need
# to either copy the entire script to /tftpboot/tuning.cust and
# edit the lines you want to execute, or just copy over the portions
# of this sample that you want executed to /tftpboot/tuning.cust
#
# These settings are only a sample and should be changes to the preferred
# settings for your system.
#
# For further recommendations on tuning, refer to the Administration Guide
#--------------------------------------------------------------------
#
#   Set default mbuf pool size for all TCP/IP and thread buffer
#
#  /usr/sbin/no -o thewall=16384

#
#   Set default sb_max size for all IP connections
#
#  /usr/sbin/no -o sb_max=163840

#
#   Set default TCP send window size for all TCP/IP connections
#
#  /usr/sbin/no -o tcp_sendspace=65536

#
#   Set default TCP receive window size for all TCP/IP connections
#
#  /usr/sbin/no -o tcp_recvspace=65536

#
#   Set default UDP send window size for all UDP/IP connections
#   Effective maximum is limited to 65536
```

© Copyright IBM Corp. 1995, 1997

```
#
#  /usr/sbin/no -o udp_sendspace=32768

#
#   Set default UDP receive window size for all UDP/IP connections
#
#  /usr/sbin/no -o udp_recvspace=65536

#
#   Set rfc1323 feature on for faster throughput for High Performance Networks.
#
#  /usr/sbin/no -o rfc1323=1

#
#   Set default Maximum Transmission Unit size for transfers across networks.
#
#  /usr/sbin/no -o tcp_mssdflt=1448
#
#   Enable the kernel to forward packets
#
#  /usr/sbin/no -o ipforwarding=1
```

Appendix E. SAGE Job Descriptions

This appendix describes the job descriptions for the system administration levels discussed in “Who Should Use This Book” on page xvi.

The System Administrators Guide of USENIX (SAGE), a professional organization for system administrators, has developed a set of job descriptions for system administrators. The Core Templates described in this appendix describe the core set of attributes for system administrators. The “Additional Skill Areas” on page 240 provides details on additional skill areas that may be important to your site.

For more information, contact the USENIX Association or access the World Wide Web: **http://www.sage.usenix.org/sage/**.

Core Templates Defined by SAGE

The following are templates for the core skills required for Junior and Intermediate/Advanced System Administrators.

Junior System Administrator

Required skills

- Strong interpersonal and communication skills; capable of training users in applications and UNIX fundamentals, and writing basic documentation.
- Highly skilled in using most UNIX commands/utilities.
- Familiarity with most basic system administration tools and processes; for example, can boot/shutdown a machine, add and remove user accounts, use backup programs and fsck, maintain system database files (groups, hosts, aliases).
- Fundamental understanding of a UNIX-based operating system; for example, understands job control, soft and hard links, distinctions between the kernel and the shell.

Required Background

One to three years of system administration experience.

Desirable Background

- A degree in computer science or a related field.
- Familiarity with networked/distributed computing environment concepts; for example, can use the route command, add a workstation to a network, and mount remote filesystems.
- Ability to write scripts in some administrative language (Tk, Perl, and shell).
- Programming experience in any applicable language.

© Copyright IBM Corp. 1995, 1997

Appropriate Responsibilities

Administers a small site alone or assists in the administration of a larger system. Works under the general supervision of a system administrator or computer systems manager.

Intermediate/Advanced System Administrator

Required Skills

- Strong interpersonal and communication skills; capable of writing purchase justifications, training users in complex topics, making presentations to an internal audience, and interacting positively with upper management.
- Independent problem solving; self-direction.
- Is comfortable with most aspects of UNIX system administration; for example, configuration of mail systems, system installation and configuration, printing systems, fundamentals of security, installing third-party software.
- A solid understanding of a UNIX-based operating system; understands paging and swapping, interprocess communication, devices and what device drivers do, file system concepts ("inode", "superblock").
- Familiarity with fundamental networking/distributed computing environment concepts; can configure NFS and NIS, can use nslookup or dig to check information in the DNS, understands basic routing concepts.
- Ability to write scripts in some administrative language (Tk, Perl, and shell).
- Ability to do minimal debugging and modification of C programs.

Required Background

Three to five years system administration experience.

Desirable Background

- A degree in computer science or a related field.
- Significant programming background in any applicable language.

Appropriate Responsibilities

- Receives general instructions for new responsibilities from supervisor.
- Administers a midsized site alone or assists in the administration of a larger site.
- Initiates some new responsibilities and helps to plan for the future of the site/network.
- Manages novice system administrators or operators.
- Evaluates and/or recommends purchases; has strong influence on purchasing process.

Additional Skill Areas

Use this list to identify additional skill areas that may be important at your site.

Local Environment Experience

Experience with the specific operating systems, applications, or programming languages in use at the site (for example SunOS, AIX,

CAE/CAD software, FrameMaker, Mathematica, Fortran, Ada). Experience with the work done by the users at the site.

Heterogeneity Experience
Experience with more than one UNIX-based operating system. Experience with sites running more than one UNIX-based operating system. Familiarity with both System V and BSD-based UNIX operating systems. Experience with non-UNIX operating systems (for example, MS-DOS, Macintosh OS, or VMS). Experience with internetworking UNIX and other operating systems (MS-DOS, Macintosh OS, VMS).

Programming Skills
Extensive programming experience in an administrative language (Tk, Perl, and shell). Extensive programming experience in any applicable language.

Networking Skills
Experience configuring network file systems (for example, NFS, RFS, or AFS). Experience with network file synchronization schemes (for example, rdist and track). Experience configuring automounters. Experience configuring license managers. Experience configuring NIS/NIS+. Experience with TCP/IP networking protocols (ability to debug and program at the network level). Experience with non-TCP/IP networking protocols (for example, OSI, Chaosnet, DECnet, Appletalk, Novell Netware, Banyan Vines). Experience with high-speed networking (for example, FDDI, ATM, or SONET). Experience with complex TCP/IP networks (networks that contain routers). Experience with highly complex TCP/IP networks (networks that contain multiple routers and multiple media). Experience configuring and maintaining routers. Experience maintaining a site-wide modem pool/terminal servers. Experience with X/X terminals. Experience with dial-up networking (for example, SLIP, PPP, or UUCP). Experience at a site that is connected to the Internet. Experience installing/configuring DNS/BIND. Experience installing/administering Usenet news. Experience as postmaster of a site with external connections.

Security Experience with network security (for example, building firewalls, deploying authentication systems, or applying cryptography to network applications). Experience with classified computing. Experience with multi-level classified environments. Experience with host security (for example, passwords, uids/gids, file permissions, file system integrity, use of security packages).

Site Specialities
Experience at sites with over 1000 computers, over 1000 users, or over a terabyte of disk space. Experience with supercomputers. Experience coordinating multiple independent computer facilities (for example, working for the central group at a large company or university). Experience with a site with 100% uptime requirement. Experience developing/implementing a site disaster recovery plan. Experience with a site requiring charge-back accounting.

Documentation
Background in technical publications, documentation, or desktop publishing.

Databases

Experience using relational databases. Experience using a database query language. Experience programming in a database query language. Previous experience as a database administrator.

Hardware

Experience installing and maintaining the network cabling in use at the site. Experience installing boards and memory into systems. Experience with SCSI device setup and installation. Experience installing/configuring peripherals (for example, disks, modems, printers, or data acquisition devices). Experience with board-level diagnosis and repair of computer systems. Experience with component-level diagnosis and repair of computer system.

Management

Budget responsibility. Experience in writing personnel reviews, and ranking processes. Experience in interviewing and hiring.

Appendix F. Boot/Install Server Configuration Commands

This appendix lists the names of the boot/install server configuration commands which make up setup_server. For more information on these commands, refer to the *Commands and Technical Reference*.

Table 11. Boot/Install Server Configuration Commands

Command	**Description.**
allnimres	Allocates NIM resources from NIM server to client and prepares the client node for boot/installation.
unallnimres	Unallocates NIM resources from NIM server to client.
mknimclient	Makes a node a NIM client of it's boot server as specified in the SDR.
delnimclient	Deletes the NIM client definition of a node on it's boot server.
mknimmast	Configures a node as a NIM master.
delnimmast	Unconfigures a node as a NIM master.
mknimint	Creates the necessary interfaces on a NIM master.
mknimres	Creates the necessary NIM resources on a NIM master.
mkconfig	Creates the config.info file on the server (must run on the server)
mkinstall	Creates the install.info file on the server (must run on the server)
setup_CWS	Setup the necessary files and other conditions on the control workstation.
create_krb_files	Creates the necessary Kerberos and tftp access files on a boot server.
export_clients	Exports required file systems from a NIM master to its clients.
setup_server	Sets up a boot/install server (same function, different internals).

© Copyright IBM Corp. 1995, 1997

Appendix G. Reserving Ports

The availability infrastructure, consisting of Topology Services (TS), Group Services (GS) and Event Management (EM), and Performance Toolbox Parallel Extensions (PTPE), allocate port numbers from the range 10000 to 10100, inclusive. TS, GS, and EM allocate port numbers when they are configured on the control workstation.

- TS and GS allocate one port number per system partition.
- PM allocates one port number per system partition plus one.
- PTPE allocates one port number when it is installed.

If a port number from this range is already listed in **/etc/services** on the control workstation, then these subsystems try another port number. Therefore, if any customer subsystem uses port numbers in the range 10000-10100, such port numbers must be reserved in **/etc/services** on the control workstation before TS, GS, EM and PTPE allocate port numbers.

Procedures

Topology Services, Group Services, Event Management and Performance Toolbox Parallel Extensions allocate their port numbers when their control scripts, respectively **hatsctrl**, **hagsctrl**, **haemctrl**, and **spdmdctrl**, are executed with the **-a** flag. Allocated port numbers are saved in the System Data Repository (SDR). If port numbers are found in the SDR from a previous invocation of a control script, then the saved port numbers are used and new values are not allocated.

When PTPE is installed, **spdmdctrl -a** is executed as part of post installation procedures. When the command **syspar_ctrl —A** is invoked, the **hatsctrl**, **hagsctrl**, and **haemctrl** scripts are invoked with the **-a** flag. As part of installation and migration procedures, syspar_ctrl —A is invoked. Specifically, it is invoked as part of the "Start System Partition-Sensitive Subsystems" step in chapter 2 of this book and in the migration chapter. If port numbers must be reserved in /etc/services, it must be done prior to installing PTPE and prior to "Start System Partition Sensitive-Subsystems" in chapter 2 or when preparing to migrate as described in chapter 4.

To reserve a port number, enter it in the /etc/services file on the control workstation using an editor or by invoking the smit clientnet command. The service name and protocol should be specified for the application or subsystem that is using the port number. If the application or subsystem does not run on the control workstation, then the port numbers can be reserved by using "dummy" service names. In the latter case, reserve the port number for use with both the **tcp** and **udp** protocols.

Considerations for Network Information Service (NIS)

If the control workstation is a NIS client, port numbers must be reserved using standard NIS procedures. This involves updating the NIS services map on the master server and any slave servers that serve the NIS domain to which the control workstation belongs. See the "Network Information Service" chapter of "AIX Version 4 System Management Guide: Communications and Networks", SC23–2526, for the procedures to update NIS maps.

© Copyright IBM Corp. 1995, 1997

Resolving Port Number Conflicts

It may be the case that at the time PTPE is installed or the availability infrastructure sybsystems are configured, you do not know that an application or subsystem you intend to install later is also using port numbers in the range 10000 through 10100. You do not reserve the port these port numbers, which leads to a conflict at a later time. If the application or subsystem cannot be configured to use a different port number, the port numbers used by PTPE and or the availability infrastructure subsystems can be re-allocated to avoid any conflict. Use the following procedure:

1. Execute the following commands on each node, in the order listed:

   ```
   haemctrl –c
   hagsctrl –c
   hatsctrl –c
   spdmdctrl –c  (only if PTPE is installed)
   ```

2. Execute the following commands on the control workstation, in the order listed:

   ```
   haemctrl –u
   hagsctrl –u
   hatsctrl –u
   spdmdctrl –u  (only if PTPE is installed)
   ```

   The —u flag is the same as the —c flag of these scripts with the addition of removing the subsystem's port numbers from the SDR. Note that a PTF for PTPE including APAR IX68352 must be installed in order to execute the —u flag on the spdmdctrl script.

   Caution: Steps 1 and 2 must execute successfully before proceeding.

3. Reserve the port numbers needed by your application or subsystem.

4. Execute the following commands, first on the control workstation and then on each node, in the order listed:

   ```
   hatsctrl –a
   hatsctrl –s

   hagsctrl –a
   hagsctrl –s

   haemctrl –a
   haemctrl –s

   spdmdctrl –a (only if PTPE is installed)
   spdmdctrl –s (only if PTPE is installed)
   ```

Glossary of Terms and Abbreviations

This glossary includes terms and definitions from:

- The *IBM Dictionary of Computing*, New York: McGraw-Hill, 199
- The *American National Standard Dictionary for Information Systems*, ANSI X3.172-1990, copyright 1990 by the American Institute (ANSI). Copies can be purchased from the American National Standards Institute, 1430 Broadway, New York, New York 10018. Definitions are identified by the symbol (A) after the definition.
- The *ANSI/EIA Standard - 440A: Fiber Optic Terminology*, copyright 1989 by the Electronics Industries Association (EIA be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue N.W., Washington, D.C. 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary* developed by Subcommittee 1 International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.

The following cross-references are used in this glossary:

> **Contrast with.** This refers to a term that has an opposed or substantively different meaning.
> **See.** This refers the reader to multiple-word terms in which this term appears.
> **See also.** This refers the reader to terms that have a related, but not synonymous, meaning.
> **Synonym for.** This indicates that the term has the same meaning as a preferred term, which is defined in the glossary.

This section contains some of the terms that are commonly used in the SP publications.

IBM is grateful to the American National Standards Institute (ANSI) for permission to reprint its definitions from the American National Standard *Vocabulary for Information Processing* (Copyright 1970 by American Nat which was prepared by Subcommittee X3K5 on Terminology and Glossary of the American National Standards Committee X3. ANSI definitions are preceded by an asterisk (*).

Other definitions in this glossary are taken from *IBM Vocabulary for Data Processing, Telecommunications, and Office Systems* (SC20-1699) and *IBM DATABASE 2 Guide for TSO Users* (SC26-4081).

A

address. A character or group of characters that identifies a register, a device, a particular part of storage, or some other data source or destination.

AFS. A distributed file system that provides authentication services as part of its file system creation.

AIX. Abbreviation for Advanced Interactive Executive, IBM's licensed version of the UNIX operating system. AIX is particularly suited to support technical computing applications, including high function graphics and floating point computations.

AIX Version 3. The IBM AIX Version 3 for RISC System/6000 (also known as AIX/6000). It is based on UNIX System V, conforms with POSIX IEEE Standard 1003.1, is compatible with Berkeley Software Distribution 4.3 (4.3 BSD), and is designed to meet Trusted Computing Base level C2 security.

Amd. Berkeley Software Distribution automount daemon.

API. Application Programming Interface. A set of programming functions and routines that provide access between the Application layer of the OSI seven-layer model and applications that want to use the network. It is a software interface.

application. The use to which a data processing system is put; for example, a payroll application, an airline reservation application.

application data. The data that is produced using an application program.

ARP. Address Resolution Protocol.

ATM. Asynchronous Transfer Mode. (See *TURBOWAYS 100 ATM Adapter*.)

Authentication. The process of validating the identity of a user or server.

Authorization. The process of obtaining permission to perform specific actions.

© Copyright IBM Corp. 1995, 1997

B

batch processing. * (1) The processing of data or the accomplishment of jobs accumulated in advance in such a manner that each accumulation thus formed is processed or accomplished in the same run. * (2) The processing of data accumulating over a period of time. * (3) Loosely, the execution of computer programs serially. (4) Computer programs executed in the background.

BMCA. Block Multiplexer Channel Adapter. The block multiplexer channel connection allows the RISC System/6000 to communicate directly with a host System/370 or System/390; the host operating system views the system unit as a control unit.

C

call home function. The ability of a system to call the IBM support center and open a PMR to have a repair scheduled.

charge feature. An optional feature for either software or hardware for which there is a charge.

CLI. Command Line Interface.

client. * (1) A function that requests services from a server and makes them available to the user. * (2) A term used in an environment to identify a machine that uses the resources of the network.

Client Input/Output Sockets (CLIO/S). A software package that enables high-speed data and tape access between SP systems, AIX systems, and ES/9000 mainframes.

CLIO/S. Client Input/Output Sockets.

CMI. Centralized Management Interface provides a series of SMIT menus and dialogues used for defining and querying the SP system configuration.

connectionless. A communication process that takes place without first establishing a connection.

connectionless network. A network in which the sending logical node must have the address of the receiving logical node before information interchange can begin. The packet is routed through nodes in the network based on the destination address in the packet. The originating source does not receive an acknowledgment that the packet was received at the destination.

control workstation. A single point of control allowing the administrator or operator to monitor and manage the SP system using the IBM AIX Parallel System Support Programs.

D

daemon. A process, not associated with a particular user, that performs system-wide functions such as administration and control of networks, execution of time-dependent activities, line printer spooling and so forth.

DASD. Direct Access Storage Device. Storage for input/output data.

DCE. Distributed Computing Environment.

DFS. Distributed File System. A subset of the IBM Distributed Computing Environment.

DNS. Domain Name Service. A hierarchical name service which maps high level machine names to IP addresses.

E

Error Notification Object. An object in the SDR that is matched with an error log entry. When an error log entry occurs that matches the Notification Object, a user-specified action is taken.

ESCON. Enterprise Systems Connection. The ESCON channel connection allows the RISC System/6000 to communicate directly with a host System/390; the host operating system views the system unit as a control unit.

Ethernet. (1) Ethernet is the standard hardware for TCP/IP local area networks in the UNIX marketplace. It is a 10-megabit per second baseband type LAN that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by collision detection (CSMA/CD). (2) A passive coaxial cable whose interconnections contain devices or components, or both, that are all active. It uses CSMA/CD technology to provide a best-effort delivery system.

Ethernet network. A baseband LAN with a bus topology in which messages are broadcast on a coaxial cabling using the carrier sense multiple access/collision detection (CSMA/CD) transmission method.

event. An action that takes place in the operation of the system software.

expect. Programmed dialogue with interactive programs.

F

Failover. Also called fallover, the sequence of events when a primary or server machine fails and a secondary or backup machine assumes the primary workload. This is a disruptive failure with a short recovery time.

fall back. Also called fall back, the sequence of events when a primary or server machine takes back control of its workload from a secondary or backup machine.

FDDI. Fiber Distributed Data Interface.

Fiber Distributed Data Interface (FDDI). An American National Standards Institute (ANSI) standard for 100-megabit-per-second LAN using optical fiber cables. An FDDI local area network (LAN) can be up to 100 km (62 miles) and can include up to 500 system units. There can be up to 2 km (1.24 miles) between system units and/or concentrators.

File Transfer Protocol (FTP). The Internet protocol (and program) used to transfer files between hosts. It is an application layer protocol in TCP/IP that uses TELNET and TCP protocols to transfer bulk-data files between machines or hosts.

file. * A set of related records treated as a unit, for example, in stock control, a file could consist of a set of invoices.

file server. A centrally located computer that acts as a storehouse of data and applications for numerous users of a local area network.

foreign host. Any host on the network other than the local host.

FTP. File transfer protocol.

G

gateway. An intelligent electronic device interconnecting dissimilar networks and providing protocol conversion for network compatibility. A gateway provides transparent access to dissimilar networks for nodes on either network. It operates at the session presentation and application layers.

H

HACMP/6000. AIX High Availability Cluster Multi-Processing/6000.

HACWS. High Availability Control Workstation function, based on HACMP/6000, provides for a backup control workstation for the SP system.

help key. In the SP graphical interface, the key that gives you access to the SP graphical interface help facility.

High Availability Cluster Multi-Processing/6000. An IBM facility to cluster nodes or components to provide high availability by eliminating single points of failure.

High Performance Switch. An IBM multi-stage packet switch for high-performance communication between processor nodes.

HiPPI. High Performance Parallel Interface. RISC System/6000 units can attach to a HiPPI network as defined by the ANSI specifications. The HiPPI channel supports burst rates of 100 Mbps over dual simplex cables; connections can be up to 25 km in length as defined by the standard and can be extended using third-party HiPPI switches and fiber optic extenders.

home directory. The directory associated with an individual user.

host. A computer connected to a network, and providing an access method to that network. A host provides end-user services.

HSD. The data striping device for the IBM Recoverable Virtual Shared Disk. The device driver lets application programs stripe data across physical disks in multiple IBM Virtual Shared Disks, thus reducing I/O bottlenecks and hot spots.

I

Internet. A specific inter-network consisting of large national backbone networks such as APARANET, MILNET, and NSFnet, and a myriad of regional and campus networks all over the world. The network uses the TCP/IP protocol suite.

Intermediate Switch Board. Switches mounted in the High Performance Switch expansion frame.

IP address. A 32-bit address assigned to devices or hosts in an IP internet that maps to a physical address. The IP address is composed of a network and host portion.

Internet Protocol (IP). (1) A protocol that routes data through a network or interconnected networks. IP acts as an interface between the higher logical layers and the physical network. This protocol, however, does not provide error recovery, flow control, or guarantee the reliability of the physical network. IP is a connectionless protocol. (2) A protocol used to route data from its source to it destination in an Internet environment.

ISB. Intermediate Switch Board.

K

Kerberos. A service for authenticating users in a network environment.

kernel. The core portion of the UNIX operating system which controls the resources of the CPU and allocates them to the users. The kernel is memory-resident, is said to run in “kernel mode” and is protected from user tampering by the hardware.

L

LAN. (1) Acronym for Local Area Network, a data network located on the user's premises in which serial transmission is used for direct data communication among data stations. (2) Physical network technology that transfers data a high speed over short distances. (3) A network in which a set of devices is connected to another for communication and that can be connected to a larger network.

local host. The computer to which a user's terminal is directly connected.

log database. A persistent storage location for the logged information.

log event. The recording of an event.

log event type. A particular kind of log event that has a hierarchy associated with it.

logging. The writing of information to persistent storage for subsequent analysis by humans or programs.

M

mask. To use a pattern of characters to control retention or elimination of portions of another pattern of characters.

menu. A display of a list of available functions for selection by the user.

Motif. The graphical user interface for OSF, incorporating the X Window System. Also called OSF/Motif.

MTBF. Mean time between failure. This is a measure of reliability.

MTTR. Mean time to repair. This is a measure of serviceability.

N

naive application. An application with no knowledge of a server that fails over to another server. Client to server retry methods are used to reconnect.

network. An interconnected group of nodes, lines, and terminals. A network provides the ability to transmit data to and receive data from other systems and users.

NFS. Network File System. NFS allows different systems (UNIX or non-UNIX), different architectures, or vendors connected to the same network, to access remote files in a LAN environment as though they were local files.

NIM. Network Installation Management is provided with AIX 4.1 to install AIX on the nodes.

NIM client. An AIX system installed and managed by a NIM master. NIM supports three types of clients:

- Standalone
- Diskless
- Dataless

NIM master. An AIX system that can install one or more NIM clients. An AIX system must be defined as a NIM master before defining any NIM clients on that system. A NIM master managers the configuration database containing the information for the NIM clients.

NIM object. A representation of information about the NIM environment. NIM stores this information as objects in the NIM database. The types of objects are:

- Network
- Machine
- Resource

NIS. Network Information System.

node. In a network, the point where one or more functional units interconnect transmission lines. A computer location defined in a network.

Node Switch Board. Switches mounted on frames that contain nodes.

NSB. Node Switch Board.

NTP. Network Time Protocol.

P

parallel environment. A system environment where message passing or SP resource manager services are used by they application.

Parallel Environment. A licensed IBM program used for message passing applications on the SP or RISC System/6000 platforms.

parallel processing. A multiprocessor architecture which allows processes to be allocated to tightly coupled multiple processors in a cooperative processing environment, allowing concurrent execution of tasks.

parameter. * (1) A variable that is given a constant value for a specified application and that may denote the application. * (2) An item in a menu for which the operator specifies a value or for which the system provides a value when the menu is interpreted. * (3) A name in a procedure that is used to refer to an argument that is passed to the procedure. * (4) A particular piece of information that a system or application program needs to process a request.

partition. See system partition.

Perl. Practical Extraction and Report Language.

pipe. A UNIX utility allowing the output of one command to be the input of another. Represented by the | symbol. It is also referred to as filtering output.

port. (1) An end point for communication between devices, generally referring to physical connection. (2) A 16-bit number identifying a particular TCP or UDP resource within a given TCP/IP node.

process. * (1) A unique, finite course of events defined by its purpose or by its effect, achieved under defined conditions. * (2) Any operation or combination of operations on data. * (3) A function being performed or waiting to be performed. * (4) A program in operation. For example, a daemon is a system process that is always running on the system.

protocol. A set of semantic and syntactic rules that defines the behavior of functional units in achieving communication.

PMR. Problem Management Report.

Problem Management Report. The number in the IBM support mechanism that represents a service incident with a customer.

Primary node or machine. (1) A device that runs a workload and has a standby device ready to assume the primary workload if that primary node fails or is taken out of service. (2) A node on the High Performance Switch that initializes, provides diagnosis and recovery services, and performs other operations to the switch network. (3) In IBM Virtual Shared Disk function, the node at which the logical volume is actually local and that acts as server node to I/O requests from other nodes.

R

RAID. Redundant array of independent disks.

remote host. *See foreign host*.

RISC. Reduced Instruction Set Computing (RISC), the technology for today's high performance personal computers and workstations, was invented in 1975. Uses a small simplified set of frequently used instructions for rapid execution.

rlogin (remote LOGIN). A service offered by Berkeley UNIX systems that allows authorized users of one machine to connect to other UNIX systems across a network and interact as if their terminals were connected directly. The rlogin software passes information about the user's environment (for example, terminal type) to the remote machine.

RPC. Acronym for Remote Procedure Call, a facility that a client uses to have a server execute a procedure call. This facility is composed of a library of procedures plus an XDR.

RSH. A variant of RLOGIN command that invokes a command interpreter on a remote UNIX machine and passes the command line arguments to the command interpreter, skipping the LOGIN step completely. See also *rlogin*.

S

SCSI. Small Computer System Interface.

server. (1) A function that provides services for users. A machine may run client and server processes at the same time. (2) A machine that provides resources to the network. It provides a network service, such as disk storage and file transfer, or a program that uses such a service. (3) A device, program, or code module on a network dedicated to providing a specific service to a network. (4) On a LAN, a data station that provides facilities to other data stations. Examples are file server, print server, and mail server.

Small Computer System Interface (SCSI). An input and output bus that provides a standard interface for the attachment of various direct access storage devices (DASD) and tape drives to the RISC System/6000.

shell. The shell is the primary user interface for the UNIX operating system. It serves as command language interpreter, programming language, and allows foreground and background processing. There are three different implementations of the shell concept: Bourne, C and Korn.

Small Computer Systems Interface Adapter (SCSI Adapter). An adapter that supports the attachment of various direct-access storage devices (DASD) and tape drives to the RISC System/6000.

SMIT. The System Management Interface Toolkit is a set of menu driven utilities for AIX that provides functions such as transaction login, shell script creation, automatic updates of object database, and so forth.

SNMP. Simple Network Management Protocol. (1) An IP network management protocol that is used to monitor attached networks and routers. (2) A TCP/IP-based protocol for exchanging network management information and outlining the structure for communications among network devices.

socket. (1) An abstraction used by Berkeley UNIX that allows an application to access TCP/IP protocol functions. (2) An IP address and port number pairing. (3) In TCP/IP, the Internet address of the host computer on which the application runs, and the port number it uses. A TCP/IP application is identified by its socket.

standby node or machine. A device that waits for a failure of a primary node in order to assume the identity of the primary node. The standby machine then runs the primary's workload until the primary is back in service.

subnet. Shortened form of subnetwork.

subnet mask. A bit template that identifies to the TCP/IP protocol code the bits of the host address that are to be used for routing for specific subnetworks.

subnetwork. Any group of nodes that have a set of common characteristics, such as the same network ID.

supervisor basecode. Microcode that is loaded at time of manufacture and gives the card the ability to load supervisor microcode during system operation.

supervisor microcode. Microcode that is loaded via supervisor basecode and contains the instruction that is the supervisor application.

supervisor microcode files. Files whose content is supervisor microcode. These files reside on the control workstation.

SUP. Software Update Protocol.

Sysctl. Secure System Command Execution Tool. An authenticated client/server system for running commands remotely and in parallel.

System Administrator. The user who is responsible for setting up, modifying, and maintaining the SP system.

subsystem. A software component that is not usually associated with a user command. It is usually a daemon process. A subsystem will perform work or provide services on behalf of a user request or operating system request.

syslog. A BSD logging system used to collect and manage other subsystem's logging data.

system partition. A group of nonoverlapping nodes on a switch chip boundary that act as a logical SP system.

T

tar. Tape ARchive, is a standard UNIX data archive utility for storing data on tape media.

Tcl. Tool Command Language.

TclX. Tool Command Language Extended.

TCP. Acronym for Transmission Control Protocol, a stream communication protocol that includes error recovery and flow control.

TCP/IP. Acronym for Transmission Control Protocol/Internet Protocol, a suite of protocols designed to allow communication between networks regardless of the technologies implemented in each network. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the underlying protocol is the Internet Protocol.

Telnet. Terminal Emulation Protocol, a TCP/IP application protocol that allows interactive access to foreign hosts.

Tk. Tcl-based Tool Kit for X Windows.

TMPCP. Tape Management Program Control Point.

token-ring. (1) Network technology that controls media access by passing a token (special packet or frame) between media-attached machines. (2) A network with a ring topology that passes tokens from one attaching device (node) to another. (3) The IBM Token-Ring LAN connection allows the RISC System/6000 system unit to participate in a LAN adhering to the IEEE 802.5 Token-Passing Ring standard or the ECMA standard 89 for Token-Ring, baseband LANs.

transaction. An exchange between the user and the system. Each activity the system performs for the user is considered a transaction.

transceiver (transmitter-receiver). A physical device that connects a host interface to a local area network, such as Ethernet. Ethernet transceivers contain electronics that apply signals to the cable and sense collisions.

transfer. To send data from one place and to receive the data at another place. Synonymous with move.

transmission. * The sending of data from one place for reception elsewhere.

TURBOWAYS 100 ATM Adapter. An IBM high-performance, high-function intelligent adapter that provides dedicated 100 Mbps ATM (asynchronous transfer mode) connection for high-performance servers and workstations.

U

UDP. User Datagram Protocol.

User Datagram Protocol (UDP). (1) In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. UDP is used for application-to-application programs between TCP/IP host systems. (2) A transport protocol in the Internet suite of protocols that provides unreliable, connectionless datagram service. (3) The Internet Protocol that enables an application programmer on one machine or process to send a datagram to an application program on another machine or process.

UNIX operating system. An operating system developed by Bell Laboratories that features multiprogramming in a multiuser environment. The UNIX operating system was originally developed for use on minicomputers, but has been adapted for mainframes and microcomputers. **Note:** The AIX operating system is IBM's implementation of the UNIX operating system.

user. Anyone who requires the services of a computing system.

user ID. A nonnegative integer, contained in an object of type *uid_t*, that is used to uniquely identify a system user.

V

Virtual Shared Disk, IBM. The function that allows application programs executing at different nodes of a system partition to access a raw logical volume as if it were local at each of the nodes. In actuality, the logical volume is local at only one of the nodes (the server node).

W

workstation. * (1) A configuration of input/output equipment at which an operator works. * (2) A terminal or microcomputer, usually one that is connected to a mainframe or to a network, at which a user can perform applications.

X

X Window System. A graphical user interface product.

Index

A

adapters xxii
adding 27
  frame 25, 181
  nodes 186
  switch 196
Amd issues 113
applying ptfs to the system 221
authentication 20, 30
  initialize as an authentication client system 36
  initialize as the primary authentication server 31
  initialize as the secondary authentication server 34
  initialize to use AFS authentication 37
  initializing SP authentication services
    as the authentication client system 20, 94
Automount issues 113

B

basic AIX image
  installing 6
  working with the 6
bffcreate command 25, 26
boot/install server
  configure boot/install server as NIM master 10
  configure control workstation as boot/install
    server 61
building an installation image 218

C

chdev command 16
chfs command 23
coexistence 3
commands 26, 39, 40, 52, 54
  CSS_test 209
  dsh 218
  Eannotator 38, 203
  Eclock 206
  Eprimary 39, 205
  Estart 40, 208
  Etopology 39, 204
  spbootins
    propagating installation image 54, 221
  spdelfram 26, 185
  spdelnode 189, 195
configuration 23, 26, 42
  reconfiguring RS/6000 SP 27, 30, 31, 40
    adding a frame 181
    adding a switch 196
    adding nodes 186
    deleting a frame 26, 184
    deleting nodes 27, 188
configuration *(continued)*
  reconfiguring RS/6000 SP *(continued)*
    replacing a fixed disk 41, 209
    replacing Ethernet adapter 43, 212
    replacing I/O planar card 212
    replacing nodes with different node 193
    replacing nodes with equivalent node 29, 190
configuring
  High Availability Control Workstation 18, 87
control workstation, restoring from a mksysb
  image 223
css option, updating 216
CSS_test command 40, 209
customization 4

D

deleting 26
  frame 183
  nodes 27, 188
directories created during installation 58, 229
disk, fixed 41
  replacing 209
documentation xvii, 30
dsh command 53, 218

E

Eclock command 40, 206
Eprimary command 39, 205
Estart command 208
Ethernet adapter
  replacing 44, 212
Etopology command 39, 204
extension nodes 1

F

first boot customization file (script.cust)
  sample file 61, 231
first boot customization file (tuning.cust)
  sample file 61, 237
fixed disk 41
  replacing 209
fixed disk, replacing a 210
frame supervisor 40, 209
frames 25, 26
  adding 25, 181
  deleting 26, 184
  spdelfram command 185

© Copyright IBM Corp. 1995, 1997

G
graphical user interface xvii

H
High Availability Control Workstation, installing and configuring 87
High Performance Switch 196
High Performance Switch-LC8 187
HTML 30

I
I/O planar card 43
  replacing 43, 212
IBM Virtual Shared Disk xix
install_cw command 2, 39
installating a new system 11
installation
  directories creating during 229
installation images 53
  building 218
  propagation 54, 221
installation overview 1
installing
  program updates 215
installing and configuring the High Availability Control Workstation 87
IP address aliases 104

K
Kerberos principal 91

L
login control 85
LPP images 9
lppsource, directory of installable LPP images 9

M
machine objects 8
maintenance
  installing program updates 47, 215
manual pages for public code xxiii
microcode update process 44
migrating
  HACWS migration strategy 164
  overwrite/preservation install 158
  paths to migrate the control workstation 115
  paths to migrate the nodes 145
  post-migration activity 177
  recovery procedures 177
  to the latest level of PSSP 106
migration 200
migration install 3
mkdev command 16
mklv command 22
mksysb, adding one to the control workstation 217
mksysb, replacing one on the control workstation 50, 217
mksysb, restoring the control workstation 50, 217
mksysb, restoring the node 217
mkvg command 22

N
netinstall image testing on a single node 54, 220
network adapters 16
Network Installation Manager (NIM) 3
Network Time Protocol (NTP) xiv
NIM client 3
NIM master 3
NIM objects
  Machine 8
  Network 8
  Resource 8
node 29
  replacing 29, 190, 193
nodes 27, 47
  adding 186
  deleting 27, 188
  replacing with different 30, 193
  replacing with equivalent 29, 190
  software maintenance on down nodes 216
  updating 217

O
Objects
  Machine 8
  Network 8
  Resource 8
overview of installation 1
overwrite install 3
overwrite/preservation install 158

P
partition-senstive subsystems, starting 54
partition-senstive subsystems, verifying 55
per node 50
  basis updating 217
per-node
  update installation 47, 215
perl scripts 243
Perspectives xvii, 2, 225
port numbers 245
prepare the control workstations 19, 88

print management programs 49
updating 217
print subsystem
updating 49, 217
printing documentation xvii
program update installation 215
propagating an installation image 54, 221
PSSP
reinstalling 49, 216
ptfs to the system, applying 56, 221

R

reconfiguring a system for use with the SP Switch 37, 200
reinstall update installation 47, 215
reinstallation 218
reinstalling PSSP 216
replacing 42, 44
an I/O planar card in a node 212
Ethernet microchannel adapter 45, 212
fixed disk 42, 210
I/O planar card 212
replacing a frame supervisor 209
restoring a control workstation from makesysb image 223
RS-232 control lines 90

S

SAGE
system administrator descriptions 62, 239
sample files
script.cust 231
tuning.cust 61, 237
Scalable POWERparallel Switch-8 (SP Switch-8) 196
script.cust 59
sample file 59, 231
serial adapter 97
service
installing 215
software maintenance 45, 47, 53, 215
installing program updates 47, 215
updating through reinstallation 53, 218
SP Switch 200
SP Switch-8 187
SP system
applying ptfs to the 56, 221
spbootins command
propagating installation image 221
spdelfram command 185
spdelnode command 28, 189, 195
ssp.docs 30
supervisor microcode update process 44
switch
adding 34, 196
switch topology file
storing in the SDR 38, 203
Switches
High Performance Switch 196
Scalable POWERparallel Switch-8 (SP Switch-8) 196
system administration
SAGE job descriptions 62, 239
System Administrators Guide of USENIX, see SAGE 239
System Monitor Graphical User Interface xviii, 2, 58, 225

T

thin node
replacing I/O planar card 44, 212
time service choices 41
token ring-bridge gateway 76
topology file, selecting 65
trademarks xiii
tunable values 120
tuning.cust 61
sample file 61, 237

U

updating 49, 50
on a per node basis 217
the css option 216
the print subsystem 217

V

varyonvg command 22
verification
cluster software 97
netinstall image 220
node verification test 78
SDR and System Monitor test 39
switch verification test 79

W

wide node 44
replacing Ethernet adapter 212
Worm software 64

Communicating Your Comments to IBM

IBM Parallel System Support
Programs for AIX
Installation and Migration Guide

Publication No. GC23-3898-04

If you especially like or dislike anything about this book, please use one of the methods listed below to send your comments to IBM. Whichever method you choose, make sure you send your name, address, and telephone number if you would like a reply.

Feel free to comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. However, the comments you send should pertain to only the information in this manual and the way in which the information is presented. To request additional publications, or to ask questions or make comments about the functions of IBM products or systems, you should talk to your IBM representative or to your IBM authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

If you are mailing an RCF from a country other than the United States, you can give the RCF to the local IBM branch office or IBM representative for postage-paid mailing.

- If you prefer to send comments by mail, use the RCF at the back of this book.
- If you prefer to send comments by FAX, use this number:
  - FAX: (International Access Code)+1+914+432-9405
- If you prefer to send comments electronically, use this network ID:
  - IBMLink: (United States customers only): KGNVMC(MHVRCFS)
  - IBM Mail Exchange: USIB6TC9 at IBMMAIL
  - Internet e-mail: mhvrcfs@vnet.ibm.com
  - World Wide Web: http://www.s390.ibm.com/os390

Make sure to include the following in your note:

- Title and publication number of this book
- Page number or topic to which your comment applies

Optionally, if you include your telephone number, we will be able to respond to your comments by phone.

Reader's Comments — We'd Like to Hear from You

IBM Parallel System Support
Programs for AIX
Installation and Migration Guide

Publication No. GC23-3898-04

You may use this form to communicate your comments about this publication, its organization, or subject matter, with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you. Your comments will be sent to the author's department for whatever review and action, if any, are deemed appropriate.

Note: Copies of IBM publications are not stocked at the location to which this form is addressed. Please direct any requests for copies of publications, or for assistance in using your IBM system, to your IBM representative or to the IBM branch office serving your locality.

Today's date: _____

What is your occupation?

Newsletter number of latest Technical Newsletter (if any) concerning this publication:

How did you use this publication?

[ ]	As an introduction	[ ]	As a text (student)
[ ]	As a reference manual	[ ]	As a text (instructor)
[ ]	For another purpose (explain)		

Is there anything you especially like or dislike about the organization, presentation, or writing in this manual? Helpful comments include general usefulness of the book; possible additions, deletions, and clarifications; specific errors and omissions.

Page Number: Comment:

Name

Address

Company or Organization

Phone No.

Reader's Comments — We'd Like to Hear from You
GC23-3898-04

Cut or Fold
Along Line

Fold and Tape | **Please do not staple** | Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Department 55JA, Mail Station P384
522 South Road
Poughkeepsie NY 12601-5400

Fold and Tape | **Please do not staple** | Fold and Tape

Cut or Fold
Along Line

Program Number: 5765-529

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GC23-3898-04